GTI

Security Considerations for 5G Smart City Whitepaper

http://www.gtigroup.org

GTI Security Considerations for 5G Smart City Whitepaper

Version:	V1.0
Deliverable Type	**□Procedural Document** **□Working Document**
Confidential Level	**□Open to GTI Operator Members** **□Open to GTI Partners** **□Open to Public**
Working Group	
Task	
Source members	CMCC
Support members	Huawei, CAICT
Editor	China Mobile Cybersecurity R&D Center
Last Edit Date	09-03-2020

Approval Date	DD-MM-YYYY

Document History

Date	Meeting #	Version #	Revision Contents
DD-MM-YYYY		NA	
DD-MM-YYYY			
DD-MM-YYYY			
DD-MM-YYYY			
DD-MM-YYYY			

Table of Contents

1 Executive Summary

New Smart City is the result of the deep integration and iterative evolution of next-generation information technologies and urban modernization. With features such as high bandwidth, low latency, and massive connections, 5G networks are providing new driving forces for Smart City development, and achieving intelligent perception, precise management, and convenient services, playing an important role in applications such as smart government, smart traffic, smart manufacturing, and smart grids. Changes brought by 5G technologies accelerate the development of smart cities while also posing certain security threats. To respond to these threats, municipal administrators and city constructors can provide security facilities and capabilities at different layers of 5G + new smart cities, such as the terminal layer, network layer, platform layer, and application layer. This document focuses on the potential security threats and challenges brought by the application of 5G technologies to Smart City, and the security capabilities required to address these threats.

2 Abbreviations

Abbreviation	Explanation
AF	Application Function
AI	Artificial Intelligence
AMF	Access and Mobility Management Function
API	Application Programming Interface
CPE	Customer Premise Equipment
DDoS	Distributed Denial of Service
EMS	Element Management System
IMSI	International Mobile Subscriber Identity
IPS	Intrusion Prevention System
LTE	Long Term Evolution
MANO	Management and Orchestration
MEC	Multi-access Edge Computing
NEF	Network Exposure Function
NFV	Network Function Virtualization
NSSAI	Network Slice Selection Assistance Information
PCF	Policy Control Function
PDCP	Packet Data Convergence Protocol
RBAC	Role Based Access Control
SBA	Service Based Architecture
SDN	Software Defined Network

SMF	Session Management Function
SUCI	Subscription Concealed Identifier
UDM	Unified Data Management
UE	User Equipment
VR/AR	Virtual Reality/Augmented Reality
WAF	Web Application Firewall
WLAN	Wireless Local Area Network

3 References

The following documents contain provisions which, through reference in this text, also constitute provisions of the present document.

[1] Research Report on Smart City Security System. CCIA, Working Group on Security Standard of Smart City, March 2017

[2] IoT: the next wave of connectivity and services (https://www.gsmaintelligence.com/research/2018/04/iot-the-next-wave-of-connectivity-and-services/665/)

[3] 5G + Smart Grid. https://carrier.huawei.com/cn/success-stories/Industries-5G/5G-Injecting-new-kinetic-energy-into-smart-grids

[4] ENISA: THREAT LANDSCAPE FOR 5G NETWORKS, November 2019

[5] NFV-SEC. https://www.etsi.org/deliver/etsi_gs/NFV-SEC/

[6] 5G + Smart Traffic. https://cloud.tencent.com/developer/article/1550447

[7] Bao Zuojun. Discussing 5G Network Technologies in Smart Traffic Construction [J]. China ITS Journal. 2019, 226(01):81-82+102.

[8] GB/T 37971-2019, Information Security Technology - Framework of Smart City Security System

[9] Ahmad I , Kumar T , Liyanage M , et al. Overview of 5G Security Challenges and Solutions[J]. IEEE Communications Standards Magazine, 2018, 2(1):36-43.

