1

Introduction to 5G Wireless Systems

Fifth-generation wireless networks, or 5G, are the fifth-generation mobile wireless telecommunications beyond the current 4G/International Mobile Telecommunications (IMT)-Advanced Systems [Panwar et al., 2016]. 5G wireless network is not only an evolution of the legacy 4G cellular networks but also a new communication system that can support many new service capabilities [Fang et al., 2017a]. In this chapter, we will introduce a general background of 5G wireless networks and 5G security, including motivations and objectives, security drives and requirements, and a general 5G wireless network architecture.

1.1 Motivations and Objectives of 5G Wireless Networks

The research and development of 5G technology is focused on achieving advanced features such as enhanced capacity to support a greater number of users at faster speeds than 4G, increased density of mobile broadband users to improve coverage [Xu et al., 2021], and supporting device-to-device (D2D) communications and massive machine-type communications [NGMN Alliance, 2015]. 5G planning also aims to provide better network performance at lower latency and lower energy consumption to better support the implementation of the Internet of Things (IoT) [Andrews et al., 2014]. More specifically, there are eight advanced features of 5G wireless systems as follows [Warren and Dewar, 2014]:

- Data rate: 1–10 Gbps connections to endpoints in the field;
- Low latency: 1-ms latency;
- Bandwidth: 1000× bandwidth per unit area;
- Connectivity: 10–100× number of connected devices;
- Availability: 99.999% availability;
- Coverage: 100% coverage;
- Network energy efficiency: 90% reduction of network energy usage;
- Device energy efficiency: Up to 10 years of battery life for low-power devices.

To achieve these eight advanced network performance features, various technologies [Agiwal et al., 2016] are applied to 5G systems, such as heterogeneous networks (HetNet), massive multiple-input multiple-output (MIMO), millimeter wave (mmWave) [Qiao et al., 2015], D2D communications [Wei et al., 2016], software-defined network (SDN) [Dabbagh

5G Wireless Network Security and Privacy, First Edition. Dongfeng (Phoenix) Fang, Yi Qian, and Rose Qingyang Hu.

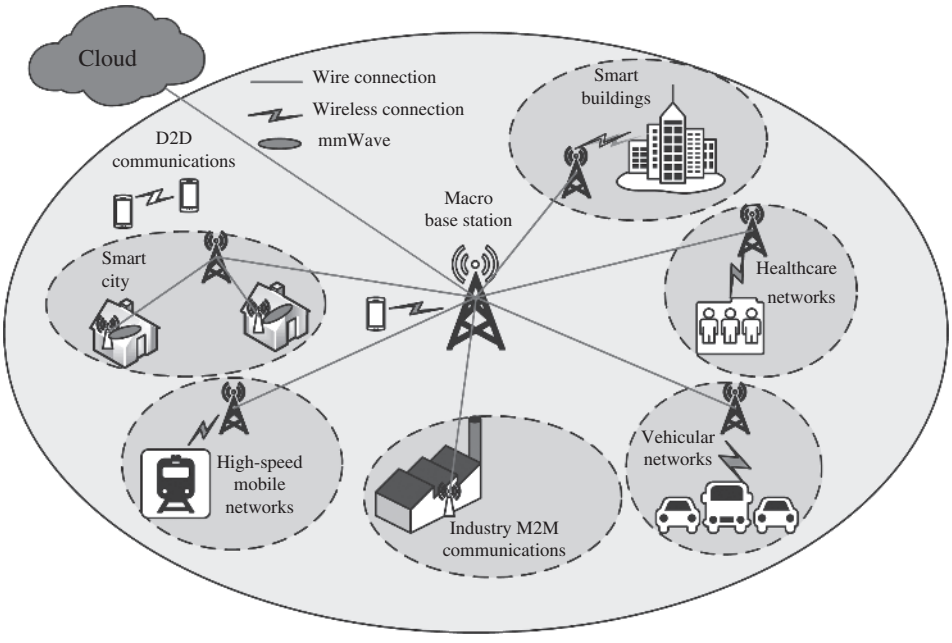

Figure 1.1 A generic architecture for 5G wireless systems.

et al., 2015], network functions virtualization (NFV) [Zhang et al., 2015], and networking slicing [NGMN Alliance, 2016]. The standardization process for 5G wireless systems has been carried out. Figure 1.1 illustrates a generic 5G wireless systems.

5G wireless systems can provide not only traditional voice and data communications but also many new use cases [Xu et al., 2022, Wang et al., 2021b], new industry applications, and a multitude of devices and applications to connect the society at large [AB Ericsson, 2018] as shown in Figure 1.1. Different 5G use cases are specified, such as vehicle-to-vehicle and vehicle-to-infrastructure communications [Fang et al., 2019b], industrial automation, health services, smart cities, and smart homes [Global Mobile Suppliers Association, 2015]. It is believed that 5G wireless systems can enhance mobile broadband with critical services and massive IoT applications [Qualcomm, 2016]. With the new architecture, technologies, and use cases in 5G wireless systems, it will face new challenges to provide security and privacy protections [Huawei, 2015].

