The IEEE 28th International Symposium on Industrial Electronics, 12-14 June 2019, Vancouver, Canada

Analysis of SDN-based security challenges and solution approaches for SDWSN usage

Reza Ishmael Mathebula, Bassey Isong, Naison Gasela

Department of Computer Science North-West University Mafikeng, South Africa
ishimathebula@gmail.com; isong.bassey@ieee.org; naison.gasela@nwu.ac.za

Adnan M. Abu-Mahfouz
Council for Science and Industrial Research (CSIR) Pretoria, South Africa
a.abumahfouz@ieee.org

https://ieeexplore.ieee.org/abstract/document/8781268

Abstract

In recent years, wireless sensor networks (WSNs) and software defined networks (SDN) have witnessed overwhelming research interests in both industry and the academia. Most of these researches have been devoted to address several security challenges in the traditional WSN to mitigate network-based threats and attacks. SDN emanated as one such solutions which has been adopted in WSN to address its inherent network inflexibility, a paradigm called Software-Defined Wireless Sensor Networks (SDWSN). Albeit, SDWSN emerged as a consolidated solution, there is no guarantee that it is totally immune to current dynamic and complex security threats and vulnerabilities that grow explosively on a daily basis. Therefore, this paper aim to explore and analyze some of the security challenges faced by SDWSN. A comprehensive analysis is conducted using the content analysis approach on existing SDN researches in order to identify the existing security techniques, their impacts, and the drawbacks of each approach. The implication is on directing the research interest through having insights into current security challenges.