Research on Data Security Framework for the New Generation Mobile Network

Li Lu(✉), Li Su, Huizheng Geng, and Yingqing Liu

China Mobile Research and Institute, Beijing, China
{luli,suli,genghuizheng,liuyingqing}@chinamobile.com

Abstract. 4G network has greatly stimulated the development of the mobile Internet industry and facilitated the life of ordinary people. 5G network is new generation mobile network, and is the symbol of the mobile network from closed to open. 6G is also new generation network, and will continue to open. 6G will supports integration of space and earth information network and provides services for human health, industrial manufacturing and so on by digital twin network, is closely integrated with personal life and industry development. The security of the data carried by the new generation mobile network will become more important. However, the open network architecture and the application of new technology make data security face challenges. This paper firstly analyzes the data planes and flow scenarios for the new generation mobile network, and then summarizes key security threats of data in new network scenarios. Finally, based on the security requirements of data, a data security framework for the new generation mobile network: data life cycle security monitoring framework based on digital twin network is proposed, data monitoring framework (DMF) for short, which digitizes data life cycle of the new generation mobile network based on digital twin network and dynamically maintain the security status of data lifecycle through monitoring data activities and timely feedback of abnormal results.

Keywords: data security · digital twin network · life cycle · monitoring

1 Introduction

The 5th mobile network introduces new network technologies and architectures such as network exposure, network function virtualization (NFV), network slicing, and mobile/multi-access edge computing (MEC) [1]. The network exposure service could open up part of 5G capacities to third parties [2]. NFV technology virtualizes computing and storage resources, allowing flexible allocation of resources on demand for different network functions. Network slicing provides end-to-end logical networks for industry users to meet their needs for customized network capabilities [3]. MEC enables localized, near and distributed deployment of applications, services, and content, further reducing business delays and saving back haul bandwidth. At present, 6G network has not formed a clear architecture, but it can be predicted that 6G network will be more flexible and open, MEC will get a more long-term development [4]. NFV, network slicing and other new technologies will be more fully used.

N. Radojević et al. (Eds.): ICAID 2022, AHIS 7, pp. 1228–1238, 2023.
https://doi.org/10.2991/978-94-6463-010-7_127

Just as service based architecture introduces new network functions such as network function registration, discovery, and authorization [2], the new generation mobile network requires more complex control instructions to manage more flexible network functions than traditional mobile communication networks. Application of the new technology for improving the network performance and enhancing the ability of network customization will put forward new requirements for network management functions, thus promoting the generation of more management data. In the future, the wider coverage and stronger communication capability can meet the diversified business needs of different scenarios, including satellite communication and underwater communication [5], and will introduce user data of different types, different sensitivity levels to the new networks.

2 Related Work

In recent years, researchers have studied the security of 5G network architecture and related technologies from various angles. In 3GPP Release 15 specification [6], the 5G security architecture are designed, including the security procedures performed within the 5G system. Reference [7] proposes a service-based cloud architecture called Mimicloud for 5G based on dynamic and heterogene techniques, providing flexible reconfiguration mechanisms to protect containers and eliminate attack. Reference [8] proposes solutions to challenges and future directions for secure 5G systems. Reference [9] provides an overview of the security challenges in 5G technologies and the issues of privacy in 5G. Furthermore, presents security solutions to these challenges. Reference [10] presents existing NFV security solutions and products, also surveys NFV security use cases and explore promising research directions in this area. Reference [11] conducts a comprehensive survey to analyze various cryptographic, biometric and multifactor lightweight solutions for data security in mobile cloud. 6G security research is just beginning. Reference [12] presents potential challenges in the development of 6G technology and possible solutions.

