

Performance Evaluation of Mobile RPL-Based IoT Networks under Sinkhole Attacks

Md. Ataullah * and Naveen Chauhan

Department of Computer Science and Engineering, National Institute of Technology Hamirpur, Hamirpur, Himachal Pradesh, 177005, India; naveen@nith.ac.in.

* Correspondence author: mdataullah.khan@gmail.com

Abstract: The rapid expansion of Internet of Things (IoT) deployments has increased reliance on Low-power and Lossy Networks (LLNs), where the Routing Protocol for LLNs (RPL) is widely adopted. However, RPL networks are vulnerable to sinkhole attacks that manipulate routing information to disrupt communication. This study evaluates the performance of mobile RPL-based IoT networks under such attacks, considering both mobility and attacker presence. Key metrics, including packet delivery ratio, inter-packet time, power consumption, and isolated nodes, are analyzed using Cooja simulations. Results indicate that mobility intensifies attack impact, causing instability and performance degradation, emphasizing the need for mobility-aware security mechanisms.

Keywords: 6LoWPAN, IPv6, IoT security, RPL, Sinkhole attack.

1. Introduction

The Internet of Things (IoT) has enabled large-scale interconnection of resource-constrained devices across diverse application domains such as smart environments, industrial automation, and healthcare. These systems commonly rely on Low-power and Lossy Networks (LLNs), where efficient and lightweight routing is essential. The Routing Protocol for LLNs (RPL), standardized by the Internet Engineering Task Force (IETF) (RFC 6550), has emerged as a widely adopted routing solution for such environments due to its adaptability and energy efficiency [1,2].

Despite its advantages, RPL is susceptible to several security threats arising from its distributed and resource-constrained nature. Among these, the sinkhole attack is particularly critical, as malicious nodes can manipulate routing metrics to attract network traffic, leading to packet loss, data interception, and network disruption [3].

Most existing studies on RPL security primarily focus on static network scenarios, whereas real-world IoT deployments often involve node mobility and dynamic topologies. Mobility introduces additional challenges, including frequent topology changes, unstable routing paths, and increased vulnerability to attacks. However, the combined impact of mobility and sinkhole attacks has not been sufficiently explored.

Although previous studies have investigated the impact of routing attacks in mobile RPL networks, they differ from the present work in terms of both the attack type and network scenarios considered. Hkiri et al. [4] evaluated the effects of decreased-rank attacks, whereas Sharma et al. [5] focused on version number attacks. In contrast, this study examines the impact of sinkhole attacks on mobile RPL-based IoT networks. Furthermore, while Sharma et al. [5] considered two network scenarios, namely a fully static network and a hybrid network comprising both static and mobile nodes, this work extends the analysis by incorporating an additional fully mobile network scenario in which all nodes are mobile. This enables a more comprehensive assessment of sinkhole attack effects under varying mobility conditions.

The evaluation presented in this study is based on simulations conducted in the Cooja [6] environment using Contiki OS [7]. A simulation-based approach was adopted because the objective is to analyze the impact of sinkhole attacks on mobile RPL-based IoT networks under controlled mobility and attacker-density conditions. Such controlled experimentation enables systematic assessment of network-level

metrics, including Packet Delivery Ratio (PDR), Inter-Packet Time (IPT), power consumption, and the number of isolated nodes. By examining static, hybrid, and fully mobile scenarios, this work aims to provide a comprehensive understanding of how mobility influences network resilience against routing attacks.

The outcomes of this study offer valuable insights into the design of secure and efficient IoT routing mechanisms, particularly in dynamic environments where mobility cannot be ignored. The acronyms used in this study can be found in the Table 1.

Table 1. Acronyms employed in the document.

Acronyms	Meaning
6LoWPAN	IPv6 over Low-power Wireless Personal Area Networks
CBOR	Concise Binary Object Representation
CCRL	Compressed Certificate Revocation List
CNN	Convolutional Neural Network
CoAP	Constrained Application Protocol
DAG	Directed Acyclic Graph
DAO	Destination Advertisement Object
DAO-ACK	Destination Advertisement Object Acknowledgment
DDAO	Dropped Destination Advertisement Object
DDoS	Distributed Denial-of-Service
DIO	DODAG Information Object
DIS	DODAG Information Solicitation
DODAG	Destination-Oriented Directed Acyclic Graph
DoS	Denial of Service
DNM	Detection based on Node pruning and Model fusion
DTF	Dynamic Trust Factor
HMM	Hidden Markov Model
ICMPv6	Internet Control Message Protocol version 6
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IoT	Internet of Things
IPT	Inter-Packet Time
IPv6	Internet Protocol version 6
LLNs	Low-power and Lossy Networks
LSTM	Long Short-Term Memory
NDNoT	Named Data Networking of Things
OCSP	Online Certificate Status Protocol
OF	Objective Function
PDR	Packet Delivery Ratio
PSCM	Prime Sequence Code Matrix
QoS	Quality of Service
RAD	Rank Attack Detection
RPL	Routing Protocol for Low-power and Lossy Networks
SECaaS	Security-as-a-Service
UDGM	Unit Disk Graph Medium
UDP	User Datagram Protocol

Contributions

The main contributions of this study are summarized as follows:

- A comprehensive performance evaluation of RPL-based IoT networks under sinkhole attack scenarios, explicitly incorporating node mobility.
- Comparative analysis across static, hybrid, and fully mobile network configurations to understand the combined effects of mobility and attacks.
- Quantitative assessment using key performance metrics, including PDR, IPT, power consumption, and number of isolated nodes.
- An extensive simulation study using the Contiki Cooja environment with up to 50 nodes and

varying attacker densities, providing realistic insights into network behavior.

- Identification of mobility as a critical factor that significantly influences attack impact, highlighting the need for mobility-aware security solutions in RPL-based IoT systems.

The structure of the paper is outlined in the following sections. Section 2 provides a background of pertinent research, offering insights into the scope of this study. Section 3 describes the related work of this study. In Section 4, the paper explores performance metrics and evaluation parameters. Section 5 presents the result analysis in terms of number of isolated nodes, PDR, IPT and power consumption. Section 6 discusses implementation overhead, limitation and outlines directions for future research. Lastly, Section 7 presents the final observations.

