Security and Privacy in 5G Applications: Challenges and Solutions

Qin Qiu[1], Sijia Xu[1], and Shengquan Yu[2(✉)]

[1] China Mobile Communications Group Co., Ltd., Beijing 100032, China
{qiuqin,xusijia}@chinamobile.com
[2] Advanced Innovation Center for Future Education, Beijing Normal University, Beijing 102206, China
yusq@bnu.edu.cn

Abstract. 5G is a new generation mobile network that enables innovation and supports progressive change across all vertical industries and across our society. 5G usage scenarios face new security risks due to the technology used and the characteristics of the specific application scenario. The security risks have become a key factor affecting the development of 5G convergence services. First we summarize the technical characteristics and typical usage scenarios of 5G. Then, we analyze the security and privacy risks faced by 5G applications, and give the system reference architecture and overall security and privacy solutions for 5G applications. Based on the three major applications scenarios of eMBB, uRLLC, and mMTC, we also provide specific suggestions for coping with security and privacy risks.

Keywords: 5G · Security · Privacy · eMBB · uRLLC · mMTC · MEC · Network slicing

1 Introduction

The fifth-generation mobile networks (5G) is a new generation mobile network that enables innovation and supports progressive change across all vertical industries and across our society [1]. 5G mobile communication technology is based on a new architecture [2]. The 3rd Generation Partnership Project (3GPP) has provided complete system specifications for 5G network architecture, see Fig. 1. Components of the core network can be instantiated multiple times to support virtualization technologies and network slicing. The architecture is driven by the motivation to remove the data overlay that has been traditionally used in previous generations of mobile networks [3].

The introduction of new key technologies such as Network Function Virtualization (NFV), Software Defined Network (SDN), network slicing, Multi-access Edge Computing (MEC) [5], mm Wave Communication [6] and massive MIMO [7] will greatly improve the network's support for various applications. The International Telecommunication Union (ITU) identifies three new usage scenarios of 5G (depicted in Fig. 2),

D. Wang et al. (Eds.): SPNCE 2020, LNICST 344, pp. 22–40, 2021.
https://doi.org/10.1007/978-3-030-66922-5_2

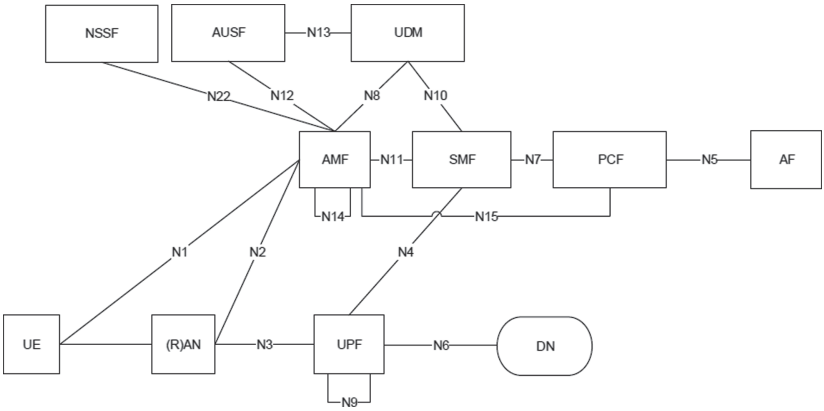

Fig. 1. 3GPP 5G system architecture for non-roaming cases [4]

which are enhanced mobile broadband (eMBB), ultra reliable and low latency communications (uRLLC), and massive machine type communications (mMTC), and proposes eight key performance indicators (KPI) [7]. Regarding these KPIs, 5G has high performances, reaching 10 times the peak rate of 4G, shortening the transmission latency to milliseconds and handling a million concurrent connections per square kilometer [8, 9]. The above-mentioned new features enable 5G to extend the traditional human-to-human communication to intelligent interconnections of man-to-things, and things-to-things. The rich and diverse 5G applications and their broad development prospects will change the traditional mode of social production, people's lifestyle and social governance, and start a new era of ubiquitous and intelligent internet. The European Union even predict

