INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ORIGINAL ARTICLE

Impact Analysis of Malicious IoT Node Placement for Blackhole Attack Detection and Mitigation using Deep Learning-Based Trust Evaluation

M Shameer[1]*, P Rutravigneshwaran[2]

1 Research Scholar, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore 21, Tamil Nadu, India
2 Assistant Professor, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore 21, Tamil Nadu, India

OPEN ACCESS

Received: 14/06/2025
Accepted: 25/07/2025
Published: 20/08/2025

Citation: Shameer M, Rutravigneshwaran P (2025) Impact Analysis of Malicious IoT Node Placement for Blackhole Attack Detection and Mitigation using Deep Learning-Based Trust Evaluation. Indian Journal of Science and Technology 18(32): 2581-2593. https://doi.org/10.17485/IJST/v18i32.1109

* **Corresponding author**.

mdsameer09@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: The objective of this study is to create a deep learning-based trust evaluation mechanism that can detect blackhole incidents and investigate how faulty node positions impact IoT network performance. **Methods:** Six LoWPAN networks competing with the RPL protocol were simulated on IPv6 with Contiki OS and the Cooja simulator. Contiki is a light-weight operating system suitable for low-power devices. The standard simulator Cooja is widely used for RPL implementations, which allows testing and simulating networks for IoT devices. We simulated three models incorporating both internal and external hostile nodes. Using a deep learning-based Multilayer Perceptron (MLP) trust evaluation system, black hole assaults were detected through network metrics implementation, packet delivery ratio, latency, throughput, and power utilization. **Findings**: Our results emphasize the critical importance of implementing effective security mechanisms into use to locate and reduce internal black hole attacks. IoT systems need these mechanisms to maintain energy efficiency, network reliability, and overall integrity, especially in cases where reliability is crucial. Our research findings support the enhancement of security in RPL-based IoT systems and help researchers mitigate threats in an effective way. **Novelty**: This study presents significant outcomes, including Packet Delivery Ratio (PDR) of 94.44% and throughput of 87,406.38 bps, comparable to scenario S-II, which achieved a PDR of 69.23% and a throughput of 2,463.33 bps using a deep learning-based trust system concurrently with IoT network performance, particularly in the presence of core and outward blackhole occurrences.

Keywords: Blackhole attacks; Deep learning; IoT security; RPL; Trust framework

1 Introduction

Driven largely by expansions in information and communication technology, the swift entry of the digital era has resulted in a growing need for improved operational services. Considered a disruptive discovery, IoT significantly enhances many sides of human life, including business operations, customer support, and decision-making processes[1]. While many industries benefit from the IoT's quick development recently, healthcare stands out for consuming IoMT (Internet of Medical Things) innovations. Embedded medical devices, wearables for geriatric monitoring, clinical equipment associated with the internet, remote operations in hospital rooms, and remote vital monitoring, including blood pressure and heart rate, constitute part of the IoMT. Although the IoMT ecosystem is extremely advantageous, it is vulnerable to hacking due to the wide scope and absence of security safeguards[2].

The vulnerabilities in the IoMT healthcare environment could also have a similar effect on the other IoT systems. Though IoT offers certain advantages, the security concerns pose a noteworthy risk. IoT devices are particularly vulnerable to several types of attacks due to inherent limits: restricted memory, processing capabilities, and small battery limits. Research conducted in 2020 reveals blackhole assaults as a particularly concerning threat in which evil nodes trash all arriving packets, therefore upsetting routing mechanisms and jeopardizing network connectivity. Such incidents not only make vulnerable data transmission truthful but also lower overall network performance, which underlines the critical need for effective security procedures[3].

The research gaps found in the literature[4] are summarized as follows:

- Lack of trust evaluation mechanism exhibited in deep learning-based IoT security approach.
- Detecting and isolating malicious nodes using existing trust assessments is not effective.
- Implementation of heavy cryptographic protocols is not suitable for low-power and memory-constrained devices.
- The limited integration of direct and indirect trust scores results in a low threat detection rate.

This article details Deep Learning-based Trust (DLT) assessment technique designed to identify and manage black hole breakouts in Internet of Things environments. The suggested system employs a comprehensive trust evaluation procedure combining advice from other network entities with direct observations to handle existing security issues.

The Deep Learning-based Multilayer Perceptron (MLP) method increases the integrity and reliability of nodes in the network. This is accomplished by effectively recognizing and neutralizing black hole assaults. We have closely investigated certain performance metrics like latency, delivery, and exposure percentage. Important mathematical modeling and simulation-based studies have been conducted. The results fully show that, in comparison to other methods, the DLT mechanism significantly raises the security of these exchanges. The performance metrics derived from the proposed model indicate that the Packet Delivery Ratio (PDR) of 94.44% is higher than that of the KmeanT model, which had a PDR of 82.5%, as noted in reference[5]. Also, great success enables one to assist IoT technology in maintaining its secure expansion and multiplication. The paper's structure continues: Section 2, research methods, introduces technique, setup, and scenarios. The third part describes the outcomes and debate. Conclusions exist in the fourth part.

1.1 IoT Architecture Perspective

The IoT architectural approximation calls the elements and their collaborations, allowing real-world things to relate with virtual reality. Although other models exist, a typical architectural framework notes four important layers: insight, network, function, and contract layers[6].