3 Our Work

With the surge of data volume and data applications, people's cognition of the value of data is constantly enhanced. Data security and privacy protection have become an important issue of common concern to individual users, industry users and even national governments. And application of new technology and new mobile network architecture may introduce complex data security risks, so it is necessary to analysis data security risks of the new mobile network which is based on open architecture and integrates a variety of new technologies, and eliminate risk, providing key data with security environment. However, the existing research has not considered the new generation mobile network data security comprehensively. Therefore, this article analyzes the security requirements and proposes a data security framework for the new generation mobile communication network based on digital twin network, mainly for 5G and 6G network. The data security framework proposed in this paper has the following significance: (1) it provides reference for the design of data security mechanism for mobile network, (2) it can help prevent

incomplete deployment of security mechanisms or policy failure caused by disorder of management or configuration error in the large-scale, wide coverage, multi-scene and unmanageable network, (3) it is helpful for timely detection of hidden and complex data risks in the new generation mobile network, (4) by combining the security frame proposed in this paper with other digital twin network models such as network optimization, network operation and maintenance, threats to data caused by network maintenance and update can be found in time, and countermeasures can be proposed timely.

4 Analysis on Data for the New Generation Mobile Network

4.1 Analysis on Data Plane

There are many different kinds of data in the new generation mobile network, and the importance of data is various. In order to protect the data according to its characteristics, we divide the data involved in network activities of control plane, user plane and management plane into control plane data, user plane data and management plane data respectively according to ITU-T x.805 [13]. Control plane data is the interactive control information between the users and the network, and it is the necessary data for the network to realize the information communication activities between the network functions and provide appropriate services for the users. User plane data is the actual user data stream generated by the user's access and usage of the network, and it is the data involved in the operation perceived by the user and directly participated in. Management plane data is the data generated and collected by network management activities.

4.2 Analysis on the Data Stream

Data stream for the new generation mobile network has following characteristics: (1) the network environment through which the data flows is open. The data of management and control plane are no longer closed in the operator network, but may be open to third parties, (2) data flows through many different nodes. Network activities of different planes all involve diversified nodes, including virtual machines, containers, and dedicated physical equipment and so on from node nature, and including MEC platform, various terminals for node type. 6G even includes aircraft, and various monitoring devices in body area network, (3) the system environment through which the data flows is complex, involving various scenes of transmission, computing and storage resources sharing. In addition, different plane data stream have their own characteristics:

Control plane data is mainly transferred in the access network and the core network, and will be transferred to various management systems of operator as well as third-party platforms [2]. Control plane data flows through most nodes, which involves multi-type network functions, systems or components, and the data faces complex security risks.

Management plane data is mainly transferred within and between the mobile network management systems [14, 15]. Besides, the management systems collect the data from the core network and the access network. The management plane data involves the most human-computer interaction processes, and the data is threatened greatly by personnel.

User plane data flows between application service providers, MEC nodes, network functions and various terminals which may from underwater, ground and space [16]. It mainly flows through diversified environments, facing threats from multiple sources.

5 Data Security Risks for the New Generation Mobile Network

The new generation mobile network is built based on open architecture, and introduces new technologies such as NFV and MEC, facing various security threats. Data in the new generation mobile network mainly faces the following security risks and challenges:

- General data security risks: without proper security protection, data may face risks such as leak, damage in its life cycle. For example, data may be leaked from transmission nodes if encryption mechanism is not applied in the process of transmission. Data is vulnerable to leakage if identity authentication and access control mechanism are not properly configured in data usage phase.
- Data security risks introduced by new technologies and new architecture: NFV, network slicing, MEC, etc. will aggravate data security risks. Virtualization layer increases data exposure. Data may face risks of illegal access, tampering, destruction if network slicing isolation failure. MEC platforms, which deploy multiple applications and have interfaces to open data to third parties, may become new data exposure nodes.
- Data security risks introduced by network exposure: the new generation mobile network is based on open architecture, can open its network capacity and network management capacity externally. Internally, it can realize multi-source network data analysis and support multi-dimensional analysis capability. Network exposure means the output of data and the potential risk of data leakage.
- Policy consistency data security risks: the data types for the new generation mobile network are diverse, and the data of different types in different planes leakage or tampering have different impacts on enterprises and the public, so the data needs different security requirements. If same security policies are applied to all data, it may result in insufficient protection or waste of resources.

