Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Review:

Discussion on a new paradigm of endogenous security towards 6G networks*

Xinsheng JI†1,2,3, Jiangxing WU2,3, Liang JIN2, Kaizhi HUANG†‡2,3, Yajun CHEN2,
Xiaoli SUN2, Wei YOU2, Shumin HUO2, Jing YANG2

1*Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China*
2*National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, China*
3*Purple Mountain Laboratories: Networking, Communications and Security, Nanjing 211111, China*
†E-mail: jixs@pmlabs.com.cn; huangkaizhi@tsinghua.org.cn

Received Feb. 18, 2022; Revision accepted June 14, 2022; Crosschecked Sept. 30, 2022

Abstract: The sixth-generation mobile communication (6G) networks will face more complex endogenous security problems, and it is urgent to propose new universal security theories and establish new practice norms to deal with the "unknown unknown" security threats in cyberspace. This paper first expounds the new paradigm of cyberspace endogenous security and introduces the vision of 6G cyberspace security. Then, it analyzes the security problems faced by the 6G core network, wireless access network, and emerging associated technologies in detail, as well as the corresponding security technology development status and the integrated development of endogenous security and traditional security. Furthermore, this paper describes the relevant security theories and technical concepts under the guidance of the new paradigm of endogenous security.

Key words: 6G security; New paradigm of endogenous security; Core network; Wireless access network
https://doi.org/10.1631/FITEE.2200060 **CLC number:** TN918

1 Introduction

A paradigm is essentially a theoretical system and a research framework, and it is a coordinate frame of reference and a basic method for conducting scientific research, establishing a scientific system, and applying scientific ideas (Kuhn, 1996). In 2007, Jim GRAY proposed to divide scientific research into four types of paradigms in his speech "The Revolution of Scientific Method," namely, observation and discovery, analysis and induction, numerical simulation, and use of massive, heterogeneous, and diverse data resources to discover new scientific laws (Gray, 2009).

The Chinese scientist Jiangxing WU first summarized the development paradigm of cyberspace security (Wu JX, 2022), pointing out that there are three development paradigms of cyberspace security: the first paradigm is "the functional safety development paradigm based on redundant configuration and voting;" the second paradigm is "the security development paradigm based on encryption, authentication, and authorization" (Li HQ and Li, 2001); the third paradigm is "the development paradigm of network security based on detection and analysis," which includes three developmental stages: virus and Trojan killing stage (Zhang YS and Mi, 2003), software and hardware vulnerability discovery and repair stage (Manzuik et al., 2006), and attack behavior feature perception and blocking stage (Wu H, 2009; Feng and Xu, 2010). The above three paradigms have encountered an unavoidable

‡ Corresponding author

* Project supported by the National Key Research and Development Program of China (Nos. 2020YFB1806607 and 2022YFB2902202) and the National Natural Science Foundation of China (Nos. 61521003 and 61701538)

ORCID: Xinsheng JI, https://orcid.org/0000-0002-2209-5456; Kaizhi HUANG, https://orcid.org/0000-0002-7084-3826

challenge in the current high-intensity cyber confrontation environment: how to deal with unknown cyber attacks based on unknown vulnerabilities, backdoors, viruses, and Trojans without access to prior knowledge? To this end, there is an urgent need to develop a new paradigm of endogenous security in cyberspace, which can effectively defend against "unknown unknown" security threats (Wu JX, 2022).

Throughout the history of mobile communication security development, the first-generation mobile communication (1G) basically had no security measures, the second generation (2G) provided basic information encryption and one-way authentication, the third generation (3G) provided two-way authentication, the fourth generation (4G) strengthened network element authentication, and the fifth generation (5G) strengthened identity protection. These systems consider mainly information security measures such as identity authentication, data encryption, and privacy protection, but do not pay sufficient attention to cyberspace security protection under high-strength cyberspace counterattack conditions. The sixth-generation mobile communication (6G) will achieve intelligent interconnection of everything and provide ubiquitous communication support (Yang P et al., 2019; Fettweis and Boche, 2021). As a key support for the future digital world and intelligent society, the 6G network security requires in-depth planning and realization of broad functional security while fully considering information security requirements, so as to create a strong and reliable digital connection base for the future society.

This paper first expounds the new paradigm of endogenous security development in cyberspace; afterward, based on the demand vision of 6G cyberspace security, it analyzes the security issues faced by the 6G core network and the wireless access network, in addition to the current security development status; then, it presents the relevant security theories and technical concepts under the guidance of the new paradigm. Moreover, we analyze the development of traditional security technology for mobile communication and its effective integration and supplementary enhancement with endogenous security technology; we further discuss how to effectively deal with new security threats caused by emerging enabling technologies and how to use emerging enabling technologies to enhance endogenous security.

2 New paradigm of cyberspace endogenous security

The lexical meaning of "endogenous" is that in a system or a model, there are factors (or variables) that are interdependent or entangled with each other. Unlike embedded or built-in factors, only those factors that cannot be separated from a system or a model can be called endogenous. Endogenous security refers to the quantifiable, designable, verifiable, and measurable security function obtained by using endogenous effects such as the system's own architecture, function, and operating mechanism. It is not built in or embedded in the existing technologies but provides endogenous security capabilities to deal with known and unknown security threats by designing security structures. The development paradigm of cyberspace endogenous security has been proposed by Wu JX (2018b, 2020a, 2020b, 2022), whose objectives are to develop an endogenous security theory and technology system that does not rely on prior knowledge, such as vulnerability backdoor discovery and attack feature analysis, to establish a set of practical norms to effectively solve the common problems of endogenous security in cyberspace, and to provide an innovative dynamic heterogeneous redundancy (DHR) structure, providing quantifiable design and verifiable metrics of cyberspace security and safety capabilities, which can effectively prevent "unknown unknown" security threats that are unknown cyberspace attacks caused by unknown vulnerabilities, backdoors, viruses, and Trojans without access to prior knowledge for the defender.

2.1 DHR structure

The DHR structure is the backbone of 6G communication security, functional safety, and supply chain security. As shown in Fig. 1 (Wu JX, 2020b), the DHR structure includes an input agent, a functionally equivalent heterogeneous executor set, a strategy ruler, an output agent, and a negative feedback controller. The input agent distributes the input sequence to multiple functionally equivalent heterogeneous executors and performs strategy ruling on the output vector processed by the executor; the strategy ruler judges the compliance of the content of the output vector; the negative feedback controller is activated when an undesired ruling state is found, and the differential mode output executor is replaced

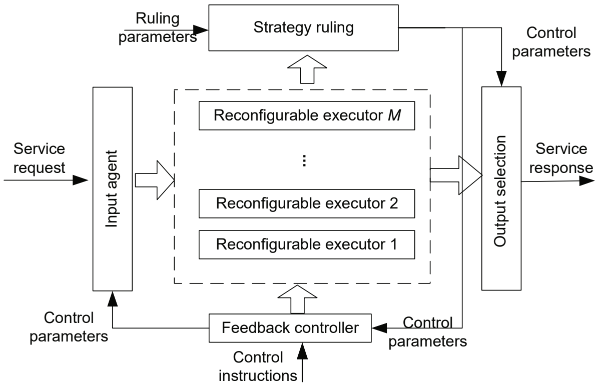

Fig. 1 Dynamic heterogeneous redundancy (DHR) structure model (Wu JX, 2020b)

and cleaned. This multi-dimensional dynamic reconfiguration feedback operating environment based on iterative ruling facilitates defense by the heterogeneous fault-tolerant mechanism against any independent human trial-and-error or blind attack, and the feedback control loop causes the "uncertainty effect" under the condition of functional equivalence in the heterogeneous redundant environment (Liu LS et al., 2009).

The uncertainty effect of quantum physics can render human trial-and-error or blind attack on the mechanism ineffective. Mimicry of the biological world can produce defense fog to improve the defense capabilities of the system. Inspired by the above phenomenon, the inherent randomness, diversity, and redundancy of the DHR structure can produce similar uncertainty effects of quantum physics and mimicry of the biological world. Therefore, we can simultaneously deal with the "dark function based man-made attacks" and failures caused by random failures of software and hardware relying only on mechanisms such as heterogeneous configuration, policy ruling, feedback control, and multi-dimensional dynamic reconfiguration, without external prior knowledge or additional defensive measures. In other words, the DHR structure can provide generalized functional safety (safety & security) by integrating functional safety (safety) and information security (security) and can provide a practice norm against general uncertain disturbances.

2.2 Endogenous security mechanism of the DHR structure

As shown in Figs. 2 and 3, the general uncertain disturbance based on the common endogenous security problem can be transformed into the "differential mode or common mode" disturbance problem within the structure by the endogenous security mechanism of DHR. Adjusting redundancy, heterogeneity, comparison length, closed-loop response time, ruling strategy, and feedback function can quantify and control the common mode escape probability and duration. Therefore, the endogenous security technology based on the DHR structure can transform an "unknown unknown security threat" into a "known unknown security threat" through the rediscovery of "true relatively axiom." In theory, all differential mode disturbances can be detected and dynamically prevented or corrected (Wu JX, 2020b, 2022). Moreover, with the help of the adjudication-based feedback control mechanism, it is exponentially difficult to attempt to form a coordinated attack escape through heterogeneously unstable attack surfaces, and the escape probability of general uncertain disturbances in the common mode form within the architecture can be controlled within the set threshold. Endogenous security technology based on the DHR structure provides a new development paradigm with quantifiable design and verifiable metrics for the effectiveness of cyberspace security defense (Wu JX, 2022).

The new paradigm of endogenous security in cyberspace can prove from the theoretical and methodological perspectives that the contradictions of "openness and security, advanced and reliability, autonomy and trustworthiness, and functional safety and cyberspace security" can be highly unified within the scope of the endogenous security theory and methodology, which will become an important route to effectively solve cyberspace security problems.

3 Demand vision for 6G cyberspace security

Although the global 5G network is still in the early stage of commercial use, the global competition on 6G scientific research to meet the future network needs after 2030 has begun. What deserves special attention is that in the current initial discussions on 6G vision, requirements, and key technologies in various countries around the world, security has received extraordinary attention. Scientific research institutions, operators, and communication equipment manufacturers have released white papers one

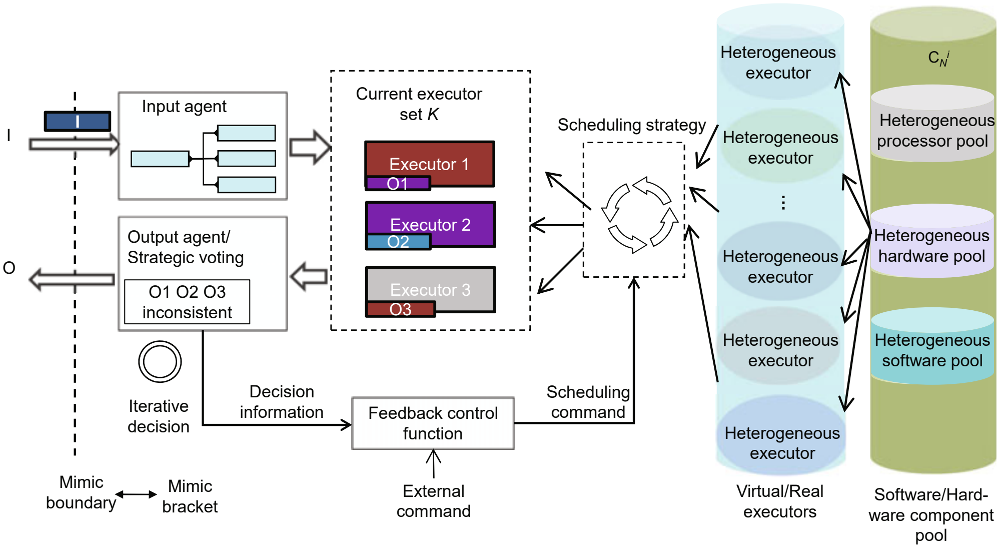

Fig. 2 Normal dynamic heterogeneous redundancy (DHR) operation mechanism (Wu JX, 2022)

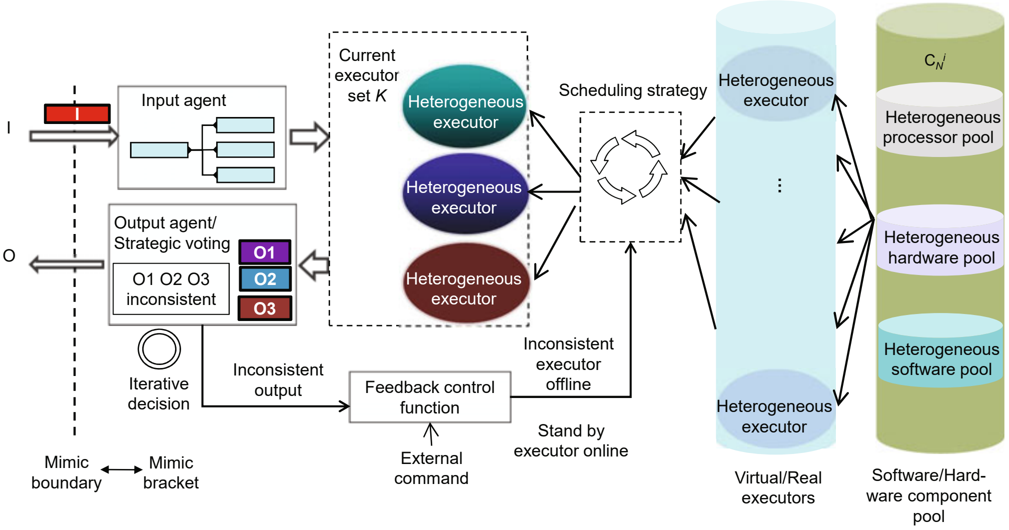

Fig. 3 Operation mechanism for differential mode events (Wu JX, 2022)

after another, proposing their own visions for 6G cyberspace security. The United States, the European Union (EU), China, and other countries and organizations have begun to deploy 6G cyberspace security research projects.

The Chinese government and research institutes are the first in the world to put forward the vision of 6G endogenous security. On one hand, facing the core requirement that 6G will provide key services for a world where humans, machines, and things are highly integrated, new expansions are made to the connotation and extension of mobile communication security, and 6G security is required to pay attention to the generalized robust control and generalized functional safety of 6G networks based on traditional information security, including confidentiality, integrity, availability, and privacy protection (Wu JX, 2022). On the other hand, facing the mission assurance requirements of 6G under high-intensity and complex network conditions, it is necessary to break the traditional mobile communication development paradigm of technical performance streaking and supplementary security measures. At the beginning of 6G design, innovative theories and technical frameworks should be used to explore the new development paradigm that supports the integration of network communication and cyberspace safety and security as the two wheels driving 6G forward.

