Journal of Engineering Research 12 (2024) 133–139

Contents lists available at ScienceDirect

Journal of Engineering Research

journal homepage: www.journals.elsevier.com/journal-of-engineering-research

Safeguarding IoT networks: Mitigating black hole attacks with an innovative defense algorithm

Iraq Ahmad Reshi [a,*], Sahil Sholla [a], Zahoor Ahmad Najar [b]

[a] Department of Computer Science and Engineering, Islamic University of Science and Technology, Awantipora, Kashmir, India
[b] Department of Information Technology, Central University of Kashmir, Ganderbal, Kashmir, India

ARTICLE INFO

Keywords:
Internet of things
Security
Black hole attack
NS2
IoT Security

ABSTRACT

The Internet of Things (IoT) and Wireless Sensor Networks (WSNs) have rapidly spread in recent decades, leading to remarkable innovation and integrated possibilities. The switch from IPv4 to IPv6, made possible by advancements in networking technology and the use of nanodevices, has further improved connectivity. This move allows for connecting a wider range of devices to servers. Nevertheless, the increasing interconnectivity has brought about difficulties in efficiently overseeing and analysing the enormous amount of data produced throughout all levels of the IoT. The requirement of comprehensive security management is particularly concerning for IoT devices due to their large quantity and small size. Within the layered architecture of IoT, the network layer assumes pivotal importance in ensuring security, bearing responsibility for storing routing information and executing corresponding decisions. The Black Hole attack is a frequently encountered and significant concern among the security attacks addressed. This paper thoroughly examines the consequences of the Black Hole attack on IoT networks, carefully analyzing its impact. Furthermore, it presents a novel mitigation algorithm designed to counter such threats efficiently. The research employs NS2 and Simulink to run extensive simulations, enabling the evaluation of network throughput and Packet Delivery Ratio (PDR). Applying the proposed mitigation strategy to a network affected by the Black Hole attack results in a significant improvement in throughput, which closely resembles that of an unaffected network. The observed Packet Delivery Ratio (PDR) is measured at 98.21%. This highlights the algorithm's effectiveness in mitigating the detrimental effects of the Black Hole attack on IoT networks.

Introduction

The Internet of Things (IoT) has the potential to revolutionize a wide range of industries, including healthcare, intelligent systems, and critical applications. Nevertheless, this widespread growth raises a crucial issue: security. As the interconnectivity of IoT nodes, networks, and infrastructures grows, the susceptibility to security threats intensifies, necessitating prompt attention and robust measures. The utilization of the Routing Protocol for Low-Power and Lossy Networks (RPL) in enabling communication among IoT devices, although beneficial because of its efficient core, also exposes weaknesses. The vulnerabilities included in RPL, and those inherited from sensor networks entail substantial security threats, as emphasized by Zahra et al. [23]. The complex characteristics of IoT and RPL networks make them vulnerable to a range of attacks, including Specific Forwarding, Jamming, Sinkhole, Wormhole, Sybil, Flood, Gray Hole, and the highly threatening Black Hole Attacks. These attacks pose a risk to the security and reliability of Wireless Sensor Networks (WSN) [9,18].

The Internet of Everything (IoET) is an interconnected ecosystem that includes various technologies such as body sensors, VANETs, smartphones, and autonomous vehicles. The expansion of the Internet of Things (IoT) increases the complexity of safeguarding these interconnected entities. The constrained capabilities of sensor nodes, including transmission range, processing speed, storage capacity, and battery power, exacerbate security risks in various IoT applications. Despite their many advantages, IoT devices' processing power and battery capacity limits make it difficult to apply standard cryptography systems. The vulnerability to security attacks, as emphasized by Mali et al. [16], encompasses a wide range of risks. The Black Hole attack is the most hazardous since it can cause significant energy losses, network congestion, and performance deterioration.Black Hole attack alongside the gray hole is one of the prominent attacks in IoT networks [15].

* Corresponding author.
E-mail address: rshiraq333@gmail.com (I.A. Reshi).

https://doi.org/10.1016/j.jer.2024.01.014
Received 1 August 2023; Received in revised form 13 December 2023; Accepted 15 January 2024
Available online 20 January 2024