6 Data Security Requirements for the New Generation Mobile Network

Based on the above data security issues, we summarize the overall data security requirements and give security requirements for different plane data based on characteristics of different plane:

- Overall data security requirements: all the data in the network should be able to flow normally and orderly. Data with different security requirements should be protected by corresponding levels of confidentiality, integrity and availability. The openness of the network environment and the diversity of the nodes through which the data flows should not increase security risks for data.

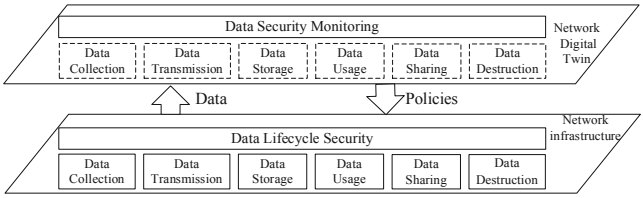

Fig. 1. Data monitoring framework DMF

- Security requirements for control plane data: control plane data needs high integrity and availability requirements, and some of the key data needs high confidentiality requirements. Critical information related to the network should be controlled by the network operator to prevent data leakage or destruction during the flow of various network nodes. The data related to network user's personal information should be protected from disclosure and malicious use.
- Security requirements for management plane data: management plane data needs high integrity, availability and confidentiality protection requirements. Data should be protected properly against threats, including from personnel.
- Security requirements for user plane data: according to different user needs, industries and business types, there is great differences in confidentiality, integrity and availability requirements for user plane data. Adaptive security mechanisms should be imposed according to user plane data security requirements, and user plane data should be under the control of the users.

7 Data Security Framework for the New Generation Mobile Network

7.1 Security Framework Design

In view of the above data security risks and security requirements, this paper proposes data life cycle security monitoring framework based on digital twin network, data monitoring framework (DMF) for short. Firstly, we define the data life cycle of the new mobile communication network, and then propose the key security dimensions of each stage of data life cycle in physical network. Finally, we digitize each stage of data life cycle and monitor security status of each phase of data life cycle with digital twin network. The framework is shown in Fig. 1.

7.2 Data Life Cycle Security Dimensions

Data life cycle theory is commonly used in the data collection and processing of business systems. The mobile network data security protection can also be considered from the perspective of data life cycle if the network is regarded as a large data processing system containing all kinds of terminals and many network nodes that realize data processing, transmission and storage. In this paper, data life cycle is defined as data collection, transmission, storage, usage, sharing and destruction [17]. The main security dimensions

and corresponding key security measures of each stage in data life cycle for the new generation mobile network are as follows:

- Data collection
  Data collection includes the creation of network data in the process of network activities and the acquisition of data from external networks, systems or platforms. Data security can be considered from two dimensions. Data creation security dimension: for control plane and management plane data, access control of key data creation areas in network nodes should be ensured and the corresponding security mechanism should be ensured in terminals for user plane. Data acquisition security dimension: data source authentication and key data encryption transmission and verification should be implement, etc.
- Data transmission
  Mobile network data transmission is defined as data transmission between terminals and network nodes, network nodes and external network nodes, and within network nodes. There are commonality and characteristic security requirements in three-plane data transmission. Common aspects: the data in the new generation mobile network will go through a variety of transmission environments, and security environments are required. Transmission environment security dimension includes enhanced interface control and appropriate security configuration, etc., to prevent data leakage from transmission nodes. In terms of characteristics: transmission mechanism security dimension is important and the security mechanism requirements for data in different planes are different. Adaptive security mechanism should be applied to control plane data according to the transmission scene and data type. Management plane data is relatively sensitive and the amount of data is small, so the security transmission mechanism should be applied. User plane data security mechanism should be applied according to data security requirements. For example, apply anti-quantum transmission encryption to user plane data with high security requirement.
- Data storage
  The data stored in the mobile network is mainly control plane and management plane data. In the future user-centric architecture, the physical location of storage nodes will be more dispersed, and the nodes may still be deployed in a virtualized environment, which will face more physical and network security risks. Storage system security needs to be enhanced and secure storage method for data with high security requirements should be applied. Storage system security dimension: including apply security operating system based on trusted technology, etc. Storage method security dimension: including enhanced data encryption, or store data with blockchain [18], etc.
- Data usage
  We divide the data usage scenarios into basic data usage and data analysis. The basic data usage refers to the data query between network nodes and the data calculation in nodes. The data analysis refers to the aggregation analysis of data by the network. Data usage security dimension: (1) for the control plane data, attention should be paid to the authentication among kinds of interfaces and the restriction of data access rights of nodes to prevent the theft of data by fake nodes, (2) for management plane data, blockchain could be used to carry out authorization and recording of data access,