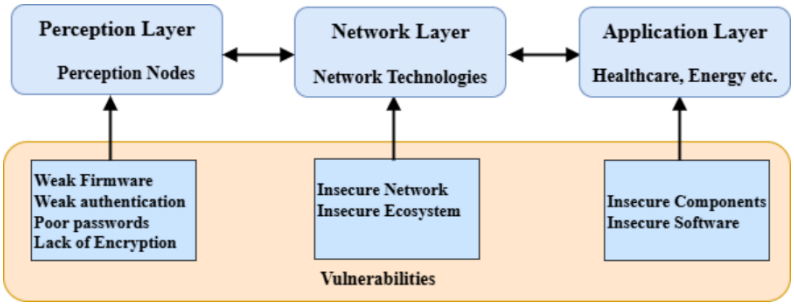

Fig 1. IoT Architecture and Vulnerabilities

Firstly, Figure 1 shows the accountability of perception in gathering information from the physical world, while observation layer forms the spine of IoT. Secondly, the simulated environment receives data from network layer derived from perception layer. Thirdly, the application layer derives the needed functionality and insights by using the data acquired from the network layer. Data visualization, real-time monitoring, control actions, and decision-making grounded on gathered data define key characteristics of the application layer. Numerous vulnerabilities exist when transitioning between different layers, as depicted in Figure 1.

1.2 RPL

Most IoT applications depend on infrastructure that is cost-effective with long operational times. Low Power and Lossy Networks (LLNs) delivers required speed, cost-effectiveness. However, Routing Protocol for Low-Power and Lossy Networks (RPL) lacks the security method required to distribute keys equally among nodes. This makes the RPL prone to vulnerabilities. For example, a malicious node that uses RPL's auxiliary devices to target smart devices and compromise the grid. The black hole assault example Vehicular Ad-hoc Networks (VANET), as discussed in [7], comprises a malicious vehicle intercepting the data and dropping the packets to disrupt communication.

1.3 RPL Attacks

RPL attacks are sporadically regarded as groups: resource, traffic, and network topology-oriented assaults [8], which are further classified in Table 1 as follows:

Table 1. RPL Attack Types [9]

RPL Attacks	Types	Impact
Resource-based	Hello Flooding	Massive network traffic is generated.
	Increased Rank	Interruption of routing topology
	Version Number	Drains the node's power resources
Traffic-based	Sybil	Weakens the network performance
	Decreased Rank	Increasing the network traffic
	Selective Forwarding	Dislocation of the network
Network topology-based	DIO	The network will break down.
	Warm hole	Exhaust network resources
	Black hole	Packets are dropped without reaching their destination
	Sink hole	Disrupts the network communication path

1.4 Impact of Black hole Attacks

An infected sensor device deceptively claims to have the fastest path to the target. Also, dropping the data packets by rerouting them will result in a black hole assault [4]. This attack can seriously affect data integrity and disrupt network operations. Because of their resource-constrained character and reliance on multi-hop communication, blackhole attacks especially pose a threat in Wireless Sensor Networks (WSN). The case study example mentioned in [7], a black hole assault, and the WSN generally suffer in network performance. Rates of packet delivery diminish, latency rises, and the network's throughput. The countermeasure for this attack is to detect and isolate the malicious node.

Related Works

Recent literature articles under evaluation cover trust management, hybrid Intrusion Detection Systems (IDS), extending Machine Learning (ML), Deep Learning (DL), and cybersecurity, mostly black hole threats, and are compiled in the below **Table 2 and Table 3**, which exhibit research gaps such as the use of traditional cryptographic methods, lacking trust and deep learning integration, no malicious node placement analysis, and performance indicators not covered completely. The proposed work has addressed these identified gaps by implementing a novel DL trust evaluation mechanism to detect black holes in the IoT healthcare environment.

Table 2. Summary of recent literature work (2025-2024)

Citation	Methodology	Disadvantages	Proposed Work	Key Findings
[10], 2025	Enhanced Support Vector Machine	Attack detection accuracy is missing.	Cross-layer attack detection.	High throughput and less packet loss.
[11], 2025	Primary Component Analysis	Latency is exhibited. Complex threats are not considered.	DL model Bi-directional Long short-term memory	Effectively mitigates cyberattacks in the IoMT.
[12], 2025	Zero trust-enabled trust evaluation	Computation Complexity.	Mechanism to access adjacent nodes trust.	Risk-Based Access Control Engine.
[13], 2024	DDoS, KNN	Identifying types of DDoS attacks.	SMOTE's use fills dataset gaps and improves performance.	Hybrid algorithm to detect DDoS attacks.
[14], 2024	Multilayer perceptron	No Trust evaluation mechanism.	Deep learning-based detection framework.	Improved security using the MLP model.
[15], 2024	Machine learning pipeline	Doesn't cover IoT protocols.	Parallel combination of CNN.	Novel Cooperative approach to IDS.
[16], 2024	Delta Threshold model	Trust calculations are not optimized.	Optimized Reporting Module	High BHA detection rate.
[17], 2024	Deep learning, Performance metrics	Limited memory and processing power.	Hybrid IDS approach with ML and DL.	Enhanced network security.

