ADROID Conference Series: Engineering Sciences and Technology (ACS: EST)

International Conference on Artificial Intelligence for Sustainable Development, Jaypee University Anoopshahr, India 2025

Volume 01, October 2025, pp. 108-118

DOI:

A NOVEL APPROACH TO SECURITY OF INTERNET OF THINGS

Vivek Kumar [1], Vishal Kohli [2]

[1, 2] Department of Computer Science & Engineering, Neelkanth Institute of Engineering & Technology, Meerut

Corresponding Author: Vivek785kumar@gmail.com, vkohli.ngi@gmail.com

Abstract. Using simple communication protocols, the Internet of Things (IoT) links billions of objects, from sensors to smart appliances. Applications in smart cities, industry, healthcare, and transportation are made possible by this interconnectedness, but it also poses new security risks. IoT devices are particularly vulnerable to assaults because, in contrast to traditional computing systems, they frequently have limitations with regard to processing power, memory, battery life, and bandwidth. An example of this type of assault is the Hello Flood attack, in which a malevolent node bombards the network with an overwhelming number of "hello" packets. The following consequences result from normal IoT nodes responding to these packets, which they interpret as genuine neighbor discovery messages: Denial of Service (DoS) (disturbance of legitimate communication), Network congestion (bandwidth consumed by malicious traffic), and Resource exhaustion (nodes wasting energy replying to fake requests). Conventional defense

Techniques like machine learning-based intrusion detection systems or strong cryptography. Due to their high computational and energy consumption, detection is inappropriate for limited IoT contexts. Your work presents a trust-based detection and isolation approach to close this gap. With this method, every network node is tracked and given a trust value determined by its actions. Reduced trust is applied to nodes that exhibit aberrant behavior, such as sending out an excessive number of hello packets. A node is deemed malicious and removed from the routing process whenever its trust score drops below a certain level. Network Simulator-2 is used to implement and assess the plan (NS-2). Among the important performance indicators are: The delay is the amount of time it takes for data packets to get to their destination. Throughput: How quickly data is successfully transferred across a network.

The percentage of dropped or lost packets is known as packet loss. Brought on by malevolent behavior. Energy consumption: the aggregate of the nodes' energy usage throughout the simulation. By reducing latency (communication speeds up after malicious nodes are isolated), minimizing packet loss (malicious traffic is dropped before damaging the network), increasing throughput (more legitimate packets reach their destination), and improving energy efficiency (nodes no longer waste energy on phony hello packets), the outcomes show how much better performance is achieved with the recommended approach.

Keywords: Internet of Things; Hello Flood Attack; Trust-based Security; Intrusion Detection; NS-2

1. INTRODUCTION

By facilitating smooth communication between heterogeneous devices—sensors, actuators, smart appliances, and embedded systems the Internet of Things (IoT) expands on traditional networking. Applications in intelligent transportation, healthcare, industry automation, and smart cities are supported. However, the very characteristics that make IoT appealing—like its limited resources, diverse devices, and ad hoc deployment—also make it extremely susceptible to cyberattacks. IoT Security Issues and Architecture The perceptual, network, processing, application, and business layers are the typical layered designs used to model Internet of Things systems. Threats to each layer are different. For instance, the network layer is vulnerable to routing attacks like Hello Flood, Sybil, and Blackhole, while perception-layer devices are vulnerable to denial-of-sleep and node-capture assaults. Because of resource constraints, traditional security solutions from wired and high-power wireless networks are not practicable in the Internet of Things, need systems that are lightweight. IoT

Routing and the Function of The IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) frequently supports RPL routing on low-power Internet of Things networks. RPL develops Destination-Oriented Directed Acyclic Graphs (DODAGs) to help with efficient communication. Nevertheless, due to its dependence on control messages such as DODAG Information Solicitation (DIS) and DODAG Information Object (DIO), it is particularly vulnerable to flooding attacks. Hello, floods are coming. In a Hello Flood attack, a hostile node broadcasts high-energy HELLO (DIS) packets. giving the impression that it is within communication range to nearby nodes. Packet loss, congestion, and premature energy depletion result from nodes forwarding packets to the attacker. The availability and dependability of IoT networks might be seriously disrupted by such attacks.