besides the management of personnel accounts should be enhanced, (3) for user plane data, security measures should be applied on the management and control of the interfaces in the network edge, preventing unauthorized applications and unauthorized nodes from accessing user data, and ensuring that user data is under user control. Data analysis security dimension: mainly consider the application of data desensitization, privacy computing technology, and AI-based data operation audit.

- Data sharing
  5G network has supported to open up some network capabilities and network management capabilities to third parties. In order to meet diversified business needs, there will be more open scenarios of capabilities in 6G network, accompanied by more data sharing. There are two security dimensions for data sharing. Shared content security dimension: apply data desensitization or privacy computing technology to minimize content shared externally and avoid sensitive data being sent out of the network. Sharing mode security dimension: includes the marking of outbound data through structured data watermark technology, etc.
- Data destruction
  There are many data destruction scenarios in the new generation mobile network which introduce virtualization technology and MEC mode. In addition to the traditional user logout and offline of network elements, data destruction scenarios include virtual machine migration, MEC application migration and so on. Data destruction security could be considered from to dimensions. Destruction method security dimension: multiple data destruction methods are integrated to destroy data completely. Destruction scope security dimension: data that should be destroyed in each scene should be sorted out and completely destroyed.

7.3 Data Life Cycle Security Monitoring Based on Digital Twin Network

With the expansion of network coverage and the continuous convergence of heterogeneous networks, complex security risks in the new generation mobile network can no longer be prevented only through various security mechanisms of data life cycle, and the failure of any security mechanism may means serious data security problems. Digital twin network is proposed to build the real-time mirror of physical network for solving the challenges faced by network optimization and maintenance [19, 20]. With the help of the digital twin network, it can also deal with the data security problems in the new generation network. Under the condition that the security mechanism has been applied, we can construct a digital twin network for data life cycle security supervision to digitize the data life cycle and monitor its security status. The alarm information or security policies will be sent through the interface between the digital twin network and the physical network when abnormal situations are detected. Data security-oriented digital twin network in the new generation mobile network includes the following parts:

- Network Oriented DMF (NODMF)
  NODMF digitizes the life cycle for control and management plane data based on digital twin network for mobile network and besides, it support monitoring abnormal events of the data life cycle.

Data acquisition: In order to digitize the data life cycle, data collected by network nodes from external, data stored in network nodes, data transmitted over network and operation log should be mainly collected in addition to the basic configuration data of network functions and environmental information required for the construction of general digital twin network. SNMP, Netflow and other methods can be used to collect data. For collecting data stored in nodes, data types of which can be obtained by scanning storage nodes with the help of network data scanning technology. In order to reduce the pressure of data collection and processing, key network nodes and interfaces can be selected, and the list of core data types can be established based on data security requirements. Only data in key areas of concern are collected, and only data types in the key data list are analyzed and processed.

Network model construction: First of all, network node model and topology model corresponding to the physical network in the key area are constructed to realize the digital description of the physical network. Further, we mark the nodes on the control plane and the nodes on the management plane respectively, and then further mark the key nodes in the two planes, such as the nodes that can collect data from the external network, the nodes that can open data to the outside, and the nodes that can store data centrally and so on. Using these markers, the nodes can be selected purposefully in data analysis, and the network can be more clearly described when the network is presented visually.