Table 3. Summary of Earlier Research and Proposed Work (2023-2019)

Citation	Methodology	Disadvantages	Proposed Work	Key Findings
[18], 2023	svBLOCK		Improves Network Security in LLNs.	Isolates and lessens black holes.
[19], 2023	SSOPNN	No proof of concept. Limited attack types in the dataset.	Feature selection technique with Pearson's correlation.	Enhanced SSOPNN-based threat detection.
[20], 2023	K-means and Trust Management	No Comparative Analysis.	KmCtrust model for IoBT.	Improved network security in IoBT.
[21], 2022	Quantitative Analysis	Less focus on experiment.	Innovative framework to detect RPL spells.	Attack mapping and action resolution.
[22], 2022	Distributed Timer-based detection	Inspection of cross-layer security is not exhibited.	Two-step verification model.	Lightweight black hole detection mechanism.
[23], 2021	Random Forest	Trust, orchestration issues exist.	Security framework for Fog-IoT systems.	Critical security and trust issues are dealt.
[24], 2020	Risk identification	Performance metrics are not assessed.	Framework for secure WSN and IoT.	Cyberattack detection and mitigation techniques.
Proposed	DL, ML, Trust Evaluation	Testing under large network environment is needed	Innovative DLT techniques and trust mechanisms.	Precise malicious node detection, network security. Reduced latency and error rates.

SSOPNN: Squirrel Search Optimized Probabilistic Neural Network, IoBT: Internet of Battle Things, KNN: k-Nearest Neighbors, DDos: Distributed Denial of Service, CNN: Convolutional Neural Network

2 Methodology

Deep learning's increased flexibility to varied data characteristics allows it to perform better with larger datasets. IoT systems produce significant amounts of data, and the attacks aimed at them have various characteristics that are not easily discernible using linear models. Figure 2 shows the simulation length recorded using Cooja plugins; log files were examined for many routing techniques to extract characteristics. The suggested method uses pre-processed datasets that include vital components like node ID, temporal data, packet length, energy metrics, performance metrics, and total packets sent and received, which helps in training the system. By analyzing these characteristics, a learning algorithm builds a strong detection system capable of identifying hostile nodes and disturbances and achieves network security. Algorithm 1 shows an approach to ascertain and separate blackhole spells in an IoT network.

Algorithm 1: Proposed DLTrust Algorithm
1: **Data Preparation:**
2: Import dataset (dataset.csv) and shuffle rows
3: Split into X (features) and Y (labels)
4: **Feature Selection:**
5: Train Randomized Decision Trees, drop insignificant features
6: **Trust Evaluation:**
7: Initialize trust scores for all nodes
8: **for** each node **do**
9: Compute **Packet Forwarding Score (PFS)**:

$$PFS = \frac{\text{Packet Forwarded}}{\text{Total Packets Received}}$$

10: Compute **Confidence Level (CL)**:

$$CL = \alpha \times \text{ Recent Behavior } + (1-\alpha) \times \text{ Historical Behavior}$$

11: Update **Trust Score (TS)**:

$$TS = w_1 \times PFS + w_2 \times CL$$

12: **if** $TS <$ Threshold **then**
13: Mark node as untrustworthy
14: **end if**
15: **end for**
16: **Dataset Splitting:** Partition into training (X_{train} ,Y_{train}) and testing sets (Xtest, Ytest)
17: **Deep Learning Model:**
18: Define and configure a sequential model
19: Set optimizer (AdaDelta) and compile with MSE loss function
20: Train the model using X_{train}
21: Save model and weights
22: **Prediction and Trust Re-Evaluation:**
23: Load prediction dataset ($df_{predict}$), extract and scale $X_{predict}$
24: **for** each node in $df_{predict}$ **do**
25: Recalculate *PFS* and *CL*
26: Update trust scores and exclude untrustworthy nodes
27: **end for**
28: **Classification and Output:**
29: Perform classification and present results
30: End the function

Figure 3 shows the flow of proposed methodology normalizes PFS value from 0 to 1. CL is the weighted average of how nodes behave and how they interact with each other over time. The weights for TS are w1=0.4 and w2=0.6. The threshold value is 0.7. Trusted nodes have values over 0.7, whereas partially trusted nodes have values below 5. TS is less than 0.5 for black hole nodes[5].

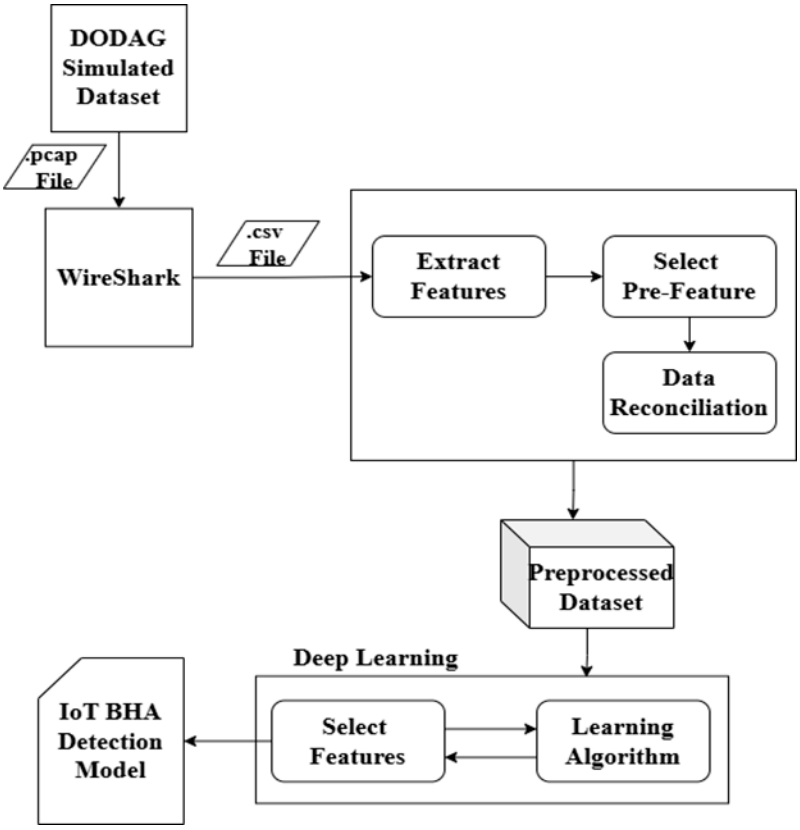

Fig 2. BHA detection Methodology

Experimental Analysis:

2.1 Simulation Setup

The simulation parameters used in this experiment are inspired by reference topology; the scenarios conducted by means of Contiki and Cooja simulator have specific objectives. Procedures of the experimental evaluation process are as follows:

First, create a topology.