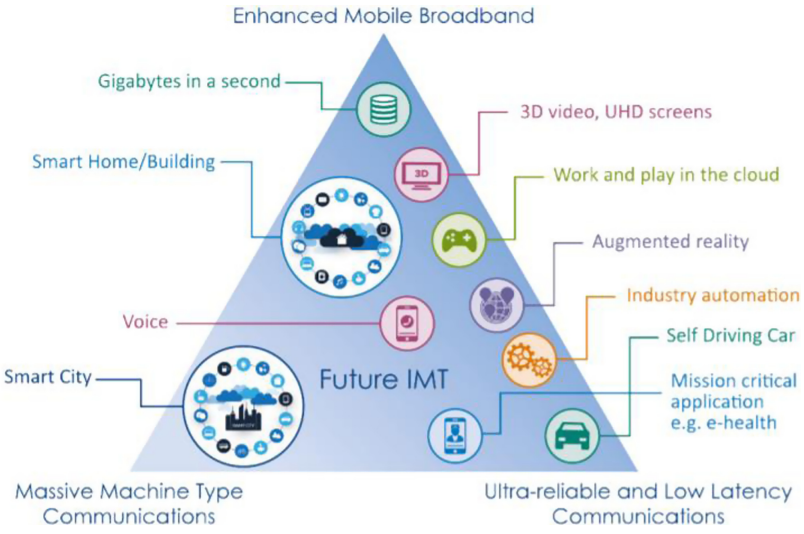

Fig. 2. 5G main usage scenarios defined by ITU [8]

that 5G will become the backbone of vital societal and economic functions – such as energy, transport, banking, and health, as well as industrial control systems [10]. According to HIS Markit [11], 5G will generate a global economic output worth $13. 2 trillion and create 22.3 million jobs by 2035.

5G applications face new security risks due to the technology used and the characteristics of the specific application scenarios, and that has become a key factor affecting the development of 5G convergence services. This paper makes contributions in the following aspects:

1. Summarizes the technical characteristics and typical application scenarios of 5G, including the features of large bandwidth, low latency, and high-volume connection introduced by new technologies such as edge computing and network slicing, and introduce smart manufacturing, smart traffic, smart grid and smart campus enabled by these technologies.
2. Analyze the security and privacy risks faced by 5G applications, including privacy leakage in the eMBB scenario, DDoS attacks in the uRLLC scenario, and remote control in the mMTC scenario;
3. Provide the system reference architecture and overall security and privacy solutions for 5G applications, including the device layer, network layer, platform layer, and service layer, and provide security and privacy goals and corresponding solutions layer by layer;
4. Provide specific suggestions for security and privacy risks for typical application scenarios, including deployment of edge computing node in the eMBB scenario, preventing application data from tampering/falsification/replay attacks in the uRLLC scenario, and lightweight equipment authentication in the mMTC scenario, etc.

The abbreviations in Table 1 are applied in this paper.

2 Usage Scenarios and Applications of 5G

The ITU [9] divides the main 5G use cases into three categories:

- *eMBB* focuses on applications with extremely high bandwidth requirements. The main applications include 4K/8K ultra high definition mobile video and immersive AR (augmented reality) and VR(virtual reality) services. It meets people's needs for a digital life.
- *uRLLC* focuses on services that are extremely sensitive to latency, such as autonomous driving/assisted driving, remote control, and industrial Internet. It meets people's needs for the digital industry.
- *mMTC* covers scenarios with requirements for high connection density, such as smart transportation, smart grids, and smart cities. It meets people's needs for a digital society.

Based on the above three types of usage scenarios, 5G enables a variety of intelligent applications, including smart manufacturing, smart traffic, smart grids, smart campus,

Table 1. Abbreviations

Abbreviations	Explanation
5G	5th Generation Mobile Network
AF	Application Function
AI	Artificial Intelligence
AMF	Access and Mobility Management Function
API	Application Programming Interface
AUSF	Authentication Server Function
CPE	Customer Premise Equipment
DDoS	Distributed Denial of Service
eMBB	enhanced Mobile Broadband
EMS	Element Management System
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IPS	Intrusion Prevention System
LTE	Long Term Evolution
MANO	Management and Orchestration
MEC	Multi-access Edge Computing
mMTC	massive Machine Type Communications
NEF	Network Exposure Function
NFV	Network Function Virtualization
NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slice Selection Function
PCF	Policy Control Function
PDCP	Packet Data Convergence Protocol
RAN	Radio Access Network
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
UPF	User Plane Function

(*continued*)

Table 1. (*continued*)

Abbreviations	Explanation
uRLLC	Ultra-Reliable and Low Latency Communications
VR/AR	Virtual Reality/Augmented Reality
WAF	Web Application Firewall
WLAN	Wireless Local Area Network

etc. We will analyze how the new technologies enable these applications in detail (see Fig. 3). In Fig. 3, the blue points are the typical 5G applications and the grey points are some specific use cases of these applications.

