Dr. Agus Wibowo, M.Kom, M.Si, MM.

Manajemen Kedaulatan Jaringan Siber

YAYASAN PRIMA AGUS TEKNIK

Manajemen Kedaulatan Jaringan Siber

Dr. Agus Wibowo, M.Kom, M.Si, MM.

YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

ISBN 978-623-8642-28-1 (PDF)

Manajemen Kedaulatan Jaringan Siber

Penulis :
Dr. Agus Wibowo, M.Kom, M.Si, MM.

ISBN : 987-623-8642-28-1

Editor :
Dr. Joseph Teguh Santoso, S.Kom., M.Kom.

Penyunting :
Dr. Mars Caroline Wibowo. S.T., M.Mm.Tech

Desain Sampul dan Tata Letak :
Irdha Yunianto, S.Ds., M.Kom

Penebit :
Yayasan Prima Agus Teknik Bekerja sama dengan
Universitas Sains & Teknologi Komputer (Universitas STEKOM)

Anggota IKAPI No: 279 / ALB / JTE / 2023

Redaksi :
Jl. Majapahit no 605 Semarang
Telp. 08122925000
Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

Distributor Tunggal :
Universitas STEKOM
Jl. Majapahit no 605 Semarang
Telp. 08122925000
Fax. 024-6710144
Email : info@stekom.ac.id

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa, yang telah memberikan berkat dan rahmatNya sehingga penulisan buku ini dapat diselesaikan dengan baik. Buku ini berjudul **"Jaringan Kedaulatan: Konsep, Teknologi, dan Prototipe"** Dalam era digital yang ditandai dengan kemajuan teknologi informasi dan komunikasi, kedaulatan siber menjadi isu yang sangat relevan bagi negara-negara di seluruh dunia, termasuk Indonesia. Dengan meningkatnya ancaman siber yang dapat mengganggu keamanan nasional, perlindungan data, serta privasi individu, penting bagi kita untuk memahami dan mengelola aspek-aspek tersebut dengan baik.Kedaulatan jaringan siber tidak hanya mencakup perlindungan terhadap infrastruktur digital, tetapi juga pengaturan dan pengawasan terhadap data yang beredar di ruang siber.

Melalui buku ini, penulis berupaya memberikan wawasan mendalam mengenai manajemen kedaulatan jaringan siber, termasuk tantangan yang dihadapi, strategi yang dapat diterapkan, serta peran penting dari berbagai pemangku kepentingan. Diharapkan, buku ini dapat menjadi referensi yang bermanfaat bagi akademisi, praktisi, dan pembuat kebijakan dalam upaya menciptakan ekosistem siber yang aman dan berdaulat.

Bab 1 menyajikan latar belakang historis dan eksplorasi kedaulatan jaringan dalam konteks dunia maya, sementara Bab 2 membahas interpretasi kedaulatan jaringan dari perspektif internasional dan tantangan-tantangan yang ada. Bab 3 memberikan panduan mendetail mengenai arsitektur jaringan kedaulatan dan proses-proses yang terkait, diikuti oleh Bab 4 yang membahas teknologi utama, termasuk skema autentikasi dan perlindungan privasi. Terakhir, Bab 5 menyajikan prototipe jaringan kedaulatan serta aplikasinya dalam berbagai konteks, termasuk jaringan privat, industri, dan publik.

Harapan saya, buku ini dapat memberikan manfaat dan wawasan yang berguna bagi pembaca, peneliti, dan praktisi di bidang jaringan dan teknologi informasi. Semoga buku ini dapat memberikan kontribusi positif dalam pengembangan pengetahuan dan praktik manajemen kedaulatan jaringan siber di Indonesia.

Semarang, Agustus 2024
Penulis

Dr. Agus Wibowo, M.Kom, M.Si, MM.

DAFTAR ISI

BAB 1
KEDAULATAN DAN KEDAULATAN JARINGAN

Kedaulatan nasional merupakan subjek dasar teori dan praktik hukum internasional kontemporer, menempati posisi yang krusial. Untuk mempelajari kedaulatan internet, kita perlu memiliki pemahaman yang akurat tentang konsep kedaulatan tradisional. Dalam bab ini, kami memperkenalkan kedaulatan dari tiga perspektif: latar belakang historis kedaulatan tradisional, kemampuan beradaptasi kedaulatan di dunia maya atau kedaulatan jaringan, dan kedaulatan di era dunia maya. Terakhir, kami mendefinisikan kedaulatan di dunia maya dari perspektif yurisprudensi.

1.1 LATAR BELAKANG HISTORIS

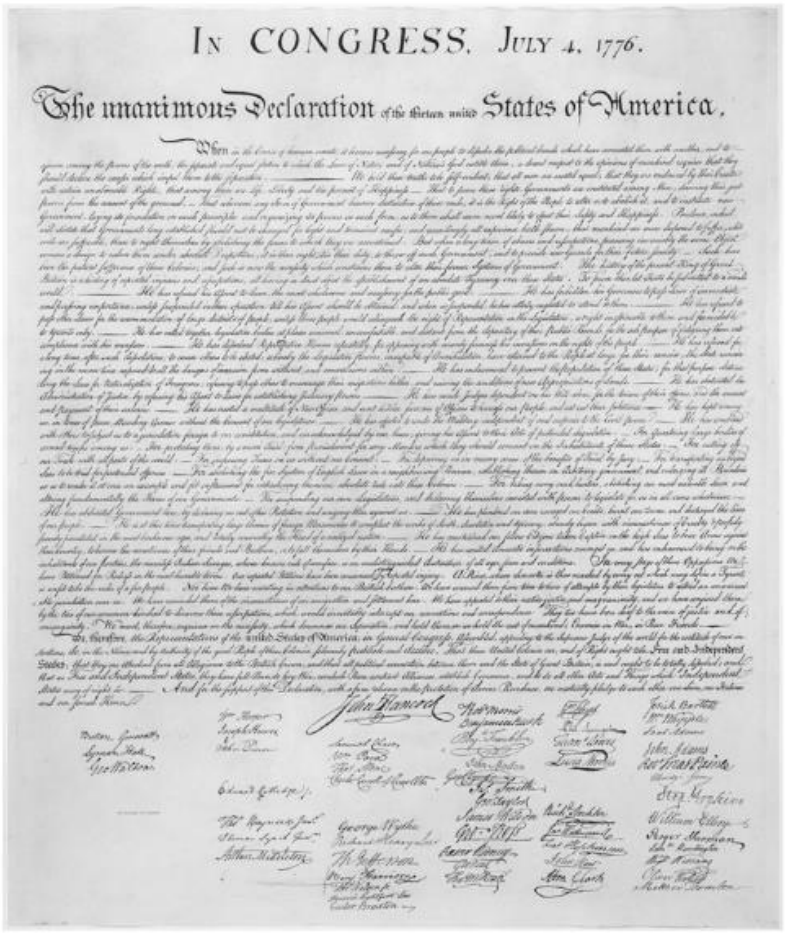
Kedaulatan, kekuatan politik tertinggi dan eksklusif yang dijalankan suatu negara atas yurisdiksinya. Kedaulatan adalah otoritas tertinggi untuk menentukan nasib sendiri.

1.1.1 Asal Mula Kedaulatan Tradisional

Penulis Dictionary of Taxation, Wang Meihan, mengemukakan bahwa “Kedaulatan nasional adalah atribut terpenting yang membedakan suatu negara dari kelompok sosial lainnya. Kedaulatan adalah kekuasaan tertinggi yang melekat pada suatu bangsa di dalam negeri maupun kemerdekaan dan hak berdaulat di lingkup internasional. Setiap negara berhak memilih sistem sosial dan bentuk negaranya, menyelenggarakan pemerintahannya, dan secara mandiri memutuskan dan menangani urusan internal dan eksternalnya sesuai dengan kebijaksanaan dan kondisi nasionalnya. Segala bentuk agresi atau campur tangan oleh negara lain dilarang”. Dalam Deklarasi Kemerdekaan Amerika Serikat, para pendiri negara menunjukkan bahwa akar kedaulatan nasional terletak pada semua warga negara. Sebelumnya, persepsi kedaulatan telah lama diperdebatkan (Gambar. 1.1).

Jean Bodin adalah seorang ahli hukum dan filsuf politik Prancis yang pertama kali dengan tegas mengemukakan konsep kedaulatan. Definisi klasiknya tentang kedaulatan dalam The Six Books of a Commonwealth adalah: “Kekuasaan tertinggi untuk memerintah warga negara dan rakyat, yang Tidak Dapat Dibagi, Tidak Dapat Dipindahtangankan, dan Tidak Dapat Dimusnahkan, tidak terikat oleh hukum atau waktu. Itu adalah kekuatan yang melekat pada negara, dan kekuatan yang melekat ini ada selamanya dan mewakili legitimasi penyatuan kekuasaan negara”. Dengan kata lain, negara ada untuk para penguasa yang berdaulat. Karena warna penguasa monarki yang kuat, pandangan tentang kedaulatan ini disebut teori kedaulatan monarki (Gambar 1.2).

Johannes Althusius adalah seorang ahli hukum Jerman, ia mengemukakan bahwa, “Negara menjalankan kedaulatannya, tetapi kedaulatan adalah milik rakyat, dan kekuasaan ini harus dilimpahkan kepada para administratornya sesuai dengan ketentuan hukum negara”, menyempurnakan teori kedaulatan monarki (Gambar 1.3).


IN CONGRESS, JULY 4, 1776.

The unanimous Declaration of the thirteen united States of America.

Gambar 1.1 Deklarasi Kemerdekaan Amerika Serikat

Menurut hubungan internasional saat itu, Hugo Grotius, seorang ahli hukum dan pemikir besar Belanda, lebih jauh menggeneralisasi konsep kedaulatan: “Kedaulatan berarti bahwa pelaksanaan kekuasaan tidak dibatasi oleh orang lain. Ketika suatu negara menangani urusan internal tanpa kendali orang lain, hal itu terwujud sebagai kedaulatan” (Gambar 1.4).

Makna negara berdaulat modern muncul setelah terbentuknya negara kapitalis dengan sentralisasi otoritas. Pada akhir tiga dekade perang agama di Eropa, negara-negara Eropa menandatangani Perdamaian Westphalia, yang menetapkan prinsip-prinsip kedaulatan nasional, wilayah nasional, dan kemerdekaan nasional, dan kemudian, Sistem Westphalia dengan negara sebagai unit dasar didirikan. Kemudian, karena munculnya dan berkembangnya Komunitas Eropa dan organisasi internasional lainnya, semakin banyak sarjana barat percaya bahwa kedaulatan nasional tidak dapat dipindahtangankan, dan konsep kedaulatan, sebagai landasan dalam menangani urusan politik nasional dan hubungan internasional, secara bertahap diterima oleh komunitas internasional dan berkembang menjadi konotasi baru (Gambar. 1.5).

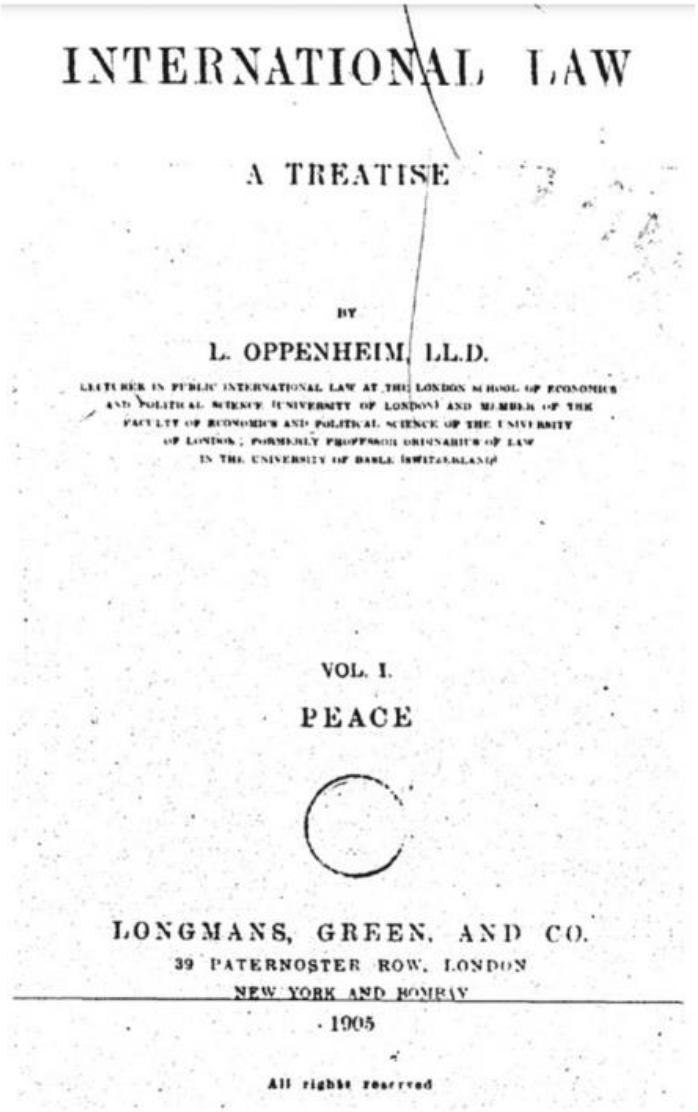
Gambar 1.2 Potret Jean Bodin

Gambar 1.3 Johannes Althusius, ukiran oleh Jean-Jacques Boissard

Gambar 1.4 Potret Hugo Grotius karya Michiel Jansz.van Mierevelt, 1631

Gambar 1.5 Perjanjian Westphalia di Münster (Gerard Terborch 1648)

Pada tahun 1905, ahli hukum Jerman yang terkenal L. F. L. Oppenheim mengemukakan dalam bukunya Oppenheim's International Law bahwa, "Kedaulatan merupakan kewenangan tertinggi suatu negara, bukan berarti kedaulatan lebih tinggi dari semua negara berdasarkan hukum internasional, tetapi menyiratkan kemerdekaan penuh". Selain itu, Pasal 2 Piagam PBB juga memuat ketentuan tentang kesetaraan kedaulatan negara-negara anggota. Kemunculan konsep kedaulatan mendorong penyempurnaan tatanan internasional dan sistem hukum internasional (Gambar 1.6 dan 1.7).



INTERNATIONAL LAW

A TREATISE

BY

L. OPPENHEIM, LL.D.

LECTURER IN PUBLIC INTERNATIONAL LAW AT THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE (UNIVERSITY OF LONDON) AND MEMBER OF THE FACULTY OF ECONOMICS AND POLITICAL SCIENCE OF THE UNIVERSITY OF LONDON; FORMERLY PROFESSOR ORDINARIUS OF LAW IN THE UNIVERSITY OF BASLE (SWITZERLAND)

VOL. I.

PEACE

LONGMANS, GREEN, AND CO.

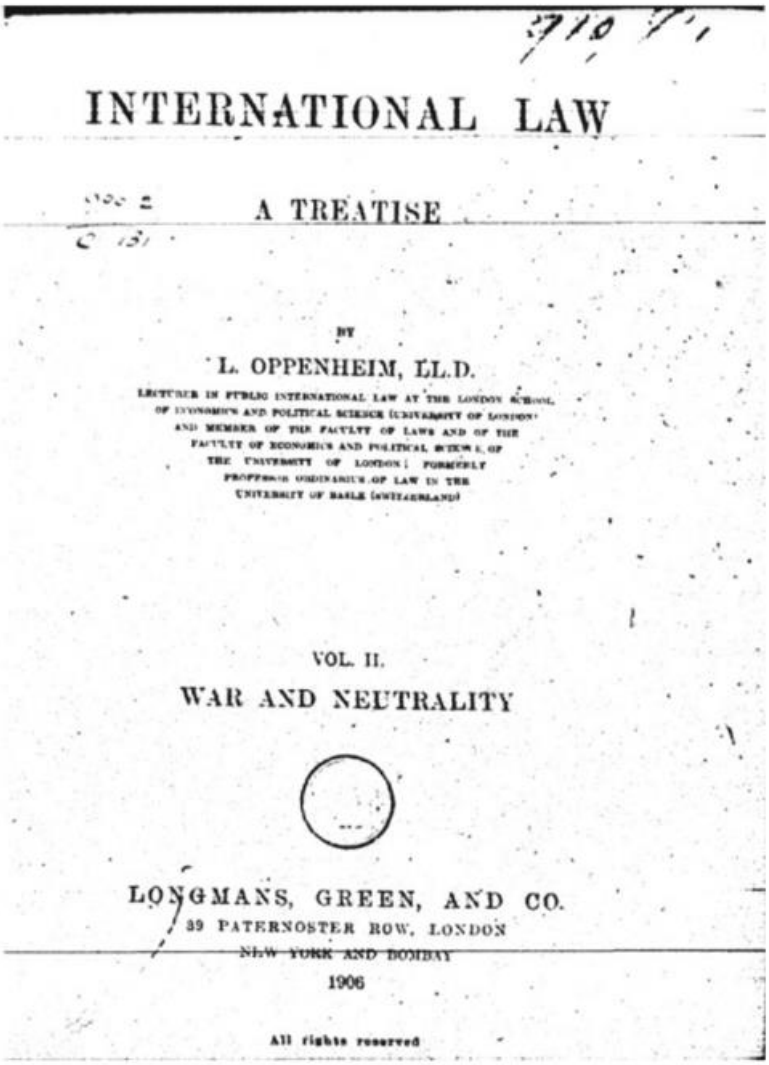
39 PATERNOSTER ROW, LONDON

NEW YORK AND BOMBAY

1905

All rights reserved

Gambar 1.6 Hukum Internasional: sebuah risalah. Vol. 1. Perdamaian oleh L. Oppenheim, LL.D.



INTERNATIONAL LAW

A TREATISE

BY

L. OPPENHEIM, LL.D.

LECTURER IN PUBLIC INTERNATIONAL LAW AT THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE (UNIVERSITY OF LONDON) AND MEMBER OF THE FACULTY OF LAWS AND OF THE FACULTY OF ECONOMICS AND POLITICAL SCIENCE, OF THE UNIVERSITY OF LONDON; FORMERLY PROFESSOR ORDINARIUS OF LAW IN THE UNIVERSITY OF BASLE (SWITZERLAND)

VOL. II.

WAR AND NEUTRALITY

LONGMANS, GREEN, AND CO.

39 PATERNOSTER ROW, LONDON

NEW YORK AND BOMBAY

1906

All rights reserved

Gambar 1.7 Hukum Internasional: sebuah risalah. Vol. 2. Perang dan Netralitas oleh L. Oppenheim, LL.D.

1.1.2 Kedaulatan Tradisional

Elemen dasar negara berdaulat adalah penduduk, wilayah, rezim, dan kedaulatan. Inti dari membangun bangsa dan negara adalah kedaulatan. Kedaulatan adalah kekuatan tertinggi yang dimiliki suatu negara untuk menangani urusan internal dan eksternalnya secara independen.

Negara berdaulat perlu memastikan empat hak dasar yurisdiksi, pembelaan diri, kemerdekaan, dan kesetaraan. Secara khusus, negara memiliki kekuatan untuk menjalankan yurisdiksi atas semua orang dan masalah di dalam wilayahnya, serta warga negara di luar wilayahnya. Negara memiliki hak untuk membangun sistem politik dan sosial ekonomi yang dikombinasikan dengan keadaannya. Untuk menjaga kemerdekaan politik dan integritas teritorialnya, negara memiliki hak untuk mempertahankan diri terhadap agresi dan ancaman

asing. Negara sepenuhnya independen dan bebas dari campur tangan eksternal untuk menjalankan kekuasaan negara.

Dalam hukum internasional, semua negara berdaulat, apa pun ukuran, kekuatan, sistem politik, ekonomi, ideologis, dan sosialnya, adalah setara. Jean Bodin, pendiri teori kedaulatan, mengemukakan bahwa, "Kedaulatan adalah asas keberadaan suatu negara, dan merupakan kekuasaan tertinggi suatu negara yang tidak dapat dibagi dan dipindahtangankan di dalam wilayahnya". Kedaulatan memiliki arti penting dalam pertukaran antarnegara. Intinya, kedaulatan merupakan dasar untuk membedakan negara dan dengan demikian menghasilkan simbol-simbol negara berdaulat, seperti nama nasional, bendera nasional, lambang nasional, batas negara, lagu kebangsaan, kebangsaan, bahasa nasional, dan warga negara. Secara keseluruhan, kedaulatan mengandung tiga unsur: wilayah, rakyat, dan rezim, yang dijelaskan dalam pasal 78, paragraf pembukaan pertama, dan paragraf pembukaan kedua Piagam Perserikatan Bangsa-Bangsa:

> "*Sistem perwalian tidak berlaku bagi wilayah yang telah menjadi Anggota Perserikatan Bangsa-Bangsa, yang hubungan di antara mereka harus didasarkan pada penghormatan terhadap asas persamaan kedaulatan*." "*Kami, rakyat dari negara-negara bersatu, bertekad untuk menyelamatkan generasi mendatang dari malapetaka perang, yang dua kali dalam masa hidup kami telah membawa kesedihan yang tak terkira bagi umat manusia, dan untuk menegaskan kembali keyakinan pada hak asasi manusia yang fundamental, pada martabat dan nilai pribadi manusia, pada hak yang sama antara pria dan wanita dan negara-negara besar dan kecil, dan untuk membangun kondisi di mana keadilan dan penghormatan terhadap kewajiban yang timbul dari perjanjian dan sumber hukum internasional lainnya dapat dipertahankan, dan untuk mempromosikan kemajuan sosial dan standar hidup yang lebih baik dalam kebebasan yang lebih besar, dan untuk tujuan-tujuan ini untuk mempraktikkan toleransi dan hidup bersama dalam damai satu sama lain sebagai tetangga yang baik, dan untuk menyatukan kekuatan kita untuk menjaga perdamaian dan keamanan internasional, dan untuk memastikan, dengan penerimaan prinsip-prinsip dan institusi metode, bahwa kekuatan bersenjata tidak akan digunakan, kecuali untuk kepentingan bersama, dan untuk menggunakan mesin internasional untuk mempromosikan kemajuan ekonomi dan sosial semua orang, telah memutuskan untuk menggabungkan upaya kita untuk mencapai tujuan-tujuan ini. Oleh karena itu, pemerintah kita masing-masing, melalui perwakilan yang berkumpul di kota San Francisco, yang telah menunjukkan semua kewenangan mereka yang terbukti benar dan sah, telah menyetujui Piagam Perserikatan Bangsa-Bangsa saat ini dan dengan ini mendirikan sebuah organisasi internasional yang dikenal sebagai Perserikatan Bangsa-Bangsa*."

Singkatnya, kedaulatan negara meliputi tiga unsur: daratan, lautan, udara, sumber daya, orang-orang di dalam wilayah dan warga negara di luar wilayah, serta rezim yang setara dan independen. Hanya unit politik dengan wilayah yang tetap, populasi tertentu, bentuk organisasi rezim tertentu, dan kedaulatan yang dapat disebut negara berdaulat.

1.1.3 Misi Kedaulatan

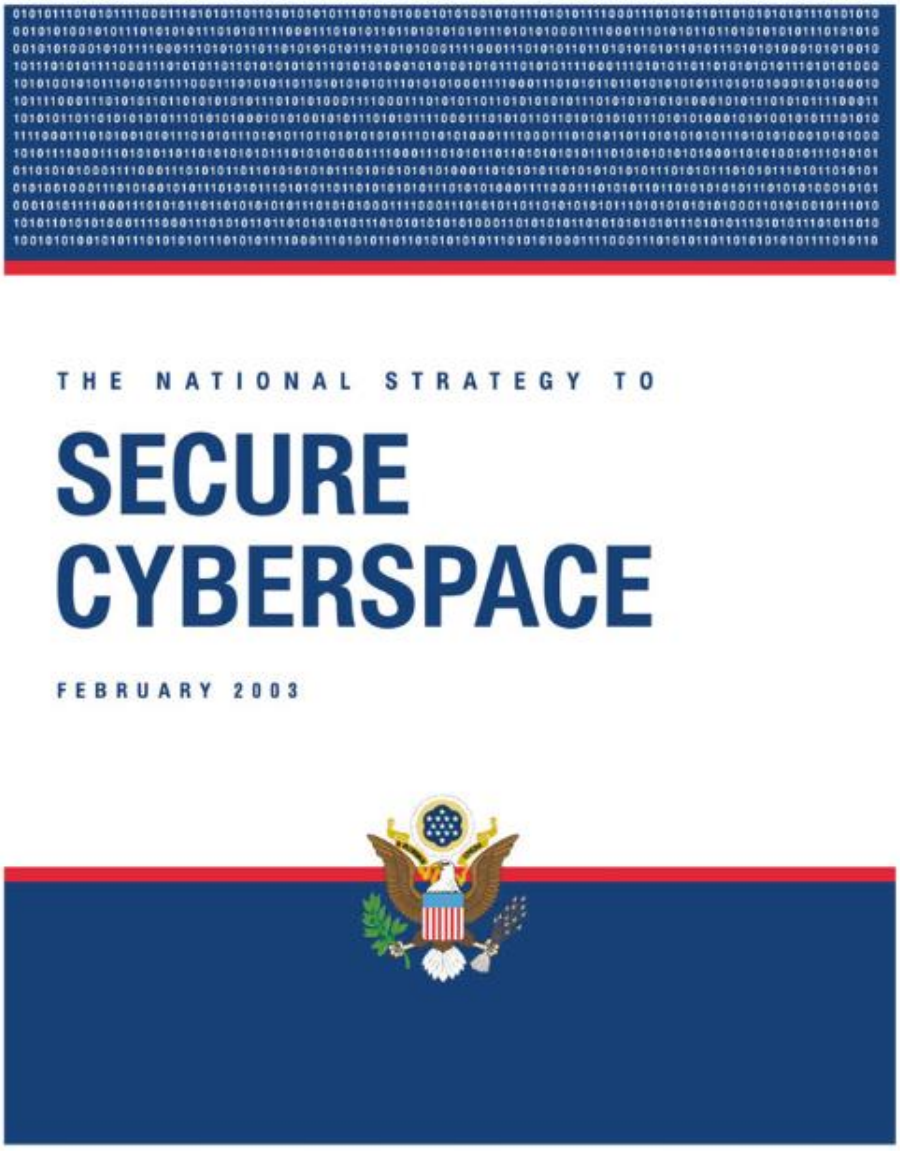
Berdasarkan pembahasan di atas, kedaulatan memiliki sifat internal dan eksternal. Atribut internal tertinggi dari kedaulatan adalah kekuatan politik yang berkuasa dari suatu negara, yang mewujudkan kesatuan internal negara melalui cara legislatif, administratif, yudikatif, militer, ekonomi, budaya, dan cara lainnya. Atribut eksternal kedaulatan berasal dari atribut internal tertinggi dari kedaulatan, yang terdiri dari penentuan nasib sendiri suatu negara dan integritas teritorial, yang diwujudkan melalui cara militer, hukum, diplomatik, ekonomi, dan cara lainnya. Kedaulatan menuntut pemerintahan berdasarkan hukum secara internal dan mempertahankan kemerdekaan dan otonomi secara eksternal. Bentuk hukum kedaulatan umumnya didefinisikan dalam konstitusi atau hukum dasar. Ia memiliki sifat internal dan sifat eksternal. Sifat eksternal kedaulatan adalah pengakuan timbal balik internasional. Singkatnya, misi wajib kedaulatan adalah untuk melawan agresi asing dan menenangkan interior.

1.2 ADAPTABILITAS KEDAULATAN DI DUNIA MAYA

Kedaulatan nasional merupakan subjek dasar teori dan praktik hukum internasional kontemporer, menempati posisi penting. Dunia maya, ruang fundamental selain ruang darat, laut, dan udara, tetapi tidak memiliki kode etik internasional. Dalam beberapa tahun terakhir, semakin banyak perhatian difokuskan pada adaptasi kedaulatan nasional di dunia maya. Terutama setelah merebaknya insiden dunia maya yang ganas seperti PRISM, diskusi tentang kedaulatan di dunia maya terus berlanjut.

1.2.1 Komposisi Dunia Maya

Persoalan tentang bagaimana membagi batas dunia maya berarti bagaimana membentuk dunia maya dan membangun kedaulatan. Sebelum membahas adaptasi kedaulatan nasional di dunia maya, kami akan memperkenalkan konstitusi dunia maya dari tiga aspek: definisi, atribut hukum, dan batas-batas dunia maya.



Gambar 1.8 Strategi Nasional Pengamanan Dunia Maya (Februari 2003)

Dunia maya berbeda dari ruang tradisional laut, darat, dan udara. Berbagai negara memiliki posisi dan pandangan yang berbeda tentang atribut hukum dan pelaksanaan hak di dunia maya. *International Telecommunication Union* (ITU) mendefinisikan dunia maya sebagai "medan fisik dan non-fisik yang diciptakan oleh dan/atau terdiri dari beberapa atau semua hal berikut: komputer, sistem komputer, jaringan, dan program komputernya, data komputer, data konten, data lalu lintas, dan pengguna". Pada tahun 2003, Amerika Serikat mendefinisikan dunia maya sebagai "jaringan infrastruktur teknologi informasi yang saling bergantung" dalam Strategi Nasional untuk Mengamankan Dunia Maya. Definisi dunia maya memengaruhi penentuan kedaulatan jaringan. Kedaulatan jaringan menentukan rasionalitas yurisdiksi negara atas infrastruktur dan konten informasi dunia maya serta hak pertahanan eksternal. Komunitas internasional membutuhkan definisi yang terpadu tentang dunia maya dan kedaulatan jaringan berdasarkan hukum (Gambar. 1.8).

Saat ini, ada dua jenis atribut hukum utama tentang dunia maya: teori infrastruktur dan teori domain. Dalam teori infrastruktur, Internet dianggap sebagai infrastruktur penting suatu negara, dan Internet dalam batas-batas nasional berada di bawah yurisdiksi kedaulatan. Infrastruktur Informasi Nasional: Agenda Aksi, yang dikeluarkan oleh pemerintah AS, dengan jelas mendefinisikan konsep ini. Dan pemerintah Tiongkok juga membuat pernyataan serupa dalam dokumen-dokumen terkait. Dalam teori domain, dunia maya dianggap sebagai area tempat kedaulatan dapat dilaksanakan, dan pemerintah harus mengklaim hak yang sah untuk membela diri terhadap serangan dunia maya, yang ditetapkan dalam Strategi Internasional untuk Dunia Maya yang diumumkan oleh pemerintah AS (Gambar. 1.9).

Penetapan batas dunia maya oleh suatu negara di bawah kedaulatannya juga merupakan masalah batas dunia maya. Sama seperti dunia maya didefinisikan sebagai domain fisik dan non-fisik, batas-batas dunia maya juga harus mencakup batas-batas fisik dan non-fisik. Batas-batas dunia maya adalah kumpulan batas-batas geografis fisik dan batas-batas jaringan non-fisik. Batas geografis fisik adalah batas teritorial dalam lingkup kedaulatan suatu negara, termasuk batas teritorial negara, dan ruang geografis yang dicakup kedaulatan nasional, seperti konsulat dan pesawat udara. Batas jaringan nonfisik adalah batas tidak berwujud yang ditetapkan melalui teknologi jaringan, seperti firewall, sistem kata sandi, perlindungan dinamis sistem deteksi intrusi, dan hambatan teknis lainnya.

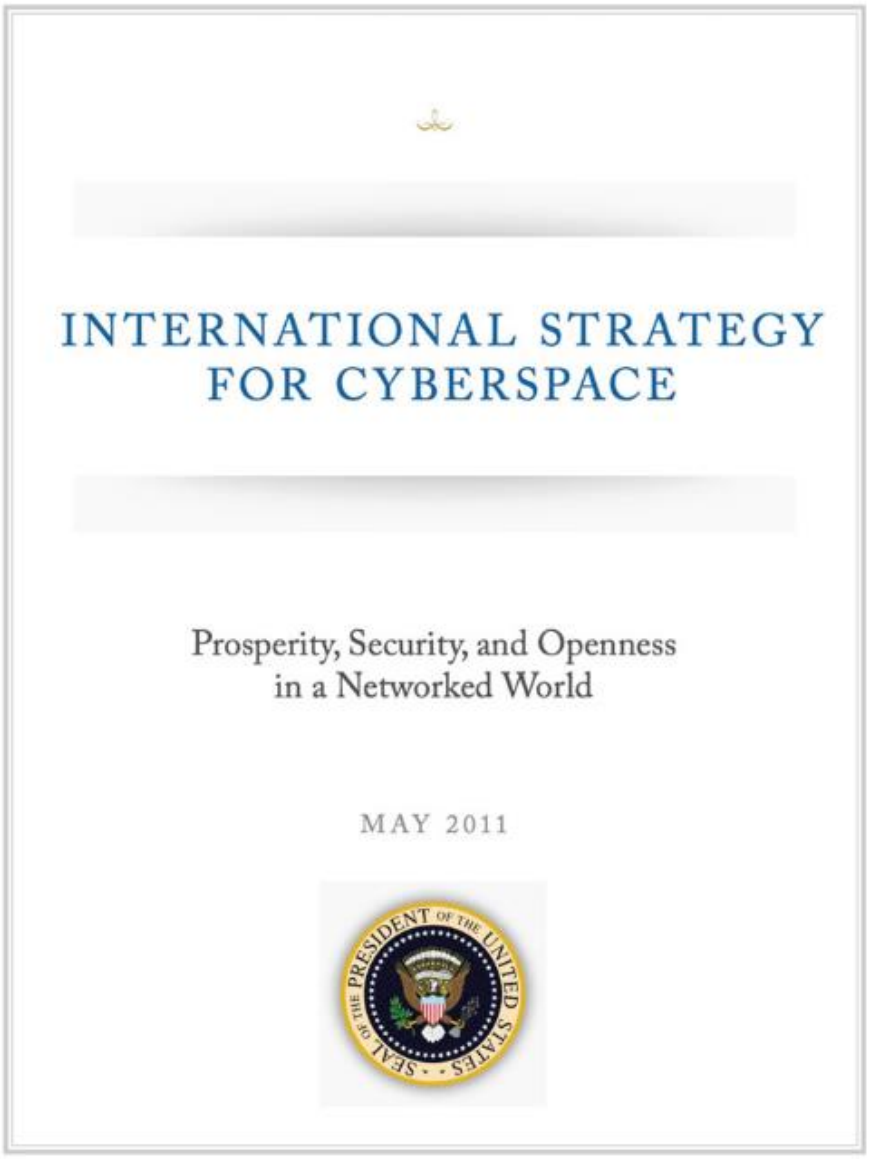
Pembagian yurisdiksi nasional atas dunia maya adalah membagi batas dunia maya di antara negara-negara di dunia maya global dengan alasan mengakui keberadaan dunia maya, dan untuk menentukan kedaulatan nasional di dunia maya.

1.2.2 Kedaulatan Jaringan di Era Baru

Kedaulatan jaringan adalah produk era baru, yang berasal dari keberadaan dunia maya. Berbeda dengan wilayah darat, laut, dan udara yang batasnya relatif stabil, di dunia internet, batas negara telah meluas ke dunia virtual, dan batas jaringan tidak terlihat dan cakupan spasialnya tidak jelas. Di satu sisi, perkembangan teknologi dan inovasi jaringan memperluas ruang batas jaringan. Negara-negara bersaing ketat untuk mengembangkan, memiliki, menganalisis, dan menerapkan sumber daya informasi dunia maya.

Dengan permainan kebijakan antara berbagai negara, kekuatan kemampuan teknologi informasi, dan tingkat status internasional yang berubah, batas-batas kedaulatan jaringan terus berubah dan menyesuaikan. Di sisi lain, munculnya organisasi-organisasi internasional seperti *Perserikatan Bangsa-Bangsa* (PBB), *Organisasi Perdagangan Dunia* (WTO), dan *Organisasi Internasional untuk Standardisasi* (ISO) telah membawa peluang dan tantangan baru bagi pengembangan kedaulatan jaringan. Munculnya organisasi-organisasi internasional ini semakin memperluas dan memperkuat komunikasi dan koordinasi di antara mitra-mitra internasional. Pertukaran perdagangan dan budaya memberikan peluang yang baik untuk komunikasi budaya. Peningkatan komunikasi antara teknik-teknik dan peralatan canggih di dunia telah menciptakan kondisi yang menguntungkan bagi jaringan untuk meningkatkan tingkat teknologi secara keseluruhan dan mempercepat peningkatan teknologi. Pada saat yang sama, dalam persaingan internasional, kekuatan siber dapat secara efektif memperluas

batas kedaulatannya melalui kekuatan teknologi, sementara yang relatif lemah dihadapkan pada kompresi dan penyesuaian ruang lingkup kedaulatan jaringan yang terus-menerus.



Gambar 1.9 Strategi Internasional untuk Dunia Maya (Mei 2011)

Mengambil contoh China Broadcast Network, setelah China bergabung dengan Organisasi Perdagangan Dunia (WTO), peluang dan tantangan yang ada telah meningkatkan rasa urgensi untuk melakukan reformasi dan pengembangan sistem penyiaran dan televisi China. Hal ini membantu industri radio dan televisi mengembangkan layanan video profesional yang memenuhi kebutuhan personal dan generasi baru radio dan televisi seperti televisi definisi tinggi (HDTV) dan televisi interaktif (ITV), yang akan memperluas ruang bagi kelangsungan hidup dan pengembangan radio dan televisi. China memainkan peran aktif dan konstruktif dalam WTO. Bergabungnya China ke WTO telah membawa tantangan baru bagi industri radio dan televisi. Persaingan antara media tradisional seperti siaran televisi, audio-

video, buku, surat kabar, dan media baru seperti Internet akan semakin intensif. Iklan, program, bakat, dan sumber daya lainnya akan didistribusikan ulang.

Dengan masuknya kelompok media asing yang besar, budaya dan nilai-nilai eksotis dapat menekan ruang hidup budaya lokal dan membawa pengaruh potensial dan mendalam pada industri siaran televisi. Dalam proses perlindungan hak cipta, China Broadcast Network terus memperkuat komunikasi dan koordinasi dengan dunia. Pada tahun 1980, China menjadi anggota Organisasi Hak Kekayaan Intelektual Dunia (WIPO). Pada tahun 1992, China menyetujui Konvensi Berne untuk Perlindungan Karya Sastra dan Seni serta Konvensi Hak Cipta Universal. Pada tahun 1993, China menyetujui Konvensi untuk Perlindungan Produser Rekaman Suara terhadap Penggandaan Rekaman Suara Secara Tidak Sah. China menjadi anggota keluarga hak cipta dunia. Bergabungnya China ke WTO telah mempercepat proses legislasi hak cipta China, dan selanjutnya meningkatkan tingkat perlindungan hak cipta.

Organisasi penyiaran menikmati perlindungan yang luas atas program mereka berdasarkan Undang-Undang Hak Cipta, yang selanjutnya memperluas hak-hak tetangga mereka. Dalam hal perlindungan hak cipta, baik China maupun anggota WTO lainnya, melaksanakan kegiatan dalam kerangka TRIPS, menikmati hak dan kewajiban yang sama satu sama lain, menikmati perlakuan nasional dan perlakuan negara yang paling disukai, dan menyediakan mekanisme penyelesaian sengketa untuk menyelesaikan sengketa hak cipta. Selain itu, aksesi ke WTO kondusif untuk mempromosikan saling pengertian dan kerja sama antara Tiongkok dan negara-negara anggota WTO dalam legislasi dan penegakan hukum hak cipta, memperkuat komunikasi informasi hak cipta, mempelajari isu-isu baru perlindungan hak cipta yang dihadapi bersama, dan terus meningkatkan tingkat perlindungan hak cipta.

Dalam hal perlindungan hak cipta, sebagai produk budaya, program-program dalam jaringan siaran diperlakukan oleh masing-masing negara dengan kebijakan khusus yang berbeda dari barang dagangan umum. Dalam negosiasi untuk aksesi ke WTO, Tiongkok tidak pernah membuat komitmen apa pun untuk membuka program radio dan televisi. Bahkan jika beberapa saluran TV luar negeri diluncurkan di beberapa wilayah Tiongkok, saluran-saluran itu hanya ditangani sebagai kasus kerja sama yang saling menguntungkan. Ini akan membantu meningkatkan pertukaran budaya antara Tiongkok dan negara-negara dan kawasan lain dengan alasan melindungi hak cipta jaringan penyiaran, untuk memanfaatkan sepenuhnya keuntungan dan menghindari kerugian. Industri radio dan televisi Tiongkok akan semakin mempercepat laju reformasi dan keterbukaan, dan selanjutnya, mempromosikan pengembangan kedaulatan jaringan di WTO. Dalam Bab 3, kami mengusulkan arsitektur jaringan kedaulatan berdasarkan Jaringan Penyiaran Tiongkok.

1.3 EKSPLORASI KEDAULATAN JARINGAN

Para cendekiawan di dalam dan luar negeri telah membuat serangkaian prestasi dalam studi kedaulatan di era Internet, yang memiliki signifikansi teoritis yang besar untuk mempromosikan tata kelola internasional dunia maya. Namun secara keseluruhan, studi kedaulatan di era Internet masih dalam tahap awal.

1.3.1 Perdebatan Teoritis

Terdapat empat pandangan utama tentang perdebatan teoritis kedaulatan jaringan: teori penolakan kedaulatan di dunia maya, teori non-kedaulatan di dunia maya, teori kedaulatan terbatas di dunia maya, dan teori kedaulatan penuh di dunia maya.

1. Teori Penolakan Kedaulatan di Dunia Maya

Para ahli strategi Internet yang memiliki kepentingan dalam arsitektur jaringan saat ini, menganjurkan kesamaan atau atribut global Internet. Ini untuk memperlakukan dunia maya sebagai ruang internasional yang mirip dengan laut lepas, dan bukan untuk menegaskan kedaulatan nasional. Konsep ini, meskipun belum matang dan kontroversial, menimbulkan tantangan bagi kedaulatan negara di dunia maya. Meskipun teori ini menganjurkan kebebasan jaringan dan mempromosikan model tata kelola dunia maya yang “de-government”, pada dasarnya, teori ini masih menunjukkan kendali kedaulatan dunia maya di mana-mana. Misalnya, pada 27 Oktober 2015, Senat AS memperkenalkan Undang-Undang Pembagian Informasi Keamanan Siber tahun 2015. RUU tersebut memungkinkan industri swasta untuk berbagi informasi yang dikumpulkan tentang pengguna mereka dengan Departemen Keamanan Dalam Negeri (DHS). RUU tersebut memberi Amerika Serikat hak untuk melacak dan menangkap warga negara lain, terlepas dari kewarganegaraan atau lokasi mereka.

RUU tersebut memutus hubungan yang setara antara negara-negara saat melacak tersangka kriminal. RUU tersebut pada dasarnya mengendalikan kedaulatan negara di dunia maya. Pada tahun 2018, Departemen Pertahanan AS merilis Strategi Siber yang menekankan konsep “Pertahanan maju”. Hal ini telah ditafsirkan oleh dunia luar sebagai militer AS akan menerapkan serangan jaringan dan gerakan pertahanan di negara-negara lain. Pada bulan Agustus tahun itu, Presiden AS Donald Trump menandatangani perintah yang membatalkan Arahan Kebijakan Presidensial no. 20 (PPD-20) Presiden Barack Obama, yang memberikan kebebasan lebih kepada militer untuk menyebarkan senjata siber canggih tanpa diblokir oleh Departemen Luar Negeri atau komunitas intelijen. Sebelumnya, Presiden AS juga memberikan kebebasan kepada militer untuk menyebarkan senjata siber canggih tanpa hambatan.

Singkatnya, kepentingan pribadi jaringan IP telah menggembar-gemborkan risiko "Cyber Pearl Harbor" selama bertahun-tahun, tetapi mereka bertanggung jawab atas penggunaan senjata siber pertama di dunia terhadap fasilitas asing. Sebagai pemrakarsa perang siber, genre ini bukan hanya negara paling kuat dalam perang siber tetapi juga negara yang telah meluncurkan perang siber terbanyak.

2. Teori Ketidakdaulatan dalam Dunia Maya

Mirip dengan teori peniadaan kedaulatan, teori ketidakdaulatan juga merupakan salah satu pandangan penting tentang pengelolaan dunia maya karena sifat virtual dunia maya. Pandangan ini beranggapan bahwa dunia maya adalah ruang bebas bagi seluruh umat manusia, dan pemerintah serta kekuasaan publik tidak dapat mengaksesnya, sehingga wajar jika tidak akan muncul masalah kedaulatan nasional. Dengan kata lain, pandangan ini menekankan kebebasan individu di bawah kendali rasional, menganjurkan pembedaan antara kewenangan individu dan kewenangan sosial, serta tidak membatasi kewenangan individu tanpa merugikan kepentingan orang lain. Pandangan ini berawal dari teori liberal, menganut

prinsip hak asasi manusia atas kedaulatan, dan menganjurkan anarkisme jaringan. Sifat virtual dunia maya memberi individu kemudahan untuk menggunakan sumber informasi virtual secara bebas, dan sampai batas tertentu menjamin bahwa kebebasan berbicara dan berperilaku warga negara di dunia maya tidak tunduk pada kendala dan kendali eksternal.

Meskipun teori peniadaan kedaulatan dan teori ketidakdaulatan menganjurkan kebebasan jaringan, titik tolak keduanya berbeda. Dari perspektif otonomi jaringan, teori non-kedaulatan mengecualikan intervensi kekuasaan publik dari pemerintah, "untuk menolak semua undang-undang, semua kekuasaan, semua hak istimewa, hak pilih, pengaruh resmi dan hukum".

3. Teori Kedaulatan Terbatas di Dunia Maya

Teori kedaulatan terbatas di dunia maya berasal dari "teori kedaulatan terbatas" dalam "teori kedaulatan negara". Teori ini menganjurkan bahwa negara harus mematuhi konvensi internasional dalam menjalankan kedaulatan, dan menekankan bahwa dalam proses menjalankan kekuasaan, sebagian kekuasaan dapat ditransfer ke organisasi dan lembaga internasional untuk memperluas kepentingan bersama di antara negara-negara. Di sisi lain, teori ini menganjurkan bahwa suatu negara harus melepaskan kepentingan kedaulatannya yang terbatas dan mendapatkan kepentingan nasional yang lebih besar. Profesor Yan Xuetong, seorang sarjana hubungan internasional, menunjukkan bahwa "Kedaulatan adalah bagian dari kepentingan nasional, yang dapat disebut kepentingan kedaulatan. Kepentingan kedaulatan tidak selalu sejalan dengan kepentingan semua negara. Misalnya, untuk masuk ke WTO, Tiongkok harus menyerahkan sebagian kekuatan pengambilan keputusan ekonomi domestik dan yurisdiksi ekonominya, sama seperti negara anggota lainnya, tetapi ini tidak berarti menyerahkan kepentingan nasional".

Oleh karena itu, teori kedaulatan terbatas di dunia maya menganjurkan bahwa, "tujuan menjaga kedaulatan adalah untuk mencapai kepentingan nasional yang lebih besar, bukan kedaulatan itu sendiri. Sejumlah kecil kedaulatan nasional dapat dibatasi atau diserahkan kepada kepentingan nasional yang lebih besar". Teori kedaulatan terbatas di dunia maya menegaskan bahwa semua negara memiliki kedaulatan jaringan. Pada saat yang sama, teori ini menekankan keseimbangan dan pilihan antara kedaulatan dunia maya dan kepentingan nasional. Teori ini menganjurkan bahwa negara-negara berdaulat harus memberikan permainan penuh pada antusiasme dan inisiatif mereka, mencapai tata kelola bersama di bawah konsensus internasional dan ketentuan perjanjian, dan mencapai kesatuan dialektis antara kemutlakan dan relativitas di bawah kerangka Perserikatan Bangsa-Bangsa.

4. Teori Kedaulatan Sempurna dalam Dunia Maya

Para penganut kedaulatan mutlak percaya bahwa keberadaan negara berdaulat didasarkan pada kedaulatan mutlak, dan menjaga kedaulatan berarti melindungi haknya untuk bertahan hidup dan berkembang dalam masyarakat internasional; semua negara harus mematuhi prinsip-prinsip dasar kemerdekaan, kesetaraan, saling menghormati, non-agresi, dan non-intervensi. Dalam sejarah perkembangan hubungan internasional, teori kedaulatan mutlak negara memainkan peran penting dalam melindungi pembentukan, konsolidasi, dan pengembangan negara-negara Eropa. Teori ini memiliki penghalang dan efek perlindungan

tertentu bagi mayoritas negara Asia, Afrika, dan Amerika Latin yang muncul setelah "Perang Dunia II" untuk mempertahankan kedaulatan dan menjaga kemerdekaan dan martabat nasional. Teori kedaulatan mutlak negara juga telah sepenuhnya ditransplantasikan ke dalam teori dunia maya.

Dalam tatanan sosial internasional, negara-negara berkembang sering kali berada pada posisi yang kurang menguntungkan, yang kedaulatan nasionalnya berada dalam keadaan rapuh dan tidak aman, dan mereka mudah menjadi objek campur tangan oleh hegemoni jaringan beberapa kekuatan besar. Oleh karena itu, negara-negara lemah umumnya mengklaim bahwa dunia maya memiliki kedaulatan penuh, dan masyarakat internasional perlu mengatur dunia maya secara ketat, memantau informasi domestik secara ketat, menolak informasi eksternal, dan menjaga kedaulatan jaringan nasional. Namun, perkembangan dan popularisasi teknologi internet yang pesat telah memberikan tekanan yang semakin besar pada negara-negara berkembang untuk "mempopulerkan internet dengan sikap terbuka atau terus mempertahankan status quo yang terbelakang".

Singkatnya, dunia maya memiliki karakteristik virtualitas, keterbukaan, dapat dibagikan, dan rentan, yang membuat kedaulatan nasional mudah melemah di dunia maya. Namun dunia maya bukanlah "tanah di luar hukum". Di bidang kedaulatan mana pun, ketaatan pada hukum adalah masalah prinsip. Secara khusus, beberapa tahun terakhir orang telah melihat munculnya bentuk-bentuk canggih seperti terorisme dunia maya, militerisasi dunia maya, dan konflik dunia maya antarnegara. Masyarakat internasional harus secara aktif mengeksplorasi solusi untuk tata kelola keamanan dunia maya, merumuskan rencana praktis, dan meningkatkan hukum dan peraturan yang relevan berdasarkan kerja sama yang setara. Pada saat yang sama, tata kelola dunia maya, penelitian teknologi jaringan, dan perumusan standar harus dilakukan secara aktif untuk memastikan bahwa dunia maya memiliki hukum untuk diikuti.

1.3.2 Eksplorasi dan Praktik

Negara-negara memiliki pemahaman yang berbeda tentang kedaulatan jaringan, teori, dan hukum di jaringan. Negara-negara dengan kekuatan nasional yang kuat memiliki lebih banyak suara di dunia. Oleh karena itu, ada berbagai skema praktis untuk tata kelola dunia maya saat ini.

1. Konstruksi Hegemoni Internet yang Ofensif

Seperti yang disebutkan di bagian sebelumnya, orang-orang yang memiliki kepentingan dalam arsitektur jaringan saat ini, menganjurkan kesamaan atau atribut global Internet. Pandangan politik, terutama AS, mengejar kebebasan Internet, yang sepenuhnya ditunjukkan dalam strategi diplomatiknya. Pada tahun 2015, AS menganggap strategi diplomatik kebebasan Internet sebagai proyek prioritas dan memasukkannya dalam Strategi Internasional untuk Dunia Maya, "Ketika AS atau sekutunya diserang dunia maya, AS akan menggunakan semua cara kekerasan yang mungkin (diplomatik, ekonomi atau bahkan militer) untuk mencegah atau membalas". Alvin Toffler, seorang futuris terkenal di dunia, menunjukkan bahwa, "Kubus Rubik politik dunia akan berada di tangan orang-orang dengan kekuatan informasi di masa depan. Mereka akan menggunakan hak-hak yang mereka miliki,

seperti hak untuk mengendalikan jaringan dan menerbitkan informasi, dan memanfaatkan keunggulan budaya dan bahasa Inggris yang kuat untuk mencapai tujuan yang tidak dapat ditaklukkan oleh kekerasan maupun uang".

Dalam hal tindakan, skema tersebut mencoba mewujudkan pemantauan dunia maya dalam skala global. Dalam proses ini, keunggulan teknologi secara bertahap akan berubah menjadi keunggulan kekuatan dan membantunya mewujudkan hegemoni Internet. Untuk mengganggu rezim lain dan menerapkan pengawasan dunia maya dalam skala internasional dengan lebih mudah, alasan umum bagi mereka adalah untuk melawan kekuatan teroris dan mempromosikan kebebasan berekspresi.

Tujuan akhir mereka adalah untuk mencapai hegemoni jaringan dengan memonopoli otoritas pembuat aturan jaringan internasional. Operasi normal Internet tidak dapat dipisahkan dari server root dan sistem nama domain. Server akar DNS yang ada berada di tangan beberapa negara, yang mengendalikan distribusi nama dan alamat domain Internet, dan memberikan legitimasi dan kepatuhan untuk penerapan kebijakan hegemoni siber dengan memanipulasi *Internet Corporation for Assigned Names and Numbers* (ICANN). Amerika Serikat melakukan yang terbaik untuk menekan kepentingan negara-negara Internet yang sedang berkembang.

2. Pembangunan Strategi Keamanan Siber yang Defensif

Dibandingkan dengan kepentingan pribadi dalam sistem Internet saat ini, negara-negara berkembang memiliki kekuatan nasional yang relatif lemah secara keseluruhan, tingkat teknologi jaringan yang rendah, dan suara yang terbatas di dunia maya. Mereka berkomitmen untuk mempromosikan modernisasi kapasitas tata kelola jaringan di tingkat nasional.

Pada tataran teoritis, dengan munculnya era jaringan, kekuatan-kekuatan ini menyadari pentingnya dunia maya. Untuk melawan hegemonisme dan mengonsolidasikan kekuasaan, mereka dengan tegas menyerukan kedaulatan jaringan dan menganjurkan agar masyarakat internasional bersama-sama menetapkan aturan dan regulasi untuk menjaga kedaulatan dunia maya dan mencapai pembangunan bersama di dunia. Rusia, Brasil, dan negara-negara lain telah menyerukan regulasi jaringan, penghormatan terhadap kedaulatan jaringan, dan perlindungan kedaulatan nasional.

Dari segi kebijakan, skema yang disebutkan di atas memerlukan fokus pada peningkatan teknologi jaringan dan tingkat tata kelola jaringan. Saat ini, kepentingan pribadi di Internet dapat menempati posisi yang menguntungkan karena kekuatan nasionalnya yang komprehensif dan teknologi canggih. Di sisi lain, negara-negara berkembang sangat bergantung pada Internet. Jika mereka ingin mendapatkan status yang sama di dunia maya, mereka harus memperkuat konstruksi teknologi. Peningkatan tata kelola dunia maya juga merupakan cara penting bagi negara-negara berkembang untuk mengatasi serangan hegemoni jaringan. Negara-negara berkembang terus memperkuat undang-undang jaringan, dengan membuat undang-undang tentang kode etik di dunia maya. Menurut statistik, lebih dari 90 negara di dunia telah merumuskan undang-undang perlindungan keamanan siber khusus, dan di masa depan, semakin banyak negara berkembang akan membuat undang-

undang tentang kode etik di dunia maya dan menjaga keamanan siber melalui cara-cara yang sah.

3. Pola Tata Kelola Internasional

Sulit bagi satu negara berdaulat untuk menjaga keamanan siber dan mengatur dunia maya sendiri. Diperlukan partisipasi yang luas dan kerja sama yang mendalam di antara semua negara. Berdasarkan uraian di atas, dapat disimpulkan bahwa tidak satu pun dari dua strategi keamanan dunia maya di atas dapat mencapai tata kelola yang baik di dunia maya. Terkait hal ini, beberapa organisasi internasional dan negara berdaulat mengajukan pola tata kelola internasional dunia maya berikut ini:

(1) Pola Tata Kelola PBB: sebagai organisasi internasional yang paling berwenang di antara pemerintah, Perserikatan Bangsa-Bangsa telah mencoba mendominasi tata kelola internasional dunia maya, dengan mencoba mencapai kesepakatan internasional tentang tata kelola jaringan. Di antara mereka, KTT Dunia PBB tentang Masyarakat Informasi telah memainkan peran penting dalam proses tata kelola dunia maya internasional, menyediakan platform bagi para aktor internasional yang relevan untuk mengekspresikan tuntutan kepentingan mereka dan memainkan peran aktif dalam mempromosikan tata kelola dunia maya yang multidimensi. Namun, operasi Perserikatan Bangsa-Bangsa tidak dapat dipisahkan dari dukungan keuangan pemerintah, dan koherensi kebijakan Perserikatan Bangsa-Bangsa akan dibatasi sampai batas tertentu dengan syarat dibatasi oleh dana nasional. Pada tahun 2014, Amerika Serikat dengan tegas menolak menyerahkan kendali ICANN kepada Perserikatan Bangsa-Bangsa. Oleh karena itu, pola tata kelola PBB sulit untuk mengubah monopoli sumber daya jaringan yang dipimpin oleh Amerika Serikat.

(2) Pola Tata Kelola "Multi-stakeholder": Agenda Tunis, yang diadopsi oleh PBB pada tahun 2005, untuk pertama kalinya mengusulkan pola tata kelola "multi-stakeholder". Pada suatu waktu, pola ini dianggap sebagai pendekatan terbaik untuk tata kelola Internet, dan memberikan pola inovatif yang lebih universal dari tata kelola global. Pola "multi-stakeholder" mengakui keterbatasan manajemen pemerintah dalam dunia maya, mencoba mengeksplorasi peran organisasi non-pemerintah, dan menganjurkan praktik demokrasi partisipatif, untuk menentukan bentuk dan aturan Internet dan mewujudkan otonomi dunia maya. Meskipun pola ini memiliki beberapa efek dalam mengakomodasi kepentingan semua pihak, namun sulit untuk dipraktikkan. Model tata kelola "multi-stakeholder" tidak pasti dalam menentukan hak-hak pemangku kepentingan, dan secara umum dipertanyakan apakah para peserta dapat mencapai keberagaman dan mekanisme pembangkitan negara-negara yang representatif. Oleh karena itu, masih banyak cacat dalam pola ini dalam hal memenuhi ekuitas yang dikejar oleh negara-negara berkembang.

(3) Pola Tata Kelola yang Berpusat pada Negara: pola tata kelola yang berpusat pada negara menganjurkan tata kelola fungsi negara dari atas ke bawah dalam tata kelola dunia maya, dengan meyakini bahwa pemerintah adalah aktor utama dalam tata kelola dunia maya dan harus sepenuhnya menindak kejahatan jaringan dan menjaga

keamanan dunia maya. Hal ini memungkinkan negara-negara berkembang untuk menikmati hak yang sama dengan negara-negara maju, menghindari konflik kepentingan di antara para pemangku kepentingan dan desentralisasi organisasi, mengurangi biaya tata kelola, dan meningkatkan efisiensi tata kelola.

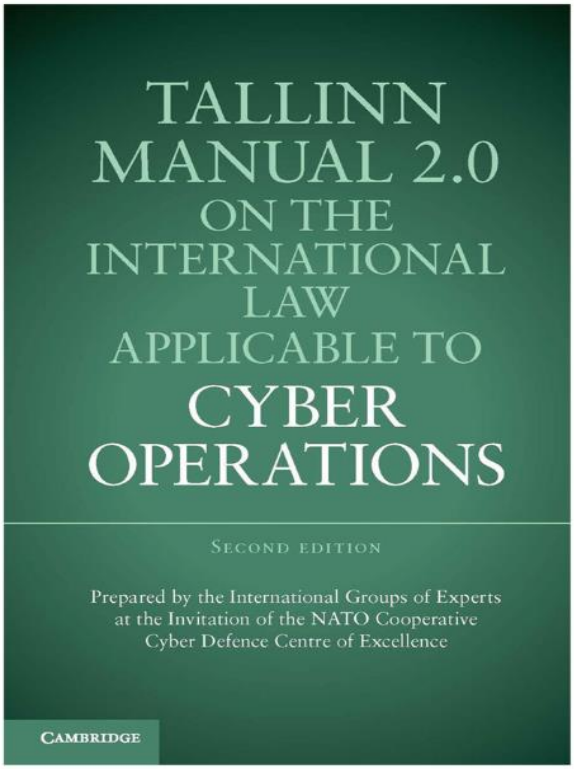
1.4 TINJAUAN UMUM KEDAULATAN JARINGAN

Mengambil kedaulatan nasional sebagai titik awal untuk mendorong perumusan kode etik internasional di Internet merupakan pilihan terbaik yang sesuai dengan kepentingan sebagian besar negara. Dihadapkan dengan pemahaman dan praktik kedaulatan jaringan, perlu dibentuk tindakan hukum dan saran untuk menjaga kedaulatan dunia maya internasional. Penting untuk membentuk sistem tata kelola dunia maya yang sejalan dengan realitas pembangunan semua negara, dan melindungi suara tata kelola internasional di dunia maya, menyediakan dasar teoritis untuk melawan hegemoni jaringan atas kekuatan teknologi, mempertahankan kedaulatan jaringan, mengatur dunia maya, dan berpartisipasi dalam perumusan aturan internasional yang relevan.

1.4.1 Konotasi Hukum Kedaulatan Jaringan

Apakah suatu negara dapat menjalankan yurisdiksi di dunia maya dianggap sebagai generasi pertama dari masalah kedaulatan dunia maya, dan bagaimana suatu negara menjalankan yurisdiksi dianggap sebagai generasi kedua dari masalah tersebut. Para sarjana Barat beranggapan bahwa masalah generasi pertama telah terpecahkan, dan kini kita tengah menghadapi masalah generasi kedua. Seperti disebutkan di atas, perbedaan pendapat utama dalam masyarakat internasional saat ini adalah bagaimana kedaulatan nasional dilaksanakan di dunia maya.

Keberadaan dan perkembangan dunia maya relatif singkat, dan telah berkembang pesat seiring dengan perkembangan teknologi informasi modern serta memiliki struktur yang lebih kompleks dan khusus. Pemahaman masyarakat terhadap dunia maya masih terus berkembang, dan pelaksanaan kedaulatan negara di dunia maya juga terus berkembang. Dikombinasikan dengan teori-teori dunia maya, praktik-praktik internasional yang relevan, dan komposisi dunia maya yang beragam, pelaksanaan kedaulatan negara di dunia maya tidak boleh digeneralisasikan, tetapi harus dianalisis dan diperlakukan secara berbeda berdasarkan kondisi aktual. Pertama, komposisi fisik dunia maya secara umum dianggap sebagai infrastruktur jaringan. Sebagai ruang buatan, dunia maya diciptakan oleh perusahaan-perusahaan dan individu-individu dari berbagai negara di dunia nyata melalui berbagai infrastruktur seperti komputer, router, dan server. Infrastruktur-infrastruktur ini adalah basis fisik atau perangkat keras dunia maya, dan didistribusikan dalam wilayah negara-negara berdaulat yang berbeda. Negara-negara memiliki kedaulatan penuh dan eksklusif atas infrastruktur jaringan ini. Meskipun negara-negara barat cenderung menekankan kewajiban negara-negara berdaulat terhadap infrastruktur jaringan, seperti pengawasan dan pencegahan. Mereka bahkan mendesak pemerintah keamanan informasi Perserikatan Bangsa-Bangsa untuk mengadopsi dokumen konsensus (A/70/174) yang memuat beberapa norma perilaku negara yang bertanggung jawab di ruang internasional.



Gambar 1.10 Sampul depan Manual Tallinn 2.0

Menurut analisis hukum, tidak ada negara yang dapat menggunakan fasilitas jaringan untuk melibatkan atau mengarahkan, mengendalikan pihak swasta untuk terlibat dalam tindakan yang melanggar kewajiban nasional. Hal ini telah lama disepakati dalam hukum internasional. Setiap negara harus memantau perilaku pribadi seseorang yang menggunakan infrastruktur jaringan di dalam batas negara untuk melakukan tindakan ilegal terhadap negara lain, tetapi kewajiban untuk melakukannya harus sepadan dengan kemampuan mereka dan tidak boleh diperkuat secara tidak semestinya. Kedua, mengenai informasi virtual di dunia maya, Internet telah menjadi salah satu pembawa terpenting transmisi dan pertukaran informasi kontemporer, yang menentukan bahwa transmisi dan penyimpanan informasi masif adalah salah satu fungsi inti dunia maya.

Karena sifat dunia maya yang global dan reproduktifitas data, penyimpanan dan transmisi data lintas batas adalah fenomena umum, yang juga merupakan salah satu perbedaan utama antara dunia maya dan ruang fisik tradisional. Apakah suatu negara dapat menjalankan yurisdiksi atas data di dunia maya merupakan masalah yang kompleks dan kritis. Singkatnya, kedaulatan jaringan suatu negara mencakup kedaulatan atas infrastruktur jaringan fisiknya dan kedaulatan atas informasi dan data jaringan yang tidak berwujud. Dalam hal peraturan khusus, sistem hukum laut negara bendera dapat digunakan sebagai acuan untuk menyelesaikan masalah di antara keduanya. Diskusi internasional tentang cara menjalankan kedaulatan negara di dunia maya menjadi hal yang teratur dan konkret. Misalnya, pada tanggal 2 Februari 2017, Manual Tallinn 2.0 tentang Hukum Internasional yang Berlaku untuk Operasi Siber, yang diterbitkan oleh Pusat Keunggulan Pertahanan Siber

Kooperatif NATO (CCDCOE), menguraikan kedaulatan jaringan dan yurisdiksi serta kewajiban kehati-hatian yang terkait dengannya (Gambar. 1.10).

1.4.2 Lapisan Kedaulatan Jaringan

Di masa lalu, fokus kedaulatan jaringan sering kali tertuju pada evolusi dan perluasan kedaulatan. Namun, telah menjadi fakta yang tak terbantahkan bahwa dunia maya, sebagai garis depan kelima, merupakan medan pertempuran penting bagi semua negara. Negara yang berbeda memiliki tuntutan yang berbeda untuk keamanan dunia maya, dan ketentuan kedaulatan jaringan mereka juga berbeda. Komunitas internasional harus menghormati dan memahami pandangan negara yang berbeda. Huang Zhixiong, seorang ahli hukum internasional di Tiongkok, mengajukan kerangka kerja tiga lapis untuk menganalisis kedaulatan jaringan, yang digunakan untuk menemukan domain yang berlaku sebelum eksklusivitas dan keterasingan.

1. **Lapisan Bawah**

   Lapisan bawah adalah lapisan fisik, yang mencakup berbagai infrastruktur jaringan. Pada tingkat ini, standardisasi internasional dan konektivitas global harus diupayakan. Untuk mengatasi kesenjangan digital, negara-negara perlu melakukan transfer kolektif dan negara-negara maju mengekspor hasil mereka ke negara-negara berkembang.

2. **Lapisan Tengah**

   Lapisan tengah adalah lapisan aplikasi, yang mencakup banyak aplikasi Internet dalam kehidupan nyata, dan mencerminkan aktivitas manusia dalam sains dan teknologi, budaya, ekonomi, perdagangan, dan kehidupan. Pada lapisan ini, pengaruh kedaulatan jaringan harus lebih disesuaikan dengan kondisi lokal, pemerintahan bersama yang dinamis, damai, multilateral, dan mencapai keseimbangan antara kebebasan dan ketertiban.

3. **Lapisan Atas**

   Lapisan atas adalah lapisan inti yang mencakup politik, hukum, keamanan politik, dan ideologi, yang terkait dengan fondasi pemerintahan. Itu adalah kepentingan inti suatu negara dan tidak dapat diganggu gugat. Keamanan siber tidak boleh digunakan sebagai alasan untuk menduplikasi pembagian kekuatan antara musuh dan diri kita sendiri di ruang tradisional. Semua Peradaban, budaya, dan negara harus saling menghormati dan hidup berdampingan secara damai. Seperti yang dikatakan pemimpin Tiongkok Xi Jinping dalam pidatonya di markas besar UNESCO pada tahun 2014, “pertukaran antar peradaban tidak boleh didasarkan pada superioritas atau derogasi satu peradaban”. Singkatnya, pada lapisan tengah dan lapisan bawah kerangka segitiga, kedaulatan jaringan dapat ditransfer sampai batas tertentu, sementara di lapisan atas, peran dominan pemerintah tercermin.

1.4.3 Peran Kedaulatan Jaringan di Setiap Tahap

Pandangan Tiongkok tentang kedaulatan jaringan mengekspresikan posisi Tiongkok dalam hubungan internasional di dunia nyata. Pandangan tersebut tidak memberikan penjelasan apa pun di luar konsep kedaulatan tradisional. Tiongkok menekankan kedaulatan

atas dunia maya dan memiliki pemahaman yang sangat jelas tentang tahap perkembangannya dan misi historis pemerintahnya.

Pada upacara pembukaan Konferensi Internet Dunia kedua (WIC, Wuzhen, Tiongkok), Presiden Tiongkok Xi Jinping menyatakan, "*Tujuan kami adalah membuat pencapaian pengembangan Internet bermanfaat bagi lebih dari 1,3 miliar orang Tiongkok dan orang-orang di negara lain*". Ia juga mengusulkan agar pengembangan Internet di Tiongkok harus dipandu oleh visi pembangunan yang berpusat pada rakyat, dan menyebutkan kedaulatan jaringan saat membahas hubungan antara keamanan dan pembangunan dalam pidato penting pada tanggal 19 April.

Oleh karena itu, pembangunan nasional harus dianggap sebagai prioritas utama, dan kedaulatan jaringan harus melayani pembangunan nasional. Negara harus memperjuangkan kedaulatan jaringan, memastikan bahwa setiap negara dapat secara mandiri merumuskan kebijakan dan rencana yang sesuai untuk pembangunannya sesuai dengan kondisi nasional di dalam negeri, mengupayakan partisipasi yang setara dalam tata kelola Internet, dan menjadikan tatanan dunia maya lebih adil dan merata. Singkatnya, jaringan kedaulatan, termasuk data, harus melaksanakan tujuan-tujuan untuk memajukan pembangunan nasional dan keamanan nasional.

1.5 PERLUNYA MENDUKUNG KEDAULATAN JARINGAN

Dengan latar belakang revolusi informasi dan globalisasi, kedaulatan jaringan berasal dari kedaulatan politik, kedaulatan ekonomi, dan kedaulatan budaya dalam proses pembentukan masyarakat informasi dan konsep informasi baru yang diwakili oleh Internet dan jaringan komunikasi elektronik global. Ini adalah bagian dari kedaulatan nasional modern. Meskipun interkomunikasi dan virtualisasi merupakan karakteristik khas dunia maya, realitas fondasinya, termasuk pembawa informasi, konten, dan fasilitas untuk transmisi informasi, menentukan bahwa dunia maya sama sekali bukan "tanah di luar hukum" yang mengecualikan kedaulatan negara dan tidak dapat dibiarkan berkembang tanpa batas.

1.5.1 Perlunya Membagi Kedaulatan Informasi

Istilah "informasi" diusulkan dan digunakan sebagai istilah ilmiah yang berasal dari tahun 1928 ketika L. R. V. Hartley membedakan antara "pesan" dan "informasi" dalam esainya Transmission of Information. Pembawa informasi bermacam-macam, seperti sinyal, intelijen, data, materi, pengetahuan, simbol, dan sebagainya. Dalam pengertian hukum, informasi sebagai suatu bentuk sumber daya tidak hanya merupakan gambaran informasi di dunia fisik, tetapi juga merupakan keberadaan yang konkret dan dapat dideskripsikan, yaitu suatu sistem simbol yang memenuhi syarat-syarat tertentu. Yang menjadi perhatiannya adalah masalah apakah isi informasi itu sah, apakah cara produksi, perolehan, dan penyebaran informasi itu sah, tanggung jawab hukum apa yang harus dipikul atas produksi, perolehan, dan penyebaran informasi yang tidak sah, dan bagaimana cara memikul tanggung jawab hukum tersebut. Inti dari penerapan internet adalah pertukaran informasi. Melalui penerapan teknologi komunikasi, keluaran dan transmisi informasi secara instan dapat dicapai. Segala sesuatu di dunia dapat dihitung, diukur, direkam, dan dianalisis dalam bentuk data, lalu dibagikan ke

seluruh dunia. Terdapat hubungan kepentingan yang kompleks di antara negara-negara di dunia. Dalam hukum internasional tradisional, yang berlandaskan kedaulatan teritorial, suatu negara memiliki kedaulatan tertinggi atas semua orang, benda, urusan, dan tindakan di dalam wilayahnya, termasuk arus informasi. Oleh karena itu, tidak diragukan lagi bahwa manusia memiliki batas-batas negara ketika menggunakan teknologi komunikasi untuk memperoleh dan menyebarluaskan sumber daya, terutama konten sumber daya harus mematuhi ketentuan hukum negara berdaulat.

Masyarakat internasional telah mencapai konsensus tentang perlindungan privasi pribadi dan hak kekayaan intelektual di bidang penyebaran informasi daring, serta pengawasan terhadap hal-hal yang melibatkan narkoba, kekerasan, pornografi, dan membahayakan keamanan nasional. Hal ini juga membuktikan bahwa meskipun informasi merupakan keberadaan data virtual, kontennya terkait dengan semua aspek ekonomi, politik, dan budaya suatu negara, dan jaminan keamanan informasi memengaruhi keamanan negara dan hak-hak warga negara. Namun, Internet telah sangat melemahkan kontrol negara atas penyebaran informasi dan perilaku individu di dalam wilayahnya. Serangan jaringan juga mengancam infrastruktur jaringan nasional dan sistem informasi vital, yang memerlukan perlindungan oleh militer. Apabila kedaulatan jaringan diabaikan dan kedaulatan negara yang berada di atasnya tidak diakui, maka hal tersebut merupakan bentuk pengingkaran terhadap eksistensi kedaulatan informasi dan penolakan terhadap independensi kedaulatan serta perlindungan kedaulatan yang setara dalam nilai-nilai hukum.

1.5.2 Perlunya Wilayah Jaringan

Dalam bidang informasi tradisional, seperti surat kabar, buku, radio, dan televisi, negara dapat berperan dalam pengendalian. Namun, dalam dunia internet, kontradiksi antara regionalisme kedaulatan negara dan sifat jaringan yang lintas batas merupakan masalah yang sulit bagi negara untuk mengendalikan penyebaran informasi internet.

Dunia maya hadir dalam bentuk virtualisasi berdasarkan pembawa data. Tidak diragukan lagi bahwa kontennya dan sumber atau sarana transmisi data memiliki signifikansi praktis. Semakin banyak orang menampilkan identitas, perilaku, properti, dan kepentingan mereka di dunia maya. Semakin banyak pembayaran keuangan dan perdagangan internasional dilakukan melalui platform daring. Ruang nyata dan dunia maya menunjukkan tren fusi bertahap. Pada saat yang sama, lokasi geografis dan lingkungan ruang masyarakat bergantung pada wilayah dan yurisdiksi negara. Singkatnya, dunia maya tidak dapat menjadi keberadaan yang tidak nyata.

Jaringan membawa kemudahan yang sangat besar bagi kehidupan dan produksi manusia. Akan tetapi, di sisi lain, muncul pula tindakan-tindakan ilegal seperti serangan hacker, virus jaringan, dan sebagainya. Sebagian orang memanfaatkan internet untuk melakukan tindakan-tindakan yang melanggar hukum internasional, seperti perdagangan manusia, perdagangan narkoba, dan perdagangan senjata. Di samping itu, sebagian orang memanfaatkan kemudahan dan kesulitan dalam memantau internet untuk melakukan tindak pidana. Dilema-dilema ini memengaruhi keamanan ekonomi, politik, dan budaya suatu negara. Jika keamanan dunia maya tidak terjamin, maka akan sulit untuk menyelesaikan

sengketa jaringan yang rumit, dan keamanan negara serta warga negara akan terancam dalam jangka panjang, yang tidak mendukung perkembangan teknologi informasi.

Dunia maya telah menjadi wilayah kelima negara, di samping empat wilayah yaitu darat, laut, udara, dan angkasa. Keamanan dunia maya memengaruhi dan menentukan keamanan wilayah lain sampai pada taraf tertentu. Penguatan konsep kedaulatan jaringan memungkinkan pemerintah, dalam posisi menjaga kedaulatan nasional, dan memiliki hak untuk membangun keamanan informasi nasional di batas jaringan dan meninjau informasi yang diekspor dan diimpor.

1.5.3 Perlunya Membuat Aturan Berdasarkan Hukum

Teknologi informasi diciptakan oleh manusia. Kode dapat mengontrol identitas, waktu, tempat penggunaan jaringan. Input kode yang berbeda akan menghasilkan hasil yang berbeda, yang menentukan perbedaan aktivitas jaringan. Oleh karena itu, pengendalian merupakan salah satu fondasi arsitektur Internet. Internet membutuhkan aturan operasi tertentu untuk menjamin fungsi dasarnya, seperti otentikasi, kompatibilitas, interkoneksi, dan sebagainya. Dari aturan operasi Internet, kita juga dapat melihat pengendalian dunia maya. Dunia maya melibatkan faktor teknologi, politik, ekonomi, budaya, dan lainnya, sehingga aturan perlu dirumuskan.

Sistem hukum nasional memiliki signifikansi besar terhadap penyesuaian perilaku jaringan, tetapi ada juga banyak keterbatasan. Khususnya, ketika ruang virtual membawa hubungan hukum yang nyata, karakteristik Internet membawa serangkaian kesulitan untuk penerapan dan implementasi hukum, dan kelayakan serta legitimasi hukum tradisional berbasis wilayah pun dipertanyakan. Oleh karena itu, konsep kedaulatan jaringan memudahkan pembuatan undang-undang di dunia maya dan memberikan dukungan teoritis untuk penerapan hukum yang ada di dunia maya.

Dunia kode tidak dapat dipisahkan dari regulasi hukum. Tata kelola hukum harus dipadukan dengan tata kelola teknis. Tata kelola hukum lebih diutamakan daripada tata kelola teknis, dan tata kelola teknis tidak boleh menerobos kerangka tata kelola hukum. Ada banyak preseden yang membuktikan pentingnya merumuskan aturan jaringan berdasarkan hukum. Misalnya, Pengadilan Virginia Amerika Serikat memutuskan bahwa cnnews.com, nama domain yang didaftarkan oleh Shanghai Meiya Company, melanggar hak merek dagang CNN. Ketika pengadilan memutuskan untuk menangguhkan nama domain tersebut, hal itu menunjukkan bahwa pemerintah telah campur tangan dalam tata kelola dunia maya. Pada saat yang sama, karena jaringan dapat dikendalikan, maka perilaku yang berkaitan dengan kepentingan nasional dapat dikendalikan, untuk mencapai tujuan melindungi keamanan dunia maya nasional. Selain itu, beberapa kasus, seperti persyaratan penyaringan Jerman terhadap penyebaran informasi ilegal di Internet dan tindakan keras Singapura terhadap pernyataan ekstremis melalui model Internet, membuktikan adanya pengendalian dunia maya dan menunjukkan perlunya merumuskan aturan berdasarkan hukum. Dari perspektif menjaga keamanan nasional dan menjaga perdamaian dan keamanan dunia, perlu untuk mengatur dunia maya secara tepat di tingkat nasional dan mengakui keberadaan kedaulatan jaringan.

1.6 JARINGAN KEDAULATAN YANG DIATUR BERSAMA

1.6.1 Jaringan IP dan Kelemahannya

Internet berawal dari Amerika Serikat, yang mendefinisikan standar jaringan IPv4 saat ini, memimpin dunia dalam teknologi IP, dan menciptakan ruang virtual berbasis DNS untuk masyarakat manusia. ICCAN, sebuah organisasi swasta di California, adalah administrator DNS. Secara objektif, Amerika Serikat memiliki keuntungan monopoli sepihak atas negara-negara lain di dunia maya, dan negara-negara lain hanyalah pengguna Internet AS. Namun, tiga peristiwa berikut terjadi di Amerika Serikat:

a) Setelah bentrokan berdarah yang terjadi pada tanggal 6 Januari 2021, ketika Kongres diserbu oleh pendukung Trump, platform daring terbesar di negara itu, termasuk Twitter, Facebook, Google, Apple, YouTube, Reddit, Instagram, Snapchat, Discord, Pinterest, memblokir semua konten yang diposting oleh Presiden Trump dan timnya dan menutup akun media sosial mereka. Orang paling berkuasa di dunia, Presiden AS yang pernah memberi wewenang kepada militer Amerika untuk melancarkan serangan siber ke negara lain, tiba-tiba kehilangan saluran daringnya untuk berkomunikasi dengan puluhan juta pemilihnya tanpa proses peradilan dalam setengah bulan terakhir masa jabatannya, tetapi tidak ada yang dapat ia lakukan. Raksasa internet AS dengan mudah mengesampingkan kebebasan berbicara Presiden AS! Sistem supremasi hukum yang dibatasi oleh pemisahan kekuasaan legislatif, yudikatif, dan administratif telah hilang di dunia maya virtual. Di manakah hukum dan keadilan?

b) Pada tanggal 17 Desember, Badan Keamanan Siber dan Keamanan Infrastruktur (CISA) Departemen Keamanan Dalam Negeri AS mengeluarkan "peringatan yang sangat tidak biasa" yang mengatakan bahwa serangan siber terhadap lembaga pemerintah AS dan perusahaan swasta telah berlanjut selama seminggu terakhir, mencapai tingkat risiko "serius" tertinggi pada saat kritis untuk pemilihan presiden 2020. Data dari beberapa mesin pemungutan suara Dominion yang terhubung ke Internet secara misterius terhapus, dan bahkan data pemilu terhapus dari server lokal di beberapa daerah. Telah ditunjukkan bahwa tujuan akhir dari serangan siber tersebut mungkin adalah para peretas yang mencoba menghancurkan data kecurangan pemilu! Apakah itu negara yang bermusuhan atau kampanye domestik yang bermusuhan? AS, tempat lahirnya teknologi jaringan IP, dan kampanye politik terbesarnya, pemilihan presiden, dimanipulasi dan diganggu oleh para penentangnya! Bagaimana kinerja birokrasi keamanan siber pemerintah AS?

c) Pada tahun 2013, Edward Joseph Snowden, mantan karyawan CIA, melarikan diri ke Hong Kong untuk mencari suaka politik di Rusia. Ia mengungkapkan bahwa Badan Keamanan Nasional (NSA) telah menjalankan program pengawasan elektronik rahasia, PRISM, sejak tahun 2007 di bawah George W. Bush. Secara resmi dikenal sebagai US-984XN, program tersebut memantau komunikasi dan aktivitas Internet semua warga Amerika. Warga negara Amerika tidak memiliki privasi apa pun. Bagaimana hak asasi

manusia dan privasi warga negara dapat dilindungi dan dihormati? Apa yang terjadi dengan hak-hak alami Konstitusi AS?

Alasan terjadinya peristiwa di atas adalah bahwa arsitektur IP saat ini memiliki cacat bawaan. Alasan untuk (A) adalah bahwa nama domain IP dikelola oleh satu organisasi, dan akun pengguna di setiap situs Web hanya dikelola oleh platform itu sendiri, sehingga mudah untuk menghapus pengguna. Alasan mengapa peristiwa kelas (B) sering terjadi adalah bahwa keuntungan asimetris dari musuh jelas, yang berasal dari kekurangan bawaan arsitektur jaringan IP paket datanya tidak dapat dilacak dan tidak ada jaminan keamanan. Alasan untuk (C) adalah bahwa privasi data pengguna di jaringan IP tidak dijamin, yang pada dasarnya adalah streaking.

Kelebihan semantik IP mencakup atribut ganda identitas dan lokasi, paket data yang tidak dapat dilacak, keamanan yang tidak terjamin dan kinerja layanan yang tidak terjamin, dll., yang membuatnya tidak sesuai untuk persyaratan seluler, waktu nyata, dan keamanan tinggi di Internet masa depan. Oleh karena itu, sekuat apa pun Amerika Serikat, lembaga-lembaga pemerintah dan perusahaan-perusahaannya, pejabat-pejabat senior dan warga biasa semuanya sangat khawatir dan gelisah tentang keadaan Internet saat ini, termasuk arsitektur teknologinya, operasinya, pengelolaannya, dan tata kelolanya. Belum lagi negara-negara lain yang menggunakannya.

1.6.2 Jaringan Kedaulatan

Seruan dari Sebagian Besar Negara di Dunia

Setelah Peristiwa Snowden pada tahun 2013, Uni Eropa, Inggris, Rusia, dan Tiongkok menyerukan pengelolaan bersama atas dunia maya manusia, tetapi sejauh ini belum ada kemajuan nyata. Demi keamanan Rusia sendiri, pada bulan Februari 2020, Presiden Putin memerintahkan dimulainya uji coba jaringan yang rusak, membangun "jaringan internal", infrastruktur Internet terbesar di dunia yang berbasis pada Jaringan Rusia (RuNet) yang dibangun sendiri. DNS yang dikendalikan oleh pemerintah Rusia diterapkan untuk mengalihkan lalu lintas domestik, tidak lagi bergantung pada akar DNS di luar negeri.

Presiden Tiongkok Jinping XI mengemukakan bahwa "tidak ada keamanan dunia maya, tidak ada keamanan nasional." Pada Konferensi Internet Dunia 2015 di Wuzhen, Tiongkok, ia mengusulkan semua negara untuk bersatu untuk "mempromosikan reformasi sistem tata kelola Internet global, bersama-sama membangun dunia maya yang damai, aman, terbuka, dan kooperatif, serta membangun sistem tata kelola Internet global yang multilateral, demokratis, dan dikelola bersama." Ini adalah aspirasi bersama semua negara di dunia.

Cog-MIN: Solusi Pertama untuk Jaringan Kedaulatan di Dunia

Oleh karena itu, dalam konteks tata kelola bersama dunia maya global, penulis buku ini mengusulkan arsitektur jaringan multi-pengenal yang diatur bersama (Cog-MIN, atau disingkat MIN). Kami menciptakan konsorsium blockchain berskala besar berdasarkan satu suara untuk satu negara untuk mengelola nama domain teridentifikasi tingkat atas. Secara luas, konsorsium blockchain hierarkis digunakan untuk manajemen independen di setiap negara. Log perilaku pengguna di semua tingkatan direkam oleh blockchain di semua tingkatan. Cog-MIN diusulkan untuk menjadikan identitas sebagai identitas inti dasar yang

sangat diperlukan. Untuk kompatibilitas dengan IP, Cog-MIN mendukung identifikasi jaringan termasuk alamat IP, konten, layanan, dll., pada saat yang sama. Ia menggunakan kriptografi asimetris untuk mendukung semua keterlacakan data, sehingga keamanan dan keandalan yang tinggi menjadi DNA arsitektur Cog-MIN. Cog-MIN telah memecahkan dilema jaringan IP terkait pengenal tunggal dan manajemen terpusat. Bidang manajemennya menggunakan sistem multi-pengenal (MIS), yang mendukung koeksistensi pengenal jaringan termasuk identitas, konten, informasi geografis, dan alamat IP. Sistem ini dibangun berdasarkan blockchain konsorsium pemungutan suara untuk memastikan perlindungan privasi dan pengelolaan secara bersamaan. MIS mengharuskan semua pengguna untuk mendaftar menggunakan identitas asli mereka dan menyimpan data menggunakan teknik kriptografi modern. MIN mengubah jaringan menjadi ruang yang aman, damai, demokratis, dan transparan, alih-alih ruang tanpa aturan hukum.

MIN mengusulkan mekanisme penandatanganan dan penerimaan data yang dapat dilacak pada bidang data. Peralatan inti MIN adalah router multi-pengenal (MIR) yang mengintegrasikan berbagai inovasi. Yang pertama adalah algoritma HPT-FIB dengan menggabungkan tabel hash dan pohon awalan yang mendukung intertranslasi antara berbagai jenis pengidentifikasi dalam ukuran puluhan miliar entri. Yang kedua adalah model pengalamatan berdasarkan pemetaan koordinat dalam ruang hiperbolik, untuk menangani pertumbuhan eksponensial tabel FIB. Yang ketiga adalah skema terowongan untuk mengangkut paket IP melalui MIN, untuk mendukung penyebaran MIN secara progresif pada jaringan IP. Arsitektur MIN yang diusulkan dalam buku ini mendukung de-IP alami dan progresif, yang akan dipilih oleh pengguna dan pasar tanpa harus melakukan de-IP secara kompulsif. Dapat diprediksi bahwa di masa mendatang, IP akan tetap berada di posisi utama di AS, sementara negara-negara lain secara bertahap akan meninggalkan IP dan menggunakan MIN untuk kedaulatan mereka sendiri di dunia maya. MIN memastikan interkoneksi antara jaringan kedaulatan setiap negara dan jaringan IP AS. Dengan kata lain, IP menjadi jaringan internal Amerika sendiri, sementara negara-negara lain membentuk sistem jaringan multilateral berdasarkan MIN.

1.6.3 Jaringan Kedaulatan yang Diatur Bersama

Prototipe Berdasarkan Cog-MIN

Skenario penerapan MIN dapat diklasifikasikan ke dalam tiga skala:

(1) skenario skala kecil seperti jaringan privat keamanan tinggi perusahaan, industri, dan departemen pemerintah;

(2) skenario skala menengah Internet industri, jaringan privat Internet kendaraan, dan kota pintar;

(3) Ruang siber keamanan tinggi skala besar untuk kondominium multilateral dan otonomi kedaulatan untuk menggantikan jaringan IP yang ada, Perserikatan Bangsa-Bangsa untuk Ruang Siber (UNC) untuk Jaringan Kedaulatan Negara-negara berdasarkan Cog-MIN.

Pada bulan Maret 2019, kami telah berhasil meluncurkan prototipe pengujian pertama jaringan kedaulatan yang diatur bersama di dunia berdasarkan Cog-MIN pada jaringan

operator di wilayah Tiongkok Raya. Pada bulan Oktober 2019, MIN dan sistem prototipe-nya dipilih sebagai pencapaian teknologi terkemuka dari Konferensi Internet Dunia Keenam di Wuzhen, Tiongkok. Cog-MIN mengambil identitas sebagai identifikasi jangkar dan mendukung beberapa mekanisme pengalamatan, perutean, dan fallback identifikasi. Mengambil identitas sebagai pengenal jangkar, Cog-MIN mendukung beberapa mekanisme pengalamatan, perutean, dan fallback pengenal. IPv4, IPv6, IPv9, NewIP, Jaringan 5.0, dan Pengidentifikasi Jaringan Masa Depan yang dikenal seperti konten dan layanan semuanya dapat diintegrasikan pada arsitektur Cog-MIN.

Sistem manajemen multi-pengenal yang berbasis pada konsorsium blockchain skala besar hierarkis dan algoritma penerjemahan multi-pengenal mendukung persyaratan di atas dari penerjemahan, pengalamatan, dan perutean beberapa pengidentifikasi. Cog-MIN akan mengakhiri persyaratan peningkatan berkelanjutan arsitektur jaringan dengan evolusi berkelanjutan skema pengalamatan dan perutean lapisan jaringan, yang kondusif bagi koeksistensi dan transisi alami berbagai sistem identifikasi. Ini akan sangat menghemat biaya dan memperpanjang siklus layanan peralatan yang ada hingga kemampuannya yang terbaik. Diharapkan bahwa Cog-MIN untuk arsitektur jaringan paket data adalah apa yang dilakukan Signaling No. 7 untuk sistem telekomunikasi. Dukungan Signaling No. 7 untuk layanan dasar dan berbagai layanan cerdas masa depan telah menjadikannya terminator dari semua sistem persinyalan sebelumnya sejak No. 1.

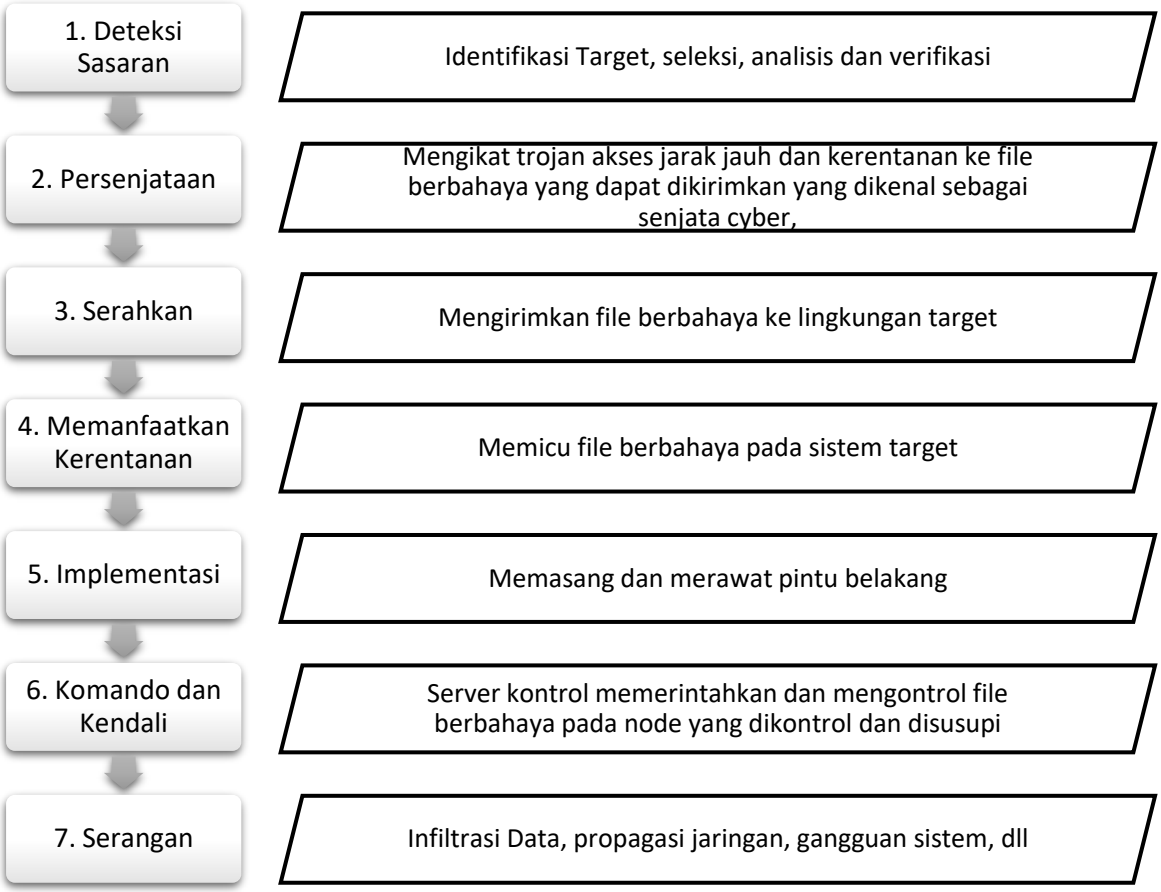
Sekarang jaringan pribadi berdasarkan Cog-MIN, yang digunakan pada jaringan IP operator, telah diterapkan pada beberapa skenario tertentu. Dalam hal tujuannya untuk menjadi Perserikatan Bangsa-Bangsa yang benar-benar multilateral dan mengatur dunia maya secara global, Cog-MIN masih dalam tahap konseptual dan awal, dengan banyak pekerjaan perintis yang belum dilakukan oleh rekan-rekan global. Tujuan penerbitan buku ini sekarang, menurut pepatah Tiongkok, adalah untuk "melempar batu bata dan menarik batu giok." Kami ingin menyumbangkan ide-ide kami untuk membangun dunia maya yang damai, aman, terbuka, dan kooperatif yang diatur oleh aturan hukum untuk seluruh umat manusia.