2. Background

In recent years, the widespread increase in IoT devices has resulted in the development of various communication protocols customized to the limitations and requirements of these devices. The RPL stands out as one of the most prominent protocols designed specifically for IoT applications. This chapter offers a detailed examination of the RPL protocol and sinkhole attack.

2.1. Overview of RPL Protocol

RPL refers to an IPv6 routing protocol defined by the IETF for IoT systems with constrained resources [8]. RPL forms the network nodes in the form of a Destination-Oriented Directed Acyclic Graph (DODAG). This kind of topology uses an Objective Function (OF) and routing metrics, which include the hop count, ETX, or energy levels, to facilitate route selection. The rank value for each node specifies its position within the DODAG, thus avoiding any routing loop. The DIO, DIS, and DAO are the control messages used for forming connectivity in the network. Since RPL uses routing information from neighboring nodes, it becomes susceptible to routing attacks such as sinkholes.

RPL is created specifically for constrained environments like IoT networks, where devices operate with constrained energy resources, memory, and processing capabilities [9]. RPL enables efficient routing in such networks by providing a lightweight, energy-efficient, and adaptable routing solution [10]. Figure 1 illustrates the integration of RPL, an algorithm that utilizes distance vector routing, coupled with the 6LoWPAN adaptation layer.

RPL uses OF to identify the optimal route for packet transmission within the network. The OF evaluates various metrics such as energy consumption, latency, and link quality to select the most suitable route [11]. RPL supports both proactive and reactive routing strategies, allowing nodes to maintain a dynamic routing topology while conserving energy. It organizes nodes into a Directed Acyclic Graph (DAG), with nodes acting as routers and maintaining parent-child relationships to efficiently forward packets [12].

The fundamental structure in RPL is the DODAG, which depicts the routing topology of the network as shown in Figure 2. It is rooted at a designated destination node and expands outward when nodes connect to the network [13]. The DODAG evolves dynamically as a reaction to alterations in network conditions. An RPL instance is a logical partition within a network, identified by a unique Instance ID. Each instance operates independently, allowing multiple RPL instances to coexist within the same network infrastructure. Nodes in the RPL network use DAO messages to inform their parent nodes in the DODAG about their presence and capabilities. DAO messages provide details about a node's rank, its preferred parent, and supported data traffic. When a DAO message is received, the parent node responds to it with an acknowledgement, confirming the establishment of the parent-child relationship. DAO acknowledgements serve as a mechanism for maintaining route stability and reliability.

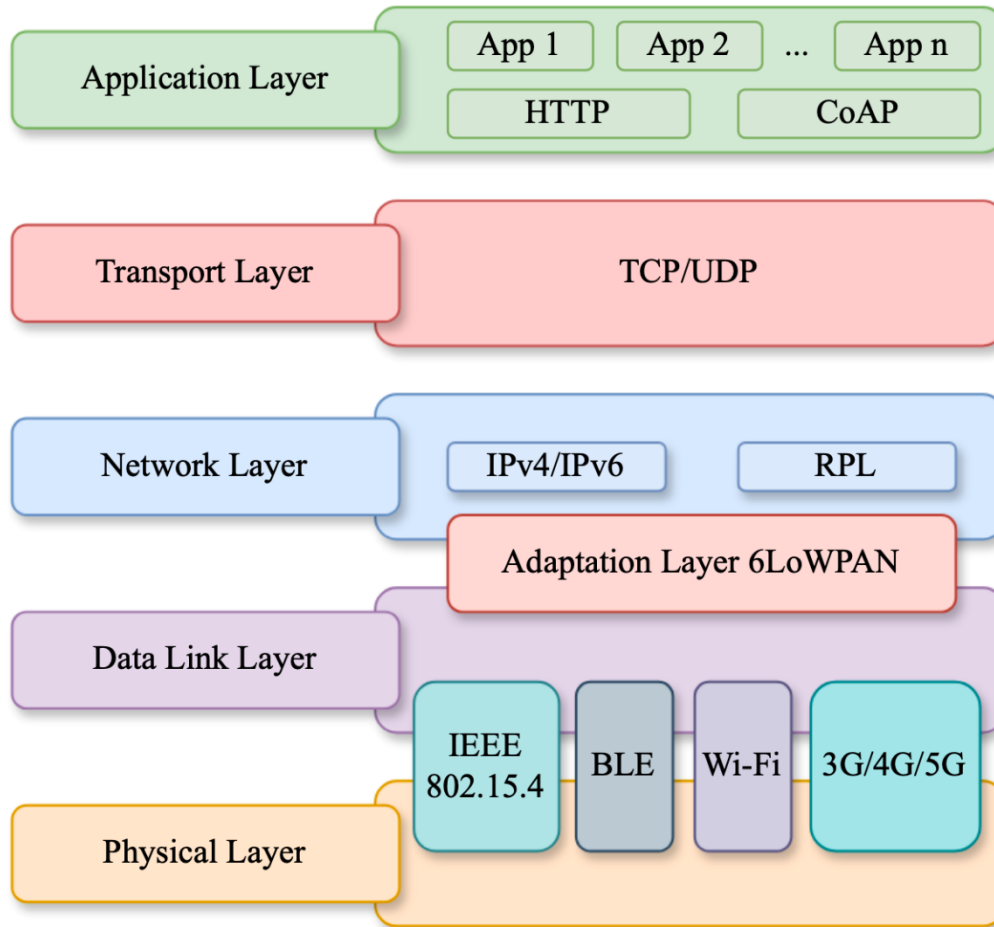


Figure 1. Architecture of IoT Network with Adaptation Layer.