In the second step, at a designated point, create a malevolent node to initiate the attack.

In the third step, use the topologies in the simulator and record RPL protocol data.

Create the output of the Collect View for the chosen set of measurements in Step 4.

Follow steps 3 and 4 for every assessed attack scenario.

Sixth step: project and assess the result of every attack.

The proposed three scenarios for this attack: 100% of nodes inside the sink node's radio range and 50% external. We establish a reference topology without malicious nodes or attacker nodes in the first scenario. In the second case, an assailant node is placed indoors within radio range of the root node. In the third scenario, nodes are placed outdoors in a range. Nodes 12 and 13 launch an attack on nodes 4, 5, 6, 7, and 8, causing them to lose all their packets.

2.1.1. Scenario-I (S-I)

Figure 4 represents devoid of blackhole assaults, involved one sink node, eleven sender nodes, and no malicious nodes. Figure 5 illustrates nodes like 2.2 and 10.10 have superior energy efficiency, maybe because of reduced routing or data forwarding. By

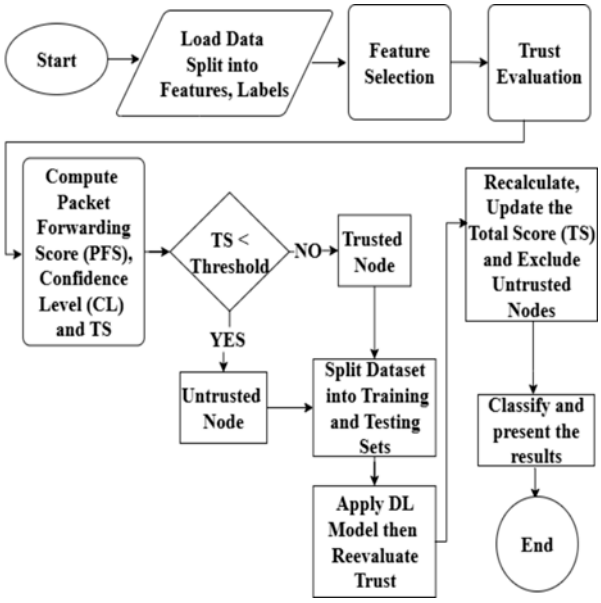

Fig 3. Proposed Algorithm Flowchart

forwarding more packets to adjacent nodes, nodes 9.9 and 10.10 use more power and increase the graph's radio and listen cycle. A trust-aware system may signal these nodes for closer monitoring due to high energy utilization, which may imply malicious behavior like Black Hole or Wormhole assaults.

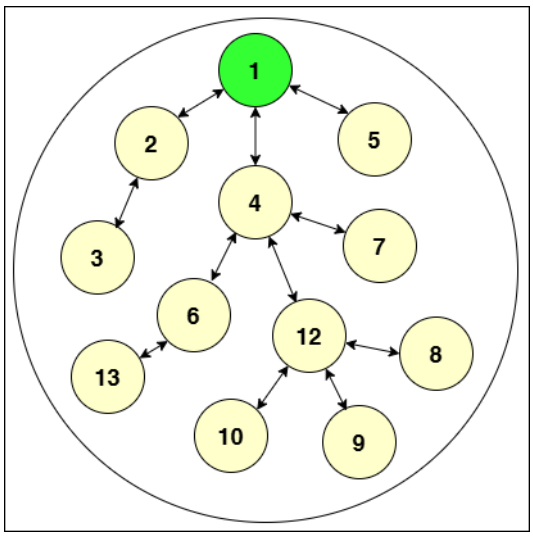

Fig 4. No Malicious Nodes

2.1.2. Scenario-II (S-II)

Figure 6 and Figure 7 display mockup results for the black hole attacks, which included two malevolent nodes inside the range, eleven sender nodes, and one sink node. Temperature, power depletion, packet delivery, and end-to-end latency ratio were all determined to be subpar in this scenario. Power analysis reveals considerable power inefficiencies when two malicious nodes exist. Quick identification and separation of dangerous nodes helps one to reduce energy drain and guarantee balanced power consumption over the network.

