SMTrust: Proposing Trust-Based Secure Routing Protocol for RPL Attacks for IoT Applications

Publisher: IEEE

Syeda Mariam Muzammal; Raja Kumar Murugesan; Noor Zaman Jhanjhi; Low Tang Jung **All Authors**

Abstract: With large scale generation and exchange of data between IoT devices and constrained IoT security to protect data communication, it becomes easy for attackers to compromi...**View more**

Metadata

Abstract:

With large scale generation and exchange of data between IoT devices and constrained IoT security to protect data communication, it becomes easy for attackers to compromise data routes. In IoT networks, IPv6 Routing Protocol is the de facto routing protocol for Low Power and Lossy Networks (RPL). RPL offers limited security against several RPL-specific and WSN-inherited attacks in IoT applications. Additionally, IoT devices are limited in memory, processing, and power to operate properly using the traditional Internet and routing security solutions. Several mitigation schemes for the security of IoT networks and routing, have been proposed including Machine Learning-based, IDS-based, and Trust-based approaches. In existing trust-based methods, mobility of nodes is not considered at all or its insufficient for mobile sink nodes, specifically for security against RPL attacks. This research work proposes a conceptual design, named SMTrust, for security of routing protocol in IoT, considering the mobility-based trust metrics. The proposed solution intends to provide defense against popular RPL attacks, for example, Blackhole, Greyhole, Rank, Version Number attacks, etc. We believe that SMTrust shall provide better network performance for attacks detection accuracy, mobility and scalability as compared to existing trust models, such as, DCTM-RPL and SecTrust-RPL. The novelty of our solution is that it considers the mobility metrics of the sensor nodes as well as the sink nodes, which has not been addressed by the existing models. This consideration makes it suitable for mobile IoT environment. The proposed design of SMTrust, as secure routing protocol, when embedded in RPL, shall ensure confidentiality, integrity, and availability among the sensor nodes during routing process in IoT communication and networks.

Published in: 2020 International Conference on Computational Intelligence (ICCI)

Date of Conference: 8-9 Oct. 2020 **DOI:** 10.1109/ICCI51257.2020.9247818

Date Added to IEEE *Xplore*: 09 November 2020 **Publisher:** IEEE

ISBN Information: **Conference Location:** Bandar Seri Iskandar, Malaysia, Malaysia

Contents

Internet of Things (IoT), as part of the fourth industrial revolution, is emerging in various areas and continuing to expand. Smart devices have been evolved in almost every field of human life. Factories, industries, and governments are adopting autonomous systems to increase efficiency, better production, and overall economic benefits. IoT involvement is further propagating in many other areas like healthcare, energy management, military, agriculture, supply chain and smart cities, aiming to build up a smart world.