FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 13, Issue 3 | Pages 602-608 | e-ISSN: 2347-470X

Performance and Security Impacts of Blackhole Attacks on RPL-based IoT Networks for IoMT Applications

Shameer M.[1*], and Rutravigneshwaran P.[2]
[1]*Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, India, mdsameer09@gmail.com*
[2]*Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, India, rutra20190@gmail.com*

***Correspondence:** *mdsameer09@gmail.com; Tel.: +91 7285905603*;

ABSTRACT- Blackhole attacks stance a substantial menace to Routing Protocol for Low-Power and Lossy Networks (RPL)- based Internet of Things (IoT) networks. This study investigates the impact of such attacks on key performance metrics, including power consumption and Directed Acyclic Graph Identification Object (DIO) packet delivery. Using the Contiki and Cooja simulators, we analyze the effects of scenario-based blackhole attacks under various conditions. Our findings show that blackhole attacks lead to significant increases in CPU and radio energy consumption, with CPU utilization rising by 15-20% and radio listen energy increasing by 20-25%, while idle power consumption remains unchanged. These results highlight network vulnerabilities and inform the design of more resilient, trust-centric IoT networks, particularly for critical applications like remote healthcare monitoring.

Keywords: RPL Attacks, IoT Security, Blackhole Attacks, IoMT, 6LoWPAN.

ARTICLE INFORMATION
Author(s): Shameer M., Rutravigneshwaran P;
Received: 25/06/2025; **Accepted:** 22/09/2025; **Published:** 30/09/2025;
E- ISSN: 2347-470X;
Paper Id: IJEER250654;
Citation: 10.37391/ijeer.130326
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-13/ijeer-130326.html

Publisher's Note: FOREX Publication stays neutral with regard to jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

The widespread use of IoT devices has led to significant innovations diagonally manifold industries, principally in healthcare *via* Internet of Medical Things (IoMT). This embraces implanted medical gadgets, geriatric observing wearables, clinical tools linked with internet and dedicated operating rooms in hospitals [1]. A patient's vitals, comprising heart rate and blood pressure, can be monitored remotely using these devices [2]. Though beneficial, the IoMT ecosystem's pervasiveness and openness make it a prime target for hacks and threats [3]. However, this rapid growth has also introduced substantial security vulnerabilities, particularly in blackhole attack in RPL-based Wireless Sensor Networks (WSN). Blackhole assaults pose a substantial risk to these networks by disrupting normal routing operations and degrading acute performance indicators such as Packet Delivery Ratio (PDR) and End-to- End Delay (E2ED). While there has been an increase in research focusing on Machine Learning (ML), Deep Learning (DL), and hybrid algorithms for detecting assaults in RPL-based 6LoWPAN networks, many attacks, including Version Number (VN) and Hello Flood (HF) attacks, remain understudied [4]. Existing studies indicate that while deep learning-based solutions offer improved adaptability and accuracy; they often face challenges related to high computational demands and resource limitations in low- power devices. Furthermore, existing research frequently fails to reflect the complexities of real-world IoMT systems, which can hinder the development of effective security measures. This research seeks to probe the sway of blackhole assaults on RPL-based WSN, providing insights into them vulnerabilities and guiding the design of more resilient, trust- centric IoT networks suitable for mission-critical applications in healthcare [5].

The Routing Protocol for Low-Power and Lossy Networks (RPL) is a vital etiquette premeditated to aid efficient communication in limited resource environments, like WSN utilized in the IoMT. RPL operates by establishing a Directed Acyclic Graph (DAG) to optimize routing paths centered on innumerable metrics, including link quality and energy consumption. This protocol is particularly suited for IoMT applications, where devices often operate on limited power and require reliable data transmission for critical healthcare monitoring [6]. *Figure 1* illustrates the normal DODAG network topology where node 1 with green color is a sink node which is interconnected to all the other nodes.

In IoMT networks, RPL deployment has risks. The blackhole occurrence, when a mischievous node impersonates the quickest way to the destination, is a major concern. Valid nodes transit their data through this hijacked node, which drops packets instead of forwarding them, disrupting communication [7-8]. This attack not only degrades essential performance metrics such as PDR and E2ED but also compromises the integrity and reliability of healthcare data transmission, which is crucial for patient monitoring and safety.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 13, Issue 3 | Pages 602-608 | e-ISSN: 2347-470X

