Securing Next-Generation Wireless Networks: Challenges and Opportunities. (extended abstract)

Alex Sprintson[0000−0002−5768−5800]

Texas A&M University, College Station TX 77843, USA
spalex@tamu.edu

Abstract. This paper outlines the security and privacy issues in the design of next-generation wireless broadband networks. As such networks are expected to play an increasingly important role in modern society, there is an increasing focus on their security and robustness. Such networks are expected to satisfy stringent security requirements that will guarantee uninterrupted service to the users. The goal of this paper is to present a taxonomy of such requirements that will be relevant in the long and short terms. The paper will also outline the directions for future research in this area that will enable system operators to meet these requirements.

Keywords: Wireless broadband Networks · Network Security · Network Privacy.

1 Introduction

Wireless broadband networks have seen continuous development and evolution over the last two decades. Each new generation of cellular technology brought new capabilities, including increasing data rate, lower latencies, and increased coverage.

It is widely recognized that broadband wireless networks have reached a turning point in their evolution. Fifth-generation and beyond cellular networks are expected to connect billions of heterogeneous Internet of Thing (IoT) devices, enable machine-to-machine communications, and support a variety of mission-critical services in multiple application domains, including transportation, public safety, and defense. The next-generation networks are expected to have a high degree of reliability and availability, and meet strict requirements on performance and service assurance. This is in contrast to today's cellular systems which are designed to serve users utilizing smartphones to communicate and access the content. The new capabilities will enable exciting new applications such as Augmented Reality/Virtual Reality (AR/VR) and video analytics.

The future wireless broadband networks constitute a complex system, which leverages modern technologies, including software-defined networking (SDN) and Network Function Virtualization (NFV). The transition to SDN leads to a great

emphasis on software implementation, including at the base station radio level. In addition, the future broadband networks are expected to rely on cloud technologies, including edge cloud, to support network operation. Furthermore, such networks can benefit from the convergence and maturation of multiple technologies, including mmWave technologies for high data rate, ultra-low latency applications, utilizing beamforming and massive MIMO technologies for increasing date rate and increasing transmission rates, as well as reaching mobile end-points inside the buildings.

The future mobile networks are expected to attract new groups of uses can use different slices of the networks for their unique applications. The service providers can offer mobile infrastructure as a service to different industries such as defense, smart grid, transportation, and smart agriculture, that have unique requirements. As a result, such networks will attract new stakeholders. Such networks are expected to provide not only connectivity services but will also offer real-time compute and control capability, as well as facilitate content distribution.

Due to the increasing reliance of the different sectors of modern society on mobile broadband services, their security and reliability have become issues of paramount importance. However, the current focus of the developers, standard bodies, and network operators is on performance and functionality, while security and resilience remain an afterthought. The system design lacks principled approaches, which could result in multiple security vulnerabilities and unpredictable behaviors.

The goal of this paper is to highlight fundamental longer-term challenges in security next-generation networks. We will also outline several promising approaches that have the potential to address these challenges.

2 Security goals and challenges

Security a complex system that spans a very large geographical area is a formidable task. The mobile broadband system is expected to be one of the largest engineering systems in the world. The complex structure of the system, its reliance on wireless medium for user access, and the backhaul, its large user base creates many attack surfaces for malicious agents. Furthermore, the limited capabilities of the IoT devices make it harder to deploy sophisticated security functions, which will force network designers to rely on light-weight security methods. It is likely that some elements of the system will remain exposed and highly vulnerable to attacks.

2.1 Goals

The main goal of the mobile broadband system is to provide *end-to-end* security, which will ensure that every network application can function securely. This goal can be only be achieved through holistic solutions that coordinate security functions among various network elements.

Another important goal for the next-generation wireless broadband networks is to achieve a drastic reduction (several orders of magnitude) in the overall number of vulnerabilities compared to the current systems. This is due to the fact that future networks can be used in life-critical systems and the failure of such networks to operate can result in very significant economic damage.

The security requirements can be different for a different group of users. For example, the network slices that are used for industrial control applications or intelligent transportation systems must higher levels of security and reliability than slices that serve traditional consumers.

Furthermore, future networks can offer security as a service. This could include a formal specification of the provided security guarantees as well as an agreement on the consequences of these security guarantees are not met.

Enabling high levels of security should come at a reasonable cost and incur minimum overhead in terms of system efficiency. Accordingly, the major goal of the system designers is to strike a reasonable trade-off between security and efficiency.

2.2 Challenges

In general, the more complex system is more difficult it is to secure it. In particular, the large number of configuration parameters will result in a negative impact on the attack surface. The next-generation systems are expected to offer great flexibility, which makes securing it more difficult.

Securing next-generation systems requires appropriate solutions to the following challenges:

Physical layer security. The air-interface and radio access networks use a shared medium hence are vulnerable to intentional interference and jamming. The next-generation systems are expected to share spectrum among multiple service providers and technologies, which can make it harder to detect malicious users.