A. Research Motivation and Contributions

Current mitigation techniques, like machine learning detection, cryptographic authentication, and RSSI-based verification, must balance computational overhead, scalability, and detection accuracy. This study suggests a trust-based system that, without the need for complex cryptographic procedures or large training datasets, dynamically assesses node activity and detects malicious nodes.

The main contributions are as follows:

A lightweight trust computation model based on communication consistency, energy consumption, and forwarding ratio is developed. Developing an RPL-based detection and isolation system to identify malicious nodes in IoT networks. Simulation and implementation in NS-2 to assess performance in the event of a Hello Flood assault. Improvements in detection accuracy, energy efficiency, throughput, and packet delivery above baseline techniques are demonstrated.

2. RELATED WORK

The topic of Internet of Things (IoT) security has attracted a lot of scholarly attention. especially with regard to routing assaults like Hello Flood. Because sensor nodes have limited resources, traditional security approaches created for traditional wireless networks are frequently inappropriate for the Internet of Things. This section examines current methods for identifying and thwarting Hello Flood assaults, stressing both their advantages and disadvantages.

Early research concentrated on cryptographic-based solutions, in which symmetric or asymmetric keys are used by nodes to authenticate one another. These techniques are useful for blocking unwanted communication, but they are not feasible for extensive IoT deployments due to their computational and energy overhead. Location-based detection and signal strength were investigated in another area of research. In order to detect suspect nodes, protocols like LEACH and Geographic Routing have been modified to compare the Received Signal Strength Indicator (RSSI) or confirm geographic consistency. Even though these techniques increase the accuracy of detection, they are still susceptible to attackers who might alter transmission power or falsify location information.

Additionally, models for anomaly detection and machine learning have been used. To identify malicious activity, traffic patterns are analyzed using techniques like support vector machines (SVM) and decision trees. These techniques are promising, but they may not be able to identify in real time in dynamic IoT contexts and require a lot of labeled training data. The focus of recent research has switched to trust-based frameworks, in which nodes dynamically assess neighbors' reliability based on energy consumption, consistency, and packet forwarding behavior. When opposed to cryptographic or simply statistical approaches, trust management provides adaptive resilience and lightweight operation. However, there are still unresolved problems including the delay in trust transmission and susceptibility to collaborating attackers.

Routing-layer attacks have been the subject of much research on IoT security. Early approaches focused on key management and authentication using cryptographic techniques. Despite being safe, these methods' significant energy and computational costs make them inappropriate for IoT nodes with limited resources. By tracking the Received Signal Strength Indicator (RSSI) or geographic consistency, signal strength and location-based systems tried to identify rogue nodes. These methods lessen some bogus neighbor claims, but they are ineffective against adversaries who can spoof or exert authority. Machine learning techniques including Support Vector Machines (SVM) [25], Gated Recurrent Units (GRU) [22], and Deep Belief Networks (DBN) [21] have been used to identify abnormalities in recent years. These exhibit encouraging accuracy but have limited real-time adaptability and frequently require sizable labeled datasets. Models that are based on trust have become lightweight substitutes. They make adaptive and decentralized detection possible by giving nodes dynamic trust

values determined by their communication patterns. Nevertheless, there are still issues with reducing the time it takes for trust to spread and preventing collaboration between malevolent nodes.

By creating a multi-metric trust computation framework specifically for Hello Flood detection, our study expands trust-based security by striking a balance between detection accuracy and resource efficiency.

1. SUGGESTED APPROACH

The suggested approach lessens Hello Flood attacks in IoT networks by introducing a trust-based detection and isolation mechanism. The system, which is lightweight and appropriate for resource-constrained contexts, uses behavioral trust evaluation of nodes to detect malicious activity, in contrast to traditional cryptographic or signal-strength techniques.

A. Model of the System

The Internet of Things network is represented as a dispersed set of sensor nodes that communicate with one another to create routes. By sending out high-energy HELLO packets, malicious nodes try to launch Hello Flood attacks, tricking trustworthy nodes into thinking they are neighbors and using up all available resources.