Data life cycle mapping: Data collection mapping is realized by monitoring and digitizing the data stream collected by data collection nodes. Data transmission mapping is realized by monitoring and digitizing the data stream between terminals and network nodes, network nodes and external network nodes, and between network nodes. Data usage (i.e., data operation) and data destruction are realized by digitizing operations which are parsed from real-time operation logs of network nodes and request/response messages between network nodes. Data sharing is realized by monitoring and digitizing the data flow sent out by network exposure nodes. In addition, data types scanned from storage nodes as the initial data, combined with data usage and data destruction operations, can realize the mapping of data storage.

Security monitoring and evaluation methods: Security status of network data can be evaluated based on rules, model analysis results and detection results based on security baseline. Rule-based: we can generate security rules for different life cycle stages according to the security mechanism of data life cycle, and match the data stream that violates security rules. Model-based analysis: Artificial intelligence (AI) algorithms such as deep learning and machine learning can be used to build a data security flow model according to data access frequency, types of data being accessed, nodes being accessed and other factors, to determine dangerous data flow scenarios and to identify high-risk data analysis behaviors, especially for data analysis scenarios. Based on security baseline: we can construct a module for security baseline detection in digital twin network to detect automatically whether the node configuration meets the requirements of security baseline, so as to reflect the security level of the nodes.

The data life cycle security state can be monitored and evaluated based on the data life cycle security dimensions proposed above, so as to improve the data security at all the stages: (1) data collection: the method based on baseline can be used to enhance data creation security. For example, we can check whether the security configuration

of the critical data creation area in the digital twin network function is correct. Rule-based method can be used to enhance data acquisition security. For example, if data type A should be encrypted in the collection stage, the rule will be the data A can't be parsed from the collected data, (2) data transmission: the method based on baseline can be used to enhance transmission environment security. For example, we can check whether interface configuration is correct. Rule-based method can be used to enhance transmission mechanism security. For example, we can make a rule that B can't be parsed from data transmitted between node G and node H, (3) data storage: the method based on baseline can be used to enhance storage system security and rule-based method can be used to enhance storage method security. For example, we can make a rule that data A can't be found in stored data, (4) data usage: the method based on baseline and rule-based method can be used to enhance data basic usage security. For example, we can make a rule that account H does not have the access rights of data B. Module-based method can be used to enhance data analysis security, (5) data sharing: rule-based method can be used to enhance shared content and sharing mode security. For example, we can make a rule that data B can only be sent to users in user ID list, (6) data destruction: enhancement for destruction method security dimension is out of scope, but we can use rule-based method to enhance destruction scope security. For example, application function migration and the data destruction operation can combined to make a rule to determine whether the data is completely destroyed. The corresponding security policy can be issued to the physical network when abnormal events are detected. By discovering and resolving data lifecycle security issues in time, the data security status can be effectively maintained.

- User Oriented DMF (UODMF)
  For industrial parks, hospitals and other scenes with high user plane data security requirements, UODMF can be built at the edge nodes. UODMF digitizes the user data life cycle based on digital twin network for network edge and besides, it support monitoring abnormal events of the data life cycle.

8 Experiment and Analysis

In this part, the data security supervision process based on digital twin network is simply simulated. 5 servers are used to set up 5 network nodes to simulate a small area in network. We develop a scanning tool to scan and acquire the data stored in network nodes, and PacketBeat tool is used to capture the data between network nodes. We construct a simplified digital twin network by digitizing network nodes, network node data storage state and data stream between network nodes. The server uses 16 GB memory, 8-core CPU, 10,000 MB network card, and the network traffic processing speed is about 430 MB/s.

Data transmission between network nodes is visualized as shown in Fig. 2. In this experiment, data transmission rules between network nodes are formulated, and timely reporting of illegal data transmission is realized through analyzing the data types transmitted between network nodes.