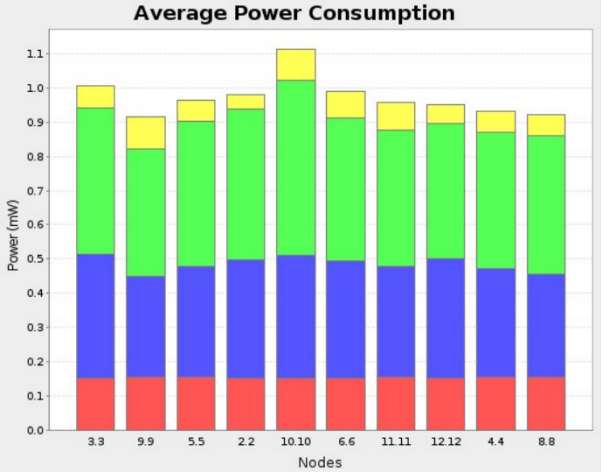

Fig 5. Power consumption with no malicious nodes

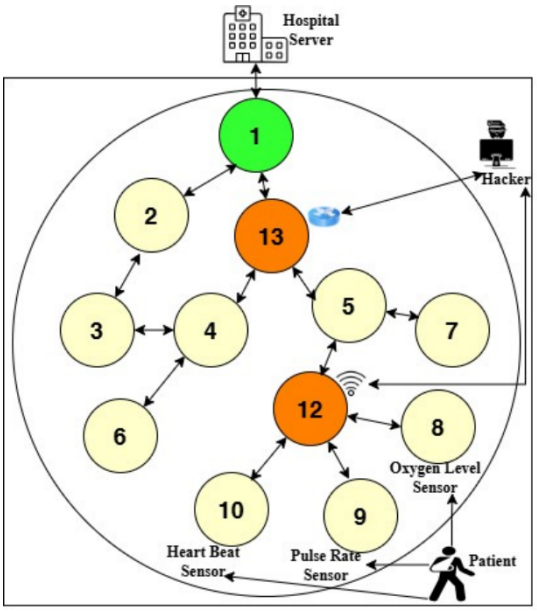

Fig 6. Malicious nodes present inside

2.1.3. Scenario-III (S-III)

There are two attacking nodes placed outside the range, eleven sender nodes, and one sink node that contains the black hole assaults in the simulation shown in Figure 8 below. From this test, we perceived abnormalities in power ingesting, packet transfer, end-to-end delay ratio, and temperature reading.

Figure 9 illustrates how radio listening and transmission contribute significantly to power consumption in IoT networks. Communication overhead causes some nodes to have higher energy consumption, so accenting the need for effective resource management.

2.1.4. Functioning Statistics

Use the subsequent formulas for execution computations:

Computer Power

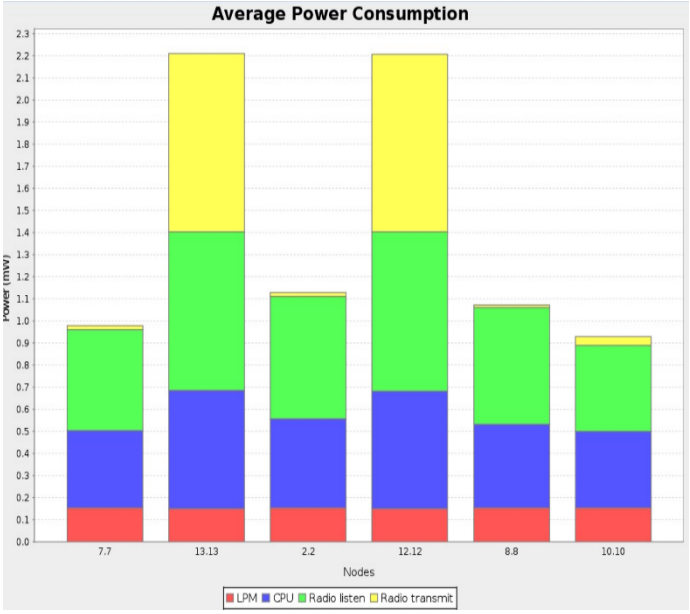

Fig 7. Power Consumption with malicious nodes inside

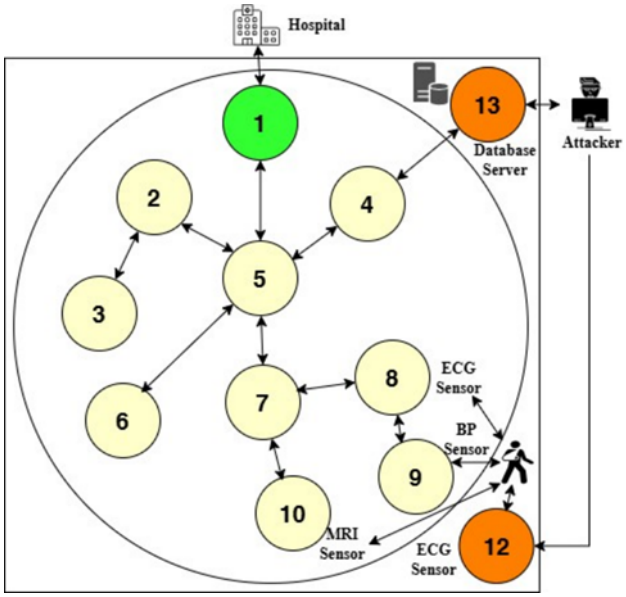

Fig 8. Malicious nodes present outside

Using its functional period, Low Power Mode (LPM) interval, transmission spell, response period, voltage provision, and normalization factor for power computation, the CPU is vital in power calculations.

$$\text{Power} = \frac{3v(cpu \times 0.5 + lpm \times 0.0005 + T_x \times 17.4 + R_x \times 18.8}{32768} mJ \quad (1)$$