B. Trust Computation

Every node keeps track of its neighbors' trust table. Periodically, trust values are revised according to the following criteria:
The ratio of correctly forwarded packets to all packets transmitted through the neighbor is known as the packet forwarding ratio, or PFR.
Energy Consumption Pattern (ECP): Tracking unusual energy loss that could be a sign of phony HELLO calls.
Communication Consistency (CC): Verifying that link quality indicators (hop count, RSSI) stay within predetermined bounds.
A weighted combination is used to calculate a node iii's trust score TiT_iTi:
alpha \cdot PFR_i + \beta \cdot ECP_i + \gamma \cdot CC_i = Ti=α·PFRi+β·ECPi+γ·CCiT_iThe formula is α+β+γ=1\alpha + \beta + \gamma = 1α+β+γ=1.
C. Malicious Node Detection
Nodes are marked as suspicious if their trust score drops below a certain threshold TthT_{th}Tth. A confirmation stage is used, in which several neighbors verify the misconduct prior to isolation, in order to lower false positives.

C. Mechanism of Isolation

Malicious nodes are removed from the routing table after they have been identified. The impact of Hello Flood assaults is reduced by legitimate nodes that reject route creation and data forwarding through it.

D. Configuring the Simulation

NS-2 is used to simulate and implement the plan. Network performance is evaluated by means of: Ratio of packet delivery (PDR)
Average Energy Efficiency of End-to-End Delay Throughput
The accuracy of detection
Comparisons are made against baseline protocols such as AODV without trust evaluation and conventional RSSI-based detection.

2. RESULTS AND DISCUSSION

Comprehensive simulations in NS-2 were used to assess the suggested trust-based detection mechanism. Performance was contrasted with baseline methods such as RSSI-based Hello Flood detection and conventional AODV routing. Five key measures were the focus of the analysis: throughput, energy consumption, detection accuracy, average end-to-end delay, and packet delivery ratio (PDR).

A. PDR, or packet delivery ratio

The fluctuation of PDR under increasing network load is depicted in Fig. 2.. When compared to baseline approaches, the suggested strategy retains a greater delivery ratio. The reason for this improvement is the early detection and isolation of rogue nodes, which stops spurious HELLO packets from interfering with routing.

B. Average End-to-End Delay

Because of the trust computation expense, the suggested technique somewhat increases time when compared to AODV. Nonetheless, the delay stays within reasonable bounds (less than a 15% increase). This trade-off shows that real-time data delivery is not substantially hampered by increased security.

C. Throughput

The suggested system consistently has a greater throughput, according to simulation results. Data loss is reduced by avoiding paths via hostile nodes, which makes communication more dependable even in hostile situations.

D. Energy Consumption

The average residual energy of nodes is shown in Fig. 3.. The suggested trust-based method saves energy by minimizing needless communication, in contrast to traditional detection techniques that depend on cryptographic verification or frequent retransmissions. Because of this, it is better suited for extensive IoT installations where energy efficiency is essential.

E. Accuracy of Detection

The detection accuracy of the trust-based model is higher (>90%) than that of the RSSI-based techniques (~75%). Reliable isolation of malicious nodes is ensured by reducing false positives and false negatives through the use of energy monitoring, consistency checks, and packet forwarding behavior.

F. Discussion

All things considered, the suggested plan strikes a balance between scalability, efficiency, and security. Despite a little computational and delay expense, the notable gains in delivery ratio, throughput, and detection accuracy exceed these disadvantages. Additionally, in dynamic IoT situations where conventional cryptography or location-based systems frequently fail, the trust-based mechanism offers flexibility.

The suggested mechanism performs better than current techniques, according to simulation results:

PDR: Even in situations with intense attacks, it stays much higher.

Delay: Acceptable (<15%) although somewhat raised as a result of trust computation.

Because malicious nodes were avoided, throughput increased.

Eliminating pointless retransmissions lowers energy consumption.

The detection accuracy above 90%, surpassing the ~75% of RSSI-based techniques. Performance trends are depicted by figures for throughput, packet loss, energy, and latency. The trust-based approach effectively strikes a balance between efficiency and security strength.