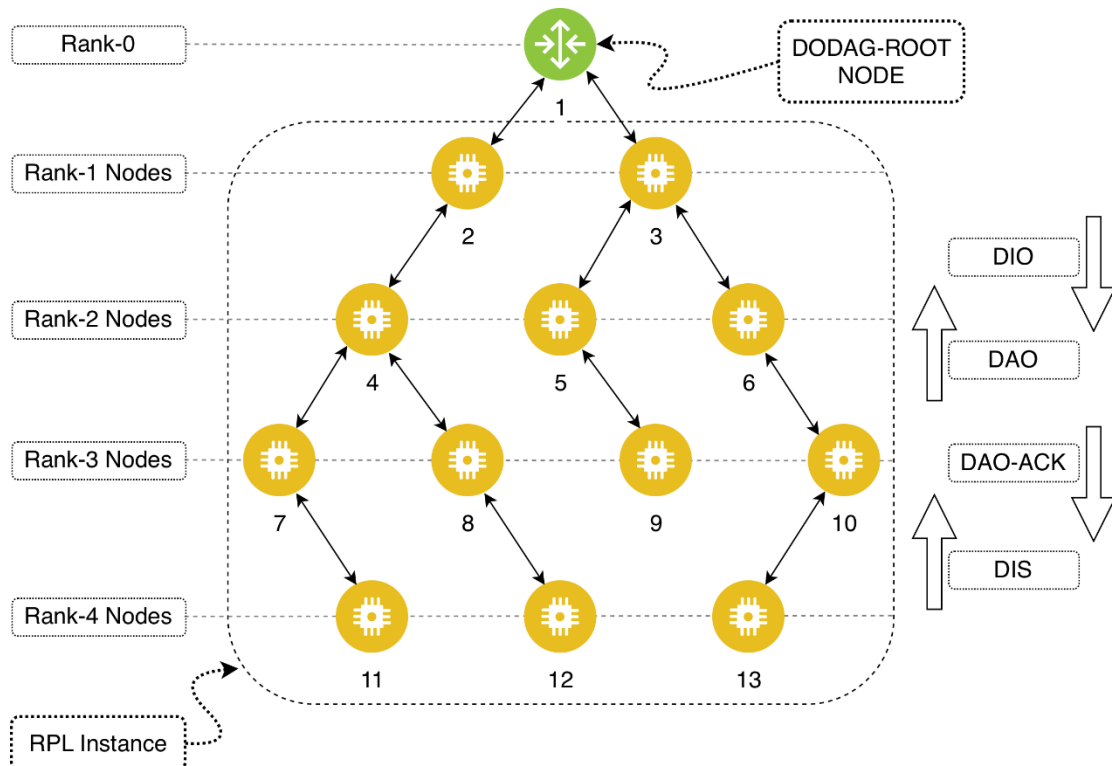


Figure 2. A single-instance RPL network with a single DODAG.

RPL constructs the DODAG in a bottom-up manner, starting from the root node and expanding outward as nodes join the network [14]. Every node chooses its parent according to the OF to reduce energy usage and packet loss. Nodes in the DODAG are assigned ranks based on their position relative to the root node. Ranks determine the order in which nodes forward packets and influence the path selection process. RPL constantly observes the network topology and modifies the routing paths as needed in response to changes such as node failures, mobility, or environmental conditions. Route maintenance mechanisms maintain the robustness and adaptability of the routing infrastructure. In the realm of IPv6-based networks, the RPL introduces a set of ICMPv6 control messages tailored to its operation within LLNs. These messages serve crucial roles in managing and maintaining the routing topology, ensuring efficient communication in resource-constrained environments. Below, we explore the key ICMPv6 control messages associated with RPL:

- **DIS:** A node that wants to join the DODAG sends out DIS messages [2]. When a node desires to join a DODAG but lacks information about potential parent nodes or the DODAG's configuration, it broadcasts a DIS message. Upon receiving a DIS, suitable DODAG parents respond with a DIO.
- **DIO:** This type of message carries crucial details regarding the DODAG, including its configuration parameters, such as OF, DODAGID, and various metrics. Upon receiving a DIS or as part of periodic DIO transmissions, DIO messages are disseminated by DODAG parents to provide comprehensive routing information to neighbouring nodes. This enables nodes to make informed decisions about joining or optimizing their participation in the DODAG.
- **DAO:** Nodes use DAO messages to communicate their accessibility and the resources they have available to upstream nodes in the DODAG. When a node intends to send data to destinations outside the DODAG, it sends DAO messages towards the root of the DODAG. These messages inform upstream nodes about the node's presence and resource availability, enabling efficient routing path establishment.
- **DAO-ACK:** This type of message serves as acknowledgements for received DAO messages, confirming successful DAO propagation. When a DAO message is received, intermediate and root nodes generate DAO-ACK messages to acknowledge successful receipt and deal with the DAO. DAO-ACK messages help ensure reliability in DAO message delivery.

2.2. Sinkhole Attack

In the context of the RPL, a sinkhole attack represents a significant security threat. This attack diverts data flow directed towards an attacking node, known as the sinkhole, instead of the intended destination [15]. The sinkhole node, appearing legitimate, deceitfully asserts itself as having the fastest or most dependable route to a specific destination. This manipulation can occur through a decreased rank attack, wherein the attacking node deliberately reduces its rank to entice neighbouring nodes into selecting it as their preferred parent. Once traffic is rerouted to the sinkhole node, the attacker can intercept, manipulate, or launch further attacks on the communication. This may result in unauthorized entry, data leaks, or interference with essential network operations. Sinkhole attacks target the security gaps in routing protocols to compromise network operations or compromise nodes to gain control over the network's routing information. The attacker may falsify routing messages or utilize compromised genuine nodes to propagate false routing updates, tricking other nodes into routing traffic through the sinkhole. So, in short, it intercepts all signals from a wireless network and reroutes some information. Consequently, if a packet is intercepted, the intended recipient does not receive the message [16].

This paper implements sinkhole attacks using a combination of decreased rank and blackhole attacks. Blackhole attacks typically involve the malicious node intentionally dropping all packets it is meant to forward, effectively disrupting communication similar to a DoS attack. Blackhole attacks are classified as topology attacks as shown in Figure 3, which aim to disrupt the network's topology-building processes. This interruption may result in the isolation of one or more nodes within the network. The Sinkhole attack model illustrated in Figure 4 is implemented according to Algorithm 1.