4 5G Enables Smart City

4.1 Smart City

Smart City is a form of urban construction and development. It involves the utilization of next-generation information technologies to promote information, physical, and social space integration across cities. These technologies include 5G, IoT, cloud/edge computing, big data, as well as spatial and geographic information integration. In addition, Smart City adopts various application systems to accelerate the economic development and transformation of cities, improve government and public service efficiency, facilitate the work and life of citizens, as well as effectively protect and utilize the environment, realizing the harmonious development of economy, society, and environment.

Traditional Smart City mainly builds on the fundamental information network and cloud computing platform, configures comprehensive sensing devices, and aligns basic information resources. In contrast, new Smart City centers on five development concepts: "innovation, coordination, green, openness and sharing". With increased emphasis on the deep integration and iterative evolution of next-generation information technologies and urban modernization, new Smart City further enhances public service efficiency and governance capabilities in cities, provides better services for citizens, and improves the accuracy, efficiency, as well as transparency of city services.

4.2 Smart City in the 5G Era

The consensus across the communications industry is that 4G has changed people's lives, and 5G is set to change societies. To achieve

sustainable city development and new industry driving forces, it is necessary to accelerate the deep integration of next-generation communication technologies with urban development so as to solve urbanization problems through information-based methods. At present, Smart City is developing towards intelligent perception, precise management, and convenient services. In terms of smart government, smart traffic, smart manufacturing, and smart grids, 5G and artificial intelligence (AI) technologies have been playing an increasingly important role.

- **5G + Smart Government**

Information-based governments at all levels aim to utilize the high-speed, multiple-access, and low-latency advantages of 5G technologies to promote smart examination and approval, smart services, and smart disclosure in government affairs.

Governments can use 5G high-definition (HD) live broadcast for remote government examination and approval, and 5G terminals for high-precision information collection and big data intelligent analysis. Furthermore, government officers can provide enterprises with door-to-door services by utilizing a 5G government affairs toolbox, breaking the time and space restrictions of government services.

- **5G + Smart Traffic**

Smart traffic involves vehicles, road infrastructures, traffic management facilities, transportation planning, digital transportation platforms, and various transportation-based applications. In the future, the travel landscape can cover a smart traffic system where various components function in cohesion.

In the 5G era, a vehicle-road collaborative service system will be built based on the Internet of Vehicles (IoV) to provide panoramic traffic information to road users on 5G networks, ensuring road safety. For example, with vehicle recognition, geomagnetic induction, HD surveillance, weather monitoring, and other data collection methods, traffic video, people, vehicle, weather, and road condition data can be collected and transmitted to the central cloud on 5G networks in real time. Based on video analysis technologies, abnormal traffic events, such as congestion, illegal parking, slippery roads caused by rain and fog, and fire accidents, can be dynamically monitored and predicted, allowing vehicles to change lanes or avoid affected roads.

5G also accelerates the future implementation of autonomous driving. In March 2019, 3GPP initiated a project to develop the 5G V2X technology based on 5G new air interfaces in R16. As a key part of V2X application, autonomous driving is dependent on the high bandwidth and low latency features of 5G networks. In autonomous driving scenarios, vehicles collect large-scale data by using cameras and sensors, and interact with transportation facilities, other traffic participants, and cloud computing data centers. This type of data communication requires high-bandwidth and low-latency channels, which are the basis of 5G networks.

- **5G + Smart Manufacturing**

Featuring ultra-high bandwidth, massive connections, and ultra-low latency, 5G networks function as communication channels for industrial interconnection. The Industrial Internet involves a wide variety of industrial equipments, diverse data types, and high requirements for real-time data. The features of 5G networks coincide with the needs of the Industrial Internet.

The 5G Time-Sensitive Networking (TSN) technology can guarantee low end-to-end latency of Industrial Internet services. The 5G high frequency and antenna technologies support precise positioning and high-bandwidth communication within factories, greatly improving operation accuracy in remote control. The combination of 5G and Augmented Reality (AR) technologies enables remote guidance and assistance of operations. With real-time videos, voices, 3D marking, and frozen images, the technologies provide assembly personnel on production lines with dynamic graphic and text operation guidance, remotely analyze causes, and rapidly solve problems to effectively reduce product quality issues. In addition, Automatic Guided Vehicles (AGVs) on 5G networks can automatically and accurately distribute material across different building floors and workshops to achieve smart logistics.

