2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)

Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning

Fatima-tuz-Zahra
School of Computing & IT (SoCIT), Taylor's University
Subang Jaya, Malaysia
fatemah.tuz.zahra@gmail.com

NZ Jhanjhi
School of Computing & IT (SoCIT), Taylor's University
Subang Jaya, Malaysia
noorzaman.jhanjhi@taylors.edu.my

Sarfraz Nawaz Brohi
School of Computing & IT (SoCIT), Taylor's University
Subang Jaya, Malaysia
sarfraznawaz.brohi@taylors.edu.my

Nazir A. Malik
Department of Computer Science, Bahria University
Islamabad, Pakistan
nmalik.buic@bahria.edu.pk

***Abstract*—Internet of Things (IoT) is a paradigm in digital technology which is prevalently revolutionizing various sectors like healthcare, military, business and more. However, the incremental deployment of this advanced technology has also caused critical security issues simultaneously. In particular, IoT networks are continuing to grow vulnerable to security attacks due to exponential connectivity of 'things' with each other in the smart infrastructure. Due to this increased vulnerability, it has become crucial to address the issue of insecure routing in these IoT devices. IoT uses RPL, which is a specially designed standard for networking that caters to the resource-constrained and lightweight nature of IoT devices, for information broadcast. It is equally prone to routing attacks like any other class of protocols in wireless networks. Various solutions have been proposed by researchers to counter them including version, rank, sinkhole and wormhole attacks since last decade. However, given the huge impact, neither detection nor mitigation method has been found which addresses rank and wormhole attacks when they are initiated at the same time on an IoT network. In this paper, a rank and wormhole attack detection framework is proposed, by employing machine learning approaches, which address the stated issue. This research aims to contribute toward design and development of high-performing and effective solutions for routing attacks in RPL-based IoT networks.**

Keywords*— *RPL, Internet of Things, rank attack, wormhole attack, machine learning

I. Introduction

Internet of Things (IoT) is a network of things connected to the internet that are seamlessly embedded in our daily lives. These things are connected to the internet for smart communication and partial independence in decision making. Smart IoT devices or 'things' can range from a baby's shoes to an elderly patient's pacemaker, in which Radio Frequency Identification (RFID) tags, small sensors, and actuators are embedded for smart wireless communication. This network has gradually upgraded all the way up to smart homes, connected healthcare information systems, vehicles, parking systems, and smart cities [1], [2], [3].

Given the fact that most of the fundamental concepts of IoT have originally been derived from Wireless Sensor Networks (WSNs), they are commonly confused with each other. In general, WSNs and IoT networks share a few similarities but there are notable differences in their characteristics as well. A comprehensive overview in the next sub-section will help in understanding the reason why the discussion of interconnection of these two networks is important and to what extent they are similar as well as different from each other. It will also help in identifying their unique characteristics.

A. Similarities between WSNs and IoT:

There are several similarities between WSNs and IoT, which are listed as following [4]:

1. Nodes in both WSN and IoT networks are deployed depending on the application domain, that is, it can be ambulant or static/fixed, deterministic or random. This situation is also a reason for significant challenges when routing the data for all kinds of traffic.
2. Nodes in both networks are resource constrained. Conventionally majority of the nodes depend on power-scavenging systems and technologies to function, such as thermal and wind energy [5]. Many of them have inadequate storage capacity as well as low processing power and potential. This characteristic of the nodes requires equally lightweight routing and security protocols to be used in networks that employ such nodes.
3. Networks are usually designed to work in severe and harsh conditions where links are dissipating while nodes switch on and off to cope as they are built using energy-preserving techniques. In addition, many nodes are widely dispersed, and they possibly become mobile when required. This is considered to be their coping mechanism. Given the fact that nodes are designed as aforementioned, routing protocols also need to match these features and must be designed keeping scalability, speed, and resource-efficiency in consideration.
4. Nodes in both WSN and IoT networks are repressed because they are designed to achieve application-specific objectives only [6] which consequently makes them highly vulnerable to internal and external, WSN-inherited and RPL-specific attacks.

B. Differences between WSNs and IoT:

In contrast with similarities, WSNs and IoT networks have some marked differences which will help us in understanding their individual characteristics as well as

978-1-7281-4956-1/19/$31.00 ©2019 IEEE