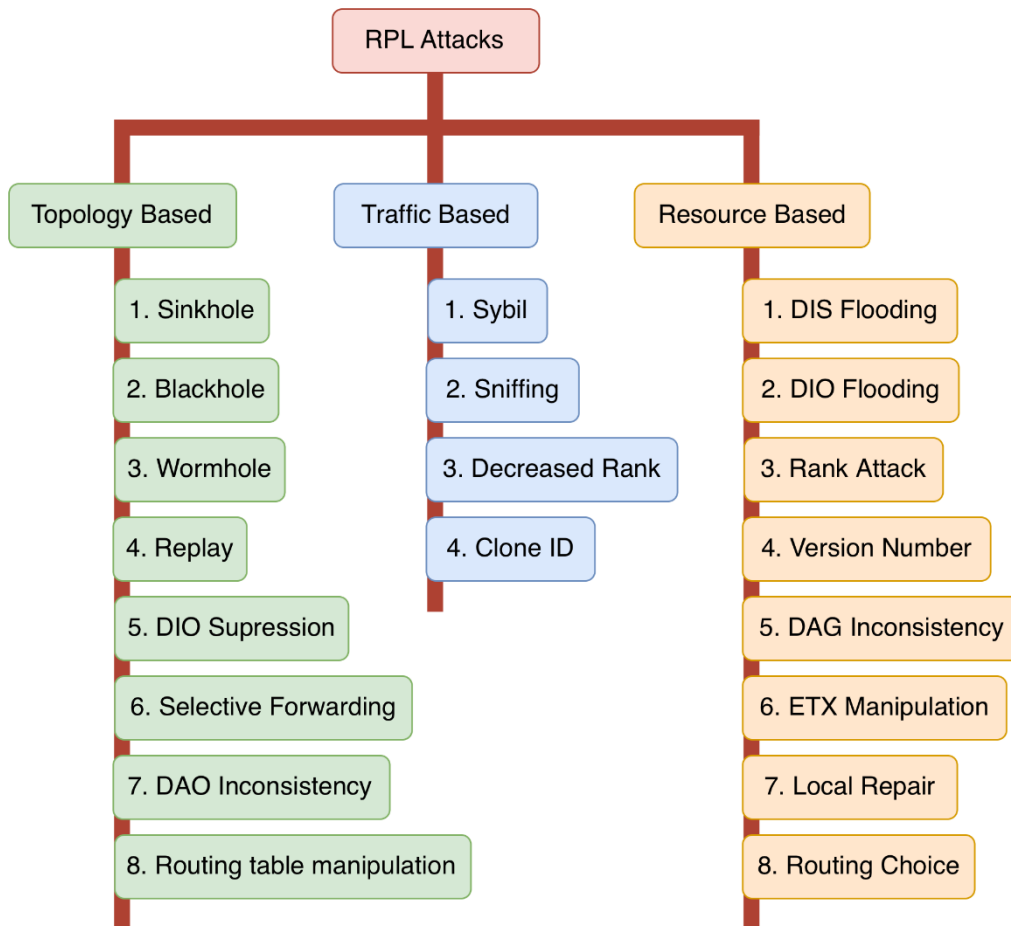


Figure 3. Attacks targeting RPL in 6LoWPAN.

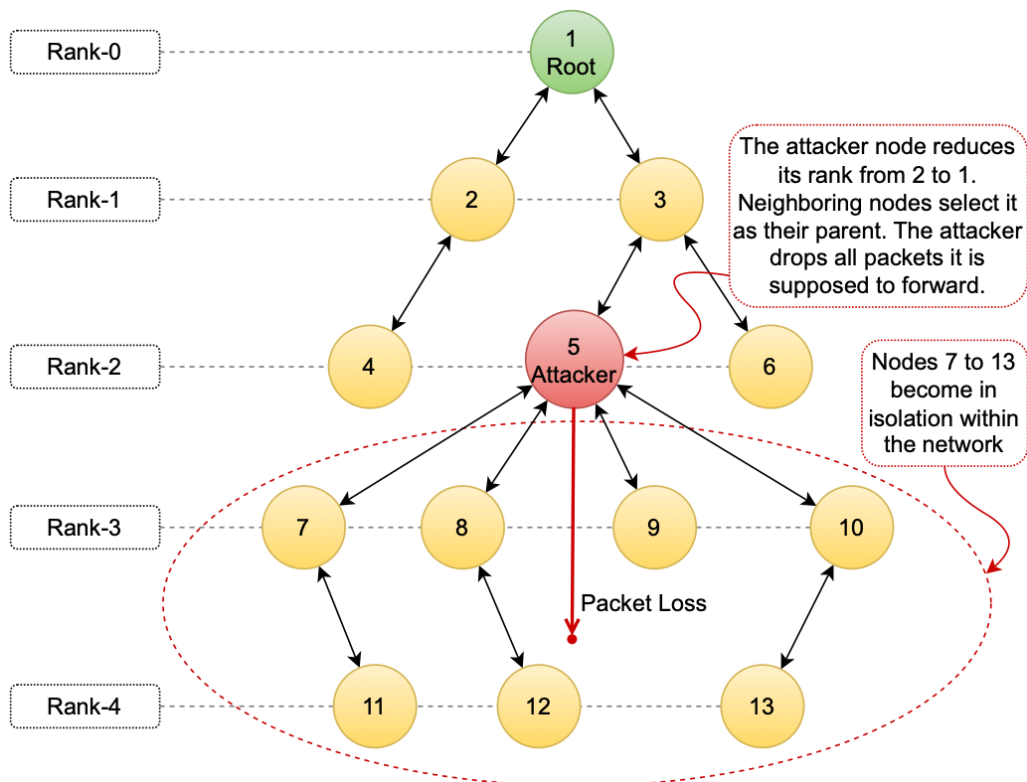


Figure 4. Sinkhole attack through the combination of Decreased rank and Blackhole attacks.