Hardware and Supply Chain security This includes a trustworthy hardware design that ensures that each hardware component of the system functions according to the specification. Since the network devices are expected to be manufactured by different providers, factory device identity management tools can be used to mitigate potential risks.

Software/ Software-Defined Networking (SDN) Security. With the advent of SDN of approaches, more network functions will be implemented in software. The software implementations, however, are prone to vulnerabilities and errors.

Slicing/Virtualization Security. Since the future networks support different slices, there is a need to properly separate them so the users or different slides cannot adversely affect each other. The orchestration mechanisms should include security features to eliminate attack doors at the time of slide creation and resource allocation.

IoT Security. The large number of IoT devices connected to the future wireless broadband networks will probably be the weakest link in the entire

system. Light-weight tools will be required to support end-to-end encryption and identify management for such devices. Developing scalable security mechanisms will be the key to addressing this problem. The attacker can also explore the fact that the IoT devices have severe energy constraints due to limitation on the battery capacity or on the amount of energy that can be harvested from the environment.

The security challenges are exacerbated by the fact that the currently adopted standards (including these developed by the 3GPP) are leaving many critical security enhancements as optional. Furthermore, the ambiguity and the lack of formal representation of standards requirements open the door for different interpretations by vendors, which weakness the security properties of the operational systems. Furthermore, the networks are designed to support backward compatibility with older generations, which weakens the impact of newer security enhancements.

Open source In today's networks, the networking solutions are provided by individual vendors that follow a "closed source" approach for their software stacks and utilize closed ("black box") hardware. The closed nation of their systems makes it harder to secure these networks due to the lack of visibility inside the black box devices as well as due to the lack of certainty in their behavior. However, open source solutions may introduce additional security challenges [1].

3 Opportunities

The security challenges present unique opportunities for researchers and developers. This section presents some of the concepts and tools that have the potential to address the challenges referenced in Section 2.2.

Provable security/security by design. In most engineering systems, the performance and flexibility of the systems are prioritized while security and privacy are treated as an afterthought. By addressing security requirements at the early stages of the design process, the developers and the system architects can eliminate entire categories of threats. Security by design can be coupled with the *clean slate* approach while the system architects are not constrained by compatibility requirements or by the requirements to be compatible with the existing systems.

Composable security. The services provided by the next generation wireless broadband systems cut across multiple layers and include multiple network components. Indeed, the fifth-generation networks are expected to provide end-to-end slicing capabilities. Accordingly, there is a need to coordinate the security functions be provided by multiple layers and network components. This, in turn, will require tools to reason and analyze the joint behavior of distributed security mechanisms to ensure the correctness of operations, eliminating duplicate efforts, and minimizing the performance overhead.

Machine learning (ML)/Artificial Intelligence (AI) Security. ML/AI tools and techniques are expected to play a significant role in the next-generation

wireless systems. Due to their reliance on training data sets, ML/AI tools can be exploited by the attacker to steer the system to the unstable state [5].

Programmable security. It is highly desirable to move from the static (decided in advance) security policies to dynamic policies that can be easily updated during the operation of the system. Security functions can also be programmed by following the SDN approach, as opposed to the current practices in which the security policies are configured. Programmable security provides more flexibility in responding to the highly evolving threats [3].

Developing Security Metrics and Indices While there exists a large body of work on assisting reliability of engineering systems in the presence of conventional failures, assessing risk in the case of directed attacks is not we understood. Accordingly, it would be useful to develop a probabilistic methodology for assessing the ability of systems to withstand directed attacks aimed at the different system components. This methodology would lead to the development of security indices that can quantify the degree of resilience of the given system.

Use of formal methods Formal methods can be leveraged to enable provable security guarantees about systems at specification and design time as well as to enable security measurement, verification, and validation at deployment time [2]. In addition, the formal methods can benefit the network standardization process through the development of a methodology to formally specify and reason about the network protocols. This methodology will address the problems associated with traditional ways of describing protocols using a natural language [4].

References

1. Boswell, J., Poretsky, S.: Security considerations of open ran (last accessed 19 Oct 2020), https://www.ericsson.com/en/security/security-considerations-of-open-ran.
2. Chong, S., Guttman, J., Datta, A., Myers, A., Pierce, B., Schaumont, P., Sherwood, T., Zeldovich, N.: Report on the nsf workshop on formal methods for security. arXiv preprint arXiv:1608.00678 (2016)
3. Gu, G., Ott, D., GMU, K.S., Al-Shaer, E., Cardenas, A., Chen, Y., Enck, W., Hu, H., Moreau, D., Nita-Rotaru, C., et al.: Programmable system security in a software-defined world–research challenges and opportunities (2018)
4. McMillan, K.L., Zuck, L.D.: Formal specification and testing of quic. In: Proceedings of the ACM Special Interest Group on Data Communication, pp. 227–240 (2019)
5. Papernot, N., McDaniel, P., Sinha, A., Wellman, M.: Towards the science of security and privacy in machine learning. arXiv preprint arXiv:1611.03814 (2016)