1.2 Security Drives and Requirements

To accomplish the objectives of 5G wireless networks, several fundamental security drivers and requirements are necessary. Figure 1.2 illustrates the main drives for 5G wireless security as supreme built-in security, flexible security mechanisms, and automation. Supreme built-in security is needed since, in 5G, new use cases, new technologies, and new networking paradigms are introduced. The other use cases can introduce specific requirements, such as ultra-low latency in user communications, which will require improving the

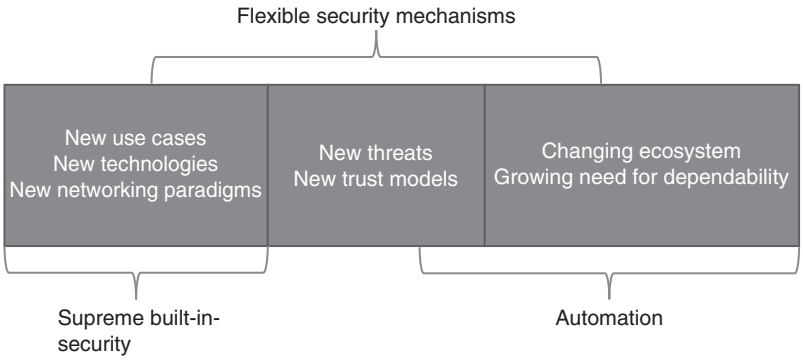

Figure 1.2 Security drives and requirements for 5G wireless security.

performance of the current security mechanisms. New technologies not only yield advanced service capabilities but also open the door to vulnerabilities and thus impose new security requirements in 5G [Liyanage et al., 2016]. In HetNet, different access technologies may have different security requirements, and a multi-network environment may need highly frequent authentications with stringent delay constraints [Wang et al., 2016b]. Massive MIMO has been deemed a critical 5G technique to achieve higher spectral efficiency and energy efficiency. It is also considered a valuable technique against passive eavesdropping [Deng et al., 2015]. Furthermore, SDN and NFV in 5G will support new service delivery models and thus require new security aspects [Chen et al., 2016b, Tian et al., 2017]. With the advent of 5G networking paradigms, a new security architecture is needed. To address these issues, security must be considered an integral part of the overall architecture and should initially be integrated into the system design.

To support various use cases, new technologies, new networking paradigms, new threats, new trust models in an optimal way, and flexible security mechanisms are needed with changing ecosystem and growing need for dependability. Based on the current research on 5G wireless networks, security services on 5G wireless networks have more specific requirements due to the advanced features that 5G wireless networks have, such as low latency, and high energy efficiency. With various applications on 5G wireless networks and their network performances, flexible security mechanisms are desired with better efficiency performance [Xu et al., 2019].

The trust models of the legacy cellular networks and 5G wireless networks are presented in Figure 1.3 [Huawei, 2015]. Not only full trust but also semi-trust or not trust are considered. Authentications are required not only between subscribers and the two operators (the home and serving networks) but also among service parties in 5G wireless networks. Moreover, for the use case of vertical industries, the security demands vary significantly among different applications. For instance, mobile devices require lightweight security mechanisms as their power resource constraint, while high-speed services require efficient security services with low latency. Therefore, the general flexibility for 5G security mechanisms is another critical requirement [Schneider and Horn, 2015]. Authentication management in 5G is more complex due to various types of and a massive number of devices connected. For different applications, different authentication models can be implemented. In Figure 1.3, user authentication can be done by the network provider, service provider, or both.

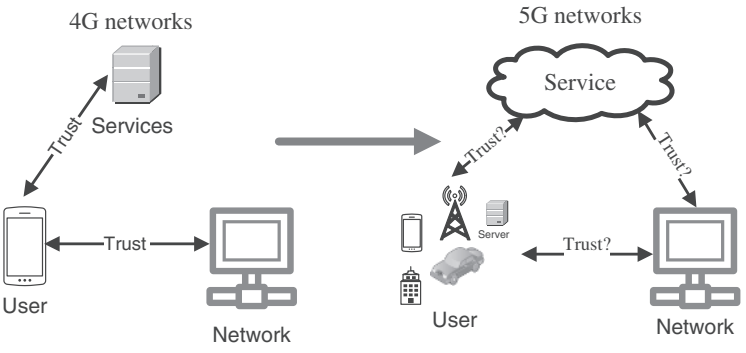

Figure 1.3 Trust model of 4G and 5G wireless networks.

Besides the supreme built-in security and flexibility security mechanisms, security automation is also a key element. It combines automated holistic security management with automated and intelligent security controls [NOKIA, 2017]. Since more personal information is used in various applications, such as surveillance applied over 5G wireless networks, privacy concerns escalate. Moreover, various services in 5G can be tied closer than before. For example, the fixed telephone line, internet access, and TV service can be terminated simultaneously due to the outage of a major network [Huawei, 2015]. Therefore, security automation is needed to make the 5G system robust against various security attacks.