MIN-VPN Versus IP-VPN: Peningkatan Keamanan Eksponensial Telah Dibuktikan

Sejak 2020, dengan tujuan memenuhi persyaratan keamanan tinggi, kami telah mengembangkan versi pertama dari produk sistem MIN-VPN jaringan pribadi keamanan tinggi ini berdasarkan Cog-MIN untuk memenuhi kebutuhan praktis pengguna seperti kantor seluler, manajemen identitas, manajemen hak, penyimpanan log, deteksi perilaku, dan autentikasi identitas. Ini mengintegrasikan blockchain skala besar, informasi geospasial, biometrik pribadi, komputasi tepercaya, kriptografi, keamanan endogen, AI, dan teknologi lainnya. Ini menyediakan lima fitur keamanan yang ditetapkan oleh industri global: autentikasi, kontrol akses, kerahasiaan data, integritas data, dan non-repudiasi.

Ini dapat secara efektif menahan pelanggaran otorisasi, serangan peniruan identitas, kontrol bypass, kuda Troya atau trap gate, dan serangan lainnya. Min-VPN menggunakan berbagai cara autentikasi teknis untuk memastikan keamanan sistem. Pengguna ilegal pertama-tama perlu mencuri kata sandi akun dan kunci pribadi pengguna, kemudian berpura-pura lolos dari deteksi in vivo, dan akhirnya menerobos beberapa mekanisme pertahanan

keamanan internal untuk mencuri sumber daya jaringan internal. MIN-VPN memadukan arsitektur perlindungan hierarkis dari beberapa mekanisme keamanan dan membangun model pertahanan keamanan yang dinamis dan terpadu melalui verifikasi kata sandi, verifikasi sertifikat, deteksi in vivo, deteksi perilaku cerdas, dan keamanan endogen, yang dapat mengurangi tingkat keberhasilan serangan hingga di bawah urutan sepuluh hingga dua puluh kecil, atau 10−20 (Gambar 1.11).



Gambar 1.11 Model rantai serangan klasik dan pemilihan mode serangan

Kami telah menerapkan MIN-VPN pada jaringan IP operator, dengan mengambil IP-VPN arus utama sebagai sistem referensi, dan menggunakan rantai serangan klasik dan metode serangan untuk melakukan berbagai uji serangan komparatif. Setelah pengujian yang lama oleh sejumlah tim profesional pihak ketiga, hasilnya menunjukkan bahwa lingkungan MIN-VPN dapat secara efektif melindungi dan melawan serangan jaringan IP tradisional di semua tautan rantai serangan di bawah skenario jaringan IP ke MIN dan MIN ke MIN, sedangkan IP-VPN tidak dapat melakukannya. Hasil pengujian ditunjukkan sebagai berikut (Gambar 1.12).

Fase Serangan	Tujuan penyerangan	Hasil Test IP-IP	Hasil Test IP-MIN	Hasil Test MIN-MIN

Pengintaian	Host discovery		Dapat Ditemukan	Temukan host uang bukan milik CUTV	Tidak ada yang ditemukan
	Pemindaian Ping		Dapat dideteksi	Tidak terdeteksi	Tidak terdeteksi
	Identifikasi Sistem Operasi		Sidikjari sistem dapat diperoleh	Tidak ada yang ditemukan	Tidak ada yang ditemukan
	Port Scan		Dapat mendeteksi semua layanan port	Tidak dapat menemukan informasi port apapun	Tidak ada yang ditemukan
Eksploitasi	Implantasi trojan	Trojan TCP	Terhubung	Tidak dapat Terhubung	Tidak dapat Terhubung
		Trojan UDP	Terhubung	Tidak dapat Terhubung	Tidak dapat Terhubung
		Trojan ICMP	Terhubung	Tidak dapat Terhubung	Tidak dapat Terhubung
	Web Shell		Terhubung	Tidak dapat Terhubung	Tidak dapat Terhubung
Tindakan	Keracunan ARP	Sniff	Sniff Successfully	Non-Intranet	Sniff failed
		Forced disconnection	Terputus	Non-Intranet	Gagal

Gambar 1.12 Hasil Percobaan Pengujian IP ke IP-VPN versus IP ke MIN-VPN, MIN ke MIN

Untuk informasi lebih lanjut tentang sistem dan produk kami, silakan kunjungi situs web MIN. Kami bersedia menyediakan produk atau layanan kepada pelanggan di berbagai negara untuk tujuan nonmiliter. Jika waktunya tepat, kami dapat menyumbangkan kode sumber MIN kepada komunitas global.

BAB 2
INTERPRETASI KEDAULATAN JARINGAN

2.1 KOMUNITAS INTERNASIONAL DAN KEDAULATAN JARINGAN

Dalam beberapa tahun terakhir, dengan integrasi Internet dan berbagai bidang ekonomi dan sosial, situasi keamanan di dunia maya telah berubah dengan cepat. Semakin banyak permainan jaringan di tingkat nasional dan serangan serta pertahanan jaringan menjadi lebih intens. Kedaulatan jaringan telah menjadi salah satu kedaulatan yang diperjuangkan semua negara.

Sejak pembentukan prinsip kedaulatan nasional oleh Dewan Perdamaian Westphalia pada tahun 1648, menegakkan kedaulatan dan menentang hegemoni telah menjadi isi penting dari praktik tata kelola internasional. Lebih dari 30 tahun setelah kelahirannya, sistem DNS telah terbukti lebih tangguh dari yang diharapkan sebagai infrastruktur Internet. Namun, domain root, domain tingkat atas yang penting, dan sertifikat root sebelumnya dikendalikan oleh pemerintah AS atau oleh ICANN nirlaba yang disahkan pemerintah AS karena beberapa faktor historis. Selain itu, serangan terhadap sistem nama domain telah menjadi salah satu ancaman paling signifikan terhadap keamanan Internet global. Kemampuan otonom Internet di berbagai kawasan, yaitu kedaulatan jaringan, selalu terancam, dan masyarakat internasional telah lama mengkhawatirkan hal ini.

Pada tahun 2003, World Summit on the Information Society (WSIS) diadakan di Jenewa. Konferensi tersebut mengadopsi Deklarasi Prinsip Jenewa, yang menguraikan kedaulatan jaringan negara-negara, “otoritas kebijakan untuk isu-isu kebijakan publik yang terkait dengan Internet adalah hak kedaulatan Negara. Mereka memiliki hak dan tanggung jawab untuk isu-isu kebijakan publik internasional yang terkait dengan Internet”. Pada tanggal 2 Februari 2017, NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) mengumumkan di situs webnya bahwa Manual Tallinn 2.0 telah diterbitkan secara resmi. Dibandingkan dengan versi awal, Manual Tallinn 2.0 membagi dunia maya menjadi tiga lapisan: lapisan fisik, lapisan logis, dan lapisan sosial, dan menetapkan bahwa semua objek, fasilitas, dan personel yang terlibat dalam ketiga lapisan ini dapat dikendalikan oleh negara berdasarkan prinsip kedaulatan. Pada saat yang sama, Manual tersebut juga menegaskan bahwa negara memiliki kedaulatan eksternal di bidang dunia maya dan negara bebas untuk terlibat dalam aktivitas jaringan dan menyetujui perjanjian jaringan internasional.

Sejak inti strategi AS bergeser dari pertahanan komprehensif menjadi serangan dan pencegahan pada tahun 2015, persaingan antarnegara untuk mendapatkan dominasi dan kekuatan wacana di dunia maya menjadi lebih ketat. Pada tanggal 14 Desember 2017, Komisi Komunikasi Federal mengumumkan penghapusan prinsip netralitas jaringan. Pada tahun yang sama, Inggris menggunakan serangan siber dan pengacauan untuk pertama kalinya dalam operasi militer gabungan. Pada tanggal 12 Februari 2019, Duma Negara Rusia mengesahkan sebuah rancangan undang-undang, yang dirancang untuk memastikan pengoperasian

Internet di negara tersebut jika akses ke server di luar negeri terputus. Pemerintah Jepang merilis Rencana Kesiapan Angkatan Pertahanan Jangka Menengah yang baru, yang berencana untuk membentuk sebuah komando guna mengoordinasikan pasukan profesional di luar angkasa dan dunia maya dari tahun 2019 hingga 2023 untuk meningkatkan ukuran dan kemampuan pasukan pertahanan jaringan.

Kode Etik Internasional untuk Keamanan Informasi (selanjutnya disebut "Kode") merupakan sebuah upaya internasional untuk mengembangkan norma-norma perilaku di ruang digital, yang diajukan ke Majelis Umum PBB pada tahun 2011 oleh Tiongkok dan Rusia. Pada tahun 2015, Tiongkok bersama dengan perwakilan tetap Perserikatan Bangsa-Bangsa dari negara-negara anggota Organisasi Kerja Sama Shanghai menulis surat kepada Sekretaris Jenderal Perserikatan Bangsa-Bangsa dan mengajukan Kode yang telah direvisi, yang isinya tercermin dalam resolusi Majelis Umum Perserikatan Bangsa-Bangsa tahun itu. Resolusi tersebut menegaskan kembali bahwa, "Kewenangan kebijakan untuk masalah publik yang terkait dengan Internet adalah hak kedaulatan Negara, yang memiliki hak dan tanggung jawab untuk masalah kebijakan publik internasional yang terkait dengan Internet", dan mengklaim bahwa "mematuhi Piagam PBB dan norma-norma yang diakui secara universal yang mengatur hubungan internasional, termasuk penghormatan terhadap kedaulatan, integritas teritorial, dan kemerdekaan politik semua negara", dan "Semua negara memiliki hak dan tanggung jawab untuk melindungi, berdasarkan hukum dan peraturan yang relevan, ruang informasi dan infrastruktur informasi penting mereka dari ancaman, gangguan, serangan, dan sabotase".

Pada upacara pembukaan Konferensi Internet dunia kedua, pemimpin Tiongkok Xi Jinping menunjukkan bahwa, "Komunitas internasional harus memperkuat dialog dan kerja sama berdasarkan rasa saling menghormati dan percaya, mempromosikan reformasi sistem tata kelola Internet global, dan bersama-sama membangun dunia maya yang damai, aman, terbuka, dan kooperatif, dan membangun sistem tata kelola Internet global yang multilateral, demokratis, dan transparan".

2.2 KOMENTAR INTERNASIONAL TENTANG KEDAULATAN JARINGAN

Alvin Toffler, seorang sosiolog terkenal, meramalkan dalam bukunya Third Wave pada tahun 1980-an bahwa, "*Siapa pun yang menguasai informasi dan mengendalikan Internet, akan menguasai dunia*". Saat ini, dengan berkembangnya bidang informasi jaringan, ramalan ini telah terverifikasi. Setelah memasuki abad ke-21, negara-negara melakukan berbagai tindakan jaringan, seperti kasus phishing Syrian Electronic Army, uji coba internet Rusia yang tidak terhubung ke internet, dan sebagainya, permainan antarnegara sedang dimainkan di dunia maya.

2.2.1 Era Perang Siber

Keamanan dan stabilitas nasional terkait erat dengan kedaulatan jaringan. Sejak akhir abad ke-20, pembangunan kekuatan jaringan di berbagai negara terus diperkuat, dan teknologi serta sarana serangan jaringan telah muncul satu demi satu (Gbr. 2.1).

Estonia

Estonia adalah negara pertama dalam sejarah yang mengalami serangan siber besar-besaran terhadap pemerintahan dan infrastruktur pentingnya. Dalam tiga minggu dari April hingga Mei 2007, Estonia dilanda serangan jaringan besar-besaran, yang difokuskan pada situs web presiden dan parlemen Estonia, berbagai departemen pemerintah, partai politik, tiga dari enam organisasi berita utama, dua bank terbesar, dan perusahaan komunikasi. Ketika serangan itu terjadi, hal itu menyebabkan guncangan hebat di daerah setempat, dan hampir semua situs web lumpuh, yang menyebabkan kerugian besar. Skala dan intensitas serangan siber di Estonia telah menarik perhatian komunitas militer internasional, dan itu dianggap sebagai perang siber pertama di tingkat nasional.

Gambar 2.1 Perang siber saat ini kisah dari medan perang digital (berita Lima Charlie)

Irak

Dalam hal pengoperasian Internet, karena jaringan di Asia dan Eropa melewati Amerika Serikat, Amerika Serikat dapat mengendalikan server root untuk menghitung dan memantau informasi relevan yang diselesaikan oleh semua server, seperti jumlah kunjungan dan frekuensi klik situs web. Selama Perang Irak pada tahun 2003, Amerika Serikat menggunakan hak resolusi server root untuk membatalkan semua pekerjaan penguraian aplikasi nama domain Irak "iq", dan semua nama domain Irak dengan sufiks "iq" tidak dapat dicari dari Internet, yang merupakan pukulan telak bagi kedaulatan jaringan Irak.

Libya

Pada bulan April 2004, Amerika Serikat melancarkan serangan jaringan yang menjatuhkan nama domain tingkat atas Libya, membuat situs dengan sufiks "ly" (singkatan Libya) tidak dapat dicari di mesin pencari, dan Libya menghilang dari Internet selama tiga hari.

Suriah

Pada tahun 2013, Syrian Electronic Army mengakses akun Twitter Associated Press (AP) dengan menyertakan tautan berbahaya dalam email phishing. Email tersebut dikirim ke

karyawan AP atas nama seorang kolega. Para peretas kemudian memposting laporan berita palsu di akun AP yang mengatakan telah terjadi dua ledakan di Gedung Putih dan Presiden Barack Obama telah terluka. Reaksi tersebut sangat dramatis sehingga pasar saham anjlok 150 poin dalam lima menit.

Iran

Pada bulan Agustus 2010, pembangkit listrik tenaga nuklir Bushehr di Iran diserang oleh virus jaringan komputer yang tidak diketahui asalnya. Setidaknya 30.000 komputer Iran diserang, sehingga pembangkit listrik tenaga nuklir Bushehr di Iran, yang baru saja ditutup, harus mengeluarkan bahan bakar nuklir dan menunda dimulainya operasinya. Rencana pengembangan nuklir Iran juga telah ditunda. Virus komputer tersebut kemudian dikenal sebagai Stuxnet.

Israel

Pada awal tahun 1998, Israel merekrut pemuda yang berhasil menyerbu Departemen Pertahanan AS dan mulai meningkatkan penelitian tentang perang siber. Dalam konflik Palestina-Israel dan konflik Lebanon-Israel, Israel menggunakan serangan jaringan untuk merusak halaman web dan menyerang stasiun TV guna memengaruhi arah opini publik. Militer Israel meretas komputer militer untuk mencuri rahasia guna menentukan titik fokus dan koordinat serangan yang tepat. Mereka memblokir sistem komunikasi dan komando musuh untuk mengetahui waktu pertempuran terbaik. Semua ini merupakan gambaran singkat militer Israel dalam perang siber.

Venezuela

Pada awal Maret 2019, Venezuela mengalami pemadaman listrik besar-besaran yang memengaruhi 18 dari 23 negara bagian, yang secara langsung melumpuhkan transportasi, kesehatan, komunikasi, dan infrastruktur. Presiden Venezuela Nicolas Maduro menuduh bahwa Amerika Serikat mengatur serangan jaringan ini terhadap sistem tenaga listrik Venezuela untuk menciptakan kekacauan dan memaksa pemerintah lengser melalui pemadaman listrik nasional. Beberapa analis percaya bahwa dengan tidak adanya intervensi militer langsung dan tidak langsung, meluncurkan serangan jaringan ke Venezuela mungkin merupakan pilihan terbaik bagi Amerika Serikat.

Amerika Serikat

Amerika Serikat telah mendominasi Internet selama beberapa dekade, dan kekuatan wacana jaringannya telah dipengaruhi oleh pemerintah dan kelompok dari semua negara. Amerika Serikat adalah kawasan dengan insiden kejahatan jaringan transnasional tertinggi. Negara ini juga merupakan negara yang paling populer bagi para peretas papan atas di dunia, sementara negara ini secara aktif meretas jaringan di seluruh dunia. Departemen Energi Amerika Serikat diretas sebanyak 1.131 kali antara tahun 2010 dan 2014, 159 kali berhasil. Julian Assange, pendiri WikiLeaks, pernah meretas militer AS dan memperoleh 90.000 email rahasia militer AS. Beberapa kelompok kriminal, seperti Anonymous dan New World, sering kali menantang kedaulatan jaringan Amerika Serikat. Pada bulan Oktober 2016, lembaga publik dan situs jejaring sosial di California, New York, Boston, Seattle, dan wilayah lain di Amerika Serikat diretas oleh Anonymous selama beberapa jam, yang menyebabkan hampir

separuh jaringan di Amerika Serikat lumpuh. Itu adalah salah satu serangan terbesar dalam sejarah.

2.2.2 Tata Kelola Kedaulatan Jaringan

Berdasarkan prinsip kedaulatan dunia maya, negara memegang peranan utama sebagai subjek terpenting dalam tata kelola dunia maya. Saat ini, tata kelola kedaulatan jaringan nasional utamanya dilakukan di tingkat internal dan eksternal. Secara internal, melalui perundang-undangan dan pembentukan badan pengatur khusus, dunia maya dapat secara formal berada di bawah yurisdiksi sistem hukum nasional untuk mencapai tata kelola dunia maya yang efektif dan membangun otoritas nasional di dunia maya. Secara eksternal, keamanan jaringan nasional dapat dijamin melalui langkah-langkah pertahanan keamanan jaringan, yang membangun posisi dominan negara berdaulat dalam keamanan jaringan.

1. Kebijakan Legislatif dan Regulasi Domestik

Sejak 1995, Korea Selatan telah mengubah Undang-Undang Telekomunikasi dan Perdagangan, mengesahkan Undang-Undang Dasar tentang Informatisasi Nasional dan Regulasi tentang Manajemen Keamanan Jaringan, serta undang-undang dan regulasi baru lainnya. Korea Selatan mulai menerapkan sistem nama asli Internet pada tahun 2002. Melalui serangkaian kegiatan legislatif, yurisdiksi nasional telah diperluas ke bidang Internet [5].

Sejak berdirinya Uni Eropa, serangkaian kebijakan dan regulasi yang relevan telah diperkenalkan. Selain itu, untuk melanjutkan beberapa kegiatan legislatif, banyak negara telah membentuk badan khusus untuk mengelola dunia maya. Pada awal Maret 2004, Uni Eropa membentuk Badan Keamanan Informasi dan Jaringan Eropa (ENISA). Pada Januari 2013, Uni Eropa membentuk departemen kepolisian khusus, Pusat Kejahatan Dunia Maya Eropa (EC3), untuk memerangi pornografi anak daring dan aktivitas penipuan jaringan terorganisasi.

Pemerintah Amerika Serikat telah membentuk enam badan keamanan jaringan khusus untuk memantau dunia maya. Pecahnya PRISM (program pengawasan) menunjukkan bahwa kendali pemerintah AS atas dunia maya tidak pernah terputus. Negara-negara lain, seperti Thailand dan Jepang, juga telah mendirikan lembaga untuk mengatur dunia maya. Banyak negara telah mengadopsi undang-undang dan konstruksi kelembagaan untuk mengatur perilaku di dunia maya. Kedaulatan nasional dan regulasi pemerintah tidak pernah jauh dari tata kelola dunia maya.

2. Pemerintahan Bersama Multilateral Eksternal

Internet Corporation for Assigned Names and Numbers (ICANN) adalah organisasi nirlaba yang dibentuk untuk mengelola sistem nama domain, alokasi alamat IP, konfigurasi protokol, dan sistem server induk. Organisasi ini dikelola berdasarkan kontrak oleh Internet Assigned Numbers Authority (IANA) dan entitas lain bersama dengan pemerintah AS sekarang. Untuk waktu yang lama, organisasi ini merupakan kendali sepihak oleh Amerika Serikat, yang tidak konsisten dengan harapan industri akan kebebasan Internet maupun harapan negara-negara lain akan kedaulatan jaringan. Akibatnya, seruan untuk reformasi ICANN terus berlanjut tanpa henti. Sejak tahun 2014, banyak negara, termasuk Tiongkok, Rusia, Brasil, dan India, telah mengusulkan berbagai program kerja sama multilateral mengenai tata kelola dunia maya global berdasarkan prinsip kedaulatan jaringan. Pada bulan April 2014, pada

Konferensi di Sao Paulo, Brasil dan negara-negara lain mengusulkan rencana perbaikan yang lebih moderat dalam kerangka ICANN, yang mengharuskan promosi posisi Komite Penasihat Pemerintah (GAC) ICANN, peningkatan suara negara-negara di ICANN, dan penegasan yurisdiksi independen atas sejumlah layanan terbatas di ICANN.

Institut Timur-Barat Amerika Serikat mengajukan laporan kerja pada pertemuan puncak Berlin, yang mengharuskan pemerintah negara-negara berdaulat diberi kewenangan manajemen substantif dalam sistem ICANN. Pada konferensi Pusan tahun 2014, India mengusulkan pengalihan fungsi utama tata kelola global di dunia maya dari ICANN ke International Telecommunication Union (ITU), yang secara tegas dibantah oleh Amerika Serikat, dengan menyatakan bahwa mereka tidak akan pernah mengalihkan kewenangan pengelolaan ICANN ke badan pengelola yang terdiri dari satu atau lebih negara. Skema-skema ini memperkenalkan prinsip multilateralisme, dibandingkan dengan skema Amerika Serikat. Proposal-proposal ini berupaya meningkatkan peran negara-negara berdaulat dalam tata kelola global dunia maya. Dua proposal pertama menyerukan peningkatan kewenangan regulasi bagi negara-negara berdaulat di bawah kerangka ICANN asli, sementara proposal India secara langsung menyerukan negara-negara berdaulat dan organisasi-organisasi internasional di antara mereka untuk menjadi badan utama tata kelola global di dunia maya, menggantikan fungsi dan status ICANN sebelumnya.

Oleh karena itu, dalam tata kelola ruang jaringan, berpegang teguh pada prinsip kedaulatan nasional, membangun mekanisme kerja sama multilateral internasional, dengan pemerintah di seluruh dunia saling bahu-membahu, dan melalui cara mediasi negosiasi, berpartisipasi bersama dalam tata kelola global di dunia maya, adalah cara yang paling efektif dan sah. Hanya prinsip kedaulatan negara dalam tata kelola dunia maya yang benar-benar jelas, negara dapat memastikan hak keamanan di dunia maya, dan berpartisipasi secara setara dalam tata kelola global di dunia maya. Melalui pembentukan mekanisme kerja sama multilateral, konflik internasional tentang masalah dunia maya dapat dihindari secara efektif dan semua negara berdaulat di dunia dapat hidup berdampingan secara damai dan mencapai kerja sama yang saling menguntungkan di dunia maya.

2.2.3 Tata Letak Strategis Beberapa Negara

1. Jerman

Jerman telah membentuk pasukan peretas sejak tahun 2006, dan hal ini digambarkan sebagai upaya untuk menutup kesenjangan dengan negara-negara lain. Dalam dokumen tahun 2012 yang diserahkan ke Bundestag, militer Jerman mengatakan bahwa mereka memiliki kemampuan awal untuk menyerang jaringan musuh. Pada tanggal 1 April 2017, Angkatan Bersenjata Jerman secara resmi membentuk Komando Siber dan Informasi. Komando tersebut, bersama dengan angkatan darat, angkatan laut, angkatan udara, dan layanan medis, membentuk sistem Bundeswehr, yang akan memainkan peran utama dalam aliansi NATO.

Pada tahun 2019, untuk memastikan kedaulatan digital pengguna layanan cloud di Eropa, Kementerian Federal Jerman untuk Urusan Ekonomi dan Energi meluncurkan proyek GAIA-X, yang bertujuan untuk mengembangkan infrastruktur data yang efisien dan kompetitif,

aman, dan tepercaya untuk Eropa, serta mengurangi ketergantungan pada layanan cloud dari Amazon, Microsoft, Google, dan perusahaan Amerika lainnya (Gambar 2.2). Proyek ini didukung oleh perwakilan bisnis, sains, dan administrasi dari Jerman dan Prancis, bersama dengan mitra Eropa lainnya. Anggota pendiri di pihak Jerman termasuk Beckhoff Automation, BMW, Bosch, DE-CIX, Deutsche Telekom, German Edge Cloud, PlusServer, SAP, dan Siemens. Tujuan proyek ini adalah menggabungkan infrastruktur pusat dan desentralisasi yang ada untuk membentuk sistem, yang dapat menawarkan ruang data dan layanan yang seragam. Bundesverband Information swirtschaft, Telekommunikation und neue Medien (BITKOM), menyatakan bahwa proyek GAIA-X akan memberikan kontribusi penting untuk memperkuat kedaulatan digital dan data di Eropa. “Tahap selanjutnya adalah Jerman mengundang negara-negara anggota UE lainnya untuk bergabung dengan proyek ini”, kata Menteri Ekonomi Jerman Tomas Altmaier.

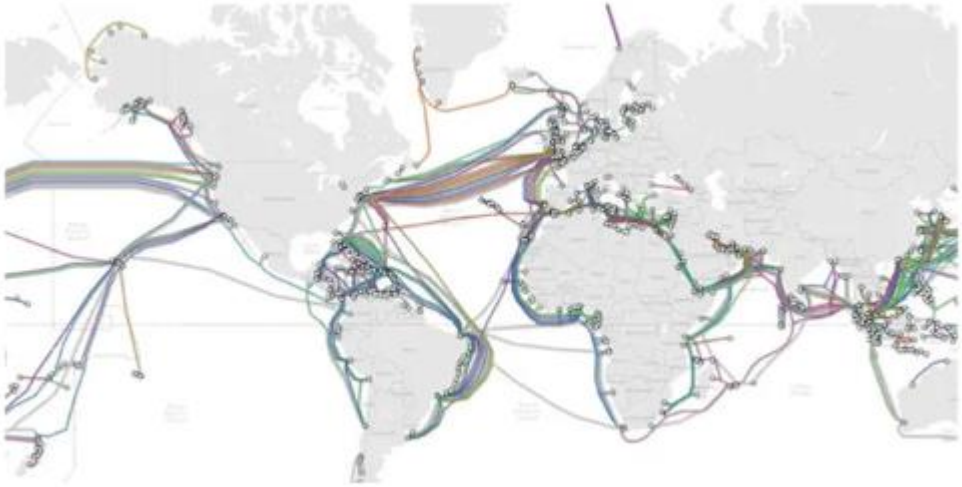
Gambar 2.2 proyek GAIA-X

2. Rusia

Rusia merupakan salah satu negara yang aktif mempersiapkan jaringan kedaulatan. Negara ini telah menguji coba internet tanpa kabel dan memperkuat pengawasan informasi jaringan melalui undang-undang nasional dan berbagai cara lainnya. Pemerintah Rusia memiliki sejarah panjang dalam hal pengawasan ketat terhadap lingkungan jaringan. Sejak tahun 2006, pemerintah telah membatasi penggunaan situs web dan aplikasi seperti jejaring sosial profesional LinkedIn, aplikasi obrolan Zello, alat pengiriman pesan instan Telegram, dan mewajibkan perusahaan asing untuk memberikan hak akses sistem kepada pemerintah guna memantau data pengguna. Pemerintah Rusia mewajibkan semua fasilitas Internet melewati pusat kendali resmi, dan mengizinkan dirinya untuk memutus koneksi eksternal kapan saja, menutup situs web yang tidak disetujui, dan memantau semua lalu lintas Internet. Pemerintah Rusia juga tengah mempersiapkan diri untuk mengadopsi serangkaian langkah teknis dan merumuskan lebih banyak kebijakan terkait di masa mendatang.

Pada bulan November 2019, Rusia secara resmi mengumumkan dan menerapkan Undang-Undang Internet Berdaulat, yang menyatakan bahwa perlu adanya persiapan untuk

menggunakan jaringan kedaulatan Rusia RuNet guna menjaga keamanan jaringan nasional jika terjadi serangan jaringan eksternal. Berdasarkan RUU tersebut, lembaga pemerintah dan lembaga keamanan, serta semua operator komunikasi, penyedia layanan pesan, dan email, harus ikut serta dalam pengujian tersebut, tetapi pengujian tersebut tidak akan memengaruhi pengguna Internet biasa. Undang-undang tersebut menetapkan bahwa infrastruktur Internet Rusia harus secara bertahap terbebas dari ketergantungan pada node asing, terutama dalam kasus serangan eksternal, Rusia dapat memutus koneksi dengan dunia luar dan mengoperasikan Internet regional secara mandiri. Rusia saat ini sedang membangun sistem nama domain (DNS), yang diharapkan akan selesai pada tahun 2021 (Gambar. 2.3).



Gambar 2.3 Peta yang menunjukkan kabel internet bawah laut di seluruh dunia

Pada tanggal 24 Desember 2019, Rusia berhasil menguji internet tanpa kabel. Hasilnya menunjukkan bahwa layanan Internet di Rusia masih dapat berfungsi saat terisolasi dari Internet lainnya. Pengujian ini memakan waktu beberapa hari dan dilakukan pada jaringan yang ditunjuk secara khusus. Ini adalah pertama kalinya bagi Rusia untuk melakukan pengujian jaringan terhadap risiko terputus dari Internet. Pengujian tersebut juga menguji stabilitas komunikasi, keamanan komunikasi seluler, termasuk masalah perlindungan data pribadi, pencegahan pembajakan panggilan dan SMS, penyadapan lalu lintas, dan keamanan penggunaan Internet of Things. Sementara itu, Rusia tengah menyiapkan versi Wikipedia buatan dalam negeri dan mewajibkan semua telepon pintar dilengkapi dengan perangkat lunak buatan Rusia yang telah terinstal sebelumnya.

3. Amerika Serikat

Sejak akhir tahun 1990-an, pemerintah AS mulai memperhatikan tantangan yang ditimbulkan oleh perkembangan Internet, dengan menekankan pentingnya membangun mekanisme keamanan informasi di dunia maya, mendirikan sejumlah lembaga keamanan jaringan, dan menerbitkan sejumlah undang-undang dan peraturan, yang berupaya menjaga keamanan informasi di dunia maya.

Pada bulan November 2008, Presiden Obama mengumumkan pembentukan panel tinjauan Kebijakan dunia maya untuk meninjau status keamanan jaringan AS. Pada bulan Desember 2009, Kantor Keamanan Siber Gedung Putih didirikan. Pada bulan Mei 2010, militer AS mendirikan Komando Siber untuk mengoordinasikan dan menjaga operasi di dunia maya. Pada bulan Mei 2011, pemerintah AS menerbitkan Strategi Internasional untuk Dunia Maya, yang menggabungkan kebijakan Internet dengan tujuan kebijakan Internasional untuk pertama kalinya. Pada bulan Juli 2011, Departemen Pertahanan AS mengeluarkan Strategi untuk Beroperasi di Dunia Maya, yang memberikan pedoman operasional khusus untuk penyebaran dan implementasi operasi jaringan militer AS. Pada tahun 2013, Presiden Obama mengeluarkan Perintah Eksekutif 13.636, yang secara eksplisit mengusulkan mekanisme untuk berbagi informasi keamanan di dunia maya.

Kemudian, *Institut Nasional Standar dan Teknologi* (NIST) memimpin kemitraan dengan sektor swasta untuk mengembangkan Kerangka Kerja untuk Meningkatkan Keamanan Siber Infrastruktur Kritis (FCIC), dan pemerintah AS memiliki perjanjian dengan sektor swasta tentang masalah keamanan siber. Pada bulan Februari 2016, pemerintah AS mengeluarkan Rencana Aksi Nasional Keamanan Siber (CNAP) dan membentuk Komisi untuk Meningkatkan Keamanan Siber Nasional untuk memastikan kemampuan keamanan informasi yang lebih besar bagi Amerika Serikat di era digital. Pada tanggal 23 Maret 2018, Presiden Trump secara resmi menandatangani Undang-Undang Clarify Lawful Overseas Use of Data (CLOUD Act), yang memberikan dasar hukum bagi AS untuk mendapatkan data asing dan pemerintah asing yang memenuhi syarat untuk mendapatkan data di AS.

Pemerintah AS sangat mementingkan kedaulatan jaringan dengan menjaga keamanan jaringan dan sistem informasi melalui penyebaran kebijakan, pembentukan lembaga, penegakan hukum, dan cara lainnya.

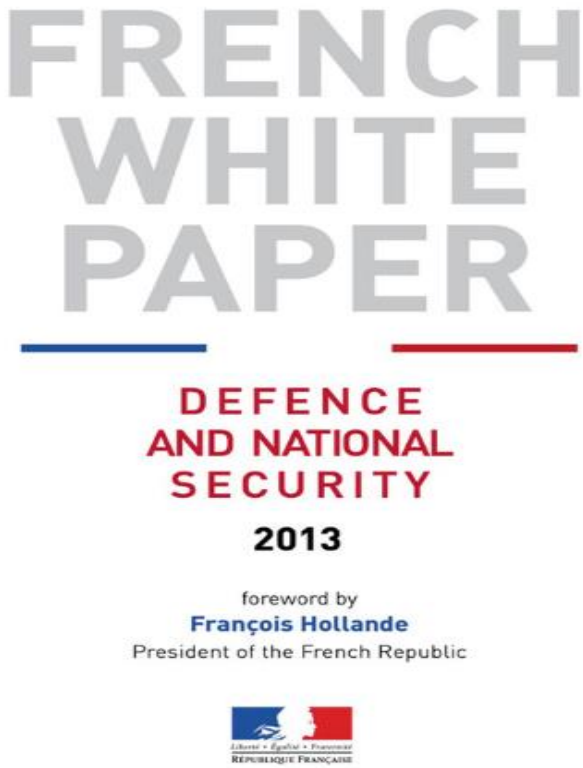
4. Prancis

Pada tahun 2013, dalam Buku Putih tentang Pertahanan dan Keamanan Nasional, Prancis mengidentifikasi serangan jaringan sebagai salah satu ancaman eksternal paling serius terhadap kedaulatan nasional dan menyerukan pembentukan pasukan pertahanan jaringan. Prancis berencana untuk mendirikan serangkaian operasi pertahanan jaringan dan menginvestasikan 1 miliar euro pada tahun 2019 untuk penelitian pertahanan dan keamanan jaringan. Pada saat yang sama, Prancis berencana untuk menyediakan pasukan pertahanan dan keamanan jaringan sipil, melatih para ahli pertahanan jaringan sipil untuk melayani pemerintah dan militer bila diperlukan (Gambar 2.4).

5. Inggris Raya

Inggris Raya telah mendirikan Kantor Keamanan Siber Inggris, yang bertanggung jawab langsung kepada Perdana Menteri, untuk menyusun rencana pengembangan pasukan perang siber dan platform aksi untuk keamanan siber di tingkat strategis. Pusat Operasi Keamanan Siber (CSOC) Inggris berafiliasi dengan Markas Besar Komunikasi Pemerintah (GCHQ) dan bertanggung jawab untuk memberikan dukungan intelijen untuk operasi perang siber militer. Pasukan Siber Nasional Inggris berafiliasi dengan Kementerian Pertahanan Nasional, dan bertanggung jawab atas pelatihan dan perencanaan operasi yang terkait dengan perang siber

militer, serta mengoordinasikan para ahli teknis militer untuk melaksanakan perlindungan keamanan bagi target jaringan militer.



Gambar 2.4 Buku putih Prancis tahun 2013 tentang pertahanan dan keamanan nasional

2.3 MENJAGA KEDAULATAN JARINGAN

Kedaulatan jaringan merupakan bagian penting dari kedaulatan nasional sekaligus perluasan kedaulatan nasional di dunia maya. Sebagaimana prinsip kedaulatan nasional menjadi dasar tatanan internasional modern, prinsip kedaulatan jaringan juga merupakan landasan tatanan internasional di dunia maya. Dalam gelombang globalisasi, teknologi berubah dengan cepat, dan Internet merupakan salah satu yang terbaik. Jika suatu negara dapat memimpin dalam masalah dunia maya, maka negara tersebut dapat memimpin dalam membangun ketertiban dan permainan aturan di dunia maya. Oleh karena itu, kita harus menanggapi tuntutan sebagian besar negara akan kedaulatan jaringan dan menjaga kedaulatan jaringan dengan tegas.

2.3.1 Memperkuat Kesadaran tentang Kedaulatan Jaringan Nasional

Dunia maya merupakan batas kelima, selain empat batas daratan, laut, langit, dan angkasa, dan penelitian tentang dunia maya masih dalam tahap awal. Negara-negara memiliki pemahaman yang berbeda tentang cara menerapkan aturan kedaulatan di dunia maya, tetapi semakin banyak pihak yang menyerukan perhatian yang lebih besar terhadap kedaulatan jaringan (Gambar. 2.5).

Gambar 2.5 Dunia Maya

Uni Eropa menganjurkan yurisdiksi atas keamanan data warga negara. Kanselir Jerman, Angela Merkel, telah lama, dan akhir-akhir ini lebih terbuka, membela perlunya Eropa untuk melindungi kedaulatan digitalnya. Inggris telah meluncurkan Program Keamanan Siber Nasional (NCSP) untuk melindungi Inggris dari serangan jaringan dan mengembangkan kedaulatan di dunia maya. Rusia telah memperkenalkan Undang-Undang Internet Berdaulat, yang menetapkan kedaulatan jaringan Rusia yang otonom dan terkendali dari lima aspek, termasuk otonomi nama domain, latihan rutin, kontrol platform, dan pemutusan sambungan Internet secara aktif.

Tiongkok adalah pencetus dan pendukung kedaulatan nasional di dunia maya. Pada bulan Juni 2010, Tiongkok menerbitkan buku putih, yang diberi nama “Keadaan Internet di Tiongkok”, yang dengan jelas menyatakan bahwa Internet di Tiongkok berada di bawah yurisdiksi kedaulatan Tiongkok, dan kedaulatan Internet Tiongkok harus dihormati dan ditegakkan. Pada tanggal 1 Juli 2015, Undang-Undang Keamanan Nasional Republik Rakyat Tiongkok mulai berlaku, dan Tiongkok mendefinisikan kedaulatan dunia maya dalam bentuk hukum untuk pertama kalinya.

Pada tanggal 16 Desember 2015, pada Konferensi Internet Dunia Kedua, Xi Jinping, Presiden Tiongkok, menghadiri upacara pembukaan dan menyampaikan pidato, serta menguraikan empat prinsip dan membuat proposal lima poin mengenai pengembangan dan tata kelola Internet. Keempat prinsip tersebut meliputi menghormati kedaulatan di dunia maya, menegakkan perdamaian dan keamanan, mempromosikan keterbukaan dan kerja sama, serta membangun tatanan yang baik. Usulan lima poin tersebut meliputi percepatan pembangunan infrastruktur internet global untuk konektivitas yang lebih besar,

pembangunan platform daring untuk pertukaran budaya dan pembelajaran bersama, promosi pengembangan inovatif ekonomi digital untuk kesejahteraan bersama, pemeliharaan keamanan siber untuk mendorong pembangunan yang tertib, pembangunan sistem tata kelola global di dunia maya untuk mendorong kesetaraan dan keadilan (Gambar 2.6).

Pada tanggal 27 Desember 2016, kantor informasi jaringan nasional Tiongkok mengeluarkan Strategi Keamanan Jaringan Nasional, yang menyerukan strategi keamanan jaringan sebagai strategi nasional, menetapkan bahwa kedaulatan jaringan adalah batas baru kedaulatan nasional. “Internet adalah bidang baru aktivitas manusia yang sama pentingnya dengan daratan, laut, langit, dan luar angkasa, dan kedaulatan nasional telah diperluas ke dunia maya, dan kedaulatan dunia maya telah menjadi bagian penting dari kedaulatan nasional. Telah menjadi konsensus komunitas internasional untuk menghormati kedaulatan dunia maya, menjaga keamanan jaringan, mencari tata kelola bersama, dan mencapai hasil yang saling menguntungkan”. Seperti kedaulatan nasional, kedaulatan jaringan tidak dapat diganggu gugat. Oleh karena itu, strategi tersebut juga mensyaratkan bahwa, “Warga negara Tiongkok harus dengan tegas menjaga kedaulatan dunia maya.

Semua aktivitas jaringan dalam lingkup kedaulatan Tiongkok tunduk pada konstitusi, hukum, dan peraturan. Kita harus mengambil semua langkah, termasuk langkah-langkah ekonomi, administratif, ilmiah, teknologi, hukum, diplomatik, dan militer, untuk melindungi keamanan fasilitas dan sumber informasi Tiongkok, dan dengan teguh menjaga kedaulatan dunia maya Tiongkok. Kami dengan tegas menentang tindakan apa pun yang menumbangkan kekuasaan negara Tiongkok atau merusak kedaulatan nasional Tiongkok melalui Internet” dan “kita harus menghormati hak semua negara untuk memilih jalur pembangunan, model pengelolaan dunia maya, dan kebijakan publik dunia maya, serta untuk berpartisipasi secara damai dalam tata kelola dunia maya internasional. Urusan dunia maya setiap negara bergantung pada rakyatnya. Negara memiliki hak, mengingat kondisi nasional mereka dan memanfaatkan pengalaman internasional, untuk memberlakukan undang-undang dan peraturan tentang dunia maya dan mengambil langkah-langkah yang diperlukan berdasarkan hukum untuk mengelola sistem informasi dan aktivitas jaringan mereka di wilayah mereka”. Pada tanggal 1 Maret 2017, Tiongkok meluncurkan Strategi Kerjasama Internasional mengenai Dunia Maya, yang membahas posisi Tiongkok mengenai isu-isu yang berkaitan dengan tata kelola dunia maya internasional, dan mengklaim bahwa, “definisi yang jelas mengenai kedaulatan dunia maya tidak hanya mencerminkan tanggung jawab dan hak pemerintah untuk mengatur dunia maya berdasarkan hukum, tetapi juga membantu mendorong pembangunan platform untuk interaksi yang baik antara pemerintah, perusahaan, dan masyarakat, dan menciptakan lingkungan ekologi yang sehat untuk pengembangan teknologi informasi dan pertukaran serta kerjasama internasional”.

Gambar 2.6 Lokasi konferensi internet dunia di Wuzhen, Cina

2.3.2 Menentang Teori Penolakan Kedaulatan di Dunia Maya

Berbagai negara memiliki sikap yang berbeda terhadap kedaulatan jaringan, berdasarkan tingkat perkembangan teknologi jaringan dan status mereka di komunitas internasional. Negara-negara maju, misalnya AS, percaya bahwa dunia maya, luar angkasa, perairan internasional, dan antariksa, merupakan infrastruktur sistem global dan termasuk dalam milik bersama global, sehingga negara-negara tidak boleh menjalankan kedaulatan nasional di sana.

Pandangan tentang penolakan Amerika Serikat terhadap kedaulatan jaringan tidak dapat dipisahkan dari strategi dunia maya globalnya, yang bertujuan untuk membangun hegemoni di dunia maya global dan memperjuangkan kepentingan nasional semaksimal mungkin. Namun pada saat yang sama, Amerika Serikat telah memberlakukan beberapa strategi dan undang-undang tentang dunia maya. Singkatnya, negara-negara maju jaringan, yang diwakili oleh Amerika Serikat, mengadopsi standar ganda dalam masalah kedaulatan jaringan. Di ruang jaringan internasional, jaringan dianggap sebagai milik bersama global, ketika mereka perlu mengumpulkan informasi lain untuk kepentingan nasional mereka. Saat ini, mereka mengklaim bahwa Perserikatan Bangsa-Bangsa tidak kompeten untuk tugas tata kelola dunia maya, dan mekanisme internasional baru untuk menjalankan tata kelola dunia maya global harus dibentuk, yang tujuannya adalah untuk memperkenalkan strategi global Amerika melalui jaringan. Namun, ketika perlu untuk memperkuat pengawasan jaringan domestik, mereka mengklaim bahwa dunia maya adalah domain kedaulatan, dan negara mereka memiliki yurisdiksi kedaulatan absolut dan eksklusif atas dunia maya.

Di komunitas internasional, negara-negara jaringan yang sedang berkembang, seperti Rusia, memiliki kekuatan tertentu dalam beberapa teknologi dan infrastruktur jaringan dan telah menjadi negara maju dalam ilmu pengetahuan dan teknologi jaringan dengan mengembangkan bisnis jaringan secara giat. Negara-negara jaringan yang sedang berkembang ini percaya bahwa jaringan harus memiliki atribut kedaulatan yang eksplisit.

Selain itu, ada beberapa negara berkembang jaringan dengan perkembangan teknologi jaringan yang relatif terbelakang. Negara-negara ini lebih mementingkan peran kedaulatan jaringan sehingga mereka dapat melindungi kepentingan yang relevan sejauh mungkin di area yang relatif terbelakang. Negara-negara berkembang jaringan telah mengambil bagian aktif dalam tata kelola masalah dunia maya dan menutupi kekurangan mereka dalam teknologi jaringan melalui undang-undang. Sementara itu, mereka telah secara aktif melakukan kerja sama dengan kekuatan jaringan yang baru muncul untuk bersama-sama menjaga kedaulatan nasional di dunia maya.

Pertentangan antara gagasan-gagasan jaringan ini biasanya tercermin dalam perebutan kendali atas sistem nama domain. Cheng Weidong, seorang sarjana Tiongkok, mengatakan bahwa teori penolakan kedaulatan di dunia maya, yang ditegaskan oleh beberapa negara maju, mengabaikan karakteristik penting jaringan, dan mengabaikan kontradiksi utama dan aspek-aspek utama kontradiksi, telah melanggar dialektika materialis Marxis dasar, juga tidak memiliki dasar praktis bidang jaringan, dan tidak dapat bertahan dalam ujian praktik.

Intinya, teori penolakan kedaulatan di dunia maya mencerminkan kepentingan khusus beberapa negara dan berupaya menggunakan penegasan kebebasan jaringan untuk menyebarkan nilai-nilai barat. Seperti yang telah ditunjukkan oleh Profesor Goldsmith dan Wu Xiuming dari Sekolah Hukum Harvard, beberapa pihak yang menentang kedaulatan, meskipun berbicara tentang tata kelola dari atas ke bawah, komunitas Internet, dan hal-hal lainnya, tidak pernah benar-benar menyerahkan kendali atas nama domain akar, dan nama domain akar masih berada di bawah kendali dan kepemilikan mereka. Betapapun kuatnya suatu negara, ia tidak memiliki hak untuk mengendalikan nama domain root. Oleh karena itu, berbicara tentang privatisasi atau internasionalisasi dapat mengalihkan perhatian para kritikus. Namun Amerika Serikat tidak pernah bermaksud untuk menyerahkan kekuasaannya atas sumber daya yang begitu penting.

Cendekiawan lain percaya bahwa teknologi leapfrog tidak dapat menjadi alasan alami untuk dunia maya yang tanpa batas dan super-teritorial, dan teori global commons dunia maya merusak dasar kerja sama internasional tentang tata kelola dunia maya. Prinsip kedaulatan merupakan prinsip dasar yang harus dijunjung tinggi dalam tata kelola dunia maya internasional. Dunia maya dalam wilayah suatu negara diatur oleh negara itu sendiri dan tidak tunduk pada faktor-faktor lain. Kalangan akademisi mengkritik teori negasi kedaulatan dalam dunia maya, yang menggambarkan dasar kedaulatan jaringan dari perspektif teori dan yurisprudensi.

2.3.3 Perdamaian dan Stabilitas di Dunia Maya

Menjaga kedaulatan dunia maya di era globalisasi membutuhkan kerja sama internasional yang lebih komprehensif. Dalam pertukaran internasional di bidang dunia maya, penggunaan dan pengembangan dunia maya harus dilakukan secara damai. Hal ini mendukung pengembangan lingkungan jaringan internasional secara keseluruhan dan merupakan perwujudan dari pengembangan damai Piagam Perserikatan Bangsa-Bangsa dan prinsip larangan penggunaan kekerasan. Saat ini, ada serangan jaringan yang tak ada habisnya di dunia maya internasional, meskipun Manual Tallinn 2.0 telah memberikan analisis terperinci tentang hak membela diri terhadap serangan jaringan, lebih penting untuk mengadvokasi penggunaan dunia maya secara damai. Kita harus menentang semua bentuk perang dunia maya dan kegiatan yang tidak damai dengan memanfaatkan teknologi informasi.

Kami akan terus mengadvokasi pentingnya kedaulatan di dunia maya, menegakkan prinsip bahwa kedaulatan jaringan tidak menoleransi campur tangan asing, dan dengan tegas menentang niat beberapa negara untuk mencampuri urusan dalam negeri negara lain dengan memanfaatkan sifat internasional Internet. Kami menganjurkan agar semua negara meninggalkan mentalitas Perang Dingin dalam tata kelola dunia maya dan standar ganda milik bersama dan kedaulatan dunia maya, mencari perdamaian melalui konsultasi dan kerja sama berdasarkan rasa hormat penuh terhadap kedaulatan jaringan negara lain, dan lebih jauh meningkatkan keamanan mereka melalui penggunaan dunia maya secara damai.

Di sisi lain, inovasi teknologi inti adalah yang paling penting untuk menentukan apakah suatu negara dapat menjadi negara yang kuat dalam jaringan, menjalankan kekuatan pertahanan di dunia maya, dan menjaga hak dan yurisdiksi independen di dunia maya. Internet adalah industri yang sedang berkembang untuk mendorong pembangunan ekonomi, serta bidang penting untuk menjaga kepentingan nasional. Hanya ketika suatu negara memiliki keunggulan teknologi di bidang dunia maya internasional, suaranya dapat ditingkatkan. Oleh karena itu, hanya dengan mengusulkan arsitektur jaringan baru dari tingkat teknis, sistem nama domain saat ini dapat benar-benar melepaskan kendalinya atas jaringan, mewujudkan tata kelola kerja sama yang setara dan multilateral di antara negara-negara, dan mewujudkan otonomi kedaulatan di bidang Internet.

2.3.4 Memperluas Konsep Kedaulatan Jaringan

Hanya dengan menghormati kedaulatan jaringan, negara-negara, terlepas dari ukuran atau kekuatannya, dapat melakukan dialog dan pertukaran dengan kedudukan yang setara, sepenuhnya melindungi kepentingan mereka di dunia maya, dan secara efektif mempromosikan solusi berbagai masalah jaringan. Sistem tata kelola Internet global saat ini belum ditingkatkan. Tiongkok mengajukan klaim kedaulatan jaringan, yang telah dipuji secara luas oleh masyarakat internasional.

Menjaga kesetaraan kedaulatan di dunia maya dapat mengakomodasi berbagai kepentingan negara yang berbeda, menghilangkan potensi konflik antarnegara, dan menciptakan peluang untuk saling menguntungkan dan hasil yang saling menguntungkan di antara negara-negara. Sementara Internet telah mengintegrasikan dunia ke dalam sebuah desa global, ia juga telah menciptakan pola kepentingan yang saling bergantung di antara

negara-negara di dunia. Hak dan kepentingan kedaulatan setiap negara di bidang informasi tidak boleh dilanggar oleh negara lain, dan setiap negara memiliki hak untuk menjaga keamanan informasinya. Kita harus menumbuhkan rasa membangun komunitas dengan masa depan bersama di dunia maya dan meninggalkan konsep lama permainan zero-sum dan pemenang mengambil semuanya di dunia maya. Setiap negara tidak dapat mencari keamanan absolutnya dengan mengorbankan keamanan negara lain. Semua negara harus mengikuti prinsip kesetaraan dalam kedaulatan jaringan, menghormati kepentingan utama negara lain, dan berpegang teguh pada prinsip bekerja sama, saling percaya, dan saling menguntungkan.

Dengan demikian, dasar yang realistis untuk kerja sama internasional akan terbentuk, dan lebih banyak negara dan masyarakat dapat menaiki kereta ekspres era informasi dan berbagi hasil dari pengembangan Internet. Negara-negara perlu mendorong konsensus di dunia maya, memperluas kepentingan kerja sama di dunia maya, memperkuat pertukaran di antara komunitas internasional mengenai teknologi keamanan jaringan, pembangunan kelembagaan, dan pengalaman manajemen. Kita harus bekerja sama untuk membangun sistem tata kelola Internet global yang multilateral, demokratis, dan transparan.

Pada tanggal 3 Desember 2017, di konferensi Internet dunia keempat, perwakilan dari Tiongkok, Mesir, Laos, Arab Saudi, Serbia, Thailand, Turki, dan Uni Emirat Arab bersama-sama meluncurkan Prakarsa Kerja Sama Internasional Ekonomi Digital “Belt and Road”. Dengan bantuan prakarsa “Belt and Road”, Tiongkok dapat menggabungkan keunggulan geografis dengan teknologi jaringan, mempromosikan konsep kedaulatan jaringan, dan mempromosikan pembangunan komunitas dengan masa depan bersama di dunia maya (Gambar. 2.7).

Gambar 2.7 Upacara peluncuran inisiatif kerja sama internasional ekonomi digital “Sabuk dan Jalan” (2017), oleh Shuqiong Pan

Gambar 2.8 Inisiatif Sabuk dan Jalan

Banyak negara di sepanjang rute "Belt and Road" telah menjaga hubungan bilateral yang baik dengan Tiongkok untuk waktu yang lama, dan mereka juga menghadapi beberapa ancaman dalam hal pembangunan ekonomi dan sosial serta keamanan nasional. Misalnya, beberapa negara memiliki tingkat pembangunan infrastruktur jaringan yang rendah, yang perlu segera ditingkatkan. Tiongkok memiliki keunggulan teknologi yang komparatif dan dapat melakukan kerja sama yang mendalam di bidang-bidang seperti pembangunan infrastruktur jaringan, untuk memperkuat dukungan dan bantuan bagi pemasyarakatan teknologi internet dan pembangunan infrastruktur di daerah-daerah terbelakang. Atas dasar saling menghormati kedaulatan jaringan masing-masing, kita harus secara giat mengembangkan dan membangun ruang siber kita, mempersempit kesenjangan digital, dan kemudian membangun "Jalur Sutra Informasi" dengan negara-negara berkembang yang luas dan beberapa negara maju di sepanjang "Sabuk dan Jalan" (Gambar 2.8).

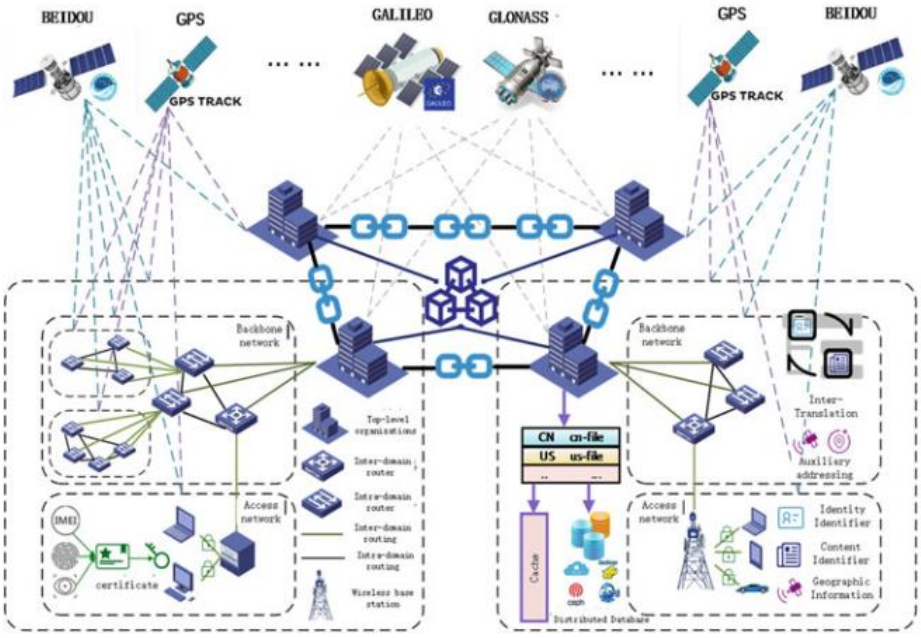
2.4 SITUASI TERKINI KEDAULATAN JARINGAN TV PENYIARAN

Jaringan TV siaran merupakan mata rantai utama dari konvergensi tiga jaringan, yaitu jaringan televisi kabel, jaringan telekomunikasi, dan jaringan komputer. Selain itu, jaringan ini merupakan representasi dari jaringan komprehensif yang efisien dan murah. Jaringan siaran memiliki keunggulan pita frekuensi yang lebar, kapasitas besar, banyak fungsi, biaya rendah, kemampuan anti-interferensi yang kuat, dan mendukung berbagai layanan untuk menghubungkan ribuan keluarga. Perkembangannya telah meletakkan dasar bagi pengembangan jalan raya informasi.

Jaringan TV siaran telah mencakup wilayah yang sangat luas. Pada tahun 2003, jumlah pelanggan Chinese Community Antenna Television (CATV) melampaui 100 juta. Setelah delapan tahun berkembang pesat, jumlahnya melampaui 200 juta pada tahun 2011. Pada

akhir tahun 2016, jumlah pengguna CATV sebenarnya adalah 252 juta, di antaranya jumlah pengguna TV digital juga mencapai 210 juta, dengan tingkat digitalisasi sebesar 83,3%. Televisi telah menjadi salah satu perangkat informasi dengan tingkat hunian rumah tangga tertinggi, dan jaringan CATV telah menjadi multimedia paling populer di rumah. Namun, jaringan CATV masih menggunakan kabel koaksial untuk mengirimkan program TV kepada pengguna pada tingkat analog. Arah pengembangan jaringan CATV mencakup TV pita lebar dua arah sesuai permintaan (VOD), akses ke Internet melalui jaringan CATV untuk TV sesuai permintaan, panggilan CATV, dll. Target pengembangan utamanya adalah menjadikan jaringan CATV menjadi jaringan komunikasi multimedia dua arah pita lebar.

Dengan pesatnya perkembangan format media baru seperti IPTV, TV Internet, dan TV seluler, jaringan TV siaran menghadapi tantangan yang belum pernah terjadi sebelumnya. Misalnya, dalam hal arsitektur bisnis video, layanan video Internet yang fleksibel dan nyaman dapat memenuhi perubahan cepat kebutuhan pengguna dan psikologi konsumen di bawah perkembangan informasi, yang membuat kubu TV tradisional terpecah. Sebagai promotor utama reformasi TV digital dalam industri radio dan televisi, jaringan kabel berada dalam situasi segmentasi dan desentralisasi jaringan, dan subjek operasi nasional masih belum terbentuk. Padahal, jaringan penyiaran memiliki beberapa keunggulan yang melekat, seperti transmisi jaringan yang aman dan andal, kualitas transmisi yang stabil dan jernih, hak cipta eksklusif atas beberapa program, dan kredibilitas yang kuat. Akan tetapi, karena kurangnya pengawasan terhadap konten, keterbukaan jaringan telekomunikasi dan internet menjadi terlalu kasual.



Gambar 2.9 Arsitektur jaringan kedaulatan

Singkat kata, transmisi sinyal saluran radio dan televisi publik merupakan salah satu layanan dasar jaringan TV penyiaran. Sebagai infrastruktur informasi nasional yang penting,

jaringan TV penyiaran merupakan sumber daya strategis nasional yang penting dan penghalang penting terhadap risiko jaringan. Oleh karena itu, jaringan TV penyiaran harus menyediakan sarana teknis untuk arahan nasional opini publik di dunia maya, dan menstabilkan kesetaraan kedaulatan di dunia maya. Kita harus membangun, memperkuat, dan meningkatkan perannya dalam sistem keamanan jaringan nasional, memperkuat jaringan TV penyiaran berdasarkan penelitian dan konstruksi jaringan kedaulatan.

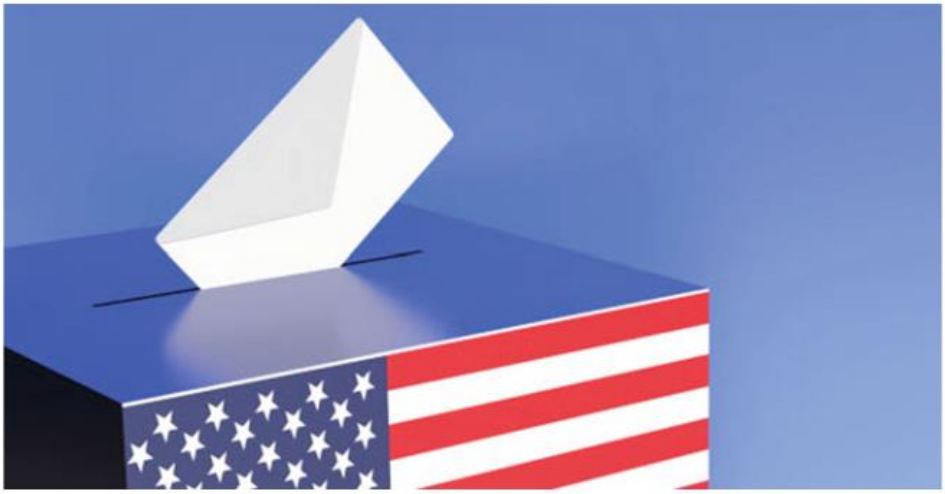
Buku ini mengusulkan dan menyiapkan jaringan kedaulatan, arsitektur jaringan masa depan yang baru, dari tingkat teknis. Hal ini membuat dunia maya menjadi dinamis, damai, tata kelola bersama multilateral, dan mencapai keseimbangan antara kebebasan dan ketertiban. Jaringan kedaulatan berdasarkan MIN adalah arsitektur Internet kedaulatan pertama yang secara teknis layak di dunia. Arsitektur jaringan kedaulatan ditunjukkan pada Gambar 2.9. Kami menggambarkan arsitekturnya, teknologi inti, aplikasi dan penyebarannya, dan memilih jaringan TV siaran sebagai skenario aplikasi yang umum untuk diperkenalkan.

2.5 KEKUATAN KEEMPAT

Pemilihan Presiden Amerika Serikat Tahun 2020 dan Kedaulatan Jaringan

2.5.1 Pemilihan Presiden Amerika Serikat

Pemilihan presiden Amerika Serikat tahun 2020 adalah pemilihan presiden empat tahunan ke-59, yang diadakan pada tanggal 3 November 2020. Seluruh 435 kursi di DPR dan 33 kursi di Senat juga dipilih untuk membentuk Kongres Amerika Serikat ke-117. Pemilihan umum pada bulan November juga merupakan pemilihan tidak langsung, di mana para pemilih memberikan suara untuk daftar anggota Electoral College, para elektor ini kemudian secara langsung memilih presiden dan wakil presiden. Pada tanggal 14 Desember 2020, para elektor memberikan suara untuk mengukuhkan Joe Biden sebagai presiden Amerika Serikat ke-46 dan Kamala Harris sebagai wakil presiden (Gambar. 2.10).



Gambar 2.10 Pemilu AS 2020

Trump mengamankan nominasi Partai Republik tanpa perlawanan serius, sementara Biden mengamankan nominasi Partai Demokrat atas pesaing terdekatnya, Senator Bernie

Sanders, dalam pemilihan pendahuluan yang kompetitif yang menampilkan kandidat terbanyak untuk partai politik mana pun di era politik Amerika modern. Calon wakil presiden Biden, Senator Harris dari California, adalah orang Afrika-Amerika pertama, orang Asia-Amerika pertama, dan calon wakil presiden perempuan ketiga yang memiliki tiket partai besar. Selain itu, ada beberapa calon yang mewakili partai politik lain dan calon independen. Isu-isu utama pemilihan tersebut meliputi dampak kesehatan masyarakat dan ekonomi dari pandemi COVID-19 yang sedang berlangsung; kerusuhan sipil sebagai reaksi atas pembunuhan George Floyd dan lainnya; Mahkamah Agung AS setelah kematian Ruth Bader Ginsburg dan konfirmasi Amy Coney Barrett; dan masa depan Undang-Undang Perawatan Terjangkau.

Gambar 2.11 Penyerbuan Gedung Capitol Amerika Serikat

Pemilihan tersebut mencatat rekor jumlah surat suara yang diberikan lebih awal dan melalui pos karena pandemi yang sedang berlangsung. Akibat banyaknya surat suara yang dikirim melalui pos, beberapa negara bagian yang masih belum jelas pemenangnya mengalami penundaan dalam penghitungan dan pelaporan suara; hal ini menyebabkan sejumlah media berita utama menunda proyeksi mereka. Setelah Hari Pemilihan, Trump dan sejumlah Republikan berusaha untuk menumbangkan pemilihan dan membatalkan hasilnya, dengan menuduh adanya kecurangan pemilih yang meluas. Pada tanggal 7 November 2020, semua media berita utama AS mengumumkan bahwa Biden dan Kamala Harris telah memenangkan pemilihan, menerima minimal 270 suara elektoral yang dibutuhkan setelah memenangkan 20 suara Electoral College Pennsylvania.

Pada tanggal 9 November 2020, bahkan setelah sejumlah media berita utama AS telah menyatakan bahwa Biden telah memenangkan pemilihan, Administrasi Layanan Umum belum mengesahkan pemenang dan menolak untuk menyetujui dokumen untuk memulai proses

transisi. Pada tanggal 23 November 2020, Administrasi Layanan Umum secara resmi menyetujui dokumen untuk proses transisi untuk melanjutkan serah terima, dan menyatakan bahwa perannya bukanlah untuk mensertifikasi orang yang dipilih, tetapi orang yang dipilih sebenarnya akan ditentukan oleh proses pemilihan yang ditentukan oleh Konstitusi Amerika Serikat (Gambar 2.11).

Gambar 2.12 Para pendukung Presiden Donald Trump memanjat tembok barat Gedung Capitol AS pada hari Rabu, 6 Januari 2021, di Washington (Jose Luis Magana/Associated Press)

Trump mengatakan dia akan meninggalkan Gedung Putih jika Electoral College memilih Joe Biden. Pada tanggal 14 Desember, Electoral College memilih presiden dan wakil presiden. Hasil pemungutan suara mengukuhkan Joe Biden sebagai presiden Amerika Serikat ke-46 dan Kamala Harris sebagai wakil presiden Amerika Serikat ke-49. Kongres dijadwalkan bertemu dalam sesi gabungan pada tanggal 6 Januari 2021, untuk secara resmi menghitung suara electoral college yang diajukan oleh negara bagian, yang dikenal sebagai sertifikasi hasil pemungutan suara setiap negara bagian. Berdasarkan Konstitusi Amerika Serikat, penghitungan dan sertifikasi suara elektoral oleh kedua majelis Kongres merupakan langkah terakhir dalam mengonfirmasi pemilihan presiden secara resmi. Namun, Capitol diserang oleh para ekstremis hari itu, perusuh menerobos perimeter polisi dan menyerbu Kompleks Capitol Amerika Serikat. Itu adalah pertama kalinya Gedung Capitol AS diserang sejak Inggris menginvasi pada tahun 1814. Sejumlah besar demonstran berkumpul di luar Gedung Capitol dan membawa bendera pro-Trump untuk memprotes pemilihan umum.

Demonstrasi kemudian meningkat menjadi kerusuhan, dengan para pengunjuk rasa bentrok dengan petugas keamanan dan gas air mata di udara. Beberapa demonstran bahkan memecahkan jendela Gedung Capitol dan memasuki bagian dalam gedung. Lima orang tewas selama kerusuhan itu. Penghitungan suara elektoral oleh Kongres terganggu oleh perusuh pro-Trump yang menyerbu Gedung Capitol. Kerusuhan ini menyebabkan penangguhan sesi gabungan untuk mengesahkan hasil pemilu. Setelah sesi gabungan Kongres Amerika Serikat mengonfirmasi Joe Biden dan Kamala Harris pada dini hari tanggal 7 Januari waktu setempat, Trump segera mengeluarkan pernyataan yang menjanjikan transfer kekuasaan yang "tertib" pada tanggal 20 Januari 2021 (Gambar 2.12).

2.5.2 Platform Media Sosial Memblokir Akun Trump

Setelah penyerbuan Gedung Capitol Amerika Serikat pada tanggal 6 Januari 2021, yang dilakukan oleh gerombolan pendukung Presiden Donald Trump, banyak platform media sosial dan perusahaan teknologi menangguhkan atau melarang akun Trump dan timnya dari platform mereka, dan banyak organisasi bisnis memutuskan hubungan dengannya. Pada tanggal 9 Januari 2021, Fox News mencantumkan platform media sosial yang telah “melarang” atau “membatasi” Trump, platform-platform ini mengambil berbagai tindakan untuk memblokir akun Trump dan akun terkaitnya.

Menurut statistik media Amerika Axios, platform yang telah mengambil tindakan untuk melarang atau membatasi Trump dan akun terkaitnya termasuk Twitter, Facebook, Google, Apple, YouTube, Reddit, Instagram, Snapchat, Discord, Pinterest, dan platform lainnya. Beberapa platform dan situs web telah menganggap “Trump” sebagai kata yang sensitif dan menghapus postingan segera setelah mereka mendeteksinya. Akun putra remaja Trump, Barron, ditangguhkan setelah ia mengirim tweet “Halo Twitter” (Gambar 2.13).

Gambar 2.13 Twitter telah menangguhkan Presiden Trump dari platformnya

"Setelah meninjau dengan saksama Tweet terbaru dari akun @realDonaldTrump dan konteks di sekitarnya, kami telah menangguhkan akun tersebut secara permanen karena risiko hasutan kekerasan lebih lanjut," kata Twitter. *"Dalam konteks peristiwa mengerikan minggu ini, kami menjelaskan pada hari Rabu bahwa pelanggaran tambahan terhadap Aturan Twitter berpotensi mengakibatkan tindakan ini."* (Gambar 2.14).

Setelah Twitter melarang akun @realDonaldTrump miliknya, Trump mencuit dari akun resmi presiden AS @Potus yang menyatakan bahwa ia akan "mencari kemungkinan untuk membangun platform kami sendiri di masa mendatang" dan mengecam Twitter. Namun, tweet tersebut dihapus dari platform segera setelah diposting (Gambar 2.15).

"Jika jelas bahwa akun lain digunakan untuk tujuan menghindari larangan, akun tersebut juga dapat ditangguhkan," kata Twitter dalam sebuah pernyataan. *"Untuk akun pemerintah, seperti @POTUS dan @WhiteHouse, kami tidak akan menangguhkan akun tersebut tetapi akan mengambil tindakan untuk membatasi penggunaannya. Namun, akun-akun ini akan dialihkan ke pemerintahan baru pada waktunya dan tidak akan ditangguhkan oleh Twitter kecuali benar-benar diperlukan untuk mengurangi kerugian di dunia nyata."* Kebijakan Twitter juga akan melarang Trump mengarahkan pihak ketiga untuk mengoperasikan akun Twitter atas namanya.

Gambar 2.14 Pernyataan resmi dari Twitter

Pendukung Trump telah bermigrasi ke platform media sosial khusus seperti Parler selama berhari-hari. Parler sempat menduduki puncak tangga unduhan aplikasi. Sebagai tanggapan, raksasa internet menargetkan Parler. Google menghapus Parler dari App Store dan Apple mengeluarkan ultimatum kepada Parler. Amazon berhenti menawarkan layanan web Parler seperti hosting. Menurut laporan *Agence France Presse* (AFP) pada 11 Januari 2021,

platform Parler tidak dapat diakses setelah tengah malam pada hari itu, yang menunjukkan bahwa platform tersebut terputus.

Gambar 2.15 Tweet Trump setelah akunnya ditangguhkan oleh Twitter

Kepala Twitter Jack Dorsey mengatakan bahwa pelarangan terhadap Presiden AS Donald Trump adalah hal yang benar untuk dilakukan. Ia menegaskan kembali bahwa pencabutan akun presiden dari Twitter dilakukan setelah adanya "peringatan yang jelas" kepada Trump. *"Kami membuat keputusan dengan informasi terbaik yang kami miliki berdasarkan ancaman terhadap keselamatan fisik baik di dalam maupun di luar Twitter,"* kata Dorsey. Namun, ia menerima bahwa tindakan tersebut akan berdampak pada internet yang terbuka dan bebas (Gambar 2.16).

Tokoh politik di Eropa tidak menyetujui keputusan platform media sosial untuk memblokir akun Trump, seperti Kanselir Jerman Angela Merkel. Steffen Seibert, juru bicara utama Merkel, mengatakan bahwa operator platform media sosial "memikul tanggung jawab besar agar komunikasi politik tidak diracuni oleh kebencian, kebohongan, dan hasutan untuk melakukan kekerasan", pada konferensi pers rutin di Berlin, pada 11 Januari 2021. Ia mengatakan bahwa adalah benar untuk tidak "menjauh" ketika konten tersebut diunggah, misalnya dengan menandainya. Namun Seibert juga mengatakan bahwa kebebasan berpendapat adalah hak fundamental yang “sangat penting.” “Hak fundamental ini dapat diintervensi, tetapi menurut hukum dan dalam kerangka yang ditetapkan oleh legislator bukan menurut keputusan manajemen platform media sosial,” katanya kepada wartawan di Berlin. “Dilihat dari sudut ini, kanselir menganggap bermasalah bahwa akun presiden AS kini telah diblokir secara permanen”.

Bruno Le Maire, menteri keuangan Prancis, mengatakan dia “terkejut” oleh keputusan Twitter untuk melarang Trump, seraya menambahkan bahwa “regulasi digital tidak boleh

dilakukan oleh oligarki digital (dan) merupakan masalah rakyat yang berdaulat, pemerintah, dan peradilan".

Gambar 2.16 Pimpinan Twitter mengatakan bahwa ia tidak merayakan atau merasa bangga dengan larangan tersebut yang muncul setelah kerusuhan di Capitol

Cédric O, menteri digital Prancis, menyampaikan kekhawatiran serupa. Ia bertanya-tanya tentang jejaring sosial yang "mungkin memutuskan untuk menyensor seseorang yang diikuti oleh 88 juta orang secara sepihak". "Mereka campur tangan dalam perdebatan publik tanpa pengawasan demokratis, tanpa tindakan keadilan, dengan hanya mengacu pada ketentuan umum penggunaan mereka", ia memperkirakan. "Bayangkan Twitter atau Facebook menjadi terpolitisasi dan menganggap bahwa mereka berada di pihak politik ini atau itu, jelasnya. Mereka dapat mengubah ketentuan layanan mereka dengan mengatakan, misalnya, 'Anda tidak diizinkan untuk membuat pro-Demokrat atau pro-Republik, atau pro-partai atau partai di Prancis. Dalam kasus seperti itu, mereka akan menyensor seluruh ekspresi tanpa pengawasan apa pun karena mereka berada di luar kendali keadilan dan pluralitas ekspresi demokratis".

Thierry Breton, komisaris Uni Eropa untuk pasar internal, mengatakan dalam sebuah opini di Politico: "Sama seperti 9/11 yang menandai pergeseran paradigma untuk keamanan global, 20 tahun kemudian kita menyaksikan perubahan sebelum dan sesudah dalam peran platform digital dalam demokrasi kita". Breton mengatakan insiden di Washington mengungkapkan "kerapuhan demokrasi kita dan ancaman yang dapat ditimbulkan oleh perusahaan teknologi yang kurang diatur terhadap kelangsungan hidup mereka". Dia menyatakan keraguan serius tentang apakah perusahaan media sosial saja yang seharusnya memiliki kekuatan untuk memblokir akun seorang presiden AS. "Fakta bahwa seorang CEO dapat mencabut pengeras suara (Trump) tanpa pemeriksaan dan keseimbangan apa pun membingungkan," tulis Breton. "Ini bukan hanya konfirmasi kekuatan platform ini, tetapi juga menunjukkan kelemahan mendalam dalam cara masyarakat kita diatur dalam ruang digital," tambahnya. Breton juga membela usulan Uni Eropa baru-baru ini untuk mengatur perusahaan

teknologi besar dengan lebih ketat, termasuk Undang-Undang Layanan Digital yang dapat menyebabkan platform menghadapi denda karena gagal mengekang konten ilegal.

"Siapa yang memutuskan kebebasan berbicara?" 20 Minuten AG mengatakan bahwa kebebasan berbicara bukan hanya masalah hukum. Kekhawatirannya adalah bahwa di dunia digital, raksasa internet memiliki keputusan akhir. Der Spiegel mengatakan bahwa raksasa internet telah membiarkan platform mereka disalahgunakan terlalu lama selama bertahun-tahun, membiarkan berita palsu dan hasutan untuk melakukan kekerasan menyebar di platform mereka dalam upaya untuk memonopoli dan memperluas, dan bahwa beberapa politisi yang berkuasa menikmati perlindungan khusus. Namun fakta bahwa para miliarder dari Silicon Valley ini dapat memutuskan sendiri siapa yang akan dilarang dan siapa yang akan diizinkan untuk berbicara daring sungguh menakutkan.

2.5.3 Mengatur Kekuasaan Platform Media Sosial

Kekuasaan keempat, yang juga dikenal sebagai kekuasaan ke-4, mengacu pada kekuasaan politik keempat selain "kekuasaan eksekutif, kekuasaan legislatif, kekuasaan yudikatif", mengacu pada media, publik, dan dengan demikian. Teori kekuasaan ke-4 menekankan kebebasan berbicara yang ditetapkan oleh pers. Teori kekuasaan ke-4 menunjukkan bahwa "tujuan kebebasan pers yang dijamin oleh konstitusi adalah untuk menjaga otonomi media, sehingga media dapat memberikan informasi, opini publik, dan program hiburan yang tidak dikendalikan atau dipengaruhi oleh pemerintah, mendorong masyarakat untuk peduli terhadap pekerjaan pemerintah dan membahas urusan publik, sehingga dapat memainkan fungsi pengawasan pemerintah."

Di era jaringan, kebebasan berbicara individu seharusnya berada di bawah kendali kedaulatan nasional, tidak ditentukan oleh platform digital. Meskipun negara selalu dan akan terus memainkan peran sentral dalam urusan internasional, aktor non-negara seperti perusahaan multinasional juga menjadi semakin penting, dan beberapa perusahaan bahkan memiliki kekuatan asosiatif yang lebih kuat daripada negara berdaulat. Misalnya, nilai pasar perusahaan induk Google, Alphabet, setara dengan gabungan PDB Belgia dan Belanda. Twitter, Facebook, Apple, dan lainnya memiliki akses ke informasi tentang ratusan juta netizen di seluruh dunia.

Raksasa internet telah memperoleh posisi yang lebih kuat di hadapan negara dan publik. Hal ini bergantung pada besarnya jumlah data yang mereka miliki, keterlibatan pengguna yang dibawa oleh layanan mereka, dan kekuatan politik dan sosial dari platform itu sendiri. Pemblokiran akun Trump oleh beberapa media sosial di Amerika Serikat justru merupakan pelaksanaan kekuatan super mereka.

Industri, teknologi, dan informasi global tumbuh lebih cepat daripada tata kelola global dan kekuatan regulasi negara-negara berdaulat. Bagaimana mendefinisikan batas kewenangan dan tanggung jawab hukum oligarki digital telah menjadi masalah dan sulit untuk mencapai kesepakatan di antara negara-negara. Pengaruh perusahaan terkait terhadap politik nasional, ekonomi, masyarakat, dan aspek-aspek lain serta tantangan yang mereka bawa semakin meningkat dari hari ke hari. Kekuatan digital yang tidak terkendali telah menyebabkan dampak negatif tertentu pada kehidupan politik tradisional, opini sosial, dan

kegiatan ekonomi. Lingkungan hukum di Amerika Serikat relatif ramah terhadap platform digital. Mengikuti tradisi Amandemen Pertama Konstitusi Amerika Serikat, politik dan masyarakat Amerika sangat berhati-hati tentang kekuatan publik yang mengganggu penyebaran opini publik. Bagian 230 dari *Communications Decency Act* (CDA) memberikan kekebalan dari tanggung jawab bagi penyedia dan pengguna "layanan komputer interaktif" yang menerbitkan informasi yang diberikan oleh pengguna pihak ketiga.

Undang-undang dalam Bagian 230(c)(2) selanjutnya memberikan perlindungan "Orang Samaria yang Baik" dari tanggung jawab perdata bagi operator layanan komputer interaktif dalam penghapusan atau moderasi materi pihak ketiga yang mereka anggap cabul atau menyinggung, bahkan ucapan yang dilindungi secara konstitusional, selama dilakukan dengan itikad baik. Ini berarti bahwa otoritas kehakiman tidak dapat meminta pertanggungjawaban perusahaan Internet atas apa yang dikatakan pengguna di platform Internet, di sisi lain, pengguna tidak dapat meminta pertanggungjawaban perusahaan Internet atas postingan mereka yang dihapus atau diblokir di platform Internet. Peraturan ini dirancang untuk mencegah Komisi Komunikasi Federal (FCC) mengganggu Internet, dan juga memungkinkan situs web untuk menyensor konten sesuai dengan kebutuhan mereka sendiri.

Selama lebih dari 20 tahun, Pasal 230 telah dikritik oleh politisi dan aktivis hak-hak sipil karena dianggap membenarkan perundungan siber, tetapi banyak orang di industri teknologi percaya bahwa pasal ini menciptakan fondasi layanan Internet modern. Sementara Departemen Kehakiman AS (DOJ) telah mengusulkan undang-undang pada tahun 2019 untuk mengubah pembagian tanggung jawab atas penyensoran konten, undang-undang tersebut menghadapi tentangan keras dari beberapa perusahaan seperti Facebook. Pada tanggal 14 Oktober 2019, Facebook dan Twitter kembali membatasi penyebaran dua laporan skandal tentang Hunter Biden, putra mantan wakil presiden Joe Biden, dengan alasan pelanggaran aturan platform tersebut. Langkah ini memunculkan kembali perdebatan tentang apakah akan mengubah Pasal 230 Undang-Undang Kepatutan Komunikasi.

Keputusan Twitter untuk menangguhkan akun Presiden AS Donald Trump mendorong para pemimpin Eropa untuk menekankan perlunya mengatur perusahaan media sosial. Thierry Breton, Komisioner UE untuk Pasar Internal, menyuarakan kekhawatiran tentang “kelemahan mendalam dalam cara masyarakat kita diorganisasikan dalam ruang digital”. Manfred Weber, ketua kelompok EPP di Parlemen Eropa, mengemukakan bahwa “kita tidak dapat menyerahkan kepada perusahaan-perusahaan Big Tech Amerika untuk memutuskan apa yang boleh dan tidak boleh kita bahas, apa yang boleh dan tidak boleh dikatakan dalam wacana demokrasi. Kita memerlukan pendekatan regulasi yang lebih ketat”.

Eropa telah mengambil sikap yang sangat berbeda dalam mengatur Big Tech dibandingkan AS, di mana perusahaan-perusahaan sering kali dibiarkan mengatur diri mereka sendiri dan biasanya menikmati tingkat kekebalan hukum yang signifikan melalui perlindungan seperti Bagian 230. Kritik terbaru terhadap platform media sosial besar ini dapat diartikan sebagai tembakan peringatan. Komisi Eropa telah mengambil inisiatif ganda dalam arah ini atas nama negara-negara anggota UE. Undang-Undang Layanan Digital dan Undang-Undang Pasar Digital adalah dua langkah penting ke depan bagi Eropa, dan keduanya terutama

ditujukan kepada raksasa Internet yang dikenal sebagai “gatekeepers” daripada perusahaan-perusahaan biasa. Undang-Undang Layanan Digital akan mengatur model bisnis dan perilaku raksasa internet sesuai dengan standar Eropa, dengan menekankan bahwa raksasa internet memiliki kewajiban hukum untuk menyensor konten, yang dapat mengakibatkan denda besar hingga ratusan juta euro jika dilanggar. Kedua undang-undang ini juga akan menciptakan preseden bagi negara-negara besar untuk menetapkan aturan bagi regulasi perusahaan digital, dan memiliki signifikansi utama yang kuat bagi perumusan norma hukum di bidang-bidang terkait di seluruh dunia.

Selama beberapa waktu, perusahaan-perusahaan Internet AS, yang diwakili oleh raksasa-raksasa Lembah Silikon, telah menjadi target "fokus" regulasi UE. Pada bulan Februari 2020, Presiden Komisi Eropa yang baru diangkat, Ursula Gertrud von der Leyen, menjelaskan konsep "kedaulatan digital", "UE harus memiliki kemampuan untuk membuat pilihannya sendiri berdasarkan nilai-nilai dan aturannya sendiri di bidang digital". Banyak media Eropa percaya bahwa Peraturan Perlindungan Data Umum (GDPR) dan Undang-Undang Layanan Digital, akan menjadi alat hukum utama bagi kepemimpinan UE saat ini untuk memastikan kedaulatan digital.

Pada saat yang sama, UE juga berupaya keras untuk membangun infrastruktur Internetnya sendiri. Dalam pidato mereka tahun lalu, Ursula Gertrud von der Leyen, Merkel, dan Presiden Prancis Macron semuanya menyebutkan ketergantungan besar Eropa pada perusahaan-perusahaan Internet AS seperti Google, Facebook, dan Twitter. Mereka mengumumkan bahwa UE akan meluncurkan platform komputasi awan "GAIA-X" sebagai platform untuk menyimpan data, berdasarkan pengembangan bersama Prancis dan Jerman. Kesimpulannya, penangguhan akun Trump menunjukkan bahwa kedaulatan digital harus diatur secara ketat oleh kedaulatan jaringan nasional, dan konsolidasi kedaulatan jaringan nasional perlu dilaksanakan dalam pembangunan jaringan berdaulat, sehingga dapat memastikan perlindungan yang efektif terhadap kedaulatan jaringan dan keamanan nasional.

BAB 3
ARSITEKTUR JARINGAN KEDAULATAN

Meskipun konsep desain awal Internet terdesentralisasi, tetapi kontrol saat ini terhadap arsitektur teknologi dasar menunjukkan bentuk terpusat yang kuat. Oleh karena itu, sangat penting untuk mengajukan arsitektur jaringan baru guna memenuhi permintaan pengembangan jaringan di masa mendatang dan mewujudkan manajemen nama domain yang terdesentralisasi melalui sarana teknis. Jaringan kedaulatan secara efektif mewujudkan pengelolaan bersama dan tata kelola bersama multilateral di dunia maya, dan mengakhiri pengelolaan terpusat di bawah pengenal IP tunggal. Pada saat yang sama, jaringan ini melindungi jaringan semua negara dari risiko hilangnya DNS dan pembutaan yang disebabkan oleh noda zona akar ICANN atau serangan peretas. Dengan dibangunnya jaringan kedaulatan, tata kelola bersama dan pengelolaan mandiri semua pihak di dunia maya dapat benar-benar terwujud.

3.1 JARINGAN KEDAULATAN

3.1.1 Definisi Jaringan Kedaulatan

Jaringan kedaulatan dengan arsitektur baru, merupakan jaringan nasional yang berpusat pada identitas yang dapat digunakan untuk mendaftarkan, menghasilkan, mengelola, dan menetapkan nama domain identitas perorangan atau organisasi perusahaan secara otonom dan terkendali.

Menurut peraturan internasional, bisnis dunia maya diatur oleh undang-undang Radio dan Televisi yang lebih ketat daripada undang-undang telekomunikasi di berbagai negara. Rilis berita jaringan telekomunikasi relatif sewenang-wenang, yang mengakibatkan banyaknya informasi palsu di jaringan, menunjukkan bahwa telekomunikasi tidak cukup dalam pengawasan konten. Jaringan penyiaran nasional mewakili suara pemerintah nasional, dan pengawasan bidang ideologisnya selalu menjadi prioritas utama bagi berbagai departemen atau industri.

Oleh karena itu, buku ini memilih jaringan siaran televisi sebagai skenario aplikasi tipikal untuk menyebarkan jaringan kedaulatan yang dikelola secara otonom sepenuhnya dengan arsitektur baru yang berpusat pada identitas yang aman, andal, mudah dikelola, otonom, dan cerdas.

3.1.2 Persyaratan Fungsional untuk Jaringan Kedaulatan

Untuk membangun jaringan kedaulatan, perlu dipastikan bahwa pengguna dalam jaringan dapat mengakses Internet dan memperoleh konten Internet. Pada saat yang sama, untuk menyesuaikan dengan gelombang pengembangan jaringan di masa mendatang, jaringan kedaulatan harus menyediakan fungsi baru untuk mendukung kebutuhan baru pengguna. Sambil memastikan untuk menyediakan sumber daya konten yang kaya, jaringan

kedaulatan juga perlu menyediakan tingkat keamanan yang lebih tinggi daripada arsitektur jaringan yang ada.

Persyaratan fungsional jaringan kedaulatan tercantum sebagai berikut:

(1) Pengidentifikasi tingkat atas yang dikelola secara multilateral untuk mendukung konektivitas.

(2) Pengidentifikasi milik suatu negara dapat dikelola secara independen oleh negara tersebut. Setiap ruang maya virtual dalam suatu negara bersifat independen satu sama lain.

(3) Manajemen pengguna klasifikasi harus didukung. Menurut pengguna dari berbagai usia dan pekerjaan, mekanisme kontrol lingkup pengguna klasifikasi memastikan lingkungan jaringan yang bersih dan aman.

(4) Pengguna dapat mengakses konten Internet yang sah. Misalnya, staf produksi dan penyiaran dapat mengakses semua konten di Internet kecuali kode dan perangkat lunak, dan pengguna dewasa biasa dapat mengakses semua konten yang tidak sensitif di Internet, tetapi pengguna di bawah umur biasa hanya dapat mengakses sumber daya tertentu.

(5) Jaringan kedaulatan dapat mendukung persyaratan 5G dan menyediakan transmisi data kabel dan nirkabel.

(6) Keamanan sumber daya dan data konten dalam jaringan kedaulatan harus dijamin, yaitu, jaringan kedaulatan harus secara efektif mencegah serangan jaringan yang ada (seperti worm dan lalu lintas berbahaya), serta memastikan pengoperasian sistem yang stabil.

(7) Jaringan produksi dan penyiaran program radio dan televisi dapat berjalan daring secara real time.

(8) Jaringan kedaulatan dapat memberikan pengalaman pengguna yang lebih baik untuk menonton video, seperti kecepatan akuisisi video yang lebih cepat dan pemutaran video yang lebih stabil. (9) Permainan elektronik, e-commerce, panggilan suara, panggilan video, dan layanan lainnya harus didukung.

(9) Konten dalam jaringan kedaulatan masih dapat memenuhi kebutuhan dasar pengguna setelah secara fisik terisolasi dari Internet, yaitu, pengguna masih dapat mengakses beberapa konten yang sebelumnya diakses yang dipublikasikan di Internet eksternal.

(10) Pengguna dalam jaringan kedaulatan dapat mempublikasikan konten secara aktif.

(11) Jaringan kedaulatan harus mendukung berbagai fungsi, seperti siaran langsung video, siaran sesuai permintaan, pemutaran, penggandaan kecepatan, dan pergeseran waktu, seperti sistem yang ada.

(12) Bisnis dasar lainnya.

3.2 TEKNOLOGI YANG ADA

3.2.1 IPv9

Sekarang beberapa peneliti menggunakan IPv9, yaitu jaringan desimal, untuk merancang jaringan berdaulat. Jaringan desimal adalah versi modifikasi dari proposal IETF

oleh Bapak Jianping Xie, direktur Shanghai General Chemical Research Institute. Sistem jaringan desimal terutama terdiri dari protokol alamat IPv9, protokol header IPv9, protokol transisi IPv9, spesifikasi nama domain digital, dan protokol serta standar lainnya. Nama domain digital mengacu pada penggunaan angka Arab 0–9 sebagai pengganti huruf Inggris tradisional sebagai nama domain. Nama domain digital, yang merupakan bagian dari sistem jaringan desimal, juga dapat digunakan secara langsung sebagai alamat IPv9.

Protokol IPv9 mengharuskan penggunaan angka Arab 0–9 sebagai alamat IP virtual, dan penggunaan sistem desimal sebagai metode representasi teks, yang mudah ditemukan oleh pengguna Internet. Untuk meningkatkan efisiensi dan kemudahan penggunaan bagi pengguna akhir, beberapa alamat dapat langsung digunakan sebagai nama domain. Karena IPv9 mengklasifikasikan dan mengkodekan layanan jaringan komputer asli, jaringan siaran kabel, dan jaringan telekomunikasi, IPv9 juga dikenal sebagai "protokol integrasi informasi yang aman dan andal generasi baru". Jaringan desimal mengacu pada jaringan baru yang menggunakan algoritma desimal dan metode representasi teks. Jaringan ini menghubungkan berbagai komputer menggunakan algoritma desimal ke dalam jaringan, dan dapat dikomunikasikan dengan jaringan yang ada.

Sistem jaringan desimal menggunakan desimal, multi-protokol dalam sistem nama domain untuk memetakan nama domain Inggris, Mandarin, dan lainnya ke alamat IP unik global. Selain itu, IPv9 membentuk sistem nama domain akar terdistribusi, memperkenalkan konsep negara dan wilayah, sehingga setiap negara memiliki sistem nama domain akarnya sendiri, untuk membangun dan mempertahankan status dan citranya sebagai negara berdaulat di Internet. IPv9 meningkatkan panjang alamat IP dari 32 dan 128 bit menjadi 2048 bit untuk mendukung lebih banyak level alamat, lebih banyak node yang dapat dialamatkan, dan menyediakan konfigurasi alamat otomatis yang sederhana. Pada saat yang sama, panjang alamat 32-bit IPv4 dikurangi menjadi 16 bit, yang memecahkan masalah komunikasi seluler dalam komunikasi seluler. Alamat IPv9 menentukan pengenal 256-bit untuk antarmuka dan grup antarmuka, dan dapat dibagi menjadi tiga jenis. Ketiga jenis alamat tersebut adalah sebagai berikut:

(1) Unicast: Satu antarmuka memiliki pengenal. Paket yang dikirim ke alamat unicast diteruskan ke antarmuka yang diidentifikasi oleh alamat tersebut.

(2) VoD Arbitrer: Umumnya, sekelompok antarmuka yang termasuk dalam node yang berbeda memiliki pengenal. Paket yang dikirim ke alamat VoD (Video-On-Demand) yang acak diteruskan ke antarmuka yang diidentifikasi oleh alamat tersebut dan diukur menurut jarak protokol routing.

(3) Multicast: Sekelompok antarmuka yang termasuk dalam node yang berbeda umumnya memiliki pengenal, tetapi paket yang dikirim ke alamat multicast akan melewati semua antarmuka dari alamat tersebut. Tidak ada alamat siaran di IPv9, dan fungsinya digantikan oleh alamat multicast. Ada lima jenis alamat IPv9:

   a) Alamat IPv9: Alamat ini berbentuk Y[Y[Y [Y[Y [Y[Y], di mana setiap Y mewakili bilangan bulat desimal antara 0 dan 232.

b) Alamat IPv9 yang kompatibel dengan IPv4: Alamat ini berbentuk Y[Y[Y [Y [Y [Y[Y [D.D.D.D, di mana setiap Y mewakili bilangan bulat desimal antara 0 dan 232, dan setiap D mewakili bilangan bulat desimal antara 0 dan 28 dari IPv4 asli.
c) Alamat IPv9 yang sesuai dengan IPv6: Alamat ini berbentuk Y[Y[Y[Y [X:X:X: X:X:X:X:X. Di mana setiap Y mewakili bilangan bulat desimal antara 0 dan 232, dan setiap X mewakili angka heksadesimal antara 0000 dan FFFF dari IPv6 asli.
d) Alamat khusus yang kompatibel.
e) Alamat desimal penuh: Untuk kenyamanan kode logistik dan aplikasi alamat desimal penuh.