Packet Delivery Ratio

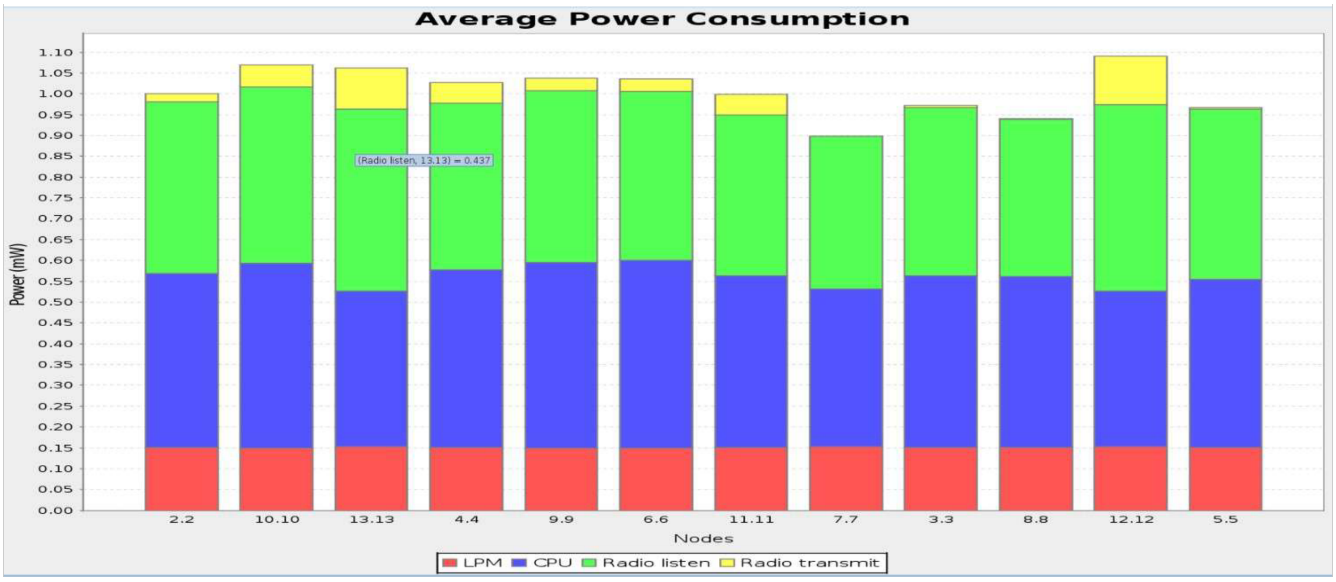

Fig 9. Power utilization when malicious nodes are outside

By means of the total packets received (tpr), total packets sent (tps), and the number of transmissions (n), the equation below computes the part of received packets relative to those transmitted.

$$\text{PDR} = \frac{\sum_{k=0}^{n} tpr}{\sum_{k=0}^{n} tps} \times 100 \tag{2}$$

For Expected Transmission Count

Critical in packet delivery are the probability of successful transmission (pt), acknowledgment (pa), and expected number of transmissions (ETX).

$$\text{ETX} = \frac{1}{pt \times pa} \tag{3}$$

Duty Cycle

Whereas LPM_time indicates the duration distributed in low-power type during the listening duty cycle, Tx_time represents the time spent in data transmission, and Duty Cycle Rx_time quantifies the CPU's active duration.

$$\text{Listen Duty cycle} = \frac{Rx\_time}{CPU\_time + LPM\_time} \times 100\% \tag{4}$$

Cycle of Transmit Duty=

$$\frac{Tx\_time}{CPU_{time} + LPM\_time} \times 100\% \tag{5}$$

Delay

The delay computation consists of finding the aggregate number of packets transferred, the receipt, and the k-th packet's transmission time.

$$\text{Delay} = \sum_{k=1}^{n} (rt(k) - st(k)) sec \tag{6}$$

Throughput

Throughput computed using Calculate the packets received, their byte count, the bit conversion factor, transmission length, and bps throughput.

$$\text{Tp} = \frac{tp \times s \times 8}{tt} bps \tag{7}$$

3 Results and Discussion

Table 4. Black hole attacks analysis result

Performance Indicators	S-II	S-III	Equation	S-II Result	S-III Result
Power:					
CPU	0.413	0.425			
LPM	0.151	0.151	(**Eq. 1**)	0.00078	0.001438
Listen Power	0.407	0.562			
Transmit Power	0.038	0.283			
PDR:					
Packets Received	45	34	(**Eq. 2**)	69.23077	94.44444
Packets Lost	65	36			
ETX:	19	20	(**Eq. 3**)	19	20
Duty Cycle:					
Listen	0.678	0.936	**(Eq. 4)**	120.2128	162.5
Transmit	0.071	0.532	**(Eq. 5)**	113.8496	828.9832
Delay	12	58	(**Eq. 6**)	12	58
Throughput:					
Total Packets	7625	233743	(**Eq. 7**)	2643.333	87406.38
Packet Size	78	84.137			

Table 4 shows the simulation effect of malevolent nodes placed both inside and outside the network range limits. Attackers targeting inside nodes (S-II) purposefully discard packets, reducing PDR by 69.23% and increasing packet loss. Still, the latency stays low (12s), and energy use is rather low since fewer transmissions occur from the rapid packet discarding. On the other hand, spiteful nodes outside the radio range (S-III) cannot physically discard packets; rather, they could change routing patterns, increase retransmissions, and cause network instability. Although with a significant increase in latency (58s), energy expenditure, and transmission overhead, this results in a quite high PDR of 94.44%. From 19 to 20, the ETX increases somewhat to indicate a rise in S-III retransmissions resulting from indirect interruptions. Moreover, the listen and transmit duty cycles in S-III show a significant increase; the transmit duty cycle reaches 828.98%, compared to 113.84% in S-II, which leads to increased energy consumption. Because of too high retransmissions, S-III's throughput is much higher (87,406.38 bps against 2,643.33 bps in S-II). These findings imply that S-II lowers PDR, but S-III aggravates network congestion, latency, and power consumption, so compromising the long-term sustainability of the network.

