International Journal of Critical Infrastructure Protection 34 (2021) 100436

Contents lists available at ScienceDirect

International Journal of Critical Infrastructure Protection

journal homepage: www.elsevier.com/locate/ijcip

Fault-tolerant AI-driven Intrusion Detection System for the Internet of Things

Faiza Medjek[a,b,*], Djamel Tandjaoui[a], Nabil Djedjig[a,b], Imed Romdhani[c]

[a] Research Centre on Scientific and Technical Information (CERIST), 03, Rue des Freres Aissou, Ben Aknoun, Algiers, Algeria
[b] Departement Informatique, Faculte des Sciences Exactes, Universite de Bejaia, Bejaia 06000, Algeria
[c] School of Computing, Edinburgh Napier University, 10 Colinton Road, EH10 5DT Edinburgh, UK

ARTICLE INFO

Article history:
Received 31 December 2019
Revised 12 October 2020
Accepted 30 March 2021
Available online 7 April 2021

Keywords:
RPL security
IoT security
IDS
Machine Learning
Deep Learning
Critical infrastructure

ABSTRACT

Internet of Things (IoT) has emerged as a key component of all advanced critical infrastructures. However, with the challenging nature of IoT, new security breaches have been introduced, especially against the Routing Protocol for Low-power and Lossy Networks (RPL). Artificial-Intelligence-based technologies can be used to provide insights to deal with IoT's security issues. In this paper, we describe the initial stages of developing, a new Intrusion Detection System using Machine Learning (ML) to detect routing attacks against RPL. We first simulate the routing attacks and capture the traffic for different topologies. We then process the traffic and generate large 2-class and multi-class datasets. We select a set of significant features for each attack, and we use this set to train different classifiers to make the IDS. The experiments with 5-fold cross-validation demonstrated that decision tree (DT), random forests (RF), and K-Nearest Neighbours (KNN) achieved good results of more than 99% value for accuracy, precision, recall, and *F*1-score metrics, and RF has achieved the lowest fitting time. On the other hand, Deep Learning (DL) model, MLP, Naïve Bayes (NB), and Logistic Regression (LR) have shown significantly lower performance.

1. Introduction

Critical infrastructures (CIs) cover various socio-economic sectors such as healthcare, agriculture, industry, gas and water distribution, transportation, energy, communications, information technology, etc. CIs are continuously changing and adapting to changes in technology. Indeed, Cyber-Physical Systems (CPS) and the Internet of Things (IoT) have emerged as core components in all advanced Cis, such as Industry 4.0 [1,2]. Since CIs are vital to daily human lives, their protection from cyber-attacks by malicious entities that cause significant impacts on the targeted CIs and their services is a serious concern. Consequently, to secure CIs, it is necessary to secure IoT networks [3].

IoT [4] consists of physical objects, usually known as things (devices) that sense, collect, and might process CIs related information. On one side, these objects are resource-constrained as they are powered by batteries and have limited computation and storage capability. On the other side, billions of these devices are interconnected and connected to the Internet under lossy and noisy communication environments such as Wi-Fi, ZigBee, Bluetooth, LoRa, GSM, WiMAX or GPRS. IoT applications have emerged in several aspects. Nevertheless, the IoT's networks rise challenges in designing efficient and secure routing protocols [5,6]. Several efforts have been made by standardisation entities to specify efficient routing protocols for the IoT. Finally, the IPv6 Routing Protocol for Low Power and Lossy Networks (RPL) [7] was designed and standardised by the IETF ROLL working group to overcome the routing challenges underpinning IoT networks. RPL specification considers limitations in both the energy power and the computational capabilities of such networks.

Besides the different characteristics of IoT components, the rapid growth of IoT applications and the increasing number of smart objects in IoT networks result in producing a massive amount of data and traffic leading to increase the IoT's vulnerabilities, and consequently, the RPL's threats [5,6]. Although the RPL specification introduces mechanisms aiming to achieve confidentiality, integrity and replay protection through control messages encryption, local and global repairs and loops detection, RPL is still susceptible to internal attacks [6]. Indeed, there are vulnerabilities from inside the RPL network that go beyond the encryption and authentication defence for the RPL communications [8,9]. In such cases, Intrusion Detection Systems (IDSs) are required as a second line of defence, where IDSs analyse activities and nodes' behaviour to detect intruders that are trying to disrupt the network.

[*] Corresponding author.
E-mail address: medjek-f@dtri.cerist.dz (F. Medjek).

https://doi.org/10.1016/j.ijcip.2021.100436
1874-5482/© 2021 Elsevier B.V. All rights reserved.