IPv9 memiliki karakteristik berikut:

(1) IPv9 mengadopsi metode dengan panjang tetap dan non-posisi seperti telepon, yang mengurangi overhead jaringan.
(2) IPv9 mengadopsi mekanisme enkripsi khusus untuk memastikan keamanan jaringan. Jaringan IPv9 lebih aman karena IPv9 memiliki lebih banyak alamat, lebih banyak mode alamat (panjang variabel, dan teknologi enkripsi alamat IP unik), dan lebih banyak definisi header ekstensi IPv9. Informasi header alamat, pesan, dan nomor protokol tidak diungkapkan, tetapi memiliki sistemnya sendiri. Bahkan jika protokol diungkapkan, hanya bagian sipil yang akan diungkapkan, dan bagian militer akan diputuskan oleh tentara. Dibandingkan dengan IPv9, berbagai langkah keamanan dalam sistem jaringan IPv4/IPv6 tidak dapat diputuskan sendiri, dan masih sulit untuk menjamin keamanan meskipun IPv4/IPv6 menggunakan IPsec (Internet Protocol Security), SSL (Secure Sockets Layer), dan langkah-langkah lainnya. Secara teori, lebih sulit untuk memecahkan protokol khusus daripada algoritma kriptografi. Selain itu, menurut standar IPv4/IPv6 saat ini, alamat 32-bit/128-bit tidak dapat dienkripsi karena hilangnya tujuan.
(3) IPv9 mengadopsi protokol TCP/IP kelas kode absolut dan kode aliran panjang, yang memecahkan kontradiksi antara transmisi audio dan video dalam rangkaian pengalihan paket. Alamat IP dapat digunakan sebagai nama domain, yang sesuai dengan telepon seluler dan jaringan pita lebar keluarga.
(4) IPv9 memiliki kategori darurat, yang dapat memastikan jalur transmisi tidak diblokir jika terjadi perang dan keadaan darurat nasional. Selain transmisi ciphertext dari komunikasi jaringan, protokol IPv9 juga menetapkan bit darurat karena standar protokolnya. Jika terjadi kerusakan sebagian jaringan militer dalam perang, router sipil yang relevan dapat segera diminta, kemudian tabel perutean dimodifikasi melalui penyiaran router, sehingga dapat mencapai tujuan permintaan perang.
(5) Karena IPv9 mengadopsi sirkuit point-to-point, perlindungan privasi pengguna diperkuat.
(6) IPv9 sangat cocok untuk transmisi jaringan nirkabel.

Selain fitur-fitur di atas, IPv9 juga independen dari jaringan IPv4 dan IPv6 asli, sehingga keamanan jaringan dan keamanan informasi dapat dikontrol dan dikelola secara independen oleh arsitektur baru. Sebagai hasil dari jaringan independen, departemen terkait dapat

mengembangkan layanan informasi publik secara independen dan fleksibel sesuai dengan kebijakan nasional. Hal ini kondusif bagi pengembangan pencarian informasi Tiongkok di masa mendatang berdasarkan perluasan sistem bisnis aplikasi tingkat lanjut.

Untuk mematuhi kebiasaan pengguna, IPv9 kompatibel dengan IPv4 dan IPv6. Di satu sisi, IPv9 telah mewujudkan fungsi penggunaan IPv4 sebagai terowongan untuk membawa transmisi data antara dua subnet IPv9. Di sisi lain, mereka juga telah mewujudkan fungsi penggunaan IPv9 sebagai terowongan untuk membawa transmisi data antara dua subnet IPv4. Dengan cara ini, interkoneksi antara IPv9 dan IPv4 tercapai.

Keuntungan utama IPv9 adalah sebagai berikut. Pertama, IPv9 memiliki sistem kekayaan intelektual independen dan sumber daya dunia maya yang besar. Kedua, sistem jaringan desimal dapat menerjemahkan alamat biner asli secara langsung ke dalam teks desimal, yang sesuai dengan kebiasaan sehari-hari pengguna. Ketiga, IPv9 hadir dengan skema desain, yaitu nama domain dan alamat IP terintegrasi, serta kode identitas orang dan objek disatukan. Hal itu membuat telepon, telepon seluler, nama domain dan alamat IP, IPTV, telepon IP, dan sebagainya bergabung menjadi satu nomor.

Dengan cara ini, proses penerjemahan antara nama domain jaringan dan alamat IP dapat dihindari, yang membuat komunikasi jaringan menjadi cepat dan langsung, serta meningkatkan kemampuan komunikasi peralatan peralihan jaringan yang ada. Keempat, dengan menggunakan mekanisme enkripsi tertentu, IPv9 menjamin keamanan jaringan. Kelima, dari sudut pandang menjaga kedaulatan, IPv9 pertama-tama mengusulkan konsep "kesetaraan kedaulatan" dunia maya. Sistem nama domain digital desimal multiprotokol yang diusulkan kompatibel dengan nama domain Inggris, Mandarin, dan nama domain lainnya yang dipetakan ke alamat IP unik global. Meskipun IPv9 memiliki banyak kelebihan, terdapat banyak kritik terhadapnya di industri, yang tercantum sebagai berikut:

(1) Bit dasar alamat sumber dan alamat tujuan yang digunakan dalam pesan IPv9 adalah 256 bit, dan maksimumnya adalah 2048 bit. Ruang alamat 256-bit adalah 2256, dan jumlah total atom materi biasa di alam semesta yang dapat diamati adalah sekitar 1080. Ruang alamatnya sebanding dengan jumlah total atom materi biasa di alam semesta yang dapat diamati. Menggunakan 256 bit sebagai ruang alamat sudah cukup besar, dan 2048 bit tidak terbayangkan. Jaringan sebenarnya tidak memerlukan ruang alamat yang begitu besar.

(2) Ruang alamat IPv9 terlalu panjang sehingga menimbulkan masalah penggunaan ruang alamat yang tidak efisien. Akan ada banyak alamat yang tidak digunakan secara efektif.

(3) Karena IPv9 menggunakan alamat sumber dan alamat tujuan dengan bit dasar 256-bit, yang menyebabkan header pesan menjadi besar, dan menyebabkan banyak masalah dalam efisiensi transmisi jaringan dan pengendalian kemacetan. Header IPv9 selalu diperlukan untuk transmisi bahkan untuk data yang sangat kecil, sehingga mengakibatkan rendahnya efisiensi transmisi jaringan. Selain itu, ukuran frame Ethernet saat ini berdasarkan IPv4 dan IPv6 adalah 1500 byte. Jika header IPv9 memakan terlalu banyak ruang, jumlah data yang ditransmisikan oleh setiap frame akan berkurang.

(4) Kapasitas memori dan komputasi perangkat di Internet of Things dan Industrial Internet terbatas, dan ruang penyimpanan biasanya kurang dari 10 KB. IPv9 dengan header yang panjang untuk transmisi data sulit memenuhi persyaratan aplikasi Internet of Things dan skenario lainnya.

(5) IPv9 mengharuskan setiap tautan di Internet memiliki MTU minimal 576 byte. Pada tautan mana pun, jika tidak dapat mengirimkan 576 byte data dalam satu paket data, segmen data terkait tautan dan penyusunan ulang harus didukung pada level di bawah IPv9. Hal ini tidak diragukan lagi meningkatkan tekanan pemrosesan data pada lapisan tautan.

(6) IPv9 secara langsung menggunakan alamat tersebut sebagai nama domain untuk permintaan konten, dan alamat nama domainnya sangat besar. Cara cepat mencari, mencocokkan, dan meneruskan permintaan konten pada router akan menjadi masalah.

(7) Metode penamaan dan pengalamatan yang digunakan dalam IPv9 merupakan tantangan besar dalam pencarian dan pengalamatan cepat dengan sejumlah besar pengenal. Pada saat yang sama, skema pengalamatan lokasi geografis yang diusulkan oleh IPv9 memerlukan konversi alamat IP dan alamat lokasi geografis. Karena alamat lokasi geografis dan alamat IPv9 sama-sama panjang, hal ini juga menjadi tantangan dalam pencarian cepat.

(8) IPv9 mengadopsi format alamat "desimal" baru, yang berbeda dari IPv4 dan IPv6, sehingga mengakibatkan hambatan pada koneksinya ke Internet.

(9) IPv9 tidak menjamin keamanan jaringan yang sebenarnya. Tujuan dari keluarga protokol TCP/IP adalah untuk membantu komputer dalam jaringan yang berbeda (seperti Ethernet, token ring, FDDI, ATM, dll.) untuk berkomunikasi satu sama lain dalam "jaringan umum" virtual, protokol yang berbeda direalisasikan secara berbeda. Oleh karena itu, IPv9 pada dasarnya adalah versi protokol yang berbeda yang berasal dari teknologi yang sama dan konvensi yang berbeda dengan IPv6. IPv9 tidak menghindari cacat bawaan IPv4 dan IPv6.

(10) Tidak ada alamat siaran dalam protokol IPv9, jadi alamat multicast digunakan sebagai ganti alamat siaran. Penggunaan IPv9 untuk membangun jaringan kedaulatan akan mengakibatkan keterbatasan waktu nyata, ekstensibilitas, dan fleksibilitas transmisi data.

3.2.2 IP Baru

Untuk mendukung aplikasi jaringan yang sedang berkembang, Huawei Technology Co., LTD. mengusulkan kerangka protokol baru yang disebut “IP Baru” pada tahun 2019. IP Baru bertujuan untuk secara mendasar mendukung alamat multisemantik dengan panjang variabel di lapisan jaringan dan memungkinkan pengguna untuk menentukan dan menyesuaikan perilaku jaringan.

IP Baru mempelajari empat persyaratan fungsional dan empat persyaratan kinerja berikut yang diusulkan oleh empat skenario target jaringan 5.0 di masa mendatang, termasuk infrastruktur TIK, Internet industri, operator seluler, dan komunikasi holografik. Keempat

persyaratan fungsional tersebut terutama mencakup keamanan endogen, pemrograman jaringan dan kinerja yang dapat diprediksi, persepsi dan kontrol berdasarkan koneksi besar, dan dukungan mobilitas di mana-mana.

Mekanisme keamanan tradisional terutama melindungi sistem dari kerentanan dan ancaman yang diketahui. Berbeda dari mekanisme tersebut, tujuan mekanisme keamanan endogen adalah untuk membangun satu set lengkap arsitektur keamanan endogen untuk jaringan masa depan. Sistem tersebut tidak hanya harus menjamin kepercayaan entitas komunikasi dan infrastruktur jaringan, tetapi juga menjamin keaslian, kesesuaian, privasi, integritas, dan kerahasiaan komunikasi ujung ke ujung, serta menyediakan ketersediaan tertentu jika terjadi kegagalan jaringan dan serangan.

Aplikasi yang berbeda memiliki persyaratan yang berbeda untuk kualitas transmisi jaringan. Menurut karakteristik dan persyaratan aplikasi yang berbeda, jaringan masa depan harus menyediakan aturan akses dan transmisi yang terencana, dapat diprediksi, dapat disesuaikan, dan dibedakan berdasarkan perilaku jaringan yang deterministik. Dengan cara ini, kualitas layanan kepastian dan diferensiasi terjamin.

Persepsi dan kendali di luar koneksi besar mengacu pada pertimbangan keseluruhan koneksi jaringan, penyimpanan, dan sumber daya komputasi di bawah premis pertumbuhan eksplosif jumlah tautan komunikasi yang disebabkan oleh peningkatan skala dan kompleksitas entitas komunikasi. Di era IoT, kelas bisnis menjadi kompleks dan beragam yang mengarah pada persyaratan mobilitas. Dukungan mobilitas juga diperlukan untuk beberapa layanan koneksi besar, sehingga jaringan masa depan akan memerlukan skema komunikasi seluler berbasis koneksi besar yang efisien, berkecepatan tinggi.

Persyaratan dari keempat kinerja tersebut terutama diukur dari segi lebar pita, penundaan dan jitter, serta tingkat kehilangan paket. Berdasarkan pewarisan kemampuan IP yang ada, para peneliti New IP telah mengusulkan banyak teknologi prospektif untuk kebutuhan masa depan. New IP bertujuan untuk menyediakan teknologi dan protokol jaringan deterministik dengan penundaan rendah, keamanan dan privasi, koneksi segala hal untuk Internet industri, yang terutama didasarkan pada komunikasi mesin cerdas masa depan. New IP mendorong evolusi berkelanjutan protokol jaringan, dan mendukung persyaratan teknis 6G dan bisnis masa depan lainnya. Saat ini, poin penelitian utama New IP tercantum sebagai berikut:

(1) Panjang alamat New IP fleksibel dan bervariasi, yang menyediakan skema perutean dan pengalamatan yang beragam. Dengan cara ini, masalah yang disebabkan oleh alamat dengan panjang tetap dan mode perutean topologi tunggal dalam jaringan IP tradisional dapat diatasi. Solusi perutean yang fleksibel ini memenuhi konsumsi rendah perangkat IoT melalui pengalamatan alamat pendek, beradaptasi dengan sifat jaringan satelit yang sangat dinamis melalui perutean geografis, dan mencapai layanan yang dioptimalkan dalam skenario komputasi tepi melalui skema perutean berbasis layanan. Skema pengalamatan yang fleksibel dan beragam memungkinkan New IP untuk diterapkan pada berbagai skenario dunia maya yang heterogen, untuk mewujudkan interkoneksi semua hal di Internet.

(2) Berdasarkan penggunaan kembali jaringan IP tradisional, New IP mencoba menambahkan mode penerusan deterministik di luar mode layanan "upaya terbaik" saat ini. Kemampuan layanan deterministik menyeluruh disediakan pada lapisan jaringan untuk memastikan latensi dan jitter rendah yang deterministik untuk aliran lalu lintas tertentu. Melalui mode ini, banyak aplikasi masa depan dengan persyaratan ketat untuk jaminan kualitas layanan jaringan akan terpenuhi, seperti manufaktur cerdas, telemedicine, mengemudi otomatis, dan sebagainya.

(3) Tujuh Prinsip Desain jaringan IP yang asli tidak mencakup faktor keamanan. Jaringan IP saat ini rentan terhadap pemalsuan alamat, paparan privasi, serangan DDoS, dan ancaman keamanan lainnya. Berdasarkan model keamanan STRIDE (mewakili enam ancaman keamanan termasuk Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, dan Elevation of Privilege), New IP menganalisis dan mempelajari arsitektur jaringan untuk membangun mekanisme keamanan endogen, yang dapat memastikan privasi pengguna. Melalui pembangunan fondasi kepercayaan terdistribusi yang solid, permintaan untuk perlindungan privasi yang diwakili oleh GDPR (*General Data Protection Regulation*) dan permintaan untuk keamanan dan kepercayaan interkoneksi industri dapat dipenuhi.

(4) Untuk mengatasi masalah protokol transportasi saat ini seperti utilisasi lebar pita yang tidak memadai, ketidakmampuan untuk memahami persyaratan aplikasi dan status jaringan, dan sebagainya, New IP mengusulkan arsitektur lapisan transportasi baru yang dikombinasikan dengan transmisi multisaluran bersamaan, pengodean jaringan, dan mekanisme kolaborasi lintas lapisan. Untuk aplikasi masa depan seperti komunikasi holografik dan kesadaran penuh serta pemrosesan video AI, New IP dapat mewujudkan fluks yang sangat tinggi, semburan data yang sangat besar, dan transmisi layanan yang dibedakan dari arus bisnis.

(5) New IP mengeksplorasi arsitektur jaringan yang dapat ditentukan pengguna. Dengan membawa instruksi dan informasi metadata dalam pesan, pengguna dapat mengekspresikan persyaratan bisnis yang lebih rinci dan beragam ke jaringan, seperti transmisi kualitatif dan sinkronisasi antara beberapa arus bisnis. Berbeda dari jaringan IP tradisional yang hanya dapat memenuhi kebutuhan pengguna akan pengalamatan topologi, New IP dapat menyesuaikan paket data sesuai dengan instruksi yang dapat ditentukan pengguna untuk mendukung skenario bisnis yang lebih kompleks di masa mendatang. Meskipun IP Baru memenuhi kebutuhan alamat multi-semantik dengan panjang variabel di lapisan jaringan dan menyediakan jaringan yang disesuaikan pengguna sebagai arsitektur baru, ada banyak kritik dalam industri karena masalah keamanan privasi, akses gratis, dan masalah lainnya.

3.3 ARSITEKTUR JARINGAN KEDAULATAN

3.3.1 Kerangka Kerja

Dengan latar belakang dan persyaratan fungsional di atas, arsitektur MIN (Multi-Identifier Network) yang dirancang sendiri diadopsi sebagai arsitektur utama jaringan

kedaulatan. Dalam buku ini, kami menggunakan sistem siaran televisi sebagai kasus aplikasi untuk memperkenalkan proses operasional jaringan kedaulatan.

Ada dua kekurangan utama dari arsitektur IP yang ada:

(1) Ada risiko sentralisasi karena alamat IP dan Nama Domain dialokasikan dan dikelola oleh satu lembaga.
(2) Beban semantik alamat IP mengurangi skalabilitas dan mobilitasnya, yang selanjutnya menghambat keamanan sistem. Komunitas global membutuhkan bentuk baru jaringan yang saling mengatur.

Untuk mengatasi dua kekurangan utama jaringan tradisional, kami mengusulkan jaringan kedaulatan berdasarkan arsitektur Multi-Identifier Network (MIN). MIN mendesentralisasikan pengelolaan pengenal pasca-IP dengan menggunakan blockchain konsorsium dengan registrasi identitas asli. Selain itu, MIN adalah arsitektur jaringan revolusioner yang mendukung koeksistensi beberapa Pengenal Jaringan, termasuk identitas, konten, layanan, informasi geografis, dan alamat IP, dll.

Pada saat yang sama, MIN mendukung kompatibilitas yang menyiratkan bahwa MIN dapat digunakan langsung melalui jaringan IP yang ada dan secara bertahap akan menggantikan jaringan IP dengan mengganti lalu lintas IP secara alami dengan lalu lintas pengenal lainnya. Pengenal utama dalam MIN adalah identitas. Setiap sumber daya harus terikat pada identitas saat diunggah atau dipublikasikan. Jaringan kedaulatan menggunakan Sistem Pengenal Multi-Pengenal (MIS) sebagai bidang manajemennya. MIS mengelola pengguna dan identitas dalam domainnya dan menyeimbangkan perlindungan privasi individu dan manajemen operator dengan kriptografi. MIS memiliki hierarki dari atas ke bawah: domain teratas diimplementasikan oleh negara-negara melalui blockchain konsorsium untuk mencapai tata kelola bersama MIN. Setiap domain bawahan dikelola oleh negara atau organisasi terkait untuk memastikan keamanan dan fleksibilitas sistemik dengan cara yang tidak terlalu bergantung, serta kekhususan dan kustomisasi di antara berbagai domain. *Multi-Identifier Router* (MIR) adalah peralatan inti MIN, yang menyediakan layanan intertranslasi dan routing identifier.

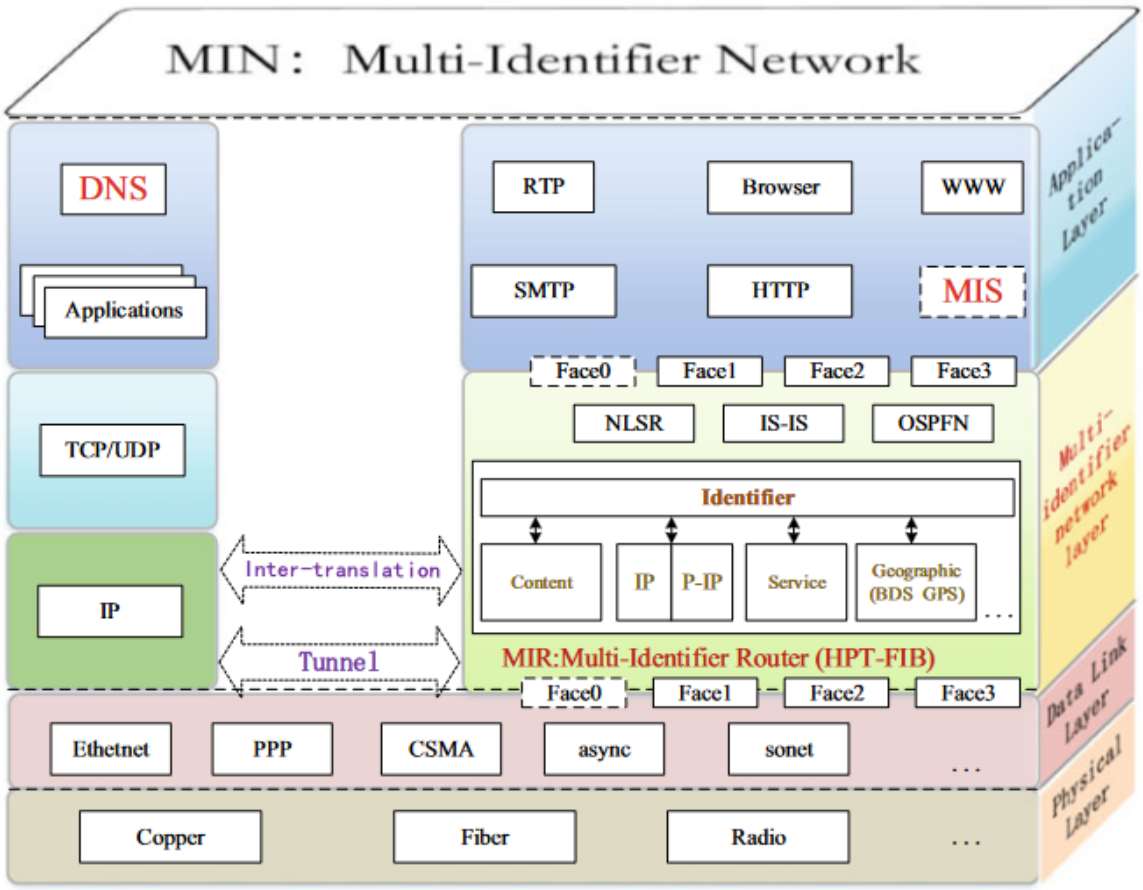
Dalam jaringan MIN, fungsi dari simpul lengkap adalah untuk berpartisipasi dalam manajemen pengguna dalam domain dan registrasi identifier pada blockchain, serta menyediakan layanan seperti transformasi identifier dan pengalamatan identifier; simpul tersebut disebut multi-identifier router. Selain itu, terdapat simpul regulasi, pengguna individu, dan pengguna perusahaan dalam jaringan. Simpul pengawas disiapkan di setiap domain sebagai antarmuka untuk akses data antara domain atas dan bawah. Simpul pengawas bertanggung jawab atas multi-identifier, seperti identitas, konten, layanan, informasi geografis, dan alamat IP.

Kami menggambarkan jaringan MIN dengan arsitektur empat lapis yang ditunjukkan pada Gambar 3.1, dan pekerjaan kami difokuskan pada lapisan aplikasi MIS dan lapisan multi-pengenal MIR. Fungsi MIS bertanggung jawab atas pembuatan dan pengelolaan beberapa pengidentifikasi. Pengidentifikasi dikirim ke simpul pengawas. Setelah verifikasi dan konsensus dicapai oleh Algoritma Konsensus, informasi atribusi dan informasi operasinya akan

dicatat pada blockchain. Teknologi blockchain menjadikan konten seluruh jaringan terpadu dan dapat dilacak, dan mencegah konten dimodifikasi secara ilegal. Lapisan aplikasi terutama dikelola oleh MIS, yang membagi seluruh jaringan menjadi jaringan domain hierarkis dari atas ke bawah. Perannya dalam MIN mirip dengan DNS dalam jaringan IP, tetapi fungsi DNS hanyalah sebagian kecil dari MIS.

Setiap simpul MIS menyimpan basis data pengidentifikasi lengkap untuk domainnya. Lapisan multi-pengenal menyediakan layanan resolusi untuk pengidentifikasi, dan juga bertanggung jawab atas penerusan dan penyaringan paket. Lapisan ini mendukung transmisi terowongan (IP-MIN-IP, MIN-IP-MIN) dan akses bersama (IP-MIN, MIN-IP) antara berbagai skenario pengidentifikasi. Setiap MIR memelihara pustaka pengidentifikasi yang baru-baru ini digunakan. Selain itu, ada beberapa teknologi yang diusulkan oleh penulis untuk meningkatkan kinerja, seperti algoritma HPT-FIB yang meningkatkan efisiensi penerjemahan dan pengalamatan multi-pengenal, model Hyperbolic Routing yang mendukung pengalamatan dalam jaringan skala besar, dan skema Transmission Control yang menjamin layanan berkualitas tinggi.

Salah satu perbedaan antara jaringan kedaulatan dan jaringan IP adalah mekanisme keamanan MIN. Pengguna mendaftar dengan informasi identitas pribadi mereka, seperti kartu identitas, nomor telepon seluler, sidik jari. Informasi pendaftaran pengguna akan disimpan dalam node blockchain untuk manajemen pengguna selanjutnya. Pengguna baru harus mendaftar dengan identitas asli mereka untuk mengakses jaringan kedaulatan. Kemudian mereka dapat secara aktif menerbitkan konten di jaringan kedaulatan. Namun, sistem blockchain akan merekam log perilaku untuk setiap pengguna. Selain itu, ada serangkaian mekanisme keamanan di jaringan kedaulatan, seperti mekanisme pengambilan konten oleh blockchain, mekanisme autentikasi identitas berdasarkan kriptografi, router multi-pengenal dengan prosedur audit konten, pertahanan tiruan dunia maya (CMD), dan sistem penyimpanan terdistribusi dengan keamanan endogen untuk menjamin keamanan pencadangan data. Keamanan MIN dianalisis di bagian ketiga bab berikutnya.



Gambar 3.1 Arsitektur jaringan kedaulatan berbasis MIN

Berdasarkan arsitektur di atas, kami mengusulkan jaringan kedaulatan multilateral yang saling mengatur. Sebagai arsitektur jaringan masa depan, MIN dianugerahi sebagai Prestasi Ilmiah dan Teknologi Internet Terkemuka Dunia dari Konferensi Internet Dunia ke-6 di Wuzhen, Tiongkok, pada tahun 2019. Arsitektur yang diusulkan telah diimplementasikan di jaringan operator untuk menguji fungsi manajemen multi-pengenal dan fungsi VoD dari transmisi jaringan. Melalui prototipe dan eksperimen di atas, kompatibilitasnya dengan jaringan IP dan penerapan progresif telah diverifikasi.

3.3.2 Sistem Multi-pengidentifikasi

MIS membagi seluruh jaringan ke dalam domain hierarkis dari atas ke bawah. Node dalam domain tingkat atas milik organisasi negara-negara besar yang bersama-sama mengelola konsorsium blockchain. Organisasi regional masing-masing mengatur domain lainnya. Di antara mereka, mode pendaftaran dan pengelolaan pengidentifikasi dan detail implementasi spesifik dapat bervariasi. Penggabungan rendah ini menjamin keamanan jaringan dan memungkinkan kustomisasi setiap domain. Subsistem MIS mewujudkan penyimpanan dan tata kelola bersama informasi pengguna dan identifikasi melalui teknologi blockchain. Modul utama MIS tercantum sebagai berikut:

(1) Modul pendaftaran pengguna. Setelah menerima permintaan pendaftaran pengguna dari klien, permintaan tersebut dipilih oleh beberapa node konsorsium. Jika konsensus

diverifikasi, setiap node blockchain akan menyimpan informasi pendaftaran pengguna dalam basis data lokal dan menyimpan informasi pengguna terdaftar dalam tabel informasi pengguna.

(2) Modul kueri pengguna. Setelah menerima permintaan kueri dari klien, modul ini akan mengkueri informasi pengguna dari tabel informasi pengguna dan mengembalikannya ke klien.

(3) Modul pembuatan pengidentifikasi. Setelah menerima permintaan penerbitan konten dari klien, permintaan tersebut dipilih oleh beberapa simpul konsorsium. Jika konsensus berhasil, setiap simpul blockchain menyimpan identitas jaringan dan alamat sebenarnya di basis data lokal dan mengirimkannya ke tabel informasi terjemahan bersama.

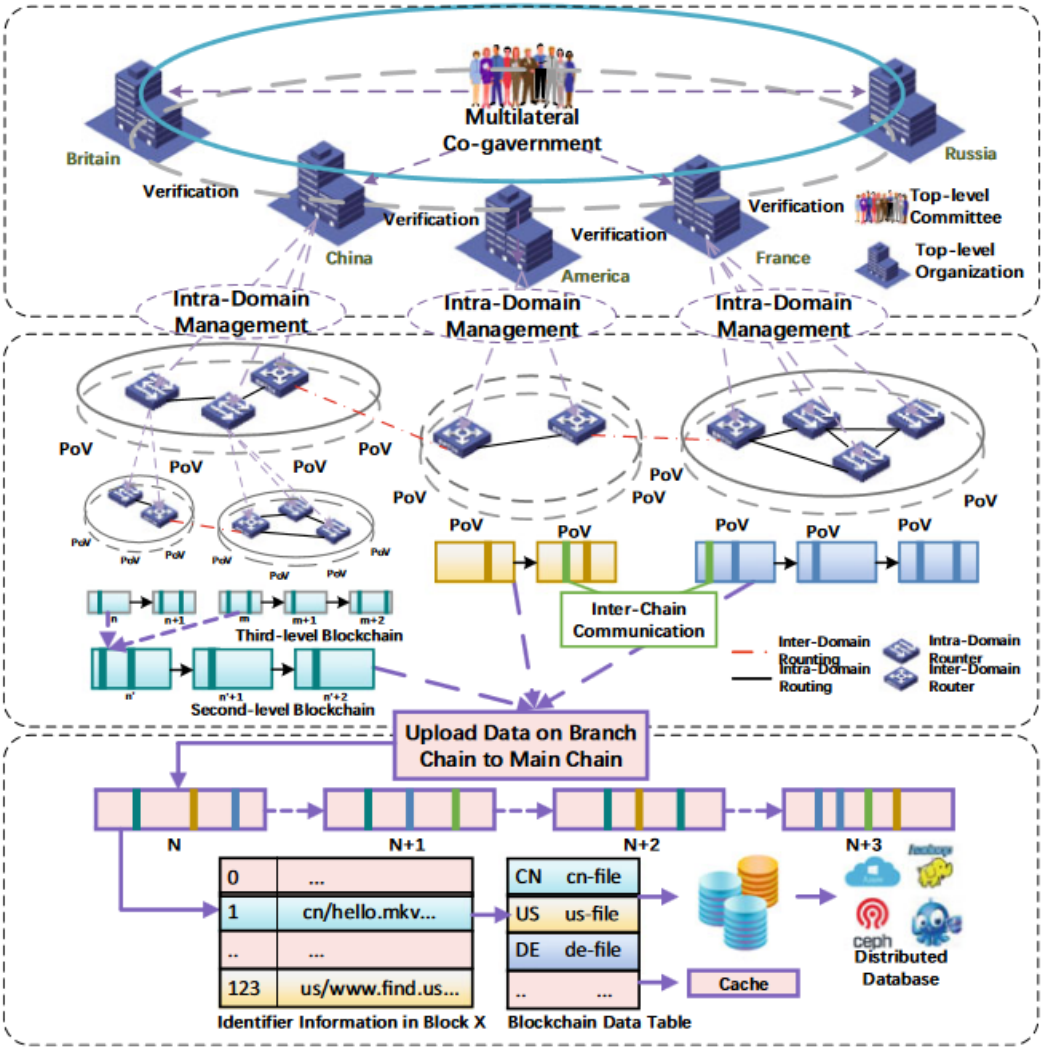
(4) Modul kueri pengidentifikasi. Setelah menerima permintaan kueri pengidentifikasi klien, modul ini mengkueri alamat sebenarnya pengidentifikasi jaringan yang sesuai dari tabel HPT-FIB dan mengembalikannya ke klien.

Proses pendaftaran adalah sebagai berikut:

- **Langkah 1**: Pengguna yang memiliki sumber daya mengirimkan permintaan pendaftaran pengidentifikasi ke simpul organisasi regulasi.
- **Langkah 2**: Setelah menerima permintaan pengguna, MIR mengirimkan data pendaftaran ke domainnya yang sesuai menurut protokol perutean tertentu.
- **Langkah 3**: Node blockchain dari domain terkait meninjau kepatuhan sumber daya setelah menerima permintaan pendaftaran pengenalnya. Jika demikian, pengenal sumber daya tersebut kemudian dipilih oleh semua node blockchain di domain tersebut untuk mencapai konsensus.
- **Langkah 4**: Node blockchain kemudian mengembalikan hasil pendaftaran ke node peminta awal. Karena informasi pengenal lengkap disimpan dalam basis data off-chain dan bukan blok on-chain, semua basis data disinkronkan secara berkala di seluruh jaringan untuk memastikan konsistensi.

Proses MIR untuk menyelesaikan pengenal adalah sebagai berikut:

- **Langkah 1**: MIR menilai bahwa pengenal tersebut adalah (1) alamat IP, lalu mengajukan kueri di HPT-FIB. Jika ada, pengenal tersebut akan diselesaikan. Jika tidak, mengakses jaringan IP tradisional melalui proksi; (2) identitas, konten, dan pengenal lainnya, lalu mengajukan kueri di cache dan HPT-FIB. Jika ada, pengenal tersebut akan diselesaikan. Jika tidak, lanjutkan ke Langkah 2.
- **Langkah 2**: Jika MIR tidak dapat menemukan pengidentifikasi, lakukan kueri domain atas secara rekursif hingga memperolehnya.
- **Langkah 3**: Jika pengidentifikasi tidak ditemukan di domain tingkat atas, lakukan kueri domain bawah sesuai dengan informasi yang dibawa oleh pengidentifikasi hingga domain terendah. Jika ada, MIR akan mengembalikan hasil yang telah diselesaikan. Jika tidak, kembalikan pesan kesalahan.



Gambar 3.2 Kerangka Kerja MIS

Dalam MIN, perilaku pengguna dalam menerbitkan dan mengakses dilindungi dan dikelola oleh MIS, dan blockchain tidak dapat disangkal mencatat tindakan ilegal. Hanya konten yang disetujui yang boleh dipublikasikan. Pada saat yang sama, pengenal yang berbeda dapat didefinisikan oleh sub-jaringan kedaulatan yang berbeda. Aplikasi visa elektronik untuk penerjemahan antara pengenal dan komunikasi konten antara jaringan kedaulatan yang berbeda dari berbagai negara diselesaikan oleh blockchain. MIS secara kredibel mencatat riwayat transaksi yang dapat dilacak dan ditanyakan. Dengan demikian, MIS memastikan bahwa informasi dan perilaku pengguna tidak dapat dirusak dan tidak dapat disangkal. Oleh karena itu, MIN akan membuat dunia maya dalam keadaan tertib dan aman, yang akan mengarahkan lalu lintas ke jaringan multi-pengenal pasca-IP yang terikat dengan identitas pengguna. Kerangka kerja MIS ditunjukkan pada Gambar 3.2.

3.3.3 Router Multi-identifier

Data plane terutama terdiri dari sakelar dan MIR. Sebagai peralatan inti dari data plane, MIR terutama digunakan untuk intertranslasi identifier, perutean dan pengalamatan, penyaringan konten, perlindungan data, dan fungsi lainnya. Agar sesuai dengan berbagai

skenario, MIR mendukung beberapa identifier jaringan dan beberapa mode transmisi secara bersamaan. Beberapa identifier mencakup identitas, konten, layanan, informasi geografis, alamat IP, dan varian lainnya. Berbagai mode transmisi mencakup mode "push" yang diwakili oleh arsitektur jaringan IP dan mode "pulling" yang diwakili oleh arsitektur Content Centric Network (CCN).

Karena skala besar jaringan IP yang ada, jaringan tersebut tidak dapat digantikan oleh arsitektur jaringan baru dalam satu hari. Banyak protokol jaringan di atas lapisan jaringan dalam jaringan IP tidak secara langsung kompatibel dengan arsitektur jaringan yang berpusat pada konten. Pertama, TCP adalah protokol ujung ke ujung yang berkomunikasi melalui alamat IP dan nomor port, yang bertentangan dengan filosofi berbasis konten CCN. Kedua, dalam CCN, komunikasi adalah proses yang diprakarsai pengguna untuk "menarik" data yang diperlukan. Namun, dalam TCP, ini adalah proses "push" di mana pengirim mengirim data, dan penerima membalas pesan pengakuan. Keduanya secara fundamental berbeda dalam semantik. Ketiga, TCP memastikan transmisi ujung ke ujung yang andal, yang tidak ditangani oleh CCN.

Untuk mewujudkan penyebaran progresif, TCP dan CCN perlu berkomunikasi secara timbal balik dalam MIN. Skema MIR dibagi menjadi dua bagian, termasuk skema kompatibilitas jaringan IP dan pengembangan arsitektur jaringan baru. Skenario transmisi yang komprehensif harus dipertimbangkan, termasuk IP-MIN-IP, MIN-IP-MIN, IP-MIN dan MIN-IP.

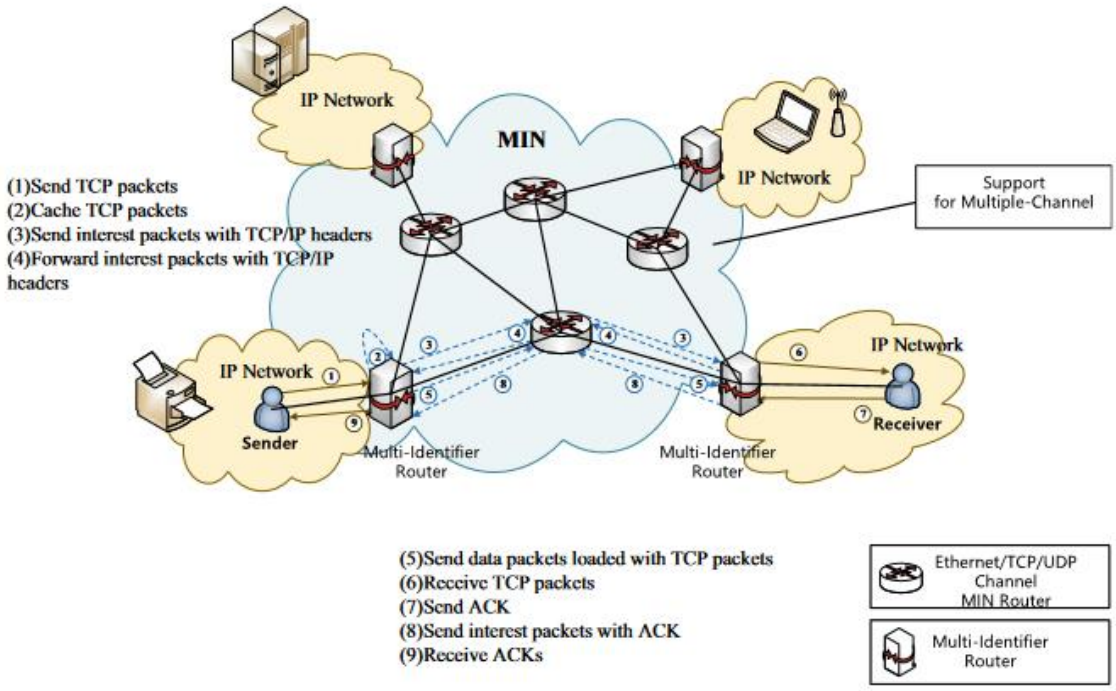
(1) **Terowongan antara IP-MIN-IP:** Modul ini meniru ide penggunaan IPv4 sebagai terowongan untuk mengirimkan paket IPv6 guna mewujudkan terowongan jaringan MIN. Terowongan ini memungkinkan jaringan MIN untuk mengirimkan paket IP, yang menyediakan kompromi untuk penyebaran jaringan kedaulatan secara progresif yang proses transmisinya mirip dengan jaringan MIN. Arsitektur modul ini ditunjukkan pada Gambar 3.3. Modul agen terowongan disebarkan pada beberapa simpul agen, yang masing-masing merupakan simpul IP dan simpul MIN. Satu sisi simpul agen adalah jaringan IP, dan sisi lainnya adalah jaringan MIN. Domain jaringan IP dalam setiap pengujian diisolasi satu sama lain. Komunikasi di antara mereka sepenuhnya bergantung pada paket yang diteruskan oleh setiap simpul agen satu sama lain. Untuk simpul dalam jaringan IP, terowongan bersifat transparan. Mode komunikasi simpul IP antara domain yang berbeda sama dengan mode komunikasi IP tradisional. Modul terowongan ini hanya bertanggung jawab untuk mengangkut paket dari satu domain ke domain lainnya.

(2) **Terowongan antara MIN-IP-MIN:** Karena jaringan IP mengadopsi arsitektur "push" dua arah, modul ini dapat langsung menggunakan fungsi pengiriman paket MIN dengan paket TCP sebagai contoh. Prinsipnya ditunjukkan pada Gambar 3.4.

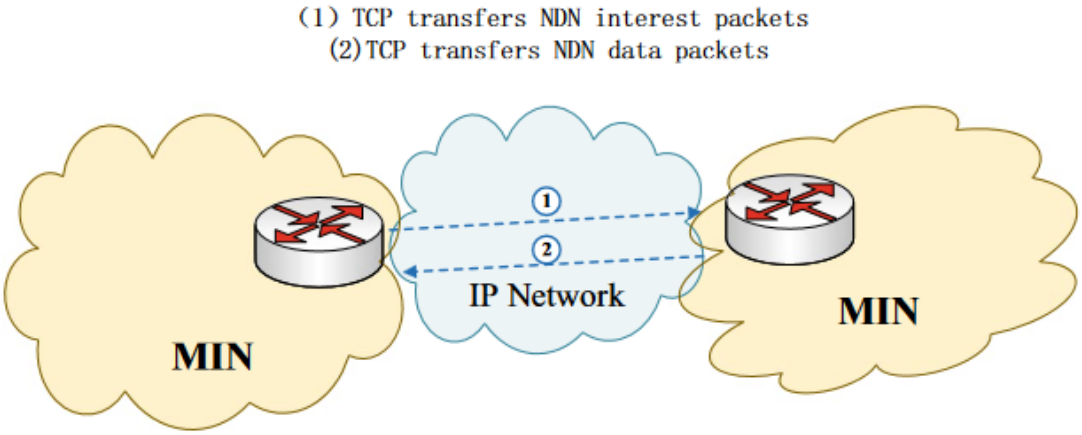
(3) **Terowongan antara IP-MIN:** Komunikasi IP-MIN berarti proses transmisi di mana host yang mengirim permintaan berada di jaringan IP dan data yang diminta berada di MIN. Arsitekturnya ditunjukkan pada Gambar 3.5. Modul dipasang pada MIR di persimpangan MIN dan jaringan IP untuk memperoleh data dari MIN untuk semua

node IP yang dapat berkomunikasi dengannya. Modul ini berkomunikasi dengan node IP melalui protokol TCP dan menarik data dari node MIN melalui pertukaran paket minat dan paket data.

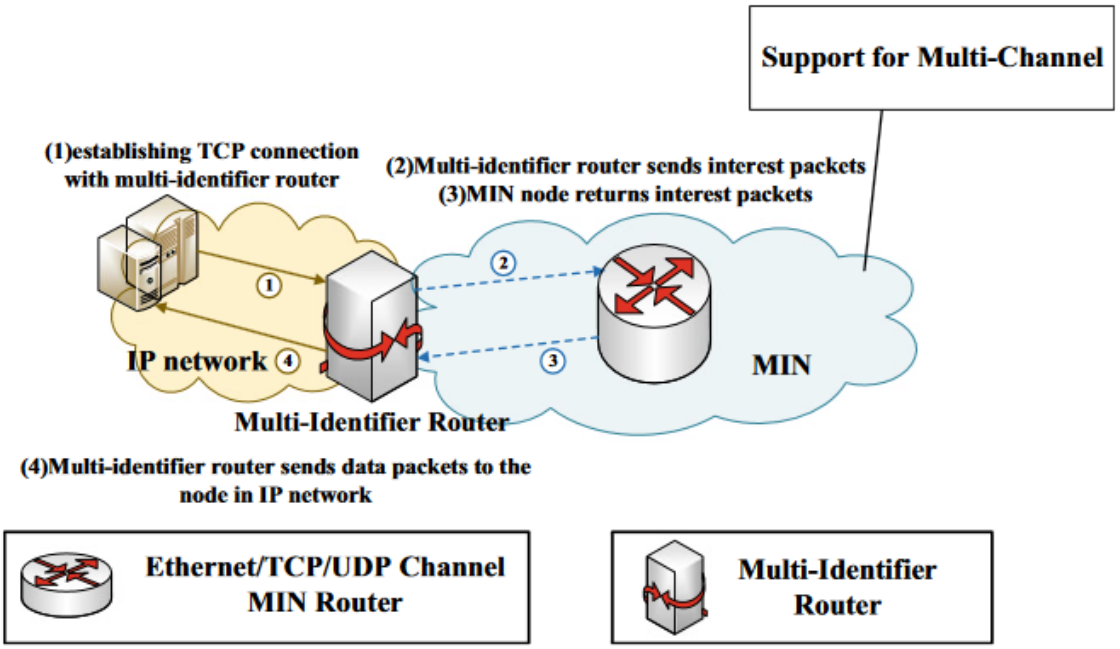
(4) **Terowongan antara MIN-IP:** Arsitekturnya ditunjukkan pada Gambar 3.6. Modul ini dipasang pada router MIR di persimpangan MIN dan jaringan IP, yang membantu node MIN di domain yang sama menarik file dari jaringan IP.



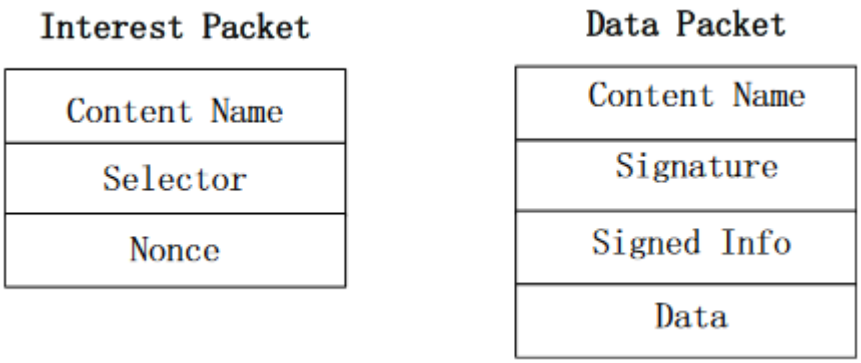
Gambar 3.3 Koneksi transmisi IP-MIN-IP



Gambar 3.4 Koneksi transmisi MIN-IP-MIN



Gambar 3.6 Koneksi transmisi MIN-IP



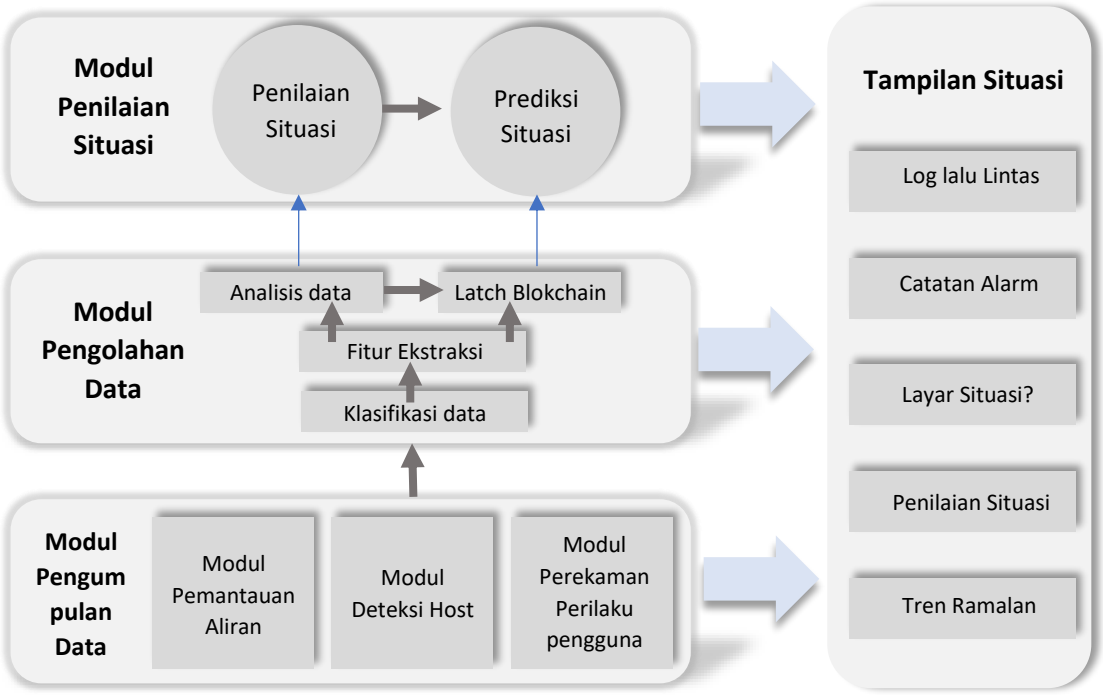
Gambar 3.7 Jenis paket

Transmisi data pada lapisan bawah MIN mirip dengan Information Centric Networking (ICN). Komunikasi dalam ICN digerakkan oleh konsumen data. Ada dua jenis pengelompokan dalam ICN, yaitu paket minat dan paket data yang ditunjukkan pada Gambar 3.7. Semua transmisi data dalam jaringan MIN dilakukan melalui kedua kelompok ini.

3.3.4 Sistem Kesadaran Situasi Keamanan

Dengan meningkatnya skala dan kompleksitas jaringan, teknologi serangan terus berinovasi, dan sejumlah besar metode serangan baru muncul. Dalam beberapa tahun terakhir, berbagai insiden keamanan muncul tanpa henti. Biasanya, perusahaan perlu bereaksi hingga serangan terjadi, yang sulit dicegah sebelumnya. Karena regulator keamanan tidak dapat mengendalikan situasi keamanan perusahaan secara real time, mereka tidak dapat mengambil tindakan efektif pada tahap awal pembentukan ancaman untuk menghindari kerugian. Perangkat keamanan, seperti firewall, WAF (*Web Application Firewall*), IDS (*intrusion detection system*), dan UTM (*Unified Threat Management*), diterapkan secara

independen di perusahaan, pemerintah, dan lembaga keuangan. Jadi, mereka menangani insiden keamanan secara independen berdasarkan kemampuan perangkat mereka. Saat ini, banyak serangan atau penetrasi keamanan yang digabungkan atau mensimulasikan perilaku akses normal, seperti CC (*Challenge Collapsar*), serangan APT (*Advanced Persistent Threat*), dll. Ancaman serangan semacam ini tidak dapat dilindungi atau diidentifikasi oleh satu sistem, sehingga perlu dilindungi secara terpadu melalui asosiasi dan analisis multi-sistem. Oleh karena itu, status keamanan seluruh jaringan dan trennya harus menjadi perhatian oleh personel keamanan jaringan.



Gambar 3.8 Arsitektur sistem kesadaran situasi keamanan

Selain arsitektur keamanan endogen dari jaringan kedaulatan, sistem kesadaran situasional keamanan MIN yang dikombinasikan dengan blockchain telah dirancang dan diselesaikan untuk lebih memastikan keamanan dan kontrol jaringan. Status jaringan dipantau secara real time oleh sistem yang diusulkan, yang diterapkan pada router batas MIN. Sistem yang diusulkan merasakan ancaman keamanan yang ada di semua level server secara real time. Secara khusus, pembelajaran mesin tingkat lanjut, pembelajaran mendalam, dan model komputasi berkinerja tinggi digabungkan untuk meningkatkan efisiensi dan akurasi analisis. Di sisi lain, teknologi rantai blok digabungkan untuk mengunci dan menemukan lokasi kejadian secara akurat. Sistem ini dapat membantu analis jaringan menilai profil risiko dan memprediksi tren masa depan (Gambar 3.8).

Sistem ini dibagi menjadi tiga lapisan, termasuk modul pengumpulan data, modul pemrosesan data, dan modul penilaian situasi. Modul pengumpulan data memantau dan mengumpulkan lalu lintas jaringan secara real-time, serta mendeteksi dan mengumpulkan data abnormal IP dan MIR melalui alat NetFlow dan dump TCP. Modul pemrosesan data

menganalisis, mengklasifikasikan, mengekstrak, dan menyimpan data yang dikumpulkan dengan Kafka dan Scapy. Selain itu, algoritma pembelajaran mendalam dan algoritma pembelajaran mesin berdasarkan klasifikasi mesin vektor tunggal digabungkan untuk meningkatkan efisiensi proses.

Untuk deteksi host, kami mengadopsi basis data fitur komprehensif untuk pengujian yang karakteristik pustakanya dapat mendeteksi 84 jenis perilaku abnormal umum untuk menangkap penyerang secara efektif. Kemudian data akan segera dianalisis dengan teknologi AI. Menurut hasilnya, lalu lintas dan peristiwa abnormal dicatat dan dilaporkan kepada administrator. Modul penilaian situasi bertanggung jawab untuk menilai dan memprediksi situasi keamanan sistem secara real time. Informasi keamanan penting akan diumpankan kembali ke administrator untuk menyesuaikan strategi pertahanan. Selain itu, semua peristiwa abnormal dikunci dalam blockchain PPoV untuk memastikan bahwa catatan peristiwa ancaman keamanan tidak dirusak, dan lintasan perilaku penyerang tidak dapat dihapus, yang memastikan integritas log keamanan sistem dan selanjutnya meningkatkan keamanan sistem itu sendiri.

Sistem kesadaran situasi keamanan mengintegrasikan berbagai teknologi keamanan seperti teknologi pemrosesan paket berbasis big data, pemodelan AI, blockchain, dan Cyberspace Mimic Defense. Teknologi ini membantu para pengambil keputusan memahami situasi keamanan sistem secara real time. Sistem kesadaran situasi keamanan melacak perilaku jaringan dan mengawasi seluruh lalu lintas di domain global untuk menjamin keamanan MIN.

3.4 PROSES DALAM JARINGAN KEDAULATAN

Jaringan kedaulatan mendukung berbagai fungsi, masing-masing dijelaskan di bagian ini dengan memilih jaringan TV Siaran sebagai skenario aplikasi yang umum.

3.4.1 Proses Pendaftaran

Pengguna perlu mengautentikasi dan mendaftar dengan informasi nyata seperti nomor ID, nomor telepon seluler, dan wajah saat mereka mendaftar akun MIN. Sistem mengunggah dan menyimpan informasi pengguna di blockchain. Antarmuka pendaftaran pengguna ditunjukkan pada Gambar 3.9.

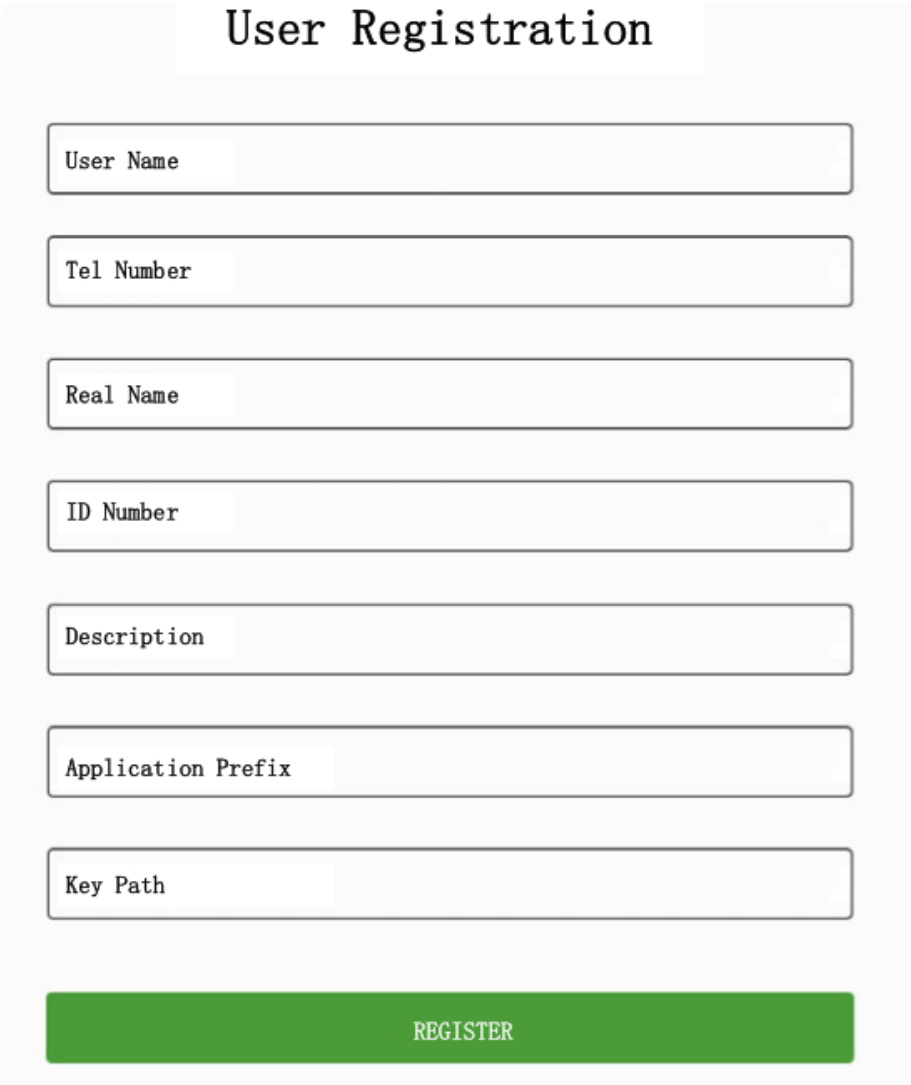
3.4.2 Menerbitkan Konten oleh Pengguna Biasa

Dalam jaringan kedaulatan, jaringan produksi dan penyiaran inti dapat menerbitkan video, audio, dan konten lainnya, pengguna yang berwenang juga dapat menerbitkan konten. Konten yang difilmkan atau diproduksi oleh pengguna yang berwenang dikirimkan ke simpul blockchain untuk pemungutan suara. Jika pemungutan suara disetujui, konten dapat dipublikasikan di jaringan kedaulatan. Proses pengguna yang berwenang untuk menerbitkan konten ditunjukkan pada Gambar 3.10.

(1) Pengguna yang berwenang masuk ke jaringan dengan sidik jari, iris, dan wajah.
(2) Setelah pengguna yang berwenang berhasil masuk ke jaringan, mereka dapat mengirim konten yang akan dipublikasikan ke simpul blockchain. Simpul blockchain dapat disebarkan pada router ID-ICN, atau dapat disebarkan sebagai server terpisah.

(3) Pemungutan suara di blockchain. Setelah pemungutan suara disahkan, pengguna yang berwenang dapat menerbitkan konten. Informasi tentang pengguna dan konten yang dipublikasikan akan disimpan di blockchain.

(4) Pengguna berhasil menerbitkan konten. Pengguna dapat menerbitkan konten dalam sistem penyimpanan terdistribusi dengan keamanan endogen atau di localhost.



Gambar 3.9 Antarmuka pendaftaran

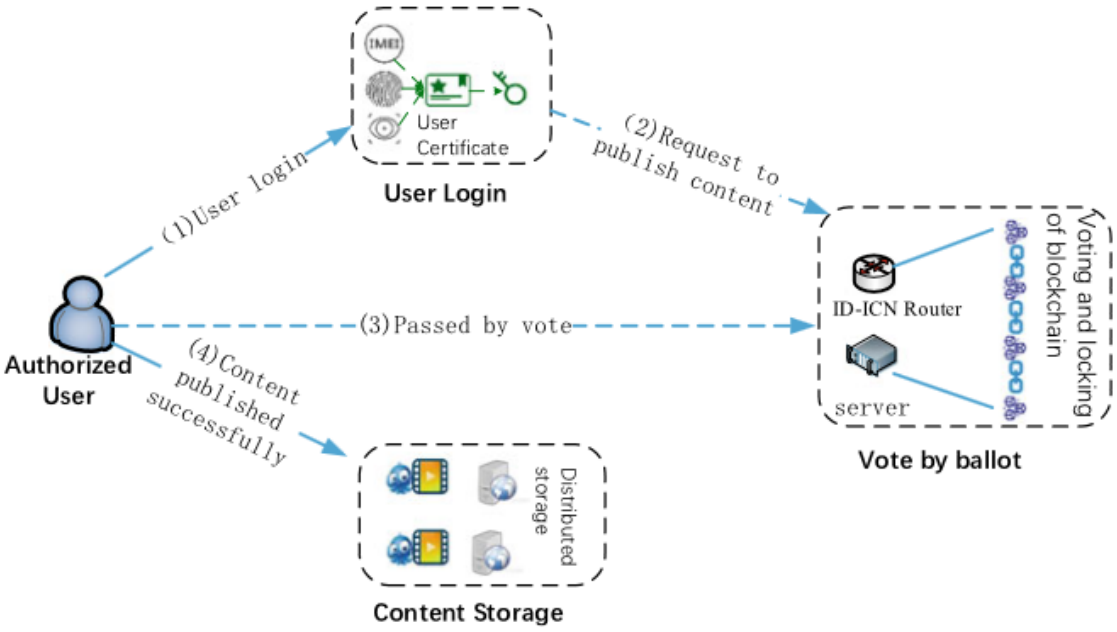
3.4.3 Penerbitan Konten oleh Staf Jaringan Penyiaran

Sumber konten utama lain yang dipublikasikan di jaringan kedaulatan adalah jaringan produksi dan penyiaran, yang ditunjukkan pada Gambar 3.11.

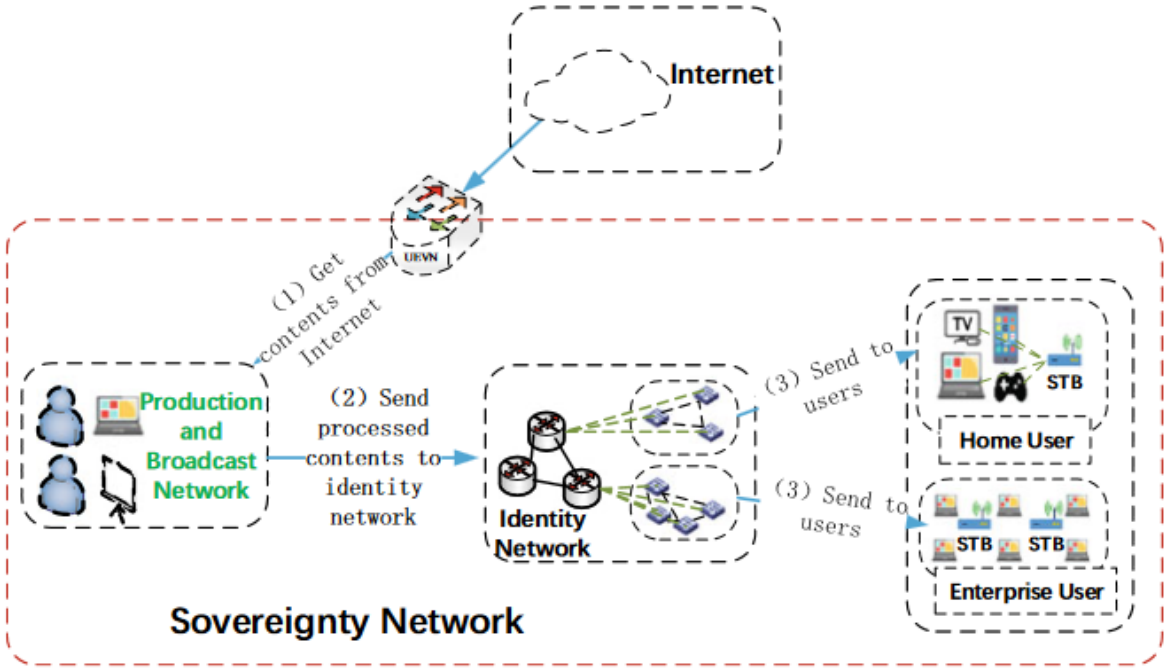
(1) Staf Jaringan Produksi dan Penyiaran memperoleh sumber konten dari Internet melalui Edge Multi-Identifier Router (EMIR) dari jaringan kedaulatan.

(2) Staf Jaringan Produksi dan Penyiaran akan memproduksi konten dan kemudian menerbitkan konten tersebut ke jaringan.

(3) Konten yang mencapai node EMIR router Edge ID-ICN dikirim ke pengguna rumahan atau bisnis.



Gambar 3.10 Pengguna biasa mempublikasikan konten



Gambar 3.11 Staf jaringan produksi dan siaran menerbitkan konten

3.4.4 Memperoleh Konten oleh Pengguna Biasa

Pengguna perusahaan dan pengguna rumahan secara kolektif disebut sebagai pengguna biasa. Proses pengguna biasa memperoleh data dapat dibagi menjadi dua klasifikasi. Yang pertama adalah penyedia data berada di jaringan IP. Ketika pengguna biasa jaringan kedaulatan memperoleh data untuk pertama kalinya, mereka perlu memperoleh data dari jaringan IP melalui EMIR. Proses transmisi data ditunjukkan pada Gambar 3.12.

(1) Pengguna biasa dalam jaringan kedaulatan masuk ke jaringan dengan sidik jari, iris, wajah, dll.
(2) Setelah pengguna biasa berhasil masuk ke jaringan, mereka dapat mengirim permintaan konten ke MIR, dan MIR mengirim permintaan ke EMIR. Atau pengguna biasa dapat langsung mengirim permintaan ke EMIR yang terhubung dengannya. Pengguna dan konten yang diminta terkait akan direkam oleh node blockchain.
(3) EMIR meninjau izin pengguna dalam permintaan konten. Metode auditnya terutama oleh dua jenis berikut. Salah satunya adalah merekam informasi pengguna dalam tanda tangan, dan EMIR memverifikasi apakah konten yang diminta oleh pengguna sesuai dengan cakupan otoritas. Pilihan lainnya adalah menambahkan domain izin ke paket minat. EMIR memverifikasi bahwa konten yang diminta oleh pengguna sesuai dengan cakupan izin berdasarkan domain izin, yang dapat mengontrol cakupan konten aksesnya menurut berbagai tingkatan. Informasi izin ditunjukkan pada Tabel 3.1. Jika konten yang diminta melebihi izin pengguna, permintaan tersebut akan dibuang. Jika masih dalam izin, maka lanjutkan ke langkah berikutnya.
(4) EMIR mengekstrak informasi konten dari permintaan konten, lalu meminta konten dari jaringan IP dengan cara tradisional.
(5) Penyedia konten menyediakan data yang diminta ke EMIR dengan cara tradisional.
(6) Data audit awal EMIR dengan teknologi penyaringan, seperti penyaringan kata kunci, klasifikasi AI, dan identifikasi.
(7) EMIR mengenkapsulasi data yang diminta dalam paket jaringan yang berpusat pada identitas, lalu mengembalikannya ke pengguna biasa sesuai dengan jalur permintaan konten.

Tabel 3.1 Tingkatan domain izin

Tingkat domain kontrol otoritas	Cakupan akses yang diizinkan	Kelompok yang sesuai
0	Semua konten Internet	Manajer, personel yang diberi wewenang oleh negara, pengguna dewasa biasa
1	Semua konten Internet kecuali kode unduhan dan perangkat lunak	Staf produksi dan penyiaran radio dan televisi
2	Teks, video, audio, gambar, halaman web, dan konten dasar harian lainnya	Personel departemen atau perusahaan tertentu, personel tertentu
3	Konten dalam rentang yang ditentukan	Pengguna di bawah umur biasa dan pengguna dengan catatan kriminal internet

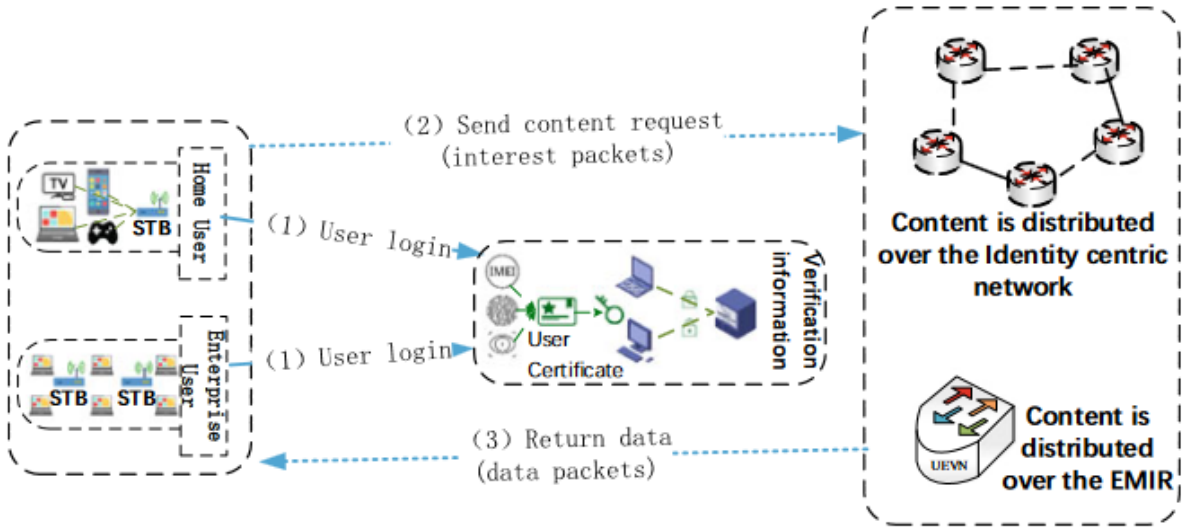
Situasi kedua dari pengguna biasa yang memperoleh data adalah bahwa penyedia konten berada dalam jaringan kedaulatan (penerbit konten adalah pengguna jaringan kedaulatan). Atau konten yang diminta telah di-cache di node jaringan kedaulatan, yaitu, pengguna sendiri atau pengguna lain telah meminta konten yang sama sebelumnya. Oleh

karena itu, data dapat langsung diperoleh dalam jaringan kedaulatan. Proses transmisi data ditunjukkan pada Gambar 3.13.

(1) Pengguna biasa dalam jaringan kedaulatan masuk menggunakan sidik jari, iris, wajah, dll.

(2) Kemudian pengguna biasa mengirim permintaan ke node jaringan atau EMIR dalam jaringan kedaulatan.

(3) Jika node jaringan kedaulatan atau EMIR telah menyimpan konten yang diminta, konten tersebut langsung dikembalikan ke pengguna. Jika tidak, data akan diminta dari data asli dan dikembalikan ke pengguna yang meminta.



Gambar 3.13 Pengguna biasa memperoleh konten dari jaringan kedaulatan

3.4.5 Memperoleh Konten oleh Staf Jaringan Penyiaran

Staf Jaringan Produksi dan Penyiaran memperoleh sumber daya dari jaringan IP untuk produksi dan penerbitan. Oleh karena itu, mereka mengakses sumber daya terutama melalui jaringan IP. Proses pemrosesan data ditunjukkan pada Gambar 3.14.

(1) Staf Jaringan Produksi dan Penyiaran masuk dengan sidik jari, iris, wajah, dll.

(2) Kemudian staf mengirimkan permintaan konten ke MIR, dan MIR mengirimkan permintaan tersebut ke EMIR. Atau staf dapat langsung mengirimkan permintaan tersebut ke EMIR yang terhubung dengannya. Staf dan konten yang diminta terkait akan direkam oleh node blockchain.

(3) EMIR memverifikasi izin staf dalam permintaan konten. Jika konten yang diminta melebihi izin staf, permintaan tersebut akan dibuang. Jika masih dalam izin, kami melanjutkan ke langkah berikutnya.

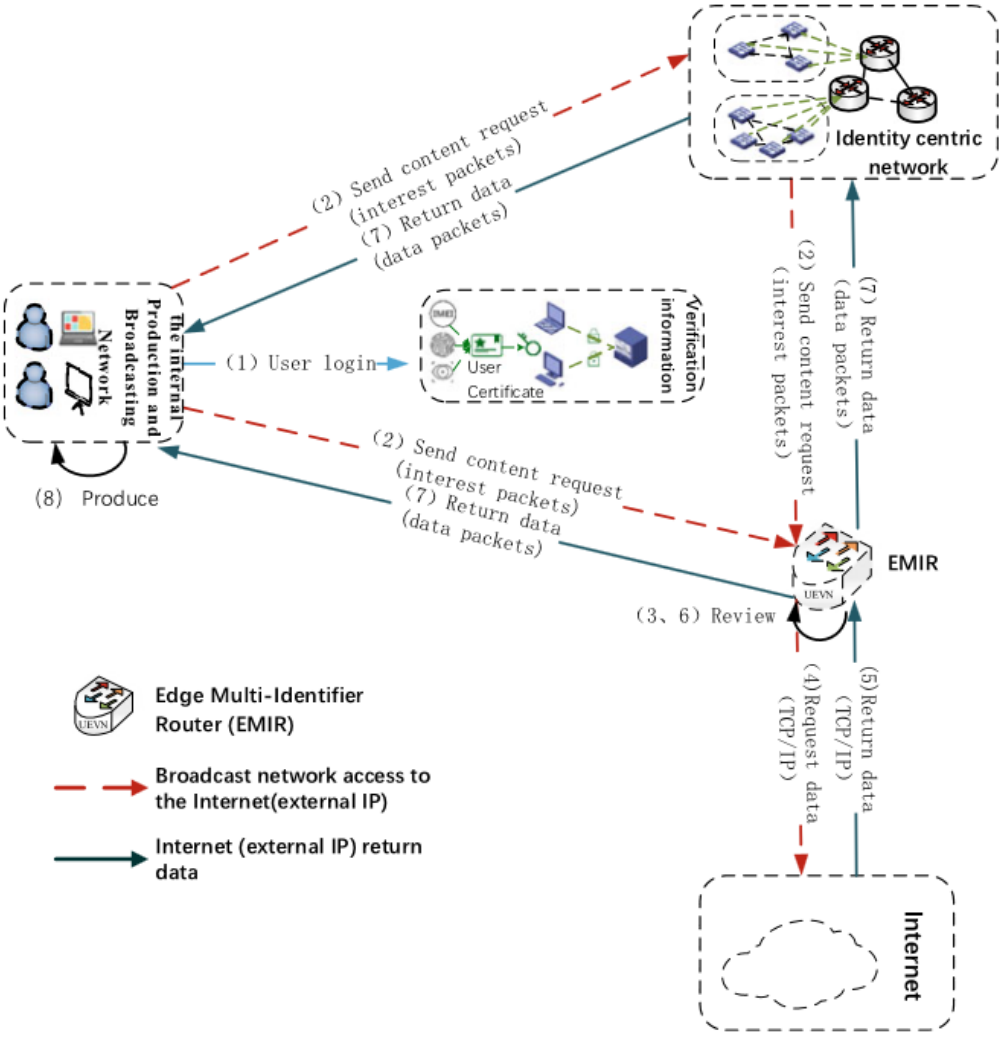
(4) EMIR mengekstrak informasi konten dari permintaan konten, lalu meminta konten dari jaringan IP dengan cara tradisional.

(5) Penyedia konten menyediakan data yang diminta ke EMIR dengan cara tradisional.

(6) Data audit awal EMIR dengan teknologi penyaringan, seperti penyaringan kata kunci, klasifikasi dan identifikasi AI.

(7) EMIR merangkum data yang diminta dalam paket data jaringan yang berpusat pada identitas, lalu mengembalikannya ke staf sesuai dengan jalur permintaan konten.

(8) Staf Jaringan Produksi dan Penyiaran memproduksi dan menerbitkan konten sesuai dengan data yang dikembalikan.



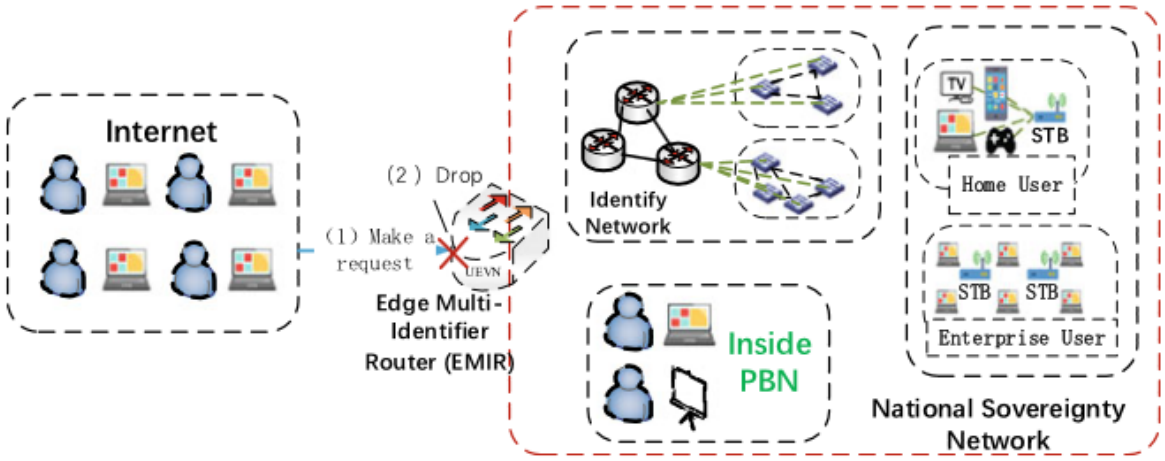
Gambar 3.14 Staf jaringan produksi dan penyiaran memperoleh konten

3.4.6 Penilaian Data Kedaulatan oleh Pengguna Ekstranet

Pengguna dalam jaringan kedaulatan dapat mengakses data dalam jaringan IP, dan pengguna atau penyerang dalam jaringan IP juga dapat mengakses jaringan kedaulatan. Namun, untuk menjamin keamanan jaringan kedaulatan, EMIR secara ketat memeriksa permintaan aktif dari jaringan IP eksternal. Prosesnya ditunjukkan pada Gambar 3.15.

(1) Pengguna IP mengirim permintaan ke EMIR.

(2) EMIR meninjau paket permintaan.



Gambar 3.15 EMIR memeriksa permintaan aktif dari jaringan eksternal

3.4.7 Algoritma Tanda Tangan di MIN

Ketika data ditransmisikan di MIN berdasarkan Identity Centric Network (ICN), setiap paket data akan ditandatangani dan didekripsi, yang ditunjukkan pada Gambar 3.16.

(1) Ketika menerbitkan paket ICN, penerbit konten menggunakan beberapa fungsi hash untuk menghitung nilai hash dari paket tersebut.

(2) Algoritma tanda tangan tertentu digunakan untuk menandatangani nilai hash dengan kunci privat milik pengguna (yaitu, kunci privat digunakan untuk mengenkripsi nilai hash secara asimetris). Tanda tangan dapat ditambahkan ke akhir paket atau ditempatkan di antara nama konten dan blok data.

(3) Penerbit konten mengirimkan tanda tangan dan paket bersama-sama ke peminta konten.

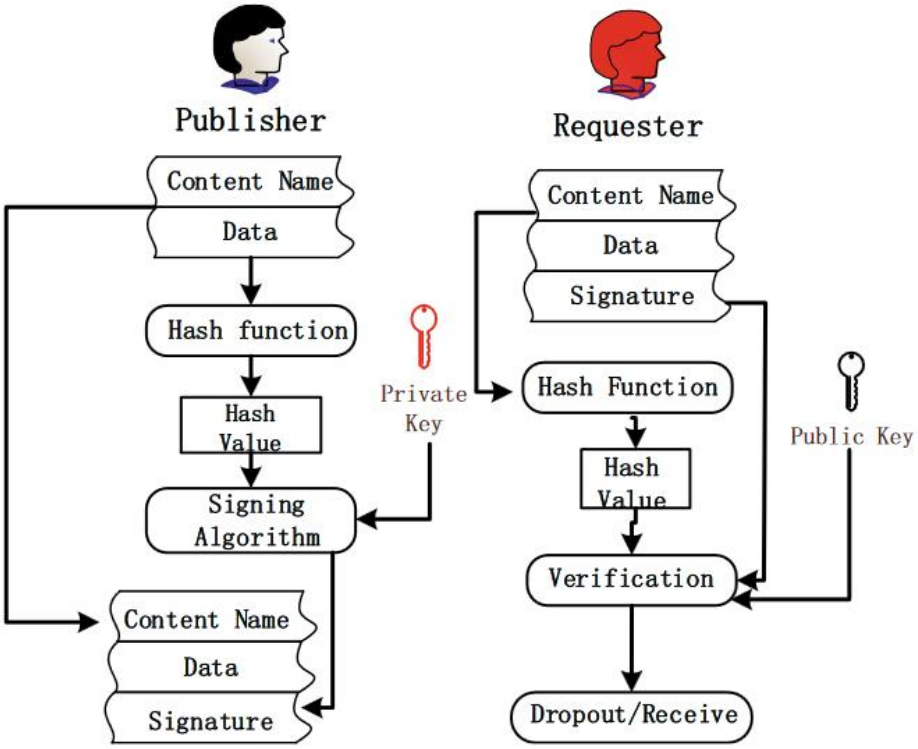
(4) Kemudian peminta memisahkan tanda tangan data dari paket. Paket tersebut digunakan untuk menghitung hash-nya menggunakan algoritma hash yang sama dengan penerbit konten.

(5) Kunci publik, nilai hash, dan tanda tangan penerbit konten digunakan untuk memverifikasi integritas data dan keandalan tanda tangan. Jika validasi lolos, paket diterima; jika tidak, paket dibuang.

3.5 MENILAI KEAMANAN JARINGAN KEDAULATAN

3.5.1 Analisis Anti-serangan

Salah satu penggunaan utama jaringan kedaulatan adalah untuk membangun jaringan yang aman dan privat. Cara memastikan keamanan jaringan privat kernel merupakan isu penting yang perlu dipertimbangkan dalam pembangunan jaringan kedaulatan. Jaringan kedaulatan berbasis teknologi blockchain akan menjamin keamanan dan keandalan dari tiga aspek: jaringan yang berpusat pada identitas, mekanisme penyaringan audit, dan mekanisme keamanan endogen.



Gambar 3.16 Proses penandatanganan dan dekripsi

1. Jaringan Berpusat pada Identitas

Pertama, jaringan kedaulatan adalah jaringan yang berpusat pada identitas dan tidak bergantung pada sistem IP. Semua serangan terhadap IP yang dibangun dengan menggunakan cacat keamanan IP tidak valid dalam jaringan kedaulatan. Kedua, kunci publik digunakan untuk menandatangani setiap paket. Ketiga, karena jaringan yang berpusat pada identitas digerakkan oleh konsumen data, hanya konten yang telah diminta yang dapat dikirim ke konsumen, dan produsen konten tidak dapat secara aktif mengirim data. Jika jaringan eksternal ingin mengirim permintaan atau penyerang ingin mengirim data secara aktif, mereka perlu memecahkan tanda tangan konsumen. Proses pemecahan terutama untuk memecahkan algoritma kriptografi terkait. Kesulitan serangan algoritma enkripsi yang ada telah mencapai tingkat eksponensial. Misalnya, algoritma RSA yang paling umum akan memakan waktu puluhan tahun untuk berjalan pada superkomputer berkinerja tertinggi saat ini. Selain itu, informasi pengguna, informasi perilaku pengguna disimpan dalam blockchain dalam jaringan yang berpusat pada identitas. Jika terdapat masalah dengan konten yang dipublikasikan atau konten yang diminta, masalah tersebut dapat langsung diketahui oleh individu yang bersangkutan guna memastikan bahwa perilaku dan sumber daya dapat dikelola dan dikendalikan.

2. Mekanisme Penyaringan Audit

Dimulai dari EMIR, jaringan kedaulatan akan menyiapkan fungsi penyaringan seperti firewall, deteksi paket, pengenalan teks, deteksi pengenalan audio, deteksi pengenalan gambar dan video, serta pemrosesan bahasa alami di setiap MIR tempat paket akan lewat. Fungsi penyaringan ini akan menyaring data yang berbahaya. Jika penyerang ingin menyerang

jaringan inti, mereka perlu menyerang setiap MIR penyaringan pada tautan secara bergantian. Seorang penyerang berjalan di sepanjang rantai serangan dengan mengambil satu langkah ke bawah rantai setiap kali menerobos filter. Jika penyerang tertangkap oleh filter, mereka bergerak mundur satu langkah di sepanjang rantai serangan. Melalui mekanisme penyaringan berlapis-lapis, penyebaran serangan secara efektif dicegah di jaringan.

3. Mekanisme Keamanan Endogen

Peralatan inti jaringan kedaulatan dibangun dengan arsitektur Cyber Mimic Defense (CMD) yang memiliki karakteristik keamanan endogen. Di bidang pertahanan siber, mirip dengan pertahanan tiruan biologis, CMD mengubah arsitekturnya berdasarkan premis fungsi layanan dan objek target, yang meningkatkan kesulitan serangan. Arsitektur umum tersebut mengkonfigurasi ulang struktur internal, sumber daya redundan, sistem operasi, algoritma inti, dan lingkungan untuk menghindari pintu belakang atau virus Trojan yang tidak dikenal. Oleh karena itu, skenario yang masuk akal disajikan kepada penyerang, yang mengganggu konstruksi dan efektivitas rantai serangan untuk melipatgandakan biaya serangan.

3.5.2 Mekanisme Keamanan

Keamanan jaringan kedaulatan dapat dianalisis dari tiga aspek di atas, di antaranya mekanisme keamanan utama tercantum sebagai berikut.

(1) Sumber daya dalam jaringan kedaulatan hanya dapat diperoleh secara aktif oleh pengguna dalam jaringan kedaulatan. Pengguna jaringan IP tidak dapat secara aktif memaksa data ke dalam jaringan kedaulatan. Oleh karena itu penyerang tidak dapat memindai dan menyerang sistem secara terus-menerus seperti dalam jaringan IP, dan bahkan tidak dapat mengirim informasi berbahaya ke jaringan kedaulatan. Hal ini akan dijamin oleh dua mekanisme berikut:
   - Jaringan kedaulatan mengadopsi mode "tarik", yaitu penerima menarik data secara aktif.
   - Jika pengguna ingin menarik data di jaringan kedaulatan, mereka perlu masuk dengan informasi identitas asli mereka. Oleh karena itu, data berbahaya yang mengalir ke jaringan kedaulatan dapat dilacak ke pengguna tertentu sehingga terhindar dari pengenalan data berbahaya yang disengaja dari jaringan IP oleh pengguna di jaringan kedaulatan.

(2) Bagi pengguna dalam jaringan kedaulatan, blockchain akan mencatat konten yang diminta, konten yang dipublikasikan, dan pengguna terkait. Informasi yang disimpan dalam blockchain tidak dapat dirusak, sehingga konten abnormal dapat ditemukan dengan cepat dan akurat oleh individu dengan keandalan tinggi.

(3) Jaringan yang berpusat pada identitas digunakan dalam jaringan kedaulatan, dan mode transmisinya sama sekali berbeda dari jaringan IP. Oleh karena itu, lingkungan operasi akan dinonaktifkan dalam jaringan kedaulatan untuk beberapa virus dan lalu lintas berbahaya yang melewati mekanisme penyaringan untuk memasuki jaringan kedaulatan, serta metode serangan yang memanfaatkan jaringan IP untuk penghancuran. Misalnya, cacing jaringan yang dapat mereplikasi dalam jaringan IP, tidak dapat menyebar dalam jaringan yang berpusat pada identitas. Manipulasi jahat

terhadap host melalui port TCP juga akan gagal. Serangan IP tradisional dapat menyebabkan kegagalan EMIR, tetapi keamanan dan keandalan pengguna, sumber daya, dan peralatan dalam jaringan kedaulatan dapat dijamin dan dilindungi dari serangan.

(4) Ruang alamat jaringan kedaulatan sangat besar sehingga menyebabkan kompleksitas komputasi yang besar dalam menjalankan program pemindaian alamat berbahaya, yang membuat pemindaian tidak layak dilakukan.

(5) Berbagai mekanisme penyaringan digunakan pada EMIR untuk mencegah data berbahaya memasuki jaringan kedaulatan, seperti prosedur audit konten AI.

(6) Setelah konten ditransmisikan ke jaringan kedaulatan, firewall, deteksi paket, deteksi pengenalan teks, deteksi pengenalan audio, deteksi pengenalan gambar dan video, pemrosesan bahasa alami, peninjauan manual, dan mekanisme lainnya digunakan untuk menyaring konten yang ditransmisikan lapis demi lapis, untuk lebih memastikan keamanan dan keandalan jaringan inti.

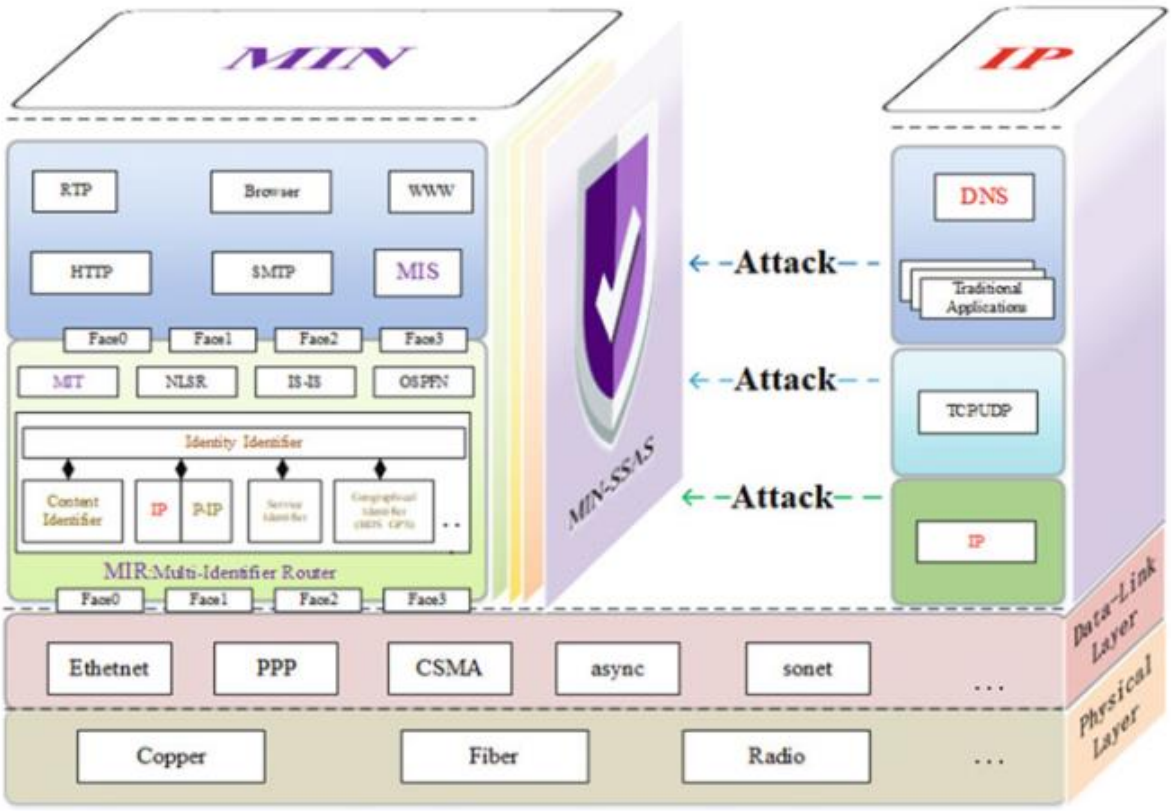
(7) Arsitektur CMD digunakan untuk membangun penyimpanan dan peralatan inti untuk lebih memastikan keamanan sistem dan operasi waktu nyata di jaringan inti.

(8) Mekanisme keamanan rutin lainnya.

3.6 ARSITEKTUR PROTOKOL JARINGAN KEDAULATAN

Karena jaringan kedaulatan mengadopsi jaringan yang berpusat pada identitas sebagai arsitektur jaringan intinya, jaringan ini sama sekali berbeda dari jaringan IP tradisional. Protokol dalam jaringan IP mungkin tidak berlaku dalam jaringan kedaulatan. Namun, lapisan tautan dan lapisan fisik jaringan IP serupa dengan jaringan kedaulatan, sehingga kedua lapisan ini dapat diterapkan dalam jaringan kedaulatan tanpa perubahan apa pun. Protokol dalam lapisan aplikasi jaringan IP perlu dimodifikasi untuk menyesuaikan jaringan kedaulatan.

Agar aplikasi jaringan kedaulatan memanfaatkan sepenuhnya karakteristik jaringan multi-pengidentifikasi, arsitektur jaringan harus didesain ulang. Seperti yang ditunjukkan pada Gambar 3.17, arsitektur jaringan terdiri dari empat lapisan: lapisan aplikasi, lapisan jaringan multi-pengidentifikasi, lapisan tautan data, dan lapisan fisik.



Gambar 3.17 Arsitektur protokol jaringan kedaulatan

Tabel 3.2 Protokol dalam jaringan kedaulatan

PROTOKOL	LAPISAN	FUNGSI
OSPF	Lapisan transportasi	Protokol perutean
IS-IS	Lapisan jaringan	Protokol perutean
BGP	Lapisan aplikasi	Protokol perutean
NLSR	Lapisan jaringan	Protokol perutean, pembuatan tabel FIB
ARP	Lapisan tautan	Analisis korespondensi nama ICN dan MAC
ARP TERBALIK	Lapisan tautan	Analisis korespondensi nama Mac dan ICN
DNS	Lapisan aplikasi	Konten ICN dan resolusi alamat riil ICN
PPP	Lapisan tautan	Protokol titik-ke-titik
NCP	Lapisan tautan	Protokol kontrol jaringan
LCP	Lapisan tautan	Protokol kontrol tautan
CSMA/CA	Lapisan tautan	Protokol penghindaran konflik
……	……	……

Arsitektur ini kompatibel dengan aplikasi tradisional, tetapi tidak sesuai persis dengan model TCP/IP. Protokol yang digunakan dalam jaringan kedaulatan ditunjukkan pada Tabel 3.2. Kami menjelaskan arsitektur protokol yang ditunjukkan pada Gambar 3.17.

Jaringan kedaulatan mengadopsi jaringan yang berpusat pada identitas sebagai jaringan inti dan mengambil pengenal identitas sebagai pengenal autentikasi inti. Dibandingkan dengan tumpukan protokol jaringan IP saat ini, jaringan kedaulatan membentuk

lapisan jaringan multi-pengenal yang menggabungkan dan menyederhanakan lapisan transport dan lapisan jaringan dalam jaringan IP. Protokol dalam lapisan aplikasi jaringan kedaulatan secara kasar mirip dengan protokol dalam lapisan aplikasi jaringan IP, sementara autentikasi ditambahkan dalam lapisan jaringan, dan identitas diambil sebagai kondisi perutean sebelumnya.

Dengan menambahkan bidang pengenal konten, penerjemahan konten dan pengenal identitas telah terwujud. Informasi identitas mewakili informasi pribadi penerbit, seperti nomor ID, nomor telepon seluler, alamat MAC perangkat penerbit, dan sebagainya. Di antara semuanya, penerusan paket di antara lapisan jaringan multi-pengenal, lapisan aplikasi, dan lapisan tautan data adalah melalui Wajah. Wajah merupakan abstraksi dari saluran komunikasi jaringan, yang tidak hanya mewakili informasi koneksi antarmuka perangkat fisik, tetapi juga informasi port antara protokol proses komunikasi. Lapisan tautan data dan lapisan fisik secara kasar mirip dengan jaringan IP saat ini, termasuk CSMA, PPP, Copper, dll.