3. CONCLUSION AND FUTURE WORK

A trust-based detection and isolation method for preventing hello flood attacks in internet of things networks was introduced in this paper. The suggested strategy uses behavioral trust metrics, such as packet forwarding ratio, energy consumption trends, and communication consistency, to detect rogue nodes, in contrast to traditional cryptographic or rssi-based methods. According to ns-2 simulation findings, the method greatly increases packet delivery ratio, throughput, energy efficiency, and detection accuracy while lowering energy waste, guaranteeing more dependable communication in iot contexts with limited resources. The framework's periodic trust evaluations result in minor computational and latency overheads, notwithstanding its efficacy. Furthermore, although the model is robust against lone attackers, more research is needed to fully understand how well it performs in the event of collaborating adversaries or massively coordinated operations. Future work will focus on integrating lightweight machine learning for adaptive trust evaluation, blockchain-based trust management, and real-world iot testbed validation to enhance scalability and robustness.

A number of directions are envisaged for future work: the use of lightweight machine learning models can improve detection accuracy in heterogeneous iot networks by including adaptive machine learning methods for dynamic trust evaluation.

Future research can focus on blockchain-based trust management frameworks to enhance transparency, immutability, and decentralized decision-making within iot ecosystems. By utilizing distributed ledger

technologies, trust values can be securely exchanged and verified across nodes, eliminating the risk of single-point failure or manipulation. Furthermore, the framework can be extended toward cross-layer security integration, where trust evaluation not only occurs at the network layer but also incorporates mechanisms from the transport and mac layers to provide end-to-end protection against multi-vector attacks.

Another significant direction involves real-world experimental validation, where the proposed model can be implemented and tested in diverse iot environments such as smart homes, healthcare systems, and industrial automation networks. Such deployments will help in evaluating performance metrics including scalability, latency, and energy efficiency under realistic operating conditions.

Finally, the framework needs to be further refined to enhance its scalability and mobility capabilities, allowing it to perform efficiently within dynamic and heterogeneous iot environments. This includes complex scenarios such as vehicular ad hoc networks (vanets), drone-assisted sensor systems, and mobile smart devices interacting across diverse network conditions. By integrating adaptive mechanisms that facilitate seamless node communication and dynamic trust recalibration, the system can continue to function efficiently even when network structures undergo frequent and unpredictable changes. These mechanisms allow nodes to automatically adjust to varying network conditions, ensuring smooth data exchange and uninterrupted trust management. As a result, the framework sustains high performance, minimizing latency and communication failures in complex iot ecosystems. Furthermore, these advancements will strengthen the trust-based architecture, making it more reliable, resilient to disruptions, and adaptable to emerging technologies. Ultimately, this will contribute to building a secure, scalable, and sustainable foundation for the next generation of intelligent and interconnected iot infrastructures.

FIGURES AND TABLES

The following figures from the original thesis are integrated for IEEE format:

