Physical Layer Security for Authentication, Confidentiality, and Malicious Node Detection: A Paradigm Shift in Securing IoT Networks

Publisher: IEEE

Elmehdi Illi; Marwa Qaraqe; Saud Althunibat; Abdullah Alhasanat; Moath Alsafasfeh; Marcus de Ree; Georgios Mantas; Jonathan Rodriguez; Waqas Aman; Saif Al-Kuwari

Abstract:

The pervasiveness of commercial Internet of Things (IoT) around the globe is expected to reach significant levels with the upcoming sixth generation of mobile networks (6G). Throughout the past years, wireless standardization units worldwide have been prominently active in the deployment and performance optimization of such IoT networks and fusing them with current and futuristic cellular networks. Nonetheless, the openness of wireless transmissions and the forecasted overwhelm in connected devices will provoke unprecedented security leakages and vulnerabilities. In addition to the key targets of the 6G and IoT, it has been of paramount importance to cater to decent and lightweight security mechanisms in ultra-massively connected heterogeneous networks. Recently, significant efforts have been made to pave the way for the integration of physical layer security (PLS) in contemporary and futuristic networks. The primary motivation behind its deployment resides in its low complexity and ability to provide information-theoretic secure transmissions, which alleviates the complexity burden caused by implementing complex cryptographic schemes. This survey overviews the recent advancement in PLS techniques with a particular interest in its application to the Internet of

Things (IoT). We review essentially recent PLS techniques aiming at ensuring message confidentiality along with node/message authentication and malicious nodes' detection, where their corresponding application scenarios and underlying pros and cons are discussed. On top of that, we explore recent findings in the incorporation of cutting-edge technologies at the physical layer, such as non-orthogonal multiple-access, reconfigurable intelligent surfaces, joint communication and sensing, and optical wireless/Terahertz communications in boosting confidentiality and authentication at the physical layer. Lastly, promising extensions and future directions are discussed based on the quantified pros and cons of each PLS category, opening up ways for timely research directions within the topic and current/future challenges faced by PLS.

Published in: IEEE Communications Surveys & Tutorials (Early Access)
Page(s): 1 - 1
Date of Publication: 25 October 2023
ISSN Information:
Electronic ISSN: 1553-877X
CD: 2373-745X
DOI: 10.1109/COMST.2023.3327327
Publisher: IEEE
Funding Agency:
10.13039/501100000830-North Atlantic Treaty Organization (**Grant Number**: grant SPS G5797)