Gambar 3.18 Konferensi Internet Dunia ke-6

Pengidentifikasi dalam MIN (*Multi-Identifier Network*) mendukung berbagai mode komunikasi dengan semantik yang berbeda seperti semantik push dan pull. Untuk menjamin kinerja transmisi dalam berbagai mode komunikasi, kami mengusulkan MIT (*Multi-Identifier Network Transmission Control Protocol*), yang memungkinkan node MIR untuk berpartisipasi dalam kontrol transmisi guna menyeimbangkan beban jaringan.

Gambar 3.19 Konferensi Internet Dunia ke-6-MIN

MIT memanfaatkan skema deteksi dan notifikasi kongesti yang eksplisit. Node MIR secara berkala mendeteksi status kongestinya dengan menggunakan algoritma AQM (Active Queue Management). Untuk memberi tahu status jaringan saat ini ke node hilir, node MIR menandai paket data melalui pengaturan tag kongesti. Setelah menerima pesan kongesti eksplisit, host akhir akan menyesuaikan kecepatan pengiriman paketnya agar dapat memanfaatkan sumber daya jaringan secara maksimal dan menghindari kongesti jaringan. Untuk paket dengan semantik tarik, penerima menyesuaikan kecepatan pengirimannya menurut tanda kongesti pada paket data yang diterima. Untuk paket dengan semantik dorong, penerima menandai paket balasan melalui tanda kongesti pada paket data yang diterima, sehingga pengirim dapat sepenuhnya memahami apakah paketnya menyebabkan kongesti jaringan melalui paket balasan.

MIN mewujudkan pemerintahan bersama multilateral dan otonomi kedaulatan di dunia maya untuk pertama kalinya. Pada tahun 2019, MIN dan sistem prototipenya dianugerahi sebagai pencapaian teknologi terdepan dari Konferensi Internet Dunia keenam di Wuzhen, Tiongkok (Gambar. 3.18 dan 3.19).

BAB 4
TEKNOLOGI UTAMA JARINGAN KEDAULATAN

Untuk mewujudkan semua fungsi jaringan kedaulatan sekaligus menjamin keamanan, teknologi utama apa yang harus digunakan dalam arsitektur? Bab ini akan menguraikan teknologi utama jaringan kedaulatan.

Jaringan kedaulatan terutama disusun oleh mekanisme penandatanganan dan penerimaan data yang dapat dilacak dan dikombinasikan dengan arsitektur protokol MIN. Berbagai inovasi diusulkan dan diintegrasikan ke dalam Multi-identifier Router (MIR) sebagai perangkat inti MIN, dan konstruksi dilakukan untuk mendukung koeksistensi multi-identifier, tata kelola bersama, keamanan endogen, serta mendukung evolusi jaringan.

Pada bidang data jaringan kedaulatan, untuk mendukung pengoperasian jaringan yang berpusat pada identitas, kami mengusulkan skema transmisi data dan merancang proses akses pengguna berdasarkan jaringan yang berpusat pada identitas, yang dijelaskan dalam Bab 4.1. Untuk memenuhi kebutuhan berbagai skenario komunikasi, kami mengusulkan dan mewujudkan skema antar-terjemahan yang mendukung beberapa pengidentifikasi yang hidup berdampingan secara setara di MIN. Kemudian untuk menjamin kemampuan evolusi endogen MIN, kami merancang mekanisme ekstensi pengenal yang memungkinkan ekstensi pengenal MIN secara bertahap. Rinciannya disajikan di Bagian 4.10. Secara umum, pengenal baru di atas jauh lebih panjang daripada alamat IP, sehingga proses antar-terjemahan dan pengalamatan multi-pengenal akan menghadapi tekanan besar dalam komputasi dan penyimpanan. Untuk tujuan ini, kami mengusulkan tabel hash dengan algoritma pohon awalan HPT, yang mempercepat proses backtracking algoritma kueri FIB dan secara efektif meningkatkan efisiensi penerjemahan dan pengalamatan multi-pengenal. HPT-FIB memiliki overhead penyimpanan yang signifikan ketika skala jaringan semakin meluas. Oleh karena itu, kami mengusulkan pengenal hiperbolik dan skema perutean alih-alih tabel penerusan untuk mengurangi overhead penyimpanan di MIR. Itu dijelaskan di Bagian 4.3. Selanjutnya, dalam rangka memenuhi permintaan pengembangan jaringan masa depan menuju integrasi ruang angkasa-terestrial, kami mengusulkan strategi perutean serakah berdasarkan teknologi perutean hiperbolik dan algoritma perutean satelit adaptif mandiri terdistribusi ringan berdasarkan penundaan untuk membangun Jaringan Multi-Identifikasi Ruang Angkasa-Terestrial (ST-MIN).

ST-MIN memanfaatkan fitur komunikasi satelit yang tidak terpengaruh oleh waktu, lokasi, atau lingkungan, yang dijelaskan dalam Bab 4.9.

Selain itu, dengan mempertimbangkan keandalan komunikasi dan efisiensi transmisi jaringan kedaulatan dalam berbagai skenario, kami mengusulkan MIT–Transmission Control Protocol, skema kontrol transmisi untuk MIN. MIT mendukung kontrol transmisi dalam semantik push dan semantik pull, yang dijelaskan dalam Bab 4.8.

Pada bidang manajemen MIN, untuk mewujudkan tata kelola bersama informasi dan identifikasi pengguna, kami mengusulkan PPoV (Parallel Proof of Vote) sebagai algoritma konsensus non-forking untuk blockchain konsorsium. Ide intinya adalah pemisahan hak suara dan hak pembukuan, yang disajikan dalam Bab 4.2. Selain konstruksi arsitektur, jaringan kedaulatan diperlukan untuk melindungi privasi pengguna dan keamanan sistem saat mengelola pengguna. Untuk tujuan ini, kami merancang berbagai mekanisme keamanan. Untuk menjamin privasi pengguna dan perilaku yang dapat dilacak, dikombinasikan dengan teknologi enkripsi asimetri, kami mengusulkan skema autentikasi identitas jaringan kedaulatan berdasarkan karakteristik biologis manusia. Untuk memberikan jaminan keamanan dan keandalan hierarkis bagi jaringan, kami mengadopsi tiga jenis mekanisme perlindungan: penyensoran jaringan, kriptografi, dan Cyberspace Mimic Defense (CMD) untuk merancang enam tingkat penghalang pertahanan. Selain keamanan struktural di atas, kami merancang Sistem Kesadaran Situasi Keamanan untuk memantau status jaringan secara real time, dan membangun model analisis matematis berdasarkan proses acak untuk menilai keamanan jaringan dan mengoptimalkan kebijakan keamanan. Mekanisme keamanan di atas dijelaskan dalam Bab 4.4, 4.5, 4.6, dan 4.7.

4.1 JARINGAN BERPUSAT PADA IDENTITAS

Jaringan berpusat pada identitas merupakan salah satu teknologi utama jaringan kedaulatan. Transmisi data dalam jaringan kedaulatan didasarkan pada jaringan berpusat pada identitas.

4.1.1 MIN Berdasarkan Jaringan Berpusat pada Identitas

Konsep inti MIN adalah bahwa beberapa pengenal dan semantik transmisi dapat hidup berdampingan dalam lapisan jaringan pada saat yang bersamaan. Untuk menggambarkan makna konkret dari beberapa pengenal, pengenal diklasifikasikan berdasarkan dua dimensi, termasuk bentuk pengenal dan semantik pengenal. Dalam hal dimensi bentuk pengenal, pengenal dapat diklasifikasikan ke dalam tiga jenis berikut:

(1) Pengenal datar. Pengenal datar biasanya terdiri dari serangkaian nilai atau karakter yang tidak beraturan. Jadi, pengenal seperti itu sulit untuk digabungkan dalam tabel perutean. Beberapa arsitektur jaringan (seperti XIA) menggunakan nilai hash dari kunci publik atau irisan data sebagai pengenal untuk perutean, yang merupakan contoh umum pengenal Flat.

(2) Pengenal hierarkis. Penamaan hierarkis menentukan bahwa setiap konten biasanya memiliki pengenal yang mirip dengan URL Web, seperti “/lab/pku/icon.jpg”. Jenis pengenal ini digunakan dalam lapisan Jaringan Named Data Networking (NDN) untuk perutean. Pengenal dalam IPv4 atau IPv6 juga dapat dilihat sebagai pengenal hierarkis.

(3) Pengenal koordinat spasial. Setiap simpul dalam jaringan dipetakan ke dalam ruang geometris dengan koordinat. Dalam model perutean hiperbolik, koordinat hiperbolik digunakan untuk memandu perutean, seperti (R_1, θ_1).

Di sisi lain, dalam hal dimensi semantik pengenal, setidaknya ada dua jenis semantik transmisi yang tercantum sebagai berikut:

(1) Semantik dorong titik-ke-titik. Ini adalah jenis semantik yang diungkapkan oleh pengenal alamat IP tradisional, yang dicirikan oleh pengirim data yang dapat secara aktif mendorong data ke penerima data tanpa permintaan dari penerima data. Router hanya meneruskan paket saat menangani paket jaringan semantik tersebut.

(2) Semantik tarik titik-ke-multi-titik. Ini adalah jenis semantik yang diungkapkan oleh pengenal ICN, yang dicirikan oleh pengirim data hanya dapat mengirimkan data ke penerima dengan premis bahwa penerima meminta data. Saat router menangani paket dalam semantik dorong, ia akan merekam jalur pengembalian paket dan menyimpan data dalam cache.

Perangkat jaringan dapat memproses berbagai jenis pengenal. Perangkat yang mendukung pengenal yang sama dapat dibagi menjadi satu area yang disebut ruang pengenal. Untuk mendukung perluasan pengenal baru di masa mendatang, jaringan saat ini harus memiliki satu atau lebih pengenal dasar. Pengenal dasar yang paling umum adalah pengenal identitas, yang secara langsung menggunakan nilai hash kunci publik perangkat jaringan sebagai pengenal untuk perutean. Itu termasuk pengenal datar, dan kami mendefinisikan semantik transmisinya adalah semantik transmisi titik-ke-titik. Setiap perangkat dalam jaringan harus mendukung pengenal identitas, dan setiap perangkat akan terikat pada pengenal identitas. Definisi formal ruang pengenal diberikan di bawah ini.

1. Definisi Simbol

(1) $I = \{i_0, i_1, i_2, \ldots, i_k\}$mewakili himpunan semua pengenal yang ada dalam ruang MIN. i0 merujuk pada pengenal identitas perangkat jaringan, yang merupakan salah satu yang paling penting. $\{i_1, i_2, \ldots, i_k\}$ berisi pengenal lain yang dapat diperluas, seperti pengenal konten, pengenal layanan, pengenal geografis, IP, dan sebagainya.

(2) V mewakili semua perangkat dalam MIN.

(3) N adalah subhimpunan dari I, yang terdiri dari beberapa pengenal, misalnya, $N = \{i_0, i_1\}$

(4) $S^N = (V_N, N)S^N$merepresentasikan ruang pengenal, yang merupakan 2-tuple. V_N merepresentasikan subset perangkat jaringan V dalam ruang pengenal, dan N merepresentasikan subset semua pengenal yang didukung oleh ruang pengenal S^N.

2. Definisi Ruang Pengenal

Set $S^N = (V_N, N)$dapat merepresentasikan ruang pengenal dalam MIN jika dan hanya jika S^N memenuhi kondisi berikut:

(1) Restriktif: $V_N \subseteq V, N \subseteq I$

(2) Atomisitas: $i_0 \in N$;

(3) Konsistensi: $\forall_v \in V_N, \forall i_j \in N, v$ mendukung i_j;

(4) Penutupan: jika $\exists v \in V$, dan untuk $\forall i_j \in N, v$ mendukung i_j, maka $v \in V_N$.

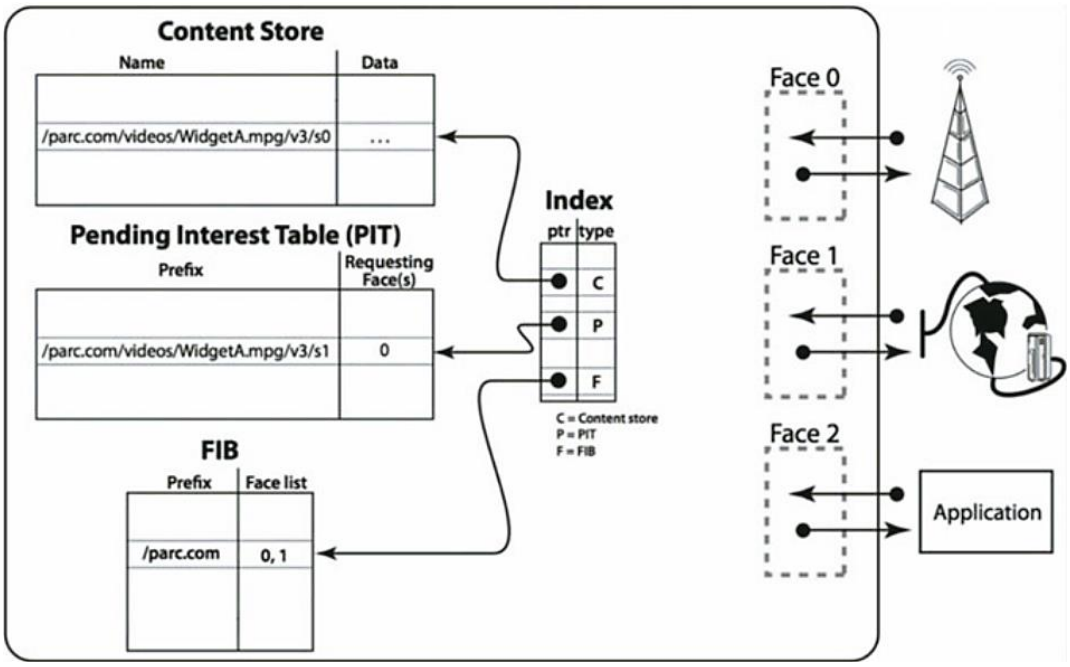
4.1.2 Skema Transmisi Data

Karakteristik skema transmisi data dalam MIN adalah mendukung berbagai semantik transmisi yang hidup berdampingan pada lapisan jaringan pada saat yang sama, termasuk semantik tarik dan semantik dorong. MIR memproses paket masuk dengan metode yang berbeda sesuai dengan jenis pengenalnya, dan mekanisme ini memungkinkan lapisan jaringan MIN agar kompatibel dengan berbagai semantik transmisi.

Pengenal identitas adalah pengenal dasar MIN, dan memiliki dua fitur. Pertama, semantik transmisi pengenal identitas adalah semantik dorong. Kedua, pengenal identitas dapat berupa nilai hash kunci publik pengguna atau perangkat. Semantik dorong titik-ke-titik adalah metode yang paling penting dalam penerusan paket. Ketika router menerima paket masuk, router hanya perlu mencari FIB (Basis Informasi Penerusan) untuk memutuskan hop berikutnya tempat paket akan dikirim. Jika tidak ditemukan kecocokan di FIB, router akan membuang paket. Kedua ujung dalam sesi point-to-point dapat memvalidasi pengenal satu sama lain tanpa badan sertifikasi pihak ketiga dengan menggunakan nilai hash dari kunci publik sebagai pengenal identitas. Ini disebut fungsi pengenal yang disertifikasi sendiri. Semantik transmisi dasar lainnya dalam MIN adalah semantik tarik, yang merupakan semantik transmisi umum dalam Information Centric Networking (ICN). Transmisi data dalam ICN digerakkan oleh konsumen (penerima). Ada dua jenis paket dalam ICN: Paket Minat dan Paket Data. Ada tiga struktur data utama: Forward Information Base (FIB), Content Store (CS), dan Pending Interest Table (PIT). FIB digunakan untuk meneruskan paket minat ke sumber yang cocok dengan data. FIB dalam jaringan kedaulatan menyimpan daftar wajah yang keluar daripada satu wajah tunggal. Selain itu, hampir identik dengan FIB dalam IP. FIB ICN memungkinkan beberapa sumber data untuk ditanyakan secara paralel. CS sama dengan memori buffer dari router IP, tetapi strategi penggantiannya berbeda. Karena setiap paket IP termasuk dalam sesi point-to-point yang terpisah, paket tersebut tidak memiliki nilai lebih lanjut setelah diteruskan ke hilir. Jadi, IP "melupakan" paket tersebut dan mendaur ulang cache (pengganti MRU) segera setelah penerusan selesai. Paket ICN bersifat idempoten, mengidentifikasi diri sendiri, dan tersertifikasi sendiri, sehingga setiap paket ICN mungkin berguna bagi banyak konsumen, misalnya, banyak host membaca berita yang sama atau menonton video YouTube yang sama. Untuk memaksimalkan kemungkinan berbagi dan meminimalkan persyaratan bandwidth hulu dan latensi hilir, node ICN perlu mengingat paket yang masuk dengan strategi substitusi LRU atau LFU selama mungkin.

PIT mencatat jalur pengembalian yang diinginkan yang diteruskan ke sumber konten hulu, sehingga paket data yang dikembalikan dapat dikirim ke hilir ke peminta. Dalam ICN, hanya paket-paket yang diminati yang dirutekan karena paket-paket tersebut menyebar ke hulu ke sumber-sumber data yang memungkinkan dan meninggalkan "jejak". "Jejak" ini menyediakan jalur kembali ke peminta sumber untuk paket yang cocok. Setiap entri PIT adalah jejak. Setelah entri PIT digunakan untuk meneruskan paket data yang cocok, entri PIT dihapus (paket data menggunakan paket yang diminati). Entri-entri PIT yang tidak menemukan paket-paket yang diminati yang cocok dengan paket tersebut pada akhirnya akan habis waktunya oleh model status lunak; konsumen mengirimkan paket-paket yang diminati berulang kali jika

mereka masih menginginkan paket tersebut. Proses transmisi data dalam jaringan yang berpusat pada informasi ditunjukkan dalam Gambar 4.1.



Gambar 4.1 Proses transmisi data dalam jaringan sentris informasi

Peminta mengirimkan paket yang diminati dengan nama konten. Router yang menerima permintaan akan merekam muka kedatangan paket yang diminati, dan melakukan Algoritma Pencocokan Awalan Terpanjang (LPM) untuk nama konten.

Pertama-tama, CS di-query. Jika konten yang diminta ada di CS, konten tersebut dikembalikan langsung ke peminta, dan paket minat dibuang; pada kenyataannya, konten tersebut telah terpenuhi.

Kemudian, nama konten paket minat di-query di PIT. Jika terdapat entri PIT yang sama persis, tampilan kedatangan paket minat ditambahkan ke daftar tampilan yang meminta entri PIT. Kemudian paket minat dibuang karena paket minat yang sama telah dikirim ke node hulu. Oleh karena itu, router akan mengirim salinan paket data ke setiap tampilan masuk yang sesuai yang tercatat di PIT saat paket data tiba.

Terakhir, nama konten paket minat di-query di FIB. Jika terdapat entri yang cocok, paket minat perlu dikirim ke hulu ke sumber data. Jika daftar FIB yang di-query tidak kosong, paket minat kemudian dikirim ke semua tampilan yang dicadangkan, dan entri PIT baru dibuat sesuai dengan paket minat dan tampilan kedatangannya.

Jika paket minat tidak cocok dengan entri apa pun di FIB, paket tersebut dibuang. Ini berarti bahwa node ini tidak memiliki data yang cocok dan tidak tahu cara menemukan data yang cocok. Setelah paket minat mencapai node yang memiliki sumber daya yang diminta, paket data yang berisi nama, konten, dan tanda tangan penerbit diteruskan ke peminta di sepanjang jalur terbalik paket minat.

Selama transmisi data, baik paket minat maupun paket data tidak membawa alamat host atau antarmuka apa pun. Selain itu, ICN memperkenalkan desain cache jaringan. Router yang dilalui paket data akan menyimpan konten yang benar dalam memori buffernya, yaitu CS. Cache di ICN dapat membantu mengurangi penundaan dan penggunaan bandwidth dalam proses pengunduhan konten. Jika cache telah menyimpan konten permintaan, cache tersebut dapat dikembalikan ke peminta tanpa mengakses sumber data saat permintaan tiba di router.

Proses penerusan data dalam jaringan yang berpusat pada informasi adalah sebagai berikut. Ketika beberapa paket minat meminta data yang sama pada saat yang sama, router merekam tampilan masuk paket minat ini di PIT dan hanya meneruskan paket minat pertama yang diterima. Saat paket data dikembalikan, router menemukan entri yang cocok dalam PIT dan meneruskan paket ke wajah yang tercatat dalam entri.

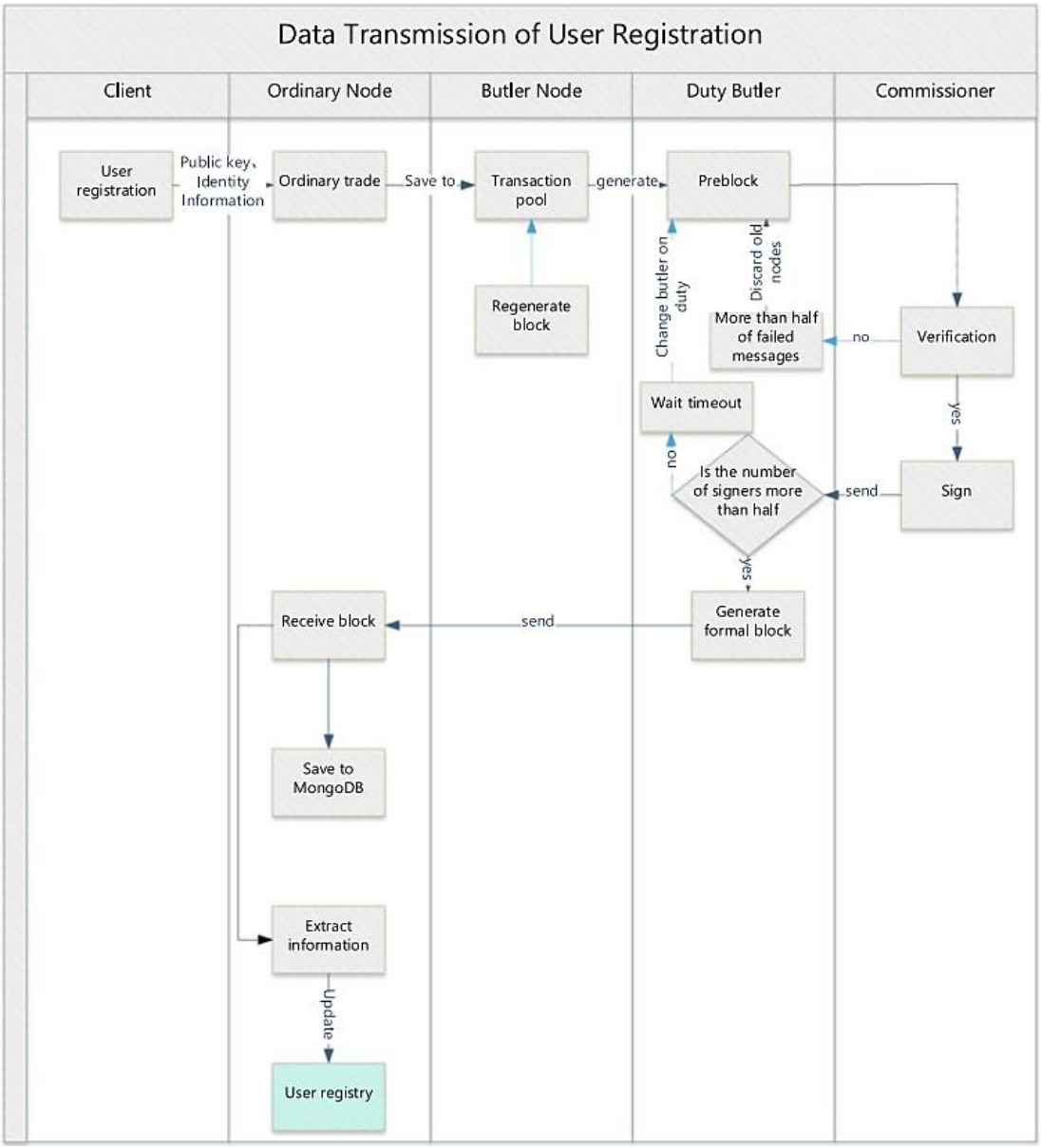
4.1.3 Proses Akses Pengguna

Dalam jaringan yang berpusat pada identitas, strategi manajemen yang menggabungkan informasi identitas diperkenalkan untuk akses pengguna. Untuk mendorong pengguna agar bertanggung jawab atas konten yang dipublikasikan, konten baru yang dipublikasikan oleh pengguna dikaitkan dengan informasi identitas mereka.

Proses pendaftaran pengguna ke jaringan kedaulatan berdasarkan blockchain ditunjukkan pada Gambar 4.2.

Setiap pengguna dalam jaringan kedaulatan adalah simpul klien. Pengguna dalam jaringan kedaulatan harus mendaftar dengan identitas asli mereka. Klien membuat kunci publik dan privat, kemudian mengirimkan kunci publik, informasi identitas, dan informasi yang ditandatangani dengan kunci privat ke simpul mana pun dalam blockchain. Semua simpul blockchain membuka utas layanan. Ketika simpul blockchain menerima permintaan yang dikirim oleh klien, format permintaan diperiksa terlebih dahulu. Kemudian simpul blockchain mencari informasi pengguna di basis data lokal dan cukup memvalidasi beberapa konten. Jika salah satu langkah di atas gagal, pesan kesalahan dikembalikan ke klien. Jika semua verifikasi berhasil, simpul blockchain merangkum permintaan pendaftaran pengguna sebagai transaksi umum dan mengirimkannya ke semua simpul konsorsium.

Petugas yang menerima transaksi biasa menyimpannya di kumpulan transaksi. Di awal setiap putaran konsensus, petugas yang bertugas mengambil transaksi biasa dari kumpulan transaksi untuk menghasilkan pra-blok dan mengirimkannya ke semua komisioner untuk ditandatangani.



Gambar 4.2 Proses akses pengguna

Komisioner yang menerima pra-blok harus memverifikasi header pra-blok dan setiap transaksi sesuai dengan aturan yang ditetapkan sebelumnya. Ada tiga jenis validasi: tidak ada validasi, validasi probabilistik, dan validasi kata kunci terhadap daftar filter khusus. Jika verifikasi gagal, komisioner akan mengirim pesan kegagalan ke kepala pelayan yang bertugas. Jika tidak, tanda tangan header blok akan dikembalikan ke kepala pelayan yang bertugas.

Jika lebih dari separuh komisioner yang terkumpul menolak tanda tangan, kepala pelayan yang bertugas akan menghapus pra-blok dalam memori, mengambil transaksi dari kumpulan lokal untuk membuat pra-blok dan mengirimkannya ke semua komisioner untuk ditandatangani. Jika lebih dari separuh komisioner yang terkumpul menyetujui tanda tangan, kepala pelayan yang bertugas akan menyimpan tanda tangan di header blok dan menghitung jumlah kepala pelayan yang bertugas untuk periode konsensus berikutnya. Kemudian menambahkan stempel waktu untuk menjadikan pra-blok sebagai blok formal. Blok formal

akhirnya dirilis ke jaringan blockchain. Jika kurang dari setengah tanda tangan yang diterima, kepala pelayan yang bertugas akan menunggu hingga waktu habis, yaitu 20 detik. Kemudian kepala pelayan yang bertugas akan diganti dan pra-blok akan dibuat ulang dan dikirim ke komisaris untuk ditandatangani.

Dalam blockchain, setiap simpul yang menerima blok formal akan memverifikasi tanda tangan komisaris dan apakah jumlah tanda tangan lebih dari setengah komisaris. Jika validasi berhasil, blok disimpan dalam basis data MongoDB. Informasi pendaftaran pengguna kemudian diekstraksi dari blok dan disimpan dalam registri pengguna. Informasi pengguna di luar blockchain juga disimpan melalui MongoDB. Mengingat MongoDB adalah jenis NoSQL (Not Only SQL), data internal disimpan dalam format seperti JSON yang disebut BSON, yang berbeda dari konsep tabel data dalam basis data relasional umum. Namun, karena kunci data pengguna yang tetap dan tidak ada struktur bersarang, hal itu dapat disamakan dengan tabel informasi pengguna dalam basis data relasional. Prosedur di atas mengimplementasikan proses dari pengiriman permintaan hingga penyimpanan dalam basis data dan tabel informasi di luar blockchain. Dengan menambahkan permintaan pendaftaran pengguna dalam proses konsensus, merangkum informasi pendaftaran pengguna ke dalam transaksi biasa, memverifikasi transaksi, mengambil informasi pengguna dari transaksi, dan menyimpan ke basis data, prosedur ini mewujudkan kombinasi blockchain dan fungsi pendaftaran pengguna.

Kolom dan maknanya yang terdapat dalam tabel informasi pengguna ditunjukkan pada Tabel 4.1. Contoh tabel informasi pengguna ditunjukkan pada Tabel 4.2.

Tabel 4.1 Tabel informasi pengguna

Kunci	Nilai	Deskripsi
Pubkey	String	Kunci publik pengguna terdaftar
Awalan	String	Awalan pengenal ICN
Level	Int	Tingkat pengguna (0/1:1 dapat menerbitkan konten; 0 hanya dapat menonton)
Stempel waktu	Double	Stempel waktu
Real_msg	String	Informasi identitas asli

Tabel 4.2 Contoh tabel informasi pengguna

Kunci Publik	Awalan	Tingkat	Stempel waktu	Real_msg
07602c1c5…	/Stasiun bukit emas	1	334505	Zhujiang, 1375…, 51222…, deskripsi
……	……	……	……	……

4.2 TEKNOLOGI BLOCKCHAIN KONSORSIUM TERKELOLA MULTILATERAL SKALA BESAR

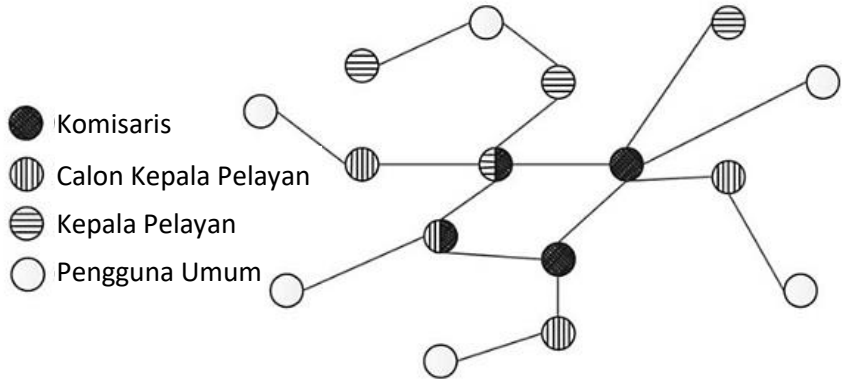
Blockchain berasal dari cara unik untuk menyimpan data dalam sistem mata uang kripto seperti Bitcoin. Blockchain dapat menyimpan semua data historis, catatan transaksi, dan informasi terkait lainnya di masa lalu dengan menggunakan struktur penyimpanan data blockchain yang merujuk sendiri. Bitcoin telah memperkenalkan mekanisme konsensus ke dalam teknologi blockchain, yang membuat manipulasi data hampir mustahil bagi penyerang

dalam kesulitan komputasi. Mekanisme konsensus memainkan peran penting dalam aplikasi blockchain, yang secara langsung memengaruhi keamanan dan kinerja produk. Dengan menggabungkan penyimpanan terdistribusi, kriptografi, mekanisme konsensus, dan transmisi peer-to-peer, teknologi blockchain mencapai konsensus spontan dalam lingkungan yang terdesentralisasi dengan inti melindungi kepentingan kelompok. Secara umum, blockchain dibagi menjadi tiga jenis: blockchain publik, privat, dan konsorsium. Teknologi blockchain berasal dari blockchain publik. Namun, dalam penerapan praktis, blockchain publik mengalami berbagai pembatasan di berbagai negara karena transparansinya, informasi pribadi yang tidak dapat dilacak, dan pengendalian yang lemah. Sebagai kompromi antara blockchain publik dan privat, blockchain konsorsium memiliki keuntungan mewujudkan "desentralisasi parsial" antara beberapa lembaga yang ada, menjadikan konsorsium mereka efisien dan adil.

Pembangunan jaringan kedaulatan mengadopsi algoritma konsensus baru dan efisien yang diusulkan sendiri—PoV (Proof of Vote), yang cocok untuk blockchain konsorsium.

4.2.1 Algoritma Konsensus PoV

Ada empat peran dalam PoV: komisaris, kepala pelayan, kandidat kepala pelayan, dan pengguna biasa. Peran bersama dalam tingkat tertentu diperbolehkan, seperti yang ditunjukkan pada Gambar 4.3.



Gambar 4.3 Empat peran dalam jaringan PoV

1. Komisaris

Seorang komisaris adalah anggota komite konsorsium. Beberapa perusahaan atau lembaga dari berbagai wilayah di dunia membentuk komite konsorsium dan mengelola sistem blockchain konsorsium bersama-sama. Komisaris baru harus diterima melalui undang-undang konsorsium yang diusulkan atau konsultasi offline, dan diwakili oleh node yang bekerja di jaringan blockchain konsorsium. Node tersebut menggunakan CS (Server Komersial) untuk menyediakan layanan.

Komisaris memiliki karakteristik sebagai berikut:

(1) Komisaris memiliki hak untuk merekomendasikan, memberikan suara untuk, dan mengevaluasi kepala pelayan node pembukuan.

(2) Komisaris berkewajiban untuk memverifikasi dan meneruskan blok dan transaksi.

(3) Konsorsium yang berbeda dapat menetapkan bobot suara sesuai dengan bagiannya, yang dapat tercermin dalam proporsi tanda tangan komisaris. Secara default, setiap komisaris memiliki hak dan kewajiban yang sama dan memiliki kedudukan yang sama.
(4) Ketika sebuah blok mendapat suara mayoritas, blok tersebut akan ditandai sebagai sah dan ditambahkan ke blockchain. Hasil pemungutan suara mewakili keinginan semua komisaris.

2. Kepala Pelayan

Kepala pelayan mengkhususkan diri dalam memproduksi blok. Jumlah node kepala pelayan terbatas. Mereka dapat dianggap sebagai node representatif dalam algoritma konsensus tradisional, tetapi perbedaannya adalah bahwa otoritas kepala pelayan diawasi dan dipilih oleh komisaris dalam konsorsium. Peran kepala pelayan dirancang untuk memisahkan hak suara dan hak pembukuan. Komisaris tidak memiliki hak untuk memproduksi blok. Namun, seorang kepala pelayan harus mengumpulkan transaksi dari setiap komisaris melalui jaringan, mengemasnya ke dalam blok, dan menandatanganinya.

Untuk menjadi kepala pelayan, seseorang perlu mengambil dua langkah:

(1) Mendaftar sebagai kandidat kepala pelayan.
(2) Berpartisipasi dalam pemilihan di akhir setiap masa jabatan. Kandidat kepala pelayan akan dipilih oleh komisaris dan yang berhasil akan dipilih sebagai kepala pelayan.

Para kepala pelayan bergiliran membuat blok secara acak selama masa jabatan dan menerima pemilihan ulang setelah masa jabatan mereka berakhir.

3. Calon Butler

Sistem ini memberi nomor kepada para butler {0, 1, 2, …, n − 1} yang memenangkan pemilihan di setiap putaran. Karena jumlah butler terbatas, komisioner hanya dapat memilih butler dari kandidat butler melalui pemungutan suara. Jika kandidat butler kalah dalam pemilihan, mereka dapat tetap online, dan menunggu pemilihan berikutnya.

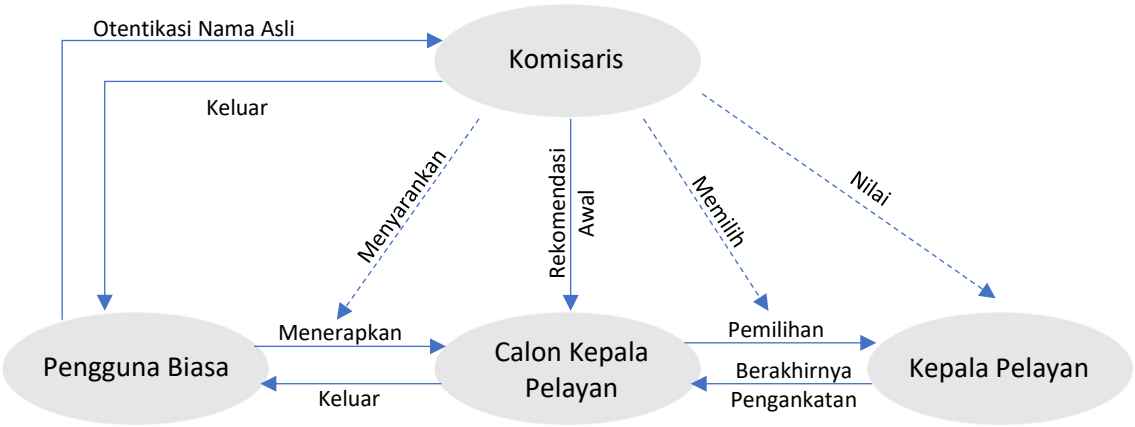
Ada tiga langkah untuk mengajukan kandidat butler:

(1) Daftarkan akun pengguna di sistem konsorsium dan kirimkan permintaan kepada komisioner untuk menjadi kandidat butler.
(2) Kirimkan surat rekomendasi. Setelah memverifikasi dan memastikan bahwa informasi identitas kandidat butler benar, komisioner menandatangani surat rekomendasi yang dibuat melalui pemanggilan fungsi enkripsi asimetris. Kunci pribadi dan publik masing-masing digunakan untuk mengenkripsi dan mendekripsi surat rekomendasi untuk mencegah pemalsuan.
(3) Bayar uang jaminan untuk menjadi kandidat butler. Komisioner dapat mempertahankan peran ganda sebagai kandidat butler dengan merekomendasikan diri mereka sendiri.
(4) Pengguna Biasa

Ketiga node ini menggunakan kriptografi untuk mengautentikasi identitas mereka dan perlu menandatangani nilai hash dari pesan operasional mereka. Sebaliknya, pengguna biasa memiliki karakteristik berikut:

(1) Tidak diperlukan identifikasi. Perilaku pengguna biasa dapat bersifat sewenang-wenang dan anonim. Dalam implementasi tertentu, nama asli pengguna mungkin diperlukan sesuai dengan konfigurasi blockchain konsorsium, atau informasi identitas pengguna dalam transaksi dapat disembunyikan oleh fungsi enkripsi.
(2) Pengguna biasa dapat bergabung atau keluar dari jaringan kapan saja.
(3) Pengguna biasa tidak dapat berpartisipasi dalam pembuatan blok, hanya dalam distribusi dan pembagian blok.
(4) Pengguna biasa dapat melihat seluruh proses konsensus saat menerima layanan sistem. Dalam proses pembuatan blok, pengguna biasa memiliki kewajiban untuk berpartisipasi dalam proses penerusan blok.

Gambar 4.4 menunjukkan hubungan antara keempat peran tersebut.

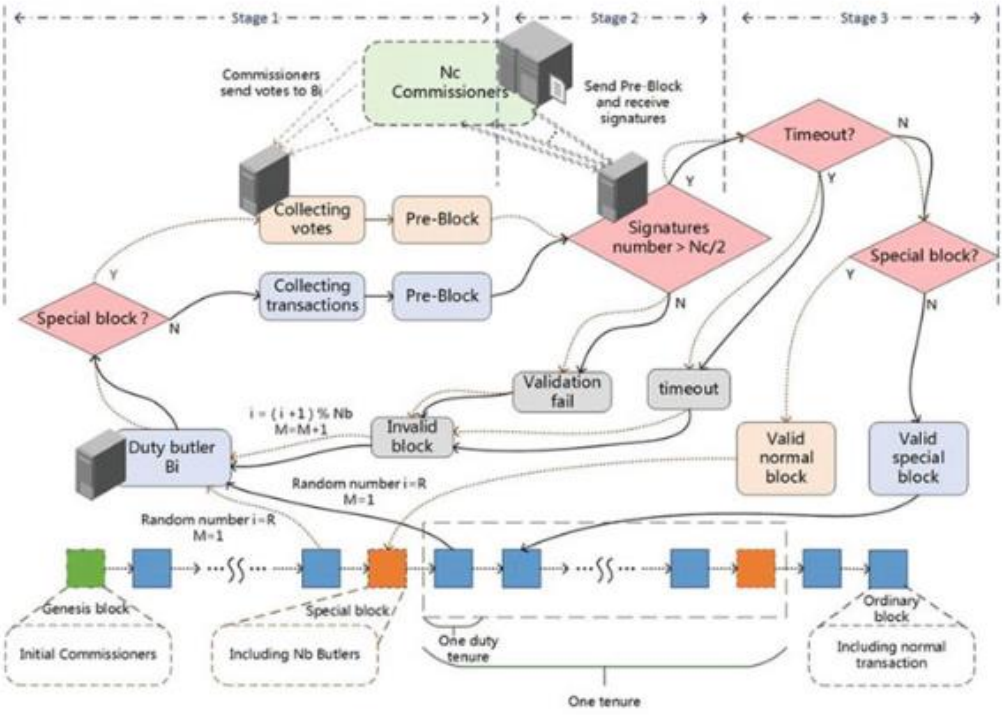


Gambar 4.4 Konversi empat peran

4.2.2 Proses Konsensus PoV

Proses konsensus PoV secara keseluruhan ditunjukkan pada Gambar 4.5. Setelah inisialisasi, setiap node pertama-tama memasuki fase pembuatan blok genesis, yang dibuat bersama oleh para komisioner dan berisi informasi anggota konsorsium awal dan kelompok pertama kepala pelayan.

Saat blok genesis dibuat, sistem akan secara otomatis memasuki siklus "membuat blok biasa BW + 1 blok khusus". Setiap siklus adalah masa jabatan, dan satu putaran konsensus dapat melewati M kepala pelayan yang bertugas untuk akhirnya membuat satu blok. Kepala pelayan mengedarkan pekerjaan selama bertugas dan tidak bertugas, dan secara berkala mengajukan permohonan kepada sebagian besar komisioner untuk sinkronisasi blok guna memastikan status terbaru dirinya. Siklus pembuatan blok juga merupakan siklus tugas kepala pelayan yang dipilih untuk membuat blok. Setiap blok berisi angka acak R yang dibuat oleh algoritma angka acak, yang menentukan jumlah kepala pelayan yang bertugas berikutnya i = R.



Gambar 4.5 Proses pembuatan blok

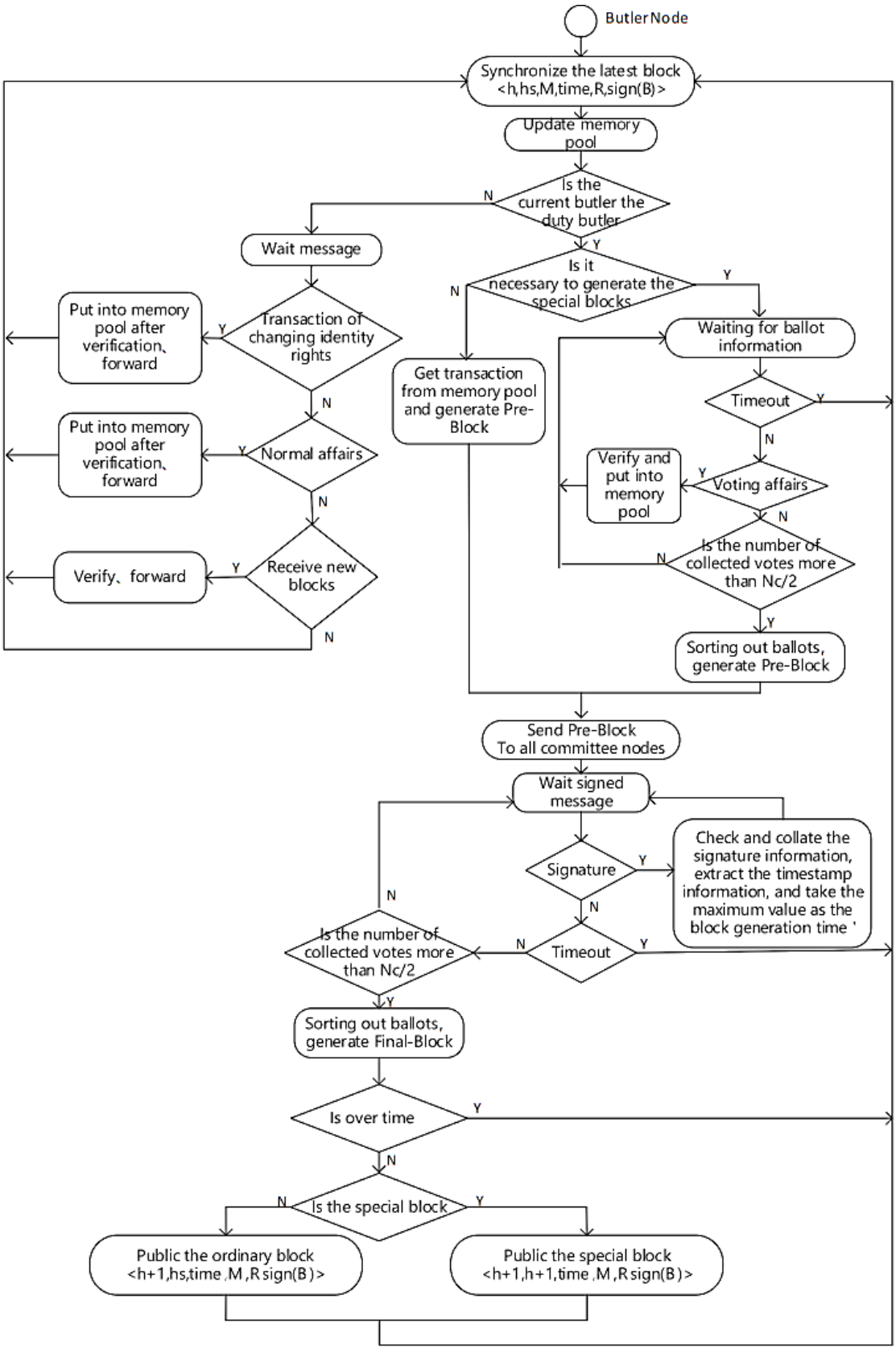
Setelah blok genesis dibuat, simpul kunci untuk membuat blok adalah komisaris dan pelayan. Gambar 4.6 dan 4.7 masing-masing menunjukkan diagram alir perspektif pelayan dan komisaris blok biasa, di mana〈h; hs; M; waktu; R; tanda B〉mewakili tinggi blok, tinggi blok khusus terbaru, siklus tugas biaya, stempel waktu, nomor acak, tanda tangan pelayan, dan atribut kunci lainnya di blok saat ini.

Gambar 4.6 dan 4.7 menjelaskan proses kunci pembuatan blok biasa dan blok khusus hanya dari perspektif komisaris dan pelayan. Di sisi lain, simpul lain, seperti kandidat pelayan dan pengguna biasa berada dalam siklus berkelanjutan untuk menyinkronkan blok, memperbarui data yang disimpan, meneruskan blok, mengirimkan, dan meneruskan transaksi. Sebagian besar operasi ini berada di lapisan jaringan dan lapisan data. Mengirimkan transaksi aplikasi umum berada di lapisan aplikasi dan biasanya dioperasikan oleh dompet.

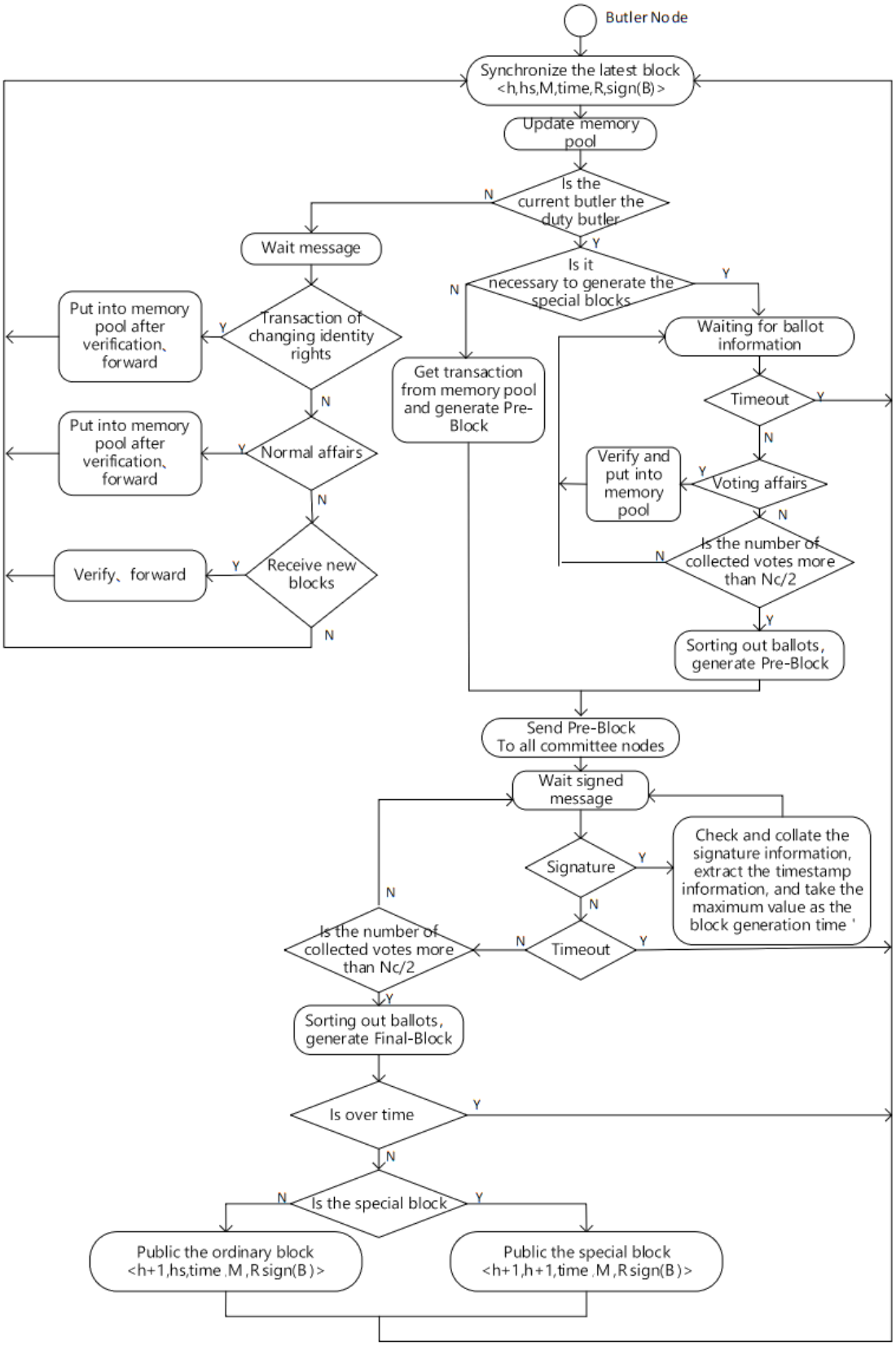
Algoritma 4.1 memberikan pseudocode untuk menjalankan algoritma PoV pada sebuah node. Setelah serangkaian inisialisasi, node menentukan cara menjalankan proses PoV berdasarkan status dan konfigurasinya sendiri.

Algorithm 4.1: The running process of PoV state machine

Input:
Initial state.
Begin
System_init()
{*gen_com_ list*} set_commissioner_list_genesis() // set the initial commissioner list
{*Block_list*}←BLOCK_SYNC() // synchronize the latest block and update variables and memory pools
examine({*com_list*}, {*bul_list*}, {*bc_list*}, {*user_list*})
myaddr←key_manager.get_my_public_key() // get the address of the node, which is the public key
if *my_addr*{*com_list*}{bc_list} **then**
  if *my_addr*{*com_list*} **then**
    run the commissioner's working process
  end if
  if *my_addr*{*bc_list*} **then**
    run the butler candidate's working process
  end if
  else if *my_addr*{*user_list*} **then**
  run the ordinary user's working process
  else then
    Forward_block_and_message() // forward blocks and messages
  end if
End of Algorithm



Gambar 4.6 Bagan alir untuk menghasilkan blok biasa dan blok khusus (perspektif Butler)



Gambar 4.7 Diagram alir pembangkitan blok biasa dan blok khusus (perspektif komisaris)

Algoritma 4.2 menguraikan penerapan proses komisaris, termasuk fase pembuatan blok genesis dan pembuatan blok biasa.

Algorithm 4.2: The commissioner's working process

Input:
Initial state.
Begin
1: **while** *is_connecting_to_network*==*true* **do**
2: {*Block_list*}←BLOCK_SYNC() // synchronize the latest block and update variables and memory pools
3: *Height*←make_get_height_request_mag() // request the latest height
4: **if** *Height*==NULL // there are no blocks in the network yet
5: send Tx_PERMISSION<gen_com, com, *NULL*, *my_addr*, *sign*>
6: **if** *is_needed_to-be_bulter*==*true* **then**
7: send Tx_PERMISSION<com,bc,*self_recommand*,*my_addr, sign*>
8: **end if**
9: **if** *my_addr*==min(sort({*com_list*})) **then** // the initial commissioner with the smallest public key is the acting committee one
10: generate the genesis block
11: **end if**
12: **else then**
13: the commissioner process enters the phase of generating blocks
14: **end if**
15: **end while**
End of Algorithm

Algoritma 4.3 menggambarkan implementasi proses kandidat butler.

Algorithm 4.3: The butler candidate's working process

Input:
Initial state.
Begin
1: **while** *is_connecting_to_network*==*true* **do**
2: {*Block_list*}←BLOCK_SYNC() // synchronize the latest block and update variables and memory pools
3: process the received voting transaction, validate and put it into the memory pool
4: process the received identity changing transaction, validate and put it into the memory pool
5: process the received ordinary transaction, validate and put it into the memory pool
6: process the other message, verify its validity and forward it
7: process the received new block, verify its validity and update the information
8: if *my_addr*{*bc_list*} then
9: the butler candidate process enters the phase of the butler's tenure
10: **end if**
11: **end while**
End of Algorithm

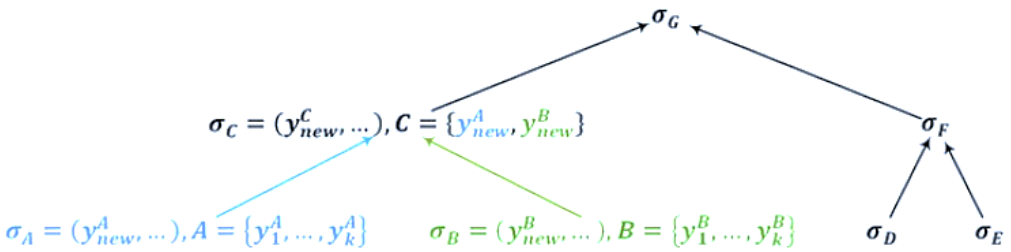
PoV ini telah diperbarui menjadi versi Parallel PoV yang sangat efisien, atau segera disebut sebagai PPoV.

4.2.3 Mekanisme Tanda Tangan Hirarkis PoV

Karena pembagian kerja di antara node dalam jaringan yang berpusat pada identitas berbeda, jaringan kedaulatan mempertimbangkan untuk menggunakan skema tanda tangan grup/cincin hierarkis. Tanda tangan node dalam jaringan membentuk struktur pohon, dan setiap node atasan mengelola sekelompok node bawahan sebagai daunnya. Node non-daun dan daunnya membentuk grup/cincin. Tabel kunci publik dengan semua kunci publik dalam grup/cincin dikelola secara lokal di mana format tanda tangan node daun dan non-daun masing-masing adalah $\sigma = (r, s)$ dan $\sigma = (y_{new}, \hat{r}_1, \ldots, \hat{r}_t, s), \hat{r}_i = (r_i, \sigma_i)$, seperti yang ditunjukkan pada Gambar 4.8.

Tanda tangan superior dihasilkan oleh kombinasi tanda tangan subordinat dan berisi semua informasi dari node subordinat. Jadi, verifikasi tanda tangan superior juga mencakup pohon yang diakar oleh tanda tangan tersebut. Selain itu, menurut persyaratan keamanan skema tanda tangan grup hierarkis, manajer grup hanya dapat melacak identitas penanda tangan dari node daunnya dan tidak dapat membuka tanda tangan yang dihasilkan oleh anggota di grup lain. Dengan membuat grup di antara node dengan level dan identitas yang berbeda, manajer grup superior dapat dengan cepat menemukan grup yang bermasalah dan mengidentifikasi node jahat yang sesuai.

Untuk mengurangi ukuran pohon tunggal dan kompleksitas verifikasi berulang, pohon tanda tangan dibagi menjadi dua jenis menurut kepemilikan dan tujuannya: pohon tanda tangan ring untuk pemungutan suara dan pohon tanda tangan grup umum. Mekanisme tanda tangan hierarkis berdasarkan teknologi tanda tangan grup/ring dengan blok PoV ditunjukkan pada Gambar 4.9.



Gambar. 4.8 Tanda tangan grup/cincin hierarkis

(1) Setiap pengguna biasa di domain bawah membuat transaksi dan melampirkan tanda tangan S. Pengguna tersebut juga menerima transaksi intradomain dan memverifikasi kebenaran dalam hal konten dan tanda tangan. Jika benar, transaksi tersebut diteruskan ke node lain di domain tersebut. Butler mendengarkan transaksi intradomain dan memasukkan transaksi yang valid ke dalam kumpulan lokal.

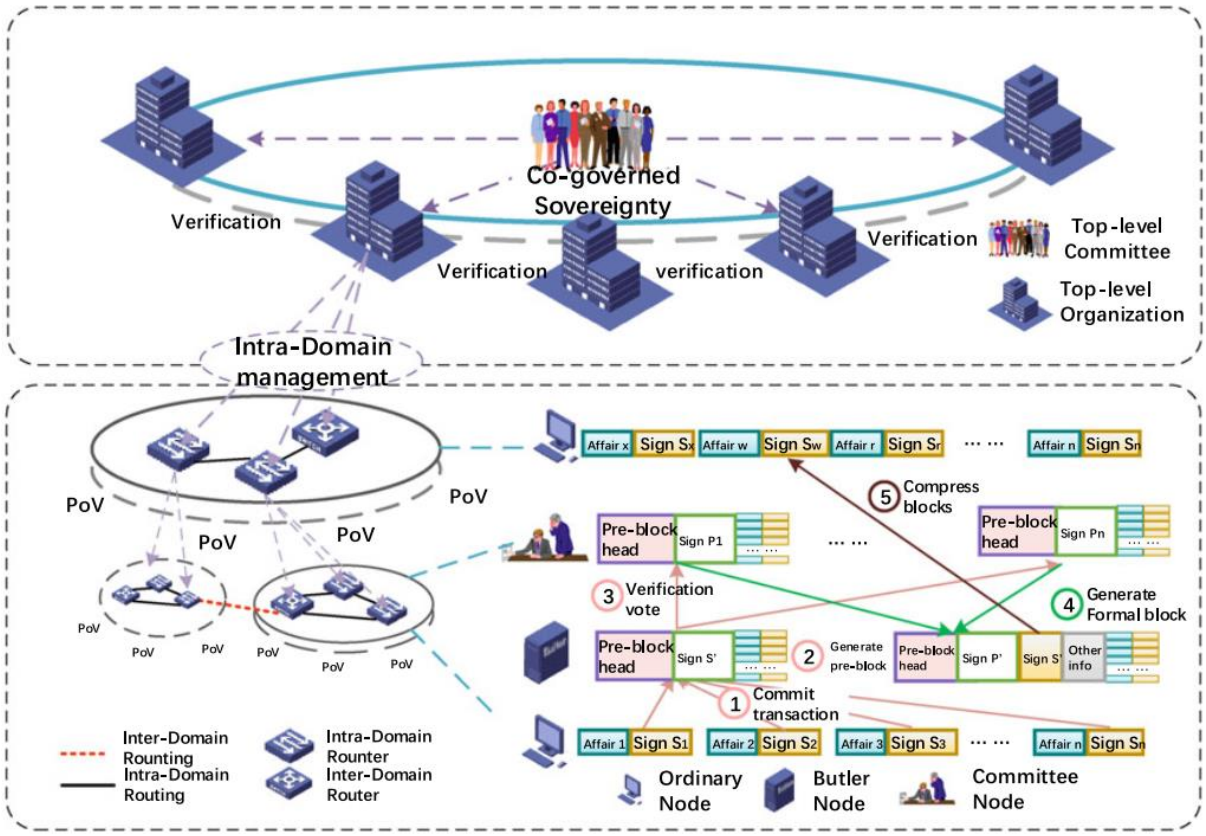
(2) Butler yang bertugas secara teratur mengambil transaksi dari kumpulan dan merangkumnya ke dalam prablok. Pengguna biasa yang menjadi anggota transaksi tersebut ditambahkan ke grup butler yang bertugas untuk membuat tanda tangan

grup superior baru S'. Kemudian, butler yang bertugas mengirimkan prablok dan S' kepada komisaris dan butler di domain tersebut.

(3) Setelah komisaris menerima prablok, ia akan memverifikasi transaksi dan tanda tangan butler S'. Jika ia setuju untuk membuat blok yang sesuai, ia akan mengirimkan kembali tanda tangannya P dan stempel waktu sebagai tiket kepada butler yang bertugas.

(4) Jika telah mengumpulkan tanda tangan dan stempel waktu dari lebih dari setengah komisaris intra-domain sebelum batas waktu, kepala pelayan yang bertugas akan membentuk lingkaran dengan komisaris yang termasuk dalam tanda tangan ini untuk menghasilkan tanda tangan lingkaran superior baru P'.

(5) Ketika komisaris menerima blok terakhir, ia memverifikasi tanda tangan P' dan S'. Jika valid, transaksi yang terdapat dalam blok akan dihapus dari kumpulan lokal. Jika komisaris tidak berada di domain teratas, ia akan mengekstrak tajuk blok sebagai transaksi, mengganti tanda tangan kepala pelayan yang terlampir S' dengan tanda tangan grup superior baru S", dan kemudian mengusulkan transaksi sebagai pengguna biasa di domain superior. Node superior lainnya terus memverifikasi tanda tangan P' dan S". Jika komisaris berada di domain teratas, blok akan menjadi sah dan akhirnya dikonfirmasi ketika lebih dari setengah komisaris mengakui telah menerima.



Gambar 4.9 Mekanisme tanda tangan hierarkis PoV

4.3 SKEMA ROUTING UNTUK MILIARAN PENGIDENTIFIKASI GANDA

Metode Routing tradisional berdasarkan Protokol Routing datar, seperti Routing Information Protocol (RIP) dan Open Shortest Path First (OSPF), dihadapkan pada masalah sinkronisasi Informasi Routing, dan tidak dapat diadaptasi ke arsitektur jaringan hierarkis. Mempertimbangkan karakteristik manajemen hierarkis jaringan kedaulatan, protokol BGP diadopsi untuk menyinkronkan informasi routing antara sistem otonom dari jaringan tingkat yang sama. Mempertimbangkan Internet Industri masa depan dan skenario aplikasi lainnya, skala pengalamatan jaringan akan terus mengalami pertumbuhan eksplosif.

Untuk lebih meningkatkan efisiensi routing, pengidentifikasi hiperbolik dan skema routing diusulkan untuk jaringan inti yang memiliki topologi lebih stabil dan di bawah tekanan routing yang lebih besar daripada bagian lain. Kemudian tabel hash dengan algoritma pohon awalan dirancang untuk jaringan tepi yang topologinya sering berubah untuk mendukung sejumlah besar masalah routing pengidentifikasi.

4.3.1 Border Gateway Protocol

Border Gateway Protocol (BGP) adalah protokol routing vektor jarak optimal, yang digunakan untuk menghubungkan rute antar sistem otonom. Protokol BGP menyediakan sistem routing antardomain, yang menjamin bahwa sistem otonom hanya dapat bertukar informasi routing secara asiklik dan router bertukar informasi tentang jalur ke jaringan target.

BGP dimodifikasi dari Exterior Gateway Protocol (EGP), di mana EGP hanya dapat mengangkut informasi routing antar AS. Namun, EGP tidak membedakan prioritas apa pun dalam routing dan tidak mempertimbangkan cara menghindari loop routing antar AS. Jadi BGP umumnya diadopsi dalam jaringan inti operator. Berbeda dengan EGP asli, BGP menyediakan layanan yang lebih baik karena pengoptimalan routing, menghindari loop routing, routing yang efisien, dan mempertahankan sejumlah besar informasi routing. Ini adalah protokol routing berbasis kebijakan yang memungkinkan sistem otonom untuk mengangkut data berdasarkan berbagai atribut BGP. Faktor terpenting yang perlu dipertimbangkan adalah atribut BGP daripada kecepatan, saat menentukan jalur terbaik. BGP meneruskan dengan memelihara tiga tabel:

(1) tabel hubungan tetangga yang mencatat semua tetangga,
(2) basis data penerusan yang mencatat jaringan tetangga, atribut jalur, dan atribut BGP,
(3) tabel rute yang mencatat jalur optimal dan jarak rute BGP dari luar/dalam.

Jenis pesan utama tercantum pada Tabel 4.3.

Tabel 4.3 Jenis pesan BGP

Buka	Negosiasikan parameter BGP
Keepalive	Deteksi hubungan tetangga BGP
Pembaruan	Arahkan ke BGP
Pemberitahuan	Pesan kesalahan
Penyegaran	Segarkan pesan, kirim dan terima lagi

BGP mengadopsi berbagai strategi untuk membangun hubungan tetangga sesuai dengan statusnya. Dalam status Idle, BGP menolak permintaan koneksi dari tetangga. Hanya setelah menerima peristiwa Start dari perangkat ini, BGP mencoba membuat koneksi TCP dengan rekan BGP lain dan masuk ke status Connect. Peristiwa Start dipicu oleh salah satu alasan berikut: prosedur BGP dikonfigurasi oleh operator, prosedur yang ada diatur ulang, dan prosedur BGP diatur ulang oleh perangkat lunak router. Apa pun status BGP, BGP akan masuk ke status Idle setelah menerima peristiwa Error seperti pesan Notification, TCP pipe broken Notification.

Jika dalam status Connect, TCP membangun koneksi melalui jabat tangan tiga kali. Jika TCP tidak menyelesaikan jabat tangan, BGP memulai penghitung waktu Connect Retry dan menunggu TCP menyelesaikan koneksi. Jika koneksi TCP berhasil, maka BGP mengirim pesan Open ke peer dan beralih ke status OpenSent. Jika koneksi TCP gagal, dan BGP beralih ke status Active. Jika penghitung waktu Connect Retry habis dan BGP masih tidak menerima respons dari peer BGP, BGP mencoba membangun koneksi TCP dengan peer BGP lain, dan BGP tetap dalam status Connect.

Dalam status Opensent, jika jabat tangan tiga kali berhasil, dan mengirim pesan OPEN untuk menegosiasikan parameter terkait BGP (misalnya, AS, versi, autentikasi). BGP menunggu pesan Open dari peer, dan memeriksa nomor AS, nomor versi, kode autentikasi, dan seterusnya dalam pesan Open yang diterima. Jika pesan Open yang diterima benar, BGP mengirim pesan Keepalive dan beralih ke status OpenConfirm. Jika ditemukan kesalahan dalam pesan Open yang diterima, BGP mengirimkan pesan Notification ke peer dan beralih ke status Idle.

Saat memasuki status Establish, BGP dapat bertukar pesan Update, Keepalive, Route-Refresh, dan Notification dengan peer. Jika pesan Update atau Keepalive yang benar diterima, maka BGP menilai bahwa peer berjalan, dan mempertahankan koneksi BGP. Jika pesan Update atau Keepalive yang salah diterima, BGP mengirimkan pesan Notification untuk memberitahukan peer tentang masuk ke status Idle. Pesan Route-refresh tidak mengubah status BGP. Jika pesan Notification diterima, BGP beralih ke status Idle. Jika notifikasi rantai TCP diterima, BGP terputus dan beralih ke status Idle. Jika Active TCP gagal melakukan jabat tangan tiga kali, maka akan mencoba tiga kali lalu kembali ke status Idle. Keunggulan BGP:

- BGP menjamin keamanan jaringan, fleksibilitas, stabilitas, keandalan, dan efisiensi tinggi dari berbagai aspek.
- BGP menjamin keamanan jaringan melalui autentikasi dan GTSM.
- BGP menyediakan berbagai kebijakan perutean, yang dapat digunakan untuk memilih rute secara fleksibel dan menginstruksikan tetangga untuk menerbitkan rute sesuai dengan kebijakan.
- BGP menyediakan fungsi agregasi rute dan redaman rute untuk mencegah osilasi rute, yang secara efektif meningkatkan stabilitas.
- TCP digunakan sebagai protokol lapisan transport (nomor port 179) untuk menggabungkan BGP, BFD, BGP Tracking, BGP GR, serta NSR, yang meningkatkan keandalan jaringan.

- Dalam skenario dengan sejumlah besar tetangga dan skala perutean, jika sebagian besar tetangga memiliki strategi keluar yang sama, BGP menggunakan teknologi pengepakan grup yang meningkatkan kinerja pengepakan BGP.

4.3.2 Skema Pengenal Hiperbolik dan Perutean

Jaringan kedaulatan meneruskan konten berdasarkan nama, yang mengalami kendala skala identitas yang besar dan permintaan dinamis yang dibawa oleh banyak jenis pengenal baru dan banyak skenario aplikasi masa depan seperti IoT, Internet Industri, jaringan pribadi dengan keamanan tinggi.

Perutean geometris serakah (GGR) memetakan dunia maya ke dalam ruang metrik dan menetapkan alamat atau koordinat ke setiap simpul. Setiap segmen pesan jaringan yang dikirimkan dalam jaringan disertai dengan koordinat tujuannya. Setiap router menghitung jarak geometris antara setiap simpul yang berdekatan dan tujuan secara terpisah setelah menerima paket. Yang memiliki jarak terkecil akan dipilih sebagai hop berikutnya untuk penerusan. Dalam proses ini, karena informasi yang diperlukan dari setiap simpul hanya mencakup koordinat tetangganya, GGR dapat meminimalkan ukuran FIB sebanyak mungkin. GGR merupakan dasar untuk menyediakan protokol perutean untuk jaringan berskala besar. Perutean hiperbolik (HR) didasarkan pada properti jaringan yang bebas skala, yang berarti bahwa derajat simpul dalam jaringan mengikuti distribusi hukum pangkat. Melalui algoritma pemetaan, jaringan dipetakan ke ruang dengan kelengkungan negatif (yaitu, ruang hiperbolik). Ruang dua dimensi diambil sebagai contoh. Setiap simpul dipetakan ke dalam cakram dengan radius R dan diberi koordinat kutub (r, θ). Koordinat sudut θ menunjukkan posisi relatif simpul dalam jaringan, dan koordinat radial r menunjukkan derajat pusat simpul. Semakin kecil koordinat radius suatu simpul, semakin dekat ke pusat cakram. Ketika koordinat sudut kedua simpul konstan, jarak hiperbolik di antara keduanya akan berkurang seiring dengan berkurangnya koordinat radial. Oleh karena itu, perutean serakah berdasarkan jarak hiperbolik cenderung memilih simpul yang lebih tersentralisasi sebagai hop berikutnya untuk penerusan. Banyak jaringan seperti Internet IP memiliki properti bebas skala. Dengan menggabungkan algoritma pemetaan yang tepat, strategi greedy sederhana berdasarkan rentang hiperbolik dapat meneruskan pesan ke node tujuan dengan tingkat keberhasilan yang tinggi. Untuk beberapa kasus di mana penerusan gagal, strategi penerusan cerdas tambahan dapat diadopsi untuk membuat tingkat keberhasilan pendekatan perutean hiperbolik mencapai 100%.

Namun, algoritma HR juga memiliki beberapa cacat. Dibandingkan dengan protokol perutean berdasarkan algoritma jalur terpendek tradisional, jalur penerusan yang dipilih oleh algoritma HR memiliki penundaan transmisi yang lebih besar. Ini adalah kerugian inheren dari strategi greedy, dan sebagian besar algoritma pemetaan hiperbolik yang ada tidak mempertimbangkan penundaan jaringan. Untuk menghindari kerugian ini, kami telah mengusulkan algoritma perutean hiperbolik yang mengurangi latensi jaringan dan memastikan pemilihan jalur penerusan yang cepat untuk menjamin penerusan cepat jaringan kedaulatan.

Algoritma HR yang diusulkan memetakan ruang siber bebas skala ke ruang hiperbolik tiga dimensi H^3. Setiap node dalam jaringan diberi koordinat bola tiga dimensi. Jarak antara dua titik (r_1, θ_1, ϕ_1) dan (r_2, θ_2, ϕ_2) dapat dihitung berdasarkan hukum kosinus.

$$d_{12} = \cosh^{-1}(\cosh r_1 \cosh r_2 - \sinh r_1 \sinh r_2 \cos \Delta\theta_{12}) \qquad (4.1)$$

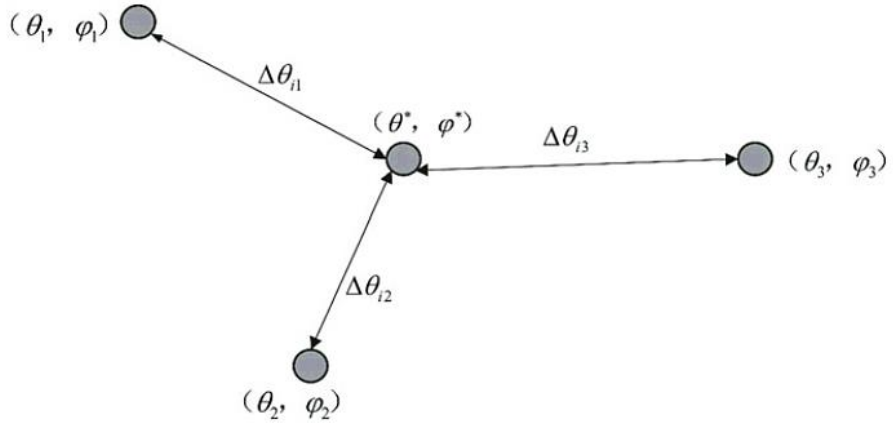
di mana $\Delta\theta_{12}$ melambangkan sudut pusat antara dua titik dan titik asal.

$$\Delta\theta_{12} = \cos^{-1}[\cos \theta_1 \cos \theta_2 + \sin \theta_1 \sin \theta_2 \cos(\theta_1 - \theta_2)] \qquad (4.2)$$

Algoritme ini mencakup dua bagian: pemetaan koordinat sudut dan pemetaan koordinat radial. Proses spesifik dijelaskan di bagian berikutnya.

1. Pemetaan Koordinat Sudut

Setiap simpul diberi koordinat sudut, yang dipetakan ke bola S^2. Bola S^2 mensimulasikan permukaan bumi, sedangkan koordinat sudut simpul mewakili posisi sebenarnya dalam jaringan seperti yang ditunjukkan pada Gambar 4.10.



Gambar 4.10 Pemetaan koordinat sudut

Koordinat sudut dari node derajat tinggi ditetapkan secara langsung sebagai lokasi geografisnya, yaitu informasi lintang dan bujur. Alasannya tercantum sebagai berikut:

- Penundaan transmisi antara dua node sebanding dengan jarak geografis di antara keduanya. Oleh karena itu pemetaan berdasarkan lokasi geografis dapat mengoptimalkan penundaan secara efektif.
- Metode pemetaan mudah dihitung.
- Metode pemetaan tidak bergantung pada informasi topologi jaringan, sehingga mempertahankan stabilitas yang kuat dalam lingkungan jaringan yang dinamis.

Kami telah mengusulkan pendekatan yang berbeda untuk node non-pusat dengan derajat rendah, karena lokasi jaringannya bergantung pada topologi lokal daripada informasi

geografis. Untuk node i yang derajatnya lebih besar dari atau sama dengan 3, ia akan menghitung penundaan rata-ratanya dari setiap node pusat, kemudian memilih tiga node pusat j_1, j_2, j_3 dengan penundaan terkecil untuk menghitung koordinat sudutnya.

Jika penundaan antara i yang koordinat sudutnya adalah (θ^*, φ^*) dan j_k yang koordinat sudutnya (θ_k, φ_k) adalah t_k, kita dapat memperoleh bahwa:

$$\min_{(\theta^*,\varphi^*)\in S^2} [|\xi| + \varepsilon(\Delta\theta_{i1} + \Delta\theta_{i2} + \Delta\theta_{i3})] \qquad (4.3)$$

$$s.t. \lambda\Delta\theta_{ik} = t_k - \xi(k = 1, 2, 3) \qquad (4.4)$$

$\Delta\theta_{ik}$ adalah sudut pusat (θ_k, φ_k) dan (θ^*, φ^*), yang dapat diperoleh dari Persamaan 4.2. Persamaan 4.2 mencerminkan hubungan proporsional langsung dari penundaan jaringan dan jarak bola, di mana variabel relaksasi ξ digunakan untuk memastikan solusi yang layak.

Istilah fungsi objektif sebelumnya memastikan bahwa nilai ξ sekecil mungkin. Istilah terakhir $\varepsilon(\Delta\theta_{i1} + \Delta\theta_{i2} + \Delta\theta_{i3})$ digunakan untuk memilih jumlah jarak bola terkecil ketika ada beberapa solusi yang layak.

Untuk simpul non-pusat dengan derajat kurang dari atau sama dengan 2, koordinat sudutnya akan langsung menyalin salah satu derajat tertinggi di lingkungan tersebut, karena hanya ada satu jalur ke simpul pusat.

2. Pemetaan Koordinat Radial

Koordinat radial r mewakili derajat pusat suatu simpul. Dalam jaringan bebas skala, r mengikuti distribusi eksponensial.

"Simpul super" dalam suatu jaringan dapat menunda pembuatan jalur yang kurang optimal. Misalnya, Shanghai memiliki jumlah pengguna Internet yang sangat besar, jadi ada beberapa "supernode" yang tinggi. Jika pesan dari kota Incheon di Korea Utara ke kota Busan di Korea Selatan, jalur penerusan yang dipilih oleh HR mungkin tertarik ke pusat Shanghai yang tinggi, yaitu, Incheon—Shanghai—Busan yang menyebabkan penundaan tambahan, karena kota-kota ini memiliki populasi yang lebih kecil daripada Shanghai.

Untuk mengatasi masalah ini, jaringan global dibagi menjadi beberapa subgraf. Node paling sentral di setiap subgraf memiliki koordinat radial yang sama. Oleh karena itu, proses penerusan lebih cenderung memilih node pusat di subgraf, yang meningkatkan lokalitas perutean dan mengurangi penundaan transmisi. m node $(i_1, i_2 \ldots i_m)$ dengan derajat tertinggi di jaringan dipilih, dan node lainnya mengukur penundaan antara mereka sendiri dan setiap i_*. Jika i_k adalah yang memiliki penundaan terkecil, maka node ini termasuk dalam subgraf yang sesuai G_k. Koordinat radial diperoleh dengan estimasi kemungkinan maksimum, dan kita memiliki kondisi sebelumnya sebagai berikut:

(1) Derajat simpul mengikuti distribusi daya $\rho(k) \sim k^{-\gamma}$, di mana derajat terendah adalah k_0, dan nilai rata-rata adalah $\bar{k}$. Koordinat derajat dan radius memenuhi hubungan berikut:

$$r(k) = R - 2\ln\frac{k}{k_0} \qquad (4.5)$$

di mana R menunjukkan jari-jari bola.

(2) Peluang menghubungkan dua simpul dengan jarak hiperbolik x adalah:

$$p(x) = \left\{1 + \exp\left[\frac{\zeta(x - R)}{2T}\right]\right\}^{-1} \tag{4.6}$$

T adalah suhu dan mewakili derajat agregasi simpul kontrol. ξ adalah kelengkungan ruang hiperbolik. R dapat diperoleh dengan integral berikut:

$$\bar{K} = \frac{N}{2\pi}\int_0^R \rho[k(r)] \int_0^R \rho[k(r')] \int_0^\pi \int_0^\pi p(x) d\varphi' d\theta' dr' dr \tag{4.7}$$

x adalah jarak hiperbolik antara (r', θ', φ') dan $r;\ 0;\ 0$.

Berdasarkan kondisi sebelumnya di atas, untuk simpul i dengan derajat k_i, kemungkinan maksimum koordinat radialnya diperkirakan sebagai:

$$r_i^* = R - 2\ln\frac{k_i - T\gamma}{k_0} \tag{4.8}$$

Jika node $i \in G_j$, koordinat diameternya adalah:

$$r_i = \log\left\{\beta + \exp\left[r_i^* + (r_0 - r_i^*)\left(\frac{R - r_i^*}{R - r_j^*}\right)^4\right]\right\} \tag{4.9}$$

β digunakan untuk menyesuaikan bobot relatif koordinat radial dan koordinat sudut dalam proses perutean.

Melalui rumus di atas, koordinat diameter r_0 dari simpul paling sentral di setiap subgraf diperoleh, dan hanya sedikit modifikasi yang dilakukan pada simpul non-sentral yang koordinat radial aslinya kecil.

Dalam algoritma pemetaan koordinat sudut, penundaan jaringan setara dengan jarak bola, dan koordinat simpul non-sentral dihitung sesuai dengan itu. Pada saat yang sama, dalam algoritma pemetaan koordinat radial, penundaan dikurangi dengan partisi subgraf. Pada saat yang sama, penundaan jaringan diambil sebagai dasar partisi subgraf.

4.3.3 Tabel Hash dengan Algoritma Pohon Awalan (HPT)

Pohon Awalan (Trie), juga dikenal sebagai Pohon Kamus, adalah struktur data yang umum ditemukan dalam pencocokan string. Dalam pohon kamus, tepi mengacu pada unit yang terdiri dari nama, seperti bit, karakter, dan sebagainya. Node mengacu pada nama tertentu yang isinya adalah kumpulan komponen yang berakar pada semua tepi pada jalur menuju node tersebut. Dalam struktur penyimpanan berdasarkan Pohon Awalan, bagian awalan yang sama di antara nama digabungkan ke jalur hulu untuk mewujudkan kompresi kapasitas data dan pelestarian hubungan logis antara nama.

Karena pohon awalan mendukung algoritma LPM (Pencocokan Awalan Terpanjang) dan memiliki efisiensi penggunaan ruang yang baik, sebagian besar jaringan menggunakan pohon awalan untuk penerusan. Kerugian dari pohon awalan adalah kecepatan pencarian di pohon awalan lambat. Pertama, overhead komputasional kira-kira sebanding dengan panjang nama yang diharapkan. Kedua, pada setiap level, algoritma pencarian perlu mencocokkan semua bagian luar node satu per satu untuk menemukan node anak untuk penurunan. Oleh

karena itu, arsitektur penerusan berdasarkan pohon awalan akan menyebabkan penundaan pencarian yang besar dan memengaruhi kinerja jaringan secara keseluruhan. Dibandingkan dengan pohon awalan, kecepatan pencarian tabel hash tidak terpengaruh oleh panjang nama dan ukuran entri, sehingga memiliki kemampuan beradaptasi yang lebih baik dalam jaringan skala besar. Namun, untuk mengatasi tabrakan hash, tabel hash juga perlu menyimpan nilai kunci penuh (yaitu, nama konten) dalam entri tabel, yang menimbulkan overhead penyimpanan yang besar. Pada saat yang sama, struktur tabel hash asli tidak mendukung algoritma pencocokan awalan terpanjang, dan implementasi linier yang paling sederhana memiliki waktu pencarian yang lama. Untuk mengatasi masalah ini, jaringan ICN yang ada biasanya menggunakan skema kompresi data seperti Hash Table berbasis footprint dan skema pengoptimalan algoritma seperti Random Search untuk meningkatkan skalabilitas sistem.

Secara umum, pengenal baru jauh lebih panjang daripada alamat IP, sehingga proses multi-pengenal akan menghadapi tekanan komputasi dan penyimpanan yang besar. Untuk tujuan ini, kami mengusulkan tabel hash dengan algoritma pohon awalan HPT, yang menambahkan entri semi-virtual ke pohon awalan. Skema ini mempercepat proses backtracking algoritma pencarian FIB dan secara efektif meningkatkan efisiensi penerjemahan dan pengalamatan multi-pengenal. Tabel hash digunakan untuk pencarian cepat, dan struktur pohon digunakan untuk menyimpan hubungan logis antara nama. Struktur utama FIB ditunjukkan pada Gambar 4.11.

Karakteristik FIB meliputi yang berikut:

(1) FIB terdiri dari tabel hash dan pohon awalan. Untuk nama apa pun yang disimpan dalam tabel, semua prefiks yang benar memiliki entri yang sesuai dalam tabel. Proses pemeriksaan keberadaan prefiks dan penambahan entri sekunder yang sesuai disebut pemfaktoran ulang FIB. Dalam FIB yang direkonstruksi, entri tabel dibagi menjadi entri riil dan entri non-riil, dan entri non-riil dibagi menjadi entri virtual dan entri semi-virtual.

(2) Dalam tabel hash, nama digunakan sebagai kunci, dan simpul dalam pohon prefiks digunakan sebagai nilai. Dengan cara ini, kita mewujudkan pengambilan informasi penerusan yang cepat.

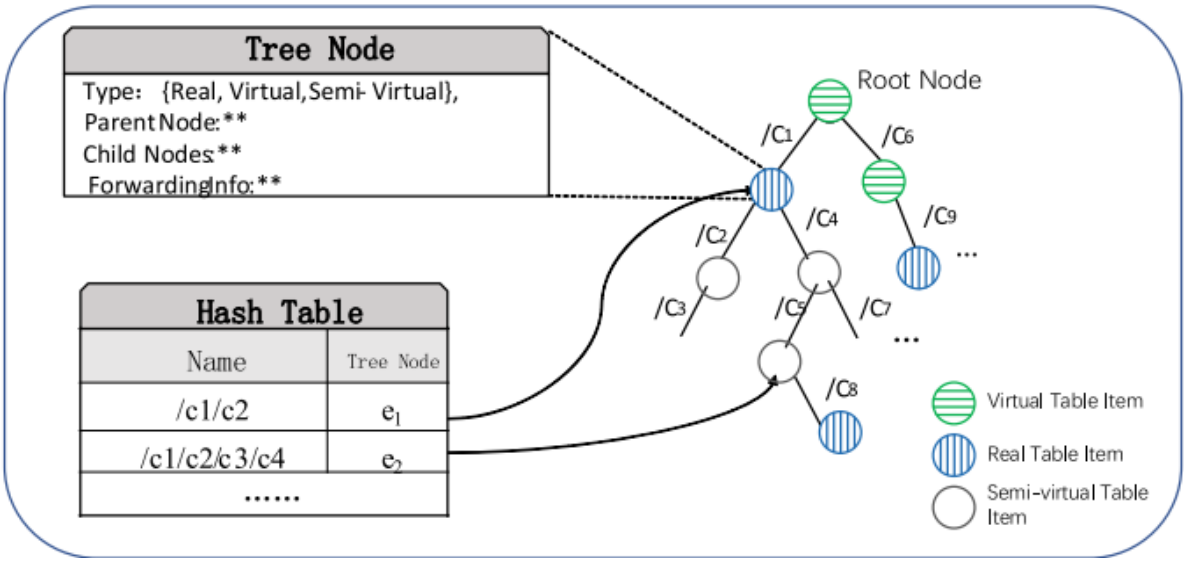
(3) Setiap sisi dalam pohon prefiks mewakili komponen nama. Setiap simpul dalam pohon prefiks mewakili nama yang menyimpan informasi penerusan yang sesuai dengan nama dan kategori entri tabel yang sesuai, serta Penunjuk untuk mempertahankan struktur pohon prefiks.

Definisi spesifik entri riil, entri non-riil, entri virtual, dan entri semi-virtual adalah sebagai berikut:

1. **Entri riil:** Nama-nama dalam entri riil merujuk ke data aktual dan digunakan untuk memandu penerusan paket-paket yang diminati. Sebelum pemfaktoran ulang FIB, semua entri tabel adalah riil.
2. **Entri non-riil:** Entri tambahan yang digunakan untuk mendukung algoritma pencarian acak disebut entri non-riil. Nama-nama dalam entri non-riil tidak merujuk ke data aktual apa pun dan tidak memandu penerusan paket-paket yang diminati.

3. **Entri virtual:** Entri non-riil dikatakan virtual jika tidak memiliki awalan riil. Ketika proses pencarian acak berakhir dengan entri virtual, proses tersebut berakhir secara langsung tanpa menghasilkan kesalahan negatif palsu apa pun.
4. **Entri semi-virtual:** Jika entri non-riil memiliki awalan riil, entri non-riil disebut entri semi-virtual dan memerlukan penelusuran balik.

Saat pengguna mendaftar dan menerbitkan sumber daya di MIN, beberapa pengenal terikat dengan sumber daya dan disimpan dalam MIS. Pengenal yang umum digunakan dan informasi antar-terjemahannya disimpan dalam HPT-FIB MIR. Jika MIR dapat meminta informasi terkait di HPT-FIB lokal, MIR akan langsung meneruskannya. Jika tidak, MIR akan memulai permintaan penerjemahan ke sistem MIS berdasarkan pengenal yang diberikan oleh pengguna. MIS mencari pengenal lain yang sesuai dengan pengenal ini, lalu memilih pengenal yang sesuai dan mengirimkannya ke MIR untuk pengalamatan. Penggunaan FIB adalah sebagai berikut.



Gambar 4.11 Struktur FIB

1. Penyisipan FIB

Pertama, kita harus menentukan apakah nama yang akan disisipkan dalam FIB ada. Jika ada, lakukan langkah penyisipan pertama (1); jika tidak, lakukan langkah penyisipan kedua (2). Langkah-langkah penyisipan ditunjukkan seperti di bawah ini.

Langkah-langkah penyisipan 1

Langkah 1: Tentukan apakah entri yang sesuai dengan nama tersebut adalah entri riil. Jika ada, perbarui informasi penerusannya; jika tidak, lakukan langkah 2.

Langkah 2: Tentukan apakah entri yang sesuai dengan nama tersebut adalah entri virtual. Jika ada, lakukan langkah modifikasi; jika tidak, lakukan langkah 3.

Langkah 3: Ubah semua entri virtual di pohon anak menjadi entri semi-virtual, lalu lakukan langkah 4, langkah Modifikasi.

Langkah 4: Ubah kategorinya menjadi entri riil dan tambahkan informasi penerusan.

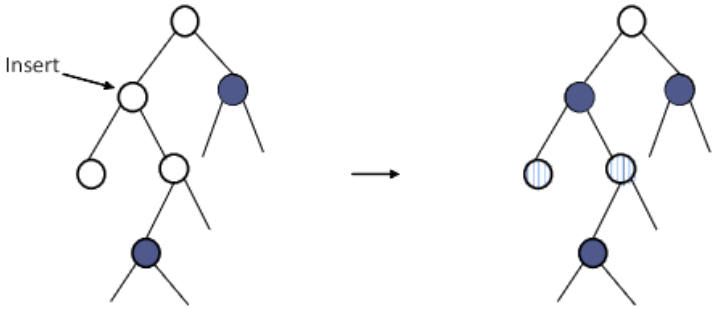
Singkatnya, pada langkah penyisipan pertama, jika nama yang akan disisipkan sudah memiliki entri yang sesuai di FIB, tidak ada masalah dengan menambahkan entri baru. Kasus entri riil itu sepele, jadi hanya entri non-riil yang dipertimbangkan. Kategori yang sesuai dimodifikasi menjadi riil. Jika entri awalnya virtual, entri virtual di sub-pohon perlu dimodifikasi menjadi semi-virtual. Jika entri awalnya semi-virtual, sub-pohon tidak perlu dimodifikasi.

Langkah-langkah penyisipan 2

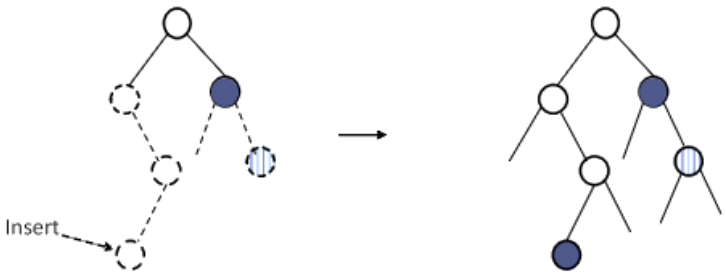
Pertama-tama, cari LPM dari nama yang akan disisipkan di FIB. Jika HIT riil, maka lakukan langkah pemrosesan pertama. Jika MISS atau HIT virtual, langkah pemrosesan kedua dilakukan.

Langkah 1: masukkan entri riil yang sesuai dengan nama, temukan semua awalan nama yang benar di FIB, dan masukkan entri semi-virtual yang sesuai jika tidak ada.

Langkah 2: masukkan entri nyata yang sesuai dengan nama tersebut, temukan semua awalan nama yang benar di FIB, dan masukkan entri virtual yang sesuai jika tidak ada.



(a) Case when there exists non-virtual entry for this name in table



(b) Otherwise

Gambar. 4.12 Langkah penyisipan FIB

Algorithm 4.4: Key inserting Algorithm

Input:
H: HT and trie-based FIB
n: $n = "/c1/c2/ .../cN"$ is the name to insert
f: the corresponding forwarding information of *n*
Output:
H: HT and trie-based FIB, with *n* inserted.
Begin

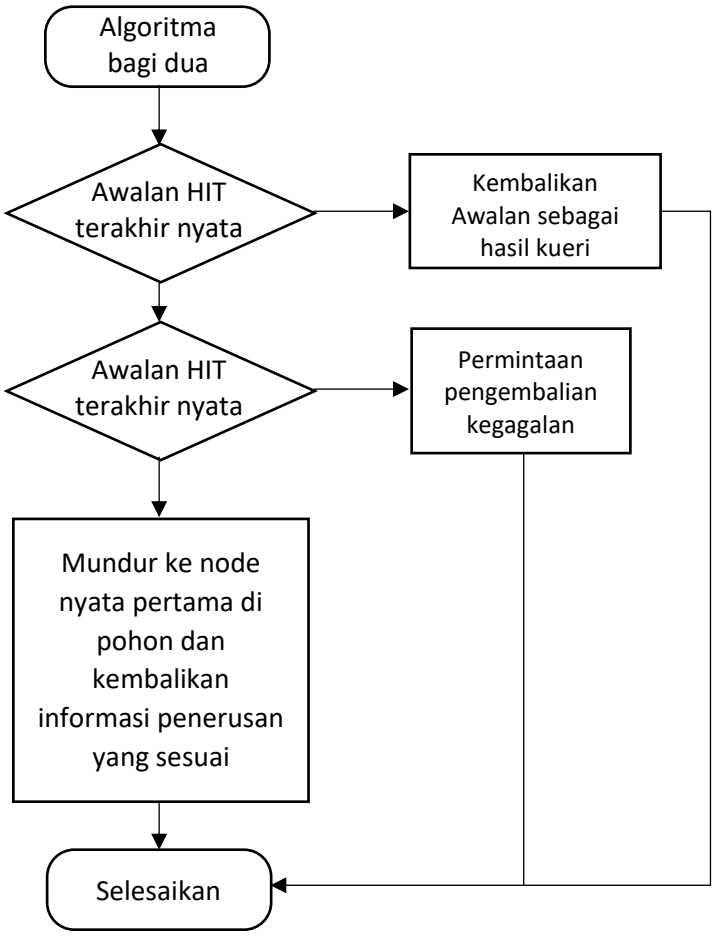
```
1:  lookup n in HT
2:  if n is the name of a real entry (n, e) then
3:      update e's forwarding information with f
4:  else if n is the name of a non-real entry (n, e) then
5:      /* as Fig. 4.13a */
6:      set e's type to real, e's forwarding information to f
7:      for each virtual entry (~, e*) in e's subtree do
8:          set e*'s type to semi-virtual
9:      end for
10: else
11:     /* as Fig. 4.13b */ create entry (n, eN) and insert it to HT
12:     set eN's type to real, eN's forwarding information to f
13:     for i = N − 1 to 1 do
14:     lookup ni ="/c1/c2/.../ci" in HT
15:         if ni is the name of an entry (ni, e) then
16:             add ei+1 to e's child list, set ei+1's parent to e
17:             if e is virtual then
18:                 set ej(i < j < N)'s type to virtual
19:             else
20:                 set ej(i < j < N)'s type to semi-virtual
21:             end if
22:             return
23:         else
24:             create entry (ni, ei) and insert it to HT
25:             add ei+1 to ei's child list, set ei+1's parent to ei
26:         end if
27:     end for
28:     add e1 to root's child list, set e1's parent to root
29:     set ej (0 < j < N)'s type to virtual
30: end if
```

End of Algorithm

Singkatnya, pada langkah kedua, jika nama yang akan dimasukkan tidak memiliki entri yang sesuai, entri riil yang sesuai dimasukkan. Pada saat yang sama, awalan diperiksa maju mundur untuk memastikan bahwa mereka ada di FIB. Jika awalan ditemukan tidak ada, entri non-riil yang sesuai dimasukkan. Proses ini berlanjut hingga algoritma mencapai LPM atau simpul akar, dan dengan demikian menentukan kategori simpul non-riil yang dimasukkan selama proses ini (Gambar 4.12).