- **5G + Smart Grids**

The International Telecommunication Union (ITU) defined three major 5G scenarios: Enhanced Mobile Broadband (eMBB), ultra-reliable and low latency communications (uRLLC), and massive machine type communications (mMTC). 5G is used in varying degrees within all aspects of power systems, covering power generation, transmission, transformation, distribution, consumption, and emergency communications.

In power generation, 5G is mainly used in new energy power prediction and status perception, as well as the management and control of distributed wind power networking. These scenarios impose high requirements on the number of wireless communication connections and latency. For example, millions of connections are required for centralized new energy monitoring, and low latency not exceeding 20 ms is required

for the control of wind power blade pitch.

In power transmission, 5G is mainly used during the monitoring of transmission lines and unmanned aerial vehicle (UAV) patrols. These scenarios impose high requirements on the number of connections and bandwidth. For example, online monitoring of transmission lines requires the connection and management of tens of millions of sensors, and UAV patrol requires 100 Mbit/s-level bandwidth.

In power transformation, 5G is mainly used in the intelligent inspection of substations. Compared to manual substations, intelligent robots reduce risks and increase operation efficiency. In this type of scenario, 100 Mbit/s-level bandwidth is required for the backhaul of HD videos.

In power distribution, 5G is widely used in the entire process from fault monitoring and locating to precise load control. These applications significantly raise low latency requirements. For example, distribution network protection and control, and micro synchronous phasor measurement of intelligent distribution networks require ultra-low latency below 10 ms, while load control based on user response requires latency to be no more than 20 ms. At the same time, connections managed during power distribution are with number in millions or tens of millions.

In power consumption, 5G applications are also very extensive, involving all aspects of power measurement and management, such as power consumption information collection, distributed energy and energy storage, electric vehicle charging piles, and smart homes. The most prominent requirement of these applications is massive connections numbering in tens or hundreds of millions.

5 Threats to 5G Smart City

5.1 Security Challenges from New Service Applications

New Smart City in the 5G era will serve vertical industries and bring forth abundant services. Different services will have varied security requirements, for example, IoT services involve complicated applications and hundreds of billions of connections. Adopting single-user authentication could lead to high costs and signaling storms. Therefore, the costs of authentication and identity management of IoT devices must be reduced to support the low-cost and efficient mass deployment of IoT devices. For IoT devices with low computing capabilities and high battery life requirements, 5G networks should ensure energy efficiency with some security protection measures. IoV services have high network latency and reliability requirements, and security threats in communications may endanger lives. Therefore, high-level security protection measures that do not cause additional communication latency are required. The latency caused by the following aspects can be optimized and reduced: identity authentication during service access, data transmission security protection, security context switching during terminal movement, and data encryption and decryption on network nodes.

Facing various application scenarios and service requirements, a unified, flexible, and scalable network security architecture is required to meet different security requirements. Specifically, 5G networks:

- Require a unified authentication framework for network access authentication in multiple application scenarios, including terminal

equipment authentication, subscriber authentication, multiple access method authentication, and multiple authentication mechanisms.

- Need to satisfy scalability requirements. For example, when a network horizontally expands or shrinks, some security function instances need to be started or terminated in time to meet security requirements.
- Need to support on-demand user-plane data protection, and deploy security protection mechanisms (including encryption endpoints, encryption algorithms, and key lengths) based on service type and security requirements.

5.2 Security Challenges from IT-based Networks

To provide higher system flexibility and efficiency, the 5G network architecture introduces new information technologies: software-defined networking (SDN) and network functions virtualization (NFV). The introduction of these new technologies has also brought new challenges to 5G network security. By introducing the virtualization technology, 5G networks have realized software and hardware decoupling. Network functions are implemented through software and no longer rely on special communication hardware platforms. On traditional networks, the protection of functional network elements depends on the security isolation among physical devices. However, virtualization has changed the situation, and previously secure physical environments have become insecure. Meeting the security requirements for manageable and controllable virtualization platforms is an important part of 5G security. In addition, network virtualization uses a significant amount of open-source and third-party software, which increases the possibility of introducing security vulnerabilities.