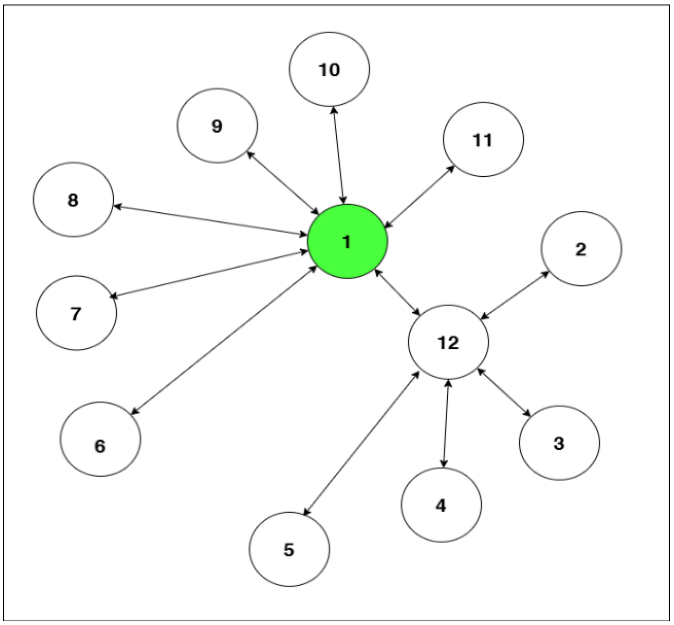

Figure 1. Network Topology

To mitigate the risks associated with blackhole attacks, it is vital to implement vigorous retreat trials that enhance the resilience of RPL-based WSN networks. This can be achieved through the integration of advanced detection mechanisms, such as ML and DL algorithms, which can identify anomalous behaviors indicative of blackhole assaults[5], [9]. Additionally, developing trust-centric models that assess the steadfastness of nodes within the network can further strengthen defenses against such vulnerabilities [10].

The ensuing segments of this work are organized in a systematic way: *section 1* articulates the concept, then *section 2* analyzes background and related studies. *Section 3* describes IoMT blackhole assault challenges. *Section 4* outlines the simulation methods used to evaluate network performance after attacks. *Section 5*, Results and Discussion then in *section 6* concluded with future work and an evaluation of results to improve IoMT network security against emerging threats.

2. BACKGROUND

2.1. Motivation

The effort to incorporate protocols used in traditional computer networks onto resource-constrained devices, such as IoT devices, are often quite challenging. The endeavor to incorporate all protocol features into such devices rapidly depletes their limited resources.

2.2. Routing Protocol for Low Power and Lossy (RPL) Networks

Low Power and Lossy Networks (LLNs) employ the distance vector routing protocol, RPL, premeditated for compatibility with IPv6. Through RPL, devices can be interconnected to form a topology referred to as a Destination Orientated Directed Acyclic Graph (DODAG). As stated by Winter et al.[11], this architecture is designed to prevent loops and directs all data created by the nodes to a single destination, the DODAG Root.

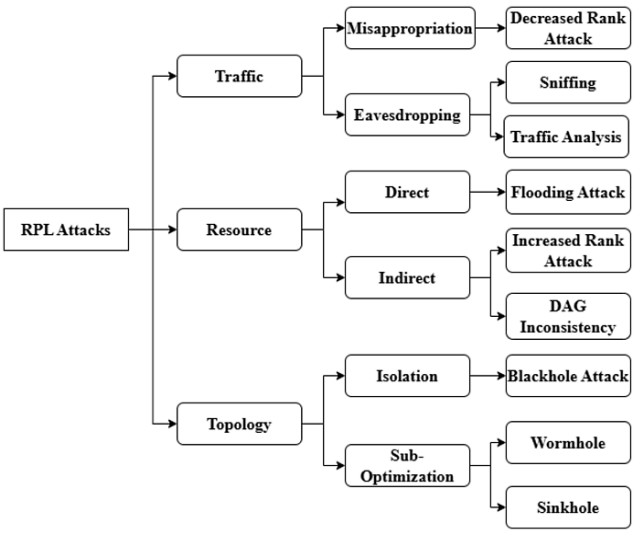

Figure 2. RPL Attacks

Figure 2 spectacles Traffic, Resource, and Topology RPL attacks. Eavesdropping and Misappropriation (Decreased Rank, Sniffing, and Traffic Analysis) compromise routing and data security. Direct (Flooding, Increased Rank) and indirect (DAG Inconsistency) resource attacks affect network resources. The isolation (Blackhole) and sub-optimization (wormhole, sinkhole) topology assaults interrupt traffic flow and connectivity. These attacks deteriorate network performance, emphasizing the need for robust security in RPL-based IoT networks[12].

2.3. Blackhole Attack

An isolated network can be subjected to a blackhole outbreak, where in a hostile node deletes all data packets intended for progressing. Network topology instability is indicated by a rise in the number of DIO packets when a Blackhole node is present, while stability is indicated by a drop in DIO messages. In this paper, we take a look at how a 6LoWPAN network gets hit by both a solo and a combined Blackhole assault[13].

An optimum DODAG gives each RPL node an upward path to the Border Route. There are nodes and their chosen parents. The packet must be sent to the node's preferred parent regardless of its fate. To develop a Blackhole attack, a hostile node lies about having an efficient route to the BR node at DODAG formation. Worse nodes become the network's parent overactive ones. Malicious nodes stealthily drop packets from other network nodes, generating a Blackhole and they can collaborate to launch a blackhole attack, making it harder to detect. *Figure 3* shows a single active Blackhole attack: node 1 is a root node and node 12 is a Blackhole. Node 12 quietly drops packets from nodes 5, 4, 3, and 2. If a node goes down, the packets will take a different route. Keep in mind that the Blackhole (node 12) spell has severed all connections to the network, leaving nodes 5, 4, and 3 without any other paths[14].