2. Pencarian FIB

Proses pencarian algoritma FIB ditunjukkan sebagai Algoritma 4.5 dan Gambar 4.13. Port untuk meneruskan paket diperoleh dengan mencari nama paket yang diinginkan melalui algoritma pencarian acak. Algoritma pencarian acak dapat dipilih sesuai dengan permintaan, seperti pencarian biner tradisional.



Gambar 4.13 Langkah-langkah pencarian FIB

Ada tiga pola berdasarkan kategori entri HIT terakhir:

(1) Jika entri tersebut adalah entri riil, pencarian LPM berhasil, dan mengembalikan informasi yang sesuai.

(2) Jika entri tersebut adalah entri virtual, dapat dipastikan bahwa tidak ada awalan riil yang cocok dalam tabel, jadi kembali tanpa kecocokan.

(3) Jika entri tersebut adalah entri semi-virtual, setidaknya ada satu awalan riil yang cocok dalam tabel. Kita dapat menelusuri kembali pohon awalan untuk menemukan awalan riil yang cocok dan mengembalikannya. Karena menelusuri kembali pohon awalan tidak melibatkan pencarian, proses ini memiliki overhead waktu yang minimal.

Seperti yang ditunjukkan pada Gambar 4.14, awalan HIT terakhir dari pencarian biner untuk nama “/c1/c2/c3/c6/c7” adalah “/c1/c2/c3”, yang merupakan entri tabel semi-virtual yang mengarah ke proses penelusuran kembali. Algoritme dimulai dari “/c1/c2/c3” untuk kembali ke belakang hingga menemukan entri riil pertama “/c1”, lalu mengembalikan informasi maju yang sesuai.

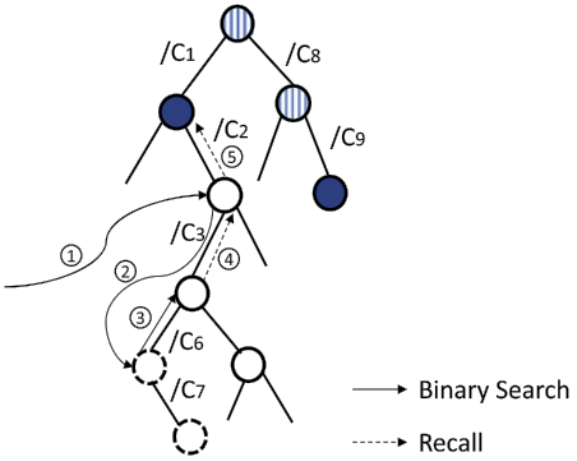
Algorithm 4.5: Searching Algorithm

Input:
H: HT and trie-based FIB.
n: *n* = *"/c1/c2/.../cN"* is the search key.
Output:
f: the forwarding information of *n*'s LPM entry
Begin

```
1:    /* Binary Search */
2:    L=1, H=N
3:    e_LPM = root
4:    while L≤H do
5:       M=(L+H)/2
6:       lookup n_M ="/c1/c2/.../cM" in HT
7:       if n_M is the name of an entry (n_M, e) in table then
8:          L=M+1, e_LPM=e
9:       else
10:         H=M−1
11:      end if
12:   end while
13:   if e_LPM is virtual then
14:      return NO FOUND
15:   else
16:      /* As Fig. 4.14 */
17:      while e_LPM is not real do
18:         e_LPM = e_LPM's parent
19:      end while
20:      return e_LPM's forwarding information
21:   end if
```

End of Algorithm

Jadi, ada dua jenis hasil pencarian. Satu adalah HIT, yang berarti ada entri riil yang sesuai di HPT FIB (yaitu, entri HIT terakhir adalah entri riil atau entri semi-virtual). Yang lainnya adalah MISS, yang berarti entri riil yang sesuai tidak ada (yaitu, entri HIT terakhir adalah virtual).



Gambar 4.14 Proses pencarian FIB

3. Menghapus FIB

Langkah penghapusan FIB digunakan untuk menemukan dan mengambil entri non-riil yang sudah kedaluwarsa. Pertama, tentukan apakah ada simpul anak dalam entri terkait nama yang akan dihapus di FIB. Jika ada, lakukan langkah penghapusan pertama; jika tidak, lakukan langkah penghapusan kedua.

Algorithm 4.6: Deleting Algorithm

```
Input:
   H: HT and trie-based FIB.
   n: n = "/c1/c2/.../cN" is the name to delete.
Output:
   H: HT and trie-based FIB, with n deleted.
Begin
1:    lookup n in HT,
2:    if n is not the name of a real entry then
3:       return
4:    end if
5:    if for n's entry (n, e), if e is not a leaf then
6:       set e's forwarding information to N/A
7:       if e's parent is semi-virtual or real then
8:          set e's type to semi-virtual
9:       else
10:         /* As Fig. 4.15a, here uses BFS */
11:         create an empty queue q and insert e into it
12:         while q is not empty do
13:            e* = q.pop()
14:            set e*'s type to virtual
15:            insert all e*'s semi-virtual child nodes into q
16:         end while
17:      end if
18:   else
19:      /* As Fig. 4.15b */
20:      remove e from its parent's child list
21:      delete entry (n, e) in HT
22:      for i = N − 1 to 1 do
23:         for ni ="/c1/c2/.../ci" and its entry (ni, ei)
24:         if ei is non-real and ei' is a leaf then
25:            remove ei from its parent's child list
26:            delete entry (ni, ei) in HT
27:         else
28:            return
29:         end if
30:      end for
31:   end if
End of Algorithm
```

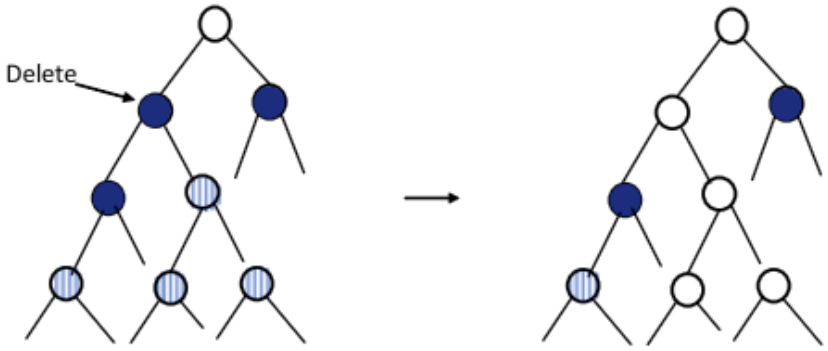
(1) *Langkah penghapusan pertama:* tentukan apakah simpul induk dari entri terkait bersifat virtual. Jika virtual, maka jalankan sub-langkah penghapusan pertama. Jika

simpul induk dari entri terkait bersifat nyata atau semi-virtual, ubah kategori entri nama menjadi semi-virtual.

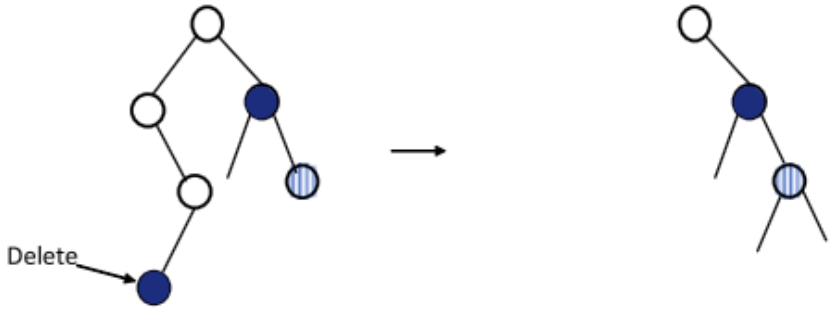
- Sub-langkah penghapusan pertama: Ubah kategori entri terkait nama menjadi virtual, lalu telusuri sub-pohon dengan nama sebagai akar. Jika salah satu simpul memenuhi syarat pertama (kategori bersifat semi-virtual) dan syarat kedua (tidak ada simpul riil pada jalur dari simpul ke namanya), maka kategori simpul tersebut diubah menjadi virtual.

(2) *Langkah penghapusan kedua:* Menghapus entri, lalu memeriksa semua awalan nama yang benar ke atas, langkah demi langkah. Jika simpul awalan yang sesuai memenuhi titik pertama (kelas tidak riil) dan titik kedua (simpul daun), maka hapus entri tersebut.

Melalui langkah penghapusan, kategori entri non-nyata dapat dijaga kebenarannya dalam lingkungan dinamis, dan entri non-nyata yang kedaluwarsa dapat ditemukan dan dipulihkan tepat waktu, sehingga dapat memastikan efisiensi dan stabilitas bidang penerusan (Gambar. 4.15).



(a) Case when name to delete is not leaf and has virtual parent



(b) Case when name to delete is leaf

Gambar 4.15 Proses penghapusan FIB

Percobaan kami menunjukkan bahwa struktur data penerusan FIB yang menggabungkan pohon awalan dengan algoritma hash dapat mendukung penyimpanan dan pencarian awalan nama berskala besar, seperti yang ditunjukkan pada Tabel 4.4.

HPT-FIB memiliki overhead penyimpanan yang signifikan ketika skala jaringan semakin meluas. Oleh karena itu, kami mengusulkan model Perutean Hiperbolik (HR) 3D alih-alih tabel

penerusan untuk mengurangi overhead penyimpanan di MIR. MIN dipetakan ke ruang hiperbolik 3D, kemudian MIR dan semua konten diberi koordinat bola 3D. Dalam HBR, MIR hanya menggunakan algoritma greedy untuk memilih MIR sebagai hop berikutnya dengan jarak hiperbolik terkecil dari tujuan untuk penerusan. Pendekatan ini secara signifikan mengurangi overhead penyimpanan MIR.

Entri HPT-FIB dari sistem ini lebih dari satu miliar, dan kecepatan pencarian mendekati log(log(N)), di mana N adalah jumlah pengenal. Desain ini sepenuhnya memecahkan masalah kesalahan negatif palsu dalam algoritma yang ada. Selain itu, MIR dapat mendeteksi dan menghapus entri tabel yang usang tepat waktu, sehingga meningkatkan efisiensi pemulihan memori.

Tabel 4.4 Hubungan antara waktu dan skala FIB

Skala FIB	100 juta	1 miliar	2 miliar	2,5 miliar	3 miliar	3,5 miliar
Waktu berjalan (Detik)	187,58	1649.75	3723,98	4925,64	6271,49	7760,69
Skala FIB aktual	100 juta	1 miliar	2 miliar	2,5 miliar	3 miliar	3,5 miliar

4.4 SKEMA AUTENTIKASI IDENTITAS BERBASIS IDENTITAS ASLI DAN BIOMETRIK

Autentikasi identitas pengguna jaringan kedaulatan didasarkan pada karakteristik biologis manusia, dan dikombinasikan dengan teknologi blockchain sebagai skema manajemen identitas terdesentralisasi. Fungsi autentikasi pengguna mengidentifikasi identitas pengguna secara akurat, dan menyimpan informasi terkait ke dalam blockchain, untuk memastikan integritas dan konsistensinya. Selain itu, dikombinasikan dengan skema manajemen identitas blockchain, ia juga mewujudkan desentralisasi autentikasi sertifikat pihak ketiga dan lembaga penghasil. Melalui skema enkripsi paling canggih, skema yang diusulkan secara efektif melindungi privasi informasi identitas pengguna.

4.4.1 Pengenalan Karakteristik Biologis Pengguna

1. Iris

Iris adalah daerah melingkar antara pupil dan sklera putih pada permukaan mata manusia. Dalam cahaya inframerah dekat, iris menyajikan tekstur yang kaya, seperti bintik-bintik, garis-garis, filamen, korona, dan kripta. Teknologi pengenalan iris diadopsi dalam autentikasi identitas dengan membandingkan kesamaan antara fitur gambar iris. Langkah inti adalah mendeskripsikan, mencocokkan, dan mengklasifikasikan fitur iris mata manusia melalui pengenalan pola, pemrosesan gambar, dan metode lainnya, sehingga dapat mewujudkan autentikasi identitas manusia secara otomatis.

Karakteristik iris tercantum sebagai berikut:

(1) Keunikan. Menurut penelitian fisiologis, tekstur iris yang terperinci ditentukan oleh faktor acak dari lingkungan perkembangan embrio. Distribusi acak dari detail tekstur meletakkan dasar fisiologis bagi keunikan iris. Gambar-gambar tersebut sangat berbeda bahkan ketika iris mata kiri dan kanan orang yang sama atau kembar. Oleh karena itu, hampir mustahil untuk menemukan dua iris yang identik di alam.

(2) Stabilitas. Iris mulai tumbuh pada bulan ketiga periode embrio bayi. Pada bulan kedelapan, tekstur utamanya telah terbentuk. Di sisi lain, karena perlindungan kornea, iris yang berkembang sepenuhnya kurang rentan terhadap kerusakan eksternal. Oleh karena itu, hampir mustahil iris berubah karena kontak fisik eksternal. Para ilmuwan telah menemukan bahwa tekstur iris hampir tetap konstan sepanjang hidup, kecuali operasi yang dapat membahayakan mata.

(3) Nonkontak. Iris adalah organ internal yang terlihat dari luar, yang pengumpulan fiturnya lebih higienis dan nyaman daripada fitur biologis yang perlu disentuh. Ini sangat berbeda dari organ eksternal seperti sidik jari dan gambar wajah. Gambar iris yang berkualitas dapat diperoleh melalui perangkat pengumpulan tanpa kontak (atau bahkan jarak jauh). Ini sangat nyaman dalam aplikasi praktis.

(4) Kapasitas besar. Akuisisi tekstur iris yang jelas memerlukan kerja sama perangkat dan pengguna khusus, sehingga sulit untuk mencuri gambar iris, dibandingkan dengan sidik jari dan wajah. Selain itu, mata juga memiliki banyak karakteristik optik dan fisiologis yang sangat baik, yang dapat digunakan untuk mendeteksi iris secara in vivo.

Proses pengenalan iris meliputi akuisisi gambar iris, praproses gambar iris, ekstraksi dan perbandingan fitur, dan pengenalan identitas pengguna.

2. Pengenalan Wajah

Pengenalan wajah merupakan salah satu jenis teknologi biometrik yang berbasis pada informasi fitur wajah. Gambar atau aliran video yang berisi wajah diambil dengan kamera untuk mendeteksi dan melacak wajah secara otomatis. Rangkaian teknologi terkait tersebut umumnya dikenal sebagai pengenalan potret atau pengenalan wajah.

Solusi yang berkembang pesat meliputi pengenalan wajah multi-cahaya berbasis citra inframerah dekat aktif dan pengenalan wajah berbasis pembelajaran mesin. Pengenalan wajah multi-cahaya berbasis teknologi citra inframerah dekat aktif dapat mengatasi pengaruh perubahan cahaya dan meningkatkan kinerja pengenalan. Karena kinerja sistem dalam hal akurasi, stabilitas, dan kecepatan lebih unggul daripada pengenalan wajah citra 3D, teknologi ini telah berkembang pesat dalam dua atau tiga tahun terakhir, yang secara bertahap menjadikan teknologi pengenalan wajah sebagai aplikasi praktis.

Teknologi pengenalan wajah yang menggabungkan pembelajaran mesin didasarkan pada berbagai teori untuk membangun model pembelajaran dan basis data wajah, yang juga dapat mewujudkan pengenalan wajah presisi tinggi tanpa peralatan fisik khusus.

Serupa dengan fitur biologis lain dari tubuh manusia seperti sidik jari, iris, dll., wajah manusia bersifat bawaan. Sulit untuk ditiru dengan karakteristik yang unik, yang menyediakan prasyarat yang diperlukan untuk identifikasi.

Dibandingkan dengan biometrik lainnya, pengenalan wajah memiliki karakteristik berikut:

(1) Tidak wajib. Proses untuk memperoleh gambar wajah tidak mengharuskan pengguna untuk bekerja sama dengan peralatan akuisisi wajah, yang hampir tidak disadari. Metode pengambilan sampel seperti itu tidak "wajib".

(2) Tanpa kontak. Proses untuk memperoleh gambar wajah tidak mengharuskan pengguna untuk melakukan kontak langsung dengan perangkat.

(3) Konkurensi. Dalam skenario aplikasi praktis, beberapa wajah dapat disortir, dinilai, dan dikenali pada saat yang bersamaan.

Selain itu, pengenalan wajah juga sesuai dengan karakteristik "mengenali orang berdasarkan penampilan", serta menjamin pengoperasian yang sederhana, hasil yang intuitif, penyembunyian yang baik, dll. Sistem pengenalan wajah terutama terdiri dari empat bagian: modul akuisisi dan deteksi gambar wajah, modul praproses gambar wajah, modul ekstraksi fitur gambar wajah, modul pencocokan dan pengenalan.

3. Sidik jari

Sidik jari adalah garis-garis pada kulit di ujung depan jari. Garis-garis tersebut tersusun secara teratur untuk membentuk pola yang berbeda. Sidik jari hampir identik dengan identifikasi biometrik karena sifatnya yang tidak dapat diubah, unik, dan mudah digunakan.

Titik awal, titik akhir, titik sambungan, dan titik percabangan garis diteliti sebagai fitur terperinci dari sidik jari. Identifikasi sidik jari membandingkan fitur terperinci dari berbagai sidik jari. Teknologi pengenalan sidik jari menggabungkan teknologi pemrosesan gambar, teknologi pengenalan pola, teknologi visi komputer, morfologi matematika, analisis wavelet, dan banyak subjek lainnya. Sidik jari dapat digunakan untuk identifikasi karena sidik jari setiap orang berbeda meskipun sidik jari orang yang sama.

Keuntungan utama dari teknologi identifikasi sidik jari tercantum sebagai berikut.

(1) Sidik jari merupakan fitur unik dari tubuh manusia, dan cukup kompleks untuk menyediakan fitur identifikasi.
(2) Keandalan dapat ditingkatkan melalui pendaftaran dan identifikasi lebih banyak sidik jari dari berbagai sidik jari. Hingga sepuluh sidik jari dapat diambil, dan setiap sidik jari bersifat unik.
(3) Kecepatan pemindaian sidik jari sangat cepat, dan sangat nyaman digunakan.
(4) Saat membaca sidik jari, pengguna harus langsung menyentuh mesin pengambil sampel sidik jari dengan sidik jarinya.
(5) Kontak langsung dengan mesin pengambil sampel sidik jari merupakan metode yang paling andal untuk mengumpulkan karakteristik biologis manusia.
(6) Mesin pengambil sampel sidik jari lebih kecil dan lebih murah daripada mesin pengambil sampel lainnya. Yang terpenting, adopsi informasi biometrik dapat sangat meningkatkan keandalan identifikasi pengguna dan secara signifikan mengurangi kemungkinan informasi fitur pengguna dicuri.

4.4.2 Pengenalan Setiap Modul

Dalam jaringan kedaulatan, sistem autentikasi berdasarkan identitas asli dan karakteristik biometrik mencakup tiga modul: rantai identitas, modul Manajemen Konten (CM), klien jaringan kedaulatan, dan terminal genggam.

1. Rantai Identitas

Rantai identitas menggunakan blockchain berdasarkan konsensus PoV sebagai sistem penyimpanan dasar untuk menyimpan informasi identitas pengguna, kunci publik, dan bagian dari informasi identitas terenkripsi. Informasi identitas mengacu pada simbol yang dapat dipetakan secara individual ke pengguna unik tertentu, seperti sertifikat yang relevan, sidik

jari, gambar iris, dan informasi wajah. Bergantung pada persyaratan skenario dengan kebutuhan keamanan tinggi, peta lokasi penyimpanan di luar rantai dapat ditulis di blok, yang menggunakan skema penyimpanan di luar rantai yang aman untuk menyimpan informasi identitas yang ditolak untuk diungkapkan oleh pengguna.

Rantai identitas juga menyediakan klien untuk menanyakan informasi identitas. Klien jaringan kedaulatan atau modul CM memperoleh informasi identitas yang sesuai dengan klien ini.

2. Modul CM

Modul CM bertanggung jawab untuk menyelesaikan operasi pengguna, seperti menambahkan, menghapus, memodifikasi, mencari, dll., serta bisnis tertentu, seperti pendaftaran, login, logout, modifikasi, dan penghapusan informasi identitas. Berbagai desain diadopsi untuk melindungi privasi dan hak pengguna. Penambahan dan penghapusan pengguna dilakukan tanpa otorisasi pengguna, sedangkan modifikasi dan permintaan informasi pengguna memerlukan persetujuannya. Faktanya, klien perlu membuat Token Akses yang sesuai atau kunci perantara dalam teknologi enkripsi ulang untuk menunjukkan izin pengguna yang diperoleh.

Selama proses pendaftaran, modul CM menyetujui sebagian informasi pengguna. Setelah disetujui, ringkasan ditandatangani dan dikembalikan ke klien. Sementara itu, sebagai verifier dalam skema manajemen identitas, modul CM memanggil rantai identitas klien untuk menulis dan meminta identitas. Selain itu, CM merangkum antarmuka biologis pihak ketiga dan berfungsi sebagai server untuk autentikasi karakteristik biologis. Karena beragamnya metode autentikasi biologis yang diusulkan dalam jaringan kedaulatan, modul CM menentukan metode autentikasi mana yang digunakan pengguna untuk login.

3. Klien Jaringan Kedaulatan dan Terminal Genggam

Klien bertanggung jawab untuk mengumpulkan dan memelihara informasi perangkat keras dan perangkat lunak yang sesuai, dan terminal genggam menggunakan antarmuka fasilitas verifikasi biologis dalam bentuk APP untuk mengumpulkan data inisialisasi dan informasi biologis selama verifikasi. Terminal genggam mengadopsi sistem Android untuk mengembangkan aplikasi Android dan aplikasi autentikasi identitas yang sesuai untuk klien jaringan kedaulatan.

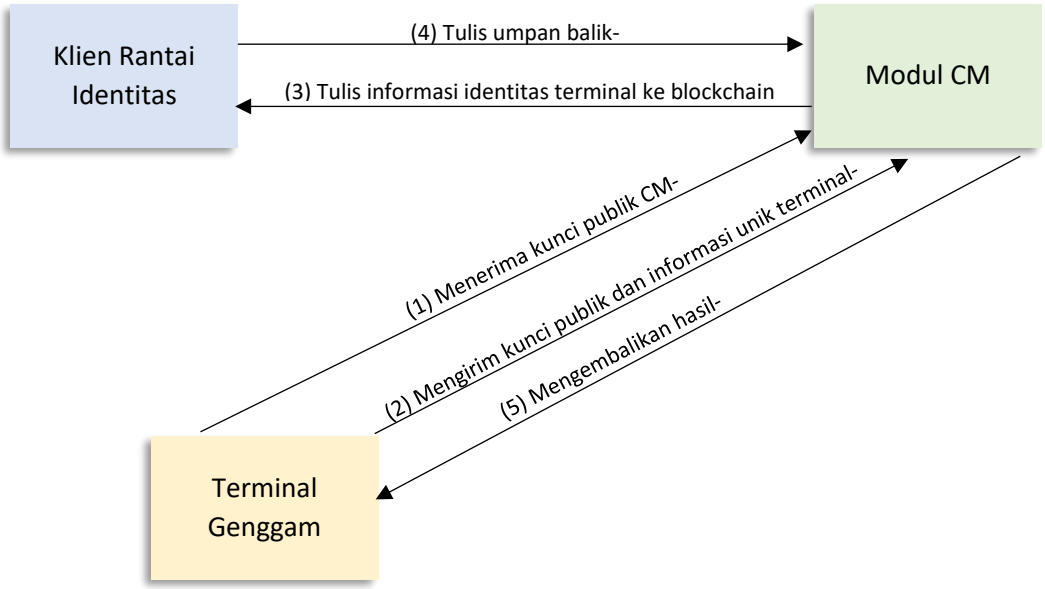
Selain itu, selama pendaftaran, Kriptografi Kurva Eliptik (ECC) diadopsi di klien untuk menghasilkan pasangan kunci publik dan privat yang sesuai, dan kemudian mengeluarkan permintaan setelah persetujuan CM. Kunci publik persetujuan, informasi klien, dan informasi identitas ditulis ke rantai identitas. Kemudian teknologi kode penghapusan digunakan oleh klien untuk membagi kunci privat menjadi n blok, yang masing-masing akan disimpan pada perangkat tepercaya. Saat memulihkan kunci privat, m blok diminta dari perangkat yang sesuai untuk mendekode kunci privat lengkap. Dengan cara ini, MIN meningkatkan stabilitas penyimpanan kunci pribadi dengan overhead penyimpanan yang rendah.

4.4.3 Skenario Aplikasi

1. Otorisasi Terminal Genggam

Seperti yang ditunjukkan pada Gambar 4.16, proses otorisasi terminal genggam adalah sebagai berikut:

(1) Perangkat end-host mengirimkan permintaan ke CM untuk mendapatkan kunci publik CM.
(2) End-host membuat kunci publik dan privat serta informasi unik, lalu mengenkripsi informasi dengan kunci publik CM dan mengirimkan permintaan ke CM.
(3) CM menulis informasi identitas perangkat ke dalam blockchain.
(4) Blockchain mengembalikan umpan balik berupa informasi tertulis.
(5) CM mengembalikan hasilnya ke end-host.



Gambar. 4.16 Otorisasi host akhir

2. Pendaftaran Pengguna

Seperti yang ditunjukkan pada Gambar 4.17, proses pendaftaran pengguna adalah sebagai berikut:

(1) Klien pertama-tama mengirimkan permintaan untuk kunci publik CM.
(2) Informasi yang relevan (misalnya, nama, nomor akun, nomor ID, dll.) disediakan dari layar pendaftaran klien, dan gambar iris dimasukkan melalui perangkat pengambilan sampel iris. Klien kemudian membuat pasangan kunci publik dan kunci privat. Kunci privat dikodekan menjadi n bagian dengan kode penghapusan (n dikonfigurasi oleh staf operasi), dan disimpan dalam perangkat tepercaya. Perlu disebutkan bahwa MIN akan menyediakan disk lokal untuk menyimpan kunci privat jika pengguna tidak menyediakan peralatan apa pun.
(3) Setelah klien mengenkripsi gambar iris dengan kunci publiknya diikuti dengan tanda tangan yang dibuat oleh kunci privat, klien menggunakan kunci publik CM untuk

mengenkripsi ciphertext gambar iris lagi dan mengirimkannya ke server CM. Setelah server CM menerima informasi pendaftaran yang dikirimkan oleh klien, klien mengembalikan tautan untuk mengirimkan informasi biometrik pengguna ke klien.

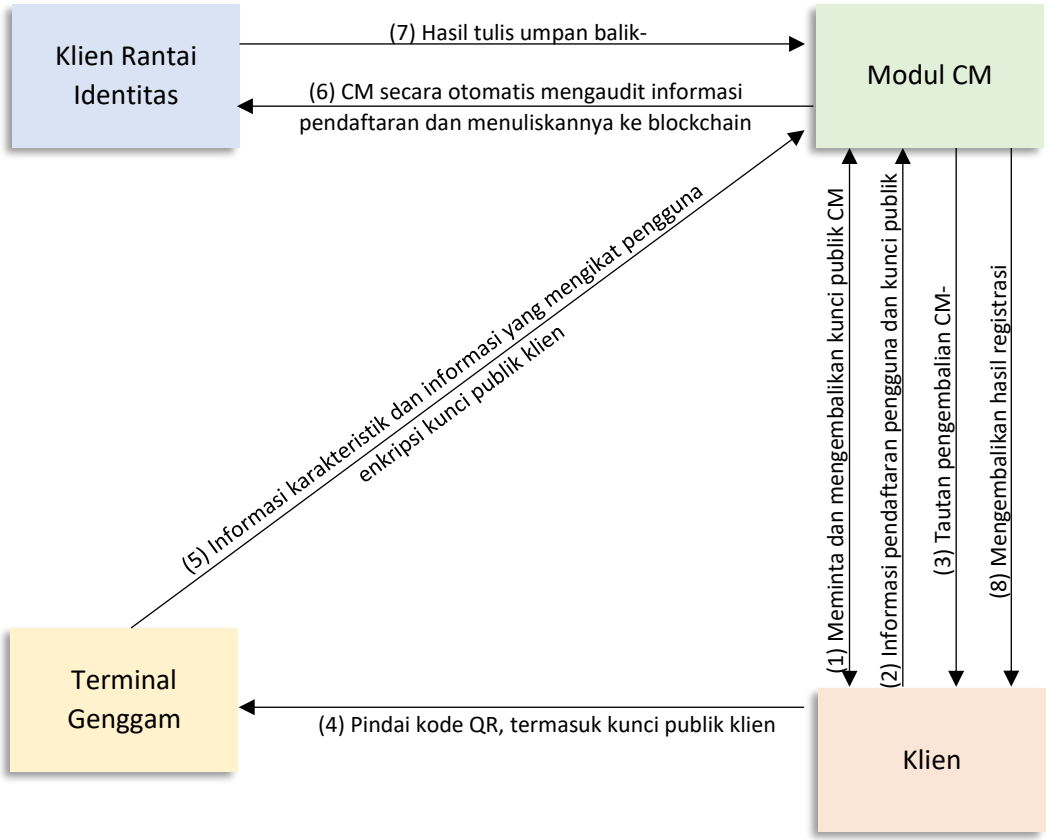
(4) Klien membuat kode Respons Cepat (QR) yang sesuai dan mengirimkannya ke terminal genggam. Kode QR berisi kunci publik klien yang diikat dengan klien oleh pengguna.

(5) Pengguna memindai kode QR dengan terminal genggam untuk masuk dengan informasi identitas, dan mengumpulkan sidik jari, wajah, dan informasi lainnya. Setelah semua tanda terkumpul, maka tanda-tanda tersebut dienkripsi menggunakan kunci publik CM dan dikirim ke server CM bersama informasi terenkripsi lainnya.

(6) Informasi registrasi yang diterima oleh server CM secara otomatis disetujui oleh sistem. Jika validasi lolos, CM akan menyimpan informasi identitas ke dalam blockchain.

(7) Blockchain memberikan umpan balik hasil kepada CM.

(8) CM mengembalikan informasi kepada klien tentang apakah registrasi berhasil atau tidak.

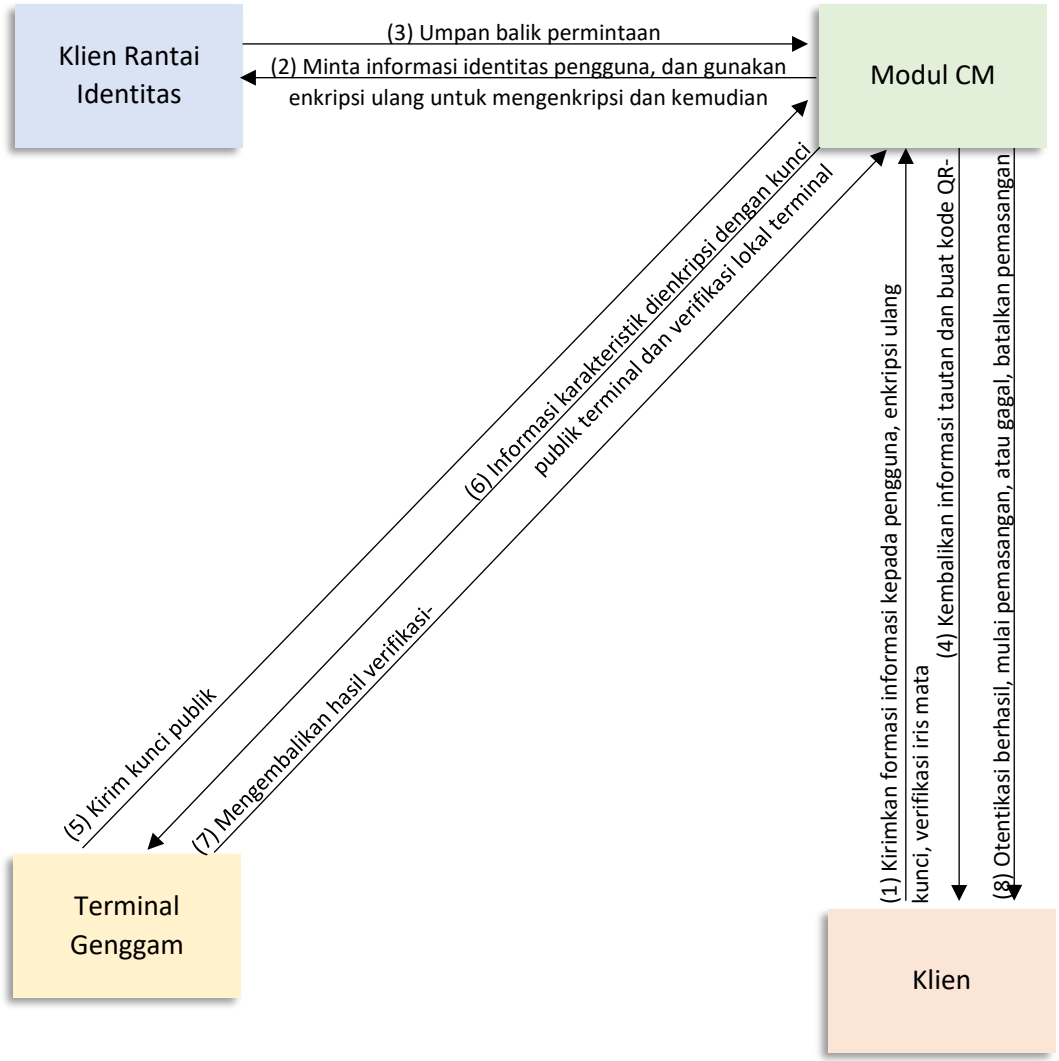


Gambar 4.17 Proses registrasi pengguna

3. Login Pengguna

Seperti yang ditunjukkan pada Gambar 4.18, proses login pengguna adalah sebagai berikut:

(1) Pengguna memasukkan nama pengguna dan kata sandi. Kemudian klien menggunakan kunci privatnya dan kunci publik CM untuk membuat kunci enkripsi ulang. Kunci enkripsi ulang tidak dapat digunakan untuk membalikkan kunci privat pengguna dan kunci publik CM, tetapi dapat didekripsi dengan kunci privat CM.
(2) Klien menggunakan kunci publik CM untuk mengenkripsi nama pengguna, kata sandi, kunci enkripsi ulang, dan informasi perangkat keras serta perangkat lunak, lalu mengirimkan teks sandi ke CM.
(3) Modul CM mencari informasi terkait pada blockchain sesuai dengan ID pengguna. Hasil kueri dikirim ke CM dan disimpan dalam cache setelah didekripsi dengan kunci pribadi CM.
(4) Modul CM mengirimkan tautan verifikasi fisik ke klien sesuai dengan kebijakan yang ditetapkan oleh administrator. Kemudian klien membuat kode QR.
(5) Terminal genggam memindai kode QR dan mengirimkan kunci publik serta informasi pengikatannya ke CM.
(6) CM mengenkripsi informasi fitur dengan kunci publik terminal genggam dan mengembalikannya ke terminal genggam, yang mengautentikasi karakteristik biometrik seperti sidik jari, wajah, dan iris.
(7) Terminal genggam mengirimkan hasil umpan balik autentikasi ke modul CM.
(8) Jika autentikasi berhasil, CM mengirimkan pemberitahuan untuk mengizinkan klien memasang sistem berkas. Jika tidak, proses masuk gagal. Proses pemasangan sama dengan proses pemasangan NFS.



Gambar 4.18 Proses login pengguna

4. Modifikasi dan Penghapusan Informasi Identitas Pengguna

(1) Modifikasi informasi pengguna.

- Jika pengguna perlu memasukkan kembali informasi biologis, prosesnya mirip dengan proses pendaftaran.
- Jika pengguna perlu mengubah informasi biologis, klien akan mengirimkan informasi terkait ke modul CM, dan CM akan menulis ulang informasi identitas yang diperbarui pada blockchain.

(2) Penghapusan informasi pengguna. Menurut ID pengguna, modul CM menulis informasi yang mewakili perilaku penghapusan ke blockchain.

4.5 PERLINDUNGAN PRIVASI DAN MANAJEMEN JARINGAN

Jaringan penyiaran digunakan sebagai contoh aplikasi jaringan kedaulatan, yang perlu melindungi privasi pengguna saat mengelola pengguna. Oleh karena itu, jaringan kedaulatan memperkenalkan teknologi blockchain, teknologi enkripsi asimetris, strategi perlindungan privasi, dan teknologi lainnya.

Selain teknologi di atas, jaringan kedaulatan menyiapkan visa elektronik. Ketika pengguna subnet kedaulatan ingin mengakses konten subnet kedaulatan lain, ia perlu mengajukan visa elektronik untuk subnet kedaulatan target. Akses ke sumber daya di subnet kedaulatan hanya dimungkinkan dengan informasi visa.

4.5.1 Jaringan Visa Elektronik Kedaulatan

Setiap negara secara independen membangun jaringan kedaulatannya sendiri dan memiliki otonomi penuh. Untuk mengakses konten web kedaulatan suatu negara, pengguna di negara lain harus terlebih dahulu mengajukan visa elektronik, lalu membawa visa yang berhasil diajukan untuk kunjungan tersebut. Pada saat yang sama, negara tersebut dapat mengendalikan izin visa dan merancang aturan akses untuk konten, seperti melarang pengguna asing mengaksesnya. Dengan cara ini, dunia maya sesuai dengan kenyataan, seperti kebiasaan Internet. Dunia maya tidak hanya dapat mewujudkan akses bersama antarnegara, tetapi juga mengelola dan mengendalikan perilaku akses. Lihat Bab 5.4.2 untuk deskripsi terperinci tentang perolehan sertifikat dan akses ke konten jaringan melalui sertifikat.

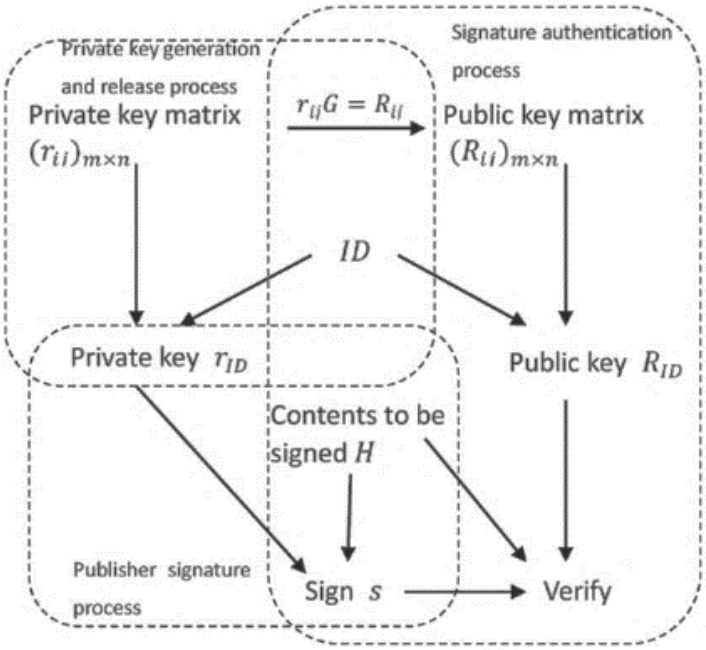
4.5.2 Enkripsi Asimetris

Arsitektur jaringan yang berpusat pada konten yang ada biasanya menggunakan "nama yang dapat diverifikasi" untuk permintaan data. Dengan kata lain, setiap nama harus berisi bagaimana kunci publik penerbitnya diperoleh, serta tanda tangan penerbit atas nama dan konten tersebut. Sebelum pesan data di-cache oleh simpul perutean atau diterima oleh peminta, informasi tanda tangannya harus diverifikasi untuk memastikan integritas, keamanan, dan keandalan nama dan konten.

Ada permintaan kunci publik yang sering terjadi di jaringan. Untuk menghemat sumber daya pita lebar dan mengurangi tekanan transmisi jaringan, jaringan kedaulatan mengadopsi skema pembuatan kunci publik dan privat berdasarkan identifikasi identitas dan matriks kombinasi. Skema tersebut dijelaskan secara singkat sebagai berikut: Kriptografi yang kami adopsi adalah Kriptografi Kurva Eliptik (ECC). Dalam ECC, jika titik dasar G pada kurva eliptik dan orde n-nya diberikan, bilangan bulat positif $r < n$ adalah kunci privat, dan titik r dikali G $rG = R$ digunakan sebagai kunci publik. Mudah untuk menghitung R dengan (R, G), tetapi tidak layak secara komputasi untuk menyelesaikan r dengan (R, G) karena masalah logaritma diskrit kurva eliptik sulit. Matriks kunci privat $\left(r_{ij}\right)_{m\times n}$ berorde $m \times n$, di mana setiap elemen rr$_{ij}$ adalah bilangan bulat positif yang memenuhi $r_{ij} < n$. Matriks kunci publik $\left(R_{ij}\right)_{m\times n}$ dapat dihasilkan oleh relasi yang sesuai $r_{ij}G = R_{ij}$ Matriks kunci privat hanya dipegang oleh otoritas manajemen kunci dan digunakan untuk distribusi kunci privat pengguna. Matriks kunci publik dipegang oleh setiap simpul jaringan dan digunakan untuk autentikasi tanda tangan data.

Seperti yang ditunjukkan pada Gambar 4.19, lembaga manajemen kunci menghasilkan kunci privat pengguna r_{ID} dengan ID identitas pengguna dan matriks kunci privat (r_{ij}) .

Misalnya, pembuatan kunci privat dapat diimplementasikan dengan cara berikut. Melalui chip kriptografi dan kriptografi, setiap ID identitas dapat secara unik menghasilkan urutan, seperti yang ditunjukkan di bawah ini.



Gambar 4.19 Proses pembuatan kunci privat

$$GenerateSub(ID) = \{i_1, i_2, \ldots, i_l, j_1, j_2, \ldots, j_l\} \qquad (4.10)$$

Kunci pribadi yang sesuai dengan ID adalah jumlah item yang sesuai dalam matriks kunci pribadi:

$$r_{ID} = r_{i_1 j_1} + r_{i_2 j_2} + \cdots + r_{i_l j_l} \qquad (4.11)$$

Demikian pula, kunci publik yang sesuai dengan ID dapat dihitung oleh verifier menggunakan matriks kunci publik dan ID identitas.

$$R_{ID} = R_{i_1 j_1} + R_{i_2 j_2} + \cdots + R_{i_l j_l} \qquad (4.12)$$

Karena beberapa titik G membentuk grup pertukaran,

$$\begin{aligned} r_{ID}G &= \left(r_{i_1 j_1} + r_{i_2 j_2} + \ldots r_{i_l j_l}\right)G \\ &= r_{i_1 j_1}G + r_{i_2 j_2}G + \ldots r_{i_l j_l}G \\ &= R_{i_1 j_1} + R_{i_2 j_2} + \ldots R_{i_l j_l} \\ &= R_{ID} \end{aligned} \qquad (4.13)$$

Oleh karena itu, (r_{ID}, R_{ID}) merupakan hubungan pasangan kunci publik-pribadi. Dengan cara ini, pemetaan satu-satu antara identitas dan kunci publik selesai, yang memastikan pengawasan dan keterlacakan perilaku jaringan. Di sisi lain, metode yang diusulkan dapat menghindari permintaan kunci publik yang sering dan meningkatkan kinerja jaringan.

4.5.3 Kebijakan Pelestarian Privasi

Ketika semua terminal pengguna meminta jaringan untuk mendaftarkan pengenal identitas, mereka perlu mengikat informasi identitas yang sesuai untuk memastikan operasi dan pemeliharaan jaringan yang normal. Pengguna membuat sertifikat identitas dengan

fungsi hash tertentu dan informasi identitas pengguna. Sistem mengirimkan kunci publik pengguna ke simpul pengawas. Pengguna menandatangani permintaan pendaftaran identitas dengan sertifikat identitasnya sendiri dan mengirimkannya ke simpul pengawasan bersama dengan permintaan pendaftaran identitas. Setelah permintaan pendaftaran identitas diterima, simpul pengawas pertama-tama menggunakan fungsi hash yang sama untuk memverifikasi keabsahan pengguna, lalu menggunakan kunci publik pengguna untuk mendekripsi tanda tangan tambahan. Simpul pengawas membandingkan dua nilai hash. Jika keduanya sama, maka tanda tangan dapat dibuktikan berasal dari pengguna, dan permintaan pendaftaran identitas dikonfirmasi oleh simpul pengawas. Jaringan kedaulatan menyimpan sertifikat identitas pengguna dalam basis data terdistribusi, memastikan bahwa identitas dapat dilacak dan dipantau nanti. Pada saat yang sama, jaringan kedaulatan mengharuskan semua identitas harus didaftarkan sebelum dapat dirutekan melalui jaringan. Selain itu, informasi identitas penerbit harus ditambahkan saat identitas didaftarkan, yang secara efektif dapat mengurangi penyebaran konten terlarang ilegal di jaringan, termasuk tetapi tidak terbatas pada web gelap jaringan IP tradisional dan data privasi pribadi. Penyaringan konten terlarang dapat lebih melindungi privasi pengguna.

Jaringan kedaulatan juga memperkenalkan kebijakan manajemen izin. Konten yang diposting oleh pengguna akan dinilai. Saat pengguna mengakses sumber daya jaringan, hak akses dapat ditentukan berdasarkan informasi identitas mereka. Hal ini dapat membantu administrator menerapkan manajemen pengguna, seperti membatasi waktu online dan bermain game harian bagi siswa dan kelompok tertentu lainnya. Klasifikasi konten Internet dapat secara efektif melindungi kesehatan fisik dan mental anak di bawah umur dan mendorong pengembangan konten Internet yang wajar dan patuh.

4.6 SISTEM KESADARAN SITUASI KEAMANAN

Selain mekanisme keamanan internal jaringan kedaulatan, untuk lebih menjamin keamanan dan pengendalian, kami hadir dengan sistem kesadaran situasi keamanan. Sistem ini menerobos masalah persepsi keamanan multi-platform untuk bekerja di berbagai jaringan, dan mengadopsi berbagai teknologi untuk mempertahankan dan meningkatkan akurasi dan perluasan. Secara khusus, sistem kesadaran situasi keamanan yang diusulkan juga digunakan pada MIR, yang menyatu dengan layanan persepsi dan perutean keamanan. Dengan cara ini, sistem kesadaran situasi keamanan tidak lagi sekadar peralatan deteksi bypass. Ia mengisolasi dan merekam paket berbahaya untuk pertama kalinya tanpa campur tangan manusia. Setelah mendeteksi, perilaku berbahaya dan informasi pengguna terkait akan secara otomatis dikirimkan ke sistem MIS, kemudian sistem MIS akan secara otomatis mencegat dan mengirimkannya untuk ditinjau secara manual. Selain itu, fungsi pencatatan lengkap disediakan, yang akan diaudit secara berkala oleh sistem. Jika ditemukan kondisi abnormal, sistem akan mendelegasikan tugas kepada pengguna dan memberikan informasi tersebut kepada administrator untuk diproses lebih lanjut. Administrator merupakan garis pertahanan terakhir untuk pemantauan keamanan.

4.6.1 Poin Inovatif

- *Dapat beradaptasi dengan berbagai sistem jaringan:* Sistem yang diusulkan dapat bekerja di berbagai jaringan. Sistem ini tidak hanya dapat diusulkan untuk jaringan IP yang ada, tetapi juga dapat beradaptasi dengan berbagai arsitektur jaringan masa depan, seperti MIN.
- *Analisis paket waktu nyata berdasarkan big data:* Sistem yang diusulkan berdasarkan teknologi big data menganalisis berbagai dimensi data keamanan masif untuk memahami ancaman keamanan yang ada dan yang mungkin terjadi di berbagai tingkatan.
- *Model berbasis kecerdasan buatan:* Pembelajaran mesin tingkat lanjut, pembelajaran mendalam, dan algoritme pengoptimalan kecerdasan kelompok digunakan untuk meningkatkan efisiensi dan akurasi analisis.
- *Antarmuka yang ramah pengguna:* Sistem yang diusulkan dapat menampilkan analisis secara waktu nyata melalui antarmuka dari berbagai perspektif, sehingga administrator dapat memahami situasi keamanan dengan jelas dan intuitif.
- *Deteksi intrusi multidimensi:* Kami mengusulkan model deteksi lengkap, termasuk tiga bagian deteksi berdasarkan aliran jaringan, host, dan perilaku pengguna. Melalui pendeteksian beberapa objek, kemampuan untuk terus memantau keamanan jaringan ditingkatkan. Dengan demikian, administrator lebih mudah menemukan anomali jaringan tepat waktu, dan dengan cepat memperkirakan tujuan serangan, cara serangan, jalur serangan, dan jangkauan dampak, sehingga dapat meminimalkan risiko dan kerugian jaringan.
- *Teknologi penyimpanan yang andal berdasarkan blockchain:* Teknologi blockchain digunakan untuk menyimpan dan menemukan kejadian secara akurat guna mencegah penyerang merusak log perilaku serangan. Oleh karena itu, administrator jaringan dapat membuat penilaian status risiko yang lebih kredibel dan prediksi tren pengembangan di masa mendatang.

4.6.2 Istilah Teknis

- **TF-IDF:** (Term Frequency-Inverse Document Frequency) teknik pembobotan yang umum digunakan untuk pengambilan informasi dan penambangan teks untuk menilai pentingnya sebuah kata bagi sebuah dokumen dalam sekumpulan dokumen atau korpus.
- **ANN**: Jaringan Syaraf Tiruan, yang memiliki kemampuan beradaptasi, belajar mandiri, dan aproksimasi nonlinier yang baik.
- **Deteksi kebaruan:** Tidak ada outlier dalam data pelatihan, dan model digunakan untuk mendeteksi outlier dalam sampel baru.
- **SVM satu kelas:** One-Class Support Vector Machine, satu jenis support vector machine, yang menggunakan metode pembelajaran tanpa pengawasan dan tidak perlu menandai label keluaran dari set pelatihan secara manual.

- **PSO:** Particle Swarm Optimization, metode perhitungan evolusioner yang berasal dari simulasi perilaku pemangsaan burung, yang memiliki algoritma optimasi kecerdasan kawanan dengan kemampuan optimasi global yang kuat.

4.6.3 Skenario Aplikasi

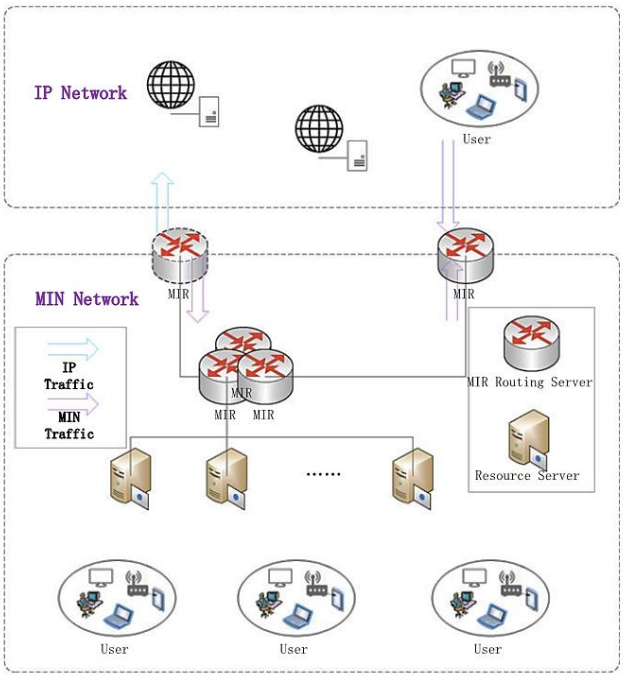
Sistem kesadaran situasi keamanan dapat diterapkan tidak hanya dalam jaringan IP tradisional, tetapi juga dalam arsitektur MIN. Berikut ini mengambil MIN sebagai contoh untuk memperkenalkan skenario aplikasi utamanya. Topologi jaringan ditunjukkan pada Gambar 4.20.

Jika MIN internal berkomunikasi dengan jaringan IP eksternal, paket MIN yang berisi permintaan sumber daya IP akan dikirim, yang akan diterjemahkan oleh Edge Multi-Identifier Router (EMIR). Sumber daya jaringan IP yang sesuai akan diminta. Setelah menerima respons yang sesuai, respons tersebut dienkapsulasi oleh EMIR, dan diteruskan sebagai paket MIN lagi. Namun, jika pengguna jaringan eksternal ingin mengakses sumber daya MIN internal, mereka diizinkan menggunakan klien MIN untuk berkomunikasi dengan MIN melalui lalu lintas MIN murni setelah autentikasi sertifikat lapis demi lapis.

Sistem kesadaran situasi keamanan diterapkan pada EMIR. Sementara kewaspadaan keamanan jaringan MIN dilakukan, lalu lintas IP juga dideteksi dan dianalisis. Selama proses ini, sistem kewaspadaan situasi keamanan diterapkan pada dua perangkat inti: server MIS dan MIR.

4.6.4 Arsitektur Sistem

Sistem kewaspadaan situasi keamanan meliputi empat modul: Deteksi Lalu Lintas Berbahaya Berbasis Jaringan Saraf BP, Deteksi Perilaku Akses Anomali Berbasis SVM Satu Kelas, Prediksi Situasi Keamanan Berbasis PSO-SVM, Model Evaluasi Ancaman Hirarkis Kuantitatif untuk Situasi Keamanan.

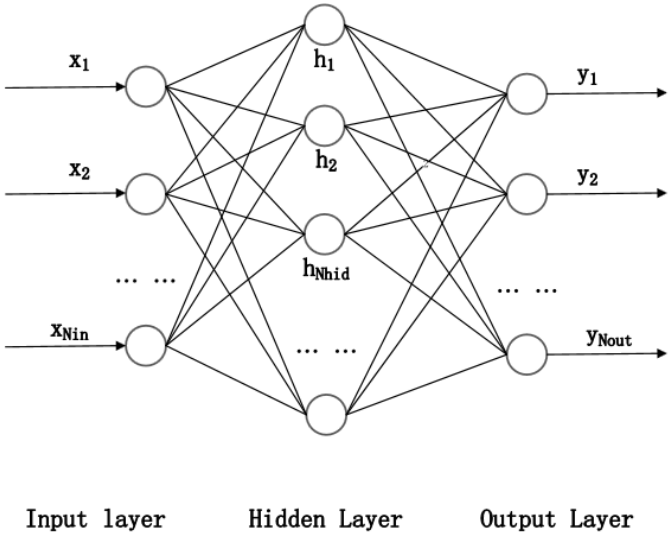


Gambar 4.20 Topologi skenario aplikasi

1. Deteksi Trafik Berbahaya Berdasarkan Jaringan Saraf BP

Deteksi DDoS berdasarkan jaringan saraf memberikan kemungkinan untuk mengatasi keterbatasan algoritma pembelajaran mesin tradisional. Sistem yang diusulkan berdasarkan algoritma jaringan saraf yang ada menganalisis teori deteksi serangan DDoS, metode, dan kumpulan data lokal. Kami membangun model deteksi trafik serangan berdasarkan enam karakteristik seperti panjang paket, interval waktu pengiriman paket, dan laju perubahan panjang paket. Kemudian skema pengoptimalan parameter untuk menyesuaikan kesalahan jaringan saraf diusulkan melalui sejumlah besar eksperimen. Metode di atas secara efektif meningkatkan akurasi deteksi DDoS, dan dapat diperluas untuk deteksi trafik serangan lainnya, seperti serangan pemindaian port, dengan menggabungkan mode deteksi jaringan saraf dengan analisis statistik.

Untuk proses ekstraksi fitur, sistem yang diusulkan meningkatkan akurasi deteksi serangan DDoS sambil memastikan konsumsi sumber daya yang rendah. Setelah penandaan, normalisasi, dan ekstraksi fitur data asli, kumpulan data yang dapat dikirimkan ke jaringan saraf untuk pelatihan diperoleh. Jaringan Syaraf Tiruan (JST) digunakan sebagai model deteksi serangan DDoS.



Gambar 4.21 Struktur jaringan saraf tiga lapis

Saat melatih jaringan syaraf multi-lapis dengan fungsi sigmoid, algoritma penurunan gradien tradisional dapat menyebabkan perubahan kecil dalam bobot dan deviasi, atau bahkan jauh dari nilai optimalnya, karena amplitudo gradien terlalu kecil. Algoritma cepat dapat memecahkan masalah perangkap kesalahan lokal. Struktur jaringan jaringan syaraf tiga lapis ditunjukkan pada Gambar 4.21.

Di mana N_{in}, N_{hid} dan N_{out} masing-masing mewakili jumlah neuron di lapisan masukan, lapisan tersembunyi dan lapisan keluaran. Wih_{ij} mewakili bobot koneksi antara neuron ke-i_{th} di lapisan masukan dan neuron ke-j_{th} di lapisan tersembunyi. Who_{jk} mewakili bobot koneksi antara neuron ke-j_{th} di lapisan tersembunyi dan neuron ke-k_{th} di lapisan keluaran.

80% dari kumpulan data yang diperoleh dari pemrosesan sebelumnya digunakan untuk melatih jaringan syaraf dan 20% untuk deteksi serangan. Kami membandingkan hasil algoritma berbasis dan yang dimodifikasi. Hasilnya ditunjukkan pada Tabel 4.5.

Tabel 4.5 Hasil algoritma berbasis dan modifikasi

Jenis-jenis algoritma	*Rata-rata waktu yang dihabiskan (ms)*	*Jumlah rata-rata penelitian*	*Akurasi (%)*
ANN tiga lapis tradisional	3027	2268	97
ANN tiga lapis yang disempurnakan	1494	919	98.4

Hasilnya menunjukkan bahwa algoritma yang dimodifikasi yang diusulkan mengurangi jumlah rata-rata iterasi lebih dari 50%. Oleh karena itu, algoritma yang dimodifikasi dapat secara signifikan mempersingkat waktu deteksi dan meningkatkan efisiensi deteksi serangan DDoS. Pada saat yang sama, algoritma yang dimodifikasi juga meningkatkan akurasi deteksi intrusi rata-rata sekitar 1,4%.

Untuk memverifikasi kemampuan generalisasi model, kumpulan data validasi model dibentuk dengan menggabungkan data aliran normal yang dikumpulkan dan data aliran DDoS manual. Hasil validasi ditunjukkan sebagai berikut (Tabel 4.6). Hasilnya menunjukkan bahwa jaringan saraf multi-lapis yang dikombinasikan dengan karakteristik statistik lalu lintas jaringan dalam sistem ini akurat dan efisien.

Tabel 4.6 Hasil Validasi Model

Nama himpunan data	Jumlah lalu lintas abnormal	Jumlah trafik abnormal yang terdeteksi	Total lalu lintas abnormal terdeteksi	Akurasi (%)	Faktor kebisingan (%)
ddosData.csv	733	733	743	100	0,13
ddosData2.csv	1733	1733	1763	100	0,07
ddosData3.csv	2111	2111	2111	100	0%

2. Deteksi Perilaku Akses Anomali Berdasarkan SVM Satu Kelas

Kami menggunakan deteksi perilaku akses anomali berdasarkan sampel putih, dan pembelajaran sampel dilakukan melalui SVM tanpa pengawasan atau satu kelas. Model minimum yang dapat sepenuhnya mengekspresikan sampel putih dibangun sebagai Profil untuk mewujudkan deteksi permintaan anomali.

Kami mengekstrak 150.000 permintaan normal dari log akses jaringan sebagai kumpulan data untuk pelatihan model, yang digunakan untuk melatih Profil sampel normal. Lebih dari 150.000 XSS, injeksi SQL, dan muatan lainnya dikumpulkan dari platform intelijen ancaman dan kumpulan data lainnya sebagai permintaan akses anomali. Algoritme frekuensi-Inverse Document Frequency (TF-IDF) digunakan untuk mengekstrak fitur teks dan

mengeluarkannya dalam bentuk matriks. TF-IDF adalah teknologi tertimbang umum untuk pengambilan informasi dan penambangan teks.

Dalam masalah klasifikasi biner dari deteksi permintaan pengecualian, kami mempertimbangkan untuk mempelajari batas minimum dari satu kelas sampel melalui satu model klasifikasi, dan yang berada di luar batas diidentifikasi sebagai pengecualian. SVM satu kelas dalam pembelajaran mesin digunakan untuk mengidentifikasi permintaan akses anomali dalam sistem, yang sesuai dengan skenario dan persyaratan bisnis.

Hasil deteksi ditunjukkan pada Tabel 4.7. Hasil menunjukkan bahwa model SVM satu kelas yang dilatih oleh kumpulan data sampel putih layak dan efektif dalam mendeteksi perilaku akses anomali.

Tabel 4.7 Hasil Deteksi

Nama kumpulan data	Jumlah lalu lintas abnormal	Jumlah trafik abnormal yang terdeteksi	Total trafik abnormal terdeteksi	Akurasi (%)	Faktor kebisingan (%)
bad_fromE.txt	4027	4027	4027	100	0
ddosData2.csv	46.083	45.908	45.908	100	99,6

3. Prediksi Situasi Keamanan Berdasarkan PSO-SVM

Sistem yang diusulkan memprediksi situasi keamanan berdasarkan deret waktu nonlinier, dan menganalisis secara komprehensif hukum historis situasi keamanan untuk memprediksi situasi keamanan di masa mendatang dalam jangka waktu tertentu atau pada saat tertentu, yang sesuai dengan skenario dan persyaratan bisnis. Atas dasar ini, model prediksi situasi keamanan jaringan bernama PSO-SVM diusulkan, yang menggabungkan Particle Swarm Optimization (PSO) dan Support Vector Machines (SVM). PSO-SVM digunakan secara efektif pada data sampel kecil untuk memperkirakan tren nilai.

Saat menyusun kumpulan data, nilai situasi keamanan dianggap sebagai urutan waktu sederhana, di mana setiap titik pemantauan sesuai dengan nilai situasi keamanan jaringan. Nilai-nilai tersebut merupakan deret waktu nonlinier. Untuk memprediksi deret waktu situasi keamanan nonlinier ini, kita perlu menemukan hubungan antara nilai situasi keamanan pada saat $i + p$ dan nilai situasi keamanan pada saat p sebelumnya $(x_i, x_{i+1}, \dots, x_{i+p-1})$. Dengan kata lain, kita perlu mengeksplorasi fungsi $x_{i+p} = f(x_i, x_{i+1}, \dots, x_{i+p-1})$. Fungsi f adalah fungsi non-linier dan merepresentasikan hubungan non-linier sepanjang deret waktu.

Menurut teori SVM, fungsi f dapat diperoleh dengan mempelajari dan melatih beberapa kelompok sampel deret waktu situasi keamanan yang diketahui.

Model prediksi PSO-SVM secara dinamis menghasilkan kumpulan sampel situasi keamanan dengan algoritma jendela geser. Nilai situasi keamanan jaringan yang sesuai dari titik pemantauan $1;\ 2;\ \dots;\ n$ adalah $a_1, a_2, \dots, a_n$. Jika ukuran jendela ditetapkan menjadi m, rekaman sampel ke-1 adalah $a_1, a_2, \dots, a_m$ Oleh karena itu, nilai situasi keamanan jaringan pada titik pemantauan $m + 1$ adalah a_{m+1}. Kemudian sampel kedua dibangun untuk merekam $a_2, a_3, \dots, a_m$, dan nilai situasi keamanan jaringan pada titik pemantauan $m + 2$

adalah a_{m+2}, dan seterusnya. Dalam sistem yang diusulkan, m ditetapkan menjadi 3, dan ukuran jendela geser ditetapkan menjadi 3. Pada saat yang sama, untuk mencegah akumulasi kesalahan, ketika model yang diusulkan digunakan untuk memprediksi nilai situasi keamanan pada titik waktu tertentu t di masa mendatang, nilai yang diprediksi pada waktu t akan dicakup oleh nilai situasi keamanan aktual, jika nilai situasi keamanan sebelum titik waktu $t - k$ telah dihitung sesuai dengan situasi praktis. Metode pembuatan set sampel ditunjukkan pada Gambar 4.22.

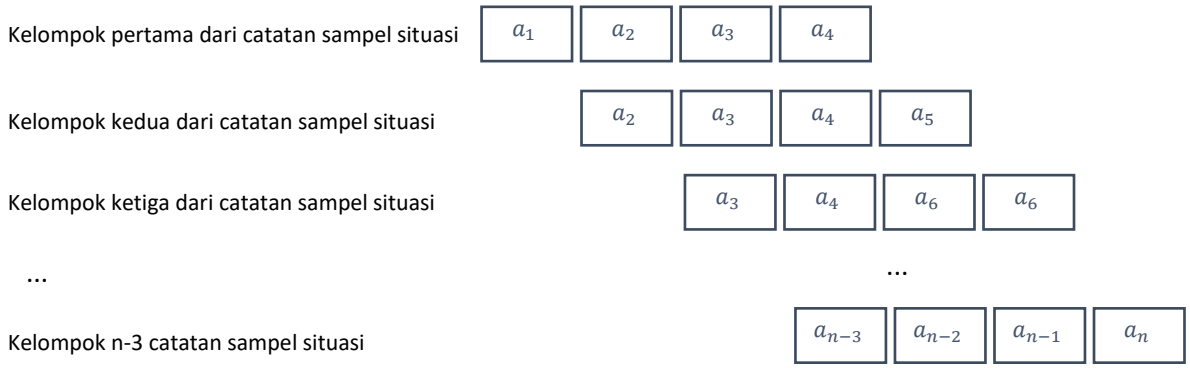
Model yang diusulkan menggabungkan model SVM berdasarkan teori pembelajaran statistik. Dibandingkan dengan model jaringan saraf, model ini saat ini merupakan skema pembelajaran dan statistik sampel kecil terbaik, yang memecahkan masalah pembelajaran berlebih, bencana nonlinier, dan dimensional. Selain itu, SVM mengadopsi prinsip minimisasi risiko struktural, dan seluruh proses solusi diubah menjadi masalah pemrograman kuadratik cembung untuk mendapatkan solusi global yang optimal dan unik, yang mengatasi beberapa kekurangan jaringan saraf. Dalam proses pelatihan, Particle Swarm Optimization (PSO) digunakan untuk mengoptimalkan parameter SVM dan memastikan keakuratan data prediktif. Dalam algoritma ini, setiap solusi dari masalah optimasi disebut partikel, dan fungsi adaptif didefinisikan untuk mengukur keunggulan setiap partikel. Sekelompok partikel dan kecepatan partikel diinisialisasi secara acak, kemudian setiap partikel bergerak dalam kawanan berdasarkan "pengalaman terbang"-nya sendiri dengan partikel lain untuk mencari solusi optimal dari seluruh ruang. Proses prediksi situasi keamanan ditunjukkan pada Gambar 4.23.

Banyak eksperimen menunjukkan bahwa model yang diusulkan memprediksi tren keamanan di masa mendatang untuk jangka waktu tertentu yang memberi kita pandangan ke depan tentang situasi keamanan jaringan, yang membantu kita mengambil tindakan pencegahan terlebih dahulu sesuai dengan situasi keamanan.

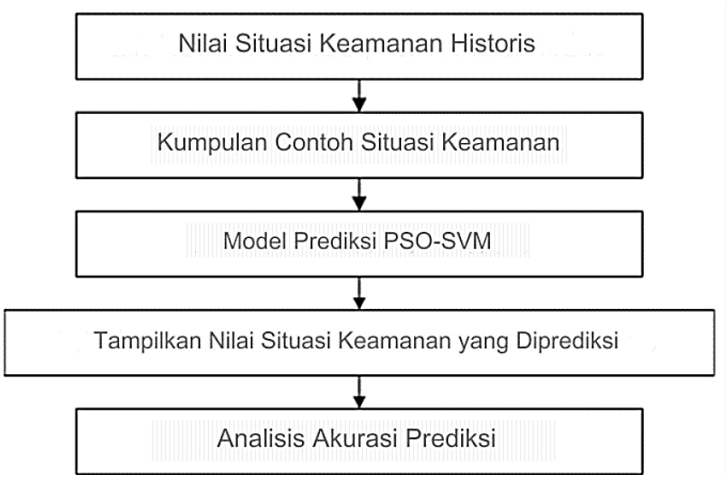
Ada beberapa keterbatasan dalam memproses sampel kecil dengan jaringan saraf, seperti mudah jatuh ke titik minimum lokal dan kecepatan konvergensi lambat. Dengan mempertimbangkan keterbatasan di atas dan fitur linear yang kuat dari nilai situasi keamanan jaringan, kami mempelajari fitur metode SVM untuk menggunakan keuntungan matematis dari pemrosesan data nonlinier, data sampel kecil. Kemudian model pemasangan nonlinier kompleks dibangun yang lebih sesuai untuk kumpulan data situasi keamanan jaringan. PSO-SVM yang diusulkan dikombinasikan dengan PSO menjamin pengoptimalan global cepat dan pemasangan nonlinier. Berdasarkan karakteristik periodik situasi keamanan jaringan, pengelompokan dan prediksi periodik dilakukan.

4. Model Evaluasi Ancaman Hirarkis Kuantitatif untuk Situasi Keamanan

Dikombinasikan dengan skenario aplikasi router batas MIN, kami mengadopsi model kesadaran kuantitatif situasi keamanan hierarkis dari strategi bottom-to-up, lokal-ke-keseluruhan. Situasi keamanan dievaluasi dari tiga aspek: kejadian abnormal, situasi host, dan situasi jaringan. Kecuali statistik frekuensi alarm, tingkat keparahan alarm, dan tingkat konsumsi bandwidth jaringan, metode yang diusulkan memberi bobot pada faktor kepentingan layanan dan host, dan menghitung indeks ancaman layanan, host, dan seluruh jaringan untuk mengevaluasi dan menganalisis situasi ancaman keamanan.



Gambar 4.22 Metode pembuatan set sampel



Gambar 4.23 Proses prediksi situasi keamanan

Indeks ancaman dihitung sebagai berikut:

$$R_{S_j}(t) = f\left(\vec{\theta}, \vec{C}_j(t), \vec{A}_j(t), \vec{N}(t), \vec{A}_d(t)\right) = \vec{\theta} \cdot \left(\vec{C}_j(t) \cdot 10^{\vec{A}_j(t)} + 100\vec{N}(t) \cdot 10^{\vec{A}_d(t)}\right) \tag{4.14}$$

di mana vektor $\vec{\theta} = (\theta_1, \ldots, \theta_h)$ mewakili trafik normal, dan h adalah jumlah periode waktu dalam sehari yang dibagi menjadi. Nilai elemen awal $\vec{\theta}$ ditetapkan oleh administrator sistem berdasarkan trafik normal rata-rata $F_i(i = 1, \ldots, h)$dari sistem jaringan yang dilindungi dalam periode waktu yang berbeda. Setelah kunjungan rata-rata dihitung, nilai elemen $\vec{\theta}$ diperoleh sebagai berikut:

$$\theta_i = \frac{F_i}{\sum_{t=1}^{h} F_t} \tag{4.15}$$

$$\text{Vector } \vec{A}_j(t) = \left(\vec{A}_{j1}, \ldots, \vec{A}_{jt}, \ldots, \vec{A}_{jh}\right) \text{ and vector } \vec{C}_j(t) = \left(\vec{C}_{j1}, \ldots, \vec{C}_{jt}, \ldots, \vec{C}_{jh}\right)$$

menggambarkan tingkat keparahan serangan dan waktu kejadian pada waktu t secara berurutan. Jenis dan nilai elemen ini diperoleh dengan menghitung basis data log peristiwa serangan.

$\vec{N}(t) = (\vec{N}_1, \dots, \vec{N}_t, \dots, \vec{N}_h)$ mewakili pemanfaatan bandwidth jaringan dan $\overrightarrow{A_d}(t) = (\vec{A}_{d1}, \dots, \vec{A}_{dt}, \dots, \vec{A}_{dh})$ mewakili vektor tingkat ancaman serangan DoS. Elemen mereka $\overrightarrow{N_i}(v) = (\vec{N}_{i1}, \dots, \vec{N}_{i2}, \dots, \vec{N}_{iv})$ dan $\overrightarrow{A_{di}}(v) = (\vec{A}_{di1}, \dots, \vec{A}_{di2}, \dots, \vec{A}_{div})$ $(i = 1, \dots, h)$ merepresentasikan pemanfaatan lebar pita jaringan dan vektor tingkat ancaman DoS dari setiap jendela waktu dalam periode waktu ke-i. v adalah jumlah jendela peristiwa analisis dalam periode ke-i. Koefisien ditetapkan sebesar 100 untuk mengubah tingkat hunian menjadi bilangan bulat guna mengevaluasi ancaman serangan DoS. Dengan menggabungkan Common Vulnerability Scoring System (CVSS), kami menetapkan tingkat ancaman peristiwa berbahaya seperti DDoS dan perilaku pemindaian. Pemanfaatan CPU meningkat lebih cepat daripada pemanfaatan lebar pita saat peristiwa serangan terjadi. Oleh karena itu, kami tidak hanya memanfaatkan pemanfaatan lebar pita, tetapi juga menambahkan pemanfaatan CPU ke dalam evaluasi.

Skema ini lebih stabil dan efisien daripada algoritma kesadaran situasi berdasarkan pembelajaran mesin, dan menghindari beberapa penyimpangan. Selain itu, kami menggabungkan skenario aplikasi MIN dan mengadopsi kesadaran situasi yang terdiri dari situasi ancaman jaringan IP dan situasi ancaman host termasuk kesadaran jaringan MIN. Evaluasi keamanan sistem secara real-time membuat hasil evaluasi lebih lengkap dan lebih tepat. Hasil percobaan menunjukkan bahwa model kesadaran kuantitatif situasi keamanan jaringan hierarkis yang diusulkan dapat secara intuitif menampilkan situasi ancaman keamanan seluruh server, sehingga administrator jaringan dapat memahami situasi keamanan secara tepat waktu dan mengetahui alasan perubahan keamanan untuk menyesuaikan kebijakan keamanan. Dengan cara ini, keamanan sistem yang maksimal terjamin. Selain itu, aturan evolusi situasi keamanan dapat diperoleh dari kurva jangka panjang, yang mengevaluasi ancaman serangan jaringan umum dan membebaskan administrator dari tugas berat analisis data alarm.

4.7 ANALISIS KEAMANAN

Untuk membangun jaringan kedaulatan, salah satu fokus utamanya adalah memastikan keamanan jaringan, terutama keamanan komponen inti. Bagian ini akan menganalisis strategi anti-serangan dan keamanan jaringan kedaulatan.

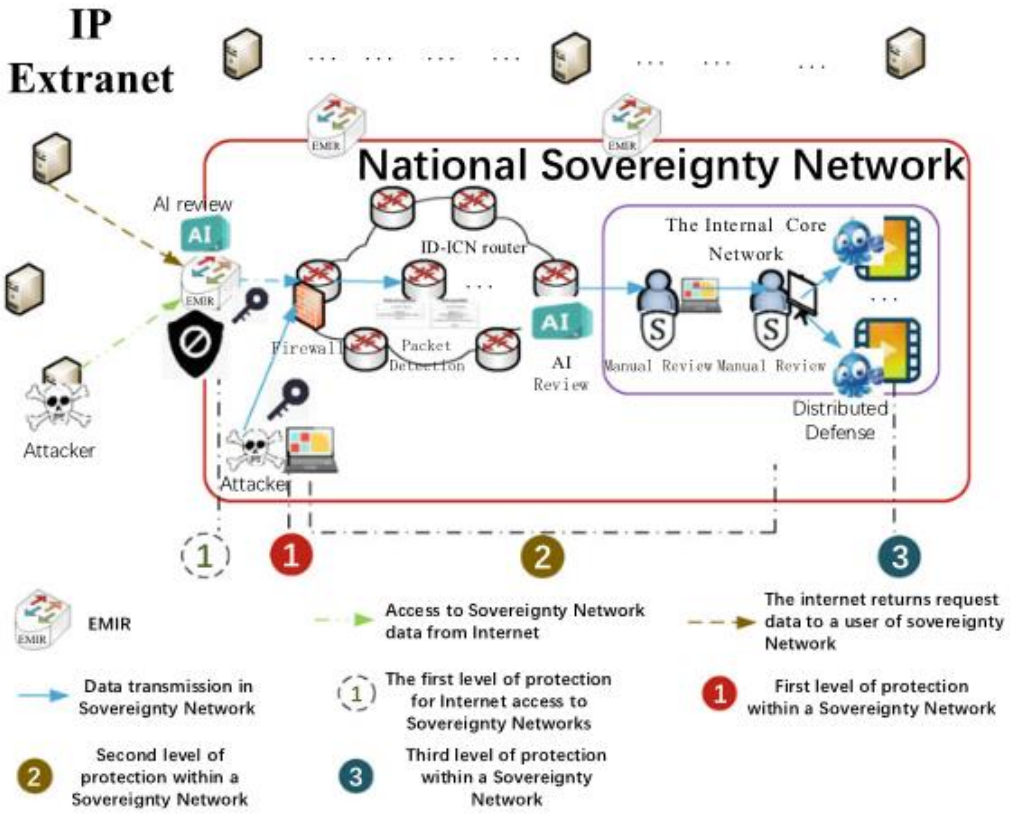
4.7.1 Mekanisme Keamanan

Untuk menjamin keamanan, jaringan IP tidak disertakan dalam jaringan kedaulatan. Perbedaan paling jelas antara perangkat dalam jaringan kedaulatan dan sistem yang ada adalah penambahan router ID-ICN dan Edge Multi-Identifier Router (EMIR) dalam jaringan kedaulatan, yang membentuk dua tingkat pertama dari penghalang pertahanan jaringan kedaulatan.

Router ID-ICN adalah router yang mendukung pengalamatan pengenal identitas dan konten serta intertranslasi data jaringan. Ketika pengguna mengambil konten tertentu, jika konten tersebut berada dalam jaringan kedaulatan, pengenal konten dan alamat asli pengguna akan diterjemahkan terlebih dahulu pada router ID-ICN, kemudian data akan ditransfer dalam jaringan yang berpusat pada identitas.

EMIR tidak hanya memiliki fungsi penerusan paket seperti MIR biasa, tetapi juga berfungsi sebagai antarmuka akses dua arah antara jaringan IP dan jaringan kedaulatan. Di sisi lain, konten yang tiba di node awalnya ditinjau dan difilter melalui prosedur audit konten relevan yang dipasang di EMIR, seperti prosedur audit konten AI. Melalui kedua mekanisme ini, serangan jaringan luar dapat diisolasi untuk memastikan keamanan jaringan kedaulatan. Jika pengguna meminta konten di jaringan eksternal, pengidentifikasi konten dan alamat IP akan saling diterjemahkan pada EMIR jaringan kedaulatan, kemudian permintaan akan diangkut ke sumber konten. Jika konten yang diminta berada di jaringan kedaulatan negara lain, multi-pengidentifikasi akan saling diterjemahkan di EMIR jaringan kedaulatan, dan kemudian data akan dikirimkan dalam jaringan yang berpusat pada identitas. Tingkat ketiga adalah arsitektur CMD, yang merupakan komponen inti dalam jaringan kedaulatan.

Singkatnya, mekanisme keamanan dalam jaringan kedaulatan terutama mencakup mekanisme perlindungan seperti EMIR, teknologi blockchain, enkripsi asimetris, dan keuntungan keamanan yang dibawa oleh transmisi data melalui jaringan yang berpusat pada identitas; perlindungan tautan yang terdiri dari mekanisme keamanan router ID-ICN seperti deteksi AI dan deteksi paket. Dan perangkat keamanan seperti router tiruan dunia maya, firewall, dan sistem penyimpanan terdistribusi. Mekanisme anti-serangan ini menyediakan sistem dengan keamanan tinggi. Kerangka mekanisme keamanan ditunjukkan pada Gambar 4.24.



Gambar 4.24 Mekanisme keamanan dalam jaringan kedaulatan

4.7.2 Mekanisme Keamanan Arsitektur Jaringan

Karena jaringan kedaulatan dibangun berdasarkan jaringan yang berpusat pada identitas, maka jaringan ini memiliki kemampuan pertahanan tertentu. Mode transmisi data dalam jaringan yang berpusat pada identitas berbeda dari jaringan IP yang ada. Jaringan kedaulatan menyaring informasi akses melalui EMIR terlebih dahulu. Hanya konten yang secara aktif diminta oleh pengguna di jaringan internal yang dapat diakses melalui EMIR. Dengan kata lain, penyerang tidak dapat memindai, menyerang, atau bahkan mengirim informasi berbahaya ke jaringan kedaulatan secara terus-menerus seperti di jaringan IP.

Dalam jaringan kedaulatan, setelah registrasi nama asli, pengguna perlu menarik data dari jaringan dengan tanda tangan mereka. Untuk data yang diminta oleh pengguna internal, konten dan peminta data dicatat oleh log blockchain. Jika terjadi keadaan yang tidak normal, sistem melacak kembali dan melakukan akuntabilitas sesuai dengan log blockchain, untuk memastikan keaslian dan keandalan informasi. Sampai batas tertentu, sistem menghindari operasi berbahaya oleh pengguna intranet.

Pada Gambar 4.24, mekanisme keamanan terutama bergantung pada teknologi kriptografi seperti autentikasi identitas. Kesulitan serangan algoritma enkripsi yang ada telah mencapai tingkat eksponensial. Misalnya, perlu waktu puluhan tahun untuk menjalankan superkomputer paling canggih untuk memecahkan algoritma RSA umum. Kesulitan memecahkan algoritma RSA terkait dengan panjang kunci.

Untuk algoritma RSA dengan kunci publik e dan modul n, kompleksitas serangan brute force adalah Satu. Cara paling umum untuk memecahkan RSA adalah melalui faktorisasi. Ketika panjang kunci 256 bit atau kurang, komputer berkecepatan tinggi dapat berhasil memfaktorkannya dalam satu hari. Panjang kunci yang panjang akan meningkatkan waktu faktorisasi. Pada tahun 1999, superkomputer Cray membutuhkan waktu lima bulan untuk memfaktorkan kunci 512-bit. Sepuluh tahun kemudian, tepatnya pada tanggal 9 Desember 2009, beberapa peneliti melaporkan bahwa mereka telah melakukan pemfaktoran kunci RSA 768-bit dan 232-bit, dan butuh waktu ribuan kali lebih lama untuk melakukan pemfaktoran kunci RSA 768-bit daripada kunci 512-bit. Diperlukan waktu 1000 kali lebih lama untuk melakukan pemfaktoran kunci 1024-bit yang umum digunakan saat ini daripada kunci 768-bit, sehingga kunci 1024-bit masih dapat memenuhi persyaratan keamanan dalam waktu yang singkat.

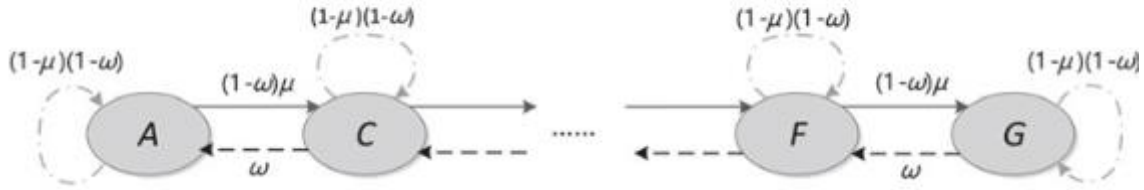
Dengan daya komputasi saat ini, diperlukan waktu dua tahun untuk melakukan pemfaktoran kunci 1024-bit, dan 80 tahun untuk melakukan pemfaktoran kunci 2048-bit. Oleh karena itu, kami berasumsi bahwa waktu penyerangan adalah 50 tahun, maka rasio keberhasilan serangan per detik dihitung sebesar $6{,}43 \times 10{-}10$.

4.7.3 Mekanisme Keamanan Tautan Jaringan

Rantai serangan terdiri dari dua bagian, termasuk simpul antara EMIR dan simpul permintaan konten, dan simpul antara simpul permintaan konten ke komponen inti jaringan yang perlu ditembus oleh penyerang. Proses serangan pada tahap ini terutama berupa penyebaran informasi berbahaya di tautan internal jaringan kedaulatan, yang dianggap sebagai pergerakan acak pada rantai serangan. Setelah konten yang diminta ditarik ke jaringan

kedaulatan, konten tersebut akan melalui beberapa mekanisme penyaringan antara EMIR dan simpul permintaan konten, seperti firewall, deteksi paket, deteksi pengenalan teks, audio, gambar, dan video, serta pemrosesan bahasa alami. Antara simpul permintaan konten dan komponen inti jaringan, konten yang dikirimkan disaring melalui serangkaian mekanisme penyensoran manusia. Penyerang perlu menerobos tingkat perlindungan untuk mencapai target, yaitu komponen jaringan inti.

Tautan jaringan lengkap terdiri dari banyak filter. Jika penyerang ingin menyerang komponen inti di sepanjang rantai serangan, penyerang perlu menyerang setiap filter di sepanjang rantai serangan. Penyerang maju di sepanjang rantai serangan, dan setiap pelarian yang berhasil dari filter mengarah satu langkah maju di sepanjang rantai serangan. Jika penyerang tertangkap oleh filter, ia akan kembali di sepanjang rantai serangan. Jika penyerang tidak berhasil melakukan serangan atau tertangkap oleh filter, ia akan tetap berada di node. Pendekatan ini menyatakan bahwa tahap berikutnya hanya terkait dengan status saat ini dan rentang langkah berikutnya konsisten dengan karakteristik rantai Markov. Oleh karena itu, rantai Markov dan Martingale digunakan untuk memodelkan dan memecahkan masalah ini.



Gambar 4.25 Rantai Markov

Probabilitas melarikan diri dari filter dilambangkan sebagai l, dan jumlah node dalam rantai serangan dilambangkan sebagai h. Probabilitas menangkap penyerang adalah x. Kami berasumsi bahwa penyerang telah melarikan diri dari k node, misalnya, ia tetap berada di node ke-k (Gambar 4.25). Proses serangan dilambangkan sebaai matriks Mh×h. Elemen Mi;j mewakili probabilitas bahwa penyerang telah lolos dari filter ke-i dan targetnya berubah ke filter ke-j. Selama serangan, penyerang bergerak sepanjang rantai serangan. Setelah menaklukkan satu simpul, penyerang akan mendapatkan informasi tentang simpul berikutnya. Selama serangan, serangan simpul tunggal hanya dapat berhasil jika serangan berhasil ditangkap. Serangan memiliki tiga arah: kembali ke simpul terakhir, maju ke simpul berikutnya, dan tetap berada di simpul saat ini. Probabilitas transisi adalah sebagai berikut:

(1) Kembali ke simpul terakhir $(M_i, i-1 = x)$. Tidak peduli apakah penyerang lolos dari perangkat, selama sistem mendeteksi penyerang, serangan tidak akan dapat dilakukan dan penyerang harus kembali ke perangkat sebelumnya.

(2) Maju ke simpul berikutnya $(M_i, i+1 = (1-x)\mu)$. Probabilitas tidak adanya deteksi efektif adalah $(1-x)$. Dan probabilitas penyerang lolos dari filter adalah μ. Oleh karena itu, probabilitas penyerang lolos dari filter ini tanpa deteksi efektif diperoleh sebagai $M_i, i+1 = (1-x)\mu$.

(3) Tetap berada di node saat ini $(M_i, i = (1 - x)(1 - \mu))$. Penyerang tetap berada di node yang sama pada slot waktu berikutnya jika penyerang tidak lolos dan tertangkap.

Rantai Markov $X_0;\ X_1;\ X_2;\ ..\ .;\ X_n$ menunjukkan sekumpulan variabel acak, di mana $X_i X_i\ 0;\ h\ ;\ X_0\ 0$ menunjukkan posisi penyerang yang tetap berada di awal slot waktu ke-i. Jika penyerang tetap berada di perangkat ke-k, kemungkinan tahap berikutnya dilambangkan sebagai berikut:

$$P\{X_{n+1} = k+1 | X_n = k\} = (1-\omega)\mu \qquad (4.16)$$

$$P\{X_{n+1} = k | X_n = k\} = (1-\omega)(1-\mu) \qquad (4.17)$$

$$P\{X_{n+1} = k-1 | X_n = k\} = \omega \qquad (4.18)$$

Karena itu,

$$E[X_{n+1}|X_n] = (1-\omega)\mu(k+1) + (1-\omega)(1-\mu)k + \omega(k-1) = k + (1-\omega)\mu - \omega \qquad (4.19)$$

Berdasarkan rantai Markov di atas, kita dapat membangun himpunan variabel acak lain M0; $M_1; M_2; \cdots$; Mn, dimana

$$M_i = X_i - [(1-\omega)\mu - \omega] \cdot i \qquad (4.20)$$

M_n dapat dibuktikan sebagai Martingale yang terkait dengan $X_0;\ X_1;\ X_2;\ \ldots;\ X_n$.

Jika penyerang lolos dari filter dengan probabilitas l, dan tertangkap dengan probabilitas x, untuk rantai serangan dengan h node, langkah-langkah sebelum penyerang menilai node target, misalnya, platform produksi dan penyiaran yang terletak di node h adalah:

$$E[S] = \frac{\theta}{[(1-\omega)\mu - \omega]} \qquad (4.21)$$

Oleh karena itu, langkah-langkah yang dilakukan penyerang untuk menilai jaringan produksi dan penyiaran direpresentasikan oleh E[S], yang dapat dihitung dengan h, x, dan l. Dengan cara ini, hubungan kuantitatif antara probabilitas batas dan parameter sistem diperoleh.

4.7.4 Mekanisme Keamanan Komponen Inti

Untuk komponen inti, kami mengadopsi mekanisme keamanan CMD (Cyber Mimic Defense), yang menyimpan data dalam sistem terdistribusi secara redundan. Setiap server independen dianggap sebagai pelaksana, dan beberapa pelaksana berstruktur heterogen melakukan tugas yang sama secara independen. Hasil yang dijalankan dikirim ke arbiter, yang akan mengeluarkan hasil sesuai dengan hasil di atas. Pada bagian ini, kami mengambil sistem dengan tiga pelaksana sebagai contoh (Gambar 4.26).

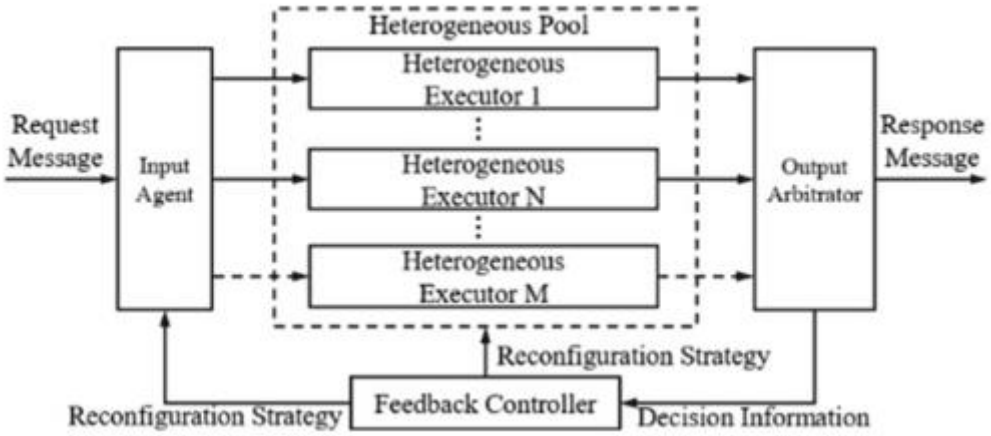
Model Generalized Stochastic Petri Net (GSPN) dibuat, di mana semua pelaksana yang bertahan diserang. Urutan kegagalan berbagai pelaksana dapat disimpulkan berdasarkan tingkat kesulitan serangannya, tetapi hal itu akan membuat analisis menjadi rumit. Mengabaikan sedikit perbedaan yang disebabkan oleh perintah serangan yang berbeda,

model GSPN yang disederhanakan ditunjukkan pada Gambar 4.27, dengan asumsi bahwa pelaksana berhasil diserang dalam urutan No. 1, No. 2, dan No. 3.

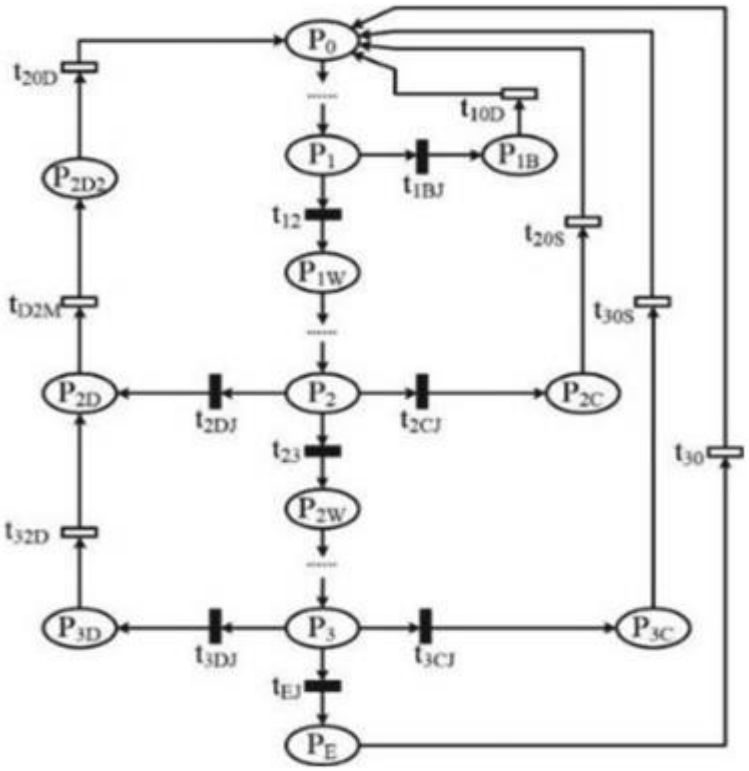
Tempat yang dilambangkan sebagai lingkaran mewakili berbagai status sistem. Tempat Pix terdiri dari elemen i dan x, di mana i mewakili jumlah pelaksana yang dikompromikan dan x mewakili status pelaksana yang diserang. Ada lima status pelaksana yang dikompromikan, termasuk bekerja (W), pelaksana minor yang dikompromikan (B), mengkompromikan sebagian besar pelaksana tanpa hasil yang konsisten (C), mengkompromikan sebagian besar pelaksana dengan hasil yang konsisten (D), dan mengkompromikan semua pelaksana dengan hasil yang konsisten (E). Fase yang paling berbahaya adalah PE, yang berarti bahwa semua pelaksana dirusak dengan hasil yang sama, yaitu sistem produksi dan penyiaran dihancurkan. Transisi menggambarkan perilaku yang berbeda dari seorang pembela atau penyerang yang mengubah sistem di antara berbagai status.