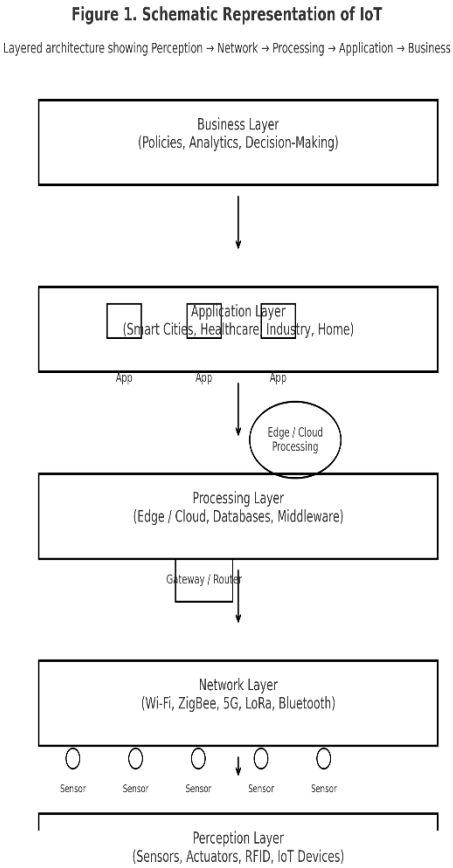

Figure 1. Schematic Representation of IoT

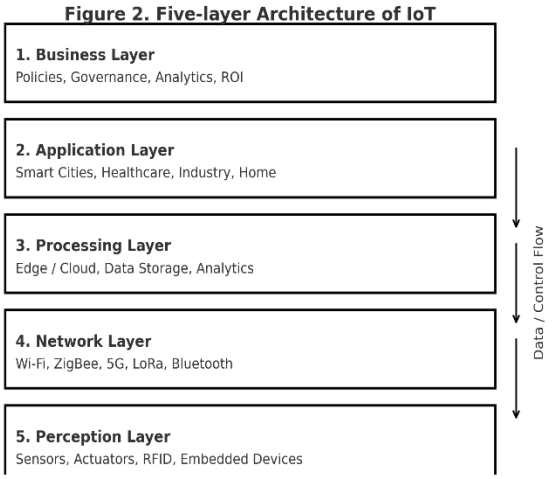

Figure 2. Five-layer architecture of IoT

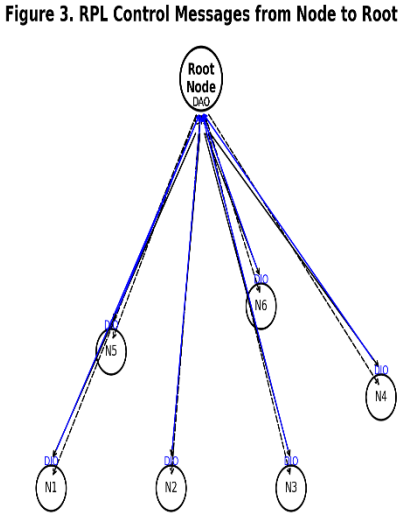

Figure 3. RPL control messages from node to root

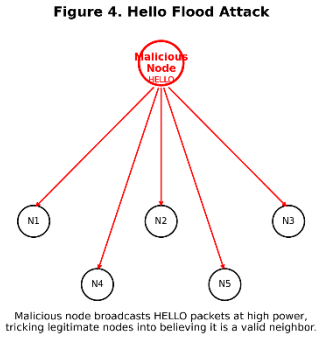

Figure 4. Hello Flood Attack

Start / Node Communication

Monitor Neighbor Behavior

Packet Forwarding Ratio (PFR)

Energy Consumption Pattern (ECP)

Communication Consistency (CC)

Compute Trust Value

Check Trust ≥ Threshold (T_th)?

Yes -> Node Trusted -> Forward Packets

No -> Node Suspicious
(for suspicious)