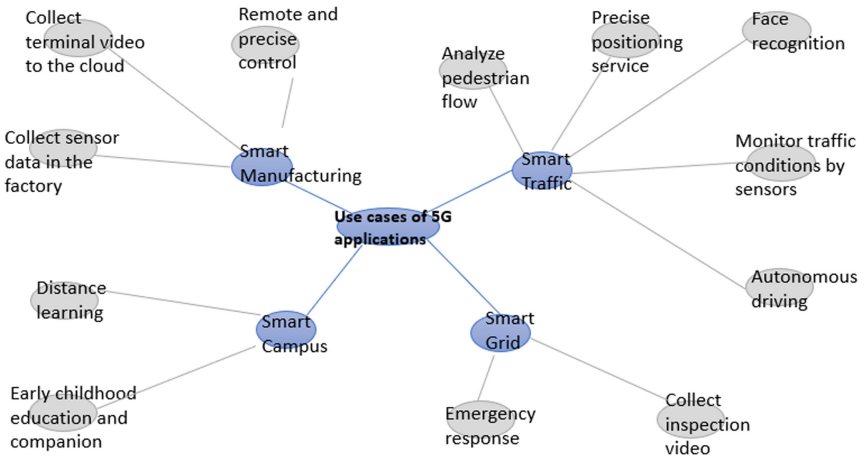

Fig. 3. Classifications of use cases of 5G applications

2.1 5G Enabled Smart Manufacturing

Smart manufacturing, today, is the ability to continuously maintain and improve performance, with intensive use of information, in response to the changing environments [12]. The applications of 5G technology in the field of intelligent manufacturing can be divided into three categories:

- utilizing 5G low-latency features, network slice, edge computing and other new technologies to ensure network quality for remote and precise control, such as engineering machinery remote control, AGV control, robot control, and on-site production line equipment control, etc.
- using 5G high-bandwidth features and edge computing technology, collecting terminal-side video to the cloud for deep analysis, such as defect detection, OCR

decoding, AR assistance, VR complex assembly, production safety behavior analysis, 5G PLC, etc.
- using 5G mass-connection, high-bandwidth characteristics and edge computing technology, collecting sensor data in the factory and transmitting it to the cloud for deep analysis, such as 5G large-scale data collection.

2.2 5G Enabled Smart Traffic

Smart traffic covers vehicles, road infrastructure, traffic management facilities, transportation planning, digital transportation platforms, and various transportation-based applications [13]. The applications of 5G technology in the transportation industry [14] can be divided into 5 categories:

- based on the user's access to the 5G base station, analyze the pedestrian flow within the coverage of the base station, such as: smart train station traffic transfer linkage, smart subway passenger flow analysis.
- based on the 5G base station's precise positioning function, to provide precise positioning services for vehicles and people, such as high-precision positioning, high-precision indoor navigation.
- based on 5G high-bandwidth transmission capabilities, using high-definition video capture and transfer back to the application platform to perform face recognition, such as passenger behavior safety analysis, and passengers exit without perception of smart train station.
- based on the 5G massive connection characteristics, connect various types of traffic sensors and other IoT devices, to analyze the health status of traffic infrastructure, and timely alert traffic conditions by analyzing various types of data received, such as infrastructure monitoring and inspection, smart subway inspections and maintenance, warning and management of smart roads.
- based on the high bandwidth, low latency, and massive connection characteristics of 5G, new technologies such as network slicing and edge computing are used to meet the high requirements of unmanned and remotely controlled driving, such as autonomous driving (autonomous driving of public transportation, freight logistics, special vehicles, autonomous driving in networked parks, 5G road test field and connected remote low-speed driving), smart ports (remotely controlled bridges, intelligent tally, unmanned transportation system), smart airport (wireless dispatch platform, driverless shuttle connection).

2.3 5G Enabled Smart Grids

Smart grid uses two-way flows of electricity and information to create a widely distributed automated energy delivery network [16]. The applications of 5G technology in the smart grid industry [15] can be divided into 2 categories:

- The application that is based on 5G low-latency features, slicing, edge computing and other new technologies, ensure emergency response of the power grid, such as distribution network differential protection, distribution network PMU, and precise load control.

- The application that is based on 5G mass-connection, high-bandwidth characteristics, and network slicing, edge computing technology, collect inspection video and transmit to the cloud for deep analysis, such as distribution automation of FTU, DTU and TTU, advanced metering, intelligent inspection, power grid emergency communications.

2.4 5G Enabled Smart Campus

Smart campus refers to a smart campus based on the Internet of Things, which integrates work, study and life. This integrated environment takes various application service systems as the carrier, and fully integrates teaching, scientific research, management and campus life. The usage scenarios of 5G in smart campuses can be summarized into two categories:

- using 5G high-bandwidth features, network slicing, and edge computing technologies for distance learning and AR content dissemination, while also ensuring campus security, such as remote teaching and research, holographic projection public courses, cloud AR interaction teaching, smart examination room, safe campus;
- use 5G slicing technology to carry out applications such as early childhood education and companion robots and 5G infant growth assessment.