Transisi dapat dibagi menjadi transisi langsung yang diukur dengan probabilitas dan transisi terjadwal yang diukur dengan penundaan perilaku. Transisi langsung dan transisi terjadwal masing-masing digambarkan oleh persegi panjang padat dan persegi panjang berongga. Transisi tijx menunjukkan bahwa perilaku x mengubah sistem dari status dengan i pelaksana yang dikompromikan menjadi status dengan j pelaksana yang dikompromikan. Ada enam perilaku arbiter, termasuk menyerang (a), mengusir pelaksana yang dikompromikan (e), mengusir pelaksana yang tidak bersalah secara keliru (m), menghentikan dan mengganti semua pelaksana yang masih hidup dengan yang baru (s), gangguan acak (d), dan arbitrasi (j).

Kami menetapkan nilai dan menggunakan SPNP untuk mensimulasikan model GSPN yang diusulkan. Jika probabilitas gangguan acak ditetapkan menjadi 0,01%, probabilitas kondisi mapan untuk merusak sistem produksi dan penyiaran CMD dihitung sebagai 1,30 10−6. Pembela dapat secara wajar memilih frekuensi gangguan acak sesuai dengan persyaratan keamanan mereka. Frekuensi gangguan acak yang berbeda sesuai dengan probabilitas kondisi mapan yang berbeda untuk merusak sistem. Korespondensi antara frekuensi gangguan dan probabilitas kegagalan ditunjukkan pada Tabel 4.8. Dengan cara ini, hasilnya diperoleh sebagai.



Gambar 4.26 Arsitektur CMD



Gambar 4.27 Model GSPN

Tabel 4.8 Hubungan antara frekuensi gangguan dan probabilitas kegagalan

Gangguan frekuensi	0.001	0.0001	0.00001	0.000001	0.0000001
Probabilitas kegagalan	1.296×10^{-7}	1.296×10^{-6}	1.296×10^{-5}	1.296×10^{-4}	1.295×10^{-3}

4.7.5 Keuntungan Keamanan yang Dihasilkan oleh Jaringan Kedaulatan

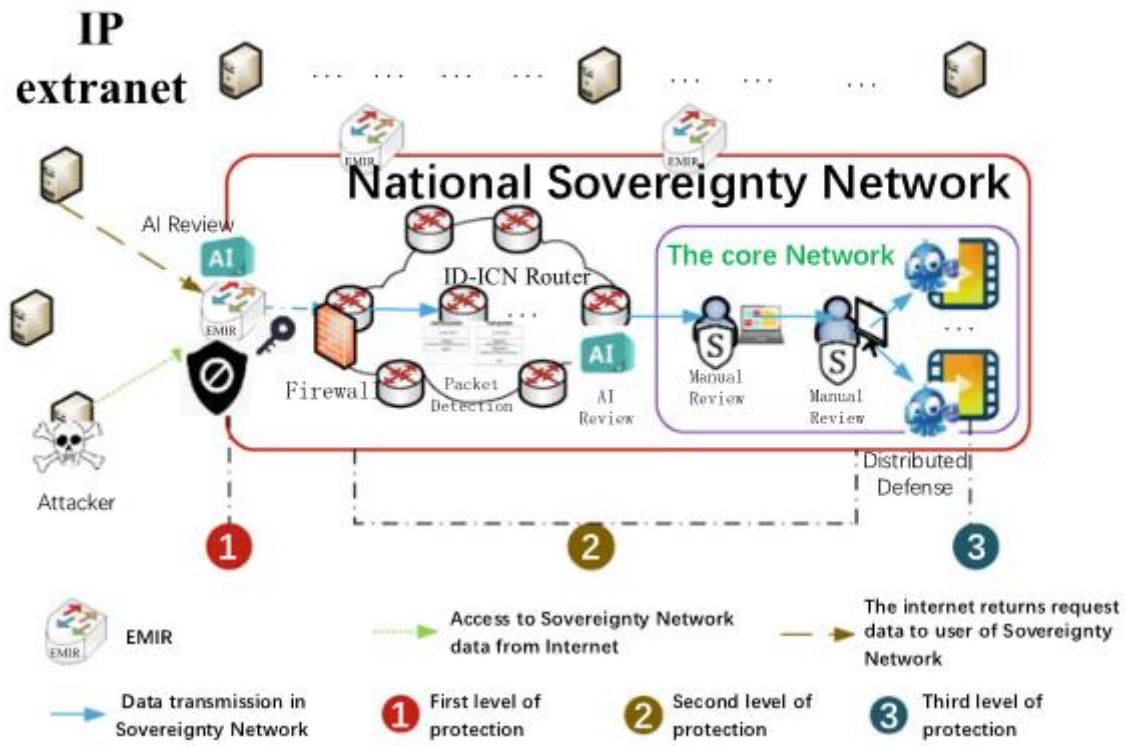
Kami mengasumsikan penyerang dari jaringan eksternal, yang proses penyerangannya ditunjukkan pada Gambar 4.28. Untuk level ketiga, ketika probabilitas gangguan acak adalah 0,0001, probabilitas kondisi mapan untuk memecahkan sistem produksi dan penyiaran CMD dihitung sebesar 1,30 10−6.

Untuk level kedua, kami mengasumsikan bahwa ada lima filter dengan efektivitas yang sama (yaitu, x1 ¼ x2 ¼ x3 ¼ x4 ¼ x5 ¼ 0:137931) dan penyerang lolos dari setiap filter dengan probabilitas l ¼ 0:160. Maka kita memiliki

$$E[S] = \frac{0}{[(1-\omega)\mu - \omega]} = 1.25 \times 10^{8}\,(s) \qquad (4.22)$$

Dengan mempertimbangkan efek penyaringan dari dua level pertama, waktu pemecahan sistem diperkirakan 1,517 1023 detik. Dengan kata lain, dibutuhkan waktu 4,8 1015 tahun untuk memecahkan sistem secara rata-rata.

Oleh karena itu, untuk jaringan kedaulatan dengan mekanisme penyaringan lima level, tiga redundansi sistem produksi dan penyiaran CMD dan frekuensi gangguan 0,0001, ketika tingkat kegagalan penyaringan setiap perangkat adalah 0,16 (yaitu, 1,6 dari 10 pesan berbahaya dapat lolos secara rata-rata), waktu kegagalan sistem produksi dan penyiaran mencapai 4,8 1015 tahun. Hasil perhitungan ini diperoleh dalam kondisi serangan longgar yang jelas yang mengarah pada peningkatan tingkat keberhasilan serangan.



Gambar 4.28 Proses penyerangan pada jaringan kedaulatan

Tabel 4.9 Hubungan frekuensi gangguan dan waktu kegagalan

Disturbance frequency	0.001	0.0001	0.00001	0.000001	0.0000001
Attack time (year)	4.8×10^{16}	4.8×10^{15}	4.8×10^{14}	4.8×10^{13}	4.8×10^{12}

Namun, dalam penerapan praktis, tingkat keberhasilan setiap operasi penyaringan jauh lebih tinggi dari 14%, dan tingkat keberhasilan serangan dari satu pelaksana jauh kurang dari 100%. Oleh karena itu, dalam jaringan kedaulatan, waktu kegagalan sistem inti juga lebih lama dari 4,8 x 1015 tahun. Hubungan yang sesuai antara frekuensi gangguan dan waktu untuk merusak jaringan kedaulatan ditunjukkan pada Tabel 4.9.

4.7.6 Kesimpulan

Menurut analisis di atas, jaringan kedaulatan dapat menyesuaikan konfigurasinya untuk mewujudkan pertahanan yang lebih efektif. Pembela dapat mengadopsi konfigurasi yang lebih murah dalam lingkungan yang aman. Dalam keadaan tersebut, meskipun

penyerang secara teoritis dapat membobol sistem, hal itu akan memakan waktu jutaan tahun dan tidak akan layak dalam kenyataan. Ketika lingkungan jaringan buruk, biaya pertahanan jaringan kedaulatan dapat ditingkatkan untuk ditukar dengan keamanan yang lebih tinggi. Dalam keadaan tersebut, waktu keberhasilan serangan teoritis lebih lama. Dengan kata lain, penyerang tidak dapat membobol sistem.

Dengan berbagai mekanisme keamanan, jaringan kedaulatan telah berhasil membalikkan ketidakseimbangan antara penyerang dan pembela. Dilindungi oleh serangkaian teknologi yang diusulkan, termasuk sistem jaringan yang berpusat pada identitas, blockchain, EMIR, serta teknologi CMD, jaringan produksi dan penyiaran serta sub-jaringan penting lainnya dari jaringan kedaulatan dapat bekerja pada tingkat keamanan yang tinggi.

4.8 KONTROL TRANSMISI

Mode transmisi jaringan TCP/IP tradisional didefinisikan sebagai komunikasi ujung ke ujung dalam semantik push. Namun, dengan popularitas Internet dan pertumbuhan eksponensial kuantitas data, pengguna lebih peduli tentang cara mendapatkan konten, dan tidak peduli dengan lokasi produsen konten. Untuk mengatasi masalah ini, jaringan yang berpusat pada konten dengan semantik pull telah diusulkan, yang membuat mode transmisi jaringan kompatibel dengan persyaratan komunikasi pengguna.

Dengan mempertimbangkan penyebaran progresif jaringan kedaulatan dan aplikasi dalam berbagai skenario, kami mengusulkan MIT, skema kontrol transmisi berdasarkan MIN. MIT mendukung kontrol transmisi baik dalam semantik push maupun semantik pull, mewujudkan komunikasi data yang andal dalam berbagai persyaratan bisnis jaringan kedaulatan. MIT mendeteksi kemacetan berdasarkan mekanisme manajemen antrean aktif, lalu memberi sinyal kepada klien dengan menandai paket tertentu secara eksplisit, sehingga klien dapat mengurangi laju pengirimannya sesuai dengan status kemacetan jaringan. Sementara itu, MIT mengatur laju penerusan paket pada antarmuka keluaran router dengan mempertahankan satu antrean virtual per aliran untuk menjamin pemanfaatan sumber daya jaringan yang memadai.

4.8.1 Desain MIT

MIT mendukung kontrol transmisi baik dalam semantik push maupun semantik pull, yang didefinisikan sebagai berikut:

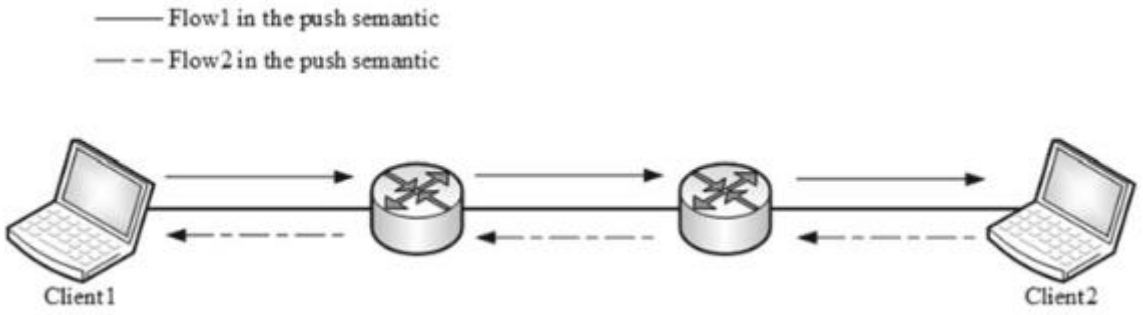
(1) Semantik Push

Semantik push adalah mode transmisi ujung-ke-ujung yang berorientasi pada host, klien berlangganan informasi terlebih dahulu, lalu server mengirim informasi yang tersedia kepada klien. Seluruh proses transmisi data didominasi oleh pengirim, dan data yang dikirimkan tidak akan di-cache di node perantara jaringan. Klien akan memeriksa data yang diterima dari server, jika tidak salah, klien mengonfirmasi hal ini dengan mengirimkan paket kembali ke server dengan tanda ack yang ditetapkan. Kontrol transmisi di bawah semantik push diwakili oleh TCP, berlaku untuk layanan Pesan Instan, seperti konferensi video waktu nyata, obrolan daring, telepon Internet, dan skenario interaksi lainnya.

(2) Semantik Tarik

Semantik tarik telah muncul dalam beberapa tahun terakhir, sebagai mode transmisi berorientasi konten yang digerakkan oleh konsumen data. Ada dua jenis paket, paket permintaan dan paket respons. Dalam semantik ini, konsumen menarik paket respons dengan mengirimkan paket permintaan ke jaringan. Satu paket respons cocok dengan satu paket permintaan, dan keduanya berisi nama konten yang diminta. Setiap node sumber konten atau node perantara yang memenuhi persyaratan dapat mengembalikan data yang diminta. Paket respons kembali melalui jalur yang berlawanan dengan paket permintaan dan konten dapat di-cache di node perantara sesuai dengan strategi caching. Kontrol transmisi di bawah semantik tarik memiliki skalabilitas yang kuat dan sering digunakan untuk distribusi konten, yang dapat mewujudkan penggunaan kembali sumber daya jaringan yang efisien.

Berdasarkan konsep-konsep di atas, kami selanjutnya mendefinisikan konsep aliran dalam semantik dorong dan semantik tarik.



Gambar 4.29 Transmisi dalam semantik push

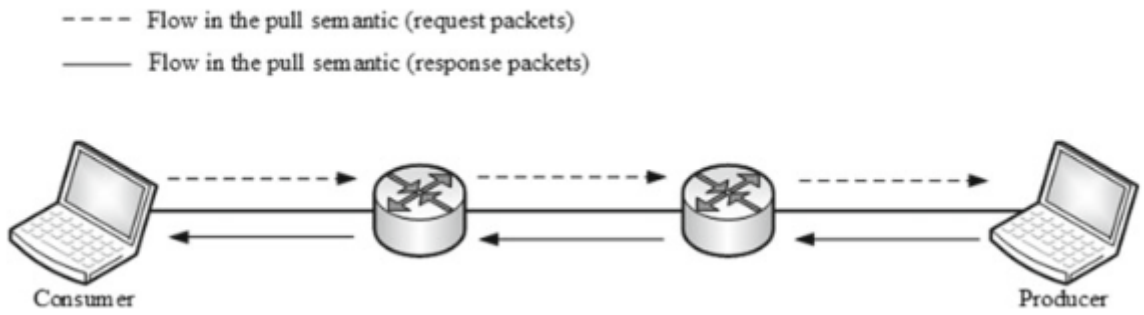
(1) Alur dalam Semantik Push

Alur dalam semantik push terdiri dari paket satu arah yang dikirimkan dari pengirim ke penerima, dan menggunakan pengenal layanan untuk mengidentifikasi alur. Misalnya, percakapan antara Klien1 dan Klien2, seperti yang ditunjukkan pada Gambar 4.29, satu alur dari Klien1 ke Klien2 dan alur lainnya dari Klien2 ke Klien1, keduanya sepenuhnya independen dan tidak terkait. Arah alur adalah dari sumber ke tujuan, dan hulu dan hilir ditentukan menurut arah alur.

(2) Alur dalam Semantik Pull

Alur dalam semantik pull terdiri dari paket permintaan dan paket respons untuk konten yang diminta, dan menggunakan nama konten untuk mengidentifikasi alur. Seperti yang ditunjukkan pada Gbr. 4.30, konsumen mengeluarkan permintaan konten, dan permintaan tersebut masuk ke cache sumber konten (produsen). Kami mendefinisikan arah konsumen sebagai hilir, arah sumber konten sebagai hulu, dan paket permintaan diteruskan dari hilir ke hulu. Setelah mencapai sumber konten, paket respons yang berisi konten yang diminta akan dikirim ke konsumen.

Baik klien maupun router terlibat dalam kontrol transmisi. Untuk mewujudkan skema pembentukan hop-by-hop, MIT mempertahankan satu antrean FIFO virtual per aliran di setiap antarmuka keluaran, yang diidentifikasi dengan nama pengenal. Kami menggunakan f i untuk mewakili aliran j di antarmuka keluaran i, menggunakan qi untuk mewakili antrean virtual aliran j di antarmuka keluaran i. Aliran dalam semantik push dan semantik pull dikaitkan dengan antrean virtual yang berbeda, yang diidentifikasi oleh pengenalnya.



Gambar 4.30 Transmisi dalam semantik tarikan

Berdasarkan definisi di atas, MIT terdiri dari empat komponen:

(1) Deteksi Kemacetan Aktif: MIT secara langsung mendeteksi status kemacetan di node perantara melalui mekanisme manajemen antrean aktif.

(2) Pemberitahuan Kemacetan Eksplisit: Setelah mendeteksi kemacetan, router memberi sinyal kemacetan dengan menandai paket, dan paket yang ditandai akan diumpankan kembali ke klien.

(3) Pembentukan Laju Hop-by-Hop: Router secara dinamis menyesuaikan laju penerusan sesuai dengan perbedaan antara kapasitas transmisi uplink dan downlink saat ini untuk mencapai pembentukan laju hop-by-hop.

(4) Penyesuaian Laju Klien: Klien secara dinamis menyesuaikan ukuran jendela kemacetan yang ditingkatkan pada paket yang tidak ditandai dan dikurangi pada paket yang ditandai.

4.8.2 Deteksi Kemacetan Aktif

Algoritma CoDel adalah mekanisme AQM (Active Queue Management). Ia mendeteksi kemacetan dengan mengukur penundaan antrean ("waktu singgah") setiap paket pada tautan keluarnya. Jika waktu singgah minimum selama periode waktu tertentu (default: 100 ms) melebihi ambang batas (default: 5 ms), ia menganggap tautan ini mengalami kemacetan. Algoritma CoDel secara efektif dapat menghindari masalah osilasi ukuran antrean yang disebabkan oleh lalu lintas yang meledak dan menjaga antrean tetap kecil selama ukuran buffer router diatur dalam rentang yang wajar.

MIT menggunakan algoritma CoDel untuk secara aktif mendeteksi kemacetan di router perantara, dan mendeteksi kemacetan dengan mengukur penundaan antrean ("waktu singgah") setiap paket pada tautan keluarnya.

4.8.3 Pemberitahuan Kemacetan Eksplisit

Kemacetan jaringan terutama disebabkan oleh kecepatan transmisi klien yang sangat cepat, yang membuat jumlah data yang dikirimkan melalui tautan melebihi kapasitas tautan dalam kondisi jaringan saat ini. Oleh karena itu, setelah router mendeteksi kemacetan jaringan, diperlukan mekanisme untuk memberi tahu klien tentang status kemacetan jaringan saat ini, sehingga klien dapat mengurangi kecepatan transmisi untuk mengurangi kemacetan jaringan.

Pemberitahuan Kemacetan Eksplisit (ECN) adalah mekanisme untuk memberi sinyal kemacetan dalam jaringan TCP/IP, router yang mengetahui ECN dapat menetapkan tanda di header IP alih-alih membuang paket untuk memberi sinyal kemacetan yang akan datang. Penerima paket menggemakan indikasi kemacetan ke pengirim, yang mengurangi kecepatan transmisinya seolah-olah mendeteksi paket yang dibuang.

MIT memberi tahu klien tentang status jaringan saat ini melalui pemberitahuan kemacetan eksplisit, yang memerlukan bidang tanda kemacetan opsional di header paket untuk mencatat status kemacetan jaringan. Ketika router mendeteksi kemacetan, router akan menetapkan bidang kemacetan dalam paket. Klien menilai status jaringan dengan menentukan apakah paket yang diterima membawa tanda kemacetan.

Melalui pemberitahuan kemacetan yang eksplisit, informasi kemacetan yang dibawa dalam paket akan diumpankan kembali ke klien. Untuk aliran dalam semantik push, setelah paket yang ditandai tiba di penerima, penerima akan menetapkan bidang kemacetan yang sesuai di header paket ACK, sehingga informasi kemacetan dalam paket yang diterima dapat diumpankan kembali ke pengirim oleh paket ACK. Untuk aliran dalam semantik pull, paket respons yang membawa tanda kemacetan akan diteruskan ke node hilir hingga mencapai klien.

4.8.4 Pembentukan Laju Hop-by-Hop

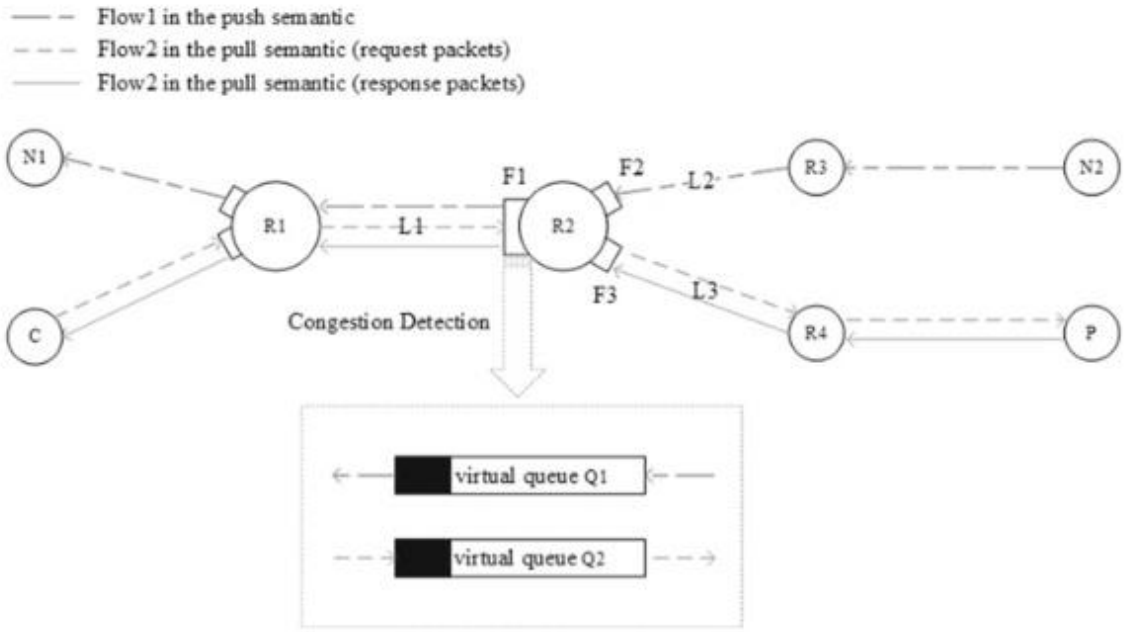
Setelah deteksi kemacetan, router akan menyesuaikan laju penerusan paket melalui mekanisme pembentukan laju hop-by-hop. Rinciannya adalah sebagai berikut:

(1) Ketika tidak terjadi kemacetan pada antrean keluar router, hal ini menunjukkan bahwa pemanfaatan sumber daya pada tautan keluar tidak melebihi kapasitas tautan. Pada saat ini, router tidak mengaktifkan mekanisme pembentukan laju.

(2) Setelah router mendeteksi bahwa salah satu tautan keluarnya mengalami kemacetan, status antarmuka keluaran yang sesuai akan ditandai sebagai kemacetan. Karena MIT mengharuskan untuk mempertahankan satu antrean FIFO virtual per aliran di setiap antarmuka keluaran, mekanisme pembentukan laju hop-by-hop dapat menyesuaikan laju penerusan paket pada antarmuka yang mengalami kemacetan melalui antrean virtualnya. Oleh karena itu, router akan secara dinamis menyesuaikan laju penerusan sesuai dengan perbedaan kapasitas transmisi uplink dan downlink saat ini untuk mencapai pembentukan laju hop-by-hop.

Perhatikan bahwa ketika klien berhenti mengirim paket, mungkin ada beberapa paket dalam antrean virtual yang belum diteruskan. Untuk mengatasi masalah ini, ketika aliran berhenti

mengirim paket, setiap router akan mendeteksi apakah antrean virtual aliran kosong, dan jika tidak, meneruskan paket yang tersisa dalam antrean virtual pada laju penerusan terakhir.



Gambar 4.31 Model pembentukan laju router

Mekanisme pembentukan laju hop-by-hop di atas ditunjukkan pada Gambar 4.31. N1 dan N2 adalah sepasang simpul terminal yang mengadopsi semantik push. C dan P masing-masing adalah konsumen dan produsen, yang mengadopsi semantik pull. R1, R2, R3 dan R4 adalah router dalam jaringan. F1, F2 dan F3 adalah antarmuka pada router R2. L1, L2 dan L3 adalah tautan yang terhubung dengan antarmuka F1, F2 dan F3 masing-masing. Flow1 adalah aliran yang mengadopsi semantik push dan Flow2 adalah aliran yang mengadopsi semantik pull. Q1 adalah antrean virtual yang dikelola untuk Flow1 di antarmuka F1 router R2, dan Q2 adalah antrean virtual yang dikelola untuk Flow2 di antarmuka F1 router R2. Dengan asumsi L1, L2, dan L3 memiliki kapabilitas yang sama, maka kemacetan jaringan dapat terjadi di tautan kemacetan L1.

Jika router R2 telah mendeteksi tautan L1 mengalami kemacetan, maka router akan menandai status antarmuka F1 sebagai kemacetan dan mengelola antrean virtual untuk setiap aliran yang melewati antarmuka F1. Untuk Flow1 dalam semantik push dan melalui antarmuka F1, paket akan diantrekan dalam antrean FIFO virtualnya Q1 yang dilayani pada laju pembentukan. Untuk Flow2 dalam semantik pull dan melalui antarmuka F1, paket permintaan akan diantrekan dalam antrean FIFO virtualnya Q2 yang dilayani pada laju pembentukan. Kemacetan pada tautan L1 akan segera diatasi melalui pembentukan laju pada antarmuka F1 router R2 dan penyesuaian laju klien berdasarkan paket bertanda yang diterima.

4.8.5 Penyesuaian Laju Klien

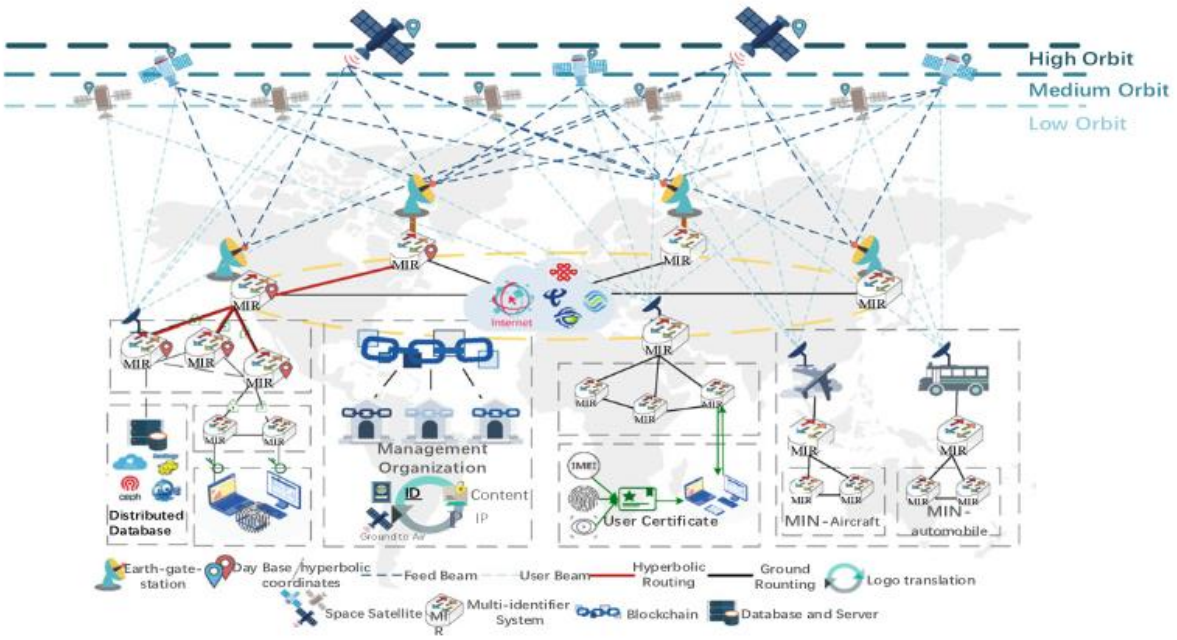
Klien mempertahankan jendela kemacetan (yang menentukan jumlah maksimum paket yang sedang dikirim) untuk setiap aliran, yang ditingkatkan pada paket yang tidak

bertanda dan dikurangi pada paket yang bertanda. Melalui mekanisme penyesuaian laju ini, klien dapat mencapai laju pengiriman yang optimal dan menyesuaikannya secara dinamis untuk beradaptasi dengan status jaringan yang berubah. MIT dapat mengimplementasikan banyak algoritma TCP berbasis kehilangan klasik seperti Reno, New Reno, HTCP, HSTCP, BIC, dan CUBIC. Satu-satunya perbedaan dengan TCP tradisional adalah bahwa penurunan jendela dipicu tidak hanya oleh batas waktu, tetapi juga oleh paket yang bertanda. Setelah bereksperimen dengannya, algoritma CUBIC dipilih untuk mekanisme penyesuaian laju klien di MIT.

Selain itu, untuk menghindari pengurangan tajam jendela kemacetan yang disebabkan oleh lonjakan lalu lintas, algoritma pemulihan kehilangan konservatif berbasis TCP SACK klasik diperkenalkan di klien. Ketika penghitung waktu klien habis, MIT menggunakan algoritma pemulihan kerugian konservatif untuk membatasi penurunan jendela: klien melakukan paling banyak satu penurunan jendela per RTT, sehingga MIT dapat mencegah osilasi jaringan yang disebabkan oleh lalu lintas yang meledak. Ketika klien menerima paket yang ditandai, mekanisme di Bagian 4.8.2 dapat secara efektif menghindari terlalu banyak paket yang ditandai. MIT tidak menggunakan algoritma pemulihan kerugian konservatif untuk membatasi penyesuaian jendela untuk paket yang ditandai, sehingga klien dapat dengan cepat merespons kemacetan jaringan.

4.9 MODEL PENGALAMATAN UNTUK JARINGAN TERPADU ANTARIKSA-TERESTRIAL

Meskipun sistem komunikasi terestrial telah berkembang pesat dalam beberapa tahun terakhir, kualitas layanannya bergantung pada morfologi permukaan dan bencana alam. Komunikasi satelit, yang tidak terpengaruh oleh waktu, tempat, atau lingkungan, secara bertahap telah menarik perhatian orang, dan Jaringan Terpadu Antariksa-Terestrial (FSTIN) telah dibentuk untuk menyediakan layanan komunikasi dengan kapasitas tinggi dan jangkauan yang lancar. Untuk meningkatkan kinerja jaringan kedaulatan, kami bermaksud membangun Jaringan Terpadu Antariksa-Terestrial berdasarkan MIN. Akan tetapi, karena konstruksi Jaringan Terpadu Antariksa-Terestrial yang bertingkat-tingkat, serta kekhususan jaringan satelit, jaringan ini rentan terhadap paparan simpul satelit, keterbukaan saluran, interkoneksi jaringan heterogen, perubahan dinamis tinggi topologi, penundaan transmisi yang besar, varians penundaan yang besar, kapasitas pemrosesan on-board yang terbatas, dan sebagainya. Jaringan Multi-Identifier Antariksa-Terestrial-Virtual Private Network (ST-MIN-VPN) diusulkan berdasarkan MIN. Strategi perutean serakah berdasarkan teknologi perutean hiperbolik dirancang untuk jaringan terestrial, dan algoritma perutean satelit adaptif mandiri terdistribusi ringan berdasarkan penundaan dirancang untuk jaringan satelit dengan tautan antarsatelit. Skema perutean dan strategi penerusan yang berbeda dirancang untuk skenario aplikasi yang berbeda. Strategi perutean dan skema manajemen mobilitas ST-MIN ditunjukkan pada Gambar 4.32.



Gambar 4.32 Arsitektur routing di ST-MIN

4.9.1 Algoritma Perutean Hiperbolik dalam Jaringan Terestrial

Ruang pengenal ST-MIN mengadopsi gagasan hierarki. Domain jaringan dibagi menjadi k level, dan topologi jaringan setiap domain level dipetakan ke ruang hiperbolik secara berurutan. MIS mengalokasikan koordinat hiperbolik untuk setiap router tepi domain, dan menggunakan setiap koordinat hiperbolik sebagai pengenal hiperbolik setiap domain. Setiap node mencatat pengenal hiperboliknya sendiri dan pengenal hiperbolik node tetangganya. Kami berasumsi bahwa seluruh domain jaringan dibagi menjadi k level, yang ditentukan oleh persyaratan aktual dan stabilitas topologi. Di setiap level, router dapat mendukung N pengenal jaringan. MIS menanamkan setiap domain level jaringan terestrial ke dalam ruang hiperbolik secara berurutan, sehingga himpunan koordinat hiperbolik $\eth Ri;\ HiÞ, i \text{¼} 1;\ 2;\ \ldots;\ k$ dari setiap domain level dapat diperoleh. Jaringan yang terbagi mendukung ruang pengenal jaringan dengan N orde besaran.

Ambil jaringan tiga tingkat sebagai contoh. Domain tingkat-1 berisi beberapa simpul domain. Topologi jaringan yang dibentuk oleh semua simpul dalam domain tingkat-1 tertanam ke dalam ruang hiperbolik untuk memperoleh set koordinat hiperbolik domain tingkat-1 R1; H1. Sebagai pengenal hiperbolik simpul dalam domain tingkat-1,

R1; H1 mengarahkan perutean antardomain antara domain tingkat-1. Setiap domain tingkat-1 dibagi menjadi beberapa domain tingkat-2, topologi jaringan yang dibentuk oleh simpul dalam domain tingkat-2 tertanam ke dalam ruang hiperbolik untuk memperoleh set koordinat hiperbolik domain tingkat-2 R2; H2, yang mengarahkan perutean antardomain dalam domain tingkat-2. Karena setiap domain tingkat-2 termasuk dalam domain tingkat-1, pengenal hiperbolik lengkapnya adalah " R1; H1 : R2; H2 ". Demikian pula, setiap domain tingkat-2 dapat dibagi lagi menjadi beberapa domain tingkat-3. Pengguna termasuk dalam domain level-3.

Saat ini, algoritma utama dari hyperbolic embedding adalah HyperMap yang diusulkan oleh Papadopoulos [26]. Ia dapat menanamkan topologi jaringan nyata yang diberikan G (V, E) ke dalam ruang hiperbolik dan menghitung koordinat hiperbolik r; h dari node yang tertanam. Prosedur Algoritma HyperMap ditunjukkan pada Algoritma 4.7.

Algorithm 4.7: HyperMap Embedding Algorithm

Input:
Undirected connected Graph $G = (V, E)$
Output:
Hyperbolic coordinates $(r_i, \theta_i)_{i=1}^{t}$ $(t = |V|)$
Begin
1: Sort node degrees in decreasing order $k_1 > k_2 > \cdots > k_t$ with ties broken arbitrarily.
2: Call node $i, i = 1,2, \ldots, t$, the node with degree k_i.
3: Node $i = 1$ is born, assign to its initial radial coordinate $r_1 = 0$ and random angular coordinate $\theta_1 \in [0,2\pi]$
4: **for** $i = 2$ to t **do**
5: node i is born, assign to its initial radial coordinate $r_i = \frac{2}{\zeta} \ln i$.
6: Increase the radial coordinate of every existing node $j < i$ according to $r_j(i) = \beta r_j + (1 - \beta) r_i$
7: Assign to node i angular coordinate θ_i maximizing the likelihood $L = \prod p(x_{ij})^{\alpha_{ij}} [1 - p(x_{ij})]^{1-\alpha_{ij}}$.
8: **end for**
End of Algorithm

Kompleksitas komputasi hyperbolic embedding dari algoritma HyperMap adalah $O\ n3$. Dalam beberapa tahun terakhir, Bläsius mengusulkan algoritma Fast Embedding untuk meningkatkan metode hyperbolic embedding dan mengurangi kompleksitas komputasi menjadi O n . Pseudocode dari Algoritma fast embedding ditunjukkan pada Algoritma 4.8:

Algorithm 4.8: Fast Embedding Algorithm

Input: Undirected connected Graph $G = (V, E)$
Output: Hyperbolic coordinates $(r_i, \theta_i)_{i=1}^{n}$ $(n = |V|)$
Begin
32: Estimate global parameters n, R, α, T
33: Estimate radial coordinates r_i
34: **for** all nodes v ∈ V **do**
35: Place v in layer L_i if $\deg(v) \in [2^i, 2^{i+1} - 1]$.
36: Embed all nodes in layers≥ $\frac{\log n}{2}$
37: **for** i = $\frac{\log n}{2} - 1 \ldots 0$ **do**
38: **for** log n times **do**
39: **for all** v ∈ $\bigcup_{j \geq i} L_j$ **do**
40: Embed v by optimizing its loglikelihood
41: **end for**
42: **end for**
43: **end for**
End of Algorithm

Dalam skema yang diusulkan, algoritma Fast Embedding digunakan untuk melakukan hyperbolic embedding untuk domain masing-masing level. Ambil domain tiga level sebagai contoh, proses spesifiknya adalah sebagai berikut:

(1) Pertama, MIS menggunakan algoritma Fast Embedding untuk menanamkan topologi jaringan dari node domain level-1 ke dalam ruang hiperbolik dan memperoleh set koordinat hiperbolik node domain level-1 R1; H1. Koordinat hiperbolik digunakan sebagai pengidentifikasi hiperbolik node domain level-1. Karena topologi domain level-1 stabil, koordinat hiperbolik node domain tidak akan berubah dalam jangka waktu tertentu. (2) Kedua, MIS menggunakan algoritma Fast Embedding untuk menanamkan setiap topologi jaringan dari node domain level-2 ke dalam ruang hiperbolik, untuk memperoleh set koordinat hiperbolik node domain level-2 R2; H2. Untuk menjaga keunikan pengidentifikasi di seluruh jaringan dan mendukung komunikasi lintas domain, pengidentifikasi hiperbolik lengkap dari node domain level-2 didefinisikan sebagai " R1; H1 : R2; H2 ", dan router tepi dari setiap domain menyediakan transformasi identitas lintas domain. Proses Greedy Routing antara domain berdasarkan pengenal hiperbolik adalah sebagai berikut:

   (1) Kami berasumsi bahwa koordinat hiperbolik dari simpul sumber adalah ðrs; hsÞ, dan koordinat hiperbolik dari simpul tujuan adalah ðrd; hdÞ. Koordinat hiperbolik dari simpul tujuan dienkapsulasi dalam paket dan simpul sumber mengirimkan paket ke simpul tujuan melalui penerusan simpul perantara.
   (2) Ketika simpul perantara menerima paket, ia akan menghitung jarak hiperbolik dari setiap simpul tetangga ðri; hiÞ ke simpul tujuan ðrd; hdÞ sesuai dengan rumus jarak hiperbolik xid ¼ arccosh cosh ri cosh rj sinh ri sinh rjcoshid , hid p p hi hd , kemudian memilih simpul tetangga terdekat sebagai hop berikutnya untuk meneruskan paket.
   (3) Melalui proses di 2), paket akhirnya mencapai simpul tujuan ðrd; hdÞ.

Algoritma 4.9 menunjukkan algoritma Greedy Routing yang dijalankan oleh setiap node dalam jaringan dengan strategi routing di atas.

Algorithm 4.9: Greedy Routing Algorithm

Input:
G: network topology, v: current node, d: destination node
Output:
$next$: the nearest neighbor node
Begin

```
1:    function GR(G, v, d)  //
2:        d_v ← hyperbolic_distance(G, v, d)
3:        for all v_n ∈ neighbors(G, v) do
4:            D_n[n] ← hyperbolic_distance(G, v_n, d)
5:        end for
6:        v_n_min, d_n_min ← key(min D_n), min D_n
7:        if d_n_min < d_v then
8:            next ← v_n
9:            return next
10:       end if
11:   end function
```

End of Algorithm

Jika terjadi kegagalan jangka pendek pada beberapa node, jalur alternatif dapat ditemukan dengan menambahkan mekanisme backtracking ke algoritma simple greedy routing. Dalam kasus ini, koordinat hiperbolik node tidak perlu diubah.

4.9.2 Routing Adaptif Berbasis Delay untuk Jaringan Satelit

Algoritma routing satelit adaptif mandiri terdistribusi berbasis delay cocok untuk jaringan satelit dengan tautan antar-satelit. Algoritma menghitung delay propagasi dan delay antrean setiap kandidat ke hop berikutnya untuk mendapatkan probabilitas pemilihan hop berikutnya. Kemudian paket diteruskan sesuai dengan probabilitas tersebut. Selain itu, ketika beban jaringan satelit rendah, transmisi data antara perangkat jaringan satelit harus dilakukan melalui jaringan satelit terlebih dahulu. Ketika jaringan satelit kelebihan beban atau tautan gagal, data akan dikirim ke stasiun bumi dan diteruskan oleh jaringan terestrial.

Algoritma mengharuskan setiap satelit untuk membuat Tabel Informasi Akses dan Tabel Informasi Status. Dalam Tabel Informasi Akses, entri AITs mencatat informasi pengguna dan stasiun bumi yang terhubung ke satelit saat ini, dan entri AITu, AITd, AITl, dan AITr mencatat informasi pengguna dan stasiun bumi yang terhubung ke satelit di arah atas, bawah, kiri, dan kanan, berturut-turut. Dalam Tabel Informasi Status, entri SITu, SITd, SITl, dan SITr mencatat status tautan, ukuran paket dalam antrean buffer, beban antrean buffer, dan koefisien redaman saluran satelit di arah atas, bawah, kiri, dan kanan, berturut-turut.

Algoritme dirancang dengan mekanisme notifikasi. Setiap simpul satelit secara teratur mengirimkan pesan notifikasi ke tetangganya, termasuk tabel informasi akses satelit saat ini AITs, ukuran paket qi dalam antrean buffer, beban Li antrean buffer, dan koefisien redaman saluran e. Ketika simpul satelit menerima paket, simpul tersebut perlu memperoleh simpul kandidat hop berikutnya sesuai dengan alamat tujuan dan informasi lokasi di header paket. Jika alamat tujuan dalam AIT, node satelit akan meneruskan paket ke pengguna di jaringan terestrial. Jika alamat tujuan dalam AITu, AITd, AITl, atau AITr, node satelit akan meneruskan

paket ke satelit terkait. Jika tidak, kandidat hop berikutnya diperoleh menurut informasi lokasi tujuan dan tabel SIT.

Bergantung pada orbit dan posisi orbit node satelit saat ini dan node satelit tujuan, jumlah kandidat untuk hop berikutnya biasanya satu atau dua. Jika hanya ada satu kandidat untuk hop berikutnya, probabilitas node ini menjadi hop berikutnya adalah 100%. Jika ada dua kandidat untuk hop berikutnya, kita harus menghitung probabilitas yang mana yang menjadi hop berikutnya. Dengan asumsi berdasarkan node saat ini, node tersebut menghadapi pilihan hop berikutnya dalam arah vertikal dan arah horizontal, dan jalur setelah dua hop sepenuhnya bertepatan, yang berarti probabilitas perhitungan hanya mempertimbangkan penundaan dua hop berikutnya. Jika hop berikutnya dalam arah vertikal adalah Nv dan hop berikutnya dalam arah horizontal adalah Nh, maka probabilitas hop berikutnya berbanding terbalik dengan total penundaan dari dua jalur dari node saat ini ke hop kedua melalui Nv dan Nh, masing-masing. Total penundaan adalah jumlah penundaan propagasi dan penundaan antrean, yang diperoleh sebagai berikut:

$$T_{total} = T_{propagation} + T_{queue} \qquad (4.23)$$

Sebagai algoritma terdistribusi, perhitungan probabilitas mengabaikan penundaan antrean pada simpul satelit lainnya. Probabilitas Pv untuk memilih hop berikutnya dalam arah vertikal dan probabilitas Ph untuk memilih hop berikutnya dalam arah horizontal dapat diperoleh dengan persamaan berikut:

$$\frac{P_v}{P_h} = \frac{T_p(intra) + T_p(inter_h) + T_q(h)}{T_p(intra) + T_p(inter_v) + T_q(v)} \qquad (4.24)$$

di mana T_p adalah penundaan propagasi dan T_q adalah penundaan antrean. Kami menggunakan R, H, dan c untuk masing-masing mewakili radius bumi, ketinggian orbit, dan kecepatan cahaya. N mewakili jumlah satelit dalam satu orbit, dan M mewakili jumlah orbit satelit. Penundaan propagasi antara satelit yang berdekatan dalam orbit yang sama dihitung sebagai berikut:

$$T_p(intra) = \frac{2\pi * (R+H)}{N * c} \qquad (4.25)$$

Asumsikan lintang N_h adalah lath dan lintang N_v adalah latv, maka penundaan propagasi antara node arus ke N_h, dan N_v ke node hop kedua adalah:

$$T_p(inter_h) = \frac{2\pi * (R+H) * \cos(lat_h)}{2 * M * c} \qquad (4.26)$$

$$T_p(inter_v) = \frac{2\pi * (R+H) * \cos(lat_v)}{2 * M * c} \qquad (4.27)$$

Asumsikan ukuran paket N_h dan

$$T_q(h) = \frac{q_h}{C * \varepsilon_h} \quad (4.28)$$

$$T_q(v) = \frac{q_v}{C * \varepsilon_v} \quad (4.29)$$

Akhirnya, menurut rasio P_v dan P_h probabilitas hop berikutnya dalam arah vertikal dan arah horizontal dapat dihitung. Oleh karena itu, node dapat meneruskan paket sesuai dengan probabilitas yang dihitung.

Proses lengkap dari algoritma perutean satelit adaptif terdistribusi berbasis penundaan adalah sebagai berikut:

Ketika node satelit menerima paket, ① jika itu adalah paket minat dengan pengenal konten, maka node satelit akan memeriksa CS dan mengembalikan salinan jika cache ditemukan. Jika tidak, node satelit akan memeriksa PIT untuk memverifikasi apakah entri untuk nama konten yang sama sudah ada, jika ada, menambahkan informasi antarmuka yang masuk ke entri dan membuang paket minat, jika tidak, membuat entri PIT baru, dan kemudian mengikuti proses perutean normal. Jika itu adalah paket data dengan pengenal konten, maka akan diteruskan sesuai dengan informasi antarmuka dalam entri PIT. Jika nama paket data tidak dapat ditemukan dalam PIT, maka akan dibuang. ② Jika paket yang diterima memiliki pengenal identitas atau pengenal layanan, paket tersebut akan diproses secara langsung sesuai dengan proses perutean normal. Proses perutean spesifik ditunjukkan pada Algoritma 4.10.

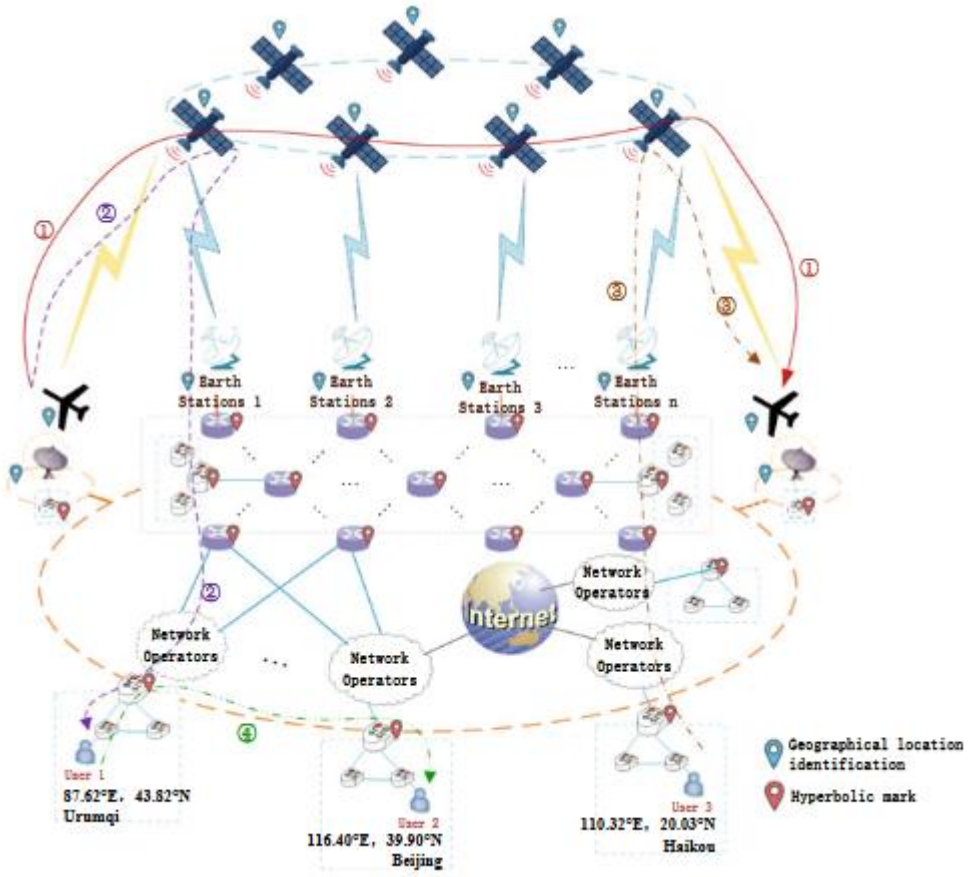
Perutean terpadu ST-MIN dapat dibagi menjadi perutean antariksa, perutean antariksa ke terestrial, perutean terestrial ke antariksa, perutean terestrial ke terestrial. ① Perutean antariksa mengacu pada perutean paket yang dikirimkan antara perangkat komunikasi yang terhubung ke jaringan satelit. ② Perutean antariksa ke terestrial mengacu pada perutean yang dilakukan perangkat jaringan satelit untuk mengirimkan paket ke perangkat jaringan terestrial. ③ Perutean terestrial ke antariksa mengacu pada perutean yang dilakukan perangkat jaringan terestrial untuk mengirimkan paket data ke perangkat jaringan satelit. ④ Perutean terestrial ke terestrial mengacu pada perutean paket yang dikirimkan antara perangkat terestrial.

Dalam perutean antariksa, proses komunikasi ditetapkan sebagai berikut. Pengirim mencari pengenal GPS penerima sesuai dengan pengenal identitas penerima di MIS. Pengenal GPS digunakan sebagai tujuan paket. Kemudian paket tersebut diteruskan di ST-MIN. Ketika kondisi jaringan satelit baik, paket tersebut dapat sampai ke penerima melalui transmisi di jaringan satelit, jika tidak, paket tersebut dikirim ke jaringan terestrial untuk diteruskan. Akhirnya, paket tersebut akan sampai ke penerima. Proses perutean ditunjukkan sebagai rute ① pada Gambar 4.33.

Algorithm 4.10: Satellite Routing Algorithm

Input:
Packet input from an input port's lower layer
Output:
Specific neighbor satellite or destination ground node
Begin

if des_id include in AIT_s **then**
    forward packet to the destination through satellite to ground interface.
else if des_id include in either of AIT_u, AIT_d, AIT_l, AIT_r **then**
    forward packet to that direction's satellite which advertise this user information.
end if
if packet' flag $LOAD = 1$ **then**
    if any ground station include in AIT_s **then**
        forward packet to the ground station.
    else if any ground station includes in either of AIT_u, AIT_d, AIT_l, AIT_r **then**
        forward packet to that direction's satellite.
    else
        choose one node with the lowest load from the neighbors except packet's incoming direction's satellite and forward packet to it.
    end if
end if
if the number of next hops $N = 1$ **then**
    if the load of the next hop $L_i >$ *the threshold* L **then**
        set packet' flag $LOAD \leftarrow 1$;
        go to 6.
    else
        forward packet to the next hop.
    end if
else
    let the load of the next hops be L_{max} and L_{min}
    if $L_{min} > L$ **then**
        set packet' flag $LOAD \leftarrow 1$;
        go to 6.
    else if $L_{max} > L > L_{min}$ **then**
        forward packet to the next hop with lower load.
    else
        forward packet to the next hop with probability P_v and P_h.
    end if
end if
End of Algorithm



Gambar 4.33 Proses routing pada ST-MIN

Dalam perutean angkasa-ke-terestrial, proses komunikasi ditetapkan sebagai berikut. Pengirim mencari koordinat hiperbolik penerima menurut pengenal identitas penerima di MIS. Pengirim menghitung secara lokal jarak hiperbolik dari beberapa stasiun darat terdekat ke penerima, dan memilih stasiun darat dengan jarak terpendek sebagai tujuan untuk mengirim paket. Setelah tiba di jaringan terestrial, setiap simpul perantara memilih simpul tetangga terdekat ke tujuan sebagai hop berikutnya dengan menghitung jarak hiperbolik antara tetangga dan tujuan. Setelah tiba di domain otonom level terendah, paket tiba di penerima melalui perutean intradomain. Proses perutean ditunjukkan sebagai rute ② pada Gambar 4.33.

Dalam perutean terestrial-ke-angkasa, proses komunikasi ditetapkan sebagai berikut. Pengirim mencari di MIS untuk mendapatkan pengenal GPS penerima sesuai dengan pengenal identitas penerima, dan satu atau lebih koordinat hiperbolik stasiun darat yang bertanggung jawab atas area penerima. Kemudian melalui perhitungan lokal, stasiun darat dengan jarak terkecil dipilih sebagai tujuan pengunggahan data. Setelah tiba di stasiun darat melalui perutean hiperbolik, paket diunggah ke jaringan satelit. Kemudian jaringan merutekan paket melalui pengenal GPS penerima, dan akhirnya mengirim paket ke penerima. Proses perutean ditunjukkan sebagai rute ③ pada Gambar 4.33.

Dalam perutean terestrial-ke-terestrial, proses komunikasi ditetapkan sebagai berikut. Pengirim mencari koordinat hiperbolik penerima di MIS melalui identitas penerima. Untuk

komunikasi lintas domain, paket akan dirutekan ke router tepi domainnya, dan kemudian akan dirutekan ke router tepi domain otonom tingkat terendah penerima melalui perutean hiperbolik. Terakhir, paket akan sampai ke penerima melalui perutean intra-domain. Untuk komunikasi intra-domain, paket akan dirutekan langsung melalui protokol perutean intra-domain. Proses ini ditunjukkan sebagai rute ④ pada Gambar 4.33.

4.10 TEKNOLOGI EKSTENSI PENGENAL

Untuk memenuhi kebutuhan berbagai skenario komunikasi, terdapat beberapa identitas yang hidup berdampingan secara setara dalam MIN. Lebih jauh, dalam pandangan mode dan skenario komunikasi baru yang akan muncul di masa mendatang, kami mengusulkan sebuah model untuk mendukung evolusi MIN. Evolusi arsitektur MIN adalah ekstensi berkelanjutan pengenal perutean dalam lapisan jaringan. Oleh karena itu, untuk menjamin kemampuan evolusi endogen MIN, kami merancang mekanisme ekstensi pengenal yang memungkinkan ekstensi pengenal MIN secara bertahap.

Pertama-tama, kami mengklasifikasikan pengenal MIN dan mendefinisikan ruang pengenal. Kemudian, kami mengusulkan format paket jaringan untuk mendukung evolusi jaringan, dan mekanisme pembuatan, pengelolaan, dan penyelesaian pengenal jaringan. Berdasarkan format paket jaringan dan sistem manajemen pengenal yang diusulkan, mekanisme yang mendukung fallback pengenal dan mekanisme perutean yang mendukung penanganan paket dirancang untuk menyediakan dukungan endogen bagi perluasan pengenal jaringan MIN.

4.10.1 Format Dasar untuk Paket Jaringan

MIT mendukung kontrol transmisi dalam semantik push dan semantik pull. Metode penyandian paket jaringan menggunakan format TLV (Type-Length-Value) tertentu untuk penyandian. Penyandian TLV membagi blok data biner menjadi tiga bidang. Bidang Type mewakili jenis blok data saat ini. Bidang Length menunjukkan Length dari bidang Value. Bidang Value digunakan untuk menyimpan data atau untuk menumpuk satu atau beberapa blok TLV. Struktur data dasar dalam mode penyandian TLV ditunjukkan pada Tabel 4.10. Panjang kolom Type dan kolom Length harus sesuai dengan ketentuan Tabel 4.11. Nilai byte pertama menunjukkan panjang kolom, dan simpan dua belas nilai untuk perluasan kolom Type dan kolom Length di masa mendatang. Jika diberikan kolom Type atau kolom Length, byte pertama kolom akan dibaca terlebih dahulu, byte ini merepresentasikan integer 8-bit yang tidak bertanda.

Jika nilai integer 8-bit yang tidak bertanda pertama berada dalam rentang [0,240], berarti kolom ini hanya memiliki satu byte. Jika nilai integer tak bertanda 8-bit pertama adalah 241, berarti bidang ini memiliki tiga byte, dan dua byte berikutnya mewakili integer tak bertanda 16-bit yang digunakan untuk menyimpan nilai bidang Tipe. Jika nilai integer tak bertanda 8-bit pertama adalah 242, berarti bidang ini memiliki lima byte, dan empat byte berikutnya mewakili integer tak bertanda 32-bit yang digunakan untuk menyimpan nilai bidang Tipe atau bidang Panjang. Menurut ketentuan dalam Tabel 4.11, ketika kita ingin merepresentasikan bidang Tipe dengan nilai 98, satu byte digunakan untuk

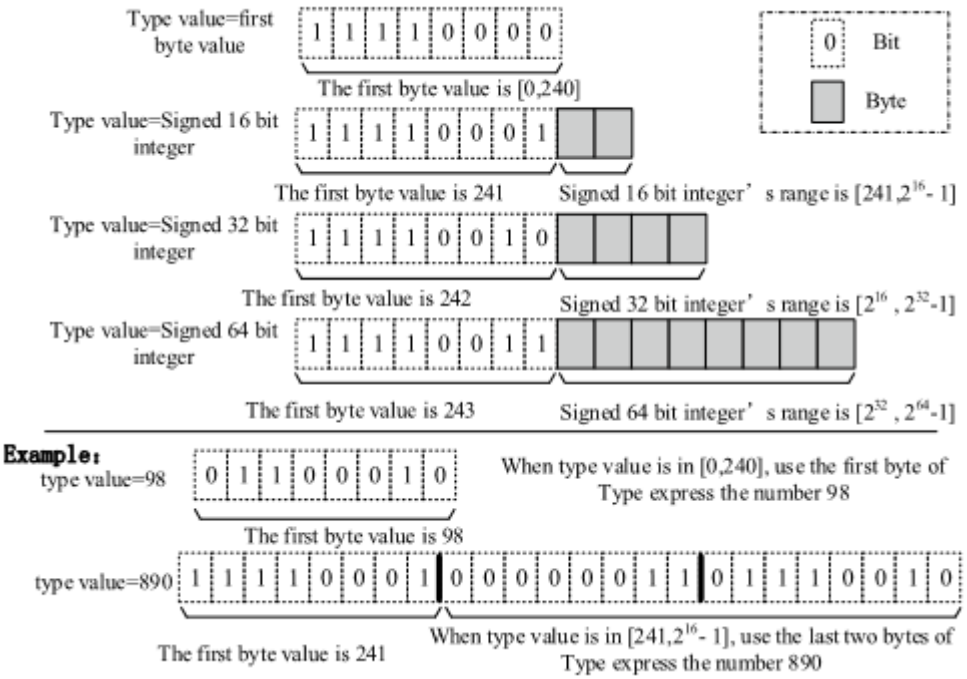
merepresentasikan nilai Tipe, dan byte ini merepresentasikan integer 8-bit tak bertanda dengan nilai 98. Ketika kita ingin merepresentasikan bidang Tipe dengan nilai 890, tiga byte diperlukan untuk merepresentasikan bidang Tipe. Byte pertama dari ketiga byte ini adalah integer 8-bit tak bertanda dengan nilai 241, dan dua byte berikutnya adalah integer 16-bit tak bertanda dengan nilai 890, seperti yang ditunjukkan pada Gambar 4.34. Begitu seterusnya, panjang bidang Tipe bisa 5, 9, atau lebih panjang. Bidang Panjang direpresentasikan dengan cara yang sama seperti bidang Tipe.

Tabel 4.10 Struktur paket dengan format TLV

Tipe	Panjang	Nilai

Tabel 4.11 Panjang bidang Jenis dan Panjang

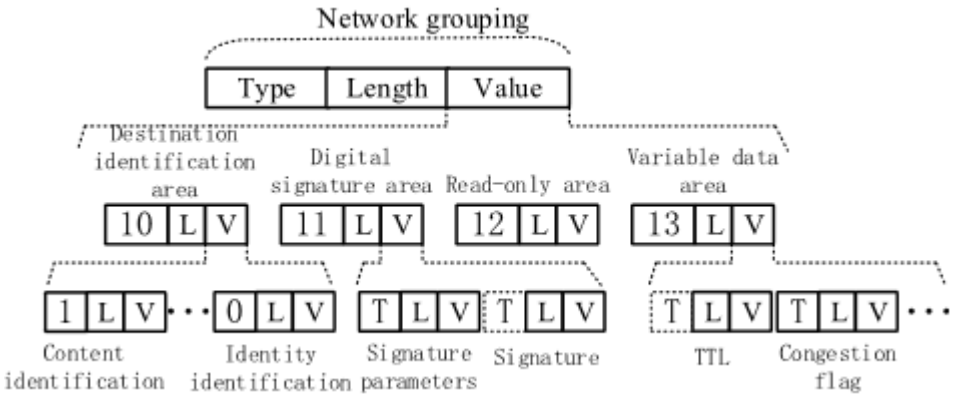
Nilai	Panjang/byte	Cakupan
0 ~240	1	0 ~240
241	3	241 ~2^{16} -1
242	5	2^{16} ~ 2^{32} – 1
243	9	2^{32} ~ 2^{64} – 1



Gambar 4.34 Struktur pengkodean jenis dan panjang

Struktur paket dalam pengodean TLV ditunjukkan pada Gambar 4.35. Setiap bidang paket jaringan dienkapsulasi dalam bidang Nilai dari struktur TLV tingkat atas, dan area yang berbeda di setiap bidang dienkapsulasi secara rekursif ke dalam bidang Nilai dari struktur TLV

bidang tersebut. Bidang dasar yang harus disertakan dalam paket dan penetapan nilai Jenis yang sesuai diberikan dalam Tabel 4.12. Pengenal paket termasuk alamat sumber dan alamat tujuan juga disusun sebagai struktur TLV, yang menggunakan bidang Jenis untuk mewakili jenis pengenal. Dengan mempertimbangkan semantik yang berbeda dari bentuk pengenal yang sama, bidang Tipe lain ditambahkan di awal bidang Nilai dari struktur TLV untuk mewakili semantik transmisi. Oleh karena itu, struktur data yang digunakan untuk menyimpan pengenal dalam paket jaringan dapat direpresentasikan sebagai "{Tipe | Panjang | Tipe-Semantik | Nilai}". Selain itu, untuk membedakan prioritas pengenal, daripada menambahkan bidang tambahan, kami menggunakan lokasi pengenal dalam paket data untuk menunjukkan prioritas. Semakin dekat lokasi identitas dengan kepala paket jaringan, semakin tinggi prioritasnya.



Gambar 4.35 Struktur paket setelah pengodean TLV

Tabel 4.12 Bidang dasar suatu paket

Nilai tipe	Nama bidang	Fungsi
10	Bidang pengenal tujuan	Menyimpan semua pengenal tujuan
11	Bidang tanda tangan	Menyimpan pengenal sumber dan tanda tangan digital paket
12	Bidang baca saja	Menyimpan data muatan
13	Bidang variabel	Menyimpan informasi yang dapat dimodifikasi oleh router perantara, seperti TTL, tanda kemacetan, petunjuk penerusan, dan sebagainya

Area pengenal tujuan dapat menyimpan beberapa pengenal tujuan untuk fallback pengenal, tetapi hanya satu dari mereka yang mewakili maksud pengirim, yang dirujuk ke pengenal asli. Semakin banyak pengenal yang disimpan di area pengenal tujuan, semakin tinggi overhead transmisi. Dengan mempertimbangkan trade-off di atas, hingga enam pengenal tujuan yang berbeda dapat disimpan dalam paket data, yang dapat disesuaikan di masa mendatang saat kemampuan komputasi ditingkatkan. Ukuran pengenal dapat ditentukan oleh pengguna. Secara umum, ukuran area pengenal tujuan tidak boleh melebihi

7,5% dari ukuran paket jaringan maksimum. Dalam versi implementasi pertama dari metode yang diusulkan, panjang maksimum paket jaringan ditentukan menjadi 8000 byte, di mana ukuran area pengenal dapat mencapai 600 byte. Panjang pengenal rata-rata dapat mendukung maksimum 100 byte, yang jauh melampaui panjang alamat IPv6 untuk memenuhi persyaratan komunikasi jaringan saat ini. Di masa mendatang, panjang pengenal dapat dikonfigurasi lebih panjang seiring dengan bertambahnya panjang paket jaringan.

Akhirnya, untuk menjelaskan mekanisme fallback identitas nanti, kami menyajikan lima pengenal umum beserta nama, nilai Jenis, semantik, dan contoh spesifik seperti yang ditunjukkan pada Tabel 4.13.

Tabel 4.13 Lima pengenal tipikal

Nilai Tipe Pengenal	Pengenal	Nilai Tipe Semantik	Deskripsi Semantik	Contoh
0	Identitas	0	Semantik komunikasi push titik-ke-titik	e98a32e6175bbd375
1	Konten	1	Semantik komunikasi push titik-ke-titik, cache router perantara	/min/pkusz/002.txt
2	Layanan	2	Semantik komunikasi tarik, paket permintaan dapat membawa data, tidak ada cache router	/min/pkusz/OA
3	Informasi geografis	0	Semantik komunikasi push titik-ke-titik	(113.97, 22.59)
4	Alamat IP	0	Semantik komunikasi push titik-ke-titik	127.0.0.1

4.10.2 Pengikatan Pengenal dalam MIS

Fungsi MIS adalah menyediakan layanan pendaftaran, kueri, pengelolaan, dan penyelesaian pengenal terpadu untuk perangkat dalam jaringan. Setiap pengguna dalam jaringan terikat pada pengenal identitas unik dalam jaringan, dan pengenal identitas pengguna juga akan terikat pada pengenal lain, termasuk konten, layanan, informasi geografis, alamat IP. Pada saat yang sama, dengan mempertimbangkan mobilitas, pengguna juga perlu terikat pada pengenal router akses.

Pengguna dapat meminta string yang dapat dibaca manusia sebagai nama set pengenalnya, mirip dengan alamat nama domain. Misalnya, pengguna dapat meminta nama "Alice" sehingga orang lain dapat menemukan ID komunikasinya. Dalam kasus ini, akuisisi pengenal komunikasi setara dengan resolusi DNS, dan proses resolusi pengenal spesifik dijelaskan di bagian tentang MIS.

4.10.3 Mekanisme Perluasan Pengenal

Perpanjangan pengenal dicapai dengan membawa identitas tujuan alternatif dalam paket jaringan. Pengenal identitas (atau pengenal dasar lainnya) tujuan harus dibawa dalam setiap paket untuk memastikan bahwa semua router dalam jaringan mendukung penerusan

paket. Dengan dukungan mekanisme pemrosesan router, proses dasar yang dilakukan pengguna saat mengirim paket dengan pengenal jaringan baru berisi langkah-langkah yang ditunjukkan sebagai berikut.

(1) Pengguna menanyakan semua pengenal entitas komunikasi dalam MIS dengan pengenal tujuan baru X atau nama pengguna.
(2) Pengguna merangkum pengenal baru X, pengenal identitas X yang sesuai, dan pengenal terkait yang memiliki semantik transmisi yang sama dengan X ke dalam bidang pengenal tujuan paket. Semua pengenal diurutkan menurut prioritas pengalamatan yang diinginkan oleh pengguna;
(3) Ketika router perantara menerima paket dan membaca jenis pengenal dari kolom Jenis di area pengenal tujuan. Kemudian menurut prioritas berbagai pengenal di area pengenal tujuan, pengenal dengan prioritas tertinggi dan didukung oleh router saat ini dipilih untuk penerusan berikutnya. Ketika router memilih pengenal lama (bukan pengenal X) untuk penerusan dan penerusan berhasil, proses ini disebut fallback pengenal;
(4) Jika router memilih pengenal dengan prioritas tinggi untuk penerusan, tetapi penerusan tidak berhasil, router akan terus memilih pengenal dengan prioritas lebih rendah untuk penerusan. Bila semua pengenal di area pengenal tujuan telah dicoba tetapi tidak ada satu pun yang dapat digunakan untuk meneruskan paket dengan sukses, paket akan dibuang.
(5) Bila paket tiba di tujuan, jika ada penantian utama untuk paket dengan pengenal baru X, X akan digunakan oleh host tujuan untuk meneruskan paket. Akhirnya, pengenal baru X digunakan untuk penerusan lokal ke proses atau penerima yang sesuai. Proses ini dapat disebut sebagai pemulihan pengenal baru X.

Sebelum paket jaringan dikirim, inilah saat yang tepat untuk memilih pengenal alternatif. Jika semua pengenal dengan semantik yang sama dimuat ke pengenal tujuan, mungkin ada masalah bahwa jumlah pengenal melebihi batas atas, dan beberapa pengenal tidak akan digunakan dalam seluruh proses komunikasi jaringan yang menyebabkan overhead komunikasi yang tidak perlu. Mekanisme deteksi ruang pengenal diperkenalkan untuk mengatasi masalah ini. Mirip dengan protokol ICMP dalam jaringan IP, menurut mekanisme deteksi, pengguna mengirim paket probe, yang hanya membawa pengenal identitas sebagai pengenal alternatif.

Router perantara mencatat jenis pengenal yang didukungnya dan memiliki semantik yang sama dengan pengenal baru X di area data variabel paket probe. Host tujuan mencatat alamat sumber, yang dapat diperoleh dalam informasi tanda tangan paket, dan urutan ruang pengenal yang sesuai, lalu mengembalikan paket balasan. Paket balasan mengembalikan informasi ruang pengenal yang terekam dalam paket pemeriksaan kepada pengirim. Menurut jenis pengenal yang terekam dalam area data variabel dari paket balasan, pengguna memilih pengenal alternatif yang sesuai dan memuatnya di area pengenal tujuan.

Perluasan pengenal yang dicapai oleh mekanisme fallback pengenal didasarkan pada satu atau beberapa pengenal fundamental yang ada di MIN. Selama pengenal mengikuti semantik push titik-ke-titik yang sederhana, pengenal dapat digunakan sebagai pengenal fundamental, dan dapat digunakan sebagai jangkar untuk proses fallback pengenal lainnya. Oleh karena itu, metode yang diusulkan memungkinkan adanya berbagai pengenal dasar di MIN sebagai jangkar fallback. Misalnya, kita dapat menggunakan pengenal identitas, pengenal informasi geografis, dan pengenal hiperbolik sebagai pengenal fundamental. Dengan perkembangan jaringan, ketika semua router tidak mendukung beberapa pengenal dasar yang usang, pengenal dasar yang usang ini juga dapat diganti secara bertahap untuk mendukung evolusi jaringan.

4.10.4 Prosedur Pemrosesan Paket

Saat router menerima paket, pertama-tama router akan menurunkan nilai TTL dalam paket sebanyak satu. Kemudian, jika nilai TTL kurang dari 0, paket akan dibuang. Jika nilai TTL lebih besar dari 0, operasi berikutnya akan dilakukan. Selanjutnya, menentukan apakah paket jaringan tersebut merupakan paket probe ruang pengenal. Jika demikian, area tertentu dalam paket akan ditetapkan untuk mencatat nomor jenis pengenal yang didukung oleh router saat ini dan memiliki semantik identitas yang sama dengan pengenal pertama paket. Saat router memproses paket dengan beberapa pengenal tujuan, maksud pengirim, prioritas pengenal, dan kemampuannya sendiri untuk mendukung pengenal tersebut harus dipertimbangkan. Prosedur pemrosesan paket ditunjukkan sebagai berikut:

- **Langkah 1**: Router membaca setiap pengenal di area pengenal tujuan dari depan ke belakang;
- **Langkah 2**: Untuk setiap pengenal, router menilai apakah router saat ini mendukung pengalamatan, penerusan, dan pemrosesan pengenal;
- **Langkah 3**: Jika router mendukung pengenal ini, router akan mencoba menggunakan pengenal ini untuk mengirimkan paket. Jika proses penerusan paket berhasil, prosedur pemrosesan paket akan berakhir; jika tidak, kembali ke Langkah 1;
- **Langkah 4**: Jika router tidak mendukung identitas, kembali ke Langkah 1;
- **Langkah 5**: Setelah semua pengenal telah dilalui, jika paket masih tidak dapat diteruskan, paket tersebut akan dibuang.

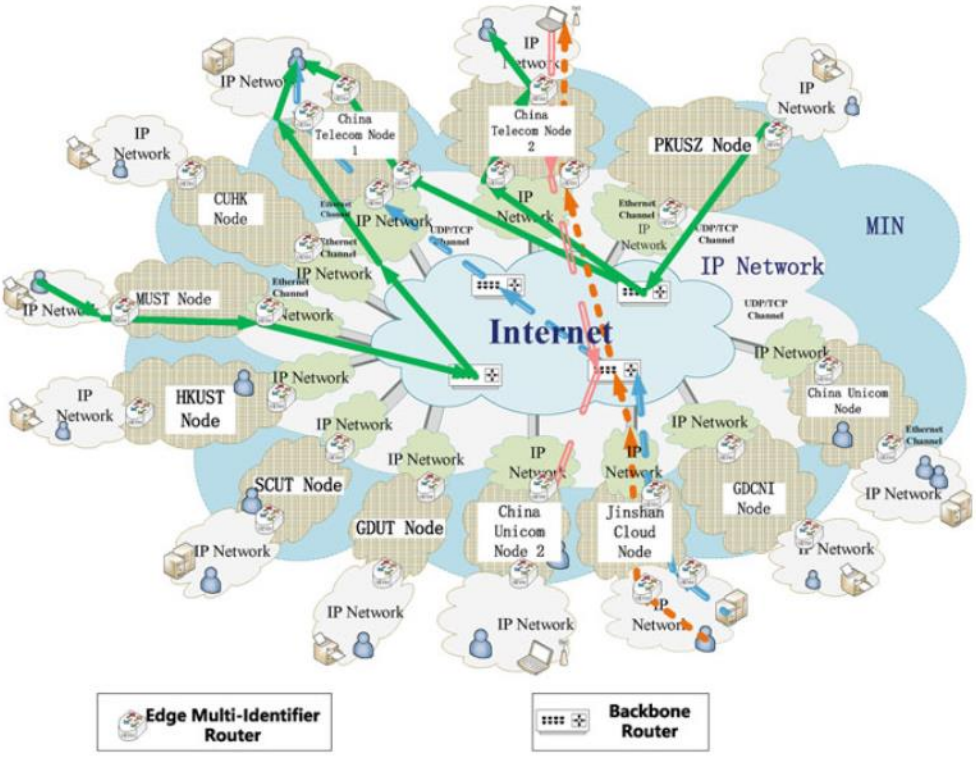
BAB 5
PROTOTIPE JARINGAN KEDAULATAN DAN APLIKASI BERBASIS MIN

Multi-Identifier Network (MIN) kompatibel dengan jaringan IP, dan mendukung de-IP secara alami dan bertahap, yang akan dipromosikan oleh pengguna dan pasar untuk peningkatan kinerjanya daripada secara kompulsif. Merupakan keadaan yang dapat diprediksi bahwa jaringan IP mungkin masih menjadi arus utama di Amerika Serikat di masa mendatang. Namun, negara-negara lain akan beralih dari IP ke MIN untuk menjaga kedaulatan mereka atas dunia maya, dan konektivitas antara mereka dan jaringan IP dijamin melalui MIN. Dengan kata lain, jaringan IP akan menjadi jaringan internal Amerika Serikat, sementara negara-negara lain akan membentuk sistem jaringan tata kelola multilateral berbasis MIN.

MIN mengintegrasikan teori dan teknologi seperti berbagai arsitektur jaringan, protokol terkait, mekanisme pertahanan jaringan, kecerdasan buatan, algoritma konsensus blockchain, dan keamanan kontrak cerdas.

MIN didasarkan pada arsitektur jaringan multi-identifier yang mengatur bersama, yang mengintegrasikan berbagai teknologi kontrol keamanan. Skenario aplikasi utama MIN adalah jaringan privat milik pemerintah, militer, industri keuangan, dan perusahaan besar lainnya dengan persyaratan keamanan tinggi. Sebagai platform layanan terpadu, MIN juga dapat diterapkan pada Internet Industri, Internet untuk Segala, dan Internet untuk Kendaraan. MIN dapat menyediakan tata kelola bersama untuk entitas internasional, seperti Organisasi Kerjasama Shanghai dan negara-negara “Satu Sabuk dan Satu Jalan”. MIN juga mendukung pembuatan registrasi identifikasi tingkat atas, manajemen siklus penuh, dan layanan analisis. Dimulai dari melakukan eksperimen jaringan dari beberapa negara, MIN bertujuan untuk membentuk jaringan publik multinasional guna menjamin kedaulatan dunia maya di setiap negara. Penerapan MIN secara luas akan membentuk Perserikatan Bangsa-Bangsa Dunia Maya dengan kedaulatan independen dan membentuk sistem jaringan publik global.

Kami telah mengembangkan tempat uji coba jaringan kedaulatan berdasarkan arsitektur MIN di lingkungan jaringan operator. Eksperimen teori dan aplikasi terkait jaringan kedaulatan telah dilakukan di tempat uji coba ini. Tempat uji coba jaringan kedaulatan meliputi Beijing, Guangzhou, Shenzhen, Hong Kong, dan Makau. Topologi dari pengujian ini, yang ditunjukkan dalam Gambar 5.1, meliputi China Telecom, China Unicom, Sekolah Pascasarjana Universitas Peking Shenzhen, Kingsoft Cloud, Universitas Teknologi Cina Selatan, Universitas Sains dan Teknologi Hong Kong, Universitas Cina Hong Kong, Universitas Sains dan Teknologi Makau, serta Institut Komunikasi dan Jaringan Guangdong, dsb.



Gambar 5.1 Topologi prototipe jaringan uji

5.1 EKSPERIMEN SISTEM PROTOTIPE

Fungsi jaringan kedaulatan diuji di jaringan Operator. Lingkungan eksperimen ditunjukkan sebagai berikut:

1. **Node IDC;** Sistem operasi server di Internet Data Center (IDC) adalah Ubuntu 16.04.
2. **Mainframe yang Digunakan dalam Pengujian**; Eksperimen menggunakan dua jenis mainframe, satu dengan Ubuntu 16.04 dan yang lainnya dengan Windows 10 Pro 64-bit. Yang pertama digunakan untuk mendemonstrasikan pemungutan suara blockchain, proses penandatanganan grup dan penandatanganan ring, sedangkan yang terakhir digunakan untuk mendemonstrasikan proses lainnya.

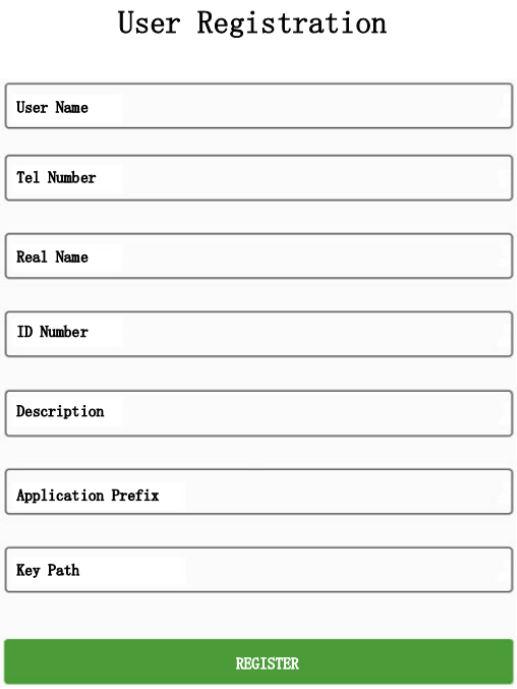
5.1.1 Pendaftaran Pengguna dan Penerbitan Sumber Daya

Deskripsi Lingkungan

Eksperimen fungsional ini dilakukan di dalam jaringan kedaulatan. Pengguna di node Kingsoft Cloud, melakukan pendaftaran dan penerbitan sumber daya.

1. Pendaftaran Pengguna

Pengguna mendaftar di klien dengan informasi identitas asli mereka, seperti nomor ID, nomor telepon, dan sebagainya. Antarmuka pendaftaran ditunjukkan pada Gambar 5.2.



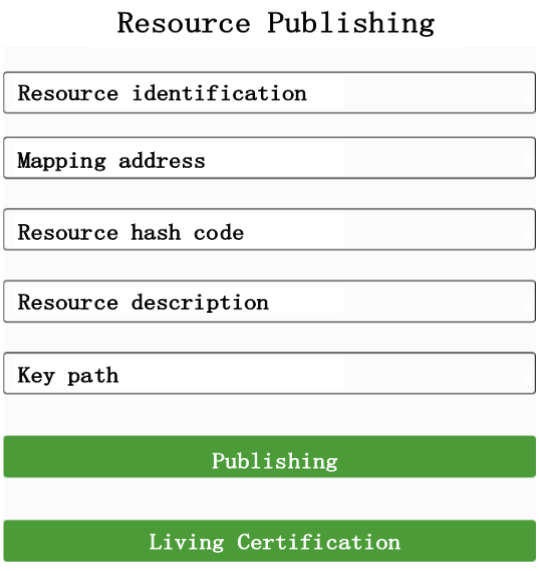
Gambar 5.2 Antarmuka registrasi

2. Penerbitan Sumber Daya

(1) Pengguna yang telah berhasil mendaftar di sistem dapat masuk ke sistem dengan sidik jari dan iris.

(2) Setelah berhasil masuk ke sistem, pengguna dapat menerbitkan sumber daya mereka yang akan ditampilkan di antarmuka klien.

Antarmuka penerbitan sumber daya ditunjukkan pada Gambar 5.3. Antarmuka penerbitan sumber daya yang berhasil ditunjukkan pada Gambar 5.4. Sumber daya yang diterbitkan dapat diakses dengan sertifikat pengguna, seperti yang ditunjukkan pada Gambar 5.5.



Gambar 5.3 Antarmuka penerbitan sumber daya

Gambar 5.4 Antarmuka setelah penerbitan sumber daya berhasil

Gambar 5.5 Menggunakan sertifikat untuk mengakses sumber daya yang dipublikasikan

5.1.2 Mengakses Sumber Daya Jaringan Internal IP

Deskripsi Lingkungan

Untuk mendemonstrasikan fungsi akses jaringan kedaulatan, pengujian transmisi video VoD telah dilakukan antara node Kingsoft Cloud dan node Sekolah Pascasarjana Universitas Peking Shenzhen.

Detail Demonstrasi

Pengguna yang Berada di Kingsoft Cloud, mengunjungi sumber daya video Perpustakaan Digital Nasional dan Basis Data Budaya Nasional, yang berlokasi di Sekolah Pascasarjana Universitas Peking Shenzhen. Hasilnya menunjukkan bahwa sumber daya video ini dapat diputar secara normal di layar klien jarak jauh.

(1) Sumber daya video: HD, 1080P

(2) Jumlah cara: 2 (dibatasi oleh lebar pita)

Hasil Demonstrasi

Pada kenyataannya, hasil penarikan video ditunjukkan pada Gambar 5.6.

Gambar 5.6 Efek penarikan video yang sebenarnya

5.1.3 Mengakses Sumber Daya IP Eksternal

Deskripsi Lingkungan

Pengguna yang Berada di Kingsoft Cloud meminta sumber daya IP, yang berada di simpul Universitas Teknologi China Selatan. Demonstrasi menunjukkan bahwa sistem mendapatkan berkas dari Universitas Teknologi China Selatan.

Detail Demonstrasi

(1) Saat pengguna mencoba mendapatkan berkas di jaringan IP untuk pertama kalinya, sistem akan meminta pengguna untuk mengajukan tanda tangan grup. Hanya pengguna yang telah melewati tanda tangan grup yang dapat mengakses sumber daya IP eksternal.

(2) Informasi akses pengguna dicatat pada simpul blockchain.

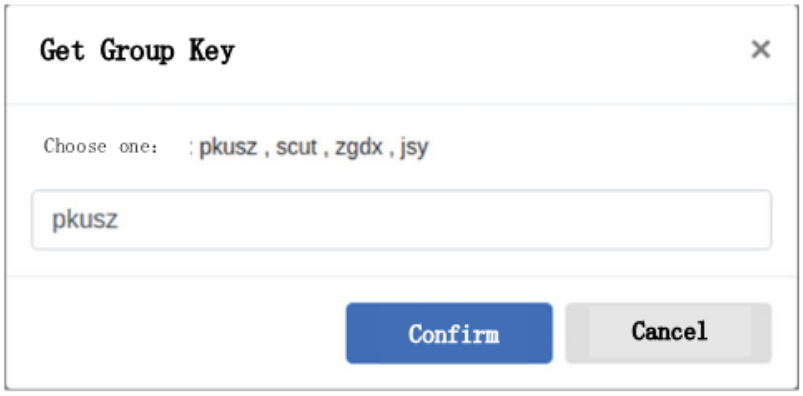
(3) Setelah semua ini, pengguna berhasil mendapatkan berkas dari simpul IP eksternal.

Hasil Demonstrasi

※ Tanda tangan grup ditunjukkan pada Gambar 5.7 dan gambar 5.8.

※ Informasi yang relevan dikunci dalam blockchain, seperti yang ditunjukkan pada gambar 5.9.

※ Pengguna berhasil mendapatkan berkas di simpul IP eksternal, seperti yang ditunjukkan pada gambar 5.10.



Gambar 5.7 Sistem meminta pengguna untuk mengajukan tanda tangan grup

Gambar 5.8 Sistem memberi tahu bahwa pengguna telah berhasil bergabung dengan grup

Gambar 5.9 Informasi tanda tangan grup terkunci dalam blockchain

Gambar 5.10 Pengguna berhasil mendapatkan berkas di node IP eksternal

5.1.4 Sertifikasi Antar Jaringan Kedaulatan

Deskripsi Lingkungan

File dengan sufiks .txt ditransfer antara pengguna China Telecom dan pengguna Sekolah Pascasarjana Universitas Peking Shenzhen.

Detail Demonstrasi

(1) Seorang pengguna Sekolah Pascasarjana Universitas Peking Shenzhen mengajukan permohonan sertifikat node di China Telecom.

(2) Jika pengajuan sertifikat berhasil, pengguna mengunduh berkas jaringan kedaulatan dari node di China Telecom.

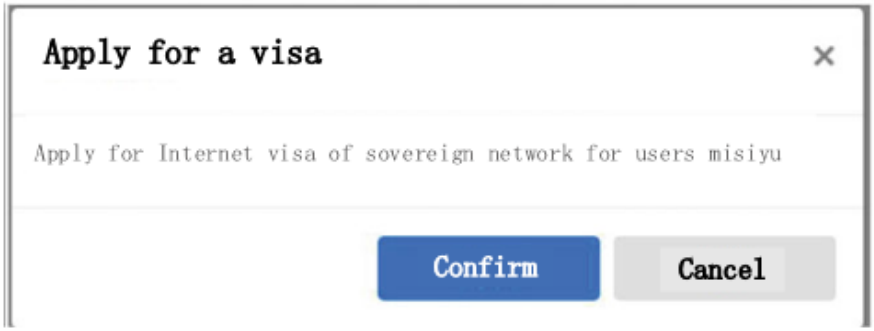
(3) Jika pengguna tidak berhasil mengajukan permohonan sertifikat, pengguna tidak akan memiliki hak untuk memperoleh berkas di jaringan kedaulatan, yang berlokasi di simpul China Telecom.

Hasil Demonstrasi

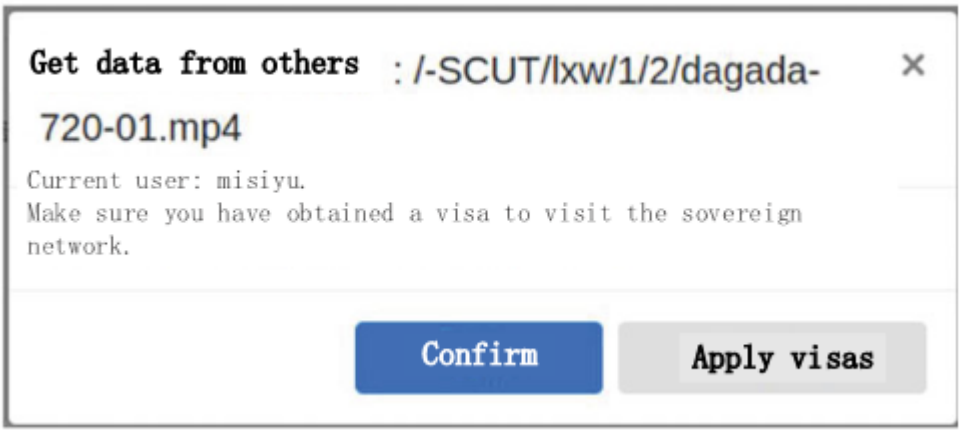
Antarmuka pengajuan sertifikat ditunjukkan pada Gambar 5.11.

Pengguna meminta konten lain dengan sertifikat mereka di jaringan kedaulatan, seperti yang ditunjukkan pada Gambar 5.12.

Informasi sertifikat dicatat dalam blockchain, seperti yang ditunjukkan pada Gambar 5.13.



Gambar 5.11 Antarmuka pengajuan sertifikat



Gambar 5.12 Seorang pengguna meminta konten lain dengan sertifikat di jaringan kedaulatan

Gambar 5.13 Informasi sertifikat

5.1.5 Fungsi Penyaringan Data EMIR

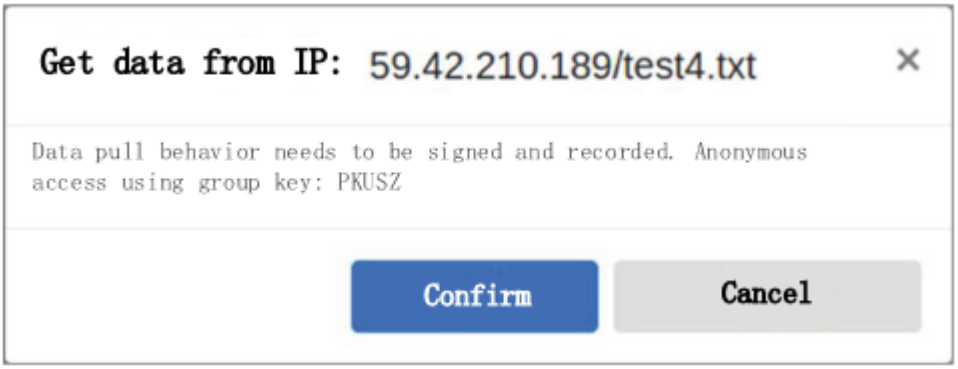
Deskripsi Lingkungan

Saat pengguna jaringan kedaulatan mengakses file .txt di jaringan IP, kata-kata sensitif dalam file tersebut akan disaring. Pengguna Kingsoft Cloud mengunjungi file tersebut, yang merupakan sumber daya IP dan terletak di simpul Universitas Teknologi Tiongkok Selatan.

Detail Demonstrasi

(1) Simpul Kingsoft Cloud mengaudit paket yang diterima.
(2) Jika paket tersebut berisi informasi berbahaya, karakter berbahaya tersebut diganti dengan “**”.
(3) Simpul Kingsoft Cloud mengirimkan file yang disaring ke klien.
(4) Saat klien mendeteksi karakter “**” yang terdapat dalam file tersebut, antarmuka menampilkan bahwa “file ini berisi kata-kata sensitif”. Hasil Demonstrasi

Hasil penggunaan tanda tangan untuk mendapatkan konten teks IP eksternal ditunjukkan pada Gambar 5.14.



Gambar 5.14 Mendapatkan konten teks IP eksternal

Sistem akan memberikan perintah saat mendeteksi informasi sensitif dalam teks, seperti yang ditunjukkan pada Gambar 5.15.

Gambar 5.15 Sistem menyaring informasi sensitif dalam teks

Versi akhir dari berkas yang didapatkan pengguna telah disaring untuk mencari informasi yang berbahaya, seperti yang ditunjukkan pada Gambar 5.16.

Gambar 5.16 Konten teks setelah menyaring informasi berbahaya

5.1.6 Transmisi Email dalam Jaringan Kedaulatan

Dua subjaringan kedaulatan Kingsoft Cloud dan Sekolah Pascasarjana Universitas Peking Shenzhen membentuk jaringan kedaulatan yang besar. Seorang pengguna Kingsoft Cloud mengirimkan email ke pengguna lain Sekolah Pascasarjana Universitas Peking Shenzhen melalui jaringan kedaulatan. Pengguna Sekolah Pascasarjana Universitas Peking Shenzhen akan menerima email ini dengan sukses.

Detail Demonstrasi

(1) Pertama, seorang pengguna jaringan kedaulatan berada di simpul Kingsoft Cloud. Pengguna lain jaringan kedaulatan berada di simpul Sekolah Pascasarjana Universitas Peking Shenzhen.

(2) Kemudian pengguna Kingsoft Cloud mengirim email ke pengguna lain dari Sekolah Pascasarjana Universitas Peking Shenzhen. Antarmuka sistem menunjukkan bahwa email telah berhasil dikirim.

(3) Terakhir, antarmuka sistem Sekolah Pascasarjana Universitas Peking Shenzhen menunjukkan bahwa kotak surat pengguna menerima email baru.

Sekolah melalui jaringan kedaulatan. Pengguna Sekolah Pascasarjana Universitas Peking Shenzhen akan berhasil menerima email ini.

Rincian Demonstrasi

(1) Pertama, pengguna jaringan kedaulatan berada di simpul Kingsoft Cloud. Pengguna jaringan kedaulatan lainnya berada di simpul Sekolah Pascasarjana Universitas Peking Shenzhen.

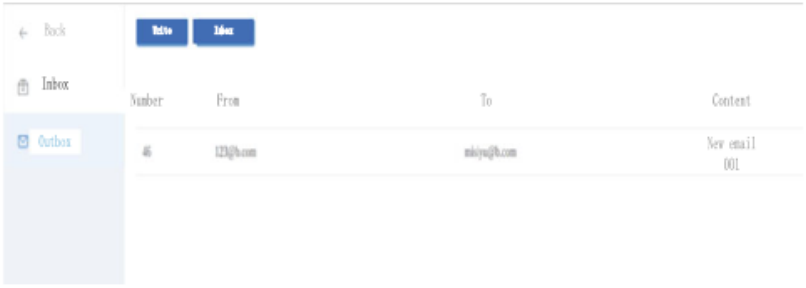
(2) Kemudian pengguna Kingsoft Cloud mengirim email ke pengguna lain Sekolah Pascasarjana Universitas Peking Shenzhen. Antarmuka sistem menunjukkan bahwa email telah berhasil dikirim.

