Opinion
Volume 15:4, 2022

Journal of Computer Science & Systems Biology

ISSN: 0974-7230 Open Access

Intrusion Detection Using Artificial Intelligence in Software-defined Wireless Sensor Networks

Lisandro Stepanov*

Department of Information Science, University of Bergen, Bergen, Norway

Introduction

The ever-decreasing cost of electronic devices, combined with the need to automatically transfer massive amounts of data between remote locations, has resulted in the Internet of Things (IoT) paradigm. The Internet of Things (IoT) is a system in which "things" (e.g., electronics and machines) communicate with one another without the intervention of humans in order to complete a specific task (e.g., controlling the temperature of an operating room). The various components of an IoT system can be dispersed across a large field or placed in an environment (e.g., human stomach, hospital laundry room) where conditions such as acidity, humidity, and temperature make wired communications [1-3] impossible.

To that end, Wireless Sensor Network (WSN) technologies are used in Internet of Things (IoT) applications where wired communications are either impossible to implement (e.g., global positioning system) or insufficient to use (e.g., wearable medical devices, ingestible sensors). Furthermore, the number of sensors present in the network, as well as security threats such as Denial of Service (DoS) attacks, must be considered when implementing IoTs. This fact emphasizes the importance of establishing adequate network management. To that end, over the last decade, a new paradigm known as the Software-Defined Network (SDN) has emerged.

Traditional processes are being drastically transformed by the SDN model, which provides centralized control of the entire network, making it easier to implement network-wide management protocols and applications such as data aggregation or cryptographic schemes. The Software-Defined Wireless Sensor Network (SDWSN) model is created by combining the SDN and WSN models. Cryptographic schemes (symmetric, asymmetric, and hybrid encryption) used in SDWSN-based IoTs are designed to protect them from security threats such as Sybil attacks (in which an attacker steals the identity of legitimate sensor nodes) and unauthorized access. Unfortunately, these schemes are rarely enough to ensure the integrity of communications in SDWSN-based IoTs [4-5].

Description

To that end, the cryptographic schemes can be supplemented with an Intrusion Detection System (IDS) to monitor SDWSN-based IoT traffics and detect unauthorized entities carrying out attacks. The IDS is typically composed of three components: the flow collector, the anomaly detector, and the anomaly mitigator. In the context of SDWSN-based IoTs, the IDS is programmatically deployed as software on the controller to optimize network performance and monitoring. The overall architecture of an IDS deployed on the SDWSN-based IoT controller is depicted. The flow collector in the IDS collects all flow features (for example, source code name, number of failed logins, and connection time) and forwards them to the anomaly detector. The anomaly detector is essential in the IDS because it assigns a class to the flow based on the features obtained from the flow collector (e.g., sybil attack, normal traffic).

Given the class assigned to the flow by the anomaly detector, the function of the anomaly mitigator is to take a stand (e.g., pass on or do not pass on the flow).As IDSs in SDWSNs, various approaches have been proposed in the literature. Among these approaches, IDSs that use a Decision Tree (DT), a Nave Bayes (NB) classifier, or an Artificial Neural Network (ANN) as an anomaly detector are widely used in the literature because they are relatively easier to implement while being very performant on classification tasks. It is worth noting that these published works used vastly different datasets to train the aforementioned anomaly detectors, and as a result, the performance of an anomaly detector on one dataset may be drastically reduced on another.

Conclusion

Furthermore, in the case of safety or mission critical networks (e.g., heart rate monitoring, automated insulin delivery) security constraints may prevent the network from using a cloud-based controller, whereas miniaturization constraints may limit the physical size and memory capacity of the controller, while performance specifications may require low latency. For these reasons, it is critical to select an anomaly detector with the shortest execution time, smallest memory size, and lowest energy consumption to ensure the best trade-off between security and performance for safety or mission critical SDWSNs. Another noteworthy observation is that, because the SDWSN is a new paradigm, there isn't a large body of literature on intrusion detection in SDWSNs

References

1. Liu, Li, Wanli Ouyang and Xiaogang Wang, et al. "Deep learning for generic object detection: A survey." *Int J Comput Vis* 128 (2020): 261-318.
2. Kunze, Lars and Michael Beetz. "Envisioning the qualitative effects of robot manipulation actions using simulation-based projections." *Artif Intell* 247 (2017): 352-380.
3. Auger, François, Mickael Hilairet and Josep M. Guerrero,et. "Industrial applications of the Kalman filter: A review." *IEEE Trans Ind Electron* 60 (2013): 5458-5471.
4. Hedman, Jonas and Thomas Kalling. "The business model concept: Theoretical underpinnings and empirical illustrations." *Eur J Inf Syst* 12 (2003): 49-59.
5. Sowa, John F and John A. Zachman. "Extending and formalizing the framework for information systems architecture." *IBM Syst J* 31 (1992): 590-616.

***Address for Correspondence:** Lisandro Stepanov, Department of Information Science, University of Bergen, Bergen, Norway, E-mail: LisandroStepanov30@gmail.com*

Received: 07-Apr-2022, Manuscript No. jcsb-22-66574; **Editor assigned:** 09-Apr-2022, Pre QC No. P-66574; **Reviewed:** 23-Apr-2022, QC No.66574; **Revised:** 28-Apr-2022, Manuscript No. R-66574; **Published:** 05-May-2022, DOI: 10.37421/0974-7230.2022.15.408

How to cite this article: Stepanov, Lisandro. “Intrusion Detection Using Artificial Intelligence in Software-defined Wireless Sensor Networks.” J Comput Sci Syst Biol 15 (2022): 408.