Introducing Mobility Metrics in Trust-based Security of Routing Protocol for Internet of Things

Syeda Mariam Muzammal
School of Computer Science and Engineering
Taylor's University
Subang Jaya, Malaysia
syedamariammuzammal@sd.taylors.edu.my

*Raja Kumar Murugesan
School of Computer Science and Engineering
Taylor's University
Subang Jaya, Malaysia
rajakumar.murugesan@taylors.edu.my

NZ Jhanjhi
School of Computer Science and Engineering
Taylor's University
Subang Jaya, Malaysia
noorzaman.jhanjhi@taylors.edu.my

2021 National Computing Colleges Conference (NCCC) | 978-1-7281-6719-0/20/$31.00 ©2021 IEEE | DOI: 10.1109/NCCC49330.2021.9428799

***Abstract*— Internet of Things (IoT) is flourishing in several application areas, such as smart cities, smart factories, smart homes, smart healthcare, etc. With the adoption of IoT in critical scenarios, it is crucial to investigate its security aspects. All the layers of IoT are vulnerable to severely disruptive attacks. However, the attacks in IoT Network layer have a high impact on communication between the connected objects. Routing in most of the IoT networks is carried out by IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL). RPL-based IoT offers limited protection against routing attacks. A trust-based approach for routing security is suitable to be integrated with IoT systems due to the resource-constrained nature of devices. This research proposes a trust-based secure routing protocol to provide security against packet dropping attacks in RPL-based IoT networks. IoT networks are dynamic and consist of both static and mobile nodes. Hence the chosen trust metrics in the proposed method also include the mobility-based metrics for trust evaluation. The proposed solution is integrated into RPL as a modified objective function, and the results are compared with the default RPL objective function, MRHOF. The analysis and evaluation of the proposed protocol indicate its efficacy and adaptability in a mobile IoT environment.**

Keywords—Internet of Things, Trust, Mobility, RPL, Security

I. INTRODUCTION

Due to the expansion of digital and technological paradigm, billions of heterogeneous IoT devices have been predicted by researchers for the upcoming years [1][2]. Additionally, there have been some attacks in previous years, such as Mirai Botnet attacks [3] and various others [4][5][6], that were made possible using the low-powered and resource-constrained IoT devices. IoT networks are vulnerable to several attacks. Most of the IoT applications employ RPL routing protocol for routing. RPL routing protocol is also prone to numerous disruptive attacks, including Blackhole, Sinkhole, Wormhole, Rank, and Version number modification attacks [7]. The packet dropping attacks in RPL cause the unavailability of data and resources. Such attacks need to be investigated to provide secure communication among the connected nodes [8]. In addition, it is crucial to provide a solution for the overall security enhancement of IoT systems [9] to fulfil the requirements of the security triad, that is, confidentiality, integrity, and availability (CIA).

One of the important components of IoT is networking, which facilitates communication and interconnectivity. Particularly, routing holds a prominent place, which involves building traffic routes for transmitting a packet from source to destination. Moreover, the security issues are crucial in networks, specifically routing, when billions of devices are connected with each other. The number of IoT-connected devices is exponentially increasing, as predicted by Statista [2], depicted in Fig. 1. Network security becomes challenging when a packet is routed through heterogeneous networks from resource-constrained devices to a server, over the Internet. Hence, with the widespread IoT applications involving routing via RPL, it is imperative to address the related attacks. Out of several security solutions proposed for secure routing, a trust-based approach possesses the significance and viability for IoT networks and routing. A robust security solution will enhance protection against attacks and facilitate the overall widescale adoption of IoT applications.

This research work proposes a trust-based approach for routing security against packet dropping attacks in RPL. IoT network is dynamic that includes both static and mobile nodes. Therefore, the mobility-based metrics are combined with the trust-based metrics to make the solution adaptable to the mobile IoT environment. Simulation experiments are conducted for evaluation of the proposed security solution and performance comparison with the default RPL objective function (OF), Minimum Rank with Hysteresis Objective Function (MRHOF).

The paper is organized as follows: Section II describes the background of the considered problem domain and the related work. Section III describes the materials and methods for the proposed solution. Section IV presents the results and discussions. Finally, Section V concludes the paper.

II. BACKGROUND AND RELATED WORK

This section describes the related work with respect to the background of the problem under consideration. In addition, trust-based approaches in the existing literature for securing IoT networks and routing are summarized.

A typical IoT architecture is composed of five layers [10]. These include the perception/ sensing layer, network/ transmission layer, middleware/ transport layer, application layer, and data/ cloud services. IoT layers suffer from various security attacks [11], including Node capturing, Denial of Service [12], Fake node or Sybil attack [13], Replay attack [14], Side-channel attack [15] and routing threats in the data forwarding process [16]. Fig. 2 shows the classification of IoT network layer attacks.

IoT network layer is composed of a layered protocol stack [17]. It consists of various communication and connectivity protocols. IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) is introduced by Internet Engineering Task Force (IETF) for wireless connectivity between resource-constrained devices. RPL is

*Corresponding Author