IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 4, May 2024

To Design a Routing Module for IoT Routing Protocols to Address Modification and Manipulation Attacks

Suresh K[1], Sohel[2], Vinay A P[3], Vinod Patil[4], Santhosh Kumar C[5]

Assistant Professor, Department of CSE[1]

Students, Department of Computer Science[2,3,4,5]

Rao Bahadur Y Mahabaleswarappa Engineering College, Ballari, Karnataka, India

Abstract*:* *Internet of Things devices have become increasingly prevalent in various domains, including smart homes, healthcare, transportation, and industrial automation. As the number of IoT devices continues to grow, so does the potential for security challenges. Routing protocols play a critical role in IoT networks by determining the path for packet transmission. However, their susceptibility to modification and manipulation attacks can have far-reaching consequences. These attacks can lead to unauthorized access to sensitive data, disruption of critical services, and even physical harm in certain applications such as healthcare and industrial automation. This paper presents the design and implementation of a security-enhanced routing module aimed at protecting Internet of Things networks from modification and manipulation attacks, particularly focusing on the challenges within the IPv6 Routing Protocol for Low-Power and Lossy Networks. Acknowledging the increasing pervasiveness of IoT devices and their susceptibility to routing disruptions, this work contributes a novel approach to augment RPL's Lamport's Keyed Hash Chain scheme security posture without impinging on the protocol's inherent resource-efficiency. Through a comprehensive simulation-based system verification process, the module demonstrates its effectiveness in mitigating common routing attacks, its adaptability in dynamic network conditions, and its fidelity to established RPL performance metrics*

Keywords: Hashing Chain, Cryptographic, Routing Protocol for Low-Power and Lossy Networks, Internet of Things, Routing Protocol

DOI: 10.48175/IJARSCT-18325