The United States, Europe, and Japan have also listed generalized security concepts, such as security, resilience, and dependability, as the core vision and early-launched projects of 6G. The National Science Foundation of the United States launched the Resilient and Intelligent Next-Generation (NextG) Systems (RINGS) program for NextG network systems (including 6G cellular, future versions of wireless fidelity (Wi-Fi), and satellite networks) (NSF, 2021). The RINGS charter points out that "NextG Systems are a Game Changer." It focuses on the development of network resilience, including security, adaptability, autonomy, and reliability. At the same time, in its project guidelines, it is mandatory for applicants to carry out collaborative and integrated innovation of two-wheel drive for NextG-oriented enabling technology groups (wireless, spectrum, and network) and elastic technology groups (security, adaptive, and autonomous), and applications for single-wheel drive are not accepted.

The North American Next G Alliance officially released the 6G roadmap report (Next G Alliance, 2022), proposing the first 6G vision in North America, the six goals of which are: (1) trust, security, and resilience; (2) enhanced digital world experience; (3) cost-effective solutions (covering all aspects of the network architecture including devices and the wireless network); (4) distributed cloud and communication systems (built on virtualization technology); (5) artificial intelligence (AI) native wireless networks (to enhance the robustness, performance, and efficiency of wireless and cloud technologies); (6) sustainability (fundamentally changing the way electricity supports communications and computer networks, while enhancing the role of information technology in protecting the environment, with the goal of achieving carbon neutrality by 2040 (Next G Alliance, 2022).

On January 1, 2021, the EU launched its 6G research project "Hexa-X" (Hexa-X, 2020), which proposes new network architecture paradigms and aims to develop the overall vision of 6G, identifying six major research challenges, including the following: (1) connecting intelligence transforming AI/machine learning (ML) technology into an important and trusted tool to improve efficiency and service experience; (2) multinetwork aggregation, aggregating multiple types of resources (including communications, data, and AI processing) for optimal connectivity at different scales; (3) sustainability, realizing energy savings and consumption reduction and promoting sustainability from the perspectives of environment, economy, and society; (4) global service coverage; (5) extreme experiences, including performance indicators such as connection speed, delay, and bandwidth capacity; (6) trustworthiness of 6G, ensuring the confidentiality and integrity of end-to-end communications and guaranteeing data privacy, network operational resiliency, and security (Hexa-X, 2020).

In June 2020, the "Society 5.0" was proposed in the Beyond Fifth-Generation (B5G) Promotion Strategy & 6G Development Roadmap released by the Ministry of Internal Affairs and Communications of Japan (MIC, 2020). It believes that the 2030 society vision is to achieve a dependable, inclusive, and sustainable society. The application scenarios of B5G/6G need to include ultra-enhanced mobile broadband (ultra-eMBB), enhanced ultra-reliable and low-latency communication (eURLLC), and ultra-massive machine-type communication (ultra-mMTC), and need to achieve ultra-low power consumption, autonomy, scalability, ultra-security, and resiliency (MIC, 2020).

Therefore, in the 6G era, security must be considered to be as important as communications, networks, and energy efficiency at the beginning of the system design. The simultaneous improvement and optimization of multiple performance objectives, such as communication, security, energy consumption, service, and efficiency, must be considered. The future network should be resilient, secure, privacy preserving, safe, reliable, and available under all circumstances; we must take generalized functional safety (safety, adaptability, autonomy, and reliability) as the bottom layer of the network architecture, establish an endogenous security model, and design the endogenous security network architecture of the next-generation communication network, as shown in Fig. 4.

The characteristics of 6G, such as network openness and integration, heterogeneous coexistence, ubiquitous interconnection, and intelligent reconstruction, pose comprehensive challenges to

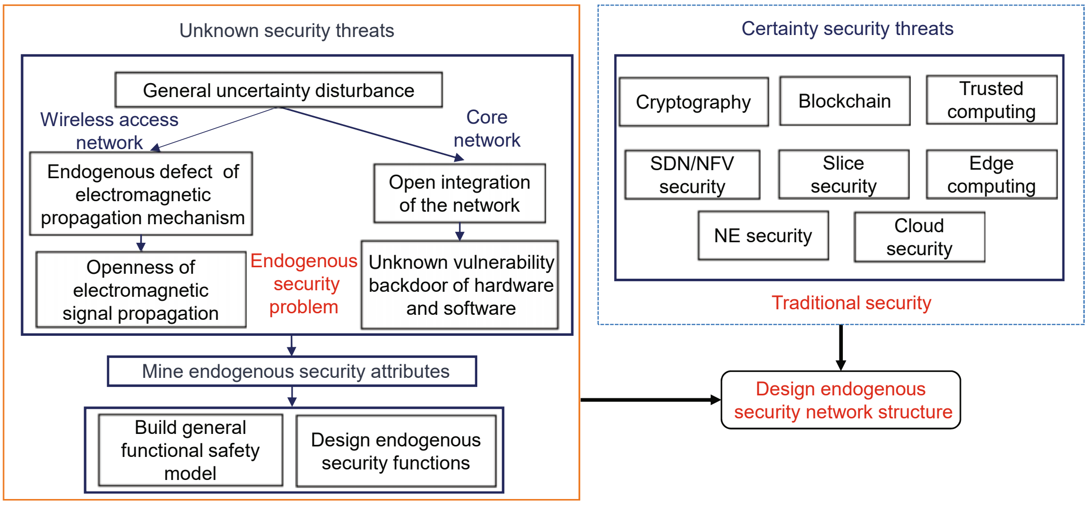
Unknown security threats
General uncertainty disturbance
Wireless access network
Core network
Endogenous defect of electromagnetic propagation mechanism
Open integration of the network
Openness of electromagnetic signal propagation
Endogenous security problem
Unknown vulnerability backdoor of hardware and software
Mine endogenous security attributes
Build general functional safety model
Design endogenous security functions
Certainty security threats
Cryptography
Blockchain
Trusted computing
SDN/NFV security
Slice security
Edge computing
NE security
Cloud security
Traditional security
Design endogenous security network structure

Fig. 4 Endogenous security network architecture (Jin et al., 2021a)

cyberspace security. It is urgent to combine security with network architecture and service design; 6G wireless transmission will be enhanced and evolve around ultra-high speed, ultra-wide coverage, ultra-large connections, ultra-low latency, ultra-high reliability, ultra-accurate positioning, and ultra-low energy consumption. In 6G, mobile communication and AI will develop together in a relationship of mutual intersection, mutual coordination, and mutual empowerment. The 6G network will support broadband full service and the Internet of Everything, as well as provide higher speeds, more connections, more reliable networks, and a broader coverage. Moreover, its interactive forms are more integrated and intelligent, and its network architecture and services are more secure and credible.

From the perspective of the long-term development trend of technology, 6G can be guided by the new paradigm of endogenous security development in cyberspace; it will consider the security of the underlying network and the upper application services as a whole, explore the endogenous security mechanism starting from the common native attributes of broad functional security and green communication network, build the endogenous security practice specification of communication and security integration, break the traditional paradigm of bare technical performance and security measures patch, and provide theoretical and technical supply for the construction of endogenous security 6G, resilient 6G, and trustworthy and scalable 6G.

Considering the possible architecture and characteristics of 6G networks, the following sections specifically give the potentially promising security theories, practice norms, and security technologies of the core network and wireless access network, as well as the integration mechanism of endogenous security, traditional security technology, and emerging enabling technology, under the guidance of the new paradigm of endogenous security.

4 Discussion on endogenous security for 6G core networks

The significant development trend of 6G network architecture is a more simplified design, a combination of centralized and distributed control, and ubiquitous access. The network architecture is more open and the network elements are more diverse, which brings network security risks and threats that are more difficult to identify and control, as well as unknown unknown attacks that are more difficult to prevent (Research Institute of CMC, 2020). In addition, the 6G network architecture shows the development characteristics of network of networks (Hexa-X, 2020), access-network-level and core-network-level multimodality has become the main development trend, and "customizable scenario" has become a key demand for interconnection. To address these trends, we need to study the endogenous security features of 6G core networks and provide new ideas for 6G core network development.

4.1 Major security problems faced by 6G core networks

The 6G core network is expected to face at least three main types of problems, as follows:

The first type is the security problems caused by the backdoor of software and hardware vulnerabilities in the context of deep integration of the 6G cloud and the network. Unlike the 5G core (5GC) network, which is simply moved to the cloud at this stage, the 6G core network will adopt a "cloud-native + microservice" architecture design. In the future open network environment, 6G core network functions will face two security threats: (1) The open-source software platform makes it difficult to avoid loopholes caused by defects and errors in design and implementation; Seventy-five percent open-source code libraries have security vulnerabilities, 49% of which are high-severity vulnerabilities (Synopsys, 2020). When a security problem occurs in open-source software, other open-source software that depends on it will be affected. This layer-by-layer dependency creates a very hidden and complex attack surface. (2) In the context of globalization of the information technology industry, it is impossible to achieve complete autonomy, control, security, and credibility at the supply chain level for any country, and it is difficult to avoid the problem of "being backdoored." Therefore, after the 6G network function is softwareized, it is necessary to focus on solving security problems, such as malicious attacks and information extraction initiated by attackers using software design vulnerabilities, and on how to suppress preset backdoors from taking effect through network structure design when network functions are untrusted.

Second, we come to the functional security issues brought about by the trend of mobile core network virtualization. In the 5G/6G era, operators and equipment providers must pay special attention to functional safety, such as the reliability and stability of the core network. On one hand, from the perspective of the entire development history of the core network, network cloudification naturally brings great challenges to the reliability and stability of the core network. Since more and more mobile communication network operators have chosen to deploy cloud-based core networks based on network function virtualization (NFV) after 2015, "black swan" events have occurred frequently and are significantly more than in the era of traditional core networks. On the other hand, network cloudification is continuing to deepen. Currently, the core network construction of operators is in the stage of optimization from virtualization to resource pooling, i.e., from "cloud-ready" to "cloud-native." It is expected that, in this process, operators and equipment providers will face more and more challenges in ensuring the reliability and stability of the core network.

Third, the single Internet protocol (IP) system will restrict the transmission performance of the 5G network in many aspects. At present, the 6G network user plane supports only IP-based routing and addressing, and it is difficult to meet the differentiated performance requirements of different application scenarios, such as the Internet of Things (IoT), industrial Internet, and satellite Internet, at the same time in actual use. For example, time-sensitive applications, location-sensitive applications, terminal power-limited applications, and other complex services pay more attention to the efficiency of network delay and operating power. Faced with the above requirements, the solutions given by the existing IP-based network architecture, such as virtual private network, network slicing, and edge computing, can serve only as a transition, which cannot fundamentally solve the problem. In the 6G era, there is an urgent need to break through the single-bearer technology development model of traditional networks, form a diversified network technology development paradigm that meets the needs of diversified vertical industries, and realize flexible and customizable information exchange through scenario-customizable interconnection technology. Polymorphic networks rely on abundant computing, storage, interconnection, transmission, and other resources to create a full-dimension definable network technology system and provide a technical environment for the unified bearing of multiple network systems (Wu JX and Hu, 2021). The above features are naturally in line with the data transmission requirements of the 6G network and are very suitable for building the user plane of the 6G core network.

4.2 State of 6G core network security and the polymorphic network

Against the background of the complex global industrial chain, all parties have paid great attention to network security in the development of 6G.

Domestic and foreign scientific research institutions, operators, and communication equipment manufacturers have released white papers one after another, proposing their visions for 6G network security. The United States, the EU, China, and other countries and organizations have also begun to lay out 6G network security research projects.

4.2.1 State of 6G core network security

1. Related works abroad

6G will support a variety of critical and personalized services in multiple application areas, including education, transportation, public health and security, and defense, making socioeconomic development even more dependent on the high availability, security, and reliability of such network systems. Current tools and techniques for network system design have not yet addressed network resilience in a comprehensive, integrated manner, resulting in unpredictable behavior due to various factors, such as security breaches, erratic updates, and incorrect system configurations. For this reason, many foreign scientific research institutions and equipment manufacturers have focused on research into the 6G elastic network. Governments and scientific research institutions in various regions, such as the United States, Europe, and Japan, have also listed generalized security concepts, such as security, resilience, and dependability, as the core vision for the list of early-launched projects of 6G. In addition, traditional security research works on topics such as privacy protection and security and trustworthiness are continuously evolving.

The National Science Foundation (NSF) of the United States launched the RINGS program for NextG network systems. The goal is to design NextG network systems from a different perspective with "resilience" as a primary consideration while pursuing superior performance. Resiliency enables network systems to adapt and recover quickly in the face of malicious attacks, component failures, and natural/man-made outages. The proposed potential technologies are as follows: (1) composable and programmable security; (2) zero-trust security; (3) formal verification of protocol implementation; (4) end-to-end slice security (NSF, 2021).

The Oulu University in Finland is one of the first universities to carry out 6G research. In March 2019, the Oulu University hosted the world's first 6G summit in Levi, Finland, and released the 6G security white paper "6G White Paper: Research Challenges for Trust, Security and Privacy" in June 2020, proposing to build a trustworthy 6G system, including the requirements of trust, security, and privacy (Ylianttila et al., 2020). Potential technologies proposed are software and AI-defined security.

Samsung has put forward the following requirements for the trustworthiness of 6G systems (Samsung, 2020): (1) a hardware-based security environment that provides secure operation and credential protection of software codes; (2) security by design to ensure that any hardware/software can be trusted; (3) increased transparency to ensure that the system recognizes how and when AI systems access any code, training data, etc. that are related to personal information; (4) provision of mechanisms to safely use user data and guarantee its privacy.

In the 6G security white paper "Security and Trust in the 6G Era," Nokia Bell Labs pointed out that 6G networks should have three characteristics: resilient network, privacy protection, and trustworthiness. This paper breaks down security-enabling technologies into the following categories: pervasive AI/ML, automated software creation, privacy-preserving technologies, and distributed ledgers.

Foreign academics have conducted in-depth research on the security requirements and challenges of 6G networks, focusing on key technologies such as security and trustworthiness, privacy protection, and AI/ML security.

The 6G network will build a human-centered intelligent service network, and network intelligence requires the support of a large amount of user data. Finding a balance between providing high-precision service and protecting user privacy will be a challenge (Porambage et al., 2021). Nguyen et al. (2021) believed that there are three main ways to achieve data privacy protection: reducing identity links in data collection, enhancing secure data storage, and controlling data sharing and use. Ziegler et al. (2021) summarized the key technologies of privacy protection in the 6G era, including multilateral computing, federated learning, blockchain, new lightweight encryption algorithms, homomorphic encryption (HE), and differential privacy (Synopsys, 2020).