Algorithm 1 Sinkhole Attack in RPL-based IoT Network**Require:** RPL network with nodes N , DODAG root R **Ensure:** Compromised network with disrupted routing

```

1: Select node  $S$  as the sinkhole node
▷ Rank Decrease Attack

2: Compute modified rank  $r'_S \leftarrow$  a significantly lower value than the legitimate rank  $r_S$ 
3: Advertise  $r'_S$  in DIO messages to neighbouring nodes of  $S$ 
▷ Blackhole Behaviour

4: Neighbouring nodes select  $S$  as their preferred parent
5: for each incoming packet  $p$  at node  $S$  do
6:   if  $p$  should be dropped then
7:     Drop  $p$ 
8:   else
9:     Forward  $p$  to the next hop
10:  end if
11: end for
▷ Attack Maintenance

12: while attack is active do
13:   Periodically re-advertise  $r'_S$  to maintain attractiveness
14:   Continue intercepting and dropping packets
15: end while

```

3. Related Work

In this section, we explore the latest studies investigating the effects and analyses of attacks in RPL-based IoT networks. An overview of research efforts focusing on RPL-based IoT networks across different attack situations is summarized in Table 2.

Yilmaz et al. [17] proposed a FL-based approach to enhance intrusion detection in RPL networks. Their study highlights how FL's decentralized model training mitigates the impact of attacker positions on IDS performance by ensuring data collection from nodes irrespective of their distance from potential attackers. Belkheir et al. [18] proposed a novel lightweight approach to mitigate blackhole attacks using collaborative packet-based detection mechanisms. Their method enhances network security by leveraging cooperative detection among nodes, effectively identifying and isolating malicious activities while maintaining low overhead. Parizi et al. [19] proposed the TARRP to enhance the reliability of IPv6 routing in LLNs. Their approach consists of two stages: first, establishing a trustworthy network topology, and second, evaluating trust levels to detect and mitigate malicious nodes. This method improves network security and resilience against attacks. Sharma et al. [20] proposed a Federated Learning (FL)-based IDS for IoT networks, where multiple clients are grouped into sets of varying sizes for training. They employed a feature ranking technique using a random forest algorithm to optimize and reduce the dataset, minimizing inference time. Each client trained three models on the refined dataset, and a central server aggregated the results using three different methods. Alsukayti et al. [21] proposed a novel variant of the Version Number (VN) attack, termed the Decreased VN (DVN) attack, which manipulates DIO messages by lowering the propagated VN value. Their experimental analysis demonstrated that the DVN attack leads to significant subnet partitioning and topological re-establishment, resulting in over 300% increase in network overhead and more than 220% rise in energy consumption. To counter this, they introduced a lightweight mitigation approach called DVN-Secure RPL (DVN-SRPL), which relies on a simple, distributed security mechanism requiring minimal changes to the RPL protocol.

Table 2: Overview of RPL-based IoT security mechanisms under different attacks.

Ref.	Year	Mechanism	Description	Mobility	Limitations
[22]	2026	ML-based adaptive routing	Detects sinkhole and blackhole.	Yes	Training overhead
[23]	2026	TH-DCNN + optimization	DL-based attack detection with clustering.	Yes	High computation
[24]	2026	MDNN + optimization	Detects HELLO flood attacks using DL.	Yes	High complexity
[17]	2025	FL-based IDS	Improves intrusion detection in RPL.	No	High overhead
[18]	2025	Collaborative detection	Detects blackhole attacks.	No	Limited scope
[19]	2025	Trust-aware routing	Enhances secure routing.	No	Ignores inactive attacks
[20]	2025	FL-based IDS	Improves detection accuracy.	No	Limited evaluation
[25]	2025	ML-based clustering	Detects sinkhole attacks efficiently.	Yes	Dataset dependency
[26]	2025	Mathematical model	Models sinkhole impact on PDR, delay, throughput.	No	No mitigation
[27]	2024	Multi-tier approach	Detects Sybil attacks.	No	No privacy analysis
[28]	2024	Blacklisting	Mitigates DAO insider attacks.	No	Weak in mobility
[29]	2024	SECaaS IDS	Detects multiple RPL attacks.	No	Static defense
[30]	2024	Logic-based encoder	Prevents multiple attacks.	No	No 100% mobility
[31]	2024	PIT-based defense	Mitigates flooding attacks.	No	Interoperability issues
[32]	2024	Ensemble IDS	Detects rank and flooding attacks.	No	No 100% mobility
[33]	2024	HMM-based IDS	Detects sinkhole attacks.	No	No 100% mobility
[4]	2024	Performance analysis	Evaluates rank attacks.	Yes	No IDS
[34]	2023	Provenance model	Detects jamming and sync attacks.	No	No 100% mobility
[35]	2023	Challenge-response	Mitigates DDAO attacks.	No	Limited scope
[36]	2023	ML-based detection	Detects DDoS attacks.	No	Dataset limits
[37]	2023	Key management	Secures communication.	No	Single point failure
[38]	2023	ML + pruning	Detects delay attacks.	No	Weak for hybrid attacks
[39]	2023	Q-learning	Detects version attacks.	No	No 100% mobility
[40]	2023	ML-based IDS	Detects multiple attacks.	No	No 100% mobility
[41]	2023	OCSF-based	Prevents replay and DoS.	No	Scalability issues
[42]	2023	Federated DL	Detects wormhole attacks.	No	No ensemble
[5]	2023	Performance analysis	Evaluates version attacks.	Yes	No IDS
[43]	2023	PSCM-based authentication	Mitigates DDAO attacks.	No	Limited scope
Our Work	2026	Simulation-based analysis	Evaluates sinkhole attack.	Yes	No IDS