Figure 10 explains the implication of malicious node placement. In the SII scenario, the presence of internal malicious nodes led to a decline in PDR, throughput, and latency equated to the SIII scenario, which involved external malicious nodes. This article recommends that future researchers consider the design of IoT networks and the placement of malicious nodes, which greatly affect the performance of the network indicators. A strong trust enabled deep learning mechanism had to be employed to detect, isolate the black hole attacks, which will result in network resilience and energy efficiency.

After the comparison of the results attained using the proposed DLT technique on par with KmeansT. RPL is lacking a trust mechanism; KmeansT is incorporated with a trust evaluation mechanism, but PDR is less when compared with the proposed DLT technique. Existing literature demonstrates a higher PDR ratio. The novelty in the DLT mechanism includes a deep learning technique along with a trust evaluation mechanism, which demonstrated better results than KmeansT (5) in performance measures like PDR, E2E delay, and throughput.

4 Conclusion

This research posits that increasing the number of intruder devices diminishes throughput, reduces the volume of delivered packets, elevates the end-to-end delay ratio, and amplifies power ingesting. The outcomes reveal that blackhole attacks have a major sway on sector performance when they target malevolent nodes. In S-II, with a PDR of 69.23% and an ETX of 19, there are noticeable disruptions. This scenario is unique among others because of two malevolent external nodes. In terms of power, audibility, and transmission, S-II measures 0.413 mW, 0.407 mW, and 0.038 mW, respectively. At present, the recorded throughput is 2643.3 bps, and the latency is 12 seconds, which exhibits excellent performance with malicious nodes. Yet two nodes outside the network range resulted in low performance on par with the earlier scenario. An ETX of 20 results in a

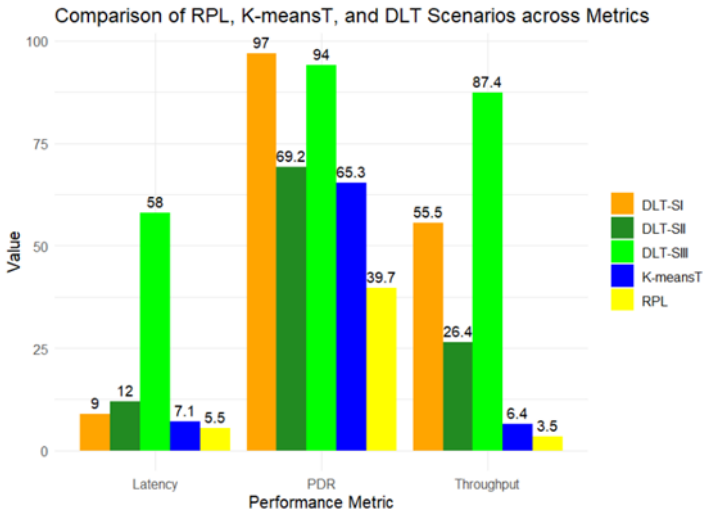

Fig 10. Results comparison of RPL, KmeansT, and DLT

substantial rise to 94.44% for the PDR. The delivery rate is higher since external nodes are unable to directly trash messages. On the other hand, a substantial 58-second lag is present here. The CPU power consumption goes up by 0.425 mW, the listening capacity goes up by 0.562 mW, and the transmission power goes up by 0.283 mW, all because it uses more energy. With a rate of 87,406.38 bps, S-III has a far faster transmission rate. The reason for this is an increase in transmission sent by malicious external nodes.

The article findings show the importance of having robust security systems that can successfully detect and prevent threats from inside the network, thereby assuring both energy efficiency and network stability. Future recommendations and work directions for the researchers are to identify the weak nodes, scale the networks by testing on the larger test beds, and deploy them in the real-time environment to achieve more accuracy.

5 Acknowledgement

The writers herein affirm that they did not accept any form of financial or outside assistance to carry out this study.