Software vulnerability is one of the root causes of security problems in today's network and information technology systems, so it is very necessary to establish a secure and trusted 6G network environment. As pointed out earlier (An et al., 2021), 6G will be used to support vertical industries; therefore, customizable, provable, and measurable trustworthiness and security are essential features that it must have. One of the paradigm shifts of 6G networks is the transition from security to multilateral trust. The new 6G network system should support native trustworthiness and achieve end-to-end security and trustworthiness. Embedding trust in 6G networks will include the following key properties (Nguyen et al., 2021): maintaining the value of information sharing while preventing false/misbehaving sources, ensuring that the possibility of any malicious event is extremely low, and avoiding single point of failure. At the same time, it is pointed out that security-enabled technologies, such as blockchain, distributed ledgers, and zero trust, play an important role in building a secure and credible 6G network.

AI/ML will be used for services across 6G security architectures, processes, and technology domains. Nguyen et al. (2021) believed that AI/ML can play three roles in 6G security: defender, attacker, and breach. Although AI/ML has great potential in enhancing cybersecurity, the introduction of AI/ML in 6G also brings new threats. On one hand, AI/ML algorithms lack interpretability and trustworthiness. A large amount of training data, as well as their own vulnerabilities, makes them vulnerable to attacks, such as poisoning attacks, reverse attacks, adversarial attacks, and inference attacks. On the other hand, AI/ML can be used as a 6G attack tool to achieve more complex calculations and unexpected attacks, such as using deep learning to analyze Wi-Fi channel state information in high-density environments. Thus, how to make full use of AI/ML to ensure the privacy and security of 6G networks is also a difficult problem.

2. Related domestic works

The traditional mobile communication security method adopts a superimposed passive security mechanism, and security and communication have formed a pattern of mutual separation, which can no longer resist the potential ubiquitous attacks and uncertain security risks of the future 6G network. For this reason, many domestic scientific research institutions have pointed out that it is necessary to break the inertial thinking of traditional patching or additional security technology research and development and to explore the endogenous safety and security mechanism integrating security and communication.

The IMT-2030 (6G) Promotion Group released the “6G Network Security Vision Technology Research Report” (IMT-2030 (6G) Promotion Group, 2021). Starting from the driving force of development of 6G security, by analyzing typical 6G scenarios and their security requirements, it proposed “active immunity, elastic autonomy” 6G security, and a vision of “virtual symbiosis, ubiquitous collaboration;” it further outlined key security technologies, including AI security, blockchain security, lightweight access authentication, wireless physical layer security, software-defined security, data security, and encryption algorithm enhancement and other technologies.

China Mobile proposed five major features of the future 6G network: on-demand service, simplicity, flexibility, endogenous intelligence, and endogenous security (Research Institute of CMC, 2020). The endogenous network of 6G security monitors the security status in real time, predicts potential risks, and combines attack resistance with the prediction of dangers, thereby realizing intelligent endogenous security, i.e., “risk prediction, active immunity.” China Unicom pointed out that the security and trustworthiness of the 6G network includes two aspects, security and trustworthiness, and based on the external network security model of the 5G network, it emphasizes endogenous security and trustworthiness (Research Institute of CMC, 2021).

Wu JX (2022) put forward new theories and new methodologies to solve the common problems of endogenous security in cyberspace and the “unknown unknown” security threats. The new paradigm of endogenous security development contributes a replicable successful template for the field of cyberspace security and the new-generation information technologies such as 6G. ZTE Corporation et al. (2021) visualized the 2030+ network architecture, described the 2030+ network endogenous security vision based on the architecture, and put forward a unified definition of network endogenous security; they proposed the initial network endogenous security requirements and envisaged three developmental stages. As has been pointed out (CICT Mobile Communication Technology Co., Ltd., 2021), the traditional security trust model can no longer meet the security requirements of 6G networks. The new-generation communication services, such as 6G's intelligent connection of all things and sensory communication, require the provision of a multi-party and cross-domain security-and-trust system, which can support not only centralization but also the coexistence of multiple trust models of decentralization and distribution.

The domestic academic community has conducted in-depth research on the security threats, security vision, and security architecture of 6G networks, and has focused on key technologies such as endogenous security, software-defined security, blockchain, and zero trust.

It is difficult to ensure the security-embedded requirements of 6G itself in the traditional plug-in network security mechanism, and redesigning of the security protocols and mechanisms from the perspective of network architecture, apart from injecting the endogenous security mechanism of "cohesion and governance" and "self-reliance" genes into the 6G network, has been proposed (Liu Y and Peng, 2020). The endogenous security architecture and key technologies of 6G network are expounded. The architecture is divided into access-side security and network-side security. Access-side security is governed by "cohesion" to achieve "gatekeeper" security for the 6G endogenous security network. The security of the network domain provides the security and stability of the network from the inside out, which is an important aspect of "self-reliance;" key technologies include identity authentication technology, access control technology, communication security technology, and data encryption technology. Su et al. (2022) proposed a 6G security construction idea based on internal security capability construction, and designed a 6G endogenous security architecture, including the security capability layer, security policy controller, security intelligence center, security management center, collaborative trust consensus facility, orchestration capability, and AI capability. The architecture is based on the network's built-in security capabilities, with trust consensus mechanism as a link, and intelligent collaborative technology as a means to form the security architecture and the operation mechanism of active immunity, trust consensus, and collaborative flexibility. Zhang CL et al. (2021) summarized the vision and core technologies of 6G networks and described the possible security problems and challenges in 6G networks based on this approach. Then, according to the current state of the technologies, the solutions to these security problems were summarized, and the security model for 6G networks was discussed therein. Liu GR et al. (2021) built a software-defined 6G security architecture, which can form differentiated, definable, and rapidly deployable native security capabilities to achieve efficient linkage and synergy among security capabilities, business links, and customer needs. Gao et al. (2021) proposed a 6G network security vision from the aspects of endogenous security, elastic security, context-aware security, multi-dimensional data security, and evaluable security. Other works (Dai et al., 2020; Jiang et al., 2020; Nie et al., 2020; Wang et al., 2021) studied the application of blockchain in 6G, including data sharing and storage, privacy protection, data tracking, identity authentication, and information supervision.

In addition, as the mobile core network continues to transfer from the closed network to the open network, security requirements are changing from strong trust to weak trust or zero trust. The application scenarios, technical forms, network environment, and regulatory requirements of 6G networks will undergo profound changes, which will change the original trust relationship, network boundaries, and threat models. Prior work (Liu JH, 2020; CCSA, 2021) has examined the mobile network security requirements and architecture from the perspective of zero trust, carried out technical research on the application of zero-trust security in mobile networks, analyzed the needs of mobile network security, and studied the solutions and key technologies to meet zero-trust security to meet the requirements of mobile network security development. CCSA (2021) analyzed different objects such as 5GC service-based interface (SBI), N32 (reference point between two SEPPs) interface, multi-access edge computing (MEC) capability open interface, non-service-based interface, network management interface, and MEC scenario one by one. Focusing on the service based architecture (SBA) scenario, CCSA (2021) pointed out that other zero-trust security technologies can be used for reference to better meet the requirements of zero-trust security. It is recommended to enhance the following aspects: (1) refinement of the access policy to ensure least privilege access; (2) network layer dynamic whitelist; (3) single-packet authentication (SPA), hidden service entrance; (4) moving target defense, changing the attack surface of the server; (5) traffic detection and visualization; (6) continuous security assessment, security rating, and security management of the whole life cycle.

4.2.2 State of the polymorphic network

Inspired by the ecological theory of diversified species in species evolution and considering the diversified development trend of the current network technology system, Prof. Jiangxing WU proposed the fourth network development paradigm, to handle the problems of rigid structure, single IP bearer, and difficulty in suppressing unknown threats in the existing network architecture. In this paradigm, the network technology system and the supporting environment are separated (Wu JX and Hu, 2021). The Fourth Paradigm aims to break the traditional network development paradigm, either by adaptive evolution under the current rigid network architecture or by using a new rigid architecture as a step-by-step replacement methodology. The methodology of this paradigm is called a research status environment, being an integrated network support environment based on full-dimension definable technologies, which are symbiosis, coexistence, dynamic concurrency, evolution, and integration. It can not only ensure the self-sustaining development of various services and network technology systems but also realize the intelligent, efficient, and secure integrated deployment and management of polymorphic networks; it has a full-dimension definable physical environment and ecological environment that are not related to specific network systems and related services.

Wu JX (2018a) analyzed the endogenous security of a polymorphic network, seeking to solve the basic security problem from the perspective of "structure determines security;" moreover, Wu JX (2018a) believed that the endogenous security effect in a polymorphic network is achieved through the technical architecture based on generalized robust control. The architecture embodies the endogenous security effects of software and hardware systems formed by a generalized robust control architecture. Hu et al. (2019) elaborated the endogenous security architecture of a polymorphic intelligent network in more detail. According to the concepts of "structure determines security" and "system is greater than the sum of parts," it is believed that an endogenous security structure based on DHR should be implanted in polymorphic intelligent networks. Based on the "true relatively axiom" polymorphic decision-making strategy scheduling and negative feedback control mechanism, it can make the executive structure representation under the condition of functional equivalence uncertain, and realize the dynamic structure of the communication system, which can disrupt the attack chain, realizing the minimal operation management on the premise of ensuring the integrity of the original system network configuration, fundamentally suppressing random failures and human deliberate disturbances and then obtaining the endogenous security effect of the network.

Li JF et al. (2020) summarized the robust control technology of polymorphic intelligent networks. Aimed at uncertain factors such as random failure of network nodes/links and network function systems containing loopholes and backdoors, they studied a network's generalized robust control mechanism using a formal description method and evaluation method, introduced mechanisms such as dynamization, heterogeneity, redundancy, and dynamic reconfiguration at the network architecture level, studied a robust network construction architecture based on closed-loop negative feedback control, studied the dynamics, randomization, and isomerization methods of network elements such as network address, topology, and routing based on the uncertainty presentation of robust control construction, studied dynamic random scheduling, heterogeneity design, output vector strategy decision, and other key technologies, developed corresponding systems on typical network equipment environments, and studied how to effectively configure and implement robust control mechanisms at the data, platform, network, and operating environment levels to build a new robust network of "high reliability and high availability."

4.3 Practice concept of endogenous security for the 6G core network

From the perspective of the new paradigm of endogenous security in cyberspace, the application of endogenous security technology based on generalized robust control and polymorphic network technology in 6G core network security is analyzed, providing theoretical guidance for the design of 6G core network endogenous security solutions.

As shown in Fig. 5, the 6G endogenous secu-

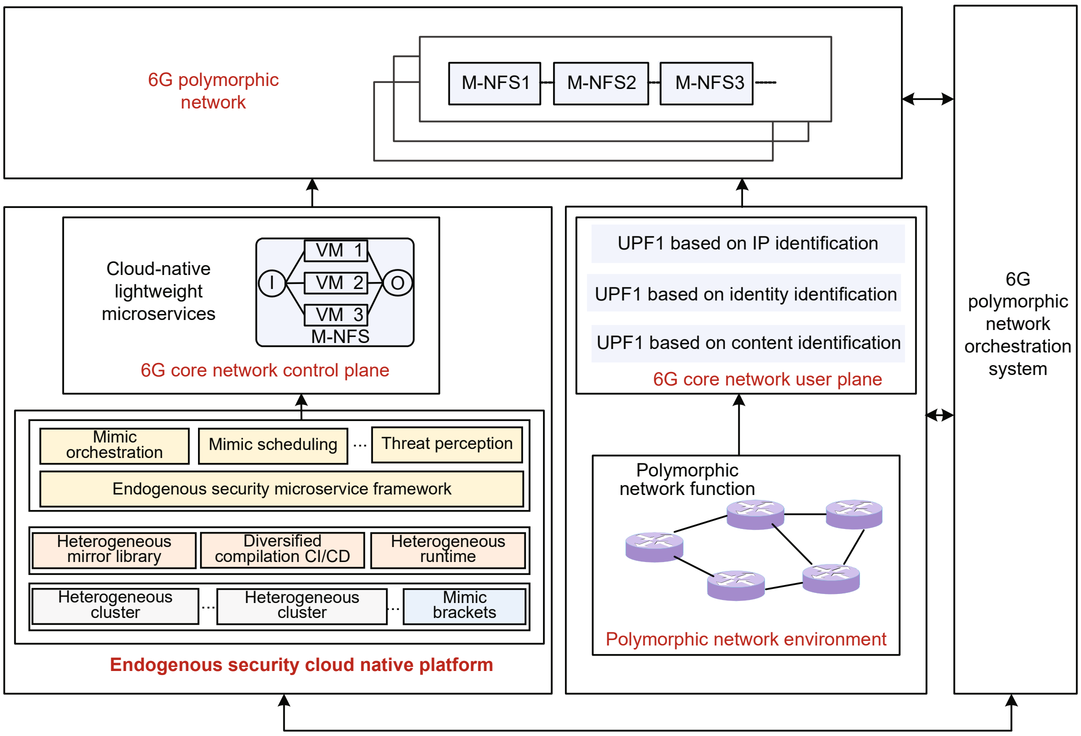
6G polymorphic network
M-NFS1
M-NFS2
M-NFS3
Cloud-native lightweight microservices
VM 1
VM 2
VM 3
I
O
M-NFS
6G core network control plane
Mimic orchestration
Mimic scheduling
Threat perception
Endogenous security microservice framework
Heterogeneous mirror library
Diversified compilation CI/CD
Heterogeneous runtime
Heterogeneous cluster
Heterogeneous cluster
Mimic brackets
Endogenous security cloud native platform
UPF1 based on IP identification
UPF1 based on identity identification
UPF1 based on content identification
6G core network user plane
Polymorphic network function
Polymorphic network environment
6G polymorphic network orchestration system

Fig. 5 The 6G endogenous safety and security core network

rity core network includes three parts: (1) the 6G core network control plane based on the endogenous security cloud-native platform; (2) the 6G core network user plane based on the polymorphic network environment; (3) the 6G network modal construction suitable for different application scenarios.

4.3.1 6G core network control plane based on the endogenous security cloud-native platform

The 6G core network control plane based on the endogenous security cloud-native platform includes two parts: the endogenous security cloud-native platform and the endogenous security control plane network function. Endogenous security cloud-native platform, as the basic environment of the 6G endogenous security core network, provides it with the basic platform capabilities of cloud computing and endogenous security. The endogenous security control plane network elements are carried on the cloud-native base, providing centralized authentication, management, control, and schedule for 6G network users, controlling the interconnection and information transfer with user access networks to realize data connection and service access.

1. Endogenous security cloud-native platform

The endogenous security cloud-native platform follows the concept of integrated design of functions and security and integrates endogenous security functions into the cloud-native platform, making it a basic capability of the cloud-native platform.