3 Security and Privacy Issues in 5G Applications

3.1 eMBB Scenario

Currently, 4K/8K high-definition video and mobile roaming immersive services based on virtual reality and augmented reality have become the main application forms of eMBB, which mainly includes the following security risks:

Failure of Monitoring Means. eMBB applications produce huge volumes of traffic which would make it extremely difficult for security devices such as firewalls and intrusion detection systems deployed in existing networks to ensure adequate security protection when it comes to traffic detection, radio coverage, and data storage [17].

User Privacy Leakage. eMBB services (such as VR/AR) contain a large amount of user privacy information, such as personal information or identification, device identification, and address information, etc., and the openness of 5G networks has increased the probability of leakage of private information, for example, the situation that different application slices based on the same infrastructure network. On the other hand, due to the development of data mining technology, the way of extracting private information has become more powerful and efficient. It can associate the device identification with the user identification (such as the user's application identification), and thereby mines the user's network behavior. Therefore, eMBB business has great risk of user privacy leakage.

3.2 uRLLC Scenario

Low latency and high reliability are the basic requirements for uRLLC services. For example, if the internet of vehicles is subject to security threats in communications, it may cause danger of life. Therefore, uRLLC services require high-level security protection measures and should not add additional communication delays. The main security risks are as follows [27]:

DDoS Attacks. Attackers can use DoS/DDoS attacks to cause network congestion or wireless interference to cause communication interruptions. As a result, uRLLC services cannot run properly, service data transmission delays cannot be guaranteed, and even communication being cut off.

Data Security Risks. Attackers use vulnerabilities in devices and protocols along network data transmission paths (5G air interfaces, core networks, and the Internet) to tamper with/forge/replay application data [14], causing the drop of data transmission reliability and harm to normal application operations. For example, in the situation of Internet of Vehicles, vehicle may be out of control.

3.3 mMTC Scenario

The 5G mMTC scenario supports IoT applications with massive devices being connected. Due to the low cost, mass deployment, and limited resources (such as processing, storage, energy, etc.) of the Internet of Things [18], the following security risks are common to IoT devices:

Counterfeit Terminals. The IoT terminal has limited resources and weak processing and computing capabilities. Therefore, it is likely that access authentication will not be performed or a simple method will be adopted for access authentication (see the schemes in [19, 20]), which brings opportunities for counterfeit terminals. Illegal terminal equipment can use the loopholes in the authentication mechanism to impersonate legitimate terminals to access the IoT application platform and report fake data, causing confusion for the operation of the IoT application.

Data Tamperings. The amount of data perceived by IoT terminals is small, but it is of great significance. Attackers can tamper with application data by exploiting weaknesses along data transmission paths (air interfaces, backhaul links, and the Internet). Therefore, it is necessary to prevent attackers from tampering with the data exchanged between the terminal and the network, and to ensure the authenticity and integrity of application data.

Data Eavesdropping. The data collected by IoT terminals deployed in special environments (such as home environments and medical environments) is very sensitive and involves user privacy information. By exploiting weaknesses along data transmission paths (air interfaces, backhaul links, and the Internet), attackers eavesdrop on application data, leading to user privacy breaches. Therefore, it is necessary to prevent attackers from eavesdropping on the data exchanged between the terminal and the network, and ensure the privacy of application data.

Remote Controls. Attackers can remotely access and control IoT terminals through software and hardware interfaces by taking advantages of the simplicity of IoT terminals and weak security protection capabilities, then use the captured terminals to launch attacks that interfere with the normal operation of IoT services [21–25].

Based on the above analyses, typical security and privacy risks of use cases in smart manufacturing, smart traffic, smart grids and smart campus are listed as below, see Table 2.

Table 2. The security and privacy risks of typical applications

Typical applications	Specific use cases	Risks examples
Smart manufacturing	AR assistance, VR complex assembly	Failure of monitoring means
	Collecting sensor data of IoT device	Data tampering & Data eavesdropping
Smart traffic	Connected vehicles	DDoS attacks& Data security risks
	Passenger behavior safety analysis	Failure of monitoring means
Smart grids	Distribution network differential protection and precise load control	DDoS attacks
	Customized network slice to satisfy the low time latency requirement	Counterfeit terminals & Management of network slices
Smart campus	Distance learning and AR content dissemination	Failure of monitoring means& User privacy leakage

4 Security and Privacy Solutions in a Systematic View

4.1 Reference Architecture of 5G Application Systems

As shown in Fig. 4, 5G applications can be modeled into of four layers – the terminal layer, network layer, platform layer, and service layer [26, 28] – from the bottom up.

- **The terminal layer** involves mobile phone terminals, and VR/AR terminals for individual users (to C), as well as industrial control terminals, CPEs, and various sensors for vertical industries (to B).
- **The network layer** is an end-to-end 5G network, including the radio base stations (RBS), MEC, the bearer network, the 5G Core network, and 5G network slices from base stations to the core network.