(3) Terakhir, antarmuka sistem Sekolah Pascasarjana Universitas Peking Shenzhen menunjukkan bahwa kotak surat pengguna menerima email baru.

Hasil Demonstrasi

Pengiriman email ditunjukkan pada Gambar 5.17, 5.18, dan 5.19.

Gambar 5.17 Antarmuka login kotak surat

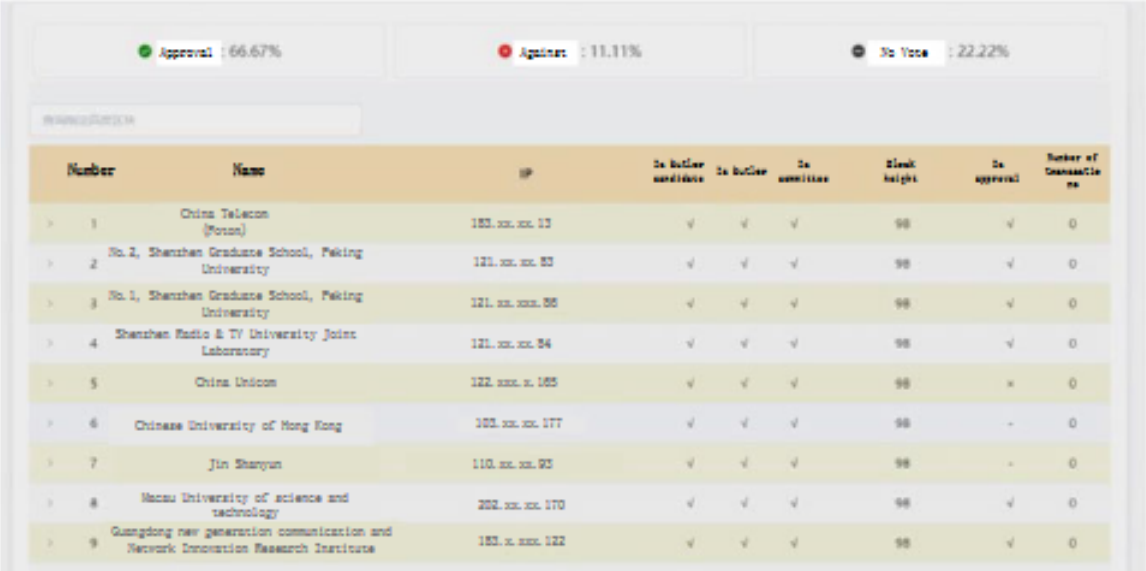


Gambar 5.18 Antarmuka kotak masuk

Gambar 5.19 Antarmuka penulisan email baru

5.1.7 Pemungutan Suara Melalui Blockchain

Proses pemungutan suara blockchain ditampilkan secara real-time oleh administrator yang ditempatkan pada host dengan sistem operasi Windows ver.10, dan informasi antarmuka ditunjukkan pada Gambar 5.20.



Gambar 5.20 Proses pemungutan suara blockchain

5.2 JARINGAN PRIVAT ANDAL KEAMANAN MIN

Pada tanggal 22 Maret 2019, MIN telah mewujudkan pemerintahan bersama multilateral dan otonomi kedaulatan di dunia maya untuk pertama kalinya. Pada bulan November 2019, MIN dan sistem prototipe-nya dianugerahi sebagai pencapaian teknologi terdepan dari Konferensi Internet Dunia keenam yang diadakan di Wuzhen, Tiongkok. Akan tetapi, ukuran jaringan IP yang ada sangat besar, sehingga sulit untuk mengganti arsitektur jaringan IP dengan arsitektur MIN yang revolusioner dalam satu hari.

Pada tahun 2020, dengan mempertimbangkan skenario aplikasi utama MIN yaitu jaringan privat virtual pemerintah, militer, industri keuangan, dan perusahaan besar lainnya dengan persyaratan keamanan tinggi, kami mengembangkan Jaringan Privat Andal Keamanan MIN (MIN-SRPN) berdasarkan lingkungan IP yang ada, yang memungkinkan jaringan IP dan MIN untuk hidup berdampingan. MIN-SRPN dapat memenuhi kebutuhan praktis kantor bergerak, manajemen identitas, manajemen otoritas, penyimpanan log, deteksi perilaku, autentikasi identitas, dan keamanan jaringan.

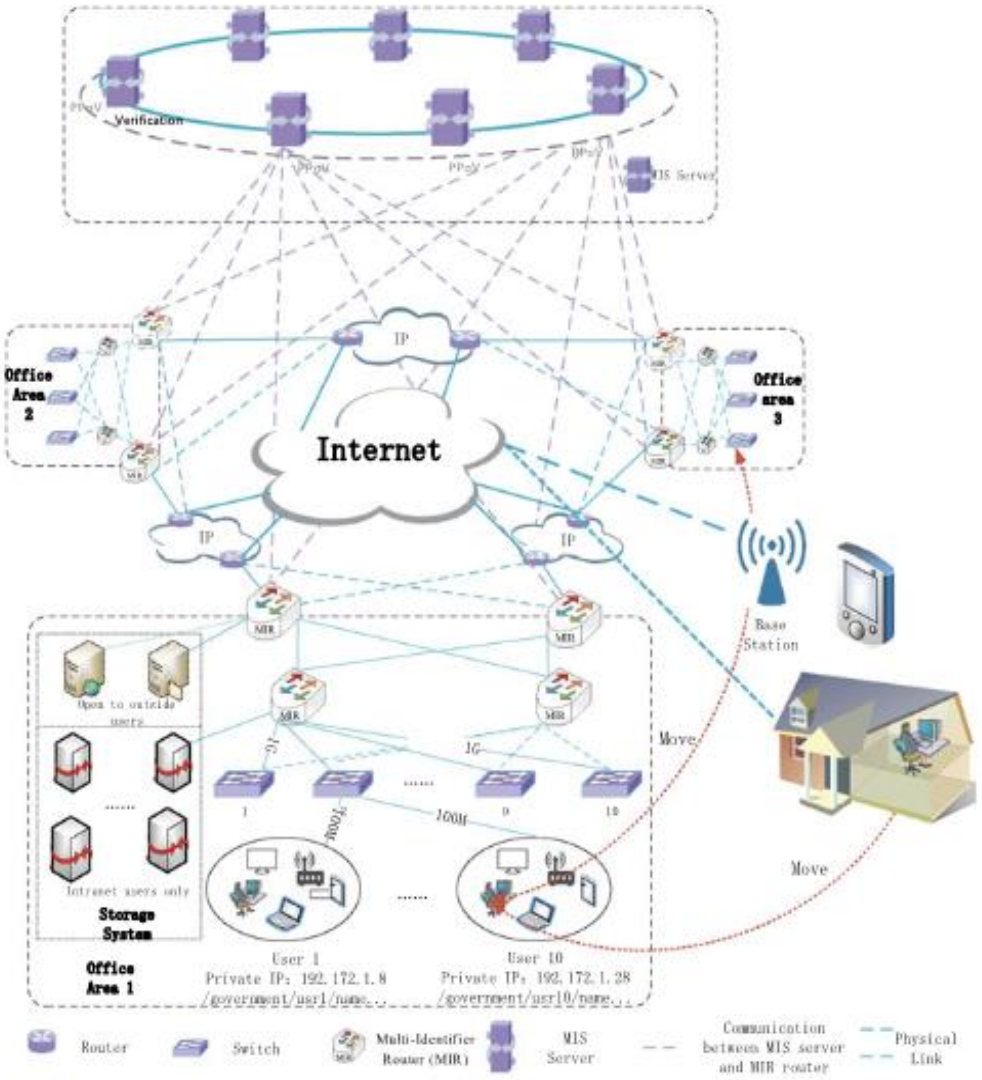
5.2.1 MIN-SRPN

Berbagai inovasi telah diadopsi dalam MIN-SRPN untuk mencapai akses jaringan yang efisien dan regulasi yang teratur. Pertama, teknologi blockchain menjamin kredibilitas catatan log. Kedua, teknologi Cyber Mimic Defense memastikan keamanan endogen dari sistem inti. Ketiga, teknologi AI digunakan untuk mendeteksi, melaporkan perilaku, dan menyadari situasi keamanan untuk memastikan keamanan jaringan. Keempat, identitas asli dan karakteristik

biologis digunakan untuk memastikan keandalan pengenal pengguna dan efektivitas manajemen pengguna. Kelima, jenis baru informasi dan data identitas pengikatan paket diusulkan untuk mengawasi jaringan secara efektif.

Terakhir, berbagai teknologi tanda tangan kriptografi digunakan untuk mencapai keseimbangan antara perlindungan privasi dan pengawasan. MIN-SRPN v1.1 telah dikembangkan secara lengkap, yang mencakup sistem latar belakang dan sistem front-end. Sistem latar belakang mencakup Sistem Multi-identifier (MIS) dan Router Multi-identifier (MIR). Sistem front-end mencakup klien administrator di Windows dan empat jenis klien pengguna di Windows, Android, macOS, dan iOS. Arsitektur keseluruhan MIN-SRPN ditunjukkan pada Gambar 5.21. Jaringan privat ini terdiri dari bidang manajemen dan bidang data, termasuk sistem penyimpanan, PC kantor, perangkat lunak kantor, MIR, server MIS, dll. Jaringan IP digunakan untuk interkoneksi dan akses bebas satu sama lain di area kantor. Beberapa pintu masuk dan keluar IP dicadangkan untuk membantu pengguna jaringan internal mengakses sumber daya eksternal secara bebas.

Pada saat yang sama, hanya satu entri MIN yang dicadangkan untuk membantu pengguna jaringan eksternal mengakses sumber daya internal. Bidang manajemen terdiri dari server MIS yang ditunjukkan dalam kotak putus-putus di bagian atas Gambar 5.21. Server MIS ini berkomunikasi dengan router pada bidang data. MIS digunakan pada node blockchain untuk merekam identitas dan log perilaku pengguna guna memastikan bahwa konten seluruh jaringan terpadu, tahan terhadap gangguan, dan dapat dilacak. Modul manajemen identitas bertanggung jawab atas fungsi-fungsi termasuk registrasi pengguna, login pengguna, dan penerbitan sertifikat. Modul deteksi perilaku bertanggung jawab untuk menyimpan dan menganalisis catatan akses pengguna guna menjamin keamanan informasi. Bidang data terutama terdiri dari terminal pengguna, sakelar, dan MIR. Sebagai peralatan inti bidang data, MIR terutama digunakan untuk pengidentifikasi antar-terjemahan, perutean, penyaringan konten, perlindungan data, dan fungsi-fungsi lainnya. MIR dalam MIN-SRPN terutama digunakan untuk entri lalu lintas, yaitu, pengguna jaringan eksternal menggunakan MIN-SRPN untuk mengunjungi sumber daya internal, dan juga digunakan untuk meneruskan sumber daya MIN.



Gambar 5.21 Arsitektur MIN-SRPN

Sistem penyimpanan utamanya untuk menyimpan sumber daya, yang dibagi menjadi sumber daya IP internal dan sumber daya MIN internal. Sumber daya IP Pribadi internal (P-IP) merujuk pada sumber daya yang terletak di jaringan IP internal. Pengguna di jaringan internal dapat dengan bebas mengakses sumber daya P-IP dengan cara tradisional, sementara pengguna di jaringan eksternal harus menggunakan MIN-SRPN untuk mengakses sumber daya P-IP. Ketika lalu lintas akses melewati MIN, MIS bertanggung jawab atas manajemen identitas dan perekaman perilaku, dan MIR bertanggung jawab atas penerusan dan autentikasi identitas.

MIN-SRPN adalah jaringan tanpa IP. Semua metode serangan dan senjata terhadap protokol TCP/IP tidak memengaruhi MIN-SRPN. Setelah periode pengujian penetrasi yang panjang oleh beberapa tim profesional, hasilnya menunjukkan bahwa MIN-SRPN dapat secara efektif kebal terhadap semua serangan dalam skenario jaringan IP-MIN dan MIN-MIN. MIN-SRPN dapat secara efektif melindungi industri dengan persyaratan keamanan tinggi. Pengguna potensial yang menarik dapat mengunjungi web1 untuk mendapatkan lebih banyak pesan.

Untuk perusahaan besar dan menengah, kami menyediakan produk dan solusi keamanan yang disesuaikan berdasarkan MIN-SRPN, sesuai dengan persyaratan pelanggan sasaran. Untuk bisnis kecil, kami berencana untuk menyediakan layanan cloud berdasarkan MIN-SRPN. Sebagai ekspor teknis, teknologi yang mendasarinya dapat dienkapsulasi dan disediakan untuk perusahaan teknologi informasi di hilir.

Kelompok Kerja Internet Industri Kementerian Perindustrian dan Teknologi Informasi Republik Rakyat Tiongkok telah mengadopsi MIN sebagai arsitektur referensi untuk sistem layanan akar pengawasan independen Tiongkok. Shenzhen Media Group Tiongkok, sebagai pelanggan dan pengguna pertama, telah menerapkan MIN-SRPN sebagai sistem manajemen sumber daya medianya untuk China United Television (CUTV). Bekerja sama dengan Some Smart City Technology Development Group Co., Ltd., Sekolah Pascasarjana Universitas Peking Shenzhen berencana untuk membangun jaringan privat keamanan hierarkis untuk lebih dari 1.000 perusahaan utama milik negara. Di masa mendatang, MIN-SRPN akan diadopsi untuk membangun Internet kendaraan, jaringan privat 5G, dan jaringan pemerintah-swasta. MIN-SRPN merupakan aplikasi MIN dalam skenario kecil. Efek skala yang ditimbulkan oleh penerapan MIN-SRPN secara bertahap akan meningkatkan proporsi lalu lintas MIN dan secara bertahap menggantikan sistem IP. Lebih jauh lagi, MIN akan menjadi sistem Internet publik global.

5.2.2 Sistem Utilitas Air Berbasis MIN-SRPN

Untuk meningkatkan tingkat keamanan jaringannya, Salah Satu Grup Penyedia Air Teratas di Tiongkok, yang disebut sebagai OT-WSG, mengadopsi MIN-SRPN ini untuk menggantikan skema IP-VPN saat ini. Setelah periode pengujian penetrasi yang panjang oleh beberapa tim profesional, hasilnya menunjukkan bahwa MIN-SRPN secara efektif dapat kebal terhadap semua serangan dalam skenario jaringan IP-MIN dan MIN-MIN.

Menurut tingkat manajemen, sistem utilitas air berbasis MIN-SRPN dari Grup Air ini terutama dibagi menjadi empat tingkat, termasuk jaringan internal grup, jaringan internal area, jaringan internal perusahaan utilitas air, dan jaringan internal instalasi air. Semua simpul terminal dalam lingkup bisnis telah terhubung dengan kabel ke MIN-SRPN.

OT-WSG berencana untuk mengadaptasi MIN-SRPN guna mencapai tujuan yang tercantum sebagai berikut. Serangan penetrasi jaringan berdasarkan cacat sistem TCP/IP dapat dicegah untuk memastikan bahwa permeabilitas anti-serangan ditingkatkan secara signifikan dibandingkan dengan jaringan IP-VPN yang ada, termasuk namun tidak terbatas pada TCP Trojan, UPD Trojan, implantasi ICMP Trojan, dan metode serangan klasik lainnya. Jumlah jalur khusus yang disewa dikurangi untuk mengurangi biaya sewa kabel komunikasi grup.

1. Analisis Persyaratan

Keamanan air minum berkaitan dengan kesehatan jutaan rumah tangga, dan pasokan air yang aman harus bergantung pada sistem informasi yang lengkap untuk membantu manajemen. Sistem informasinya rentan terhadap serangan siber. Selain itu, para penjahat bermaksud menghancurkan sistem aplikasi dan peralatan kontrol industri untuk mencapai

tujuan mereka. Untuk memastikan keamanan sistem informasi, jaringan komputer sebagai media pertukaran informasi merupakan target perlindungan utama MIN-SRPN.

(1) Konsistensi Arsitektur Jaringan

Melalui peningkatan berkelanjutan arsitektur jaringan perusahaan air yang ada, fasilitas dasar sistem (seperti serat optik dan jalur fisik) telah mencakup semua simpul bisnis, dan departemen air serta pabrik air telah menyelesaikan penyebaran fasilitas di semua tingkat jaringan utilitas air sesuai dengan arsitektur manajemen yang ada. Sistem bisnis dan sistem pencadangan data perusahaan air telah relatif lengkap. Mengingat kebutuhan perusahaan air untuk menyediakan layanan penting bagi masyarakat dalam kehidupan sehari-hari, sistem bisnis yang terlibat tidak dapat terganggu untuk waktu yang lama. Oleh karena itu, untuk mengganti jaringan yang ada, perlu untuk menjaga konsistensi dengan infrastruktur jaringan asli sebanyak mungkin dan kompatibel dengan sistem bisnis yang ada. Pada saat yang sama, kita perlu menghilangkan konstruksi yang berlebihan untuk mengurangi biaya pemutakhiran sistem jaringan.

(2) Definisi Fungsi MIN-SRPN terdiri dari dua bagian bidang manajemen dan bidang data, yang masing-masing disebut MIS dan MIR.

Semua pengguna dan perangkat di MIN-SRPN diharuskan untuk mendaftar dengan identitas asli. MIS digunakan pada node blockchain untuk merekam identitas dan log perilaku pengguna guna memastikan bahwa konten seluruh jaringan terpadu, tahan terhadap gangguan, dan dapat dilacak. Modul manajemen identitas bertanggung jawab atas fungsi-fungsi termasuk pendaftaran pengguna, login pengguna, dan penerbitan sertifikat. Modul deteksi perilaku bertanggung jawab untuk menyimpan dan menganalisis catatan akses pengguna guna menjamin manajemen informasi dengan keamanan tinggi. Bidang data terutama terdiri dari sakelar dan MIR. Sebagai peralatan inti bidang data, MIR terutama digunakan untuk pengidentifikasi antar-terjemahan, perutean, penyaringan konten, perlindungan data, dan fungsi lainnya.

Fungsi MIN-SRPN didefinisikan sebagai berikut:

(1) De-IP progresif: MIN kompatibel dengan jaringan IP, sehingga MIN-SRPN dapat langsung digunakan pada jaringan IP di seluruh dunia. Perangkat lunak lapisan aplikasi yang ada tidak perlu diubah, dan konversi protokol jaringan dapat diselesaikan dengan bantuan perangkat lunak klien MIN.

(2) Kantor bergerak: MIN-SRPN memungkinkan staf kantor terbebas dari kendala waktu dan ruang, meningkatkan efisiensi kerja, dan memperkuat kolaborasi jarak jauh. Baik dalam perjalanan bisnis maupun dalam perjalanan ke kantor, pengguna jaringan eksternal dapat menyetujui dokumen, menelusuri pengumuman, menangani urusan pribadi, mengakses sumber daya jaringan internal, dan sebagainya secara tepat waktu.

(3) Manajemen identitas: Manajemen identitas mencakup pendaftaran pengguna, login pengguna, dan penerbitan sertifikat. Pengguna baru harus mendaftar dengan identitas asli mereka untuk mengakses jaringan kedaulatan. Mereka perlu mengautentikasi dan mendaftar dengan informasi asli seperti nomor ID, nomor ponsel, dan wajah saat

mereka mendaftar akun MIN. Sistem mengunggah dan menyimpan informasi pengguna di blockchain. Setelah MIS menerima informasi login pengguna dan mengautentikasi pengguna, sistem akan menerbitkan sertifikat pengguna ke EMIR untuk autentikasi dalam perutean.

(4) Manajemen otoritas: Pengguna dapat mengakses dan hanya mengakses sumber daya resmi mereka sendiri sesuai dengan kebijakan keamanan yang ditetapkan oleh sistem, dan sumber daya yang tidak sah tidak dapat diakses secara ilegal.

(5) Penyimpanan log: Server di MIN-SRPN akan mengekstrak alamat tujuan, port tujuan, URL HTTP, dan informasi lain dari setiap paket, yang akan digabungkan dengan informasi identitas pengguna untuk membentuk catatan akses pengguna dan dikirim ke MIS.

(6) Deteksi perilaku: Sistem harus secara efektif mengelola identitas pengguna yang sah, dan mampu mendeteksi perilaku ilegal pengguna yang sah. Fungsi deteksi perilaku MIS akan menganalisis dan meninjau catatan akses pengguna sesuai dengan persyaratan pengguna dan kebijakan keamanan.

(7) Keamanan endogen: Teknologi multitanda tangan memungkinkan keterlacakan paket jaringan, termasuk tanda tangan pengguna dan router hop pertama. Semua router di MIN dapat memverifikasi validitas paket jaringan dengan memeriksa tanda tangan. Paket data ilegal dapat ditelusuri kembali ke lokasi akses individu dan pengguna.

(8) Kesadaran situasional: Sistem kesadaran situasional keamanan dapat mewujudkan pemantauan jaringan tumpukan ganda secara real-time dan deteksi keamanan host target, serta evaluasi dan prediksi keamanan keseluruhan sistem saat ini secara real-time.

(9) Menolak serangan IP tradisional: MIN dapat kebal terhadap serangan berbasis TCP/IP tradisional, termasuk serangan ARP, pembajakan DNS, port sniffing, pemindaian kerentanan, serangan Trojan RAT, dll. Serangan-serangan tersebut di bawah jaringan IP tidak dapat berperan dalam lingkungan MIN-SRPN setelah pengujian.

2. Arsitektur MIN-SRPN

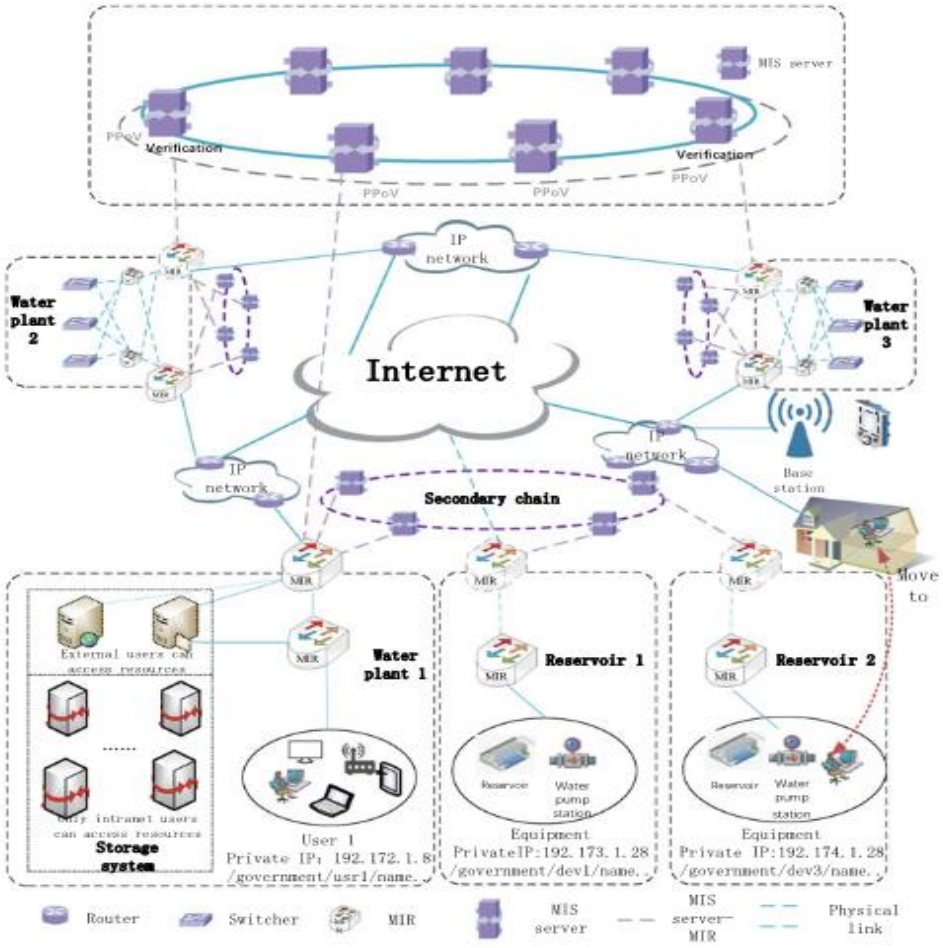
Seperti yang ditunjukkan pada Gambar 5.22, lingkungan MIN VPN akan dibangun antara kantor pusat OT-WSG dan setiap perusahaan air OT-WSG di Tiongkok. Ini adalah struktur jaringan dua lapis. Blockchain tingkat atas atau tingkat pertama terdiri dari catatan MIS di kantor pusat umum dan node MIS di kantor pusat cabang di setiap kota. Ada total puluhan node di blockchain tingkat atas, dan biasanya jumlah blockchain tingkat kedua sama. Setiap node MIS dari kantor pusat cabang di setiap perusahaan air yang berlokasi di setiap kota bersama dengan node MIS lainnya yang disebarkan di pabrik air, stasiun pompa air, dan lain-lain di kota yang sama, untuk membentuk masing-masing blockchain tingkat kedua.

Menurut tingkat keamanan sistem aplikasi, jaringan untuk melayani dapat dibagi menjadi area aplikasi umum dan area aplikasi inti. Server di area aplikasi umum terbuka untuk pengguna manajemen resmi dan terminal resmi. Server di area aplikasi inti terbuka hanya untuk pengguna manajemen resmi yang login dengan bastion host yang ditunjuk. Setelah membangun MIN-SRPN, struktur jaringan akan ditunjukkan seperti pada Gambar 5.23. MIR

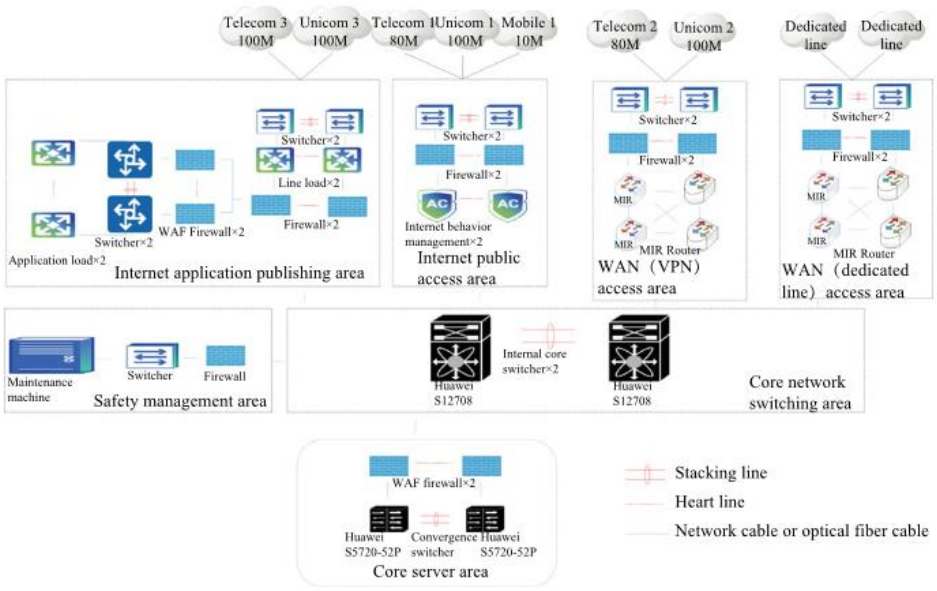
ditambahkan ke jalur khusus grup air dan setiap perusahaan air, yang menjadikan jaringan grup dan perusahaan air menjadi MIN-SRPN.

Topologi ini terutama terdiri dari sakelar, MIR, server MIS, dan perangkat lain, yang semuanya berada di lingkungan MIN. MIR disebarkan di pintu keluar setiap lokasi, dan node blockchain disebarkan pada server ini untuk membentuk sistem manajemen pengenal jaringan. Pada saat yang sama, MIR ini juga merupakan pintu keluar untuk mengakses jaringan IP. Di dalam setiap pabrik air dan stasiun pompa, MIR digunakan untuk membentuk MIN-SRPN. MIR terhubung langsung satu sama lain menggunakan kabel jaringan. Paket MIN ditransmisikan secara langsung menggunakan protokol MIN, melainkan protokol untuk komunikasi IP. MIR subnet MIN di beberapa situs menggunakan ekstranet IP sebagai terowongan komunikasi, yang secara logis membentuk MIN-SRPN yang terpadu. Arsitektur jaringan dua tingkat MIN-SRPN ditunjukkan pada Gambar 5.24. Rantai tingkat atas terdiri dari tujuh simpul jaringan awal, yang terhubung melalui Internet.

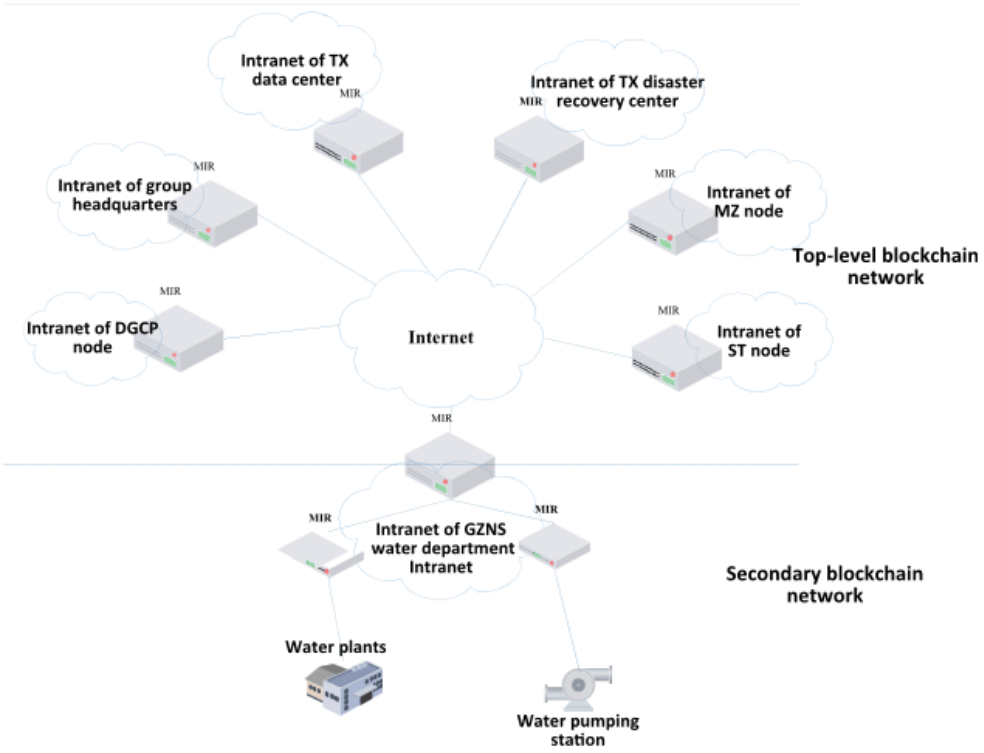
Jaringan blockchain sekunder terdiri dari MIR untuk setiap koneksi simpul dan perusahaan air atau lembaga bawahan lainnya termasuk pabrik air dan stasiun pompa air di dalam area simpul. Jaringan blockchain sekunder digunakan untuk mengautentikasi identitas penggunanya, mengelola otoritas penggunanya, serta meringankan beban jaringan jaringan blockchain tingkat atas.



Gambar 5.22 Arsitektur MIN-SRPN



Gambar 5.23 Struktur jaringan MIN-SRPN



Gambar 5.24 Arsitektur jaringan dua tingkat MIN-SRPN

Penerapan jaringan blockchain tingkat pertama pada tahap awal dirancang seperti pada Gambar 5.24. Mengingat bahwa setiap jaringan internal kelompok air merupakan jaringan IP independen, untuk memfasilitasi penerapan awal MIN-SRPN, terowongan IP diadopsi untuk mewujudkan koneksi antara sub-jaringan MIN yang terpisah. Pendekatan ini memungkinkan penerapan progresif. Jika perusahaan regional baru atau perusahaan air yang

disebut simpul baru kemudian bergabung dengan MIN blockchain tingkat atas, maka simpul tersebut dapat secara bertahap ditambahkan ke MIN tingkat atas dengan cara ini.

Ketika simpul baru bergabung dengan MIN-SRPN tingkat pertama, jaringan blockchain tingkat kedua yang sesuai dibuat sesuai dengan skala pabrik air dan stasiun pompa air di wilayah tersebut. Pada prinsipnya, simpul jaringan tingkat kedua mengambil kota-kota tingkat prefektur sebagai unit untuk penerapan. Server MIN sekunder diterapkan di semua pabrik air dan stasiun pompa air di wilayah tersebut untuk membentuk MIN-SRPN sekunder. Jika terdapat lebih dari satu perusahaan air di suatu area, disarankan untuk menetapkan satu perusahaan air sebagai simpul utama area tersebut untuk bergabung dengan MIN-SRPN tingkat pertama.

Ada dua cara untuk membentuk MIN-SRPN sekunder:

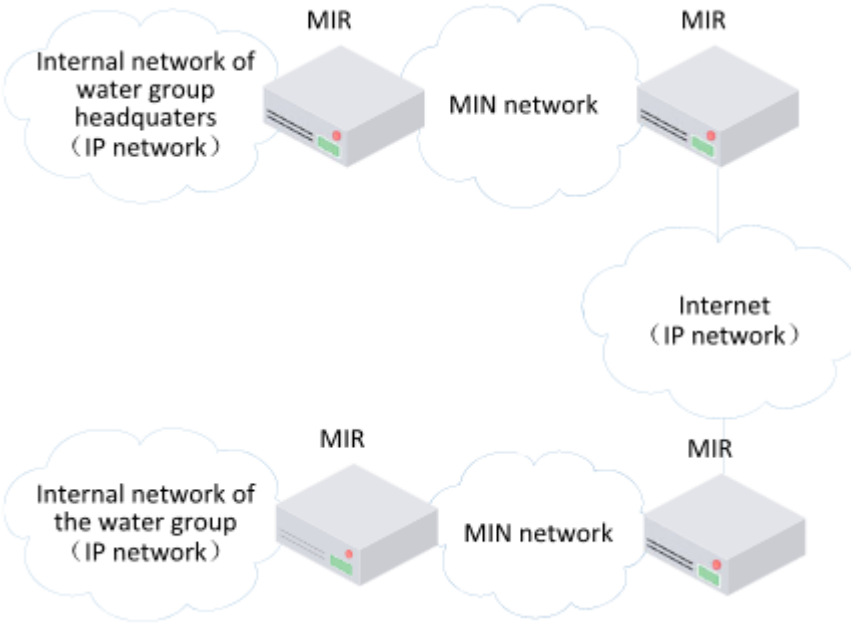
(1) Jika simpul baru dan simpul sekunder telah memasang jaringan kabel privat, hanya server MIR yang perlu dipasang pada setiap simpul sekunder di wilayah tersebut.

(2) Jika tidak ada jaringan kabel privat antara simpul baru dan simpul sekunder, jaringan tersebut perlu dihubungkan melalui jaringan publik Internet. Pemasangan antara simpul rantai sekunder dan simpul induk regional diperlukan dengan cara seperti yang ditunjukkan pada Gambar 5.25.

Menurut persyaratan OT-WSG untuk membangun jaringan yang aman dan andal, skema yang diusulkan mengadopsi MIN-SRPN dengan OT-WSG di Provinsi XYZ sebagai program percontohan. Skema tersebut membangun lingkungan jaringan yang aman dan andal tanpa mengubah topologi dasar jaringan yang ada.

5.2.3 Platform Layanan Cerdas Digital Sumber Daya Manusia Berbasis MIN

Aplikasi khas MIN-SRPN lainnya adalah platform layanan cerdas digital sumber daya manusia, yang bekerja sama dengan ShenZhen Zeneyes Digital Technology Co., Ltd.2 ShenZhen Zeneyes Digital Technology Co., Ltd. adalah perusahaan penelitian dan pengembangan inovatif yang berpusat di Shenzhen dengan teknologi blockchain mutakhir, dan berfokus pada penerapan industri digital sumber daya manusia. Proyek Sumber Daya Manusia Digital Smart Eye mereka adalah platform layanan cerdas digital sumber daya manusia yang inovatif dengan hak kekayaan intelektual independen yang dikembangkan secara mendalam dengan menggunakan teknologi big data dan blockchain. Platform ini menyediakan sistem kredit karier bagi para profesional di seluruh bidang ekologi, mendefinisikan ulang sistem evaluasi kredit dinamis karier, dan merekonstruksi ekologi digital nilai kredit karier dengan menginovasi "sistem sertifikasi kredit karier dinamis multilateral", "basis data besar keterlacakan kredit karier", "chip pekerjaan digital siklus hidup penuh", dan seterusnya.



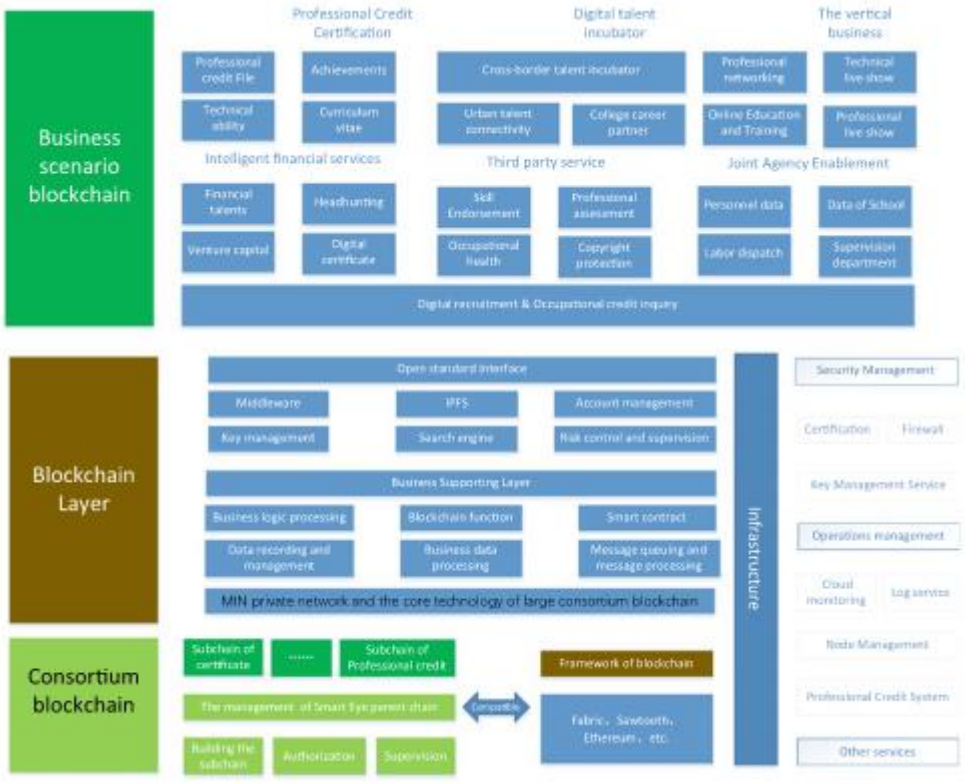
Gambar 5.25 Struktur logika jaringan

Fungsi inti dari platform layanan cerdas digital sumber daya manusia berbasis MIN adalah untuk secara objektif mendefinisikan dan mencatat seluruh sistem sertifikasi kredit siklus hidup para profesional dan membentuk basis data kredit profesional yang besar melalui penyimpanan terdistribusi, keterlacakan, dan teknologi enkripsi anti-rusak dari blockchain. Berdasarkan pembangunan basis data kredit profesional, chip kerja digital dikembangkan.

Dengan premis menghormati dan melindungi privasi individu, algoritma cerdas digunakan untuk mewujudkan pencocokan bakat yang efisien dan akurat dengan biaya hampir nol, dan kontrak cerdas digunakan untuk membentuk mekanisme koordinasi multilateral yang cepat dari transaksi dan manajemen bakat. Sementara itu, token ekologis digunakan untuk mendorong partisipasi multilateral dalam membangun nilai jangka panjang dari kredit bakat dan berkontribusi pada komunitas ekologis.

Platform layanan cerdas digital sumber daya manusia berbasis MIN menganjurkan "berorientasi pada orang, dan mengambil kredit sebagai prinsip" untuk menciptakan lingkungan digital yang kredibel, transparan, dan profesional. Dengan cara ini, seluruh dunia pekerja berintegritas mendapatkan hasil yang lebih baik dan kesempatan yang lebih adil, dan biaya serta risiko sumber daya manusia industri berkurang, sehingga meningkatkan nilai bakat dan likuiditas. Dikombinasikan dengan jaringan privat MIN dan teknologi inti blockchain konsorsium besar, blockchain konsorsium hierarkis industri vertikal sumber daya manusia digital super besar bernama Smart Eye Chain dengan keamanan tinggi dapat dibangun. Struktur Smart Eye Chain ditunjukkan pada Gambar 5.26.

Di masa mendatang, throughput Smart Eye Chain dapat mencapai 1 juta TPS. Sebagai salah satu infrastruktur digital sumber daya manusia di era Industri 4.0, ia akan berkembang menjadi lingkungan digital profesional dan pusat kolaborasi yang bersama, transparan, terkendali, universal, dan aman.



Gambar 5.26 Struktur rantai mata pintar

5.3 MIN DIADOPSI DALAM INTERNET INDUSTRI

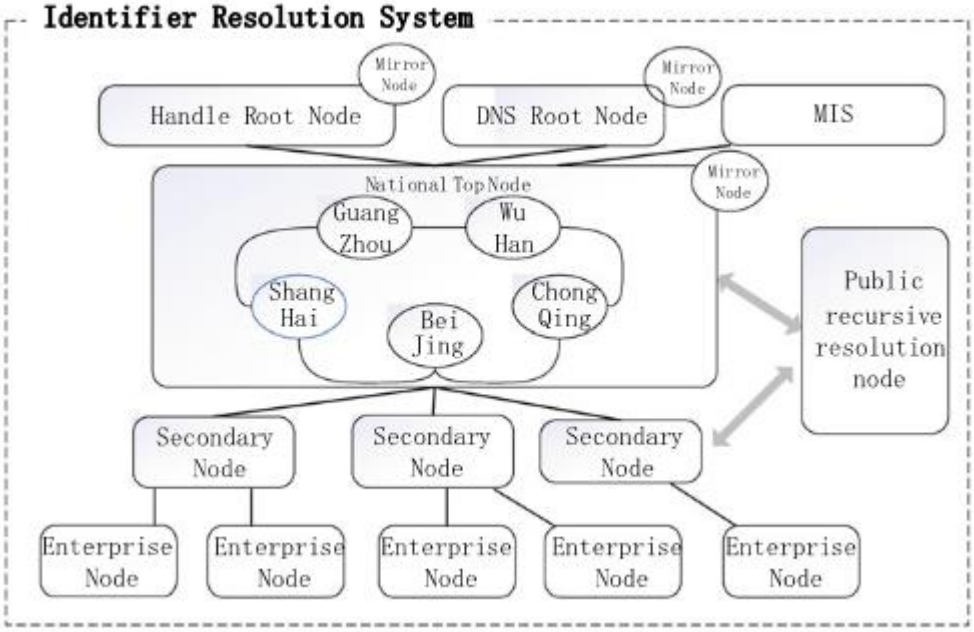
Internet of Things (IoT) menggambarkan Internet of Everything (IoE), yang merupakan jaringan yang diperluas dari Internet. IoT dapat menggabungkan berbagai perangkat penginderaan informasi dengan Internet untuk mewujudkan interkoneksi orang, mesin, dan benda kapan saja dan di mana saja. Ada dua teknologi utama dalam penerapan IoT, teknologi sensor dan teknologi tertanam.

5.3.1 Sistem Resolusi Pengenal Internet Industri Nasional dengan MIN

Sistem Pengenal Internet Industri Nasional yang ada seperti yang ditunjukkan pada Gambar 5.27. MIN telah diadaptasi sebagai Arsitektur sistem resolusi pengenal Internet Industri Nasional Tiongkok yang diberi nama MIN-II, yang dirancang menjadi empat tingkat: simpul tingkat atas nasional, simpul akar internasional yang terhubung ke simpul tingkat atas nasional, simpul sekunder, dan simpul layanan rekursif. Pada akhir tahun 2018, lima simpul tingkat atas nasional resolusi pengenal di Beijing, Shanghai, Guangzhou, Wuhan, dan Chongqing telah dioperasikan, yang sepenuhnya mendukung berbagai sistem resolusi pengenal. Hingga 15 November 2020, jumlah pengenal terdaftar telah mencapai lebih dari 915 juta, dengan 785 perusahaan terkait.

Berdasarkan simpul tingkat atas nasional, fungsi dan kapabilitas sistem terus ditingkatkan sesuai dengan rencana yang ditetapkan, dan infrastruktur jaringan sistem resolusi pengenal secara bertahap dibangun untuk integrasi terbuka, manajemen terpadu, interkoneksi, keamanan, dan keandalan. Di sisi lain, simpul sekunder bersifat tambahan, dan

sejumlah simpul sekunder telah memainkan perannya dalam meneliti pendekatan baru. Simpul Internet sekunder dibangun untuk mempromosikan aplikasi inovasi terintegrasi dari resolusi pengenal Internet Industri. Terakhir, sistem resolusi pengenal dibangun untuk aplikasi Industri. Ekologi industri resolusi pengenal dapat dibangun secara bertahap dengan mendorong demonstrasi aplikasi di banyak industri seperti penerbangan dan kendaraan mesin.



Gambar 5.27 Sistem pengenal internet industri nasional

Keamanan sistem Internet of Things sangat penting. Tidak semua node harus berjalan pada tingkat global, seperti lapisan TCP/IP. Misalnya, banyak sensor dan aktuator terminal tidak dapat menjalankan tumpukan protokol TCP/IP. Daya komputasi perangkat Internet Industri selalu rendah, yang hanya menyediakan beberapa layanan aplikasi sederhana. Keamanannya sepenuhnya bergantung pada mekanisme enkripsi bawaan karena sulit untuk memasang perangkat lunak pertahanan. Jika pengguna menyimpan kata sandi default, peretas dapat dengan mudah membobol Internet of Things. Setelah meretas Internet of Things, peretas akan beralih menyerang sistem lain di Internet of Things, bahkan mendapatkan akses ke data pengguna, yang dikenal sebagai Stepping Attack.

Beberapa kelompok peretas dapat mengeposkan aplikasi palsu atau berbahaya di Google Play untuk mencuri data pengguna agar tidak diketahui pengguna. Selain itu, mereka dapat meluncurkan serangan bergaya pemblokiran melalui botnet yang terdiri dari perangkat Internet of Things, seperti printer, kamera, monitor bayi, router rumah, dan sebagainya. Pada tanggal 21 Oktober 2016, banyak serangan penolakan layanan terjadi di penyedia DNS utama, dan target semua serangan adalah server Dyn yang merupakan penyedia sistem nama domain. Petugas keamanan jaringan percaya bahwa itu adalah botnet yang terdiri dari banyak

perangkat Internet of Things, yang menginfeksi perangkat lunak berbahaya Mirai. BBS, media Inggris, juga terkena serangan lalu lintas 602 Gbps yang memecahkan rekor.

5.3.2 Internet Industri Nasional dengan MIN

Untuk mengatasi masalah ini, Internet of Things digabungkan dengan jaringan kedaulatan.

(1) Pertama, jaringan kedaulatan adalah jaringan otonom yang aman.

(2) Kedua, jaringan kedaulatan membuat perangkat Internet of Things menggunakan pengenalnya dalam suatu domain. Hanya ketika perangkat ini perlu berkomunikasi dengan perangkat di luar domain, penerjemahan pengenal akan dilakukan. Dengan cara ini, perangkat terhubung ke Internet secara terbatas untuk mengimbangi kurangnya kemampuan akses.

(3) Ketiga, dalam sistem IoT jaringan kedaulatan, node dapat menggunakan paket minat untuk mengelola perangkat dengan beberapa tugas, seperti menyalakan peralatan rumah tangga. Data dapat digunakan untuk mengonfirmasi pelaksanaan tugas dan melaporkan hasil operasi, seperti keberhasilan atau kegagalan. Mode tarik digunakan untuk mengelola perangkat deteksi, sedangkan mode dorong digunakan untuk perangkat aplikasi IoT untuk mengirimkan data.

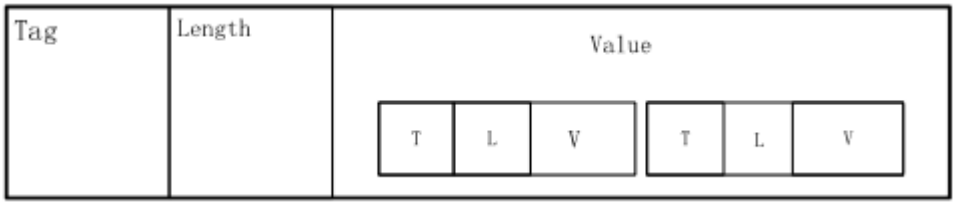
(4) Keempat, terdapat banyak cache di jalur transmisi jaringan kedaulatan. Meskipun sumber daya perangkat IoT terbatas, pengenalan cache meningkatkan efisiensi energi, laju transmisi, dan ketepatan waktu. Arsitektur MIN dapat digunakan di Internet of Things dan Internet Industri yang ada. Di Internet Industri, sistem resolusi pengenal tidak hanya merupakan bagian penting dari arsitektur jaringan, tetapi juga hub saraf yang mendukung interkoneksi dan interworking Internet Industri [6]. Dengan memberikan pengenal identitas unik untuk setiap produk, komponen, mesin, atau hak cipta kekayaan intelektual digital, sumber daya jaringan dapat dibedakan secara fleksibel dan dikelola secara efektif. 1. Sistem Pengenal Sistem layanan root, berdasarkan arsitektur MIN, menyediakan banyak fungsi, seperti pembuatan, pengelolaan, dan resolusi identitas, konten, layanan, alamat IP, dan pengenal geografis. Pada saat yang sama, ia kompatibel dengan klaster protokol TCP/IP yang ada, menyediakan layanan resolusi nama domain DNS Internet tradisional, dan menyediakan fungsi penerjemahan timbal balik antara beberapa pengenal. MIN-II mempercepat proses "Internet of everything", memastikan keterlacakan data dan perlindungan privasi dalam jaringan, dan memperbaiki masalah pengawasan yang tidak teratur dan sulit dari Internet IP yang ada.

Dalam ruang digital MIN-II, objek digital harus memiliki pengenal yang sesuai, menyelesaikan dan menggunakan pengenal secara dinamis sesuai permintaan. Di masa mendatang, pemisahan objek dan posisi digital akan terwujud, dan kelebihan muatan semantik IP dapat dipisahkan, untuk mewujudkan mekanisme pemisahan objek dan posisi digital. Namun, sistem pengenal arus utama yang ada, seperti sistem Handle berdasarkan rute reformasi, dan sistem pengenal Ecode dan OID berdasarkan rute peningkatan teknologi DNS, belum menyingkirkan sistem IP. Mekanisme terowongan multi-pengenal digunakan dalam sistem layanan akar

multi-pengenal untuk menyelesaikan berbagai transmisi terowongan dan skenario pertukaran kunjungan, seperti IP-Konten-IP, IP-Identitas-IP, Konten-Identitas-Konten, dan seterusnya.

MIN-II yang mendukung Internet Industri berfokus pada pendefinisian ulang lapisan jaringan yang ada untuk mendukung pengidentifikasi Internet Industri, berdasarkan pengidentifikasi lain yang telah didukung, termasuk identitas, konten, layanan, alamat IP, dan pengidentifikasi geografis. Pada lapisan jaringan MIN, beberapa paket pengidentifikasi, paket manajemen sistem, paket kontrol harus hidup berdampingan dan didukung untuk perutean. Metode implementasi spesifik membedakan berbagai jenis paket pengidentifikasi dengan tajuk pesan TLV. Pada lapisan jaringan MIN, informasi pengenal dienkapsulasi ke dalam pesan TLV yang dapat ditransmisikan oleh MIR dan diteruskan ke MIR berikutnya menurut Basis Informasi Penerusan (FIB).

Kemudian, skema format pesan multi-pengenal berdasarkan struktur TLV dirancang sebagai berikut. Tag paket yang diminati digunakan untuk merepresentasikan informasi identitas, yang mewujudkan ruang jaringan multi-pengenal. Secara khusus, jenis tag dalam struktur TLV digunakan untuk membedakan berbagai jenis pengenal. Pengenal Internet Industri digunakan untuk mengelola dan menetapkan berbagai jenis pengenal secara seragam kepada bawahannya, yang juga bersarang di bawah pengenal Internet Industri dalam format TLV. Menurut persyaratan standar ASNI, rentang nilai Tag adalah 1 hingga 2 byte. Untuk memenuhi kebutuhan berbagai pengenal Internet Industri di dalam dan luar negeri, serta pengenal khusus untuk berbagai industri dan perusahaan, sistem layanan akar multi-pengenal mengadopsi skema 2-byte (Gambar 5.28).



Gambar 5.28 Rata-rata pengkodean rekursif dari pengidentifikasi

Berbagai paket dalam lapisan jaringan MIN dibedakan berdasarkan tag TLV tingkat atas. Lapisan jaringan ditambahkan ke sistem yang membawa paket-paket ruang multi-pengidentifikasi. Menurut persyaratan desain, paket-paket tambahan yang digunakan untuk merepresentasikan kelas-kelas identitas dalam ruang jaringan multi-pengidentifikasi mencakup kategori-kategori berikut:

(1) Paket Minat MIN
(2) Paket Data MIN
(3) Pengidentifikasi Identitas
(4) Pengidentifikasi Layanan
(5) Pengidentifikasi Geografis
(6) Pengidentifikasi Internet Industri
(7) Paket Manajemen

(8) Paket Kontrol

Dalam lingkungan produksi Internet Industri, transmisi data berjalan secara independen dari lingkungan jaringan IP. Dalam hal ini, data ditransmisikan dengan mode transmisi jaringan yang mirip dengan yang ada di Named Data Network (NDN) [7]. Penerima meminta konten dengan mengeluarkan paket Minat, kemudian paket Data yang sesuai dikembalikan sebagai respons terhadap Minat tersebut. Berbagai jenis pengenal bergantung pada TLV tag untuk menyelesaikan proses yang sesuai, atau bergantung langsung pada mode enkapsulasi Internet Industri untuk pengemasan dan transmisi data.

Untuk pengenal Internet Industri, nilai tag dalam struktur TLV dibagi menjadi empat jenis menurut aturan tertentu, seperti yang ditunjukkan pada Tabel 5.1.

Untuk sistem pengenal domestik dan asing, sistem mengalokasikan pengenal secara seragam. Jika berbagai industri dan perusahaan perlu mendefinisikan pengenal mereka secara otonom, mereka perlu mengajukan permohonan ke MIS, yang merupakan bidang manajemen MIN. Ketika pengguna mendaftarkan pengenal identitasnya di MIS untuk pertama kalinya,pengguna perlu memberikan informasi dasar dan kunci publik ke MIS. Setelah MIS menyampaikan permintaan pendaftarannya, MIS menerbitkan sertifikat kepada pengguna dan menyimpannya di blockchain. Setelah itu, semua informasi interaksi antara pengguna dan MIS mengharuskan pengguna menandatangani dengan kunci pribadinya. MIS memvalidasi informasi tersebut sebelum operasi lebih lanjut. Ketika pengguna mengajukan pengenal khusus, MIS terlebih dahulu memverifikasi sertifikat, kemudian MIS mengalokasikan nilai tag dalam sistem untuk memastikan keunikan nilai tag, dan sesuai dengan spesifikasi yang sesuai, memastikan bahwa pengenal khusus tersebut sesuai dengan persyaratan MIN.

Tabel 5.1 Rentang dan deskripsi nilai tag dalam struktur TLV

Rentang	Deskripsi
0x01-0xFF	Bidang yang dicadangkan
0x100-0x1FF	Alokasikan ke sistem pengenal domestik dan asing yang ada, seperti Handle, GS1
0x200-0xFFF	Alokasikan ke berbagai industri
0x1000-0xFFFF	Bidang yang disesuaikan

2. Pendaftaran dan Permintaan Pengenal

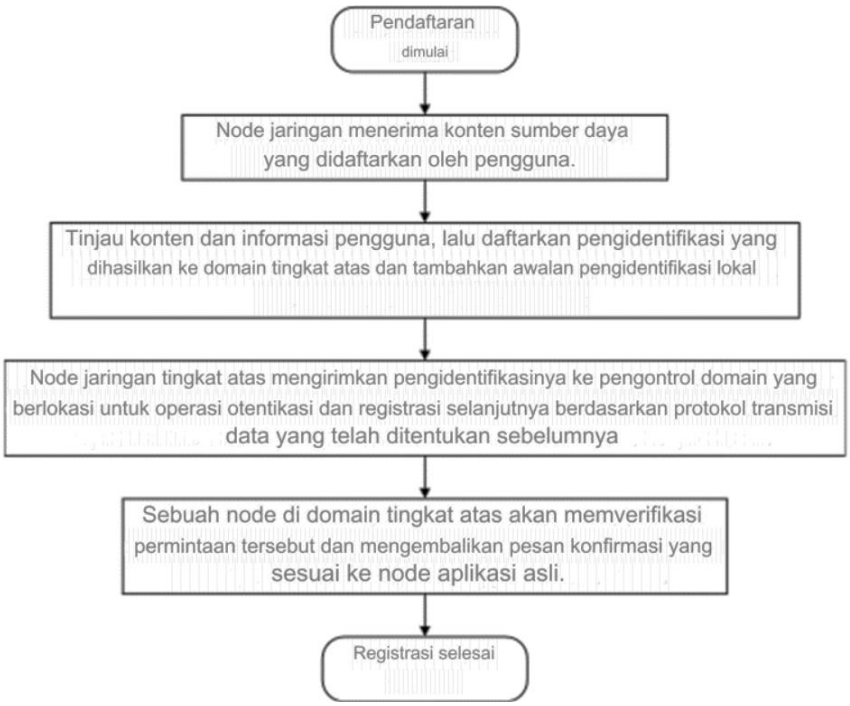
Jaringan mendukung perutean dengan berbagai jenis pengenal, termasuk pengenal identitas, pengenal konten, pengenal lokasi spasial, dan pengenal alamat IP, dsb. Pengenal konten semua sumber daya dalam jaringan terikat pada pengenal identitas penerbit. Setelah pengguna masuk ke jaringan, pengenal lokasi spasial dan sumber daya jaringan yang diakses akan dicatat di simpul pengawasan blockchain jaringan untuk pengawasan keamanan dan perlindungan data (Gambar 5.29 dan gambar 5.30).

Prosedur pendaftaran pengenal mencakup langkah-langkah berikut:

- **Langkah 1**: Mendaftarkan sumber daya: Simpul jaringan menerima konten sumber daya yang didaftarkan oleh pengguna. Pada saat yang sama, simpul jaringan

menambahkan pengenal identitas penerbit konten dan pengenal lokasi spasial sesuai dengan tempat konten disimpan;

- ☞ **Langkah 2**: Autentikasi simpul jaringan: Setelah menerima permintaan pendaftaran pengenal dari pengguna, simpul akan meninjau konten dan informasi pengguna, serta pengenal sumber daya, kemudian mendaftarkan pengenal yang dihasilkan ke domain tingkat atas dan menambahkan awalan pengenal lokal;
- ☞ **Langkah 3**: Transmisi permintaan pendaftaran pengenal: Setelah menerima permintaan pendaftaran pengenal, simpul jaringan tingkat atas mengirimkan pengenalnya ke pengendali domain yang berlokasi untuk operasi autentikasi dan pendaftaran berikutnya berdasarkan protokol transmisi data yang telah ditetapkan sebelumnya;
- ☞ **Langkah 4**: Verifikasi pengenal: Setelah menerima permintaan pendaftaran pengenal dari domain jaringan bawahan, simpul pada domain tingkat atas akan memverifikasi permintaan dan mengembalikan pesan konfirmasi yang sesuai ke simpul aplikasi asli. Skema penyimpanan terdistribusi memastikan bahwa semua pengenal yang terdaftar tidak dapat dirusak. Pengenal asli akan disimpan pada basis data terdistribusi dari domain tingkat atas. Setelah waktu yang ditentukan sebelumnya, sinkronisasi basis data terkait akan dilakukan di seluruh jaringan untuk menjamin bahwa informasi pengenal sumber daya antara domain tingkat atas masing-masing setara dan terpadu.

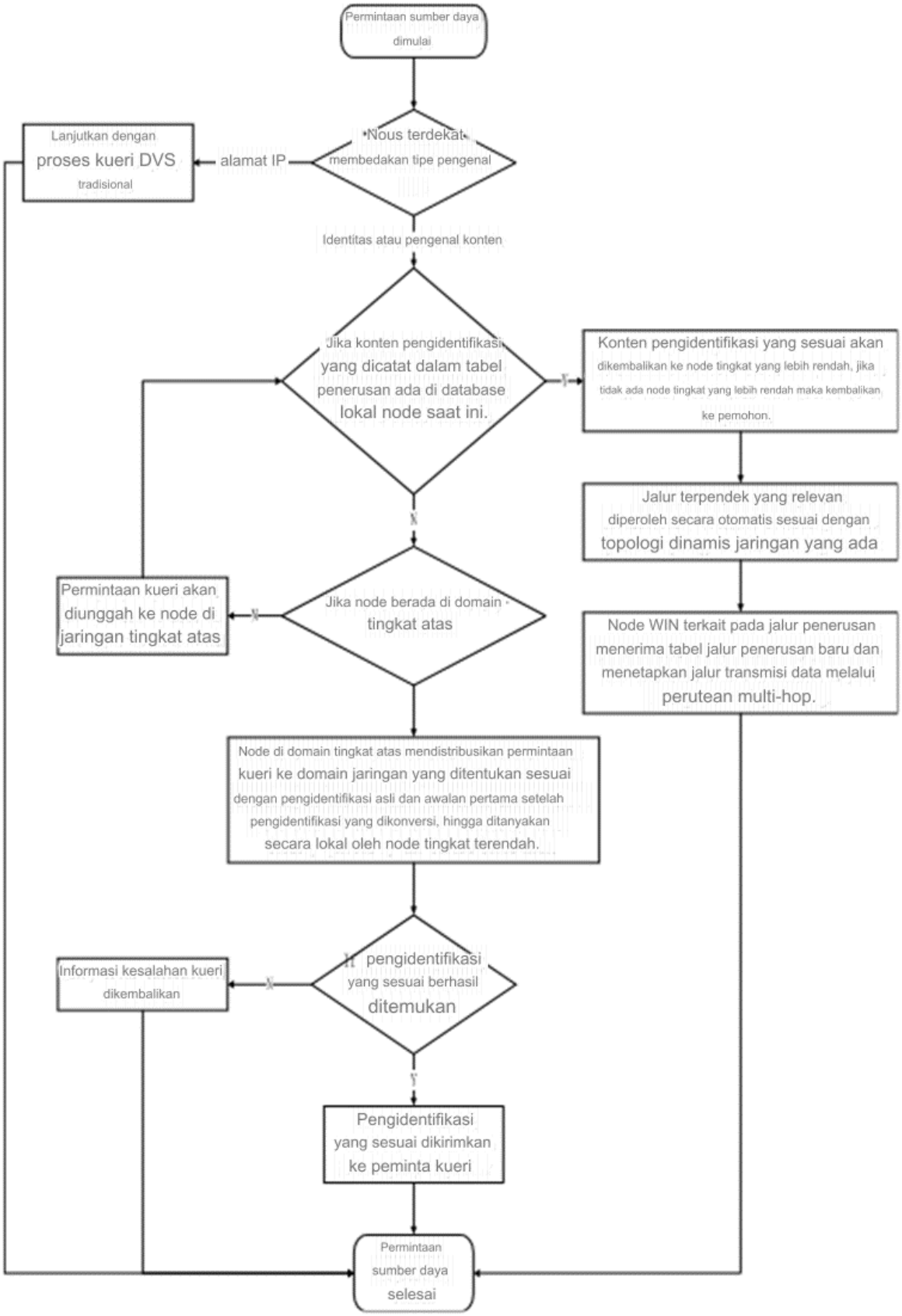


Gambar 5.29 Prosedur registrasi identifier

Prosedur permintaan sumber daya jaringan mencakup langkah-langkah berikut:

- ☞ Langkah 1: Permintaan permintaan: Permintaan permintaan dikirimkan ke node jaringan terdekat;

- Langkah 2: Permintaan data pengenal lokal: Ketika node MIN terdekat menerima permintaan, node tersebut akan terlebih dahulu mengenali jenis pengenal. Jika berupa alamat IP, node tersebut akan melanjutkan proses permintaan DNS tradisional. Jika berupa pengenal identitas atau konten, maka permintaan akan diajukan pada tabel penerusan. Jika konten pengenal yang tercatat dalam tabel penerusan sudah ada dalam basis data lokal, maka konten pengenal yang sesuai akan dikembalikan; jika tidak, langkah 3 akan dijalankan;
- Langkah 3: Meminta pengiriman permintaan: Ketika tidak ada pengenal terkait yang tersimpan dalam basis data lokal, permintaan permintaan akan diunggah ke node pada jaringan tingkat atas. Setelah menerima permintaan kueri, simpul tingkat atas akan mengkueri pengenal dengan mengikuti langkah 1 hingga langkah 2. Jika konten pengenal yang sesuai ditemukan, konten tersebut akan dikembalikan ke simpul tingkat rendah; jika tidak, permintaan kueri selanjutnya dikirimkan ke simpul tingkat atas secara rekursif hingga simpul jaringan domain tingkat atas;
- Langkah 4: Kueri pengenal, verifikasi, dan interworking: Setelah pengenal terdaftar yang relevan ditemukan, jalur terpendek yang relevan secara otomatis diperoleh menurut topologi dinamis jaringan yang ada. Kemudian simpul MIN terkait pada jalur penerusan menerima tabel jalur penerusan baru dan membuat jalur transmisi data melalui perutean multi-hop. Jika bahkan simpul di domain tingkat atas tidak menemukan pengenal yang sesuai, informasi pengenal jaringan lain yang sesuai dengan pengenal tersebut dikueri dalam basis data dengan melanjutkan seperti langkah 5; (5) Langkah 5: Distribusi permintaan pengenal: Node di domain tingkat atas akan mendistribusikan permintaan kueri ke domain jaringan yang ditentukan sesuai dengan pengenal asli dan awalan pertama dari pengenal yang dikonversi, hingga dikueri secara lokal oleh node tingkat terendah. Jika pengenal yang sesuai berhasil ditemukan, maka akan dikirimkan ke peminta kueri; jika tidak, informasi kesalahan kueri akan dikembalikan.



Gambar 5.30 Prosedur permintaan sumber daya jaringan

5.3.3 Intertranslasi Beberapa Pengenal Jaringan

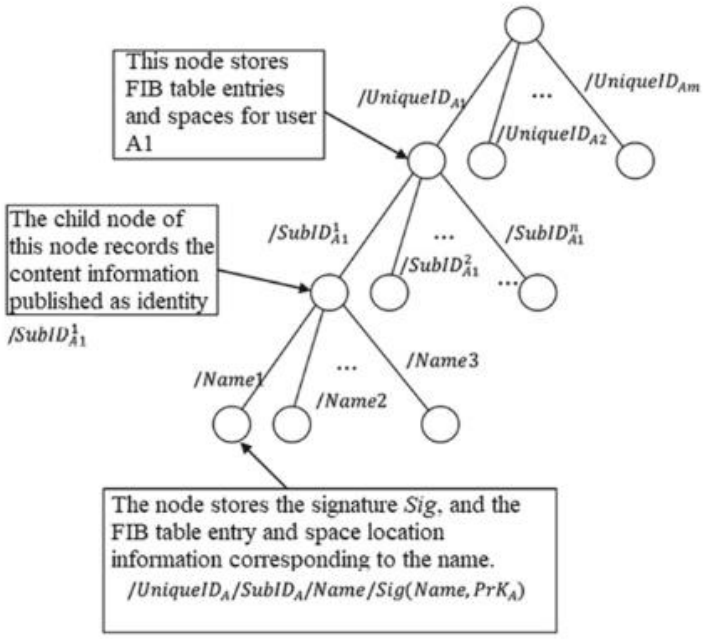
Ketika suatu konten didaftarkan dan dipublikasikan pada jaringan multi-pengenal, pengenal identitas tersebut terikat dengan beberapa pengenal, seperti identitas, konten, informasi lokasi, dan alamat IP. Oleh karena itu, beberapa pengenal perlu diberi alamat yang sama. Selain itu, pengenal dalam Internet Industri harus berorientasi pada aplikasi dan mencatat informasi produk. Di sisi lain, pengenal tersebut harus mendukung pengalamatan dan perutean. Karena keberagaman aplikasi, sulit untuk menetapkan skema penamaan hierarkis global yang sesuai untuk semua aplikasi. Oleh karena itu, dalam platform layanan Internet Industri berbasis multi-pengenal, tidak dapat dihindari bahwa beberapa pengenal jaringan dan beberapa sistem standar resolusi pengenal harus hidup berdampingan. Ruang nama yang unik secara global perlu ditetapkan, serta ruang nama yang unik untuk setiap aplikasi. Tabel penerjemahan multi-pengenal digunakan untuk membuat tabel penerjemahan antar (IFB) dan mekanisme interoperabilitas dengan pengidentifikasi umum yang ada.

1. Proses Penerjemahan Antara Nama dan Identitas

Untuk menjaga lingkungan jaringan yang aman, kami mengikat nama konten ke identitas penerbit aslinya, dan menggunakan ekstensi yang valid untuk mengidentifikasi sumber daya jaringan dalam mode berikut:

$$/UniqueID_A/SubID_A/Name/Sig(Name, PrK_A)$$

$UniqueID_A$ adalah pengenal unik global dari penerbit A, dan tidak terjadi tabrakan. Ia akan menghasilkan pasangan kunci publik-pribadi dari pengguna; $SubID_A$ adalah pengenal sekunder saat konten dipublikasikan, karena pengguna yang sama dalam jaringan mungkin memiliki beberapa identitas. Nama adalah nama konten hierarkis; Sig (Nama, PrK_A) adalah tanda tangan dari nama konten yang ditandatangani oleh A.



Gambar 5.31 Arsitektur penerusan beberapa pengidentifikasi menggunakan struktur pohon awalan

Sebelum konten diterima oleh pengguna atau di-cache di node perutean perantara, tanda tangannya harus diverifikasi untuk memastikan keabsahannya berdasarkan mekanisme keamanan yang dijelaskan di atas. Hasilnya, sumber daya apa pun dalam jaringan dapat dilacak kembali ke penerbit aslinya, yang menjamin sifat regulasi dari perilaku penerbitan dan keamanan transmisi jaringan. Berdasarkan representasi ini, pengenal dianggap sebagai bentuk khusus dari nama ekstensi, yaitu, yang memiliki nama konten kosong. Oleh karena itu, kami menggunakan struktur data pohon awalan untuk mendukung operasi penyimpanan dan kueri pada nama dan identitas. Dengan metode representasi ini, identitas dianggap sebagai bentuk khusus dari nama ekstensi; yaitu, ketika nama konten kosong, maka kami menggunakan pohon awalan sebagai struktur data untuk mendukung operasi penyimpanan dan kueri nama dan identitas seperti yang ditunjukkan pada Gambar 5.31.

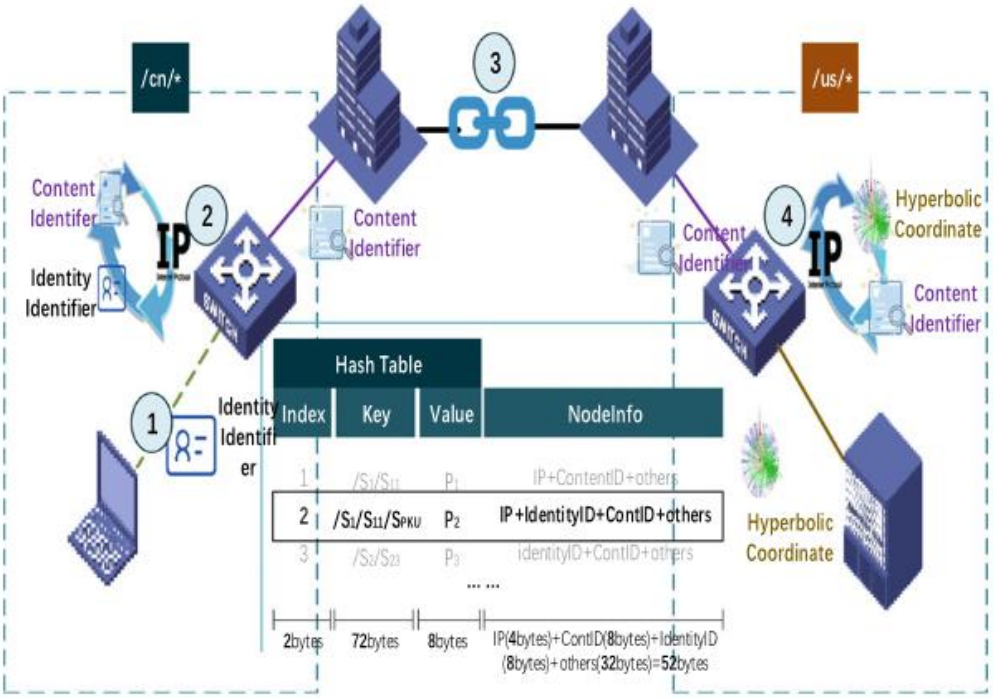
2. Penerjemahan Antara Lokasi, Nama, dan Identitas

Seperti disebutkan di atas, setiap pengguna berkorespondensi dengan pengenal lokasi spasial nyata atau virtual yang unik. Untuk nama dalam jaringan, untuk mengurangi penundaan perutean, kami menetapkan pengenal lokasinya ke lokasi simpul terdekat yang menyimpan konten nama yang sesuai, yang dihitung dan didistribusikan oleh simpul kontrol atas. Urutan transformasi ditunjukkan pada Gambar 5.32.

- Langkah 1: Permintaan sumber daya dikeluarkan dengan pengenal tertentu.
- Langkah 2: Sistem multi-pengenal melakukan kueri berdasarkan jenis pengenal: (1) Jika permintaan dikeluarkan dengan nama domain tradisional, maka DNS akan langsung dikueri. (2) Jika itu adalah alamat IP, dan ada sebagai entri tabel penerusan antar-terjemahan pengenal (IFB), penerjemahan bersama dilakukan; jika tidak, agen mengakses jaringan IP tradisional; (3) Jika pengenal tersebut adalah jenis pengenal lain seperti pengenal NDN, atau pengenal identitas, pengenal konten pertama kali di-query di CS, PIT, dan tabel penerusan antartranslasi. Jika ada, antartranslasi dilakukan; jika tidak, lanjutkan ke langkah 3.
- Langkah 3: Jika pengenal tidak ada di domain saat ini, sistem multi-pengenal akan melakukan query secara rekursif hingga ke domain teratas.
- Langkah 4: Jika tidak ada informasi pengenal tersebut di domain tingkat atas, query akan dilakukan sesuai dengan domain tingkat bawah spesifik dari informasi pengenal, hingga domain tingkat bawah yang ditentukan oleh pengenal, dan hasil yang sesuai akan dikembalikan setelah ada. Jika tidak, pesan kesalahan query akan dikembalikan. Selain itu, kami menggunakan akses dan transmisi tepercaya, penyimpanan dan pengelolaan tepercaya dari teknologi pengenal Internet Industri, serta teknologi analisis dan penambangan data dari perutean pengenal. Sistem layanan akar Internet industri dasar dibuat untuk mendukung berbagai layanan pendaftaran, analisis, dan pengelolaan pengenal dari node rekursif jaringan dan node blockchain. Sistem ini kompatibel dengan sistem protokol TCP/IP yang ada dan mendukung transisi non-aware dari jaringan IP saat ini ke jaringan MIN di masa mendatang.

(1) Setelah sistem layanan akar multi-pengenal selesai di masa mendatang, sistem ini terhubung dengan node nasional. Layanan pendaftaran dan resolusi pengenal akan

mencakup seluruh negara bagian, dan mendukung layanan transnasional. Bersama dengan node tingkat atas nasional, sistem ini menyediakan layanan akses dan resolusi untuk node tingkat kedua nasional, node rekursif, node resolusi nama domain tingkat atas, dan node infrastruktur blockchain. Pengembangan sistem ini memerlukan pembentukan pendaftaran pengenal, resolusi, manajemen data, penyimpanan informasi identitas, sistem demonstrasi aplikasi, dan solusi yang dapat diskalakan. Sistem layanan akar pengenal menyediakan semua jenis layanan resolusi pengenal, dan mengatasi fondasi yang lemah dan kesulitan koordinasi dalam bidang desain industri, manufaktur, dan aplikasi Tiongkok, menyediakan berbagi informasi dan aplikasi di seluruh perusahaan, kawasan, dan industri, mencakup semua rantai proses dan industri. Ini akan secara efektif mendukung regulasi pemerintah, membangun pola simbiosis baru dan rantai industri yang saling menguntungkan, dan membuka prospek baru untuk pembangunan yang mandiri, terkendali, dan berkelanjutan.



Gambar 5.32 Proses penerjemahan antara lokasi, nama, dan identitas

5.3.4 Resolusi Pengenal dalam Internet Industri Otomotif

Pengenal Internet Industri industri otomotif merupakan sumber daya dasar utama untuk mengidentifikasi dan mengelola kendaraan, suku cadang, dan peralatan secara lengkap. Pengenal ini serupa dengan nama domain di Internet, yang memberikan objek target sebuah "ID" yang mengenali dan mengelola sumber daya dengan cara mengganti pengenal antara dunia fisik dan dunia maya virtual secara bebas. Resolusi pengenal dalam Internet Industri otomotif adalah dengan menanyakan alamat server yang menyimpan informasi produk melalui "ID" (kode identifikasi) unik produk, atau menanyakan informasi dan layanan terkait

produk. Oleh karena itu, resolusi pengenal dalam Internet Industri otomotif merupakan dasar penting untuk mewujudkan revolusi layanan penghubung dan Internet Industri otomotif.

MIN-II bukan hanya bagian penting dari arsitektur Internet Industri otomotif, tetapi juga hub saraf yang mendukung interkoneksi Internet Industri. Dalam proses eksplorasi konstruksi simpul sekunder untuk MIN-II, konstruksi sistem resolusi pengenal dengan MIN dibagi menjadi delapan langkah: (1) identifikasi objek pengenal; (2) perumusan kode pengenal; (3) pemilihan terminal pengenal; (4) pemeliharaan data pengenal; (5) jaminan keamanan pengenal; (6) konstruksi simpul sekunder resolusi pengenal; (7) penyusunan sistem resolusi pengenal standar; (8) pengembangan perangkat lunak aplikasi berbasis pengenal. 1. Objek Pengenal dan Pengodean Pengenal Internet Industri mobil mencakup semua aspek rantai nilai industri mobil. Dikombinasikan dengan status terkini manajemen industri mobil Tiongkok dan standar terkait, kendaraan, suku cadang, organisasi, peralatan terutama digunakan untuk membangun sistem resolusi pengenal.

(1) Pengenal Kendaraan

Pengenal kendaraan terutama terkait dengan penelitian dan pengembangan (R&D) kendaraan, produksi, penjualan, dan pemeliharaan, termasuk: pengenal model kendaraan, pengenal pengumuman kendaraan, pengenal nomor pengenal kendaraan (VIN), pengenal daftar konfigurasi kendaraan, pengenal pesanan produksi kendaraan, pengenal pesanan penjualan, pengenal pesanan pemeliharaan kendaraan, dan sebagainya.

(2) Pengenal Suku Cadang

Pengenal suku cadang digunakan untuk produksi dan perawatan kendaraan, termasuk: pengenal klasifikasi suku cadang, pengenal suku cadang tunggal atau batch, pengenal pesanan pembelian suku cadang, pengenal pesanan produksi suku cadang, pengenal pesanan logistik suku cadang, pengenal pesanan penyimpanan suku cadang, dan pengenal pesanan perawatan suku cadang.

(3) Pengenal Kategori Peralatan

Pengenal kategori peralatan terutama diterapkan pada mobil selama produksi, transportasi, dan penjualan. Ini termasuk: pengenal klasifikasi peralatan, pengenal peralatan, pengenal kegagalan peralatan, pengenal fungsi peralatan, dan pengenal lokasi peralatan.

(4) Pengenal Institusi

Pengenal institusi merujuk pada berbagai jenis objek dalam rantai nilai ekologis industri otomotif. Secara umum, pengenal institusi mencakup pengenal perusahaan manufaktur kendaraan, pengenal perusahaan manufaktur komponen, pengenal perusahaan penjualan, dan pengenal layanan purnajual perusahaan. Dalam perusahaan, pengenal institusi juga menunjukkan pengenal pabrik dan pengenal bengkel serta pengenal departemen manajemen internal.

(5) Pengenal Kategori Kualitas

Pengenal kategori kualitas menyatakan standar dan tingkat produk yang diperiksa oleh industri otomotif, termasuk: pengenal standar pemeriksaan produk, pengenal tingkat kualitas, pengenal penyebab cacat, dan pengenal tingkat cacat.

Kode merupakan sarana teknis dasar bagi orang untuk menyatukan pandangan dan bertukar informasi. Tujuan pengkodean adalah untuk meningkatkan efisiensi pemrosesan informasi. Pembentukan pengkodean pengenal merupakan teknologi untuk mendefinisikan, menetapkan, dan mengelola struktur data format pengkodean pengenal Internet Industri. Saat ini, sistem teknologi pengkodean arus utama mencakup pengkodean GS1, EPC, Handle, OID, Ecode, dan sebagainya. Metode pengkodean yang diusulkan untuk pengenal Internet Industri otomotif terdiri dari awalan dan akhiran. Awalan ditetapkan oleh simpul primer dan simpul sekunder, sedangkan akhiran terutama terdiri dari pengenal aplikasi dan kode unik. Pengenal aplikasi digunakan untuk membedakan antara objek pengenal yang berbeda dalam resolusi pengenal Internet Industri otomotif. Misalnya, simpul sekunder dalam membangun MIN-II, menggunakan "V" untuk mewakili kendaraan dan "91" untuk mewakili suku cadang otomotif. Untuk kendaraan, pengkodean pengenal seperti (Tabel 5.2).

Tabel 5.2 Pengkodean pengenal

88.107.00001	/	(V)	LRDXXXXXXXXXXXX
88.107.00001	/	(91)	XXXXXXXX
Awalan	Komponen	Pengidentifikasian aplikasi	Kode unik

Terminal pengenal mencakup metode pengangkutan dan pembawa. Pembawa yang ada umumnya mencakup kode batang, kode QR, tag RFID, dan sensor [9]. Metode pengangkutan umumnya mencakup pelat nama, tag, label, laser etching, dan cap mekanis. Industri otomotif saat ini lebih menyukai penandaan langsung pengenal. Jika penandaan langsung tidak sesuai, label dan daftar digunakan untuk kasus ini. Pengemasan eksternal digunakan untuk membuat pengenal ketika penandaan langsung dan label serta daftar tidak sesuai. Berkat pengembangan kode QR, terminal pengenal Internet Industri otomotif saat ini mengadopsi pengukiran dengan kode QR dan kode batang. Laser etching umumnya digunakan pada komponen utama untuk memastikan pengenal dapat diidentifikasi dalam jangka panjang. Selain itu, dengan pengembangan Internet Industri, RFID dinilai penting bagi industri otomotif.

Manajemen Pengenal

Pengenal adalah informasi parameter utama yang diungkapkan oleh pengenal. Ada sejumlah besar OEM, produsen komponen, distributor, dan penyedia layanan di Internet Industri otomotif, semuanya memiliki pengenal sendiri berdasarkan standar data mereka. Di satu sisi, pemilik setiap pengenal perlu mendaftarkan informasi kunci dengan MIN-II berdasarkan permintaan pencarian oleh orang lain dan oleh karena itu sistem perlu melakukan operasi pendaftaran, peninjauan, dan pembaruan yang sesuai pada pengenal. Di sisi lain, karena keragaman lingkungan data pengenal, data pengenal perlu mengintegrasikan data sistem aplikasi Internet Industri yang heterogen.

Untuk memperkuat interoperabilitas sumber daya Internet Industri dalam industri otomotif dan memfasilitasi pencarian dan penemuan sumber daya Internet Industri antara berbagai sistem Internet Industri, perlu untuk memelihara dan memetakan data pengenal

dalam berbagai jenis. Sistem resolusi pengenal Internet Industri merupakan infrastruktur jaringan penting dari Internet Industri otomotif. Data pengenal merupakan informasi penting yang dihasilkan selama produksi dan operasi suatu perusahaan, yang harus dilindungi karena dapat melibatkan rahasia dagang perusahaan dan juga merupakan aset inti perusahaan. Selama pembangunan MIN-II, perlu untuk menampilkan informasi yang berbeda sesuai dengan tingkat pengguna dan waktu, dan mendukung fungsi saluran aman untuk mencegah informasi sensitif dicegat pada saat yang bersamaan.

Pembangunan MIN-II dalam industri otomotif dipisahkan menjadi tiga langkah pada tingkat keamanan:

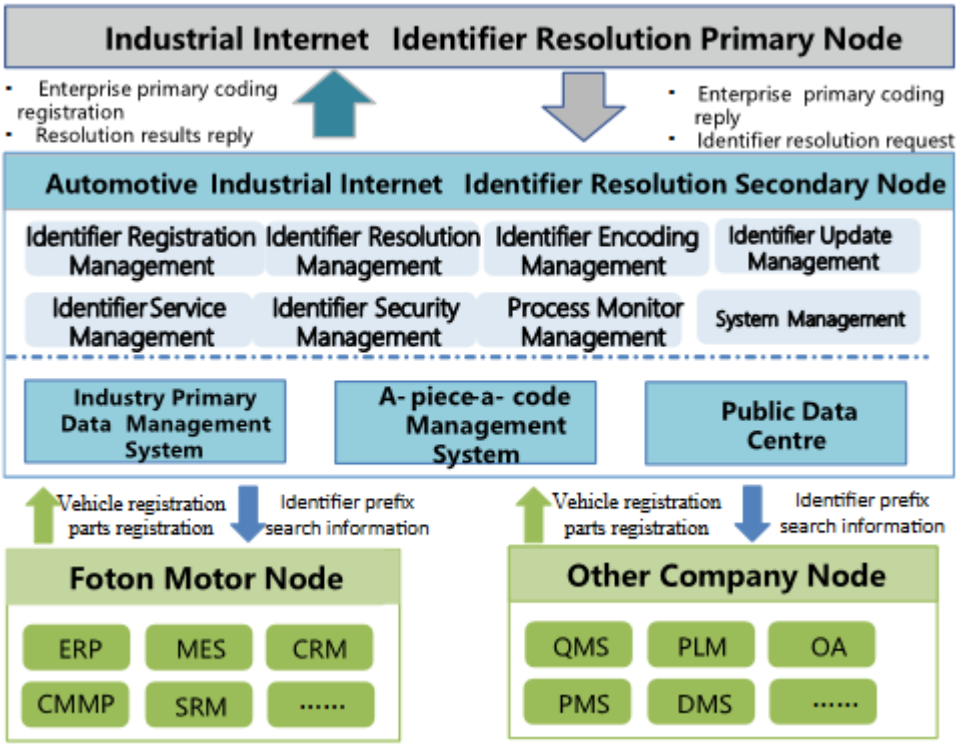
(1) Keamanan tingkat perangkat lunak. Rasionalitas arsitektur perangkat lunak dan kelengkapan protokol yang relevan merupakan masalah yang perlu dipertimbangkan secara menyeluruh terkait keamanan pengenal.
(2) Keamanan tingkat data, termasuk jaminan keamanan untuk pertukaran dan penyimpanan data besar-besaran, pengelolaan optimal agregasi data heterogen multisumber, dan tindakan pencegahan terhadap penggunaan data ilegal.
(3) Keamanan operasional. Hal ini akan menghindari penyalahgunaan pendaftaran dan pendaftaran ilegal, mengalokasikan sumber daya pengenal yang wajar, dan meningkatkan keamanan lingkungan untuk pengelolaan pengenal.

Node sekunder resolusi pengenal untuk Internet Industri otomotif adalah sistem inti yang mengimplementasikan pendaftaran, kueri, dan analisis pengenal oleh berbagai subjek aplikasi dalam industri otomotif. MIN membangun node sekunder untuk resolusi Internet Industri otomotif. Node ini digunakan untuk mendukung pendaftaran dan analisis sumber daya fisik seperti kendaraan, peralatan, dan suku cadang dalam industri otomotif, serta sumber daya virtual seperti algoritme dan proses. Sebagai platform layanan publik industri, simpul sekunder dalam MIN-II dihubungkan ke simpul primer nasional, yang menanyakan lokasi jaringan resolusi pengenal Internet Industri dari simpul sekunder dan dihubungkan ke data lokal atau sistem resolusi lokal setiap perusahaan pada rantai nilai industri otomotif, yang menanyakan lokasi penyimpanan data perusahaan dari simpul sekunder.

Karena kompleksitas dan keragaman lingkungan Internet Industri, konstruksi simpul sekunder untuk resolusi pengenal akan menghadapi sejumlah besar host yang berbeda, tempat yang berbeda, dan sistem yang heterogen. Analisis sederhana lokasi penyimpanan tidak dapat lagi memenuhi persyaratan industri otomotif yang semakin canggih untuk data Internet Industri. Oleh karena itu, saat membangun simpul sekunder untuk resolusi pengenal Internet Industri, simpul sekunder resolusi pengenal dibangun berdasarkan sistem data induk industri, sistem a-piece-a-code, dan pusat data publik, seperti yang ditunjukkan pada Gambar 5.33.

Sistem data induk industri, sebagai sistem manajemen standar data, akan menyatukan klasifikasi dan deskripsi kendaraan, suku cadang, dan aksesori dalam industri otomotif, atau memecahkan masalah "hal yang sama dengan nama yang berbeda" antara berbagai perusahaan melalui pemetaan data latar belakang. Sistem a-piece-a-code digunakan untuk manajemen kode unik dari satu bagian atau satu kelompok dalam industri, menyediakan

seluruh jaringan dengan kode unik untuk seluruh kendaraan dan suku cadang mobil. Pusat data publik berfungsi sebagai pusat penyimpanan data bersama yang menyimpan data pengenal yang terdaftar ke simpul sekunder dari simpul perusahaan sehingga mendukung asosiasi dan pemetaan pengenal. Simpul sekunder resolusi pengenal yang dibangun atas dasar ini menganalisis lokasi penyimpanan jaringan di satu sisi dan menganalisis informasi terkait dari objek identitas yang sama di sisi lain. Ini memberikan dukungan data untuk pengembangan bentuk bisnis baru dan ekologi baru dalam industri otomotif.



Gambar 5.33 Diagram integrasi simpul sekunder resolusi pengenal dalam internet industri otomotif

Standar MIN-II

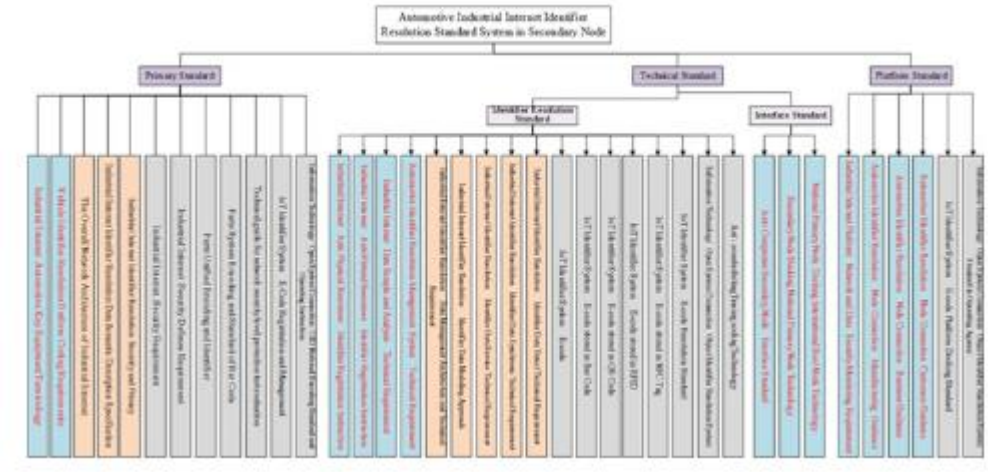
Saat ini, sistem standar pengenal utama meliputi Handle, OID (Pengidentifikasi Objek), Ecode (Kode Entitas untuk IoT), Epc, UCode, dan sebagainya, yang telah diusulkan oleh berbagai organisasi. Sistem ini digunakan untuk menandai secara unik dan menyediakan kueri informasi untuk objek item dan objek digital pada awalnya dan kini telah berkembang menjadi arsitektur informasi tingkat rendah, mirip dengan DNS di Internet.

Sistem standar resolusi pengenal Internet Industri otomotif disiapkan dengan pertimbangan penuh terhadap kebutuhan industri dan memanfaatkan serta menyerap hasil penelitian dari industri lain. Standar teknologi menjadi garis utama dan pengenal serta resolusi menjadi inti. Saat ini, sistem ini awalnya terdiri dari tiga bagian: standar dasar, standar teknis, dan struktur standar platform, seperti yang ditunjukkan pada Gambar 5.34.

(1) Standar Primer

Standar dasar terutama mendefinisikan definisi istilah untuk lini produksi mobil, peralatan listrik dan keselamatan dan mendefinisikan prinsip pengkodean, struktur data dan

metode representasi simbolik untuk kendaraan, suku cadang mobil dan aksesori. Standar ini mencapai integrasi data di seluruh perusahaan dan wilayah dan menyediakan aturan pengkodean standar untuk OEM, produsen komponen dan distributor.



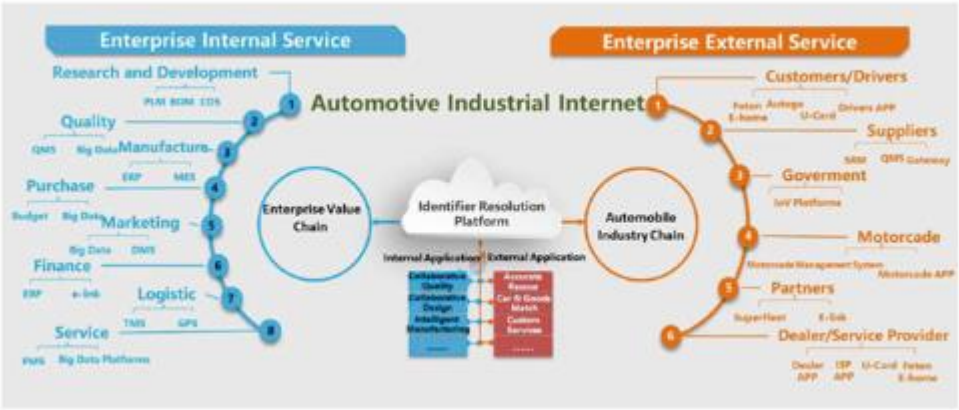
Gambar 5.34 Sistem standar resolusi pengidentifikasi internet industri otomotif

(2) Standar Teknis

Standar teknis terutama mencakup tiga bagian. Yang pertama adalah untuk menstandardisasi prinsip registrasi dan resolusi pengidentifikasi dalam sumber daya fisik termasuk kendaraan lengkap, peralatan, suku cadang dan komponen dan dalam sumber daya virtual termasuk algoritma dan proses. Kedua, menstandardisasi persyaratan teknis sumber data pengidentifikasi Internet Industri otomotif, metode analitis dan spesifikasi penyimpanan. Ketiga, standarisasi persyaratan teknis antarmuka termasuk metode transmisi data dan metode antarmuka untuk memastikan kecerdasan, kelayakan, kemajuan, dan keandalan interkoneksi multi-platform setelah platform terhubung.