The endogenous security cloud-native platform architecture can be divided into infrastructure, cloud platform, and application layers. At the infrastructure layer, traditional cloud platforms generally manage the underlying computing, storage, and network resources in a unified manner to form cloud computing clusters. The endogenous-security cloud-native platform can not only manage multiple heterogeneous computing, storage, and network resources in a unified manner, forming multiple heterogeneous clusters, but also abstract and manage the mimic brackets (such as input agents and arbiters) in a unified manner to form a resource pool of mimic brackets to realize flexible allocation and elastic scheduling of endogenous security resources. Based on the infrastructure layer, the endogenous security cloud-native platform is centered on the container cloud orchestration and management framework Kubernetes, which integrates endogenous security modules, such as heterogeneous image repositories, heterogeneous runtimes, and diverse compilation pipelines, to provide basic support for endogenous security capabilities for upper-layer applications. Among them, the diversified compilation pipeline integrates the diversified compilation technology into the continuous integration (CI)/continuous deployment (CD) pipeline by transforming the cloud-native DevOps (a term formed by the combination of software "development" and "operations") to provide support for the heterogeneity of the mimic executives. In the diversified compilation pipeline, the heterogeneity of the application layer is improved by using different compilation strategies for the same source code; the heterogeneity of the execution body image is improved by using different basic environments to package the container images. Based on a diverse compilation pipeline, an application can automatically generate a large number of heterogeneous images through a single source code, providing a heterogeneous capability foundation for application mimicry. Above the cloud platform layer, an endogenous security microservice framework is formed by refining the common requirements of microservice mimicry. The endogenous security microservice framework is based on the application management controller mode of Kubernetes, and it integrates the DHR structure of mimic defense to provide a cloud-native mimic application management function. Users can implement fine-grained control and management functions of mimic applications by calling the application programming interface (API) entry of Kubernetes. Specifically, for cloud-native microservice applications, users can flexibly select microservices that need to be protected by mimic technology through configuration, to achieve flexible allocation and management of endogenous security capabilities. The endogenous security microservice framework can automatically provide basic mimicry capabilities for microservice applications, including mimicry architecture orchestration, selection of heterogeneous executives, timing executive rotation mechanism, and attacked executive rotation mechanism. Specifically, the endogenous security microservice framework can automatically generate a mimic microservice application with DHR structure according to the calling relationship between microservices in the microservice application and the microservices to be protected. When creating multiple heterogeneous executors, the heterogeneous attributes at multiple levels (such as the underlying computing nodes, container runtimes, and images) will be considered, and the plan with the largest degree of heterogeneity will be selected to create the executor. During the running process of the mimic application, the mimic control module will periodically rotate the execution body copy to confuse the attacker. At the same time, when the mimic arbiter senses that an execution body is under attack, it will notify the mimic control module to clean and rotate the attacked execution body. Through the above functions, the endogenous security microservice framework can manage the full life cycle of the mimic application and endogenous security capabilities for the application.

2. Endogenous security control plane network elements

One of the major trends in 6G networks is that they are organized through centralized and distributed coordination and distributed autonomy. On one hand, more network functions are extended to the network edge. On the other hand, the core functions oriented to the overall situation will be concentrated, and more complex services will be supported through cloud-network integration and distributed collaboration. The distributed and customized 6G network architecture can not only resist distributed denial-of-service (DDoS) attacks and reduce the risk of single point of failure but also provide customized strategies for each user. In the centralized control part of the core network, based on the endogenous security cloud-native platform, the cloud's microservice framework and middleware capabilities (such as message queues, database services, and heterogeneous computing management) are fully used to carry out the design of microservice functions, such as 6G core network control plane authentication, data management, mobility management, session management, and access control. At the same time, given the unknown security threats brought on by the design loopholes and backdoors of microservice functions, the DHR structure can be used to build endogenous security microservices. In the edge access part of the core network, 6G will establish distributed microcloud units with different functional levels. Each microcloud unit is self-contained with full control and data-forwarding functions. Multiple microcloud units can form autonomous micronetworks according to business requirements and provide targeted network services according to specific business scenarios, user scales, and geographic environments. To this end, blockchain technology can be combined to provide a secure and credible blockchain network for the 6G network distributed isomorphic microcloud units. The blockchain can dynamically adjust the resources of the microcloud unit and record and track the data-sharing content between nodes. The microcloud unit can provide computing and storage resources for the corresponding blocks to ensure the normal operation of the blockchain.

In addition, the 6G network's service-oriented architecture not only facilitates the deployment and update of service functions but also provides more convenient conditions for attackers to fake legitimate service functions to attack. To this end, the problems of identity spoofing attacks and unauthorized access to the data of the core network elements can be solved by combining the idea of zero-trust security. For example: (1) Strengthen API security protection according to the concept of hierarchical defense in depth. Each network function of the core network must have corresponding API protection capabilities to implement the preset API security policy to monitor, analyze, and limit API calls and generate alarms when abnormal API calls occur. (2) Based on the definition of 3$^{\text{rd}}$ Generation Partnership Project (3GPP) API and Resource, the concept of zero-trust security minimum authorization is adopted to further strengthen the granularity of network repository function (NRF) authorization and to achieve more refined permission control, which can effectively reduce the attack surface of lateral attacks.

4.3.2 6G core network user plane based on the polymorphic network environment

As the user plane network function of the mobile core network, the user plane function (UPF) is a basic capability of the mobile core network, a bridge connecting operators and vertical industries, and a key to the future 6G expansion of the industry market. At present, UPF supports only IP-based routing and addressing, and it is difficult to meet the differentiated performance requirements of different application scenarios, such as the IoT, industrial Internet, and satellite Internet at the same time. For example, in the field of industrial Internet, since many operational technology (OT) manufacturers use their private protocols in the internal production process, data transmission using mobile communication networks usually requires edge gateway devices to perform protocol encapsulation and conversion. The service traffic is continuously encapsulated and decapsulated in different networks, which greatly degrades the performance of the intermediate equipment and obliterates the characteristics of the respective network, and cannot form an integrated quality or schedule. Therefore, in the 6G era, it is urgent to break through the single-bearer technology development model of traditional networks and form a diversified network technology development paradigm that meets the needs of diversified vertical industries and realizes flexible and customizable information exchange through "scenario-customizable" interconnection technology.

Polymorphic networks rely on abundant computing, storage, interconnection, transmission, and other resources to create a full-dimension definable network technology system and provide a technical environment for the unified bearing of multiple network systems. Their mode of operation is as follows: dynamically load and run various existing or future network technology systems (including business, service, or management functions) in a modal form on a full-dimension definable network support environment; customize the software and hardware groups according to the modalities' state, packet format, routing protocol, switching mode, forwarding logic, service characteristics, operation and maintenance specifications, and security policies to realize the coexistence, independent evolution and transformation, and mode of multiple network modes in the same technical and physical environment, security isolation between states and endogenous security protection functions, and so on. The above characteristics of a polymorphic network environment are naturally in line with the data transmission requirements of the 6G network and are very suitable for building the user plane of the 6G core network.

As shown in Fig. 6, the user plane of the 6G core network, based on the polymorphic network environment, consists of basic platform functions, the network modal control system, and the UPF. The basic platform function is composed of polymorphic network function equipment, which constitutes the network infrastructure and realizes the processing and

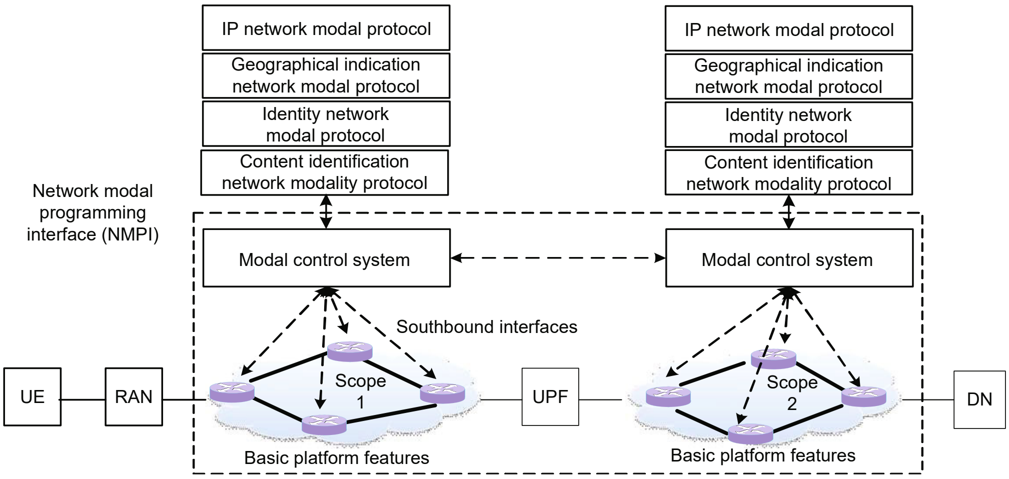
IP network modal protocol
Geographical indication network modal protocol
Identity network modal protocol
Content identification network modality protocol
IP network modal protocol
Geographical indication network modal protocol
Identity network modal protocol
Content identification network modality protocol
Network modal programming interface (NMPI)
Modal control system
Modal control system
Southbound interfaces
UE
RAN
Scope 1
UPF
Scope 2
DN
Basic platform features
Basic platform features

Fig. 6 The 6G core network user plane based on a polymorphic network environment

forwarding of various network modal data packets. The network modal control system performs modal management configuration on the "base," such as the structural configuration of the forwarding table and the configuration of the message format. Various network modalities implement protocol processing for each network mode through the protocol packet subscription/publishing interface. Based on the original functions, the UPF needs to support the forwarding and processing of packets in different protocol formats.

4.3.3 6G network modal construction suitable for different application scenarios

Through the 6G network modal orchestration system, the control plane network functions based on the endogenous security cloud-native platform and the user plane network functions based on the polymorphic network environment are arranged, and multiple logically independent virtual networks are divided for different application scenarios to meet their differentiated requirements in terms of function, performance, security, and so on.

On the control plane of the 6G core network, the microservices with endogenous security and general microservices are orchestrated together into network slices with endogenous security capabilities through the orchestration system (You W et al., 2020), as shown in Fig. 7. In each network function service (NFS) resource pool, the microservice functions are equivalent, but their security levels are different. There are both endogenous security microservices and general-purpose microservices. Therefore, at the level of control plane network slices, the endogenous security capabilities can be graded. For example, in low-level endogenous security slices, only some key microservices are required to have endogenous security capabilities, and other microservices are universal; in high-level endogenous security slices, all related microservices can be required to have endogenous security capabilities.

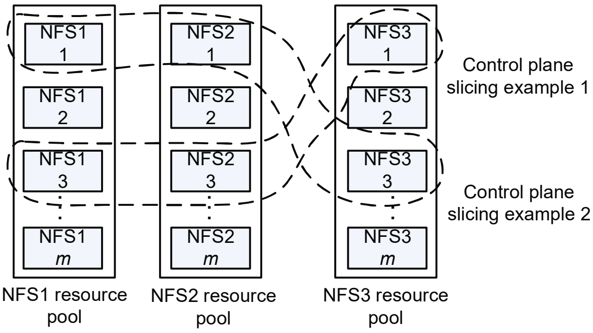

Fig. 7 Construction of control plane slice instances with different security levels (You W et al., 2020)

On the user plane of the 6G core network, through the linkage between the orchestration system and the modal control system, polymorphic network function equipment and UPF network function equipment that fit the application scenario are selected to fully meet the service data transmission performance requirements.

5 Discussion on endogenous security for 6G wireless access networks

Wireless communication systems face general uncertain disturbance because of inherent defects in electromagnetic propagation. To fundamentally overcome the endogenous security problems resulting from the wireless general uncertain disturbance, we must find the new safety and security attributes to establish the revolutionary security concept.

5.1 Wireless endogenous security problems

Due to the inherent openness of electromagnetic propagation, anyone within the broadcast range could eavesdrop on confidential information between legitimate transmitters and receivers in any unknown place and could also launch unknown wireless access attacks. For details, functional safety refers to the reliability of information transmission, and information security refers to the confidentiality and credibility of information sources in wireless communication systems. From the perspective of origin, the general uncertain disturbance affecting wireless communication security includes not only the natural disturbance factors such as terrain, landform, weather, random fading, and electromagnetic dispersion, but also artificial disturbance factors such as unintentional interference, intentional interference, and access attacks. Through the above analysis, we summarize the uncontrollability of electromagnetic propagation, as well as the reliability, confidentiality, and credibility of information transmission because of the general uncertain disturbance treated as the wireless endogenous security problems in this paper.

To overcome the wireless endogenous security problems caused by the wireless general uncertain disturbance, we must establish the innovative endogenous security scheme. As is known to all, the propagation mechanism of electromagnetic waves can be expressed by the Maxwell equation and boundary conditions. Specifically, the Maxwell equation is a common model of electromagnetic wave propagation. Its boundary conditions, which are strongly dependent on various electromagnetic propagation environments, determine the different solutions to the equation. Moreover, the electromagnetic propagation environment at different receivers is distinct. It means that the receivers at different locations have different boundary conditions, resulting in different solutions to the Maxwell equation. Hence, we can draw an interesting conclusion that the wireless environment has endogenous attributes for the wireless communication system. It essentially reveals that the space-domain resource is individual, totally different from the time-domain resource, frequency-domain resource, and code-domain resource. The significant entry point to overcome wireless safety and security problems is to explore and exploit the differences in the space-domain resources, which could break the public attribute constraint of the time-domain resource, frequency-domain resource, and code-domain resource. Consequently, using the naturally inherent differences of the space-domain resource to deal with wireless disturbances has become the main development trend for the mobile communication system.

5.2 State of wireless endogenous security

To explore and exploit the differences of the space-domain resource, novel schemes have been proposed for mobile communication systems from the third generation onward, including transceiver diversity, spatial equalization, and preequalization. To reduce the impact of random noise and burst fading, the currently outstanding technologies are proposed to combat natural disturbances, including diversity transmission/reception, beamforming, centralized or distributed multiple-input multiple-output (MIMO), and massive MIMO. In addition, outstanding technologies including cellular cells, smart antennas, space-division-multiple-access (SDMA), and space antijamming are given to resist artificial disturbances. The harmful interference could be suppressed by designing directional transmission and spatial filtering schemes. On the other hand, differences in the electromagnetic propagation environment are generally characterized by the properties of wireless channels. In fact, wireless channels could be regarded as a natural random number because it originates from the combination of line-of-sight, reflection, scattering, refraction, and other effects during the electromagnetic wave propagation. The above production mechanism determines that the channel fingerprint has some unique properties, such as the anisotropy at different places, the random time-varying nature, and third-party uncertainty relation. Based on the above concept, from the aspect of the electromagnetic wave propagation mechanism, physical layer security (PLS) schemes have been proposed in recent years which could achieve encryption and authentication in the physical layer through exploitation of the inherent security attributes, such as randomness, diversity, and time-varying nature. Thus, it will deal with the problems caused by both natural and artificial disturbances for wireless communication systems. Moreover, it could support the ability to defend against the "known unknown" security risks or "unknown unknown" security threats, thus achieving the integrated design on both security and communication. As shown in Fig. 8, due to different wireless signal propagation environments, wireless channel state information obtained by eavesdroppers and legitimate users at different locations is different. Designing a security mechanism coupled with channel state information could ensure that eavesdroppers cannot intercept information. Therefore, security enhancement can be achieved at the physical layer. Recent research on PLS among academic and industrial communities includes mainly physical layer key generation (Huang et al., 2020; Ebrahimi et al., 2021; Li GY et al., 2021), physical layer authentication (Chen et al., 2021; Perazzone et al., 2021; Xie and Hu, 2021), physical layer secure transmission (Zhang CW et al., 2021; Zhang YY et al., 2022), and physical layer secure coding (Cribbs et al., 2021; Choi et al., 2022). Based on the design concept, PLS is also called wireless endogenous security technology (Jin et al., 2021b). Wireless endogenous security unearths and uses the endogenous attributes and could design integrated schemes to achieve functional safety and information security based on the electromagnetic wave propagation mechanism (Dunkelman et al., 2014; ETSI, 2019). Consequently, wireless endogenous security will provide an innovative design idea for future wireless communication systems.