Hassan et al. [27] proposed LETM-IoT, a new trust-oriented approach designed specifically for the IoT's LLNs conditions. The LETM-IoT mechanism is implemented in a multi-tiered approach that detects three types of Sybil attacks, enhancing both the detection accuracy and the network's performance. Verma et al. [28] demonstrated that aggressive DAO insider attacks severely impact network performance. It presented Li-MSD, a blacklisting approach designed to counteract these attacks and effectively restore the performance of RPL. The Kalis2.0 [29] framework presents a SECaaS-based, context-aware, and self-adaptive IDS designed to address the diverse and the evolving characteristics of IoT networks. Given the heterogeneity of IoT devices and the evolving nature of their networks, traditional IDS approaches often fall short. Kalis2.0 adapts by autonomously gathering context information about the network, selecting the optimal detection strategies, and evolving these strategies

as the network changes. This approach ensures robust and tailored security solutions for various IoT scenarios with minimal human intervention. Vijaykumar et al. [30] introduced a new lightweight authentication protocol designed specifically for IoT systems that utilize RFID technology. This protocol employs a unique versatile digital logic encoder design architecture. The key feature of the proposed architecture is its ability to produce varied logical outputs in response to different randomly chosen control inputs. This variability significantly enhances the security of the system. Bilgili et al. [31] introduced IfNoT, a novel mechanism designed to mitigate interest flooding attacks in NDN IoT environments. These attacks involve the overwhelming of network nodes with malicious interest packets, leading to network congestion, resource depletion, and service disruption. Osman et al. [32] addressed the vulnerabilities in the RPL, widely used in IoT networks. RPL is vulnerable to a range of internal threats due to the limited resources of IoT devices and the open nature of the networks. To combat these issues, the authors proposed the ensemble learning-based IDS, which leverages ensemble learning techniques and genetic algorithms for feature selection to enhance the detection of specific RPL attacks. Bhale et al. [33] proposed an edge-assisted hybrid IDS specifically designed to detect and counteract Sinkhole attacks. The unique contribution of this research lies in leveraging edge computing to deploy the IDS close to the data source, improving the system's capacity to promptly identify and mitigate attacks. The proposed design integrates both host and network-level parameters, employing a HMM to detect anomalies.

Sadineni et al. [34] proposed the ProvLink-IoT model, which employs standards like PROV-DM and PROV-TEMPLATE to capture and analyze the provenance of network activities. This model is designed to generate provenance graphs under both normal and attack conditions, using data from the 6TiSCH protocol stack. Goel et al. [35] introduced a method called CRA-RPL to protect RPL networks from DDAO attacks. CRA-RPL enhances security by integrating a challenge-response mechanism into control messages to authenticate DAO-ACK communications. Kamaldeep et al. [36] proposed a novel dataset, IoT-CIDDS, specifically designed for IoT environments with 21 features and a single labelling attribute. Which capture the dynamics of IoT networks under DDoS attacks? The proposed framework involves two main phases: advanced feature engineering and machine learning model development. In the initial phase, the dataset is enriched through statistical analysis to understand feature distributions and correlations. The second phase involves creating and evaluating machine learning models using various algorithms to optimize the detection of DDoS attacks. Najafi et al. [37] proposed a novel method for managing cryptographic keys in IoT networks. The approach leverages a hierarchical structure based on the location and remaining energy levels of nodes within the network. It involves three main phases: key generation and distribution, node clustering, and key server selection. By utilizing a hierarchical architecture, the method produces keys that are both more concise and robust, which enhances the overall security and efficiency of IoT systems. Zhao et al. [38] introduced a baseline algorithm that uses machine learning to detect time-delay attacks by modelling system features and packet forwarding times of each network node. While effective, this approach requires monitoring all nodes, leading to high resource consumption and limited robustness. To address these issues, the authors proposed an improved algorithm called DNM. DNM optimizes detection by first pruning suspected nodes and then applying a fusion model to accurately identify malicious behaviour, thereby enhancing performance and reducing overhead. Sharma et al. [39] proposed a solution that leverages a Q-Learning strategy to identify malicious nodes executing version number attacks in LLNs. This method achieves a good balance between detection accuracy and efficiency, ensuring that legitimate nodes are not overly burdened with processing overhead. By using Q-Learning, the system is capable of adjusting in response to varying network conditions and effectively mitigate the impact of these attacks. Ors et al. [40] introduced a machine learning classifier designed to identify six different types of network attacks as well as benign traffic. The approach uses node-based feature extraction, enabling the system to pinpoint the exact network addresses of attackers rather than just indicating a general attack presence. This is achieved by analyzing traffic patterns over a sliding time window, allowing for precise detection and localization of malicious activities. Hkiri et al. [4] delved into the vulnerabilities of the RPL within the IoT ecosystem. It specifically examines how decreased rank attacks compromise network performance in both static and mobile scenarios. Höglund et al. [41] proposed TinyOCSP, a streamlined version of OCSP tailored for IoT, which leverages lightweight protocols such as CoAP and CBOR. TinyOCSP significantly reduces energy consumption and data size requirements, making certificate validation feasible for low-power devices. Additionally, the paper introduces a CCRL using Bloom filters, which further minimizes the validation overhead. These innovations are crucial for the scalability and security of IoT systems, enabling more secure and efficient authentication processes in environments with severe resource constraints. Alghamdi et al. [42] introduced a cascaded wormhole detection technique tailored for IoT networks. This technique combines federated deep learning with a DTF. The DTF assesses nodes based on two trust attributes. Meanwhile, CNN and LSTM models are trained using a federated approach,

which ensures data security and privacy for each node. Sharma et al. [5] examined the vulnerabilities and performance implications of RPL in IoT environments, specifically under the stress of a version number attack. The study highlights how RPL, developed to optimize routing in networks with limited resources such as 6LoWPAN, can be destabilized by this type of attack, which can lead to DoS conditions. The version number attack exploits RPL's handling of version numbers in its excessive control messaging, which leads to network instability and markedly reduces performance, particularly in scenarios where IoT nodes are mobile. Goel et al. [43] addressed a significant security issue in RPL-based IoT networks, specifically the DDAO attack. A lightweight approach is presented in this paper based on a challenge-response strategy using PSCM. By modifying the DAO and DAO-ACK control packets in RPL, the proposed approach authenticates the acknowledgement process, thus distinguishing between legitimate and malicious nodes.