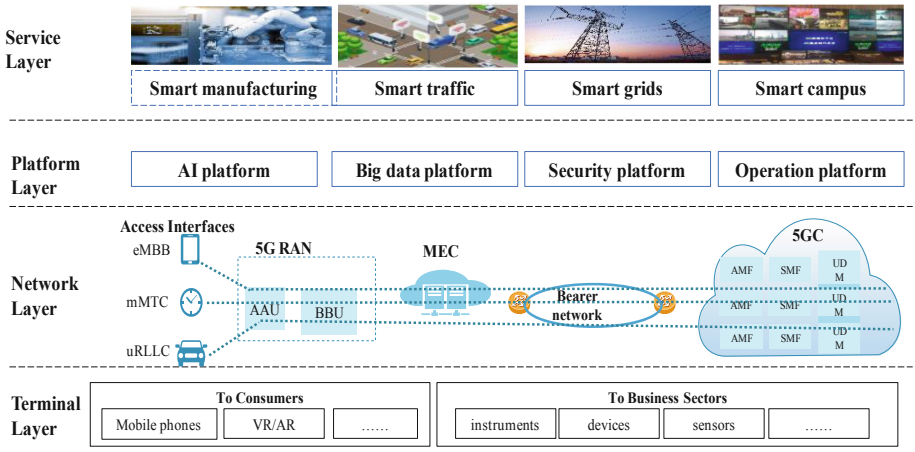

Fig. 4. Reference architecture of 5G applications

- **The platform layer** contains public IT platform systems such as the AI platform, big data platform, operation platform, and security platform. It is recognized that innovative technologies, such as artificial intelligence and big data, are good means to improve security and privacy capabilities [47, 48].
- **The service layer** is composed of 5G enabled smart application systems such as smart manufacturing, smart traffic, smart grids and smart campus.

Each layer has corresponding security goals and solutions, as shown in Table 3.

4.2 Solutions on Terminal Layer

A large number of 5G 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 become easy and likely targets to be hacked [23].

Firstly, 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 to 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 the first time to prevent major global negative effects on network services. Besides, some proactive and preventive measures are recommended in terms of terminal exception handling and signaling registration.

Secondly, for the prevention of risks brought by terminal hacking, it is recommended that certain security capabilities such as SSH security login, TLS transmission encryption, and built-in security chip being built in terminals in terms of access authentication [24, 25] on the management and O&M plane as well as encryption protection on the signaling/data plane.

Table 3. Security and privacy solutions for 5G applications

Layer	Targets	Security and privacy Solutions
Terminal layer	Prevent and defend against DDOS attacks initiated by exploited terminals	• Attack detection and self-protection mechanisms (such as active flow control) • Proactive preventive measures, e.g. terminal exceptions handling and signaling registration
	Prevent various damage caused by exploited terminals to industry production and applications	• Access authentication [49, 50] on the operation and maintenance side • Encryption protection on the signaling/data plane (such as SSH secure login, TLS transmission encryption, and built-in security chip, etc.)
Network layer	Base station air interface security	• Defense Eavesdropping and tampering of user data from air interface • Defense DDOS attack from air interface • Pseudo base station detection [52]
	MEC security	• Physical environment security control • Enterprise and operator network isolation
	5GC security	• Manage operation and maintenance plane security • Network north-south border security • East-west security within the network • Cloud-based security of the core network
	Bearer network security	• Network redundant design • Account authority management and access authentication • Increase security measures on control protocols • User plane security encryption
	5G slicing security [43]	• Isolation between slices • Secure access and use of slices • Privacy protection

(*continued*)

Table 3. (*continued*)

Layer	Targets	Security and privacy Solutions
Platform layer	Communication interface security	• Routine maintenance of various account passwords • Encryption of communication interfaces such as TLS, etc.
	Platform data security	• Data availability, integrity and privacy
Service layer	Software security of the application	• Vulnerability scanning of the software • Software operation logging • Highly available disaster recovery of software systems (such as dual-machine backup)
	Security operation and maintenance management of the application system	• Security constraints and controls for application system, e.g. multi-factor authentication for important sensitive operations • Physical security control (personal access control) of O & M operations office/machine room, etc.

4.3 Solutions on Network Layer

From the perspective of network components, the noteworthy aspects of network layer security include security in the RAN base station air interfaces [51], MECs, 5G Core, bearer networks, and 5G slices.

- Base Station Air Interface Security

Air interfaces between 5G UEs and base stations mainly have to deal with three types of security threats:

– Countermeasures of 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.
– Countermeasures of 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.
– Countermeasures of 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

To avoid physical attacks and cross-network penetration and infection of network, 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 [29–35].