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 13, Issue 3 | Pages 602-608 | e-ISSN: 2347-470X

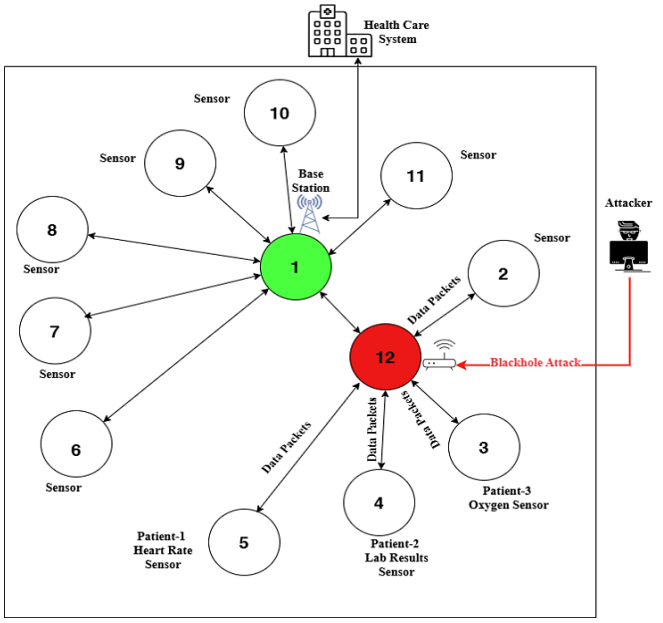

Figure 3. Blackhole attack with malicious node

Figure 4 illuminates light on which nodes will get affected when the blackhole outbreak takes place in healthcare system. An attacker can drop all the data packets received from nodes 2, 3, 4 and 5.

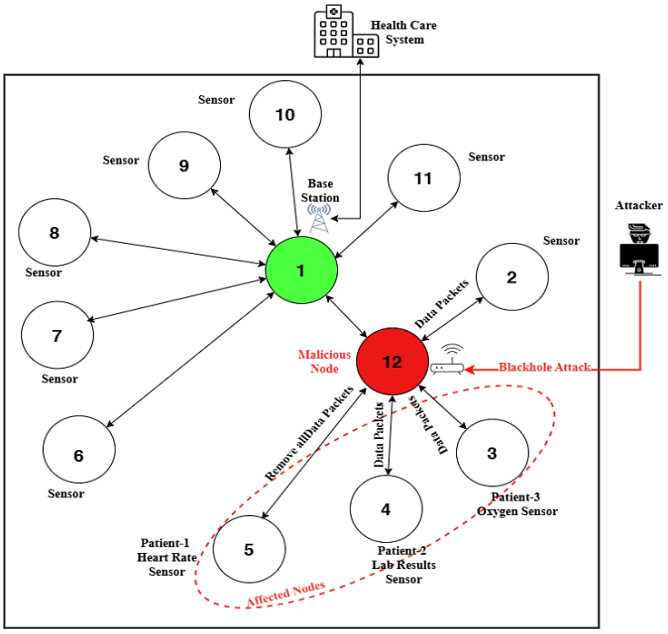

Figure 4. Blackhole disconnected nodes

3. RELATED WORKS

The literature review in the article outlines diverse approaches and procedures designed to improve security in RPL-based WSN for IoT applications, specifically on the mitigation of blackhole assaults.

The objective of this literature review is to examine and evaluate the diverse strategies and methodologies designed to protect RPL-based WSN from blackhole attacks, specifically within the framework of the IoMT. The evaluation seeks to elucidate the vulnerabilities of these networks, evaluate the efficacy of current security solutions, and pinpoint areas for additional research to bolster the resilience of IoT networks in essential healthcare applications.

Recent studies have progressively highlighted the utilization of deep learning, and hybrid methodologies for identifying attacks in RPL-based 6LoWPAN networks. Researchers[1] emphasized the promise of a hybrid lightweight system for the swift identification of assaults in IoMT instances, proving the applicability of ML approaches for real-time applications. The dependence on particular datasets raises questions regarding the generalizability of these findings across various IoMT contexts[2].

Despite attention to Version Number (VN) and Hello Flood (HF) assaults, blackhole assaults are understudied [7]. PDR and E2ED, which are essential for reliable healthcare data transfer [3], might be severely impaired by blackhole assaults, making the situation worrying. Research often ignores the complexity of real-world IoMT systems, making security plans difficult. It only uses a few databases, thus valuable studies from other sources may be missing. The research only covers ML, DL, and hybrid methods, while RPL and 6LoWPAN network terminology are not consistent.