Furthermore, 5G networks will support virtual network slicing, providing differentiated network services but posing new security challenges. For example, security protection measures need to be customized for slices based on service requirements to implement customized hierarchical security services. Security isolation between virtual network slices, as well as security deployment and management of these slices, are also required.

5.3 Security Challenges from Network Architecture Changes

For latency-sensitive service scenarios, 5G data gateways and service enablement devices can be deployed at edges of access networks or integrated with base stations based on service requirements to reduce pressure on backhaul networks, shorten latency, and improve network communication rates. This refers to the Mobile Edge Computing (MEC) technology of the 5G core network. MEC sites are generally deployed in access equipment rooms with relatively poor physical conditions or in enterprise zones not controlled by operators. This leads to relatively large risks in terms of physical security assurance and access control of network equipment. In MEC scenarios with B2B industrial applications (such as the Industrial Internet), enterprises generally require data to be transmitted within the zone. In addition, enterprises are concerned that security attacks may penetrate from carriers' networks to enterprise intranets, while operators also believe that enterprise intranets are uncontrollable and untrustworthy. This means they may spread security threats or viruses to their public networks.

To address these security requirements and challenges, secure and

thorough isolation measures must be implemented to enable mutual trust and communication between operators' public networks and enterprises' internal private networks, taking full advantage of MEC while ensuring security.

5.4 Security Challenges from Network Capability Openness

The functional architecture of the 5G core network has introduced the NEF functional component for network capability openness. In southbound direction, the NEF communicates with various service NEs in the 5G core network. In northbound direction, the NEF opens APIs to different application functions (AFs). With centralized API gateways, the NEF achieves unified openness of 5G core network capabilities.

Because AFs calling NEF APIs may come from outside operators such as the Internet, this risk of exposure may bring serious security threats to the 5G core network and, possibly, the entire 5G network. On the 5G core network, not only capabilities of the entire network, but also those between NEs within the network are opened. The 5G core network also introduces the service-oriented architecture (SBA), in which NEs provide service openness and call the open capabilities of each other through APIs. Therefore, on 5G networks, higher and more flexible security capabilities need to be supported between the core network and external third-party applications, as well as between internal NEs of the core network, to achieve secure function invocation.

5.5 Security Challenges from Multi-Access Technologies

5G networks support multiple access methods such as WLAN, LTE, fixed

networks, and new 5G radio access technology (RAT). Different access technologies have varied security requirements and access authentication mechanisms. In addition, a user may have multiple terminals, and one terminal may support multiple access methods. When a terminal switches between different access methods, or a user uses the same service on different terminals, rapid authentication is required to ensure service continuity for better user experience. Therefore, 5G networks need to build a unified authentication framework to integrate different access authentication methods and optimize existing security authentication protocols to improve the security authentication efficiency of terminals switching between heterogeneous networks and ensure service continuity of users switching between terminals or access methods.

In 5G application scenarios, some terminal devices have high capabilities with SIM/USIM cards and certain computing and storage capabilities. On the other hand, some terminal devices use IP addresses, MAC addresses, and digital certificates as identities, while some terminals have poor capabilities due to the lack of hardware to securely store identities and authentication credentials. Therefore, 5G networks need to build a unified identity management system that supports different authentication methods, identities and authentication credentials.