- 5G Core Security

The security of the 5G Core has 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.

– The security of Operation & Management plane. For MANO, EMS and other systems on the O&M plane, an access security control system 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.
– 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, being deployed in a centralized manner at the exit boundary of the data center to prevent possible security threats from external networks.
– The security of eastbound-westbound security inside the network. It is recommended that certain specific security measures to be deployed, such as network micro-segmentation and whitelist ACL, and network traffic probe collection and analysis.
– Cloud and virtualization security. Security threats caused by vulnerabilities in the OS software itself need to be prevented. VM escape threats must also be a focus where an attacked VM penetrates to the upper layer and causes risks to 5G core NEs. It is recommended that host security scanning and hardening being routinely implemented, and monitoring software being deployed at the hypervisor level of certain servers to prevent VM escape attacks [36–39].

- Bearer Network Security

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, to prevent illegal traffic interception or network replay attacks.

- 5G Slice Security

The security of 5G network slicing [43] needs to be protected by the following measures:

– 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 and use of slice resources. Moreover, the privacy protection of Network Slice Selection Assistance Information (NSSAI) needs to be provided.

4.4 Solutions on Platform Layer

The platform layer covers various intelligent analysis and processing AI platforms, big data platforms, and IT middleground [47, 48]. The security of this layer includes the following aspects.

- The security of communications interfaces. 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).
- The security of platform data. Big data is usually used in 5G applications. The security of data at the platform layer involves the security of various basic data collected and stored by the big data platform (especially data involving user privacy or sensitive information on 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, as the data amount is usually huge, more effective access control and security audit are required.

4.5 Solutions on Service Layer

The security of the service layer consists of various application system software security, secure O&M of application systems.

- Application system software security mainly involves scans for vulnerabilities and the improvement of software security (including the application software itself,

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 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, multi-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.

5 Countermeasures Against Security and Privacy Risks in 5G Applications

Based on the systematic security and privacy solutions proposed above, the following specific security measures are recommended for 5G application service developers and providers in different application scenarios [40–42]. The related layers in the reference architecture to deploy these countermeasures are also suggested (see Table 4).

5.1 eMBB Scenario

- Deploy application traffic monitoring at edge computing [35] nodes and support suspension of high-risk services in specific cases
- The secondary authentication and key management mechanism are used to perform secondary identity authentication and authorization between the terminal and the eMBB application service platform to ensure the authenticity of the terminal and platform identity and the legality of application. At the same time, negotiate and manage the service layer key between the two sides to encrypt and protect user data,thus preventing attackers from eavesdropping;
- In applications with high security requirements, the user plane of the 5G network can be protected by physical isolation or encryption to ensure the security of user data transmission between network functions;
- The network slicing or data dedicated line is used between the operator's 5G core network and the eMBB application service platform to establish a secure data transmission channel to ensure the security of user business data transmission.

5.2 uRLLC Scenario

- Establish a two-way identity authentication mechanism between the user terminal and the application server to prevent fake users from establishing connections.
- Deploy anti-DDoS capabilities to prevent network congestion, wireless interference, and communication link disruptions.
- Through the security capabilities deployed at edge computing, as well as data integrity protection, time stamp, serial number and other mechanisms, to prevent application data from being tampered/falsified/replayed and ensure the reliability of data transmission [32];

Table 4. Countermeasures against Security and privacy risks in 5G Applications

Risks	Countermeasures	Related layer
eMBB scenario		
Failure of effective monitoring means	• Application traffic monitoring at edge computing [35] nodes, suspension of high-risk services in specific cases	Network layer
User privacy leakage risk	• Perform secondary identity authentication and authorization between the terminal and the eMBB application service platform • Negotiate and manage the service layer key between the two sides to encrypt and protect user data • Physical isolation or encryption • Network slicing [43] or data dedicated line	Terminal layer/network layer/service layer
uRLLC scenario		
DDoS attack risk	• Two-way identity authentication mechanism between the user terminal and the application servers • Deploy anti-DDoS capabilities	Network layer and terminal layer
Data security risks	• Through the security capabilities deployed at edge computing [26], as well as data integrity protection, time stamp, serial number and other mechanisms [44]	Network layer
mMTC scenario		
Counterfeit terminal	• Using lightweight [45, 49, 50] security algorithms, simple and efficient security protocols to implement two-way authentication	Terminal layer
Data tampering and Eavesdropping	• Encrypt and protect the integrity of sensitive application data generated by IoT terminals [44]	Terminal layer
Remote control	• Deploy security monitoring methods [47, 48] to timely detect and prevent massive IoT devices from being controlled	Terminal layer

5.3 mMTC Scenario

- Using lightweight security algorithms, simple and efficient security protocols to implement two-way authentication between IoT terminals and the network to ensure that the access terminals are secure and reliable.
- Encrypt and protect the integrity of sensitive application data generated by IoT terminals to prevent attackers from eavesdropping, tampering, forging, and replaying business data on the transmission path
- Deploy security monitoring methods [47, 48] to timely detect and prevent massive IoT devices from being controlled, to prevent these devices from being used maliciously, such as launching DDoS attacks on air interfaces and service platforms, etc., causing network congestion and causing mMTC services to fail [46].