The authors in [8] highlighted network-based assaults and their defense's' weaknesses. Recent research shows that deep learning-based Healthcare Internet of Things (HIoT) security solutions are more adaptable and accurate than traditional methods. However, low-power devices' high computational needs and resource limits require sophisticated, efficient security algorithms for HIoT contexts.

To mitigate these weaknesses, numerous novel solutions have been suggested. Researchers in [10] proposed a mutual authentication approach that combines medium access control with enhanced on-demand vector (EAODV) routing. This method not only improves data integrity and security but also demonstrates efficacy in crucial situations, like the COVID-19 pandemic, where secure data transfer is essential, a factor that is absent from this research.

The SBAODV protocol, created by the author in [5], seeks to enhance throughput and minimize network overhead while mitigating blackhole vulnerabilities in the IoMT and Unmanned Aerial Vehicles (UAVs). The AXHE protocol, as outlined by the author in [9], augments the security of healthcare data transfer via encryption, hashing, and adaptive XOR functions, resulting in significant enhancements in detection rates.

Emerging techniques, including multigrained scanning with tailored loss functions and deep stacking networks, have demonstrated substantial improvements in detection measures [15]. Two-phase technique (TB2PA) devised by [16] proficiently detects Sybil nodes in IoMT networks, enhancing packet loss ratios and processing durations.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 13, Issue 3 | Pages 602-608 | e-ISSN: 2347-470X

The GBG-RPL protocol presented by [17] integrates the Gini index with block chain technology to safeguard smart health monitoring devices from cyber-physical vulnerabilities. This approach has shown diminished packet loss, decreased energy usage, and enhanced assault detection rates, highlighting the promise of incorporating sophisticated technology to bolster network security.

Despite these advancements, challenges remain. The intrusion detection system based on deep learning called Adam-LSTM was suggested by [4] to deal with cybersecurity risks in the IoMT. Its 97% accuracy, precision, recall, and F1 score demonstrate outstanding performance, guaranteeing dependable healthcare services while safeguarding sensitive information. On the other hand, it can't handle heavy computations and can't scale well in real- time.

The use of ML approaches to discourse confidentiality and security disquiets in the IoMT is emphasized by [18], however they contend that existing research fails to appropriately reflect real-world IoMT systems and frequently ignores performance complexity criteria.

The authors [19] developed a method that uses ML, DL, and the Harris Hawk Optimization (HHO) algorithm to detect cyber-attacks in IoMT devices, achieving an accuracy of 99.85%. However, the method faces scalability limitations due to the volume of IoMT data and computational complexity, necessitating further optimization for scalability.

Recent initiatives to integrate IoT with Software- Defined Networking (SDN) have demonstrated potential in augmenting security, diminishing costs related to administration, and optimizing network performance [20]. Nevertheless, apprehensions about data access security endure, requiring additional investigation into stringent security protocols.

The authors in [21] emphasize the advancements and problems in medical cyber-physical systems (MCPS) and the medical internet of things (M-IoT) are discussed by the writers. Data transmission security without user identity communication is achieved by utilizing the SkeyM approach, a stateless token-based authentication mechanism. The study's key focus is on practicality, and its planned next steps involve making methodological improvements to accommodate increasingly massive data sets.

To increase patient data confidentiality and privacy, combat physician misuse, and handle scalability difficulties, the authors in [22] suggested a block chain-integrated quantum authentication technique for sensor-assisted IoMT networks; nevertheless, additional exploration is required for heavy network loads.

In [23], authors proposed a hybrid framework combining SDN controllers with deep learning techniques to manage IoMT security. The approach achieves 99.97% detection accuracy and a response time under 1.8 seconds, outperforming traditional methods. Further exploration is needed for scalability and computational overhead.

This literature study emphasizes the pros and cons of the suggested models for protecting RPL-based WSNs from blackhole attacks in the IoMT, which is crucial for the security of the network. Some of the benefits include better detection capabilities thanks to cutting-edge methods like deep learning and machine learning, which in turn increase network performance measures like E2ED and PDR. Problems with scalability and high computing complexity, in particular, can make implementation impractical in settings with limited resources. Furthermore, additional study is required to provide more resilient and flexible security solutions for IoMT networks, since the current emphasis on particular attack types may overlook other vulnerabilities.

3.1. Problem Statement

Blackhole attacks disrupt routing operations and reduce network performance in RPL-based Wireless Sensor Networks (WSN). The primary problem with a basic blackhole assault is that the node and subnet that is attacking become disconnected from the rest of the network. This detachment changes the topology of the network or prevents additional nodes from entering.

4. METHODOLOGY

An approach that can detect blackhole activity, as shown in *figure 5*, involves monitoring nodes for packet drops and taking corrective measures, such as identifying and removing the offending node, when necessary. For better overall performance, we included a timeout mechanism to prevent the system from becoming stuck indefinitely. In mission critical health care applications, like remote patient monitoring, the linked nodes in the network topology shouldn't wait for the root node to respond.