Rajasekar and Rajkumar [44] explored the vulnerabilities of RPL when subjected to DIS flooding attacks in 6LoWPAN environments. The results indicate that an increase in the number of malicious nodes and when they are positioned closer to the network's sink node, the network's performance deteriorates significantly, with notable increases in E2ED and power consumption, and a decrease in PDR. Nandhini et al. [45] proposed the RAD algorithm. This algorithm leverages a non-cryptographic hash function and random sampling techniques to detect and isolate internal rank attackers while minimizing energy consumption and avoiding additional control packet overhead. The RAD algorithm enhances security and performance in IoT networks by preserving the integrity of control packets and ensuring efficient routing even under attack conditions. Sithik and Kumar [46] proposed a multi-phase approach. First, they introduce a secure authentication mechanism for RPL nodes using Blowfish encryption and a lightweight hashing algorithm to ensure only legitimate nodes can join the network. Next, they enhance network reliability and optimize parent node selection through a hybrid algorithm combining Cuttlefish and Harris Hawk optimization techniques, guided by multi-context aware decision-making. For congestion control, the study utilizes a Multi-Intelligent Agent-based Q-Learning approach to monitor and manage network traffic dynamically, alongside a virtual clustering method to alleviate congestion. Bilal et al. [47] presented a novel intrusion detection model designed to protect IoT environments from sinkhole attacks. This model utilizes resource-rich edge nodes to detect various sinkhole attackers through message exchanges. Researchers have come up with various methods to detect and handle sinkhole attacks and other threats specific to RPL networks. Many of these methods use behaviour-based or anomaly-based approaches. While there are also cryptography-based and trust-based solutions, they often don't work well in networks with limited resources. Most existing solutions also tend to ignore the effects of node mobility within the network. This paper addresses this issue by examining sinkhole attacks in networks with mobile nodes and demonstrates how the performance metrics shift with different numbers of attacker nodes. Many critical IoT applications operate on resource-constrained networks and require solutions that are lightweight, secure, scalable, and support mobility to ensure user security and privacy [48, 49]. One example is 6LoWPAN is an essential option for LLNs [50].

Researchers have come up with numerous suggested solutions that barely address mobile nodes, even though IoT networks often include them. The presence of these mobile nodes can seriously impact network performance in confined spaces. So, this paper takes a look at a cluster of mobile nodes alongside different types of attackers. They assess performance using several metrics, including the number of isolated nodes, PDR, IPT, and power consumption.

4. Performance metrics

Evaluating the performance of mobile RPL-based IoT networks when dealing with sinkhole attacks requires a comprehensive understanding of various performance metrics. These metrics give a clear view of how well the network performs, reliability, and security, which are essential for determining the influence of sinkhole attacks and the effectiveness of mitigation strategies. This chapter details the performance metrics used in this study to evaluate the performance of mobile RPL-based IoT networks under sinkhole attack conditions. This evaluation was conducted using Contiki Cooja. Contiki Cooja is a powerful and flexible open-source simulation tool specifically designed for the development and evaluation of IoT networks. Developed as part of the Contiki OS, which is widely used in IoT applications, Cooja offers a detailed and realistic simulation environment that supports a wide range of network protocols and hardware platforms.

Table 3 describes the simulation parameters used to analyze network behavior. Experimental results indicate that mobility significantly affects IoT networks. This study, which seeks to analyze network behaviour in the presence of attackers, has the following objectives:

- Analysis of performance metrics, including number of isolated nodes, PDR, IPT, and power consumption, in scenarios without attacks.

- Evaluating the effects of Sinkhole attacks on the number of isolated nodes, PDR, IPT, and power consumption.
- Examining the impact of mobility and Sinkhole attacks on the network constitutes the primary focus of this paper.

Table 3. Simulation parameters.

Parameters	Value
Simulator	Cooja (Contiki OS)
Mote type	Z1
Radio medium	UDGM
Transport layer protocol	UDP
PHY and MAC layer	IEEE 802.15.4
Scenario dimension	200 m * 200 m
Transmission range	50 m
DODAG root rank	1
Gateway nodes	1
Number of sensor nodes	10, 20, 30, 40, 50
Number of mobiles nodes	0%, 50%, 100%
Number of attacker node	0%, 10%, 20%, 30%
Speed of node	1 to 2 mps
Data packet size	30 bytes
Simulation time	30 minutes

The simulations were run for 30 minutes each, across a total of 60 scenarios, to observe their actual impact on the network. Three types of scenarios were considered: a static network with no mobile nodes, a hybrid network with 50% static and 50% mobile nodes, and a mobile network where all nodes are mobile. Additionally, we assumed that the gateway node was stationary and received the packets from the sender nodes.

Performance evaluation parameters

This simulation evaluates the performance of mobile RPL-based IoT networks under a sinkhole attack by using metrics such as number of isolated nodes, PDR, IPT, and power consumption. The definitions, formulas, use cases, and scope for these metrics are explained below.

- **Number of isolated nodes:** It refers to the count of nodes that are unable to communicate with any other nodes in the IoT network. This isolation can occur due to various reasons such as hardware failures, network congestion, interference, or malicious attacks (e.g., sinkhole attacks). The Number of isolated nodes is calculated using the following formula (Equation (1)):

$$I = N - C \quad (1)$$

where I is the number of isolated nodes, N is the total number of nodes in the network and C is the number of connected nodes that have sent at least one packet to the sink node.

Use Case:

- 1) An increased number of isolated nodes might indicate a potential attack, such as a sinkhole attack, where certain nodes are deliberately isolated to disrupt the network.
- 2) Regularly checking for isolated nodes helps in identifying and addressing connectivity issues promptly, ensuring the network's robustness and reliability.
- 3) Understanding isolation patterns can help in optimizing the placement and configuration of nodes to enhance network performance and resource utilization.

Scope: Vital for real-time monitoring systems to ensure ongoing network reliability and security.

- **Packet delivery ratio (PDR):** It represents the proportion of packets that reach their destination compared to the total number of packets sent by the source in a network. It indicates how dependable something is and the efficiency of the network in delivering data.