1.3 5G Wireless Network Architecture

1.3.1 Overview of the 5G Wireless Network Architecture

The 5G wireless network architecture is introduced here. As shown in Figure 1.4, the illustrated general 5G wireless network architecture includes a user interface, a cloud-based heterogeneous radio access network, a next-generation core, distributed edge cloud, and a central cloud. The cloud-based heterogeneous radio access network can combine virtualization, centralization, and coordination techniques for efficient and flexible resource allocation. Based on different use cases, 3GPP classifies more than 70 different use cases into four different groups such as massive IoT, critical communications, network operation, and enhanced mobile broadband. In the cloud-based heterogeneous access network, besides the 3GPP access and non-3GPP access, other new radio technologies will be added for more efficient spectrum utilization. In the first stage of 5G, the legacy evolved packet core (EPC) will still be valid. Network slicing enables different parameter configurations for the next-generation core according to different use cases. New flexible service-oriented EPC based on network slicing, SDN, and NFV will be used in the next-generation core as virtual evolved packet core (VEPC) shown in Figure 1.4. The VEPC is composed of modularized network functions. Based on different use cases, the network functions applied to each VEPC can be various. In the VEPC, the control plane and user plane are separated for the flexibility and scalability of the next-generation core. Edge cloud is distributed to

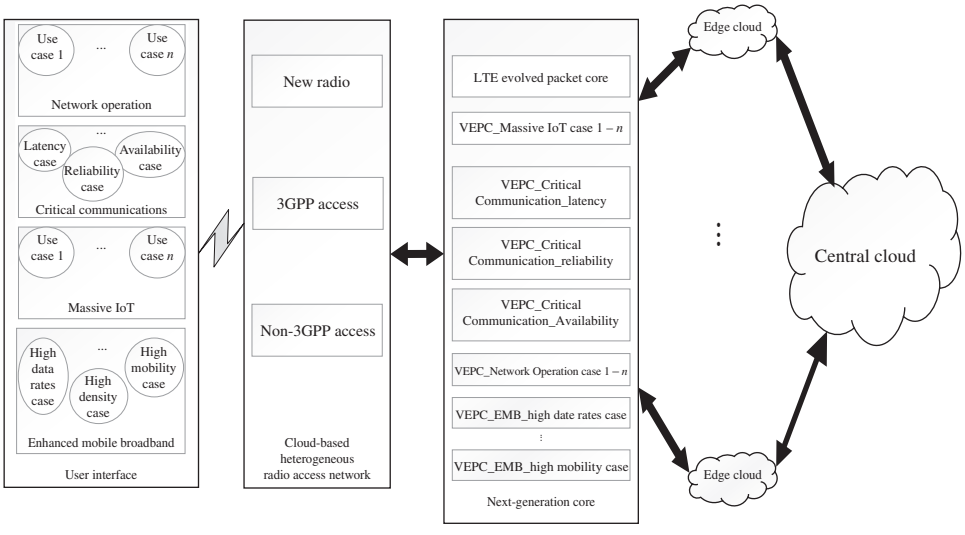

Figure 1.4 A general 5G wireless network architecture.

improve service quality. The central cloud can implement global data share and centralized control.

1.3.2 Comparison Between the Legacy Cellular Network and the 5G Wireless Network

Compared with legacy cellular networks, 5G wireless networks introduce some new perspectives and changes. (i) User equipment and services are not limited to regular mobile phones and regular voice and data services. Based on different use cases and requirements, user interfaces are classified into four different groups such as massive IoT, critical communications, network operation, and enhanced mobile broadband. Every use case can affect the radio access selection and VEPC functions. (ii) In addition to 3GPP access and non-3GPP access in the cloud-based heterogeneous radio access network, the 5G access network includes other new radios, which build the foundation of wireless standards for the next-generation mobile networks for higher spectrum utilization. The new radios can support the performance and connectivity requirements of various use cases in 5G wireless networks. Moreover, there are many technologies applied to the access network to improve the network performance, such as massive MIMO, HetNet, and D2D communications. (iii) The next-generation core will be based on the cloud using network slicing, SDN, and NFV to handle different use cases. The flexible service-oriented VEPC will be applied. With network slicing, SDN, and NFV, different network functions can be applied to the service-oriented VEPC for different use cases. The next-generation core is expected to be access-independent. Separation of control and user plane is important to achieve an access-agnostic, flexible, and scalable architecture. (iv) Edge cloud is applied to 5G wireless networks to improve the performance of the network, such as latency.

1.4 Conclusion

A general background of 5G wireless networks is introduced in this chapter. The motivations and objectives of 5G wireless networks are presented. With the expected improvements in 5G performance, security drives, and requirements are discussed. A general 5G wireless network architecture is illustrated in this chapter. Moreover, a comparison of a 5G wireless network architecture and legacy cellular network architecture is analyzed. It is clear that the 5G wireless network introduces significant flexibility to support new use cases and corresponding different service requirements. New security architecture and mechanisms are needed in 5G networks.