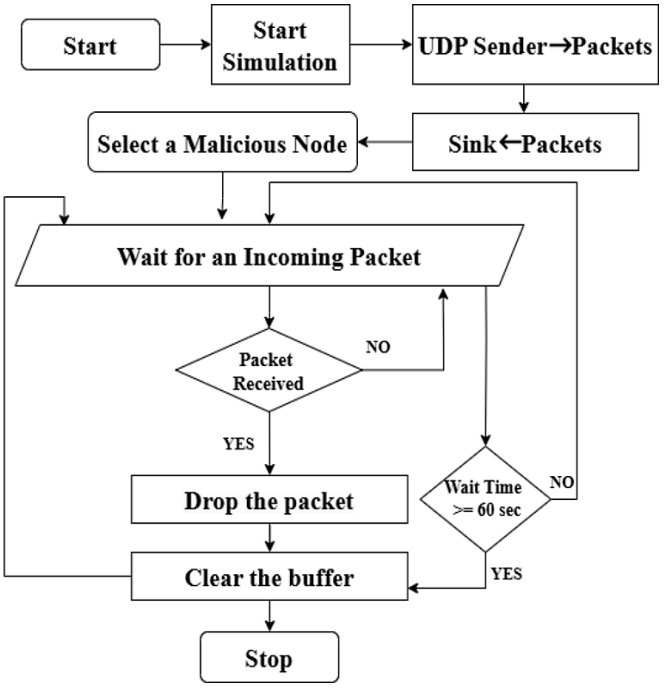

Figure 5. Methodology to detect blackhole attack

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 13, Issue 3 | Pages 602-608 | e-ISSN: 2347-470X

5. EXPERIMENTAL SETUP

This experimental setup employs Contiki and the Cooja simulator to replicate the blackhole attack. The green color node functions as a sink or root node, whereas the red color node represents a malevolent node. The remaining white nodes are client nodes. The devised scenario is evaluated in the Cooja simulator for 60 minutes across 10 iterations. In the initial case, there is an absence of a rogue node, and it is functioning normally.

5.1. Scenario-1

Figure 6, the scenario depicts 12 nodes participating in total, the central node 1 is a root node and there is no malevolent node present in the network.

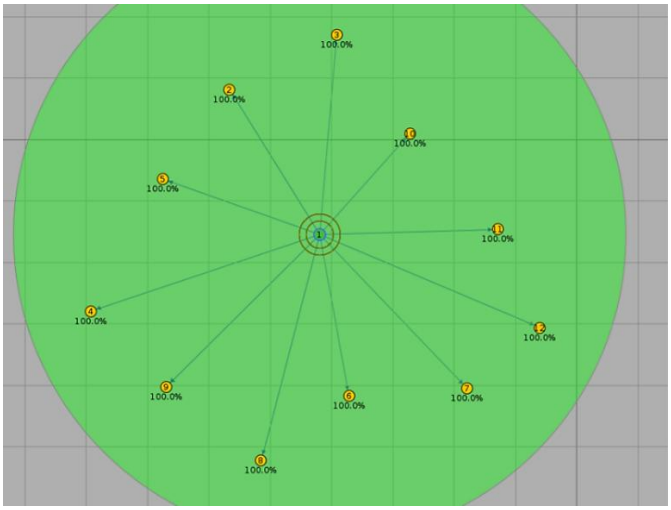

Figure 6. Scenario-1-11 Client Nodes, 1 Sink Node, 0 malicious node

The average power consumption graph generated with ZERO malicious node (pre-attack) is as follows:

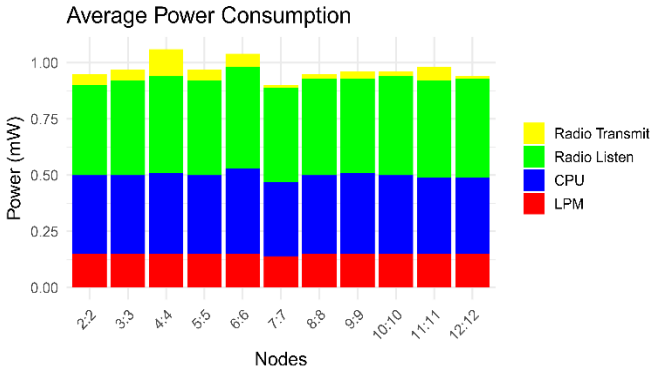

Figure 7. Average Power Consumption with 0 malicious node

5.2. Scenario-2

Figure 8 scenario there are 12 nodes participating in total, the central node1 is a sink node and one malicious node existing in the network. *Figure 9* spectacles the average power consumption graph that is created when a malicious node is present in the network arrangement.