References

1) Sadhu PK, Yanambaka VP, Abdelgawad A. Internet of Things: Security and Solutions Survey. *Sensors*. 2022;22(19):7433.
2) Hameed SS, Selamat A, Latiff LA, Razak SA, Krejcar O, Fujita H. A Hybrid Lightweight System for Early Attack Detection in the IoMT Fog. *Sensors*. 2021;21(24):8289. Available from: https://www.mdpi.com/1424-8220/21/24/8289.
3) Rekha S, Thirupathi L, Renikunta S, Gangula R. Study of Security Issues and Solutions in Internet of Things (IoT). *Materials Today: Proceedings*. 2023;80:3554–3559. Available from: https://linkinghub.elsevier.com/retrieve/pii/S2214785321051543.
4) Rao TV, Swamy VK, Karthigeyan KA, Gopalakrishnan S, Kalaichelvi T, Koteswari S. Energy Efficient Trust Based Data Communication Using AODV Protocol in MANET. *ARASET*. 2023;32(1):390–405. Available from: https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/article/view/2688.
5) S M, G L. K-Means Clustering-Based Trust (KmeansT) Evaluation Mechanism for Detecting Blackhole Attacks in IoT Environment. *IJCDS*. 2024;15(1):739–751. Available from: https://journals.uob.edu.bh/handle/123456789/5289.
6) Jia M, Komeily A, Wang Y. Adopting Internet of Things for the Development of Smart Buildings: A Review of Enabling Technologies and Applications. *Automation in Construction*. 2019;101:111–126. Available from: https://linkinghub.elsevier.com/retrieve/pii/S0926580518307064.
7) Alshammari A, Zohdy MA, Debnath D, Corser G. Real Time Vehicular Traffic Simulation for Black Hole Attack in the Greater Detroit Area. *Journal of Information Security*. 2020;11(01):71–80. Available from: https://www.scirp.org/journal/doi.aspx?doi=10.4236/jis.2020.111004.
8) Panda N, Supriya M. Blackhole Attack Prediction in Wireless Sensor Networks Using Support Vector Machine;vol. 992. Springer Nature Singapore. 2023. Available from: https://link.springer.com/10.1007/978-981-19-8865-3_30.
9) Al-Amiedy TA, Anbar M, Belaton B, Kabla AHH, Hasbullah IH, Alashhab ZR. A Systematic Literature Review on Machine and Deep Learning Approaches for Detecting Attacks in RPL-Based 6LoWPAN of Internet of Things. *Sensors*. 2022;22(9):3400. Available from: https://www.mdpi.com/1424-8220/22/9/3400.
10) Srinivasan J. Innovative Cross-Layer Defense Mechanisms for Blackhole and Wormhole Attacks in Wireless Ad-hoc Networks. *Scientific Reports*. 2025;15(1):14747. Available from: https://www.nature.com/articles/s41598-025-97094-0.
11) Rbah Y, Mahfoudi M, Balboul Y, Chetioui K, Fattah M, Mazer S, et al. Hybrid Software Defined Network-Based Deep Learning Framework for Enhancing Internet of Medical Things Cybersecurity. *IJ-AI*. 2024;13(3):3599. Available from: https://ijai.iaescore.com/index.php/IJAI/article/view/24892.

12) Ma YW, Chiu PH. A Novel Risk-Based Access Control Engine in Zero Trust Architecture for IoT Network. *International Journal of Information Security*. 2025;24(3):124. Available from: https://link.springer.com/10.1007/s10207-025-01030-2.
13) Gide AI. A Novel Approach for Addressing IoT Networks Vulnerabilities in Detection and Classification of DoS/DDoS Attacks. *IJSECS*. 2024;10(1):50–59. Available from: https://journal.ump.edu.my/ijsecs/article/view/10453/3390.
14) Ayoub K, Abdelmajid H, Ayoub T, Soukaina M. Enhancing IoT RPL Protocol Security Against Black Hole Attacks with Deep Learning Techniques. *Journal of Computer Science*. 2024. Available from: https://thescipub.com/pdf/jcssp.2024.1530.1544.pdf.
15) Li P, Wang H, Tian G, Fan Z. A Cooperative Intrusion Detection System for the Internet of Things Using Convolutional Neural Networks and Black Hole Optimization. *Sensors*. 2024;24(15):4766. Available from: https://www.mdpi.com/1424-8220/24/15/4766.
16) Khan MA, Rais RNB, Khalid O, Ahmad S. Trust-Based Optimized Reporting for Detection and Prevention of Black Hole Attacks in Low-Power and Lossy Green IoT Networks. *Sensors*. 2024;24(6):1775. Available from: https://www.mdpi.com/1424-8220/24/6/1775.
17) Shahid U, Hussain MZ, Hasan MZ, Haider A, Ali J, Altaf J. Hybrid Intrusion Detection System for RPL IoT Networks Using Machine Learning and Deep Learning. *IEEE Access*. 2024;p. 113099–113112. Available from: https://ieeexplore.ieee.org/document/10634166/.
18) Luangoudom S, Tran D, Nguyen T, Tran HA, Nguyen G, Ha QT. svBLOCK: Mitigating Black Hole Attack in Low-Power and Lossy Networks. *IJSNET*. 2020;32(2):77. Available from: http://www.inderscience.com/link.php?id=104923.
19) Aneja A. Attack Detection in Wireless Sensor Networks Using Novel Artificial Intelligence Algorithm. *2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*. 2023;p. 295–300. Available from: https://ieeexplore.ieee.org/document/10290399/.
20) Rutravigneshwaran P, Anitha G. Security Model to Mitigate Black Hole Attack on Internet of Battlefield Things (IoBT) Using Trust and K-Means Clustering Algorithm. *IJCNA*. 2023;10(1):95. Available from: https://www.ijcna.org/Manuscripts/IJCNA-2023-O-08.pdf.
21) Bang AO, Rao UP, Kaliyar P, Conti M. Assessment of Routing Attacks and Mitigation Techniques with RPL Control Messages: A Survey. *ACM Computing Surveys*. 2023;55(2):1–36. Available from: https://dl.acm.org/doi/10.1145/3494524.
22) Sharma DK, Dhurandher SK, Kumaram S, Gupta KD, Sharma PK. Mitigation of Black Hole Attacks in 6LoWPAN RPL-based Wireless Sensor Network for Cyber Physical Systems. *Computer Communications*. 2022;189:182–192. Available from: https://linkinghub.elsevier.com/retrieve/pii/S0140366422001074.
23) Junejo AK, Komninos N, McCann JA. A Secure Integrated Framework for Fog-Assisted Internet-of-Things Systems. *IEEE Internet of Things Journal*. 2021;8(8):6840–6852. Available from: https://ieeexplore.ieee.org/document/9247121/.
24) Butun I, Osterberg P, Song H. Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *IEEE Communications Surveys & Tutorials*. 2020;22(1):616–644. Available from: https://ieeexplore.ieee.org/document/8897627/.