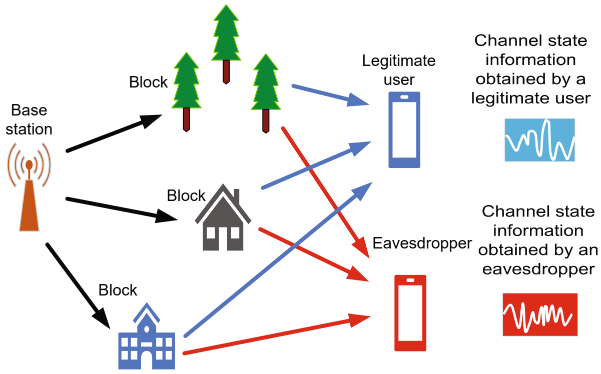
Base station
Block
Block
Block
Legitimate user
Channel state information obtained by a legitimate user
Eavesdropper
Channel state information obtained by an eavesdropper

Fig. 8 Wireless signal propagation process between the base station and users in a multipath environment (Jin et al., 2021a)

5.3 DHR structure for 6G wireless endogenous security

From the DHR structure in Fig. 1, we can conclude that a typical wireless communication system can be regarded as a natural DHR structure combined with an artificial structure, which has the original attributes of the DHR structure (Jin et al., 2021b). As illustrated in Fig. 9, the wireless channel, transmitter, and receiver are, respectively, equivalent to the heterogeneous executor, input agents, and output agents in the DHR structure. Specifically, for the wireless communication system, as the heterogeneous executor of the DHR structure, construction of different wireless channels (i.e., heterogeneous executor) is vital to the DHR structure through the dynamic transformation of the electromagnetic wave propagation environments. Hence, to achieve it, we must establish an endogenous structure based on endogenous attributes and shape the optimal environment against wireless disturbances. For the details, we can take into account the following aspects: (1) dynamic programming and reconstruction of the wireless environment to resist natural disturbances; (2) widening the differences by shaping the wireless environment to defend artificial disturbance; (3) transforming and strengthening the endogenous security attributes to fight against security threats.

Based on the above analysis, we can see that wireless endogenous security is the expansion of the endogenous security theory and DHR structure in wireless communication. Wireless endogenous security could provide theoretical guidance on the new paradigm to overcome problems related to wireless communication safety and security. Thus, it will provide the specification for the new paradigm implementation of wireless endogenous security in 6G.

5.4 Practice concept of endogenous security for 6G wireless access networks

The application of wireless endogenous security combined with reconfigurable intelligent surface (RIS) in 6G is summarized in the following subsections. The theoretical guidance on the wireless

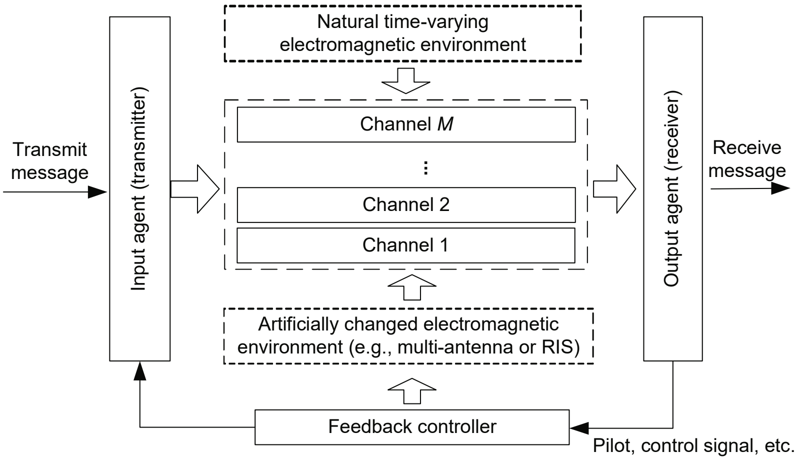
Natural time-varying electromagnetic environment
Transmit message
Input agent (transmitter)
Channel *M*
⋮
Channel 2
Channel 1
Output agent (receiver)
Receive message
Artificially changed electromagnetic environment (e.g., multi-antenna or RIS)
Feedback controller
Pilot, control signal, etc.

Fig. 9 Endogenous security structure model for wireless communication systems (Jin et al., 2021a)

endogenous security scheme design in typical application scenarios such as in ultrahigh-throughput communications, uRLLC, and mMTC could be given as follows. We hope that it can provide technical support for the intergenerational incremental effect of 6G wireless security.

5.4.1 RIS-enabled wireless endogenous security for 6G

As one of the potential candidate key technologies of 6G, RIS (Liang et al., 2021) could make it possible to control electromagnetic wave characteristics such as propagation direction, phase, amplitude, frequency, and polarization, through changes in the state of each particle unit using a field-programmable gate array (FPGA). Therefore, wireless environments could be dynamically programmed and reconstructed in real time by taking advantage of RIS, thus breaking space and spectrum limitations. In addition, the characteristics of RIS will strengthen wireless endogenous security through integration of material science and information science. Apart from exploiting the natural wireless environment and mining the endogenous security attributes, we could actively transform endogenous security attributes by reshaping the electromagnetic propagation environment, which could provide an available path to construct a controllable heterogeneous executor.

Using the flexible reconfigurable characteristics of RIS, we could construct the DHR array with space-time agile reconfigurable attributes. In other words, this array has the following unique attributes: different array elements have heterogeneous patterns at the same time; the same element has heterogeneous patterns at different times. Compared with the homogeneous array represented by massive MIMO in 5G, the antenna elements of the RIS-enabled DHR array could effectively improve the degree of freedom through dynamic agility and heterogeneous structure. The RIS-enabled wireless endogenous security scheme for 6G is shown in Fig. 10. According to the concept of "structural determinism" proposed previously (Wu JX, 2018b, 2020a, 2020b), the RIS-based DHR array can artificially construct wireless endogenous security attributes by reshaping the electromagnetic propagation environment. Based on the RIS-enabled DHR array, we could design generalized robustness to overcome uncertain disturbance problems at the physical layer, achieving the integrated design of functional safety and information security. Thus, it would provide a practice specification of the new paradigm of wireless endogenous security in 6G.

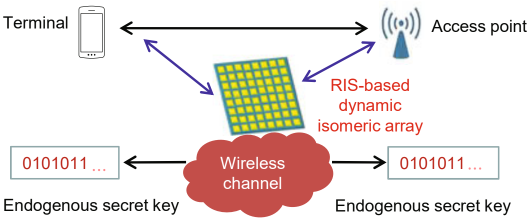

Fig. 10 RIS-enabled 6G wireless endogenous security solution (Jin et al., 2021a)

5.4.2 Wireless endogenous security for 6G ultrahigh-throughput communication

Based on the RIS-enabled dynamic heterogeneous array, the wireless channel could be optimized or even customized based on refined channel awareness. Meanwhile, high-speed security key generation will be achieved matching 6G ultrahigh-throughput communication, which will provide effective support for the wireless endogenous security implementation, with the following advantages but not being limited to these. First, fine-grained coding, modulation, filtering, and other signal transmission technologies matching each multipath could be designed when the differentiated wireless environment could be accurately analyzed (Jin et al., 2020). Meanwhile, more delicate channel characteristics could be extracted. Second, the difference between different channels could be enlarged by exploiting the RIS-enabled space-time degrees of freedom. Thus, it could improve the resolution of beamforming and the endogenous security key generation rate while improving the communication capacity. Third, it would improve wireless channel fingerprint security because it could enhance the randomness and time-varying nature of wireless channels or the noncorrelation between different channels. The above roadmap could also be applicable to uRLLC and mMTC scenarios. For example, we could design fine-grained signal transmission or processing technology to ensure reliable information transmission. At the same time, it could improve the key generation rate in the static environment (Jin et al., 2021a). We will not elaborate it here again.

5.4.3 Wireless endogenous security for 6G space-ground-integrated global coverage networks

Based on the existing 5G key technologies, it has become a consensus that 6G will build a space-ground-integrated global coverage network through integration of the space-time communication technology represented by satellites (CCID Think Tank Radio, 2020; You XH et al., 2021). However, due to the resource limitation on satellites, the exposure of key nodes (satellites), and other problems, the current security architecture for the space-ground-integrated global coverage network still follows the mobile communication network. Hence, the key security facilities are generally deployed at the ground gateway and the weakness of the existing protection capability is at the satellites for the space-ground-integrated global coverage network (Wu W et al., 2017). Nevertheless, wireless endogenous security technology could use endogenous security attributes of wireless channels to generate security keys to achieve authentication and encryption at the edge of the wireless communication network. Thus, wireless endogenous security not only protects the private key from being leaked when distributed in the public channel but also effectively reduces the resource consumption. It will strengthen and improve the security for the 6G space-ground-integrated global coverage network (Zhang J et al., 2014; Endo and Sasaki, 2019; Yin et al., 2022). However, due to limitations on the scattering paths for a single satellite-ground link, the diversity of different channels within the same beamforming coverage is a limitation. In this case, the endogenous key generation rate is very low because of the limitation on the space-time degree of freedom. Taking advantage of the dynamic agility of the RIS-based DHR, it could significantly improve the randomness of satellite-ground links and enlarge the difference between different channels by artificially controlling their wireless environments to modify wireless endogenous security attributes. Consequently, the RIS-based DHR will enhance the resolution of beamforming direction and overcome the insufficient endogenous key generation rate while improving the communication capacity. RIS-enabled wireless endogenous security provides security increment for the 6G space-ground-integrated global coverage network.

6 Integration of endogenous security and traditional security

6.1 Relations between endogenous security and traditional security

Endogenous security and traditional security are complementary to each other, as illustrated in Fig. 4. Targeting the explicit security requirements and known security threats in 6G, we can inherit and further develop the security techniques in 5G, concentrating on enhanced security for encryption, authentication, and integrity protection in traditional cryptography systems based on computational security to achieve “specific security immunity.”

Targeting the inherent drawbacks of the radio environment and the potential security threats introduced by the openness and integration of different network architectures, we can take advantage of the inherent characteristics of the wireless environment and investigate signal-level endogenous security techniques to achieve "non-specific security immunity." Forming an integrated defensive system through the integration of the two types of security techniques can not only achieve security in a malicious system with unknown security threats, but also provide accurate and efficient protection from known security threats (Wu JX, 2020a).

Endogenous security and traditional security can enhance each other. Taking full advantage of the accurate and efficient response to known attacks of traditional security techniques, we can deploy a defense system before an exception is discovered by the DHR judgment, or we can provide accurate troubleshooting, isolation, or cleanout for the exception. There are various types of traditional security techniques, and through intentionally distributed configurations, one can increase the heterogeneity of the executor and improve the ability of the DHR structure to resist common mode escape. By providing dynamic, differentiated, and smart configurations to different executors, endogenous security can provide nonlinear gain in the resistance against attacks in relation to traditional security techniques (Wu JX, 2018b).

6.2 State of traditional security techniques

At the time of writing, the Security Algorithms Group of Experts (SAGE) is evaluating efficient confidentiality and integrity algorithms for 5G. These algorithms need to satisfy mainly two requirements: providing a 256-bit security level to resist against quantum computing and providing a throughput of at least 20 Gb/s in software, which is the peak data rate for downlink transmission for 5G. The Advanced Encryption Standard (AES) is highly likely to be retained in 5G (but with the 256-bit version), as it has received special hardware support from the mainstream central processing units (CPUs), such as most Intel, AMD, and some ARM processors; thus, it can be highly efficient in software environments. SNOW 3G and ZUC need further investigation, as there exist academic attacks against them (Yang J et al., 2019, 2020) and they are not as efficient as needed in software (Yang J and Johansson, 2020). In response to 5G requirements, a new member of the SNOW family, called SNOW-V (Ekdahl et al., 2019), as a successor of SNOW 3G, was proposed in 2019 and is currently under evaluation in SAGE.

As the 6G vision is not clear yet at this moment, the exact requirements of confidentiality and integrity based algorithms for 6G are not clear. What can be expected is that at least two suits of algorithms based on different constructions will be prepared such that even if one was found to have some potential weaknesses, the backup one can still be safe. The security level of the cryptographic primitives in 6G is expected to be of 256 bits, while the required throughput can be much higher. The very initial vision about 6G is that it can provide a peak data rate of 100 Gb/s for downlink transmission, which, however, looks a little bit ambitious at this moment. At the same time, 6G will be more virtualized and cloudified than 5G, and this requires the confidentiality and integrity based algorithms in 6G be more software-efficient.

The research and applications of cryptography in 6G will closely follow the development of the cryptography community, with trends in post-quantum cryptography (PQC), lightweight cryptography (LWC), and more advanced cryptographic algorithms and protocols to provide security in different aspects.

6.2.1 Post-quantum cryptography

PQC includes cryptographic primitives that can provide resistance against quantum computing, which is the development direction of future cryptography. Though PQC is not yet implemented in the 5G system, 3GPP did mention in the 5G specification document to replace existing public-key infrastructure (PKI) with the quantum-safe one (3GPP, 2019). As the secure data transmission mode over wired connections in a mobile communication system based on Internet protocol security suite/Internet key exchange version 2 (IPsec/IKEv2) (Internet Engineering Task Force, 2019) and/or transport layer security (TLS) (Network Working Group, 2019), the adoption of PQC will closely follow the development of Internet security, which can be expected in 6G.

In 2016, the National Institute of Standards and Technology (NIST) initiated a PQC competition to solicit and select PQC primitives. The finalists and alternatives, which include key encapsulation mechanism (KEM)/encryption and signature algorithms, have been announced in 2020, as shown in Table 1. Among the seven finalists, five are lattice-based primitives, which can be the most promising construction for PQC. NIST will announce the fourth-round candidates for further investigation, and the final standardization can be expected in 2022–2024.

