A Comprehensive Review on Secure Routing in Internet of Things: Mitigation Methods and Trust-based Approaches

Syeda M. Muzammal, *Student Member, IEEE,* Raja Kumar Murugesan, *Member, IEEE,* NZ. Jhanjhi, *Member IEEE*

***Abstract*—Internet of Things (IoT) is a network of 'things', connected via Internet, to collect and exchange data. These 'things' can be sensors, actuators, smartphones, wearables, computers or any object that is interconnected to provide specific services. Similarly, Wireless Sensor Network (WSN), as a part of IoT, forwards the gathered data after sensing any event. The scalability and heterogeneity of IoT offer limited protection and is prone to diverse attacks, including WSN-inherited attacks. Moreover, IPv6 Routing Protocol for Low Power and Lossy Networks (RPL), a de facto routing protocol for IoT networks, also suffers from certain vulnerabilities based on its features and functionalities. Researchers have proposed various mitigation mechanisms for secure networks and routing in IoT. Recently, trust-based approaches have gained tremendous interest from the research community to embed security in IoT networks and routing protocols. In the existing literature, several trust models have been introduced according to the security needs of the IoT system, such as SecTrust, DCTM-IoT, CTRUST, etc. In this research, security issues and requirements of IoT networks and RPL routing protocol are studied with respect to various attacks, such as Blackhole, Spoofing, Rank, etc. Additionally, various mitigation methods and significance of trust models in IoT for secure routing are analyzed. Further, trust metrics in IoT environments including the open issues and research challenges, as well as the implication of trust as a security paradigm in IoT networks and routing protocols are discussed.**

***Index Terms*— IoT, Secure Routing, RPL Attacks, Security, Trust**

I. INTRODUCTION

THE proliferation of the Internet of Things (IoT) is occupying an essential place in our daily lives. A number of devices, that we use for our routine activities are interconnected with each other as well as connected to the Internet [1]. Smart devices, wireless sensors and technologies have seen tremendous growth in recent years [2]. According to Gartner, more than 25 billion devices [3] will be connected to the Internet by 2021, whereas Cisco predicts 75 billion [4] connected devices by the year 2025. Another forecast [5] predicts that by 2030, globally 50 billion IoT devices will be in use. In IoT, devices process and exchange information without human intervention. The autonomous behaviour, successful deployment, and adoption of IoT demands scalable, lightweight, mobile, and secure solutions for data communication among devices as well as to retain the Confidentiality, Integrity, and Availability (CIA) of the resources and exchanged information. As the number of devices increases, the probability of threats, risks and attacks to smart devices will also increase. Inadequate security may lead to severe threats, increased vulnerabilities, and cyber-attacks. This potentially augments users' security and privacy concerns via IoT devices and thus may reduce the radical growth of IoT.

IoT networks are prone to several attacks like Denial of Service (DoS), eavesdropping, Man-in-the-Middle (MITM), sniffing etc. Various cyber-attacks have become common and more powerful [6] causing significant disruptions to the IoT systems. Moreover, some of the network attacks in IoT are inherited from Wireless Sensor Networks (WSNs). Hence, there is a need to secure IoT networks from conceivable attacks and threats. Mainly, secure routing in the highly dynamic and distributed environment of IoT is still a challenge due to the heterogeneity of smart devices.

IoT networks involve several standards [7]. One such standard is IPv6 over Low Powered and Wireless Personal Area Network (6LoWPAN). This type of network comprises of resource-constrained devices, lossy links, and lower data rates. Resource-constrained means that the nodes have very low memory, energy, and processing power. 6LoWPAN networks use IPv6-based protocol stack as developed and standardized by IETF [8]. There is an additional layer in the 6LoWPAN protocol stack, the adaptation layer, for handling fragmentation. It also manages header compression along with IPv6 packets

This research work is supported by Taylor's University, Malaysia through its Taylor's PhD Scholarship Programme.

S. M. Muzammal is with the School of Computer Science and Engineering, Taylor's University, Subang Jaya, Malaysia (e-mail: syedamariammuzammal@sd.taylors.edu.my).

R. K. Murugesan is with the School of Computer Science and Engineering, Taylor's University, Subang Jaya, Malaysia (e-mail: rajakumar.murugesan@taylors.edu.my).

N. Z. Jhanjhi is with the School of Computer Science and Engineering, Taylor's University, Subang Jaya, Malaysia (e-mail: noorzaman.jhanjhi@taylors.edu.my).