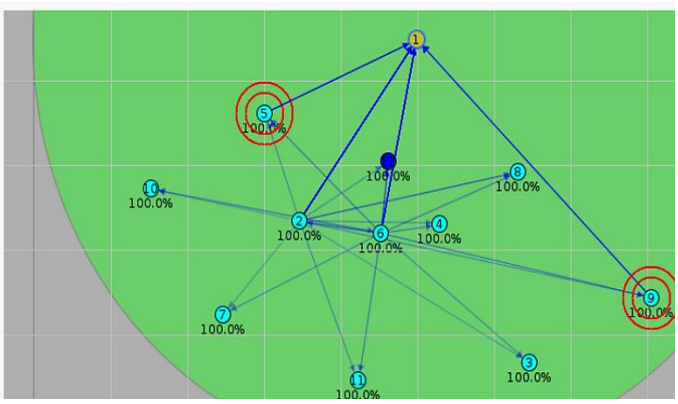

Figure 8. Scenario-2 11Client Nodes, 1 Sink Node, 1 malicious node

Experimental analysis conducted reveals that the RPL protocol refreshes preferred parent selection, affecting network performance via alterations in DAO packet flow. In Scenario 1, DAO packet activity was consistent, but Scenario 2 witnessed a substantial increase in DAO packet creation and transmission to the Root. Malicious nodes discarded DAO packets from child nodes, causing these nodes to transmit supplementary DAO messages in pursuit of a new parent via Local Repair. This conduct resulted in a rise in total DAO messages and packet losses in Scenario 2, underscoring the detrimental effect of malevolent nodes on network stability and efficiency.

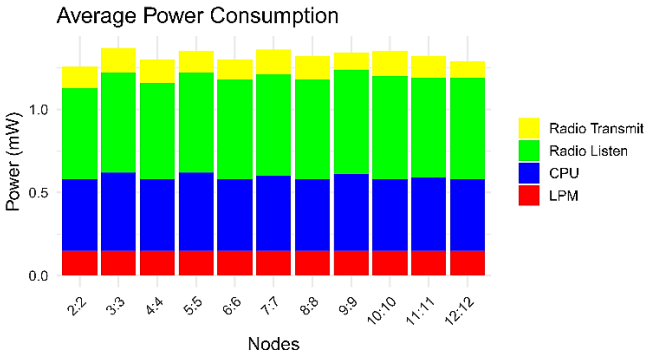

Figure 9. Average power Consumption graph with 1 malicious node

Furthermore, the malicious node sends out DAO-ACK packets but then drops out of the network since it leaves its last chosen parent value as NULL. In Scenario 2, the malicious node's disruptive influence is further demonstrated by this behavior, which significantly increases the quantity of control messages across the network.

6. RESULTS AND DISCUSSION

Table 1 illustrates how blackhole attacks affect network performance by analyzing packets transmitted and received. Scenario-1 sent 386 packets and got 678. More packets signal network inefficiencies, maybe due to external interference or intentional retransmissions. In Scenario-2, internal malicious nodes send 976 and 2203 packets. Packet duplication, flooding, and lost retransmissions from malicious nodes make this big disparity. Scenario-2 has more network instability from internal

International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 13, Issue 3 | Pages 602-608 | e-ISSN: 2347-470X

attacks than external threats. Effective detection is needed to prevent internal blackhole attacks and maintain network performance.

Table 1. Summary of packets sent and received

Scenarios	Packets Sent	Packets Received
Scenario-1	386	678
Scenario-2	976	2203

6.1. Observations and Statistical Analysis

Table II, significant variations were seen in critical variables when comparing power consumption before and after a blackhole attack. In all cases, Low Power Mode (LPM) continued to account for about 50-55% of the total power consumption, suggesting that idle energy usage was unaffected. Nevertheless, CPU utilization jumped from 10- 15% in the pre-attack scenario to 12-18% during the assault, indicating a 15-20% increase caused by the extra processing work needed to handle excessive control packets, such repeated DAO and DIO messages. Likewise, during the blackhole assault, Radio Listen's energy usage increased from 25-30% before the attack to 30-35% afterward, showing a 20-25% spike due to nodes spending more time monitoring and receiving malicious or redundant packets. Lastly, Radio Transmit energy, which was very low at 5-10% under normal circumstances, rose to 6-12% during the attack because of extra retransmissions caused by failed packets, which is a 10-20% increase. While idle power usage is unchanged, these data demonstrate that the blackhole assault significantly reduces network energy efficiency, especially in CPU and radio activities.

Table 2. Analysis of pre and post attack

Component	Pre-attack (%)	Post-attack (%)	Change (%)
LPM	~50-55	~50-55	No Change
CPU	~10-15	~12-18	+15-20
Radio Listen	~25-30	~30-35	+20-25
Radio Transmit	~5-10	~6-12	+10-20

ACKNOWLEDGEMENT

Our sincere thanks to my supervisor Dr. P. Rutravigneshwaran, Dr. S. Mythili, Head of the Department, Karpagam Academy of Higher Education, for giving us an opportunity to complete my research article.