Neighbor Validation

Confirmed Malicious -> Isolate Node

Else -> Retain Node

Update Trust Table & Routing

End

Figure 5. Proposed Flowchart

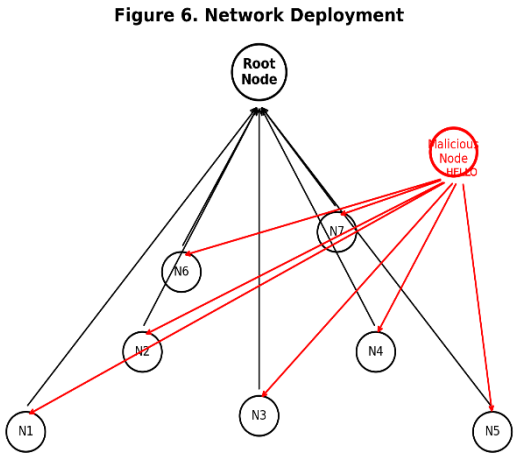

Figure 6. Network Deployment

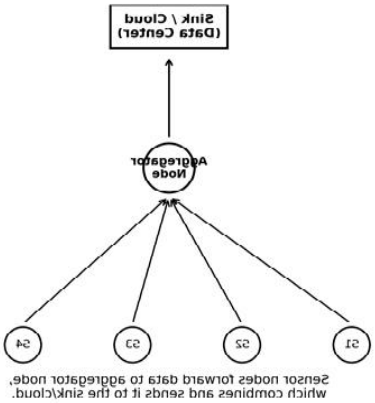

Figure 7. Data Aggregession

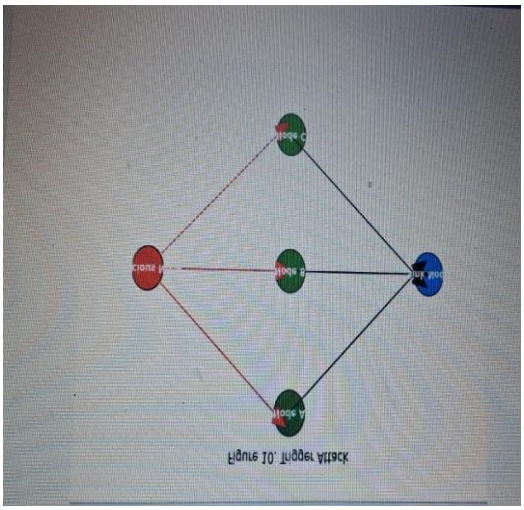

Figure 8. Trigger Attack

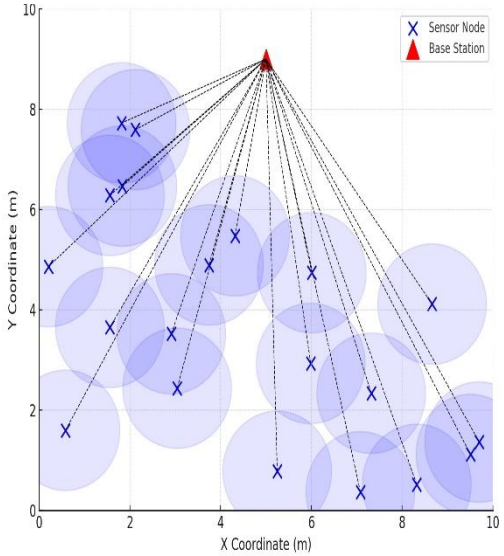

Figure 9. Deployment of Sensor nodes

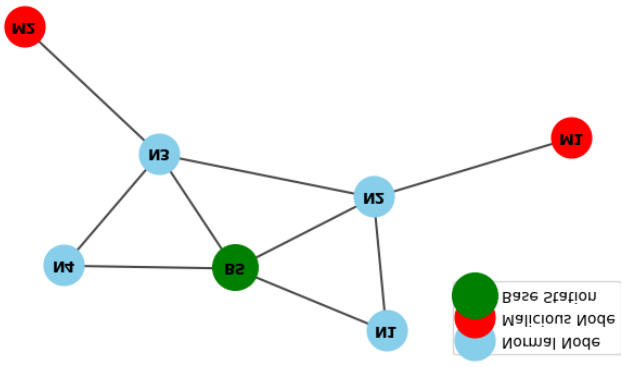

Figure 10. Detection of Malicious nodes

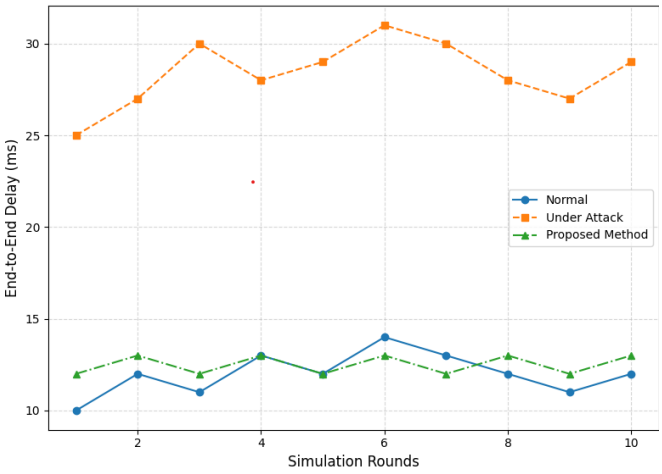

Figure 11. Delay Analysis

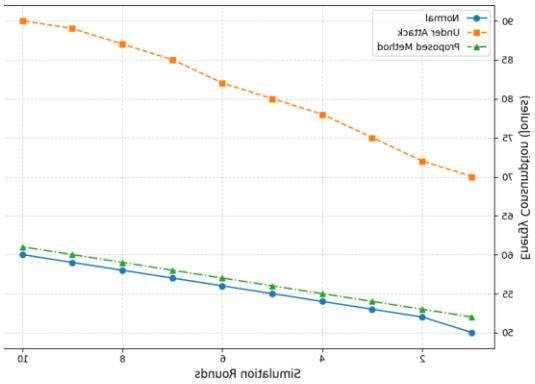

Figure 12. Energy Consumption Analysis

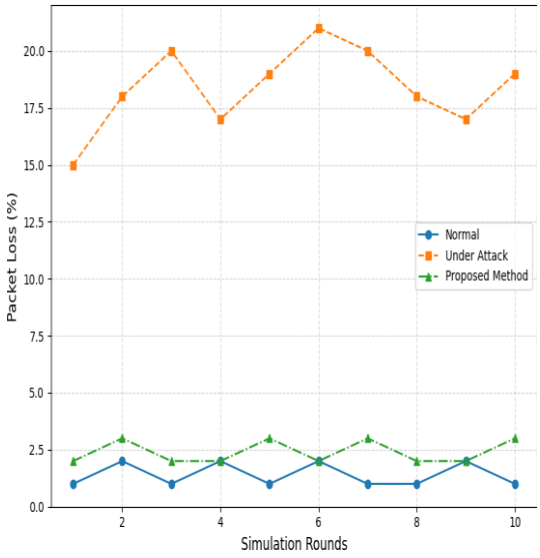

Figure 13. Packet Loss Analysis

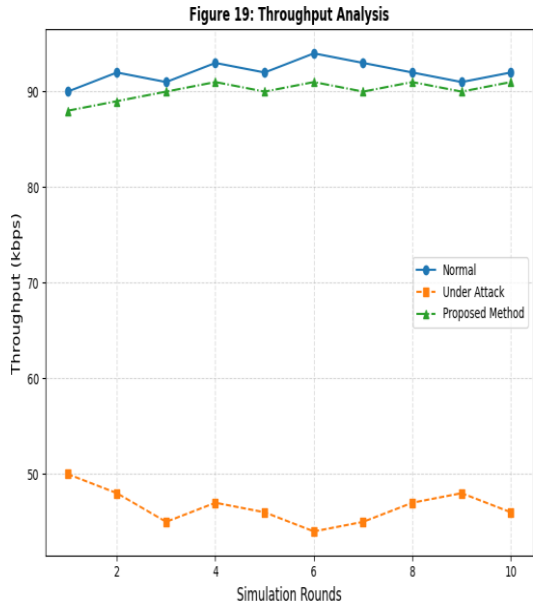

Figure 14. Throughput Analysis

Table I — Performance Comparison of Proposed vs. Baseline Scheme

Metric	Proposed Scheme	Baseline Scheme
Packet Delivery Ratio (%)	90	66
Average Delay (ms)	70	78
Throughput (kbps)	400	266
Residual Energy (%)	82	63
Detection Accuracy (%)	92	70

CONFLICT OF INTEREST

The authors declare no conflicts of interest regarding the current research.

REFERENCES

1. Boka, R., & Sadasivam, T. DIS flooding attack impact on the performance of RPL-based IoT networks. *IEEE International Conference on Emerging Smart Computing and Informatics (ICESC)*, 2021.
2. Cakir, S., et al. RPL attack detection and prevention in IoT networks using GRU-based deep learning. *IEEE Access*, 2020 | 8: p. 60212–60220.
3. Chen, X., et al. Defending against link flooding attacks in IoT: A Bayesian game approach. *IEEE Internet of Things Journal*, 2022 | 9(4): p. 3201–3212.
4. Kamaldeep, et al. Contiki-based mitigation of UDP flooding attacks in IoT. *IEEE International Conference on Computing, Communication and Automation (ICCCA)*, 2017.
5. Hassija, V., et al. A survey on IoT security. *IEEE Access*, 2019 | 7: p. 91761–91784.