There are many research activities targeting the integration of PQC into existing security protocols. For example, the Internet Engineering Task Force (IETF) has already been working on Internet drafts that integrate PQC algorithms into existing IKEv2 and TLS protocols. Some research teams, e.g., Google, Cloudflare, Cisco, Microsoft, and Amazon, are also experimenting on PQC algorithm integration in TLS, primarily on PQ key exchange and PQ signature algorithm integration. For example, Google, in collaboration with Cloudflare, uses two NIST PQ KEM candidates, NTRU-HRSS and SIKE, in Google Chrome to test the hybrid key exchange in TLS 1.3. After the announcement of the finalists and alternatives, many research teams have been working on prototyping PQ Internet security protocols with these announced primitives, e.g., the PQClean and Open Quantum Safe (OQS) projects.

The design and choice of PQC algorithms should take into account the effect on the network performance, e.g., the latency and computation overhead introduced by the integration of PQC algorithms. The computation capabilities of devices should also be considered. Due to the relatively high speed and low overhead, lattice-based PQC algorithms have received more attention and evaluation, especially about the performance of the NIST finalists in different applications and devices. Besides, lattice-based PQC algorithms have relatively high efficiency and small key/ciphertext/signature sizes, and might be the most promising solution for public key cryptography (PKC) infrastructure for IoT, e.g., NTRU (Cheng et al., 2017; Fernández-Caramés, 2020).

6.2.2 Lightweight cryptography

LWC is the primary solution for securing IoT. LWC primitives can be categorized into ultra-lightweight, low-cost, and LWC algorithms (Hatzivasilis et al., 2018; Dhanda et al., 2020). The ultra-LWC primitives (e.g., SIMON) are targeted for use in extremely constrained devices (e.g., in radio-frequency identification (RFID) tags), which typically require only up to 1000 gate equivalents (GEs). Low-cost algorithms (e.g., PRESENT, Grain) can take up to 2000 GEs and can be used in devices with higer capabilities (e.g., ATmega 128 platform). General LWC algorithms target to achieve better performance with less implementation cost compared with AES.

In 2015, NIST initiated a competition for LWC to solicit and select LWC primitives intended for use in resource-constrained devices. In March, 2021, NIST announced 10 finalists of the LWC competition, which are listed in Table 2. Five out of the 10 finalists are built on the sponge construction, four are block ciphers, and only one is a stream cipher. The software benchmarks are tested under several different microcontrollers with different capabilities by the NIST LWC group (Turan et al., 2019), and Table 2 shows the results under two different platforms: ATmega328P with an 8-bit CPU and nRF52840 with a 32-bit CPU. One can see that the speeds under the two platforms have large gaps, especially for ASCON, Xoodyak, GIFT-COFB, and SPARKLE, which perform particularly well on 32-bit platforms. PHOTON-Beetle achieves the smallest code size on 8-bit platforms. Software performance benchmark tests were also conducted under the ECRYPT Benchmarking of Cryptographic Systems (eBACS) framework for these ciphers, but on general-purpose processors from Intel (Vampire, 2016), AMD, AMR Cortex-A, and Qualcomm. ASCON and Xoodyak outperform other candidates on 64-bit platforms, which can achieve speeds up to the order of Gb/s. The hardware benchmark results are from the FPGA implementations on the Xilinx Artix-7 platform (NIST, 2021). The area is measured using look-up tables (LUTs), and the speeds are for encrypting 16-byte messages with 16-byte additional data. The results of the Grain-128AEAD algorithm are taken from Sönnerup et al. (2019), who used the number of GEs to evaluate the area.

ASCON and Xoodyak perform the best in terms of throughput, while TinyJambu and Romulus have the most compact implementations, which cost fewer than 1000 LUTs. In practice, one can choose suitable primitives based on the capabilities of platforms to design security protocols based on different requirements from different networks. For some advanced and sensitive applications, e.g., medical system and military applications, more advanced primitives can be combined, e.g., using blockchain for user privacy protection and spectrum sharing.

6.2.3 Other cryptographic primitives and protocols

Blockchain is a distributed ledger technique that can build trust and consensus among nodes in a peer-to-peer (P2P) network. It relies on node consensus to guarantee informational consistency in an untrusted environment, so that all nodes store the same transaction information. It also uses cryptographic primitives such as digital signature and hashing to provide security of the distributed networks. Blockchain is a very promising cryptographic technique and using it to build 6G distributed wireless networks is a novel and hot research direction (Nie et al., 2020). Currently, there are many research groups targeting research on blockchain for wireless networks, e.g., blockchain protocols for optimizing and improving existing consensus algorithms, blockchain modeling for IoT, and theoretical analysis of performance and security in terms of aspects such as throughput, latency, and attacking probabilities (Li YX et al., 2020; Wang et al., 2021; You XH et al., 2021). Blockchain is still in the research phase, and there are no standards established yet, thus facing various problems and challenges. First, the consensus scheme determines the performance of the blockchain system, while existing consensus schemes have different drawbacks. The three main consensus algorithms, i.e., proof of work (PoW), proof of stake (PoS), and practical Byzantine fault tolerance (PBFT), are presented in Table 3 (Nie et al., 2020). PoW consumes large computation resources but still has low throughput; PoS reduces the computation resources and improves the throughput but can introduce oligopolies, running counter to the fundamental idea of decentralization. PBFT has extreme

Table 1 Finalists and alternatives of the NIST PQC Competition (NIST, 2020)

Type	Mechanism	Scheme	Algorithm	Summary
Finalists	KEMs/ Encryption	Code-based	Classic McEliece	Short ciphertext but large public-key size, suitable for applications with short ciphertext while not suitable for Internet protocols
		Lattice-based	CRYSTAL-KYBER	Small public-key size, balanced performance in different aspects, potential decryption failures, can be used for TLS protocols, not recommended for offline decryption
			NTRU	Small public-key size, high speed, balanced performance in different aspects, long history of study, potential decryption failures, security not comparable to other lattice-based algorithms
			SABER	Balanced performance in different aspects, lightweight, potential decryption failures, can be used for general applications
	Signatures	Multivariate-based	Rainbow	Fast signature verification, large public-key size, not suitable for general applications
		Lattice-based	CRYSTALS-DILITHIUM	Easy implementations, balanced performance in different aspects, further security investigation needed
			FALCON	Minimum bandwidth requirement, high efficiency, difficult implementations, low key generation rate, good overall performance
Alternatives	KEMs/ Encryption	Code-based	BIKE	Balanced performance in different aspects, can be used for general applications, further security investigation needed
			HQC	High key generation and decryption rate, well-studied cryptanalysis, large public-key and ciphertext, potential decryption failures
		Lattice-based	FrodoKEM	Least amount of structure, less key generation time, smaller public-key size, far worse performance in all metrics than other lattice schemes
			NTRUprime	No decryption failures, security needs further investigation, can be used for many Internet protocols
		Isogeny-based	SIKE	Minimum public-key size, very small ciphertext, relatively bad performance
	Signatures	Multivariate-based	GeMSS	Minimum signature size, fast verification, relatively large public-key size, slow deployment, not suitable for low-end devices
		Symmetric-primitive-based	Picnic	Small public-key size, large signature size, performance and security need improvement, slow signing and verification
			SPHNICS+	Least likely to be broken, low speed, relatively large signature size

communication overhead and limited system expansion. Therefore, the design of consensus algorithms will be a technical challenge for blockchain. Second, in practical blockchain, consensus nodes have different capabilities and different security levels of protection (Han X et al., 2019), which introduces difficulties in matching between distributed architectures and blockchain consensus. The matching and joint optimization between blockchain and the practical network needs further investigation. Lastly, blockchain itself faces problems and challenges, and more research into integration with wireless communication, edge/fog computation, fundamental theory, and key techniques is required to promote the applications and development of blockchain in 6G (Li C et al., 2019; Nie et al., 2020).

Another very useful—though not so mature—cryptographic technique for IoT is HE (Kumarage et al., 2016; Loukil et al., 2021). As many IoT devices are resource-constrained without strong computing capabilities, the data are usually outsourced to some third-party clouds. However, these clouds may not be trustworthy and users want to keep the data private, especially for sensitive information such as medical information. HE allows users to send specially encrypted data to the clouds while still being able to perform evaluation directly on the encrypted data when needed. The evaluation results will be the same as the ones over the plaintext, and any other entity has no access to the data. Currently, the main obstacle of HE for practical applications is the expensive overhead. For example, it can take minutes, hours, or even more time to encrypt a short message (Acar et al., 2019). If this problem can be solved, HE can play a significant role in IoT.

Multi-party computation (MPC) can also be important in IoT. In many IoT applications, multiple parties need to evaluate each other's data to make better policy decisions while keeping their own data private (Guan et al., 2022). MPC allows several entities to compute a public function over their data without revealing data to others (Zhao et al., 2019). Blockchain typically focuses more on the verifiability, while MPC targets more on the confidentiality of messages during computation; therefore, the two techniques can be complementary to each other. How to integrate MPC with quantum HE and introduce quantum bit commitment to design a PQ multi-party secure computation protocol is one future research direction.

Table 2 Some benchmark results of LWC shortlisted algorithms (NIST, 2021)*

Cipher	Algorithm	Software implementations				Hardware implementations	
		ATmega328P		nRF52840		Xilinx Artix-7	
		Code size	Speed	Code size	Speed	LUT	Speed
Sponge-based cipher	ASCON	3662	17.0	1392	589.9	1790	538.3
	Elephant	6740	3.4	2600	7.6	1291	66.8
	ISAP	3742	3.1	1728	50.1	3491	60.1
	PHOTON-Beetle	1596	10.3	3124	67.0	2065	207.1
	Xoodyak	2906	19.4	3252	825.8	1355	394.1
Block cipher	GIFT-COFB	2948	24.6	1504	514.1	1041	225.6
	Romulus	4814	11.0	3256	181.8	953	209.4
	SPARKLE	3944	35.0	1688	948.1	3071	94.9
	TinyJambu	3106	15.8	888	452.3	591	105.1
Stream cipher	Grain-128AEAD	9600	6.5	2088	186.0	3347GE	1020

*ATmega328P: 8-bit AVR processor, 16 MHz, 32 KB flash, 2 KB random access memory (RAM); nRF52840: 32-bit ARM Cortex-M4 processor, 64 MHz, 1 MB flash, 256 KB RAM; code size is in bytes, software speed is in kb/s, and hardware speed is in Mb/s. GE: gate equivalent

Table 3 Performance comparison of different consensus algorithms (Guan et al., 2022)

Consensus algorithm	Type	BFT	Transaction fee	Throughput (Tb/s)	Latency
PoW	Public blockchain	<51% computing power	Yes	7	High
PoS	Public blockchain	<33% total assets	Yes	100	Low
PBFT	Consortium blockchain	<33% total votes	No	200–2000	Low

7 Integration of endogenous security and emerging enabling technologies

There is no doubt that 6G will further integrate AI, big data, and other types of emerging enabling technologies, but these technologies will inevitably lead to new security threats while bringing improved communication performance. Studying the integration mechanism of endogenous security and 6G emerging technologies can effectively solve the security problems caused by emerging technologies. At the same time, the use of enabling technologies to support endogenous security attributes can empower and enhance endogenous security. This section takes AI technology as an example to introduce the integration of endogenous security and AI technology.

7.1 Threat and empowerment of AI to 6G security

In recent years, AI technology represented by deep learning has been successfully applied to many scenarios of 5G. In many cases, AI can be used not only to violate the security and privacy of users but also to protect system security and user privacy. AI technologies such as deep learning are unexplainable and non-inferential, and their own security also has many problems. Therefore, with the gradual advent of the 6G era and the development and evolution of AI technology, AI will play a more important role in 6G security. However, the combination of 6G and AI will be a double-edged sword. How to give full play to the positive role of AI technology, as well as defend and avoid the negative impact of AI, so as to promote the healthy development of 6G, is the direction worthy of key research in the next step (Siriwardhana et al., 2021).

7.1.1 AI-based attack technologies threaten 6G security

The threats of AI to 6G security are reflected mainly in the following aspects. First, due to the large-scale data analysis capabilities of AI, combined with the speed of future computers and the automation needs of future networks, AI-based attack techniques can easily endanger privacy. The 6G network needs to collect a large amount of user data through billions of devices, and users cannot foresee how external systems will process their data. For example, intelligent authentication systems rely on physical devices (Fang H et al., 2019) and can use private user data. Unsafe IoT devices (such as low-power sensors) input personal data into the AI system, which may cause data leakage. Moreover, the installation of a powerful security protection system on some performance-restricted IoT devices puts a major test on their performance. Model inversion attacks retrieving training data on ML may also lead to infringement of user privacy (Sun et al., 2020). The second is that AI helps achieve intelligent and precise attacks (Fang BX et al., 2021). For example, AI technologies based on ML and deep search can improve attack capability, realize automatic detection of target objects, and develop intelligent and precise attack strategies. In addition, due to the ability of network-wide intelligent decision-making based on distributed edge architecture, AI-based attack systems can learn data patterns in large amounts of data at different levels, such as smart radio, edge, and cloud. Therefore, AI-based attack techniques make it easier to analyze and discover various security vulnerabilities in the 6G system. For example, AI systems can learn the most vulnerable IoT device and launch DDoS attacks against their key nodes (Benzaïd and Taleb, 2020). Third, AI technologies represented by deep learning have their own unique security threats. It is also easy to make the 6G system combined with AI susceptible to exploitation by attackers. Data poisoning, such as data injection, will destroy the training phase of the ML system, resulting in inaccurate model training. Adversarial attacks try to fool AI systems with carefully designed adversarial examples during the inference phase. Model extraction attacks, reverse attacks, and member inference attacks use API to attack ML models.

7.1.2 AI-based defense technologies empower 6G security

AI is reasonably applied to the physical layer, connection layer, and service layer of 6G, which helps enhance the capabilities of analysis, decision-making, and response of the 6G system to deal with security threats, and will fully empower 6G security (Nguyen et al., 2021). AI technology can be used at the physical layer to assist the channel coding processing, enhance the randomness of physical layer key generation, improve the beamforming alignment effect, enhance the physical layer authentication strength, improve the anti-interference ability, and so on. At the connection layer, AI technology can be used for identity verification, intrusion detection, protocol vulnerability detection, encrypted traffic detection, and so on. At the service layer, AI technology can be used to perform biometric authentication, malware detection, trusted program verification, edge/cloud control verification, container operation protection, and so on.