REFERENCES

[1] S. S. Hameed *et al.*, "A Hybrid Lightweight System for Early Attack Detection in the IoMT Fog," *Sensors*, vol. 21, no. 24, p. 8289, Dec. 2021, doi: 10.3390/s21248289. Available: https://www.mdpi.com/1424-8220/21/24/8289. [Accessed: Dec. 31, 2024]

[2] S.-E. Chafi, Y. Balboul, S. Mazer, M. Fattah, and M. El Bekkali, "Resource placement strategy optimization for smart grid application using 5G wireless networks," *IJECE*, vol. 12, no. 4, p. 3932, Aug. 2022, doi: 10.11591/ijece.v12i4.pp3932-3942. Available: http://ijece.iaescore.com/index.php/IJECE/article/view/26814. [Accessed: Dec. 31, 2024]

[3] F. Wahab *et al.*, "An AI-Driven Hybrid Framework for Intrusion Detection in IoT-Enabled E-Health," *Computational Intelligence and Neuroscience*, vol. 2022, pp. 1–11, Aug. 2022, doi: 10.1155/2022/6096289. Available: https://www.hindawi.com/journals/cin/2022/6096289/. [Accessed: Mar. 19, 2025]

[4] K. Vaisakhkrishnan, G. Ashok, P. Mishra, and T. G. Kumar, "Guarding Digital Health: Deep Learning for Attack Detection in Medical IoT," *Procedia Computer Science*, vol. 235, pp. 2498–2507, 2024, doi: 10.1016/j.procs.2024.04.235. Available: https://linkinghub.elsevier.com/retrieve/pii/S1877050924009116. [Accessed: Dec. 26, 2024]

[5] J. A. Shaikh *et al.*, "A UAV-Assisted Stackelberg Game Model for Securing IoMT Healthcare Networks," *Drones*, vol. 7, no. 7, p. 415, Jun. 2023, doi: 10.3390/drones7070415. Available: https://www.mdpi.com/2504-446X/7/7/415. [Accessed: Dec. 26, 2024]

[6] N. Alfriehat *et al.*, "RPL-based attack detection approaches in IoT networks: review and taxonomy," *Artif Intell Rev*, vol. 57, no. 9, p. 248, Aug. 2024, doi: 10.1007/s10462-024-10907-y. Available: https://link.springer.com/10.1007/s10462-024-10907-y. [Accessed: Dec. 25, 2024]

[7] T. A. Al-Amiedy, M. Anbar, and B. Belaton, "OPSMOTE-ML: an optimized SMOTE with machine learning models for selective forwarding attack detection in low power and lossy networks of internet of things," *Cluster Comput*, vol. 27, no. 9, pp. 12141–12184, Dec. 2024, doi: 10.1007/s10586-024-04598-x. Available: https://link.springer.com/10.1007/s10586-024-04598-x. [Accessed: Dec. 26, 2024]

[8] A. T. Mathew and P. Mani, "Strength of Deep Learning-based Solutions to Secure Healthcare IoT: A Critical Review," *TOBEJ*, vol. 17, no. 1, p. e187412072304060, May 2023, doi: 10.2174/18741207-v17-e230505-2022-HT28-4371-2. Available: https://openbiomedicalengineeringjournal.com/VOLUME/17/ELOCATOR/e187412072304060/. [Accessed: Dec. 26, 2024]

[9] D. A. Chaudhari and E. Umamaheswari, "A new adaptive XOR, hashing and encryption-based authentication protocol for secure transmission of the medical data in Internet of Things (IoT)," *Biomedical Engineering / Biomedizinische Technik*, vol. 66, no. 1, pp. 91–105, Feb. 2021, doi: 10.1515/bmt-2019-0123. Available: https://www.degruyter.com/document/doi/10.1515/bmt-2019-0123/html. [Accessed: Dec. 26, 2024]

[10] J. Sun, F. Khan, J. Li, M. D. Alshehri, R. Alturki, and M. Wedyan, "Mutual Authentication Scheme for the Device-to-Server Communication in the Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15663–15671, Nov. 2021, doi: 10.1109/JIOT.2021.3078702. Available: https://ieeexplore.ieee.org/document/9426898/. [Accessed: Nov. 16, 2024]

[11] T. Winter *et al.*, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," RFC Editor, RFC6550, Mar. 2012. doi: 10.17487/rfc6550. Available: https://www.rfc-editor.org/info/rfc6550. [Accessed: Dec. 27, 2024]

[12] Anthea Mayzaud, Remi Badonnel, and Isabelle Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things," *International Journal of Network Security*, vol. 18, no. 3, May 2016, doi: 10.6633/IJNS.201605.18(3).07