5.6 Security Challenges from User Privacy Protection

The diversity of services and scenarios on 5G networks and the openness of the networks increase the risk of users' private information being leaked. For example, in the smart medical system, confidential information about patients, such as medical records, prescriptions, and treatment plans, are at a risk of being leaked or tampered with during

collection, storage, and transmission. In smart traffic, private information such as vehicle locations and driving trajectory may also be leaked, and illegally traced and used. Therefore, higher requirements for user privacy protection are imposed on 5G networks. The main security threats are as follows:

- 5G networks are heterogeneous networks with various access technologies, which protect private information to different extents. Moreover, user privacy data is scattered on functional entities on 5G networks. Data mining technology enables third parties to analyze the scattered private data and obtain more private user information.
- 5G networks need to optimize and rectify the international mobile subscriber identity (IMSI) vulnerabilities on 4G networks, and use enhanced security mechanisms to protect the identities of users from being leaked, while preventing dimensionality reduction attacks to users.
- Cyber attackers may also trace and attack UEs by using UE location information or the continuity of air interface data packets. Therefore, 5G privacy protection also needs to take into account the security threats to location privacy.

In summary, 5G networks need to fully consider the risks of privacy exposure faced by user data during switching between access technologies and operators, and develop comprehensive privacy protection policies, covering the identities, locations, and accessed services of users.

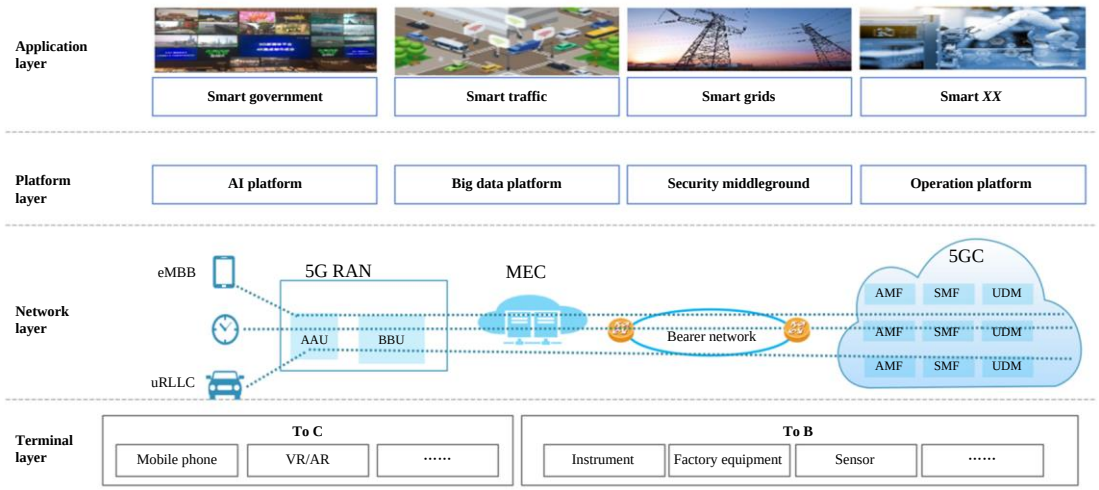
6 5G Smart City Security Recommendations

6.1 Smart City Architecture

As shown in figure 6-1, 5G + New Smart City consists of four layers – the terminal layer, network layer, platform layer, and application layer – from the bottom up.

- **The terminal layer** involves mobile phone terminals, and VR/AR terminals for individual users, as well as industrial control terminals, CPEs, and various sensors for vertical industries.
- **The network layer** is an end-to-end 5G network covering the entire Smart City, including the radio base stations (RBS), park/access MEC, the bearer network, the 5G Core network, and 5G network slices from base stations to the core network.
- **The platform layer** contains public IT platform systems such as the AI platform, big data platform, operation platform, and security middleground.
- **The application layer** is composed of smart application systems such as smart government, smart traffic, and smart grids that make the city refined, intelligent, and convenient

Figure 6-1 Smart City architecture



6.2 Terminal Layer Security

A 5G + New Smart City mainly involves two types of terminals: one for consumer users (To C) which are typically various 5G mobile phones, and one for business industries or urban public infrastructure (To B) such as 5G industrial terminals and sensors of smart factories, and 5G terminals of smart street lights. The number of IoT devices to be connected around the world is estimated to be 25.2 billion by 2025. A large number of these terminals have low power consumption, as well as limited computing and storage resources, which makes deployment of complex security policies and control over the software difficult. Consequently, these limitations make the terminals easy and likely targets to be hacked.