6 Conclusions

5G is deeply integrated with social life and vertical industries, and the security and privacy of the 5G ecosystem is largely influenced by application developers, service providers, as well as network operators and equipment suppliers. The achievement of security and privacy in 5G applications requires a comprehensive and systematic design, as well as the deployment of proper security measures according to the specific application scenarios and the needs of the industry.

In the future, in line with the continuous development of 5G applications, the security level will continue to improve. On the one hand, along with the evolution of 5G technology, the changes in application requirements, and the development of security offensive and defensive technologies, stakeholders should continue to enrich 5G security solutions, including the adoption of 5G network slicing, authentication capabilities, and other network capabilities to provide security for upper-layer applications; on the other hand, 5G network security will continue to develop in the direction of intelligence, providing a flexible and customizable security capability to facilitate vertical industries to choose security capabilities and management methods that match industry needs.

Acknowledgments. This paper is supported by the construction project of the Joint Laboratory for Mobile Learning, Ministry of Education-China Mobile Communications Corporation (no. ML2012934).

References

1. Bedo, J., Ayoubi, S., Filippou, M., et al.: 5G innovations for new business opportunities. In: Mobile World Congress, Barcelone, Spain. 5G Infrastructure Association, Mobile World Congress 2017, 5G IA Event (2017)
2. TS 22.261. Technical Specification Group Services and System Aspects; Service Requirements for the 5G system; Stage 1, 3GPP
3. 5G Network Architecture and Security, DCMS Phase 1 5G Testbeds & Trials Programme (2018)
4. TS 23.501, System Architecture for the 5G System, 3GPP

5. GS MEC-002. MEC Technical Requirements, ETSI
6. Niu, Y., Li, Y., Jin, D., et al.: A survey of millimeter wave communications (mmWave) for 5G: opportunities and challenges. Wirel. Netw. **21**(8), 2657–2676 (2015)
7. Gavrilovska, L., Rakovic, V., Atanasovski, V.: Visions towards 5G: technical requirements and potential enablers. Wirel. Pers. Commun. **87**(3), 731–757 (2015). https://doi.org/10.1007/s11277-015-2632-7
8. Setting the Scene for 5G: Opportunities & Challenges. https://www.itu.int/en/ITU-D/Documents/ITU_5G_REPORT-2018.pdf
9. IMT Vision – Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond, ITU-R M.2083-0
10. European Commission, Commission Recommendation of 26.3.2019 Cybersecurity of 5G networks
11. IHS Markit: How 5G technology contribute to the global economy The 5G Economy (201 9)
12. Jung, K., Kulvatunyou, B., Choi, S., et al.: An Overview of a Smart Manufacturing System Readiness Assessment (2017)
13. Bao, Z.: Discussing 5G network technologies in smart traffic construction. China ITS J. **226**(01), 81–82+102 (2019)
14. Basudan, S., Lin, X., Sankaranarayanan, K.: A privacy-preserving vehicular crowdsensing based road surface condition monitoring system using fog computing. IEEE Internet of Things J. (2017)
15. Saxena, N., Roy, A., Kim, H.: Efficient 5g small cell planning with eMBMS for optimal demand response in smart grids. IEEE Trans. Ind. Inform. **13**(3), 1471–1481 (2017)
16. Fang, X., Misra, S., Xue, G., et al.: Smart grid—the new and improved power grid: a survey. IEEE Commun. Surv. Tutor. **14**(4), 944–980 (2012)
17. CAICT, IMT 2020(5G) Promotion Group. 5G security Report (2020)
18. Fan, K., Gong, Y., Liang, C., et al.: Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G. Secur. Commun. Netw. **9**(16) (2016)
19. Wang, D., Wang, P.: Two birds with one stone: two-factor authentication with security beyond conventional bound. IEEE Trans. Dependable Secure Comput. **15**(4), 708–722 (2018)
20. He, D., Wang, D., Wu, S.: Cryptanalysis and improvement of a password-based remote user authentication scheme without smart cards. Inf. Technol. Control **42**(4), 170–177 (2013)
21. GTI. 5G Network Security Consideration white paper v1.0. GTI (2019)
22. ENISA Threat Landscape for 5G Networks, November (2019)
23. Ji, X., Huang, K., Jin, L., et al.: Review of 5G security technology. Mob. Commun. **43**(01), 40–45+51 (2019)
24. Wang, D., Ma, C.G., Zhang, Q.M., et al.: Secure password-based remote user authentication scheme against smart card security breach. J. Netw. **8**(1), 148–155 (2013)
25. Wang, D., Zhang, X., Zhang, Z., et al.: Understanding security failures of multi-factor authentication schemes for multi-server environments. Comput. Secur. **88**, 1–13 (2020)
26. Ahmad, I., Kumar, T., Liyanage, M., et al.: Overview of 5G security challenges and solutions. IEEE Commun. Stand. Mag. **2**(1), 36–43 (2018)
27. Schneider, P., Günther, H.: Towards 5G Security. IEEE Trustcom/bigdatase/ispa. IEEE Computer Society (2015)
28. Zhang, K., Ni, J., Yang, K., et al.: Security and privacy in smart city applications: challenges and solutions. IEEE Commun. Mag. **55**(1), 122–129 (2017)
29. ISO/IEC 23188 Information technology – Cloud Computing – Edge Computing Landscape
30. ITU-T X.5Gsec-netec "Security capabilities of network layer for 5G edge computing"
31. ITU-T X.5Gsec-ecs "Security Framework for 5G Edge Computing Services"
32. ETSI GS MEC 003 V1.1.1 Mobile Edge Computing (MEC); Framework and Reference Architecture (2016)