[13] N. Panda and M. Supriya, "Blackhole Attack Prediction in Wireless Sensor Networks Using Support Vector Machine," in *Advances in Signal Processing, Embedded Systems and IoT*, V. V. S. S. S. Chakravarthy, V. Bhateja, W. Flores Fuentes, J. Anguera, and K. P. Vasavi, Eds., in Lecture Notes in Electrical Engineering, vol. 992. Singapore: Springer Nature Singapore, 2023, pp. 321–331. doi: 10.1007/978-981-19-8865-3_30. Available: https://link.springer.com/10.1007/978-981-19-8865-3_30. [Accessed: Dec. 29, 2024]

[14] S. M. and G. L., "K-Means Clustering-Based Trust (KmeansT) Evaluation Mechanism for Detecting Blackhole Attacks in IoT

International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 13, Issue 3 | Pages 602-608 | e-ISSN: 2347-470X

Environment," *IJCDS*, vol. 15, no. 1, pp. 739–751, Aug. 2024, doi: 10.12785/ijcds/160154. Available: https://journals.uob.edu.bh/handle/123456789/5289. [Accessed: Dec. 21, 2024]

[15] P. Musikawan, Y. Kongsorot, P. Aimtongkham, and C. So-In, "Enhanced Multigrained Scanning-Based Deep Stacking Network for Intrusion Detection in IoMT Networks," *IEEE Access*, vol. 12, pp. 152482–152497, 2024, doi: 10.1109/ACCESS.2024.3480011. Available: https://ieeexplore.ieee.org/document/10716376/. [Accessed: Dec. 26, 2024]

[16] A. Shaji and N. S. Nair, "A Novel Trust Based Two Phase Algorithm to Detect Sybil Attack in IoMT Networks," in *2023 9th International Conference on Smart Computing and Communications (ICSCC)*, Kochi, Kerala, India: IEEE, Aug. 2023, pp. 309–314. doi: 10.1109/ICSCC59169.2023.10334946. Available: https://ieeexplore.ieee.org/document/10334946/. [Accessed: Dec. 26, 2024]

[17] M. Javed, N. Tariq, M. Ashraf, F. A. Khan, M. Asim, and M. Imran, "Securing Smart Healthcare Cyber-Physical Systems against Blackhole and Greyhole Attacks Using a Blockchain-Enabled Gini Index Framework," *Sensors*, vol. 23, no. 23, p. 9372, Nov. 2023, doi: 10.3390/s23239372. Available: https://www.mdpi.com/1424-8220/23/23/9372. [Accessed: Dec. 26, 2024]

[18] S. S. Hameed, W. H. Hassan, L. Abdul Latiff, and F. Ghabban, "A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches," *PeerJ Computer Science*, vol. 7, p. e414, Mar. 2021, doi: 10.7717/peerj-cs.414. Available: https://peerj.com/articles/cs-414. [Accessed: Dec. 26, 2024]

[19] S. Abbas, G. A. Sampedro, M. Abisado, A. Almadhor, I. Yousaf, and S.-P. Hong, "Harris-Hawk-Optimization-Based Deep Recurrent Neural Network for Securing the Internet of Medical Things," *Electronics*, vol. 12, no. 12, p. 2612, Jun. 2023, doi: 10.3390/electronics12122612. Available: https://www.mdpi.com/2079-9292/12/12/2612. [Accessed: Dec. 26, 2024]

[20] A. S. Ahmed and H. A. Salah, "Development a Software Defined Network (SDN) with Internet of Things (IoT) Security for Medical Issues," *JQCM*, vol. 15, no. 3, Sep. 2023, doi: 10.29304/jqcm.2023.15.3.1268. Available: https://jqcsm.qu.edu.iq/index.php/journalcm/article/view/1268. [Accessed: Dec. 27, 2024]

[21] N. S., S. Palanisamy, and N. T., "Achieving Secured Medical Network (SMN) through Stateless Mechanism and SkeyM in Medical-Internet of Things (M-IoT)," *J. Eng. Appl. Sci.*, vol. 71, no. 1, p. 128, Dec. 2024, doi: 10.1186/s44147-024-00460-4. Available: https://jeas.springeropen.com/articles/10.1186/s44147-024-00460-4. [Accessed: Dec. 27, 2024]

[22] S. Prajapat, P. Kumar, D. Kumar, A. Kumar Das, M. Shamim Hossain, and J. J. P. C. Rodrigues, "Quantum Secure Authentication Scheme for Internet of Medical Things Using Blockchain," *IEEE Internet Things J.*, vol. 11, no. 23, pp. 38496–38507, Dec. 2024, doi: 10.1109/JIOT.2024.3448212. Available: https://ieeexplore.ieee.org/document/10643610/. [Accessed: Dec. 27, 2024]

[23] Y. Rbah *et al.*, "Hybrid software defined network-based deep learning framework for enhancing internet of medical things cybersecurity," *IJ-AI*, vol. 13, no. 3, p. 3599, Sep. 2024, doi: 10.11591/ijai.v13.i3.pp3599-3610. Available: https://ijai.iaescore.com/index.php/IJAI/article/view/24892. [Accessed: Dec. 27, 2024]