Based on the assessment of the impact caused by the operation of Smart City itself, there are two kinds of notable risks on the terminal layer. First, DDoS attacks initiated by terminals need to be prevented and resisted. Such DDoS attacks may be initiated by hacked terminals, or be unintentionally caused when a large number of terminals trigger control-plane signaling registration at the same time due to software

defects or network faults. It is recommended that a set of security defense mechanisms be built at the network level for attack detection and self-protection (such as active flow control) to ensure that any DDoS attacks can be detected and sensed the first time to prevent major global negative effects on network services. For DDoS attacks of the second type, some proactive and preventive measures are recommended in terms of terminal exception handling and signaling registration. For example, in abnormal scenarios such as a network fault, signaling reconnection is not initiated immediately. Instead, a mechanism similar to CSMA-CD in Ethernet is adopted, that is, a connection is re-attempted after an unspecified time, which reduces the probability of signaling DDoS. Second, for the prevention of risks brought by hacked terminals to industrial production and applications, it is recommended that certain security capabilities (such as SSH security login, TLS transmission encryption, and built-in security chip) be built in terminals in terms of access authentication on the management and O&M plane as well as encryption protection on the signaling/data plane.

6.3 Network Layer Security

5G networks covering every corner of the city are the basic information paths of New Smart City. The security of 5G networks is vital to the security of Smart City. From the perspective of network components, the noteworthy aspects of the Smart City network layer security include security in the RAN base station air interfaces, MECs, 5G Core, bearer networks, and 5G slices.

- **Base Station Air Interface Security**

Air interfaces between 5G UEs and base stations mainly have three types

of security threats:

- User data eavesdropping and tampering over air interfaces. For the prevention of this type of security threat, SUCI encryption and encryption for air-interface PDCP data packets can be enabled.
- DDoS attacks over air interfaces. For the prevention of this type of attacks, a DDoS detection and defense system can be deployed so that base stations can implement flow control in the case of mega DDoS attacks.
- Malicious attacks and interference from pseudo base stations, such as spam short messages or valuable and sensitive information eavesdropping by such rogue base stations. For this type of attack, a unified rogue base station detection system can be deployed around the network so that rogue base stations on the network can be detected and located the first time.

- **MEC Security**

In the 5G era, MEC is widely deployed and used. To avoid physical attacks and cross-network penetration and infection of network attacks, 5G networks need to focus not only on the physical security control of MEC, but also on the isolation between enterprise networks and operators' 5G networks. Security facilities, such as firewalls and IPS, are recommended for network boundary protection.

- **5G Core Security**

The security of the 5G Core is the top priority of the security of the entire 5G network. Security protection measures for the 5G Core need to be considered from the following aspects: management and O&M plane,

security of the southbound-northbound boundary of the network, eastbound-westbound security inside the network, and cloud security at the infrastructure layer of the core network.

- For MANO, EMS and other systems on the management and O&M plane, an access security control system, including bastion hosts and 4A, is recommended to avoid unauthorized management and O&M access, and ensure secure and compliant O&M operations. In addition, to prevent security risks such as viruses and OS vulnerabilities introduced by O&M terminals, desktop cloud terminals can be used.

- For the security of the southbound-northbound boundary of the network, it is recommended that security facilities, such as firewalls, sandboxes, WAF, IPS, and anti-DDoS, be deployed in a centralized manner at the exit boundary of the data center to prevent possible security threats from external networks.

- For the eastbound-westbound security inside the network, it is recommended that certain specific security measures be deployed, such as network micro-segmentation and whitelist ACL, and network traffic probe collection and analysis.

- For the cloud security at the infrastructure layer of the core network, security threats caused by vulnerabilities in the OS software itself need to be prevented. VM escape threats that an attacked VM penetrates to the upper layer and causes risks to 5G core NEs must also be a focus. It is recommended that host security scanning and hardening be routinely implemented, and monitoring software be deployed at the hypervisor level of certain

servers to prevent VM escape attacks.