33. ETSI GS MEC-IEG 004 V1.1.1 Mobile-Edge Computing (MEC); Service Scenarios
34. ETSI GS MEC 002 V1.1.1 Mobile Edge Computing (MEC); Technical Requirements
35. Zhang, J., Zhao, Y., Chen, B., et al.: Research on edge computing data security and privacy protection. J. Commun. (2018)
36. ETSI GS NFV-SEC 001 V1.1.1 Network Functions Virtualisation (NFV); NFV Security; Problem Statement (2014)
37. ETSI GS NFV-SEC 003 V1.1.1: Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance (2014)
38. ETSI GS NFV-SEC 012 V3.1.1 Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components (2017)
39. ITU-T X.1038: Security requirements and reference architecture for software-defined networking
40. Zhang, B., Yuan, J., Qiu, Q., et al.: Research on 5G security technology and development. In: Proceedings of "5G+" China Mobile Science and Technology Association, pp 1–5 (2019)
41. Fan, N., Liu, G., Shen, J.: Analysis of mobile network security for operators in the initial stage of 5G commercialization. China Inf. Secur. **7**, 85–87 (2019)
42. China Mobile 5G Joint Innovation Center. White Paper on 5G Security for the Medical Industry (2019)
43. China Mobile 5G Joint Innovation Center. 5G Slicing Security White Paper for Vertical Industries (2018)
44. Ferrag, M.A., Maglaras, L., Argyriou, A., et al.: Security for 4G and 5G cellular networks: a survey of existing authentication and privacy-preserving schemes. J. Netw. Comput. Appl. S1084804517303521 (2017)
45. Das, A.K., Zeadally, S., Wazid, M.: Lightweight authentication protocols for wearable devices. Comput. Electr. Eng. S0045790617305347 (2017)
46. Gope, P., Lee, J., Quek, T.: Resilience of DoS attacks in designing anonymous user authentication protocol for wireless sensor networks. IEEE Sens. J. **17**(2), 498–503 (2017)
47. Wang, Y., Chu, W., Fields, S.: Detection of intelligent intruders in wireless sensor networks. Future Internet **8**(1), 2(2016)
48. Buczak, A., Guven, E.: A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun. Surv. Tutor. **18**(2), 1153–1176 (2016)
49. Duan, X., Wang, X.: Authentication handover and privacy protection in 5G hetnets using software-defined networking. Commun. Mag. IEEE **53**(4), 28–35 (2015)
50. Luo, H., Wen, G., Su, J., Huang, Z.: SLAP: succinct and lightweight authentication protocol for low-cost RFID system. Wirel. Netw. **24**(1), 69–78 (2016). https://doi.org/10.1007/s11276-016-1323-y
51. Ku, Y., Lin, D., Lee, C., et al.: 5G radio access network design with the fog paradigm: confluence of communications and computing. IEEE Commun. Mag. **55**(4), 46–52 (2017)
52. Shao, J., Zhu, D., Jin, H., et al.: A joint detection method for identifying pseudo base station based on abnormal access parameters. DEStech Transactions on Engineering and Technology Research (2017). https://doi.org/10.12783/dtetr/iceta2016/7000