A Comprehensive Evaluation of Security Issues in 5G Networks and M2M Systems

Behnam Shahriari
Department of Computer Engineering, Faculty of Engineering, Eastern Mediterranean University, Famagusta, North Cyprus, Via Mersin 10, Turkey

Gurcu Oz
Department of Computer Engineering, Faculty of Engineering, Eastern Mediterranean University, Famagusta, North Cyprus, Via Mersin 10, Turkey

Ali Hakan Ulusoy
Department of Information Technology, School of Computing and Technology, Eastern Mediterranean University, Famagusta, North Cyprus, Via Mersin 10, Turkey

Abstract

In recent years, mobile communication systems have evolved for both mobile users and network operators to meet ever-increasing service demands. In this research, we focus on Fifth Generation (5G) mobile technology. 5G technology can further develop mobile communication systems to not only connect mobile users, but also promote Machine-Type-Communications (MTC) systems. 5G technology has significantly revolutionized Internet of Things (IoT) applications. The 5G communication systems are introduced to provide a range of network services and requirements for a large number of IoT nodes. The combination of 5G networks and Machine-to-Machine (M2M) communication has started a new phase in the development of IoT systems. To support IoT applications, an improvement in the mobile communication system is required. For example, 5G technology must achieve higher speed, massive connectivity and lower latency. Since the exchanged data of IoT applications is very sensitive, acceptable data protection is required in the communication systems. To meet the security requirements of IoT-based systems, the Third Generation Partnership Project (3GPP) has equipped 5G networks with security changes such as standard Authentication and Key Agreement (AKA) protocols. The most important component of 5G security may be a secure AKA protocol. Extensible Authentication Protocol-AKA (EAP-AKA) and 5G-AKA are two of the most common protocols in 5G networks that play the role of the first safeguard to ensure secure communication. However, the existing AKA protocols are still vulnerable to some important security threats such as traffic analysis, Man-in-the-Middle (MitM), impersonation, and Denial of Service (DoS) attacks. Therefore, there is an urgent need to evaluate and improve the AKA method in 5G networks and especially in 5G-based IoT systems. Moreover, these protocols may cause some performance issues such as computational and transmission overhead, as they require additional computations for each involved node in the IoT application. Accordingly, we present a practical survey of 5G security and existing AKA approaches for 5G and 5G-based IoT systems. The survey starts with an overview of the 5G architecture and MTC systems. Then we present a classification of the main security issues in these systems. In addition, we give an objective overview of existing standard protocols and some proposed AKA protocols for 5G security. Furthermore, we give a detailed analysis of EAP-AKA and 5G-AKA schemes as a standard method in 5G systems. We give a comprehensive survey of the main related works in 5G security is provided to help other researchers in this academic field.

Keywords

5G wireless systems, network security, M2M communications, IoT systems, security vulnerabilities, MTC technology, authentication protocol, communication and computation overhead.