A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends

Yulong Zou, Jia Zhu, Xianbin Wang, Lajos Hanzo

Abstract— Due to the broadcast nature of radio propagation, the wireless air interface is open and accessible to both authorized and illegitimate users. This completely differs from a wired network, where communicating devices are physically connected through cables and a node without direct association is unable to access the network for illicit activities. The open communications environment makes wireless transmissions more vulnerable than wired communications to malicious attacks, including both the passive eavesdropping for data interception and the active jamming for disrupting legitimate transmissions. Therefore, this paper is motivated to examine the security vulnerabilities and threats imposed by the inherent open nature of wireless communications and to devise efficient defense mechanisms for improving the wireless network security. We first summarize the security requirements of wireless networks, including their authenticity, confidentiality, integrity, and availability issues. Next, a comprehensive overview of security attacks encountered in wireless networks is presented in view of the network protocol architecture, where the potential security threats are discussed at each protocol layer. We also provide a survey of the existing security protocols and algorithms that are adopted in the existing wireless network standards, such as the Bluetooth, Wi-Fi, WiMAX, and the long-term evolution (LTE) systems. Then, we discuss the state of the art in physical-layer security, which is an emerging technique of securing the open communications environment against eavesdropping attacks at the physical layer. Several physical-layer security techniques are reviewed and compared, including information-theoretic security, artificial-noise-aided security, security-oriented beamforming, diversity-assisted security, and physical-layer key generation approaches. Since a jammer emitting radio signals can readily interfere with the legitimate wireless users, we also introduce the fam- ly of various jamming attacks and their countermeasures, including the constant jammer, intermittent jammer, reactive jammer, adaptive jammer, and intelligent jammer. Additionally, we discuss the integration of physical-layer security into existing authentication and cryptography mechanisms for further securing wireless networks. Finally, some technical challenges which remain unresolved at the time of writing are summarized and the future trends in wireless security are discussed.

For the published version of record document, go to:
http://dx.doi.org/10.1109/JPROC.2016.2558521