- **Bearer Network Security**

The IP bearer network and optical transmission network between the RBS and the core network are the fundamental structure of the entire 5G network. If the bearer network is attacked and damaged, a large number of 5G services may be affected or interrupted. The security of the bearer network needs to be protected in the following aspects:

- **In network planning and design**, redundancy design needs to be adopted to avoid single points of failure. In addition, on the management plane of the bearer network, permission management and access authentication of accounts and passwords need to be implemented.
- **On the protocol control plane of the bearer network**, security measures such as MD5 authentication or SSL encryption can be configured to avoid possible routing protocol attacks such as BGP routing hijack attacks.
- **On the user plane of the bearer network,** IPsec security encryption can be deployed to ensure the integrity of network data packets, while avoiding illegal traffic interception or network replay attacks.

- **5G Slice Security**

Compared with 2G, 3G, and 4G networks, 5G has introduced the network slicing technology. The security of 5G network slicing needs to be protected from the following risks:

- Isolation between slices. The failure of one slice must not affect other slices.

- Secure access and use of slices. Access to a corresponding 5G network slice requires dual authentications and authorizations by the slice user (such as a government agency or an industrial mining enterprise) and the operator, ensuring legal access to and use of slice resources. Moreover, the privacy protection of Network Slice Selection Assistance Information (NSSAI) needs to be provided.

6.4 Platform Layer Security

The platform layer of 5G + New Smart City covers various intelligent analysis and processing AI platforms, big data platforms, and security middleground. The security of the platform layer includes the security of communications interfaces such as human-machine interfaces and machine-machine interfaces, and the security of platform data.

Human-machine communication involves the control of account password login and operation permissions of different systems, while **machine-to-machine communication** involves API invoking, information collection and transmission, and the transfer of operation instructions between platform systems and other related upstream or downstream component systems or NEs. In general, communication interface security at the platform layer mainly focuses on the routine maintenance and management of various accounts and passwords (such as regular password changes and password complexity requirements), and the encryption of communications interfaces (such as TLS).

Big data is the foundation and core of Smart City. The security of data at the platform layer is mainly the security of various basic data collected and stored by the big data platform (especially data involving user privacy or sensitive information on urban public safety), including data availability, integrity, and privacy. Availability is guaranteed by technologies such as data redundancy. Integrity is guaranteed by technologies such as data verification. For privacy, because the data amount is usually huge, traditional encryption technologies consume a lot of computing resources and are not feasible. Because the big data is huge in size and difficult to be completely copied and traditionally audited, access control and more effective security audit are required to improve security.

6.5 Application Layer Security

5G networks are the basic information paths of New Smart City. What truly reflects city intelligence is the vehicles of various forms carried on the information traffic network and various intelligent applications that support city management and operation. The security of the application layer consists of various application system software security, secure O&M, management, and the use of application systems. **Application system software security** mainly involves scans for vulnerabilities and the improvement of software security (including the application software itself, supporting OS databases, and other software systems), software operation logging, and software system high availability (HA) disaster recovery deployment (such as dual-host backup). **Secure O&M and management of application systems** focus more on the operation and use of application systems, and the security constraints and control of information on the operation management personnel, for example,

application system login accounts and passwords, two-factor authentication for important and sensitive operations, permission-based operation access control (available operations and function menus vary with different levels of accounts), and physical security control of personnel access of O&M operations offices and equipment rooms.

7 Conclusion

As information technologies are applied more widely in the construction of 5G + Smart City, along with the continuous upgrade of information and communications technologies, the security challenges have increased. Security measures need to be prepared, developed, and used simultaneously in the construction of Smart City. Emphasis needs to be laid on improving the standards and specifications of 5G Smart City security, demonstrating the secure application of 5G + Smart City, guaranteeing the security of 5G + Smart City network infrastructure, protecting the security of Smart City platforms, deepening the assessment of secure Smart City applications, as well as gradually building a comprehensive 5G + Smart City network security system which is jointly planned for long-term utilization and implemented step-by-step.