2019 IEEE 28th International Symposium on Industrial Electronics (ISIE), Vancouver, BC, Canada, 12-14 June 2019

A review of artificial intelligence based intrusion detection for Software-Defined Wireless Sensor Network

Abu-Mahfouz, Adnan MI
Council for Scientific and Industrial Research
Pretoria, 0001, South Africa
Email: AAbuMahfouz@csir.co.za

Abstract

Wireless communications and Wireless Sensor Networks (WSNs) are intensively used in manufacturing industries, in medical devices, for the determination of the position and for the guidance of military drones and bombs. Given the scope of utilization of WSNs, the security of wireless communications is a very critical problem that must be tackled accordingly. A Software-Defined Wireless Sensor Network (SDWSN) is realized by infusing a Software Defined Network (SDN) model in a WSN. In this paper, the cryptography schemes as well as the security threats related to SDWSNs are identified and the Artificial Intelligence (AI) techniques used to detect intrusions in SDWSNs are presented. It is shown that a two-level security model combining cryptography schemes and AI techniques can be used to fight malicious attacks against SDWSNs.