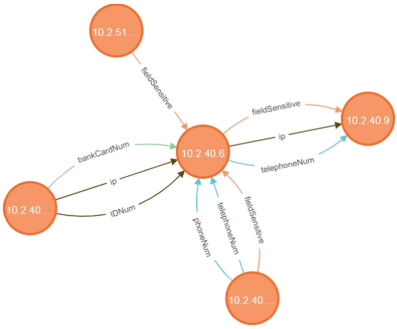

Fig. 2. Data transmission between network nodes

9 Conclusions

This paper proposes the design, data life cycle mapping and security monitoring method of the data security framework for the new generation mobile network. Combined with visualization technology, the security state of network data flow can be presented and supervised dynamically in real time, which is helpful to reduce data security risks and help network operators or users manage data. In the future, a data flow model can be generated on the basis of DMF, which can provide help for data traceability and data pollution control. In addition, potential risks exist in data collection and aggregation. Digital twin network can help physical network protect data, but data gathered in digital twin network will also face potential risk. Data desensitization, data encryption and data classification mark can be applied to digital twin network data collection, only the minimum data that meets the requirements of data monitoring and analysis is retained to reduce the data security risk of digital twin network itself.

References

1. Multi-access Edge Computing (MEC) (2019) Framework and Reference Architecture (V2.1.1). ETSI GS MEC 003-2019
2. 3GPP (2020) System Architecture for the 5G System (5GS) TS 23.501V16.7.0[S].2020.12
3. 3GPP (2018) Study on management and orchestration of network slicing for next generation network TR 28.801V15.1.0 [R].2018.01
4. Peltonen E, et al (2020) 6G white paper on edge intelligence
5. Guangyi L, et al (2020) 6G vision and needs: digital twin, intelligence ubiquity mobile communications 6
6. 3GPP (2020) Security architecture and procedures for 5G System TS 33.501V16.5.0[S].2020.12
7. Lingshu LI, et al (2021) Secure cloud architecture for 5G core network. Chin J Electron
8. Ahmad I et al (2018) Overview of 5G security challenges and solutions. IEEE Commun Stand Mag 2(1):36–43
9. Ahmad I, et al (2017) 5G security: analysis of threats and solutions. In: 2017 IEEE conference on standards for communications and networking (CSCN). IEEE
10. Yang W, Fung C (2016) A survey on security in network functions virtualization. In: Netsoft conference & workshops. IEEE, pp 15–19

11. Bhatia T, Verma AK (2017) Data security in mobile cloud computing paradigm: a survey, taxonomy and open research issues. J Supercomput 73(6):2558–2631
12. Gui G, et al (2020) 6G: opening new horizons for integration of comfort, security and intelligence. IEEE Wirel Commun 99:1–7
13. ITU-T 805 (2003) Security architecture for systems providing end-to-end communications[S]. [S.l]: ITU-T805
14. 3GPP (2018) Study on management and orchestration architecture of next generation networks and services TR 28.800V15.0.0[R].2018.01
15. 3GPP (2018) Study on management aspects of next generation network architecture and features TR 28.802V15.0.0[R].2018.01
16. 3GPP (2019) Study on management aspects of edge computing TR 28.803V16.0.1[R].2019.09
17. Security guidelines for big data lifecycle management by telecommunication operators (Study Group 17). ITU-T X.1751-2020.2020
18. Sun W, Li S, Zhang Y (2021) Edge caching in blockchain empowered 6G. China Commun 18(1):1–17
19. Grieves M (2021) Digital twin: manufacturing excellence through virtual factory replication. https://www.3ds.com/fileadmin/PRODUCTS-SERVICES/DELMIA/PDF/Whitepaper/DELMIA-APRISO-Digital-Twin-whitepaper.pdf. Accessed 11 Mar 2021
20. Liu M, et al (2020) Review of digital twin about concepts, technologies, and industrial applications. J Manuf Syst