In addition, a safe AI system can be realized based on adversarial training and moving target defense. Specifically, it includes robust training, such as input verification against poisoning attacks, adversarial training and defense distillation against adversarial attacks, and differential privacy and HE against API attacks. Among them, the balance between defensive capability and system performance is currently one of the biggest challenges in designing defense mechanisms (D'Aquin et al., 2018).

7.2 Integration concept of 6G endogenous security and AI

From the perspective of the new paradigm of endogenous security, in this subsection we analyze the key directions for further research on 6G AI security and provide theoretical guidance for the design of 6G AI endogenous security solutions. The current defense methods against the endogenous security problems of AI rely strongly on the prior knowledge of known threats, and there is still no effective means to deal with "known unknown threats" and "unknown unknown threats." The research idea of academia and industry is still dedicated to exhausting the endogenous security issues of AI. To deal with unknown threats under the unexplainable scenario and change the current patched passive defense mode in academia and industry, it is necessary to introduce new security concepts. On the other hand, one of the prerequisites for the high success rate of the attacker is to have a certain understanding of the target AI system's architecture and parameters, and the attacker will also change or even adapt the attack methods according to the defense methods deployed by the defender. So, we can try to introduce the dynamic heterogeneous redundant gene of endogenous security into the 6G AI application system, and an endogenous security model based on the DHR structure is established in the 6G AI model, as well as its key software and hardware, including the following three aspects in detail:

1. Establish endogenous security theory and security architecture under the 6G AI environment. Starting from the three aspects of endogenous security theory's safety vision—"endogenous," "not-based on prior knowledge," and "dealing with the unknown," we can analyze the endogenous security genes that 6G systems may have, and explore whether there are new endogenous security genes. On this basis, combined with the specific implementation links of 6G AI, we can study the effectiveness law of different endogenous security genes acting on different levels of 6G AI, and systematically establish the endogenous security theory and architecture of the 6G AI environment.

2. Build endogenous security protection mechanisms and methods under the 6G AI environment. After exploring the endogenous security theory and architecture in the 6G AI environment, we can combine the specific implementation links of 6G AI to build effective technical mechanisms and methods for different protection needs so as to ensure that the system performance is not significantly affected while meeting the safety performance requirements. For example, adversarial training is the current more effective defense method against adversarial attacks (Goodfellow et al., 2015). Although better system security can be achieved, performance is greatly affected. Based on the specific links of 6G AI, we can explore the introduction of diversity training methods into the architecture (Kariyappa and Qureshi, 2019; Pang et al., 2019; Sharif et al., 2019; Yang HR et al., 2020), use a variety of AI open-source frameworks (such as Caffe and TensorFlow) and models (such as VGG16 and random forest), or introduce a dynamic neural network (Han YZ et al., 2021), so as to integrate dynamic, heterogeneous, redundant, and polymorphic safety genes at different levels to establish endogenous security models and methods. The model parameters can be dynamically adjusted according to different inputs, or multiple sub-models can be dynamically rotated according to the feedback, so that the classification boundary of the entire 6G application system changes dynamically, and the attacker cannot find the optimal value of attack perturbation.

3. Design measurement, verification, and evaluation of the effectiveness of endogenous security technologies in the 6G AI environment. The evaluation

of endogenous security theories and methods in the 6G AI environment must be fundamentally different from that of general additional security protection technologies. Therefore, it is necessary to explore the security gain measurement and effectiveness evaluation methods of various endogenous security protection technologies in the 6G AI environment, including testing its ability to defend against unknown threats and heterogeneity between sub-models according to the transferability of attacks between sub-models within the architecture. The endogenous security protection technology test platform and tool library should be built in the 6G AI environment to support empirical research on the endogenous security protection theories and methods of the 6G AI environment.

8 Conclusions

6G security will focus on the requirements of high reliability, high availability, high controllability, high confidentiality, high privacy, and so on, and explore the basic theories and key technologies of 6G cyberspace endogenous security for machine communication, ubiquitous networking, wireless transmission, and space-ground integration.

This article takes the new paradigm of cyberspace endogenous security as a guide, and proposes corresponding endogenous security concepts for the 6G core network, wireless access network, and emerging enabling technologies, and also summarizes the integration development needs of endogenous security and traditional security, expecting to provide reference for the integrated development of technical performance and security control for 6G.

Contributors

Xinsheng JI initiated the work. Xinsheng JI, Jiangxing WU, Liang JIN, and Kaizhi HUANG drafted the paper. Yajun CHEN, Xiaoli SUN, Wei YOU, Shumin HUO, and Jing YANG helped organize the paper. Xinsheng JI, Jiangxing WU, Liang JIN, Kaizhi HUANG, Yajun CHEN, Xiaoli SUN, Wei YOU, Shumin HUO, and Jing YANG revised and finalized the paper.

Compliance with ethics guidelines

Xinsheng JI, Jiangxing WU, Liang JIN, Kaizhi HUANG, Yajun CHEN, Xiaoli SUN, Wei YOU, Shumin HUO, and Jing YANG declare that they have no conflict of interest.

References

3GPP, 2019. Technical Specification Group Services and Systems Aspects; Security Aspects; Study on the Support of 256-bit Algorithms for 5G (Release 16), TS 33.841 (V16.1.0). 3$^{\rm rd}$ Generation Partnership Project.

Acar A, Aksu H, Uluagac AS, et al., 2019. A survey on homomorphic encryption schemes: theory and implementation. *ACM Comput Surv*, 51(4):79. https://doi.org/10.1145/3214303

An XL, Wu JJ, Tong W, et al., 2021. 6G network architecture vision. Joint European Conf on Networks and Communications & 6G Summit, p.592-597. https://doi.org/10.1109/EuCNC/6GSummit51104.2021.9482439

Benzaïd C, Taleb T, 2020. AI for beyond 5G networks: a cyber-security defense or offense enabler? *IEEE Netw*, 34(6):140-147. https://doi.org/10.1109/MNET.011.2000088

CCID Think Tank Radio, 2020. 6G Concept and Vision White Paper (in Chinese). https://m.thepaper.cn/baijiahao_6596926 [Accessed on Mar. 18, 2020].

CCSA, 2021. Research on Zero Trust Security Applied in Mobile Network (in Chinese). https://www.ccsa.org.cn/ [Accessed on June 20, 2021].

Chen SL, Pang ZB, Wen H, et al., 2021. Automated labeling and learning for physical layer authentication against clone node and Sybil attacks in industrial wireless edge networks. *IEEE Trans Ind Inform*, 17(3):2041-2051. https://doi.org/10.1109/TII.2020.2963962

Cheng C, Lu RX, Petzoldt A, et al., 2017. Securing the Internet of Things in a quantum world. *IEEE Commun Mag*, 55(2):116-120. https://doi.org/10.1109/MCOM.2017.1600522CM

Choi J, Joung J, Cho YS, 2022. Artificial-noise-aided space-time line code for enhancing physical layer security of multiuser MIMO downlink transmission. *IEEE Syst J*, 16(1):1289-1300. https://doi.org/10.1109/JSYST.2021.3075721

CICT Mobile Communication Technology Co., Ltd., 2021. Global Coverage Scene Intelligent Connection—6G Scenes, Capabilities and Technologies Engine White Paper (V.2021) (in Chinese). https://www.cict.com/portal/article/index/id/921/cid/13.html [Accessed on Dec. 29, 2021].

Cribbs MR, Romero RA, Ha TT, 2021. Alternative codes and phase rotation extensions for alternating space-time coding-based physical layer security. *IEEE Open J Commun Soc*, 2:1123-1143. https://doi.org/10.1109/OJCOMS.2021.3075910

Dai YY, Zhang K, Zhang Y, 2020. Blockchain empowered 6G. *Chin J Int Things*, 4(1):111-120 (in Chinese). https://doi.org/10.11959/j.issn.2096-3750.2020.00154

D'Aquin M, Troullinou P, O'Connor NE, et al., 2018. Towards an "ethics by design" methodology for AI research projects. Proc AAAI/ACM Conf on AI, Ethics, and Society, p.54-59. https://doi.org/110.1145/3278721.3278765

Dhanda SS, Singh B, Jindal P, 2020. Lightweight cryptography: a solution to secure IoT. *Wirel Pers Commun*, 112(3):1947-1980. https://doi.org/10.1007/s11277-020-07134-3

Dunkelman O, Keller N, Shamir A, 2014. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. *J Cryptol*, 27(4):824-849. https://doi.org/10.1007/s00145-013-9154-9

Ebrahimi N, Kim HS, Blaauw D, 2021. Physical layer secret key generation using joint interference and phase shift keying modulation. *IEEE Trans Microw Theory Techn*, 69(5):2673-2685. https://doi.org/10.1109/TMTT.2021.3058183

Ekdahl P, Johansson T, Maximov A, et al., 2019. A new SNOW stream cipher called SNOW-V. *IACR Trans Symmetr Cryptol*, 2019(3):1-42. https://doi.org/10.46586/tosc.v2019.i3.1-42

Endo H, Sasaki M, 2019. Secret key agreement for satellite laser communications. Advances in Communications Satellite Systems. 37th Int Communications Satellite Systems Conf, p.1-11. https://doi.org/10.1049/cp.2019.1258

ETSI, 2019. 5G; Security Architecture and Procedures for 5G System. 3GPP TS 33.501 Version 15.5.0 Release 15.

Fang BX, Shi JQ, Wang ZR, et al., 2021. AI-enabled cyberspace attacks: security risks and countermeasures. *Strat Study CAE*, 23(3):60-66 (in Chinese). https://doi.org/10.15302/J-SSCAE-2021.03.002

Fang H, Wang XB, Tomasin S, 2019. Machine learning for intelligent authentication in 5G and beyond wireless networks. *IEEE Wirel Commun*, 26(5):55-61. https://doi.org/10.1109/MWC.001.1900054

Feng DG, Xu J, 2010. Network Security Principle and Technology (2nd Ed.). Science Press, Beijing, China (in Chinese).

Fernández-Caramés TM, 2020. From pre-quantum to post-quantum IoT security: a survey on quantum-resistant cryptosystems for the Internet of Things. *IEEE Int Things J*, 7(7):6457-6480. https://doi.org/10.1109/JIOT.2019.2958788

Fettweis GP, Boche H, 2021. 6G: the personal tactile Internet—and open questions for information theory. *IEEE BITS Inform Theory Mag*, 1(1):71-82. https://doi.org/10.1109/MBITS.2021.3118662

Gao F, Xia JJ, Zhang F, 2021. Security vision of 6G network. *Des Techn Posts Telecommun*, (8):29-33 (in Chinese). https://doi.org/10.12045/j.issn.1007-3043.2021.08.007

Goodfellow IJ, Shlens J, Szegedy C, 2015. Explaining and harnessing adversarial examples. https://arxiv.org/abs/1412.6572

Gray J, 2009. Jim Gray on eScience: a Transformed Scientific Method. http://katzcommunications.com/pdfs/fourthparadigm.pdf [Accessed on June 29, 2021].

Guan ZT, Zhou X, Liu P, et al., 2022. A blockchain-based dual-side privacy-preserving multiparty computation scheme for edge-enabled smart grid. *IEEE Int Things J*, 9(16):14287-14299. https://doi.org/10.1109/JIOT.2021.3061107

Han X, Yuan Y, Wang FY, 2019. Security problems on blockchain: the state of the art and future trends. *Acta Autom Sin*, 45(1):206-225. https://doi.org/10.16383/j.aas.c180710

Han YZ, Huang G, Song SJ, et al., 2021. Dynamic neural networks: a survey. *IEEE Trans Patt Anal Mach Intell*, 44(11):7436-7456. https://doi.org/10.1109/TPAMI.2021.3117837

Hatzivasilis G, Fysarakis K, Papaefstathiou I, et al., 2018. A review of lightweight block ciphers. *J Cryptogr Eng*, 8(2):141-184. https://doi.org/10.1007/s13389-017-0160-y

Hexa-X, 2020. Hexa-X. https://hexa-x.eu [Accessed on Dec. 8, 2020].

Hu YX, Yi P, Sun PH, et al., 2019. Research on the full-dimensional defined polymorphic smart network. *J Commun*, 40(8):1-12 (in Chinese). https://doi.org/10.11959/j.issn.1000-436x.2019192

Huang KZ, Jin L, Chen YJ, et al., 2020. Development of wireless physical layer key generation technology and new challenges. *J Electron Inform Technol*, 42(10):2330-2341. https://doi.org/10.11999/JEIT200002

IMT-2030 (6G) Promotion Group, 2021. 6G Network Security Vision Technologies Research Report (in Chinese).

Internet Engineering Task Force, 2019. Postquantum Pre-shared Keys for IKEv2 draft-ietf-ipsecme-qr-ikev2-08. https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-qr-ikev2-08 [Accessed on Nov. 5, 2019].

Jiang Y, Ge XH, Yang Y, et al., 2020. 6G oriented blockchain based Internet of Things data sharing and storage mechanism. *J Commun*, 41(10):48-58 (in Chinese). https://doi.org/10.11959/j.issn.1000-436x.2020211

Jin L, Lou YM, Xu XM, et al., 2020. Separating multi-stream signals based on space-time isomerism. Int Conf on Wireless Communications and Signal Processing, p.418-423. https://doi.org/10.1109/WCSP49889.2020.9299669

Jin L, Lou YM, Sun XL, et al., 2021a. Concept and vision of 6G wireless endogenous safety and security. *Sci Sin Inform*, early access (in Chinese). https://doi.org/10.1360/SSI-2021-0095

Jin L, Hu XY, Lou YM, et al., 2021b. Introduction to wireless endogenous security and safety: problems, attributes, structures and functions. *China Commun*, 18(9):88-99. https://doi.org/10.23919/JCC.2021.09.008

Kariyappa S, Qureshi MK, 2019. Improving adversarial robustness of ensembles with diversity training. https://doi.org/10.48550/arxiv.1901.09981

Kuhn TS, 1996. The Structure of Scientific Revolutions. University of Chicago Press, Chicago, USA.

Kumarage H, Khalil I, Alabdulatif A, et al., 2016. Secure data analytics for cloud-integrated Internet of Things applications. *IEEE Cloud Comput*, 3(2):46-56. https://doi.org/10.1109/MCC.2016.30

Li C, Lei B, Xie CF, et al., 2019. Trustworthy network based on blockchain technology. *Telecommun Sci*, 35(10):60-68 (in Chinese). https://doi.org/10.11959/j.issn.1000-0801.2019226

Li GY, Sun C, Jorswieck EA, et al., 2021. Sum secret key rate maximization for TDD multi-user massive MIMO wireless networks. *IEEE Trans Inform Forens Secur*, 16:968-982. https://doi.org/10.1109/TIFS.2020.3026466

Li HQ, Li J, 2001. Computer Network Security and Encryption Technology. Science Press, Beijing, China (in Chinese).