(3) Standar Platform

Standar platform terutama menetapkan teknis untuk pemantauan keamanan data jaringan dan perlindungan privasi Internet Industri dalam industri otomotif. Standar ini juga menstandardisasi pedoman operasi untuk OEM, produsen komponen, dealer, dan peserta lain dalam konstruksi resolusi pengenal di Internet Industri.



Eksplorasi Aplikasi Pengenal

Pembangunan MIN-II dalam industri otomotif merupakan dasar penting untuk penerapan Internet Industri otomotif. Di satu sisi, dengan menstandardisasi standar resolusi pengenal untuk Internet Industri otomotif, basis data pengenal untuk produk, suku cadang, dan aksesori dalam industri otomotif dibangun dan digunakan sebagai pintu masuk ke kueri pengenal Internet industri otomotif. Di sisi lain, melalui penerapan Internet Industri, teknologi baru TI, dan penerapan peralatan utama, pintu masuk ke manajemen sumber daya Internet Industri industri otomotif dibangun, produsen dan pemasok mobil nasional, perusahaan, penyedia layanan, dealer, pelanggan, dan lembaga industri lainnya dibangun dalam platform layanan data besar industri untuk industri otomotif berdasarkan hal ini (Gambar 5.35).

Kolaborasi Rantai Pasokan Berdasarkan Pengenal

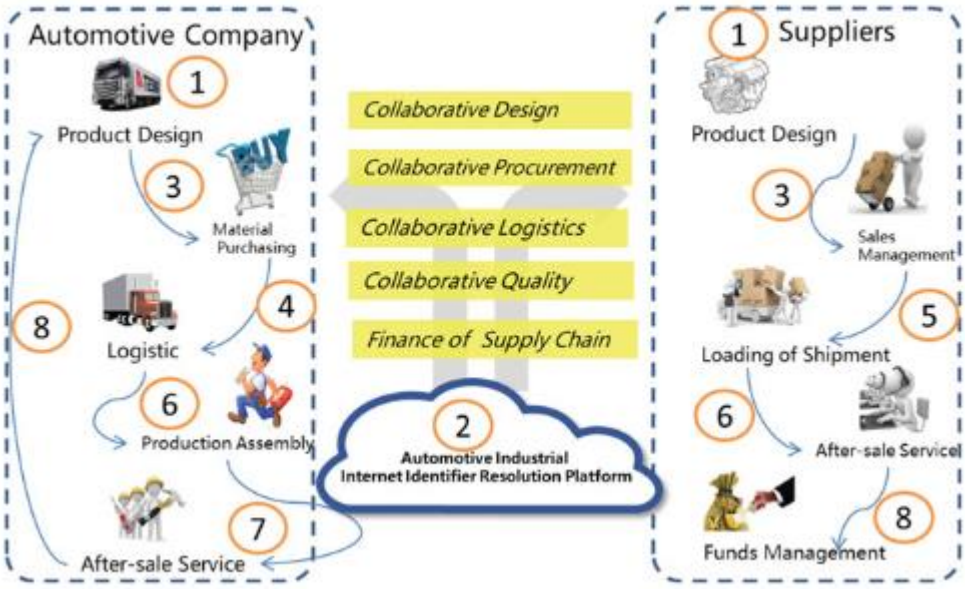
Manajemen kolaboratif rantai pasokan bukanlah manajemen sistem informasi tertentu, tetapi ekosistem yang saling terhubung yang mencakup seluruh rantai nilai perencanaan, pengadaan, pasokan, logistik, pergudangan, kualitas, transportasi, penjualan, dan layanan. Dengan bantuan platform resolusi pengenal untuk Internet Industri otomotif, seluruh kendaraan, suku cadang, pemasok, peralatan, dan perkakas diberi kode lokasi penyimpanan jaringan, yang dikombinasikan dengan kode unik mereka sendiri dalam sistem masing-masing untuk memastikan bahwa setiap data yang saling terhubung yang berpartisipasi memiliki informasi pengenal unik di seluruh jaringan dengan lingkungan dasar yang baik untuk kolaborasi rantai pasokan.

Dalam hal implementasi, dengan mengambil kebutuhan pelanggan sebagai titik awal dan mendasarkan pada layanan resolusi pengenal terpadu, manajemen rantai pasokan tidak hanya akan menghubungkan objek fisik seperti kendaraan lengkap, suku cadang produksi, dan suku cadang dalam rantai pasokan, tetapi juga memeriksa titik lemah manajemen rantai pasokan perusahaan. Ia juga merencanakan dan secara bertahap membangun sistem manajemen kolaboratif rantai pasokan yang kolaboratif dan efisien dengan merumuskan manajemen rantai pasokan yang kolaboratif.

Dalam industri otomotif dan skenario aplikasi kolaboratif rantai pasokan, proses aplikasi spesifik penggunaan resolusi pengenal ditunjukkan pada Gambar 5.36:

- **Langkah 1**: Mengodekan pengenal sumber daya kolaboratif;
- **Langkah 2**: Mendaftarkan sumber daya di atas dalam MIN-II;
- **Langkah 3**: Dalam fase desain produk, departemen R&D mendesain produk berdasarkan pengenal yang sama;
- **Langkah 4**: Persyaratan desain departemen pengadaan untuk R&D dikomunikasikan kepada pemasok tepat waktu;
- **Langkah 5**: Pemasok memperoleh persyaratan R&D berdasarkan pengenal terpadu dan segera memberikan umpan balik persyaratan produksi;
- **Langkah 6**: Perusahaan logistik memberikan umpan balik tepat waktu status logistik produk berdasarkan pengenal terpadu;
- **Langkah 7**: Berdasarkan pengenal terpadu, departemen kualitas memberikan umpan balik informasi pemeriksaan kualitas kepada departemen R&D dan pemasok;

Dibandingkan dengan manajemen rantai pasokan tradisional, manajemen rantai pasokan berdasarkan resolusi pengenal telah ditingkatkan dalam lima area berikut:



Gambar 5.36 Kolaborasi rantai pasokan berdasarkan resolusi pengidentifikasi

(1) Desain Kolaboratif, Memperpendek Siklus Pengembangan

Melalui teknologi resolusi pengenal, sumber daya R&D sepenuhnya dibagi dalam bidang Internet Industri dan menjadi mungkin bagi pemasok dan dealer untuk berpartisipasi dalam desain dan evaluasi produk kendaraan, membentuk situasi pengembangan yang sinkron dan kolaboratif, serta memperpendek siklus pengembangan secara signifikan.

(2) Pengadaan Kolaboratif untuk Mengurangi Risiko Kekurangan Material

Melalui teknologi resolusi pengenal Internet Industri, OEM dan pemasok dapat memperoleh informasi dinamis waktu nyata tentang pesanan pelanggan, tingkat inventaris, dan pesanan pembelian, yang akan mengurangi risiko kekurangan material.

(3) Kolaborasi Logistik untuk Mengurangi Biaya Logistik

Dengan Pendaftaran informasi kendaraan logistik dan informasi kargo ke MIN-II, OEM dan pemasok dapat memperoleh informasi logistik tepat waktu, serta meningkatkan efisiensi kendaraan dengan mengumpulkan arus kargo dan mengurangi biaya transportasi.

(4) Kolaborasi Kualitas untuk Meningkatkan Kemampuan Pemasok

Selama penggunaan kendaraan, penyedia layanan dan pelanggan dapat mendaftarkan masalah kualitas yang terkumpul ke MIN-II dan pemasok tidak hanya dapat memperoleh umpan balik kualitas secara tepat waktu, tetapi juga mengoptimalkan desain dan meningkatkan kualitas suku cadang pemasok.

(5) Keuangan Rantai Pasokan

Dengan menggabungkan dengan Internet of Vehicle, teknologi resolusi pengenal dapat memperoleh lokasi dan informasi perawatan kendaraan secara real-time, memberikan jaminan keuangan bagi mitra, dan memperluas bisnis mitra asisten.

Ketertelusuran Kualitas Berdasarkan Resolusi Pengenal

Dengan bantuan standar resolusi pengenal untuk Internet Industri otomotif dan platform aplikasinya, standar pengkodean ketertelusuran kualitas yang mematuhi standar industri otomotif ditetapkan. Ini membuat aturan pengkodean untuk bahan mentah, produk setengah jadi, dan produk jadi dapat dilacak. Di satu sisi, untuk meningkatkan keterbacaan kode dan mengurangi tekanan biaya keterlacakan komponen pada rantai pasokan industri otomotif, perusahaan mobil menggunakan aturan kode keterlacakan yang sama untuk menerapkan manajemen keterlacakan kualitas. Sistem analisis mengumpulkan data kualitas untuk seluruh siklus hidup komponen inti mulai dari manufaktur, transportasi, pemeriksaan kualitas, dan penyimpanan, perakitan hingga kendaraan lengkap, penjualan terminal, layanan pemeliharaan, penggantian, penghentian produksi, dan daur ulang, sehingga kualitas produk perusahaan dioptimalkan dan ditingkatkan.

Gambar. 5.37 Penelusuran kualitas berdasarkan resolusi pengenal

Dari perspektif implementasi, ketertelusuran kualitas komponen utama dalam industri otomotif perlu mencatat secara akurat korespondensi antara kendaraan dan komponen selama proses perakitan kendaraan. Informasi terkait harus dicatat secara akurat, seperti informasi dealer kendaraan, pelanggan selama proses penjualan kendaraan, catatan penggantian suku cadang dan komponen dalam layanan purnajual. Dengan cara ini, jika terjadi kesalahan, produsen kendaraan dapat dengan cepat menentukan kendaraan mana yang memasang suku cadang bermasalah, ke area mana kendaraan ini dikirim, dan ke pengguna akhir mana kendaraan ini dijual. Jika pengguna akhir ini perlu diganti dan diperbaiki, lokasi gerai layanan terdekat harus dipertimbangkan. Dalam skenario aplikasi penelusuran kualitas komponen kunci otomotif, proses aplikasi spesifik penggunaan resolusi pengenal ditunjukkan pada Gambar 5.37 berikut:

(1) Langkah 1: Pemasok mengodekan komponen kunci mobil dengan kode QR, kode batang, dan RFID, lalu mendaftarkannya di MIN-II.
(2) Langkah 2: Berdasarkan pengenal pengodean, OEM mencatat informasi produk seperti penyimpanan, pemeriksaan kualitas, pergudangan, dan perakitan, lalu mendaftarkan informasi terkait di MIN-II.
(3) Langkah 3: OEM menandai seluruh kendaraan dengan pengenal, lalu mencatat korespondensi antara kendaraan dan komponen, lalu akhirnya mendaftarkan pengenal kendaraan ke MIN-II.
(4) Langkah 4: Saat kendaraan dijual ke pelanggan akhir, petugas layanan dealer mengikat informasi pelanggan seperti nama, usia, pekerjaan, tujuan, dll. dengan informasi kendaraan dan mendaftarkan informasi penjualan ke MIN-II.
(5) Langkah 5: Penyedia layanan mencatat informasi penggantian suku cadang lama dan baru dengan memindai kode QR suku cadang selama tautan pemeliharaan dan memperoleh produksi, logistik, pemeriksaan kualitas, dan informasi lain dari suku cadang tersebut.

Produksi Cerdas Berdasarkan Resolusi Pengenal

Dalam keseluruhan proses produksi kendaraan, kebutuhan pelanggan, sumber daya produk, material produksi, transportasi logistik, dan informasi lain yang terkait dengan produksi didaftarkan dalam ekologi Internet Industri industri otomotif melalui sistem resolusi pengenal, sehingga produksi cerdas dapat menjadi fondasinya. Prosesnya terutama mencakup langkah-langkah berikut (Gambar 5.38):

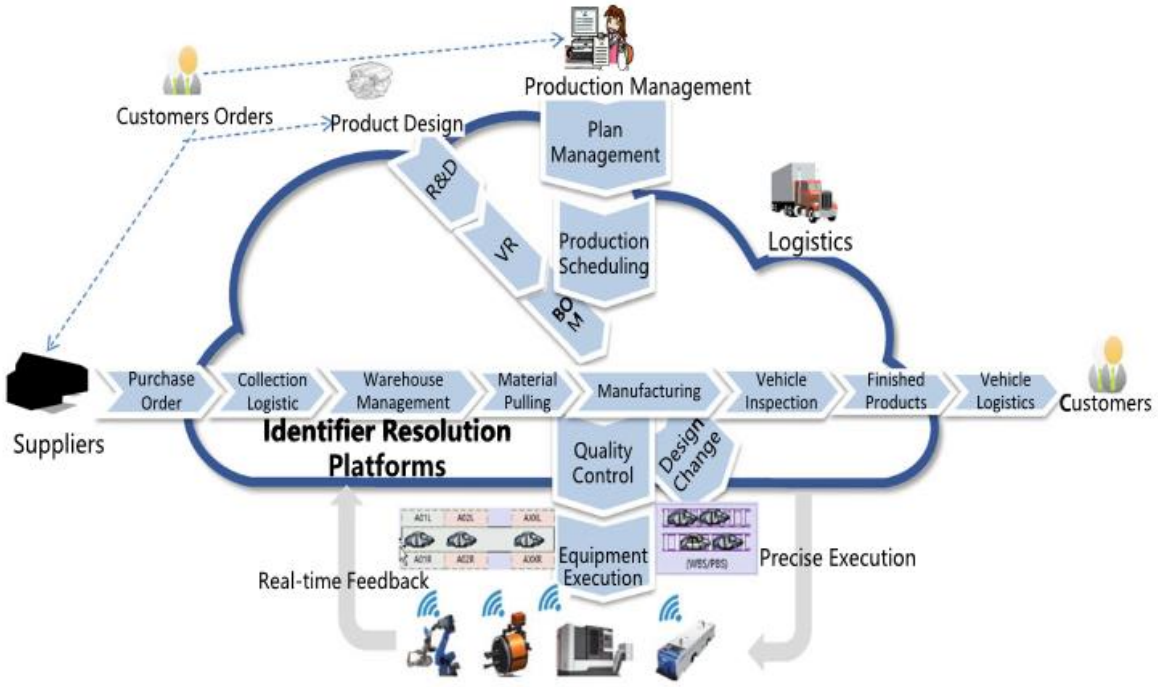
(1) Langkah 1: Pendaftaran pesanan pengenal pelanggan. Pelanggan menyelesaikan kustomisasi produk di DMS (Sistem Manajemen Dealer) dan mendapatkan nomor pesanan, kemudian sistem secara otomatis mendaftarkan informasi pesanan ke MIN-II.
(2) Langkah 2: Departemen desain produk memperoleh informasi tentang model dan konfigurasi spesifik yang terlibat dalam pesanan sesuai dengan pengenal pesanan dan mendaftarkan BOM produk yang dirancang, suku cadang, dan pengenal lainnya ke sistem resolusi pengenal.
(3) Langkah 3: Departemen pembelian dan manajemen produksi merumuskan permintaan pembelian dan perintah produksi sesuai dengan permintaan pembelian dan rencana produksi dan mendaftarkan informasi perintah pembelian dan rencana produksi ke MIN-II.
(4) Langkah 4: Pemasok memperoleh informasi spesifik material dan tanggal permintaan yang diperlukan oleh perintah pembelian melalui MIN-II dan memulai perintah produksi.
(5) Langkah 5: Perusahaan logistik memperoleh informasi seperti tanggal pengiriman spesifik dan jumlah suku cadang sesuai dengan pengenal perintah produksi dan pengenal perintah pembelian dan mengangkut material ke gudang tempat produksi berada.

(6) Langkah 6: Menurut pengenal pesanan, pengenal material dan pengenal peralatan, departemen produksi memperoleh informasi sumber daya yang diperlukan oleh pelanggan dan produksi dan menerjemahkannya ke dalam instruksi kerja untuk memandu peralatan agar dapat bekerja secara akurat. Pada saat yang sama, peralatan memberikan umpan balik hasil pemrosesan tepat waktu dan hasil eksekusi didaftarkan ke MIN-II.

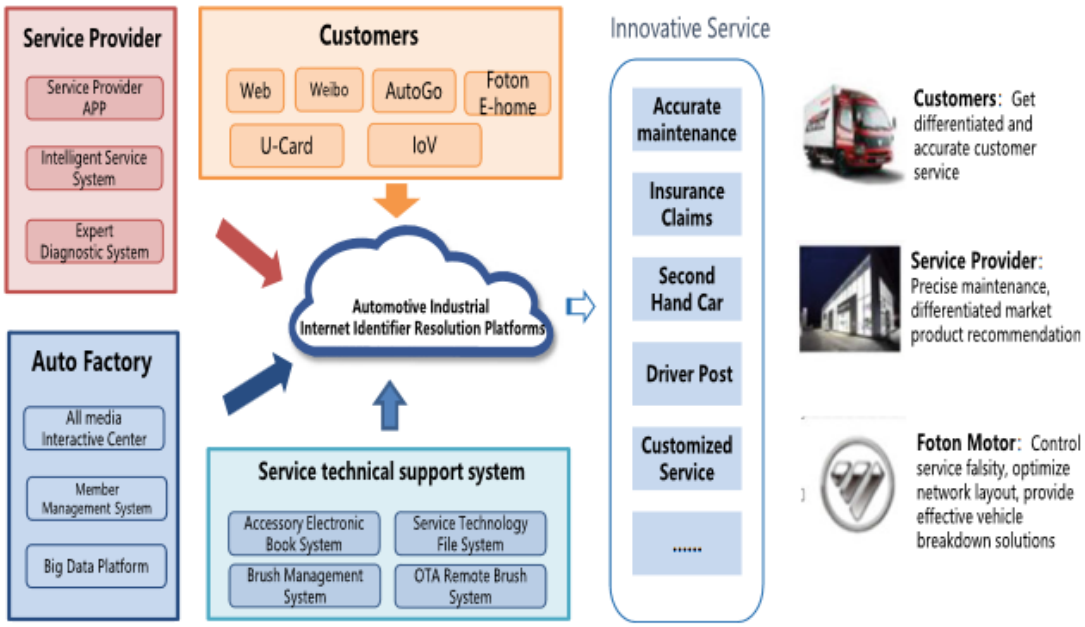
(7) Langkah 7: Melalui sistem resolusi identitas, pelanggan dapat memperoleh proses produksi spesifik dari produk yang disesuaikan tepat waktu.

Inovasi Layanan Berdasarkan Resolusi Pengenal

Dengan menciptakan sistem layanan pelanggan yang cerdas dan berbeda, sistem layanan cerdas berdasarkan MIN-II dibangun. Sistem ini tidak hanya mempromosikan interkoneksi informasi antara terminal produk dan klien, tetapi juga meningkatkan layanan purnajual tradisional menjadi layanan aktif, layanan daring jarak jauh, dan transformasi layanan cerdas.



Gambar 5.38 Manufaktur cerdas berdasarkan resolusi pengenal



Gambar 5.39 Inovasi layanan berdasarkan resolusi pengenal

Dalam layanan purnajual kendaraan tradisional, data status pengoperasian kendaraan tidak dapat langsung diketahui. Ketika kendaraan mengalami beberapa masalah, seperti berjalan lamban atau bahkan mogok saat menunggu pertolongan, teknisi servis kesulitan mendapatkan informasi kesalahan pada saat pertama dan selalu hanya mendiagnosis dan merawat di tempat. Situasi ini membuat layanan kendaraan menjadi pasif. Berdasarkan platform big data Internet Industri, data produksi kendaraan, data produk, dan data pelanggan didaftarkan ke MIN-II, yang mengetahui status pengoperasian kendaraan setiap saat, memprediksi kemungkinan kesalahan kendaraan, serta mendeteksi bagian kendaraan yang rusak secara tepat waktu bagi pelanggan. Pengingat kesalahan, pengingat perawatan, dan panduan perilaku berkendara disediakan berdasarkan teknologi di atas, seperti yang ditunjukkan pada Gambar 5.39.

Pengingat Kesalahan: Melalui MIN-II, data produksi dan perakitan kendaraan, data penjualan pelanggan, dan data waktu nyata selama pengoperasian produk dihubungkan untuk membangun model analisis big data, sehingga indikator kinerja dan tingkat kerusakan komponen utama kendaraan dipantau secara efektif. Selain itu, SMS, APP, dan mobil digunakan untuk mengirim pengingat pesan secara otomatis dan berkomunikasi dengan pelanggan melalui telepon tepat waktu sesuai dengan tingkat kerusakan. Kita harus bertanya kepadanya apakah ada masalah dengan kendaraan melalui telepon. Jika pelanggan mengajukan masalah, staf terkait segera dikirim untuk menyelesaikan masalah, guna menghindari meluasnya kerusakan yang membuat pengoperasian kendaraan lebih ekonomis dan aman.

Pengingat Perawatan: Melalui kombinasi dengan Internet of Vehicles, informasi jarak tempuh kendaraan dan kondisi pengoperasian kendaraan didaftarkan di MIN-II. Saat waktu perawatan atau jarak tempuh semakin dekat, undangan perawatan akan dikirim melalui APP

dan SMS guna menghindari pengaruh terhadap masa pakai kendaraan akibat perawatan yang tidak tepat. Hal ini tidak hanya akan memungkinkan pelanggan menghemat biaya perawatan, meningkatkan keselamatan pengemudi, tetapi juga mendatangkan keuntungan bagi stasiun layanan. Dan itu akan mengurangi tingkat kegagalan dan meningkatkan reputasi merek perusahaan pada saat yang sama. Panduan Perilaku Mengemudi: Dalam pengoperasian kendaraan, dengan memantau gigi kendaraan, kecepatan, konsumsi bahan bakar, dan data pengoperasian lainnya, kami menganalisis perilaku mengemudi pelanggan melalui analisis dan pemodelan back-end big data, untuk memberikan panduan perilaku mengemudi kepada pelanggan. Kebiasaan mengemudi yang baik sampai batas tertentu akan memperpanjang masa pakai kendaraan dan mengurangi tingkat kegagalan kendaraan.

5.4 JARINGAN PUBLIK MULTINASIONAL DENGAN PEMERINTAHAN BERSAMA DAN OTONOMI

Ruang siber telah menjadi perbatasan kelima suatu negara, di samping empat perbatasan darat, laut, udara, dan angkasa. Lebih dari itu, keamanan ruang siber memengaruhi dan menentukan keamanan wilayah lain.

Setiap negara harus mengembangkan jaringan kedaulatannya sendiri, yang pengenalnya didefinisikan secara independen untuk memastikan bahwa dunia maya sepenuhnya otonom, dapat dikelola, dan dikendalikan. Pengembangan jaringan kedaulatan global dapat dimulai dengan partisipasi beberapa negara untuk membentuk jaringan publik multinasional yang saling terhubung dengan pemerintahan bersama dan otonomi kedaulatan. Di bagian ini, kami akan memperkenalkan arsitektur, komunikasi, dan contoh jaringan publik multinasional yang saling terhubung.

5.4.1 Topologi Jaringan

Jaringan publik multinasional yang saling terhubung menghubungkan beberapa subjaringan kedaulatan negara untuk mengembangkan dunia maya yang memerintah bersama. Topologi jaringan publik multinasional yang saling terhubung ditunjukkan pada Gambar 5.40. Seperti yang ditunjukkan pada Gambar 5.40, jaringan kedaulatan antara negara-negara tetangga terhubung langsung melalui serat optik, bukan melalui Internet IP. Informasi antara jaringan kedaulatan jarak jauh ditransmisikan melalui Internet atau jaringan kedaulatan lainnya. Pengenal jaringan kedaulatan di berbagai negara ditetapkan secara independen.

Untuk konten yang dapat diakses oleh jaringan kedaulatan lain, pengenal identitasnya perlu dipublikasikan melalui protokol perutean dinamis, sehingga semua EMIR dalam jaringan kedaulatan jaringan publik multinasional yang saling terhubung mengetahui jalur penerusan untuk mengakses konten tersebut. Ketika pengguna jaringan kedaulatan lain ingin mengakses konten tersebut, mereka pertama-tama perlu mengajukan sertifikat digital ke jaringan kedaulatan target, kemudian mengirimkan permintaan tersebut ke EMIR jaringan kedaulatan mereka. Akhirnya, pengenal tersebut saling diterjemahkan di EMIR dan diteruskan. Untuk konten yang dilarang negara untuk diakses oleh pengguna jaringan kedaulatan lain, EMIR dalam jaringan kedaulatan secara langsung menolak permintaan akses tersebut. Selain itu,

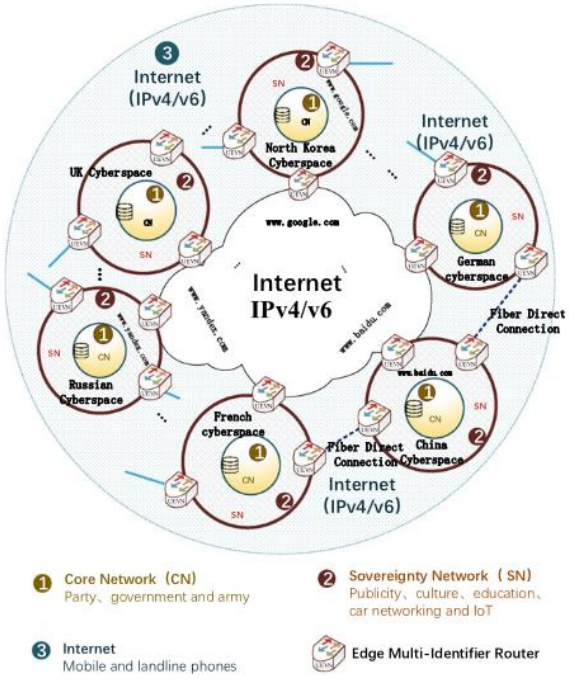
ruang lingkup perilaku sah pengguna dalam jaringan kedaulatan juga dibatasi melalui sertifikat, sehingga dapat memastikan pengelolaan dan pengendalian jaringan kedaulatan. Penyedia konten juga dapat menduplikasi sebagian atau seluruh konten mereka di Internet demi kenyamanan pengguna jaringan kedaulatan di negara lain.

5.4.2 Komunikasi Jaringan

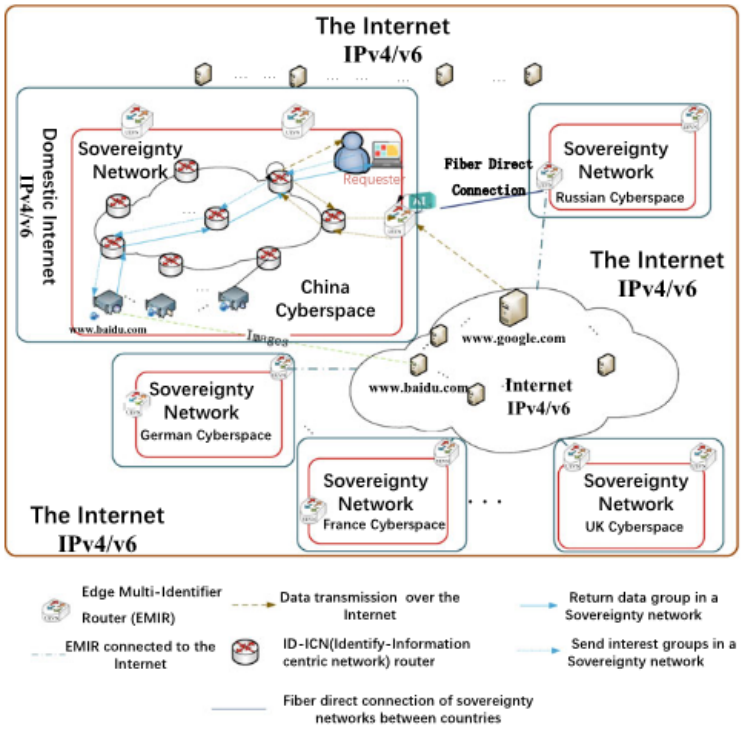
Komunikasi jaringan publik multinasional yang saling terhubung, terutama mencakup tiga jenis: (1) pengguna jaringan kedaulatan memperoleh konten di Internet, (2) pengguna jaringan kedaulatan memperoleh konten di jaringan kedaulatan lainnya, (3) transmisi titik-ke-titik seperti E-mail.

1. Pengguna Jaringan Kedaulatan Memperoleh Konten di Internet

Pengguna jaringan kedaulatan bebas mengakses konten di Internet sesuai izin mereka. Konten di Internet mencakup dua jenis, konten pada jaringan IP yang ada dan konten yang disediakan oleh pengguna jaringan kedaulatan lainnya. Penyedia konten kedaulatan menerbitkan sumber daya konten di Internet, dan pengguna lain mengakses konten secara langsung alih-alih memperolehnya dari jaringan kedaulatan lain. Pendekatan ini mengurangi proses aplikasi sertifikat dan verifikasi sertifikat. Misalnya, Baidu, mesin pencari Tiongkok, menempatkan sebagian konten terbuka di Internet IP dengan cara pencerminan. Konten terbuka ini tidak memerlukan manajemen tingkat tinggi dan dapat diakses secara bebas oleh pengguna jaringan kedaulatan lainnya sesuai izin mereka. Verifikasi izin pengguna dilakukan oleh EMIR jaringan kedaulatan. Manajemen izin pengguna dirujuk pada Tabel 3.1. Gambar 5.41 menunjukkan proses yang menunjukkan bahwa pengguna jaringan kedaulatan memperoleh konten, termasuk proses memperoleh konten dari jaringan kedaulatan dan proses memperoleh konten dari Internet IP.



Gambar 5.40 Topologi jaringan publik multinasional yang saling terhubung



Gambar 5.41 Pengguna jaringan kedaulatan memperoleh konten dari jaringan kedaulatan dan internet IP

(1) Pengguna jaringan kedaulatan Tiongkok meminta konten tanpa mengetahui lokasi konten tersebut.

(2) Permintaan konten dikirim ke router ID-ICN. Jika permintaan konten mengenai cache router ID-ICN, konten yang sesuai akan dikembalikan ke pengguna. Jika tidak, konten akan dicari di jaringan kedaulatan atau di Internet IP.

(3) Jika konten berada di jaringan kedaulatan, permintaan akan diarahkan ke sumber konten, kemudian sumber akan mengembalikan konten tersebut.

(4) Jika konten berada di Internet IP, router ID-ICN mengirimkan permintaan konten ke EMIR jaringan kedaulatan.

(5) EMIR jaringan kedaulatan akan mengaudit izin pengguna. Jika permintaan sesuai dengan cakupan izin, konten akan diperoleh mengikuti mode transmisi data jaringan IP tradisional.

(6) EMIR jaringan kedaulatan mengaudit konten data yang dikembalikan dengan teknologi kecerdasan buatan untuk menyaring data yang berbahaya, kemudian mengembalikan data tersebut langsung ke peminta konten di sepanjang arah yang berlawanan dari jalur permintaan.

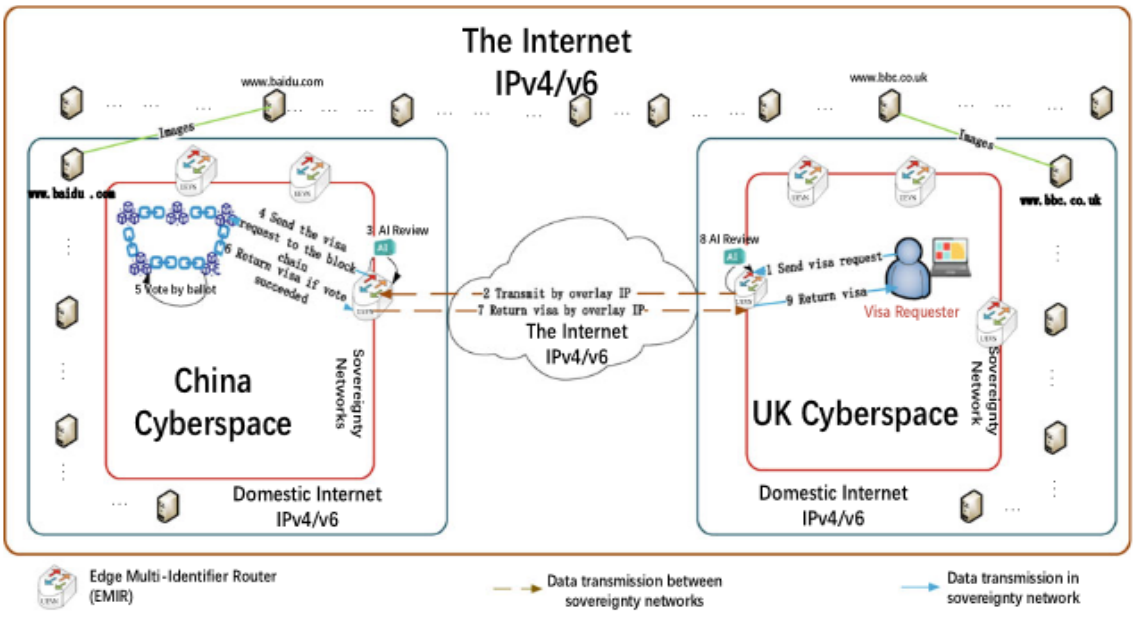
2. Pengguna Jaringan Kedaulatan Memperoleh Konten di Jaringan Kedaulatan Lain

Jika pengguna jaringan kedaulatan berencana untuk memperoleh konten di jaringan kedaulatan lain, pengguna perlu mengajukan permohonan sertifikat dari jaringan kedaulatan tempat konten tersebut berada. Proses pengajuan sertifikat ditunjukkan pada Gambar 5.42.

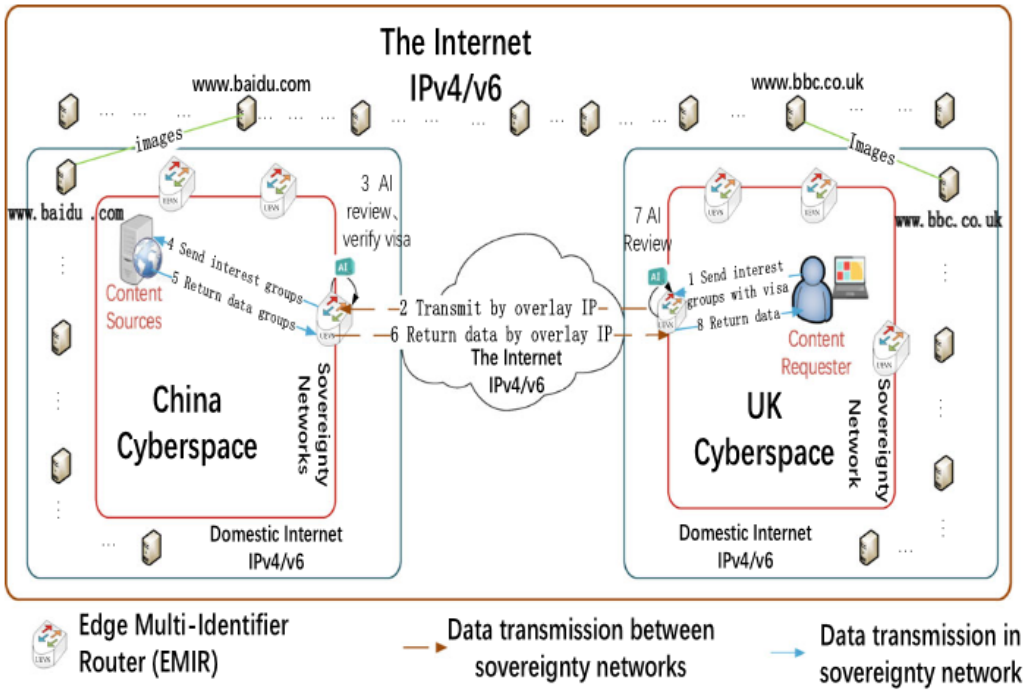
(1) Host pengguna meminta sertifikat dari EMIR jaringan kedaulatannya.
(2) EMIR jaringan kedaulatan domestik mengirimkan permintaan sertifikat ke negara tujuan melalui jaringan IP Overlay.
(3) EMIR negara tujuan mengaudit permintaan yang masuk.
(4) Permintaan sertifikat yang disetujui dikirim ke node blockchain untuk pemungutan suara.
(5) Agar permintaan mencapai konsensus, sertifikat dikembalikan ke peminta di sepanjang arah yang berlawanan dari jalur permintaan.

Pengguna yang telah memperoleh sertifikat diminta untuk memasukkan pesan sertifikat ke dalam tanda tangan paket minat saat pengguna mengakses konten pada jaringan kedaulatan terkait. Kemudian EMIR negara tujuan akan memverifikasi pesan sertifikat. Jika lolos verifikasi, pengguna dapat berhasil memperoleh konten, seperti yang ditunjukkan pada Gambar 5.43.

(1) Peminta konten mengirimkan paket minat yang membawa pesan sertifikat.
(2) EMIR jaringan kedaulatan domestik mengirimkan permintaan sertifikat ke negara tujuan melalui jaringan IP Overlay.
(3) EMIR negara tujuan memverifikasi sertifikat.
(4) Agar permintaan mencapai konsensus, EMIR jaringan kedaulatan mengirimkan paket minat ke sumber konten.
(5) Sumber konten mengembalikan konten ke peminta konten.



Gambar 5.42 Proses Pengajuan Sertifikat



Gambar 5.43 Akses konten transnasional dengan sertifikat

3. Transmisi Titik-ke-Titik Seperti Email

Bagi pengguna perorangan, mayoritas aplikasi web digunakan oleh skenario komunikasi jaringan peer-to-peer, seperti pesan instan, belanja daring, Email, dan sebagainya. Saat ini, sistem jaringan kedaulatan telah mewujudkan transmisi Email, dan proses transmisinya ditunjukkan pada Gambar 5.44.

(1) Pengirim konten mengirimkan data ke EMIR jaringan kedaulatan mengikuti mode transmisi data dalam jaringan kedaulatan.

(2) EMIR mengirimkan konten data ke server dalam jaringan IP melalui TCP/IP.

(3) Server ini mengirimkan konten ke EMIR di negara sasaran melalui TCP/IP.

(4) EMIR di negara sasaran memverifikasi konten, lalu mengirimkan konten yang disetujui ke penerima melalui mode transmisi data dalam jaringan kedaulatan. 4. Keamanan Jaringan Publik Multinasional yang Terhubung

Mekanisme keamanan jaringan publik multinasional yang saling terhubung ditunjukkan pada Gambar 5.45. Proses spesifik telah diperkenalkan pada Bagian 4.8.

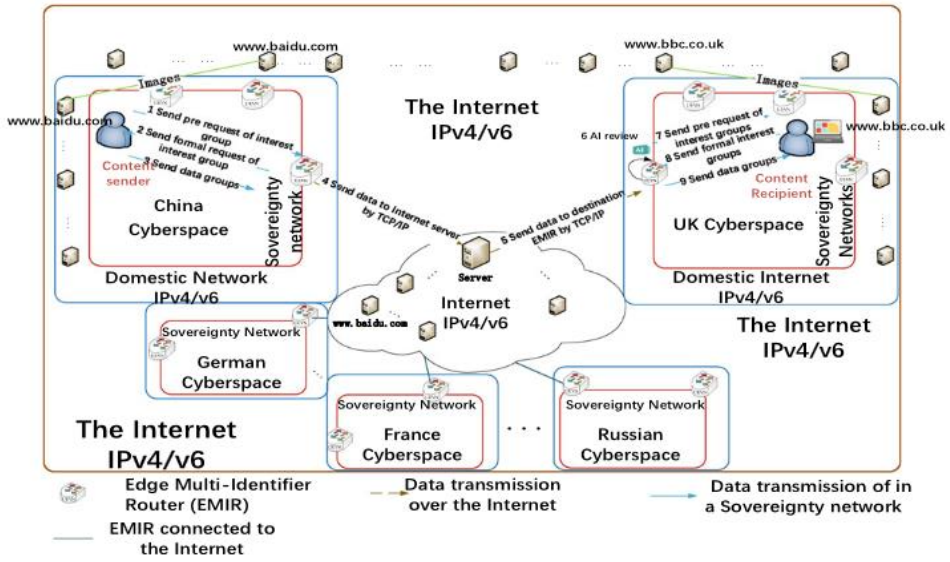
5.4.3 Contoh Jaringan Publik Multinasional yang Saling Terhubung

Tempat pengujian sistem mencakup Beijing, Guangzhou, Shenzhen, dan Hong Kong, Makau, sehingga Wilayah Teluk Raya Guangdong-Hong Kong-Makau tercakup sepenuhnya. Hong Kong mewakili wilayah berbahasa Inggris, sementara Makau mewakili wilayah berbahasa Portugis. Struktur topologi Wilayah Teluk Raya Guangdong-Hong Kong-Makau ditunjukkan pada Gambar 5.46.

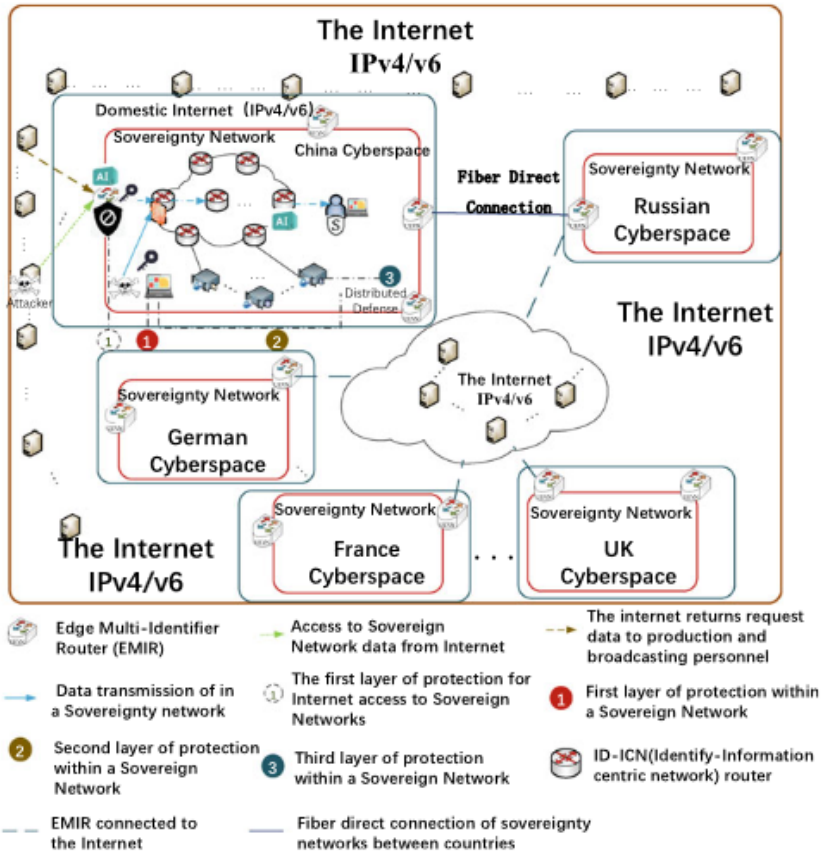
5.4.4 Perserikatan Bangsa-Bangsa di Dunia Maya

Berdasarkan pembangunan jaringan publik multinasional yang saling terhubung, jaringan kedaulatan akan menarik lebih banyak negara untuk berpartisipasi dan menarik

transisi lalu lintas dari jaringan IP ke MIN karena berbagai kelebihannya, seperti pengelolaan bersama multilateral, keamanan dan kredibilitas, otonomi yang fleksibel, kompatibilitas ke depan, ekstensibilitas ke belakang, dan sebagainya. Dengan pengembangan jaringan publik multinasional yang saling terhubung, Perserikatan Bangsa-Bangsa di dunia maya pada akhirnya akan dibangun.

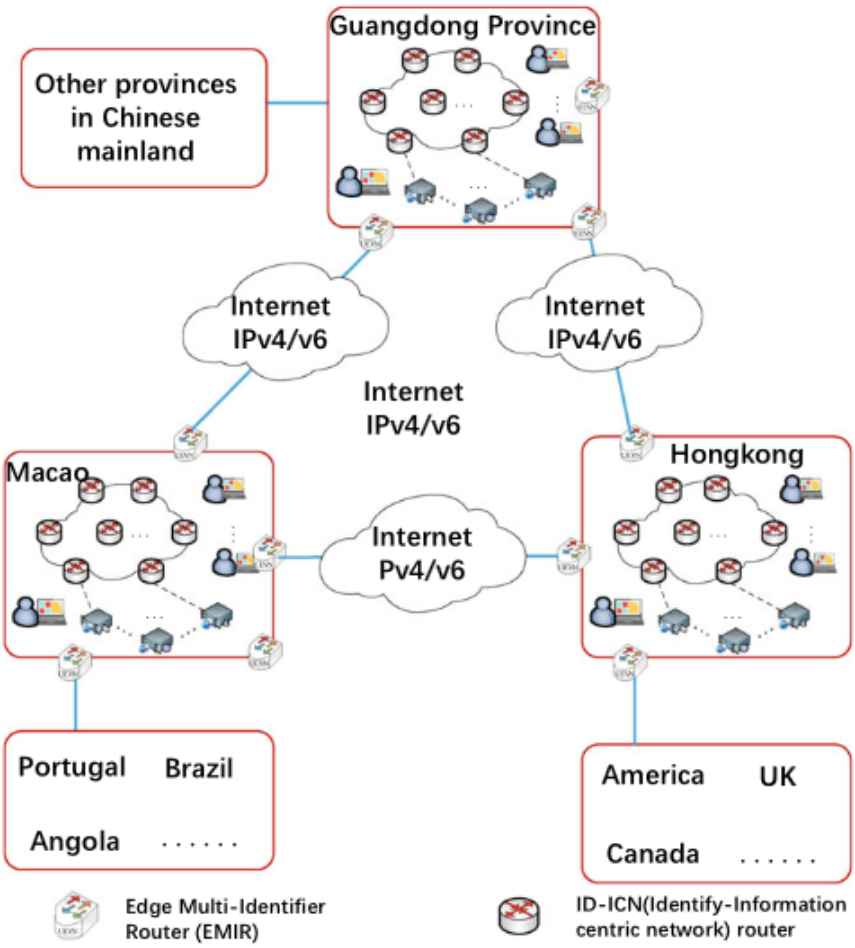


Gambar 5.44 Transmisi E-mail



Gambar 5.45 Mekanisme keamanan jaringan publik multinasional yang saling terhubung

Selama pengembangan Perserikatan Bangsa-Bangsa di Dunia Maya, kami mempercepat pembangunan infrastruktur Internet global untuk konektivitas yang lebih besar, membangun platform daring untuk pertukaran budaya dan pembelajaran bersama, mempromosikan pengembangan inovatif ekonomi digital untuk kesejahteraan bersama, menjaga keamanan siber untuk mempromosikan pembangunan yang tertib, membangun sistem tata kelola global di dunia maya untuk mempromosikan kesetaraan dan keadilan, serta memberikan jaminan yang paling efektif dan kuat untuk teknologi dan produk.



Gambar 5.46 Pengembangan jaringan kedaulatan di Wilayah Teluk Raya Guangdong-Hong Kong-Macao

5.5 DASAR DAN PERLUASAN JARINGAN MULTI-IDENTIFIER ANTARIKSA-TERESTRIAL

Dengan kemajuan teknis yang tiada henti dan permintaan layanan pengguna yang terus berkembang, sistem komunikasi darat telah berkembang pesat dalam beberapa tahun terakhir. Akan tetapi, kualitas layanannya dibatasi oleh morfologi permukaan dan bencana alam. Komunikasi satelit, yang tidak dibatasi oleh waktu, tempat, atau lingkungan, secara bertahap telah menarik perhatian masyarakat. Jaringan Multi-Identifier Antariksa-Terestrial (ST-MIN) dengan tiga lapisan heterogen termasuk jaringan satelit, jaringan berbasis antariksa, dan jaringan berbasis darat telah dibentuk untuk menyediakan layanan komunikasi dengan

kapasitas tinggi dan jangkauan yang lancar. Untuk meningkatkan kinerja jaringan kedaulatan, tujuan akhir jaringan kedaulatan adalah membangun ST-MIN.

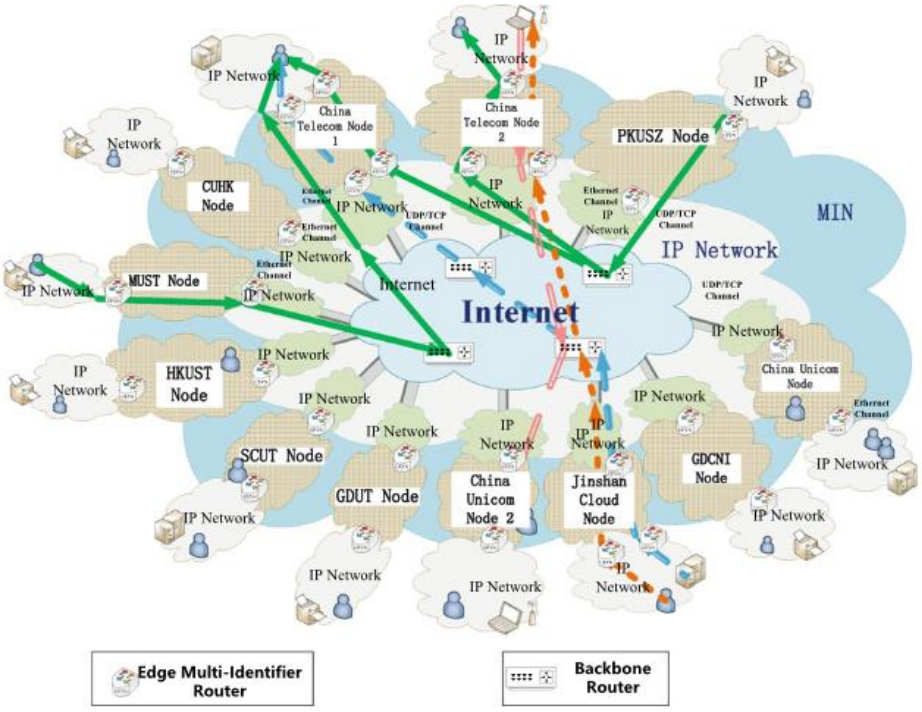
Berdasarkan arsitektur Jaringan Multi-Identifier (MIN) dan strategi perutean antariksa-terestrial yang diusulkan di Bagian. 4.8, kami selanjutnya menghadirkan banyak teknologi, seperti skema manajemen mobilitas ST-MIN, bisnis 5G, dan jaringan ruang angkasa-terestrial berbasis 6G. Lebih jauh, kami telah mengusulkan ST-MIN, serta arsitektur dan protokol yang sesuai. Kami tengah mengembangkan teknologi utama ST-MIN dan memverifikasi fungsinya melalui simulasi jaringan. Di masa mendatang, verifikasi prototipe ST-MIN akan dilakukan dalam skenario jaringan satelit nyata dan sistem demonstrasi aplikasi dikembangkan untuk industri tertentu.

5.5.1 Dasar Pekerjaan Saat Ini

Sejak Januari 2019, Sovereign Network telah diverifikasi, diuji, dan diterapkan dalam berbagai skenario bekerja sama dengan beberapa unit. Mulai Januari 2019, Universitas Peking, China Telecom, China Unicom, Jinshan Cloud, dan unit lainnya mulai menyebarkan dan memverifikasi prototipe jaringan MIN pada jaringan operator, yang ditunjukkan pada Gambar 5.47. Dari Januari 2019 hingga Maret 2019, kami telah menggunakan node berdasarkan konsensus rantai aliansi di Beijing, Guangzhou, Shenzhen, Hong Kong, Makau, dan tempat lain untuk melaksanakan transmisi data MIN. Hasilnya menunjukkan bahwa proyek tersebut layak, yang merupakan pekerjaan pertama di dunia sejauh yang kami ketahui.

Pada tanggal 22 Maret 2019, sekolah pascasarjana Shenzhen dari Universitas Peking dan Institut Komunikasi & Jaringan Guangdong bersama-sama meluncurkan perencanaan strategis, institut gabungan China Unicom, Institut Penelitian Inovasi dan Telekomunikasi Tiongkok, Universitas Teknologi Tiongkok Selatan, Universitas Teknologi Guangdong, Institut Teknologi Dongguan, Universitas Tiongkok Hong Kong, Universitas Sains dan Teknologi Makau (Shenzhen), Hong Kong dan Makau untuk meluncurkan teknologi jaringan kerja laboratorium multilateral bersama Big Bay, debut dunia prototipe ini untuk verifikasi.

Pada tanggal 22 Maret 2019, Laboratorium Teknologi Jaringan Bersama Wilayah Teluk Raya Guangdong yang disponsori bersama oleh Universitas Peking dan Institut Komunikasi & Jaringan Guangdong didirikan dan prototipe MIN pertama kali diverifikasi di seluruh dunia (Gambar. 5.48). Sponsor bersama meliputi China Unicom, China Telecom, Universitas Teknologi China Selatan, Universitas Teknologi Guangdong, Universitas Teknologi Dongguan, Universitas Teknologi Hong Kong, Universitas Sains dan Teknologi Makau, dan Universitas Hong Kong (Shenzhen). Dari April hingga Juli 2019, prototipe jaringan radio dan televisi kedaulatan berbasis MIN lulus uji dan penerimaan metrologi dan pusat uji radio dan TV, akademi perencanaan penyiaran. Kemudian prototipe jaringan radio dan televisi kedaulatan berbasis MIN diajukan untuk investasi modal oleh Administrasi Radio dan Televisi Nasional (Gambar 5.49).



Gambar 5.47 Topologi prototipe jaringan uji

Gambar 5.48 Laboratorium teknologi jaringan yang dikelola bersama oleh wilayah Teluk Guangdong

Pada bulan Maret 2020, dikombinasikan dengan situasi terkini epidemi COVID-19, untuk mencapai keamanan tinggi saat bekerja di rumah, jaringan privat keamanan tinggi MIN-VPN berbasis MIN telah dikembangkan. MIN-VPN digunakan untuk mengunggah video, gambar, dan konten program ke bagian belakang kendali penyiaran dan editor CUTV, stasiun televisi kota yang berada di bawah naungan Shenzhen Radio and Television Group (Gambar 5.50).


国 家 广 播 电 视 总 局
广 播 电 视 规 划 院
广 播 电 视 计 量 检 测 中 心

Metrology and Test Center of Radio and TV,Academy of Broadcasting Planning,National Radio and Television Administration

检 测 报 告

TEST REPORT

编 号（ Serial No. ）：200491907231493

名 称（ Name ）：广电新技术网络应用功能测试

检测类别（ Test Type ）：委托检测

委托单位（ Apply From ）：北京云视声通科技有限公司

国家广播电视总局广播电视规划院

测试类型	项目	预期结果	测试结果
	外部 IP 资源单向外访	通过 IP 网络无权访问广电新技术网络文件；通过广电新技术网络，注册用户在通过群登录认证后，可以访问 IP 网络文件。	通过
	广电新技术网络网闸访问登记	具备网络网闸访问登记功能。	通过
	广电新技术网单向外访节点的数据过滤	具备单向外访节点的数据过滤功能。	通过
	广电新技术网内部电子邮件点对点传输	具备内部电子邮件点对点传输功能。	通过
	区块链投票表决过程	具备区块链投票表决功能。	通过

八、 检测结论

本项目基础测试环境下，对广电新技术网络应用进行了功能测试，检测结论如下：

1. 被测网络具备用户注册、资源发布功能。
2. 被测网络的注册用户能正常访问该网络的发布资源。
3. 被测网络具备外部 IP 资源单向外访的权功能，通过 IP 网络无权访问被测网络文件，通过被测网络，广电新技术网络用户在通过群集名认证后，可以访问 IP 网络文件。
4. 被测网络具备网络网闸访问登记控制功能，注册用户跨网络节点获取网络文件时，需要成功申请到网络登记，才能下载网络文件。
5. 被测网络具备单向外访节点的数据过滤功能，单向外访节点能对广电新技术网络用户请求的位于 IP 网络的 txt 文件进行敏感词过滤。
6. 被测网络具备内部电子邮件点对点传输功能。
7. 被测网络具备区块链投票表决功能。

七、 检测人员

序号	签名
1	赵云永

八、 检测报告签发

批准：

审核：

证 明

广电新技术网络功能测试（项目编号 200491907231493）所使用系统完全由北京大学深圳研究生院李晖教授团队研发。

特此证明。

单位名称：北京云视声通科技有限公司

证 明 人：

日 期：2020 年 7 月 27 日

Gambar 5.49 Prototipe jaringan radio dan televisi kedaulatan

华夏城视网络电视股份有限公司

证 明

城市联合网络电视台（CUTV）是国家广电总局2011年1月批准的广播电视新媒体播出机构，是深圳广电集团牵头发起、全国城市电视台联合投资的全国新媒体联合体。现有股东36个，总局正式批准的联合开办台24个，业务合作台48个。华夏城视网络电视股份有限公司是CUTV的运营主体，通过共享牌照、内容和技术资源，为成员台提供政策支撑、技术研发、资本运作、会员服务等业务支持，共同构建全国城市台融合发展、转型升级的公共服务平台、运营服务平台。

华夏城视网络电视股份有限公司的全资子公司深圳广播网络传媒有限公司，经深圳市发改委批准，与北京大学深圳研究院共同成立了融合网络集成播控技术工程实验室，开展基于自主知识产权的技术研究、测试、验证和应用。

CUTV已于2019年12月起联合北京大学深圳研究生院的李祥教授团队将2019年马佩互联网大会获奖的《MIN：多边共管的多标识网络体系》尝试用于CUTV高安全媒体资讯应用场景，目前正在研发测试中。

特此证明。

华夏城视网络电视股份有限公司

2020年5月9日

Gambar 5.50 MIN-VPN

5.5.2 Strategi Perutean dan Skema Manajemen Mobilitas di ST-MIN

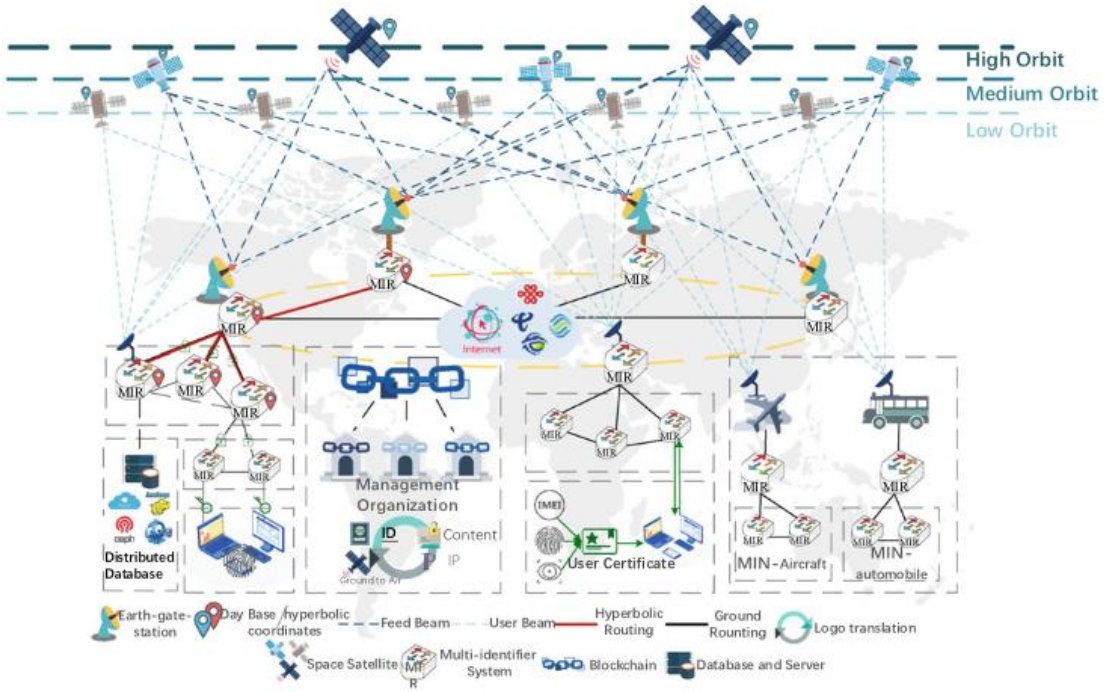
Untuk karakteristik jaringan satelit dan jaringan berbasis darat yang berbeda, kami mengusulkan algoritma perutean hiperbolik dan algoritma perutean adaptif terdistribusi berbasis penundaan di jaringan satelit. Beberapa pengenal ditangani berdasarkan MIN dan MIS, dan pemilihan jalur dan penerusan paket pengenal yang berbeda dicapai melalui MIR. Strategi perutean dan skema manajemen mobilitas ST-MIN ditunjukkan pada Gambar 5.51.

Algoritma perutean berdasarkan jarak hiperbolik mengadopsi strategi greedy sederhana dengan sedikit informasi perutean. Node saat ini hanya perlu menghitung jarak hiperbolik antara setiap node tetangga dan node tujuan, dan memilih jalur terpendek untuk penerusan. Penanaman greedy jaringan kompleks dalam ruang Euclidean memerlukan dimensi tinggi yang mengarah ke penanaman jaringan dan perhitungan jarak yang relatif kompleks.

Dalam jaringan penanaman hiperbolik, bidang hiperbolik dapat menanamkan topologi jaringan apa pun dengan berbagai ukuran dan derajat node tanpa pengurangan dimensionalitas dan komputasi berdimensi tinggi. Berdasarkan koordinat hiperbolik, greedy routing mencapai tingkat keberhasilan routing yang tinggi. Secara teoritis, penyematan hiperbolik yang baik dalam jaringan membuat tingkat keberhasilan routing mencapai 100%. Untuk jaringan bebas skala, algoritma greedy routing berdasarkan koordinat hiperbolik mendekati jalur routing yang optimal. Ruang pengenal jaringan dirancang dengan struktur hierarkis, yang ditentukan menurut permintaan aktual dan stabilitas topologi.

Bagian bawah ruang identitas jaringan terdiri dari pengguna individu, yang termasuk dalam domain otonom jaringan yang berbeda. Koordinat hiperbolik dianggap sebagai pengenal hiperbolik node AS untuk merutekan antara domain yang berbeda. Koordinat

hiperbolik setiap node domain tetap tidak berubah untuk waktu yang lama, karena topologi jaringan antara node di setiap domain hierarkis relatif stabil. Pada domain terendah, karena seringnya terjadi perubahan topologi, kami mengadopsi protokol routing intra-domain, seperti OSPF, dll., untuk menghitung overhead dari berbagai jalur sesuai dengan status tautan, kemudian router memilih jalur dengan overhead terendah sebagai jalur penerusan.



Gambar 5.51 Arsitektur routing di ST-MIN

Algoritma routing adaptif terdistribusi berbasis penundaan cocok untuk jaringan satelit dengan tautan antarsatelit. Algoritma menghitung penundaan propagasi dan penundaan antrean dari setiap hop berikutnya kandidat untuk memperoleh probabilitas setiap hop berikutnya dipilih, kemudian meneruskan paket ke hop berikutnya dengan probabilitas tertinggi. Selain itu, ketika beban jaringan satelit rendah dengan kondisi jaringan yang baik, transmisi data antara perangkat jaringan satelit harus dilakukan melalui jaringan satelit terlebih dahulu. Ketika beban jaringan satelit terlalu tinggi atau tautan gagal, paket akan dikirim ke stasiun di jaringan berbasis darat.

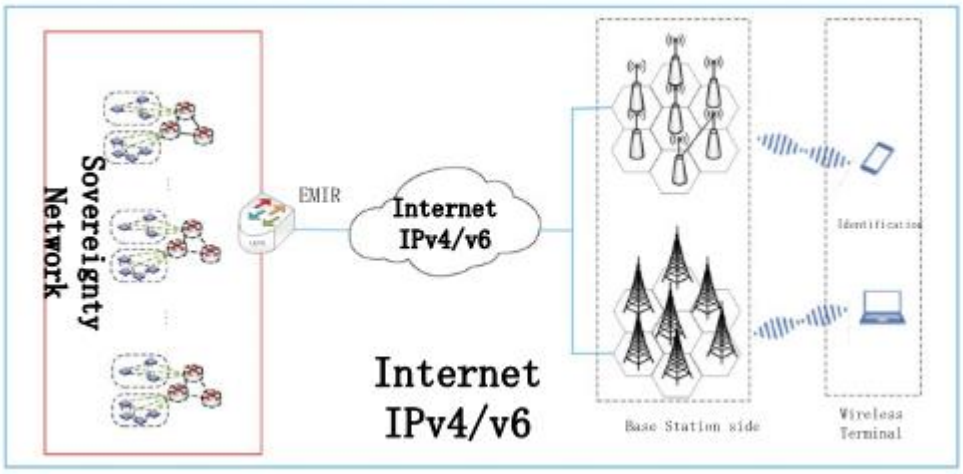
Oleh karena itu, ini adalah algoritma routing adaptif yang mengurangi penundaan transmisi paket dan kemungkinan kemacetan jaringan serta memberikan metode kontrol ketika kemacetan terjadi. Proses routing dalam ST-MIN adalah sebagai berikut: (1) Proses routing antara perangkat dalam jaringan satelit dilakukan melalui jaringan satelit terlebih dahulu. Jika terjadi kemacetan jaringan atau kegagalan tautan, jaringan berbasis darat digunakan sebagai cadangan. (2) Untuk memilih stasiun gerbang yang optimal untuk transmisi data, routing antara peralatan jaringan satelit dan peralatan jaringan berbasis darat harus mempertimbangkan secara komprehensif lokasi geografis peralatan jaringan satelit, dan jarak

hiperbolik antara stasiun gerbang dan peralatan berbasis darat target. (3) Metode meminimalkan jarak hiperbolik antara node tetangga dan node tujuan diadopsi untuk routing antara peralatan jaringan berbasis darat. Skema manajemen mobilitas dalam ST-MIN, menyimpan informasi lokasi geografis dan informasi koordinat hiperbolik node dalam node pertemuan (node RV), yang didistribusikan di berbagai domain. Sistem pertemuan terdistribusi (DRS), yang dibentuk dari node-node ini, memungkinkan jaringan untuk mengidentifikasi dan menemukan terminal dengan menjalankan protokol sinkronisasi data. Dengan cara ini, ST-MIN mendukung pengguna untuk menggunakan terminal selama proses seluler.

5.5.3 Bisnis 5G

Jaringan seluler generasi ke-5 (5G) merupakan generasi terbaru dari teknologi komunikasi seluler, yang diperluas dari sistem 4G (LTE-A, WiMax), 3G (UMTS, LTE), dan 2G (GSM). 5G bertujuan untuk menyediakan layanan dengan kecepatan data tinggi, latensi rendah, penghematan energi, biaya rendah, kapasitas sistem besar, dan konektivitas perangkat berskala besar. Fase pertama standar 5G dalam Rilis-15, memerlukan penyelesaian penyebaran komersial awal. Fase kedua dalam Rilis-16 telah diselesaikan pada bulan April 2020, dan diserahkan ke International Telecommunication Union (ITU) sebagai kandidat untuk teknologi IMT-2020.

Standar ITU IMT-2020 menetapkan beberapa persyaratan, seperti kecepatan 20 Gbit/s, lebar pita saluran lebar, dan MIMO berkapasitas besar. Jaringan 5G adalah jaringan seluler digital, di mana area layanan yang dicakup oleh operator dibagi menjadi banyak area geografis yang lebih kecil yang disebut sel. Sinyal analog yang mewakili suara dan gambar didigitalkan di telepon, kemudian diubah oleh konverter analog-ke-digital dan ditransmisikan sebagai aliran bit. Semua perangkat nirkabel 5G di dalam sel, berkomunikasi dengan susunan antena lokal dan transceiver otomatis berdaya rendah (pemancar dan penerima) di dalam sel melalui gelombang radio.



Gambar 5.52 Dukungan 5G untuk node IP dari jaringan kedaulatan

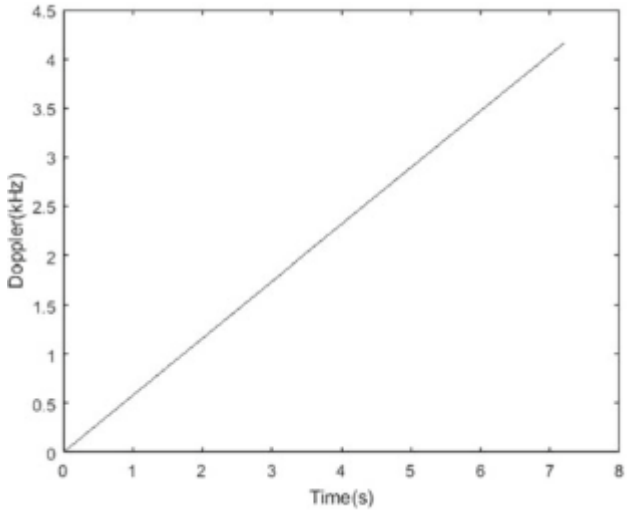
Transceiver mengalokasikan saluran dari kumpulan frekuensi umum. Saluran ini dapat digunakan kembali di sel yang terpisah secara geografis. Antena lokal terhubung ke jaringan telepon dan Internet melalui koneksi serat optik atau backhaul nirkabel dengan bandwidth tinggi. Ketika pengguna berpindah dari satu sel ke sel lain, perangkat seluler akan secara otomatis beralih ke antena di sel baru. Jaringan kedaulatan dikembangkan berdasarkan jaringan yang berpusat pada identitas (ICN), yang dikombinasikan dengan caching dalam jaringan, dan secara inheren mendukung banyak jalur, sehingga dapat mendukung komunikasi 5G dengan baik.

Caching dalam jaringan memastikan mobilitas yang baik. Saat pengguna pindah ke area jangkauan lain dari stasiun pangkalan, perangkat mereka hanya perlu mengirim paket minat lainnya. Karena konten yang diminta telah di-cache di node tertentu pada jalur permintaan terakhir, data dikembalikan secara langsung melalui pencarian node ter-cache terdekat pada jalur tersebut. Jaringan yang berpusat pada identitas secara inheren mendukung beberapa jalur, yang berarti bahwa ICN memungkinkan perangkat seluler untuk terhubung ke beberapa stasiun pangkalan pada saat yang sama tanpa memengaruhi transmisi data di luar jangkauan stasiun pangkalan saat ini. Dalam jaringan kedaulatan, stasiun pangkalan 5G bertindak sebagai node dalam jaringan pusat identitas, yang dilakukan secara langsung mengikuti mode transmisi data dalam jaringan pusat identitas. Jika stasiun pangkalan 5G terletak di luar jaringan kedaulatan, yang disebut node IP, akan menjadi masalah penting untuk mengawasi data yang mengakses jaringan kedaulatan melalui stasiun pangkalan 5G, yaitu, bagaimana mengelola pengguna seluler yang meninggalkan jaringan kedaulatan. Kami merancang proses transmisi data yang ditunjukkan pada Gambar 5.52 untuk menyelesaikan masalah ini.

(1) Perangkat terminal nirkabel dengan pengenal identitas, berkomunikasi dengan stasiun pangkalan melalui IP Overlay.
(2) Stasiun pangkalan mengirimkan data ke node keluar dari jaringan kedaulatan target mengikuti mode transmisi IP tradisional.
(3) Node keluar mengaudit identitas pengguna. Jika disetujui, node tersebut diizinkan untuk mengakses data, jika tidak, node tersebut akan ditolak.
(4) Oleh karena itu, jaringan kedaulatan mendukung bisnis dan mobilitas 5G dengan baik.

5.5.4 Skema Pengalihan Antara Satelit dan Stasiun Gerbang Berbasis 6G

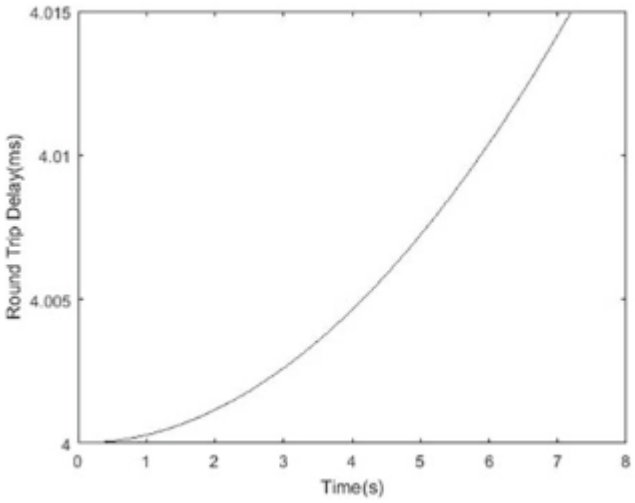
Dengan berkembangnya jaringan darat, apakah teknologi 6G dapat digunakan dalam jaringan satelit orbit rendah telah menarik banyak perhatian. Teknologi pengalihan dan arsitektur jaringan diteliti, sehingga pengguna biasa dapat beralih dengan lancar antara stasiun pangkalan satelit 6G dan stasiun pangkalan darat 6G.



Gambar 5.53 Fungsi offset frekuensi saluran

ST-MIN harus menjamin kelangsungan layanan saat terminal berpindah dalam sel nirkabel yang berbeda. Dengan asumsi bahwa satelit orbit rendah MIN juga dilengkapi dengan stasiun pangkalan 6G dan mematuhi standar 6G, skema serah terima yang lancar antara terminal dalam sel satelit dan sel darat dianalisis dan dirancang.

Sinar satelit dan sinar stasiun darat memiliki waktu tunda dan frekuensi offset yang berbeda untuk terminal 6G di darat. Selama pengalihan, waktu dan frekuensi perlu disinkronkan antara terminal dan sel baru. Gambar 5.53 dan 5.54 menunjukkan variasi penundaan saluran dan pergeseran frekuensi saat berkas satelit pada orbit 600 km melewati terminal di darat.



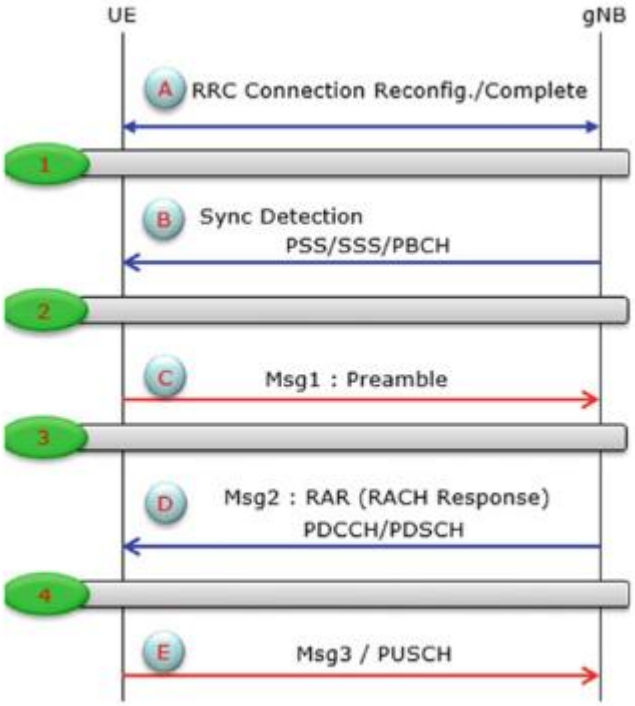
Gambar 5.54 Fungsi delay round trip saluran

Dalam kondisi seperti itu, teknologi akses acak yang digunakan dalam jaringan darat tidak dapat menyelesaikan proses sinkronisasi waktu-frekuensi. Untuk menyelesaikan peralihan antara sel darat dan sel satelit, teknologi akses acak standar 6G perlu ditingkatkan.

Selain itu, perlu untuk merancang urutan pemimpin, interval sub-pembawa, mode penyambungan urutan, yang memungkinkan akses ke sel 6G yang dicakup oleh jaringan satelit. Pertama-tama, terminal menilai apakah sel pengalihan target adalah sel yang dicakup oleh jaringan satelit. Kemudian skema peningkatan dapat diadopsi dalam proses pengalihan.

Karena keteraturan pergerakan satelit, jaringan memprediksi pengalihan terminal dan mengadopsi proses akses acak nonkompetitif untuk mengurangi waktu pengalihan antarsel. Sebagai contoh, Gambar 5.55 menunjukkan proses akses acak nonkompetitif klasik. Sel asli mengirimkan urutan pemimpin yang diperlukan untuk pengalihan ke terminal, dan terminal mengirimkan urutan tersebut langsung ke sel target. Lebih jauh lagi, menurut pergerakan satelit yang teratur, sinkronisasi waktu-frekuensi terminal tetap dapat diprediksi, sehingga dapat menyederhanakan urutan yang diperlukan bagi pengguna untuk mengakses sel target guna mempersingkat waktu yang diperlukan untuk akses. Kami memperkirakan kemampuan prediksi offset waktu-frekuensi dalam simulasi dan pengukuran di lingkungan aktual untuk menjamin peralihan yang cepat.

Karena struktur topologi ST-MIN yang kompleks, peralihan sel juga melibatkan peralihan antara jaringan inti yang berbeda dan Jaringan Seluler Darat Publik (PLMN) yang berbeda. Dalam pekerjaan mendatang, perlu untuk menganalisis proses pensinyalan dalam keadaan yang berbeda pada saat yang sama, dan selanjutnya meningkatkan proses peralihan standar protokol 6G.



Gambar 5.55 Proses akses acak nonkompetitif

5.5.5 Eksperimen dan Evaluasi ST-MIN

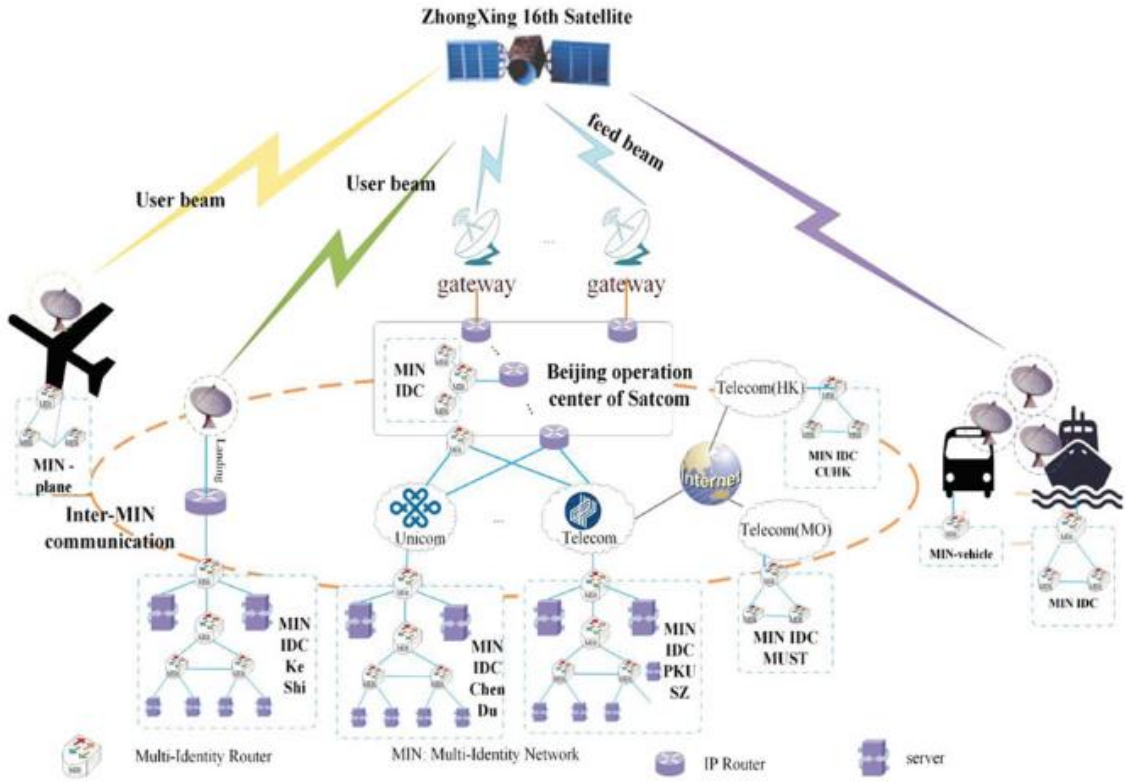
1. Pembangunan ST-MIN Testbed

Dimulai pada bulan April 2020, sebuah testbed ST-MIN dibangun bekerja sama dengan China Satellite Communications Corporation (atau China Satcom). Saat ini, testbed tersebut telah lulus uji primer dan memverifikasi kelayakan ST-MIN. Jaringan prototipe ditunjukkan pada Gambar 5.56. Jaringan uji tersebut menggunakan beberapa subnet multi-identifier kecil yang representatif, termasuk MIN-IDC (Multi-Identifier Network Internet Data Center) di Kashgar, Chengdu, dan Beijing, dan MIN-IDC di Sekolah Pascasarjana Universitas Peking Shenzhen, Universitas Cina Hong Kong, Universitas Sains dan Teknologi Makau, dan seterusnya. Beberapa subnet dihubungkan melalui Satelit ZhongXing ke-16. Penerowongan IP digunakan untuk berkomunikasi antar-subnet, dan protokol lapisan tautan digunakan untuk mentransfer paket-paket jaringan multi-identifier secara langsung di dalam subnet.

2. Uji Penerapan Sistem Manajemen Multi-pengenal Dua Tingkat

Berdasarkan uji coba ST-MIN, satu server dari setiap subnet dipilih sebagai node blockchain dan menyusun blockchain tingkat pertama dari sistem manajemen multi-pengenal kami. Blockchain tingkat pertama mencakup delapan node masing-masing dari Sekolah Pascasarjana Universitas Peking Shenzhen, China Satcom, Universitas Tiongkok Hong Kong, Universitas Sains dan Teknologi Makau, Universitas Sains dan Teknologi Hong Kong, Universitas Teknologi Tiongkok Selatan, Jinshan Cloud Co. Ltd., dan China Unicom.

Dalam jaringan pribadi Satcom, blockchain konsorsium tingkat kedua diterapkan berdasarkan sistem komunikasi Satelit ZhongXing ke-16. Sistem manajemen tingkat kedua Satcom berisi total 5 node, yang digunakan untuk mengelola pengidentifikasi komunikasi jaringan berbasis ruang angkasa. Eksperimen menunjukkan bahwa sistem manajemen dua tingkat dapat berjalan normal dan sistem manajemen multi-pengenal memiliki fleksibilitas tinggi dalam perluasan tingkat.



Gambar 5.56 Tempat pengujian ST-MIN

3. Uji Komunikasi Dasar ST-MIN

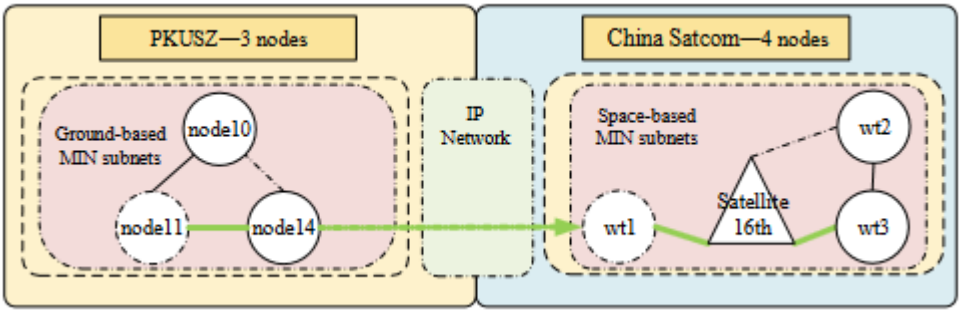
Program transfer berkas jaringan sederhana diimplementasikan untuk melakukan uji komunikasi dasar pada tempat pengujian ST-MIN. Program ini mencakup server dan klien. Server dipasang di host bernama wt3 di IDC China SATCOM di Beijing, dan klien dipasang di host bernama node11 di IDC PKUSZ di Shenzhen. Klien mengunduh berkas dari server dengan protokol kontrol transmisi sederhana berdasarkan protokol jaringan MIN. Protokol kontrol transmisi ini dapat menggunakan sejumlah jendela transmisi tetap untuk mentransfer data dengan andal dan setiap ukuran paket yang dikirimnya adalah 8000 byte. Topologi jaringan uji ditunjukkan pada Gambar 5.57. Total lebar pita tautan transmisi adalah 20 Mbps. Delapan jenis jendela transmisi tetap digunakan untuk melakukan pengujian, dan setiap pengujian diulang sepuluh kali. Hasil transmisi ditunjukkan pada Gambar 5.58. Seiring dengan meningkatnya jendela transmisi, laju transmisi meningkat hampir secara linear. Pengujian transportasi lebih lanjut memerlukan desain mekanisme kontrol transportasi yang baik berdasarkan ST-MIN, yang berada di luar cakupan artikel ini.

4. Analisis dan Perbandingan

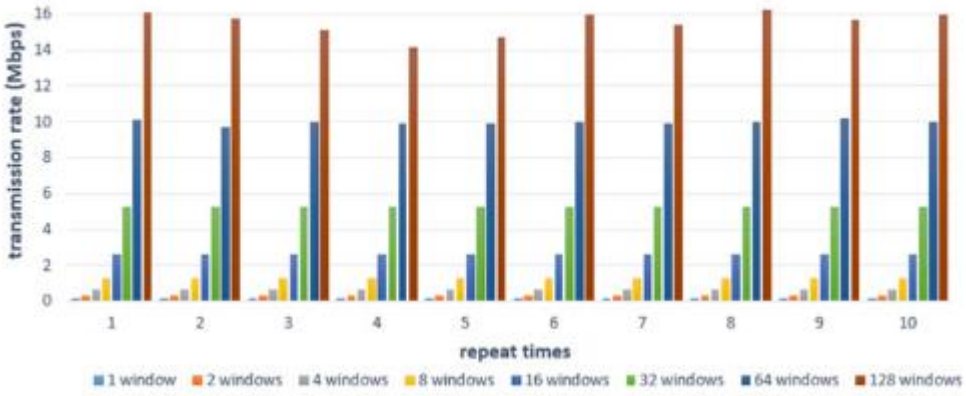
Dibandingkan dengan jaringan IP, keunggulan utama ST-MIN meliputi hal-hal berikut:

(1) Beberapa pengenal dan moda transmisi dapat hidup berdampingan, dan pengenal yang lebih tepat digunakan untuk memenuhi berbagai skenario, seperti pengenal hierarkis di jaringan darat dan pengenal geospasial di jaringan luar angkasa.

(2) ST-MIN memiliki lebih banyak fitur keamanan endogen, termasuk komputasi kepercayaan, multi-tanda tangan paket, dan pengidentifikasi autentikasi mandiri.
(3) Teknologi pengelolaan bersama dan tata kelola bersama pengidentifikasi, manajemen pemungutan suara pengidentifikasi diwujudkan melalui teknologi blockchain konsorsium.
(4) Ekstensibilitas identifikasi, alih-alih menggunakan pengidentifikasi tetap dan mode komunikasi, ST-MIN mencadangkan antarmuka untuk perluasan pengidentifikasi dan mode komunikasi di masa mendatang, yang membuat resistensi inovasi arsitektur jaringan masa depan berkurang.



Gambar 5.57 Topologi uji komunikasi dasar



Gambar 5.58 Hasil uji komunikasi dasar

DAFTAR PUSTAKA

Ahlgren B, Dannewitz C, Imbrenda C et al (2012) A survey of information-centric networking. IEEE Commun Mag 50(7):26–36

Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.

Balkin, J. M. (2018). The Future of Free Expression in a Digital Age. Yale Law Journal, 127(7), 2296-2320.

Bellovin, S. M. (2021). Network Security: Private Communication in a Public World. Prentice Hall.

Benkler, Y. (2016). Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics. Oxford: Oxford University Press.

Bennett, C. J. (2019). Network Sovereignty: The Role of the State in the Digital Age. New York: Routledge.

Castells, M. (2010). The Rise of the Network Society. Oxford: Blackwell Publishing.

Chen, X., & Zhao, Y. (2022). Adaptive Routing Protocols in Satellite Networks. Springer.

Decimal Network Information Technology Co. Ltd (2006) Decimal network working group. http://www.em777.net/. Accessed 14 Jan 2020

Deering, S., & Hinden, R. (2021). Internet Protocol, Version 6 (IPv6) Specification. RFC 8200.

DeNardis, L. (2014). The Global War for Internet Governance. New Haven: Yale University Press.

Dixon, T., & Crouse, D. (2023). Multi-identifier Networks: Concepts and Applications. Cambridge University Press.

Doyle, J., & Carroll, J. (2022). Understanding Network Routing: Basics and Advanced Techniques. Elsevier.

Drexl, A. (2020). Intellectual Property and the Internet: A Global Perspective. Cambridge: Cambridge University Press.

frontier science and discussing the basis of establishing national network sovereignty. Borderland Stud China 1:23–44

Fuchs, C. (2017). Social Media: A Critical Introduction. London: SAGE Publications.

Galloway, A. R. (2012). The Interface Effect. Cambridge: Polity Press.

Graham, M. (2010). Geography in the Age of the Internet: The New Networked World. London: Routledge.

He ZL, An HJ (2019) US extraterritorial law enforcement reform and China's response of the network sovereignty view. J Inf Secur Commun Priv 12:37–47

Hindman, M. (2009). The Myth of Digital Democracy. Princeton: Princeton University Press.

Hu, Y., & Li, B. (2022). Blockchain Technology for Secure Networks. CRC Press.

Huawei (2019) New IP. https://www.huawei.com/cn/industry-insights/innovation/new-ip. Accessed 14 Jan 2020

Jacobson V, Smetters DK, Thornton JD et al (2012) Networking named content. Commun ACM 55(1):117–124

Klein, N. (2014). This Changes Everything: Capitalism vs. The Climate. New York: Simon & Schuster.

Krebs, B. (2021). The Cybersecurity Crisis: How to Protect Networks and Data. O'Reilly Media.

Lessig, L. (2006). Code: Version 2.0. New York: Basic Books.

Li H, Wu JX et al (2019) MIN: Co-governing multi-identifier network architecture and its prototype on operator's network. In: The 6th World Internet Conference

Li H, Wu JX, Wang XG et al (2019) System and methods for managing top-level domain names using consortium blockchain. US Patent. US: 10178069B2. 2019.01.08

Li H, Wu JX, Yang X et al (2020) MIN: Co-governing multi-identifier network architecture and its prototype on operator's network. IEEE Access 8:36569–36581

Li R, Clemm A, Chunduri U et al (2018) A new framework and protocol for future networking applications. In: Association for computing machinery, pp 21–26. New York, USA

Liu, J., & Zhang, W. (2023). Distributed Networks and Sovereignty in the Digital Age. Wiley.

Mann, T. (2018). The Future of Internet Governance: A Global Perspective. Washington, D.C.: Brookings Institution Press.

Miller, M., & Lee, K. (2022). Network Security and Privacy: A Comprehensive Guide. Springer.

Morozov, E. (2013). To Save Everything, Click Here: The Folly of Technological Solutionism. New York: PublicAffairs.

Morse, A., & Smith, R. (2023). IPv9 and Future Internet Protocols. Academic Press.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online].

Nissenbaum, H. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford: Stanford University Press.

Papacharissi, Z. (2010). A Private Sphere: Democracy in a Digital Age. New York: Polity Press.

Papageorgiou, A., & Dimitriou, T. (2021). Satellite Communications and Network Design. Wiley.

Ravishankar, P., & Singh, N. (2023). Advanced Routing Algorithms for Modern Networks. Springer.

Reddy, S., & Kumar, S. (2022). Internet of Things and Cyber Security: Protecting Networks and Data. CRC Press.

Reid, F., & Smith, J. (2022). Privacy and Security in Digital Networks. Routledge.

Schafer, T., & Sharma, P. (2023). Protocol Design for Multi-identifier Networks. Elsevier.

Schmidt, C., & Meyer, T. (2022). The Future of Network Sovereignty: Governance and Control. Cambridge University Press.

Sethi, R., & Agrawal, D. (2023). Managing Network Security and Privacy. Springer.

Shirky, C. (2010). Cognitive Surplus: Creativity and Generosity in a Connected Age. New York: Penguin Press.

Sullivan, A. (2016). The Internet and the Future of Governance. Harvard International Review, 37(1), 14-19.

Sun Y, Wang CH (2019) The Internet domain and Frontier from the perspective of general

Sussman, D. (2021). Digital Sovereignty: The Future of Data and Governance. San Francisco: O'Reilly Media.

Taplin, J. (2017). Move Fast and Break Things: How Facebook, Google, and Amazon Cornered Culture and Undermined Democracy. New York: Little, Brown and Company.

TeleGeography (2020) Submarine cable map. https://www.submarinecablemap.com/. Accessed 29 Dec 2020

Vardigan, L., & Johnson, C. (2023). Modern Network Protocols and Standards. Wiley.

Wang, L., & Zhou, X. (2022). Blockchain and Network Security: An Integrated Approach. Springer.

Woollacott E (2019) Russia cuts off its internet, with mixed results. https://www.forbes.com/sites/emmawoollacott/2019/12/24/russia-cuts-off-its-internet-with-mixed-results/?sh= 234ac00b619d. Accessed 18 Nov 2020

Yang, Y., & Lee, T. (2023). Advanced Technologies in Network Security and Privacy. Routledge.

Zhao, J., & Wang, H. (2023). Exploring the Future of Network Sovereignty. Elsevier.

Zheng X, Jiang S, Wang C (2019) New IP: new connectivity and capabilities of upgrading future data network. Telecommun Sci 35(9):2–11. https://doi.org/10.11959/j.issn.1000-0801.2019208

Zheng X, Tan J, Jiang S, Wang C (2019) Analysis on the requirements of future data network. Telecomm Sci 35(8):16–25. https://doi.org/10.11959/j.issn.1000-0801.2019204

Zhuang XC (2016) Research on American information security mechanism from the perspective of network sovereignty. China Foreign Affairs University Press

Zittrain, J. (2008). The Future of the Internet and How to Stop It. New Haven: Yale University Press.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs.

Manajemen Kedaulatan Jaringan Siber

Dr. Agus Wibowo, M.Kom, M.Si, MM.

BIO DATA PENULIS

Penulis memiliki berbagai disiplin ilmu yang diperoleh dari Universitas Diponegoro (UNDIP) Semarang. dan dari Universitas Kristen Satya Wacana (UKSW) Salatiga. Disiplin ilmu itu antara lain teknik elektro, komputer, manajemen dan ilmu sosiologi. Penulis memiliki pengalaman kerja pada industri elektronik dan sertifikasi keahlian dalam bidang Jaringan Internet, Telekomunikasi, Artificial Intelligence, Internet Of Things (IoT), Augmented Reality (AR), Technopreneurship, Internet Marketing dan bidang pengolahan dan analisa data (komputer statistik).

Penulis adalah pendiri dari Universitas Sains dan Teknologi Komputer (Universitas STEKOM) dan juga seorang dosen yang memiliki Jabatan Fungsional Akademik Lektor Kepala (Associate Professor) yang telah menghasilkan puluhan Buku Ajar ber ISBN, HAKI dari beberapa karya cipta dan Hak Paten pada produk IPTEK. Sejak tahun 2023 penulis tercatat sebagai Dosen luar biasa di Fakultas Ekonomi & Bisnis (FEB) Universitas Diponegoro Semarang. Penulis juga terlibat dalam berbagai organisasi profesi dan industri yang terkait dengan dunia usaha dan industri, khususnya dalam pengembangan sumber daya manusia yang unggul untuk memenuhi kebutuhan dunia kerja secara nyata.

YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

ISBN 978-623-8642-28-1 (PDF)
9 786238 642281