Li JF, Hu YX, Yi P, et al., 2020. Development roadmap of polymorphic intelligence network technology toward 2035. *Strat Study CAE*, 22(3):141-147 (in Chinese). https://doi.org/10.15302/J-SSCAE-2019.11.010

Li YX, Cao B, Peng MG, et al., 2020. Direct acyclic graph-based ledger for Internet of Things: performance and security analysis. *IEEE ACM Trans Netw*, 28(4):1643-1656. https://doi.org/10.1109/TNET.2020.2991994

Liang YC, Chen J, Long RZ, et al., 2021. Reconfigurable intelligent surfaces for smart wireless environments: channel estimation, system design and applications in 6G networks. *Sci China Inform Sci*, 64:200301. https://doi.org/10.1007/s11432-020-3261-5

Liu GR, Shen J, Bai JP, 2021. A definable 6G security architecture. *Mob Commun*, 45(4):54-57 (in Chinese). https://doi.org/10.3969/j.issn.1006-1010.2021.04.009

Liu JH, 2020. Research on security improvement of 5G core network based on zero trust architecture. *Des Techn Posts Telecommun*, (9):75-78 (in Chinese). https://doi.org/10.12045/j.issn.1007-3043.2020.09.015

Liu LS, Yu ML, Yan Z, 2009. A Concise Course on Advanced Quantum Mechanics. Science Press, Beijing, China (in Chinese).

Liu Y, Peng MG, 2020. 6G endogenous security: architecture and key technologies. *Telecommun Sci*, 36(1):11-20 (in Chinese). https://doi.org/10.11959/j.issn.1000-0801.2020011

Loukil F, Ghedira-Guegan C, Boukadi K, et al., 2021. Privacy-preserving IoT data aggregation based on blockchain and homomorphic encryption. *Sensors*, 21(7):2452. https://doi.org/10.3390/s21072452

Manzuik S, Gold A, Gatford C, 2006. Network Security Assessment: from Vulnerability to Patch. Elsevier, Amsterdam, the Netherlands. https://doi.org/10.1016/B978-1-59749-101-3.X5000-9

Ministry of Internal Affairs and Communications (MIC), 2020. Beyond 5G Promotion Strategy—Roadmap Towards 6G. https://www.soumu.go.jp/english [Accessed on June 30, 2020].

National Institute of Standards and Technology (NIST), 2020. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. https://www.nist.gov [Accessed on July 22, 2020].

National Institute of Standards and Technology (NIST), 2021. Lightweight Cryptography. https://csrc.nist.gov/Projects/lightweight-cryptography [Accessed on July 11, 2021].

National Science Foundation (NSF), 2021. Resilient & Intelligent NextG Systems (RINGS). https://www.nsf.gov/pubs/2021/nsf21581/nsf21581.pdf [Accessed on Apr. 30, 2021].

Network Working Group, 2019. Design Issues for Hybrid Key Exchange in TLS 1.3. https://datatracker.ietf.org/doc/html/draft-stebila-tls-hybrid-design-01 [Accessed on Mar. 11, 2019].

Next G Alliance, 2022. Roadmap to 6G: Building the Foundation for North American Leadership in 6G and Beyond. https://roadmap.nextgalliance.org/ [Accessed on Feb. 1, 2022].

Nguyen VL, Lin PC, Cheng BC, et al., 2021. Security and privacy for 6G: a survey on prospective technologies and challenges. *IEEE Commun Surv Tutor*, 23(4):2384-2428. https://doi.org/10.1109/COMST.2021.3108618

Nie KJ, Cao B, Peng MG, 2020. 6G endogenous security: blockchain technology. *Telecommun Sci*, 36(1):21-27 (in Chinese). https://doi.org/10.11959/j.issn.1000-0801.2020004

Pang TY, Xu K, Chao D, et al., 2019. Improving adversarial robustness via promoting ensemble diversity. Proc 36th Int Conf on Machine Learning, p.4970-4979.

Perazzone JB, Yu PL, Sadler BM, et al., 2021. Artificial noise-aided MIMO physical layer authentication with imperfect CSI. *IEEE Trans Inform Forens Secur*, 16:2173-2185. https://doi.org/10.1109/TIFS.2021.3050599

Porambage P, Gür G, Osorio DPM, et al., 2021. 6G security challenges and potential solutions. Joint European Conf on Networks and Communications & 6G Summit, p.622-627. https://doi.org/10.1109/EuCNC/6GSummit51104.2021.9482609

Research Institute of China Mobile Communication Co., Ltd. (CMC), 2020. 2030 + Vision and Requirements Report (in Chinese). https://www.baogaoting.com/info/19757 [Accessed on Nov. 10, 2020].

Research Institute of China Mobile Communication Co., Ltd. (CMC), 2021. China Unicom 6G White Paper (V1.0) (in Chinese). https://copyfuture.com/blogs-details/20210724061236033y [Accessed on Mar. 22, 2021].

Samsung, 2020. 6G the Next Hyper Connected Experience for All. https://cdn.codeground.org/nsr/downloads/researchareas/6G%20Vision.pdf [Accessed on July 21, 2020].

Sharif M, Bauer L, Reiter MK, 2019. *n*-ML: mitigating adversarial examples via ensembles of topologically manipulated classifiers. https://doi.org/10.48550/arxiv.1912.09059

Siriwardhana Y, Porambage P, Liyanage M, et al., 2021. AI and 6G security: opportunities and challenges. Joint European Conf on Networks and Communications & 6G Summit, p.616-621. https://doi.org/10.1109/EuCNC/6GSummit51104.2021.9482503

Sönnerup J, Hell M, Sönnerup M, et al., 2019. Efficient hardware implementations of grain-128AEAD. 20th Int Conf on Cryptology in India, p.495-513. https://doi.org/10.1007/978-3-030-35423-7-25

Su L, Zhuang XJ, Du HT, 2022. Built-in security framework research for 6G network. *Sci Sin Inform*, 52(2):205-216 (in Chinese). https://doi.org/10.1360/SSI-2021-0257

Sun YY, Liu JJ, Wang JD, et al., 2020. When machine learning meets privacy in 6G: a survey. *IEEE Commun Surv Tutor*, 22(4):2694-2724. https://doi.org/10.1109/COMST.2020.3011561

Synopsys, 2020. 2020 Open Source Security and Risk Analysis Report. Synopsys, Mountain View, USA.

Turan MS, McKay KA, Calik C, et al., 2019. Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process. https://doi.org/10.6028/NIST.IR.8268

Vampire, 2016. eBACS: ECRYPT Benchmarking of Cryptographic Systems. http://bench.cr.yp.to/ebaead.html [Accessed on July 15, 2021].

Wang JH, Ling XT, Le YW, et al., 2021. Blockchain-enabled wireless communications: a new paradigm towards 6G. *Nat Sci Rev*, 8(9):nwab069. https://doi.org/10.1093/nsr/nwab069

Wu H, 2009. Network Security: Attack and Defense. China Machinery Industry Press, Beijing, China (in Chinese).

Wu JX, 2018a. Polymorphic smart network and endogenous safety and security. *Civil-Mil Integr Cybersp*, (11):11-14 (in Chinese).

Wu JX, 2018b. Principle of Cyberspace Mimic Defense—Generalized Robust Control and Endogenous Security (2^{nd} Ed.). Science Press, Beijing, China (in Chinese).

Wu JX, 2020a. Cyberspace Endogenous Safety and Security—Mimic Defense and Generalized Robust Control. Science Press, Beijing, China (in Chinese).

Wu JX, 2020b. Cyberspace Mimic Defense: Generalized Robust Control and Endogenous Security. Springer, Cham, Switzerland.
https://doi.org/10.1007/978-3-030-29844-9

Wu JX, 2022. Development paradigms of cyberspace endogenous safety and security. *Sci Sin Inform*, 52(2):189-204 (in Chinese). https://doi.org/10.1360/SSI-2021-0272

Wu JX, Hu YX, 2021. The development paradigm of separation between network technical system and supporting environment. *Inform Commun Technol Pol,* 47(8):1-11 (in Chinese).
https://doi.org/10.12267/j.issn.2096-5931.2021.08.001

Wu W, Qin P, Feng X, et al., 2017. Reflections on the development and construction of space-ground integration information network. *Telecommun Sci*, 33(12):2017342 (in Chinese).
https://doi.org/10.11959/j.issn.1000-0801.2017342

Xie N, Hu TX, 2021. Improving the covertness in the physical-layer authentication. *China Commun*, 18(3): 122-131. https://doi.org/10.23919/JCC.2021.03.010

Yang HR, Zhang JY, Dong HL, et al., 2020. DVERGE: diversifying vulnerabilities for enhanced robust generation of ensembles. Proc 34^{th} Int Conf on Neural Information Processing Systems, Article 462.

Yang J, Johansson T, 2020. An overview of cryptographic primitives for possible use in 5G and beyond. *Sci China Inform Sci*, 63(12):220301.
https://doi.org/10.1007/s11432-019-2907-4

Yang J, Johansson T, Maximov A, 2019. Vectorized linear approximations for attacks on SNOW 3G. *IACR Trans Symmetr Cryptol*, 2019(4):249-271.
https://doi.org/10.46586/tosc.v2019.i4.249-271

Yang J, Johansson T, Maximov A, 2020. Spectral analysis of ZUC-256. *IACR Trans Symmetr Cryptol*, 2020(1):266-288. https://doi.org/10.46586/tosc.v2020.i1.266-288

Yang P, Xiao Y, Xiao M, et al., 2019. 6G wireless communications: vision and potential techniques. *IEEE Netw*, 33(4):70-75.
https://doi.org/10.1109/MNET.2019.1800418

Yin ZS, Jia M, Cheng N, et al., 2022. UAV-assisted physical layer security in multi-beam satellite-enabled vehicle communications. *IEEE Trans Intell Transp Syst*, 23(3):2739-2751.
https://doi.org/10.1109/TITS.2021.3090017

Ylianttila M, Kantola R, Gurtov A, et al., 2020. 6G white paper: research challenges for trust, security and privacy. https://arxiv.org/abs/2004.11665

You W, Li YL, Bai Y, et al., 2020. Research on endogenous safety and security technology of 5G core network. *Radio Commun Technol*, 46(4):385-390 (in Chinese).
https://doi.org/10.3969/j.issn.1003-3114.2020.04.003

You XH, Wang CX, Huang J, et al., 2021. Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts. *Sci China Inform Sci*, 64(1):110301.
https://doi.org/10.1007/s11432-020-2955-6

Zhang CL, Fu YL, Li H, et al., 2021. Research on security scenarios and security models for 6G networking. *Chin J Netw Inform Secur*, 7(1):28-45 (in Chinese).
https://doi.org/10.11959/j.issn.2096-109x.2021004

Zhang CW, Yue J, Jiao LB, et al., 2021. A novel physical layer encryption algorithm for LoRa. *IEEE Commun Lett*, 25(8):2512-2516.
https://doi.org/10.1109/LCOMM.2021.3078669

Zhang J, Xiong J, Ma DT, 2014. Physical layer secure transmission algorithm in multi-beam satellite communication system. *Appl Electron Technol*, 40(11):116-119 (in Chinese).
https://doi.org/10.3969/j.issn.0258-7998.2014.11.045

Zhang YS, Mi AR, 2003. Analysis of Computer Viruses and Trojan Horse Programs. Kehai Electronic Press, Beijing, China (in Chinese).

Zhang YY, Shen YL, Jiang XH, et al., 2022. Secure millimeter-wave ad hoc communications using physical layer security. *IEEE Trans Inform Forens Secur*, 17:99-114.
https://doi.org/10.1109/TIFS.2021.3054507

Zhao C, Zhao SN, Zhao MH, et al., 2019. Secure multi-party computation: theory, practice and applications. *Inform Sci*, 476:357-372.
https://doi.org/10.1016/j.ins.2018.10.024

Ziegler V, Schneider P, Viswanathan H, et al., 2021. Security and trust in the 6G era. *IEEE Access*, 9:142314-142327.
https://doi.org/10.1109/ACCESS.2021.3120143

ZTE Corporation, China Academy of Information and Communications Technology, China Mobile Communications Group Co., Ltd., et al., 2021. Vision of Intrinsic Cybersecurity Beyond 2030.
https://www.zte.com.cn/mediares/zte/Files/PDF/white_book/202106281137.pdf [Accessed on June 28, 2021].

Xinsheng JI, first author of this invited paper, received his BE degree in Fudan University, Shanghai, China, in 1988, and his MS degree in PLA Information Engineering University, Zhengzhou, China, in 1991. He is currently a Chief Engineer of the China National Digital Switching System Engineering and Technological R&D Center (NDSC). He is a member of the National 6G Technology R&D General Expert Group, a Chief Scientist of the wireless security field of the Collaborative Innovation Center for Wireless Communication, a Deputy Director of the National Engineering Laboratory for Mobile Network Security, and an Academic Leader of the National Science Foundation Innovation Corps. He obtained the National Science and Technology Progress Award (First Prize) three times, and the National Science and Technology Progress Award for Innovation Team once. His major research interests include next-generation mobile communication and cyber space security.

Jiangxing WU is an academician of the Chinese Academy of Engineering (CAE). He is a professor and doctoral supervisor and president of the China National Digital Switching System Engineering and Technological R&D Center (NDSC). Some other positions he held include: Vice Chairman of the National High-tech R&D Program (863 Program) from the Ninth-Five-Year Plan to the Tenth-Five-Year Plan, Vice Chairman of the Information Technology Experts Group of the 863 Program, Director of the National Major Mobile Communication Project Evaluation Commission, Director and Chief Engineer of the China Next Generation Broadcasting Network (NGB) Experts Commission, Vice Chairman of the 3Tnet in the Eleventh-Five-Year Plan. Since 2016, he has served as Vice Chairman of the Space-Earth Integration Network Experts Group of the National Key Scientific and Technological Project during the Thirteenth-Five-Year Plan. He obtained the National Science and Technology Progress Award (First Prize) three times. Some other awards granted to him include: the title of National Outstanding Scientific and Technological Worker in 1997, Outstanding Contribution Award of the National Science and Technology Research Program in 2001, the title of Young and Middle-Aged Experts with Outstanding Contributions in 2003, First-Level Prize of National Teaching Achievement in 2009, and the National Innovation Competition Award in 2017. The scientific research team he led won the National Science and Technology Progress Award for Innovation Team in 2015. His research interests include cyberspace security and network architecture.

Kaizhi HUANG, corresponding author of this invited paper, received her BE degree in digital communication and MS degree in communication and information system in 1995 and 1998, respectively, from PLA Information Engineering University, and her PhD degree in communication and information system in 2003 from Tsinghua University. She is currently a professor of the China National Digital Switching System Engineering and Technological R&D Center (NDSC). She is an expert in the evaluation of national key R&D projects and NSFC projects, and won one National Science and Technology Progress and Innovation Team Award. Her research interests include wireless network security and signal processing.