The PDR is calculated using the following formula (Equation (2)):

$$PDR = \frac{\text{Number of Packets Received at Sink}}{\sum_{i=1}^N \text{PacketsSentByNode}_i} \quad (2)$$

Use Case:

- 1) Assessing the performance and reliability of different types of networks, such as IoT networks, wireless sensor networks, mobile ad hoc networks, and traditional wired networks.
- 2) PDR is a key metric to ensure QoS.
- 3) Evaluating the effectiveness of different routing protocols in delivering data packets.

Scope: In IoT networks, a high PDR ensures that data from sensors and devices is reliably transmitted to central systems for processing and action.

- **Inter-packet time (IPT):** The time interval between the arrival times of consecutive packets at a particular point in the network.

The Inter-packet time is calculated using the following formula (Equation (3)):

$$IPT = (t_{i+1} - t_i) \text{sec} \quad (3)$$

where t_{i+1} is the arrival time of packet $i + 1$, t_i is the arrival time of packet i .

Use Case:

- 1) Monitoring traffic patterns and burstiness.
- 2) Detecting anomalies or changes in network traffic.
- 3) Analyzing network load and congestion.

Scope: Usually measured at a single point in the network, such as at a gateway node in the RPL-based IoT network.

- **Power consumption:** In the context of networked systems, particularly IoT devices, it refers to the amount of electrical energy consumed by a device or system while performing its functions. It is an important metric for assessing the efficiency and sustainability of devices, especially in environments where battery life and energy efficiency are critical.

Power consumption can be calculated using the formula (Equation (4)):

$$\text{Power Consumption} = \left(\frac{E_t}{T_t} \right) \text{mW} \quad (4)$$

where $E_t = (E_{\text{Transmit}} + E_{\text{Listen}} + E_{\text{CPU}} + E_{\text{LPM}}) \text{mJ}$

Power consumption is calculated by considering the energy spent in different operational states of an IoT node, including transmission energy (E_{Transmit}), listen energy (E_{Listen}), CPU processing energy (E_{CPU}), and low-power mode energy (E_{LPM}). Transmission Energy refers to the amount of energy spent on transmitting data, while listen energy refers to the energy needed for listening to received packets. The CPU processing energy refers to the energy needed in performing routing and attack detections. The low-power mode energy refers to the energy needed in sleeping or idling the node in order to save battery life.

Total energy consumption is achieved by adding up all the above energies for the period that they operate. The time variable (T_t) denotes the observation period during which node activities are monitored and measured. It represents the cumulative duration over which transmission, reception, processing, and idle-state operations contribute to the overall energy expenditure of the network.

Use Case:

- 1) Analyzing the power consumption of each sensor node during data collection, processing, and transmission phases.
- 2) Identifying power-hungry processes and optimizing them.
- 3) Implementing energy-efficient communication protocols.

Scope: Power consumption is a critical factor across various domains and applications, particularly in IoT devices, ensuring long battery life for remote and portable devices.

5. Result Analysis

This section evaluates and analyzes the network's performance with and without a sinkhole attack. It also discusses how network performance changes when nodes move around. To implement the sinkhole attack, the 'uip6.c', 'rpl-private.h', and 'rpl-timers.c' files in the Contiki OS were modified. The 'uip6.c' file was modified to influence packet forwarding behavior, while 'rpl-private.h' and 'rpl-timers.c' were adjusted to alter RPL routing operations and timer-related functionalities required for the attack

implementation. These modifications enabled the simulation of sinkhole attack behavior within the RPL-based IoT network. For the experiments, different numbers of nodes and varying numbers of attacker nodes were used. The entire experiment is demonstrated in a static, a hybrid, and a mobile network. All the nodes used are of the Zolertia Z1 mote type, which is well-suited for sinkhole attacks due to their capabilities. To create the IoT network, the standard Z1 node utilizes 8 KB RAM and 92 KB ROM. The network consisted of both benign and malicious nodes. The first network that was analyzed was the static network. The following networks that were analyzed were the hybrid network and then the mobile network. The results were analyzed for the number of isolated nodes in the network, the PDR of the network, the IPT, and the power consumption of the network. The results for the impact of attacker nodes on the system are detailed in the subsequent sub-sections.

5.1. Number of Isolated Nodes

As previously discussed, the primary objective of a sinkhole attack is to isolate sensor nodes within an RPL-based IoT network. The "Number of isolated nodes" metric is particularly important in assessing the impact of such attacks, as it directly reflects how effectively the network is compromised. Figure 5 illustrates the effect of a sinkhole attack on different types of IoT networks: static, hybrid, and mobile. The entries marked as N/A do not indicate missing data or excluded scenarios. Instead, they represent simulation cases in which the corresponding metric recorded a value of zero.

In the static network, where all nodes remain fixed, the number of isolated nodes rises as the number of attacker nodes increases. This is because the static nature of the network makes it easier for attackers to consistently target and isolate specific nodes, leading to a significant disruption in network communication. Similarly, in the mobile network, where all nodes are mobile, the sinkhole attack also has a profound effect. The mobility of the nodes creates dynamic topology changes, which, when combined with the presence of attacker nodes, results in an increased number of isolated nodes. The attackers can exploit the movement patterns to isolate nodes more effectively, further weakening the network.

In contrast, the hybrid network, which comprises both static and mobile nodes, shows a comparatively lower increase in the number of isolated nodes. The mixed nature of the network, where half the number of nodes is mobile and half are static, makes it more challenging for attackers to isolate a significant number of nodes. The diverse movement and positioning of the nodes provide a level of resilience against the sinkhole attack.

In scenarios where there is no attack, the static network exhibits zero isolated nodes, indicating a fully connected and functional network. However, in hybrid and mobile networks, even in the absence of an attack, the number of isolated nodes increases slightly due to the inherent challenges posed by node mobility, such as temporary disconnections or changes in network topology. Overall, this analysis demonstrates that while static and mobile networks are highly vulnerable to sinkhole attacks, hybrid networks offer a more robust defense, reducing the impact of such attacks on the IoT network.

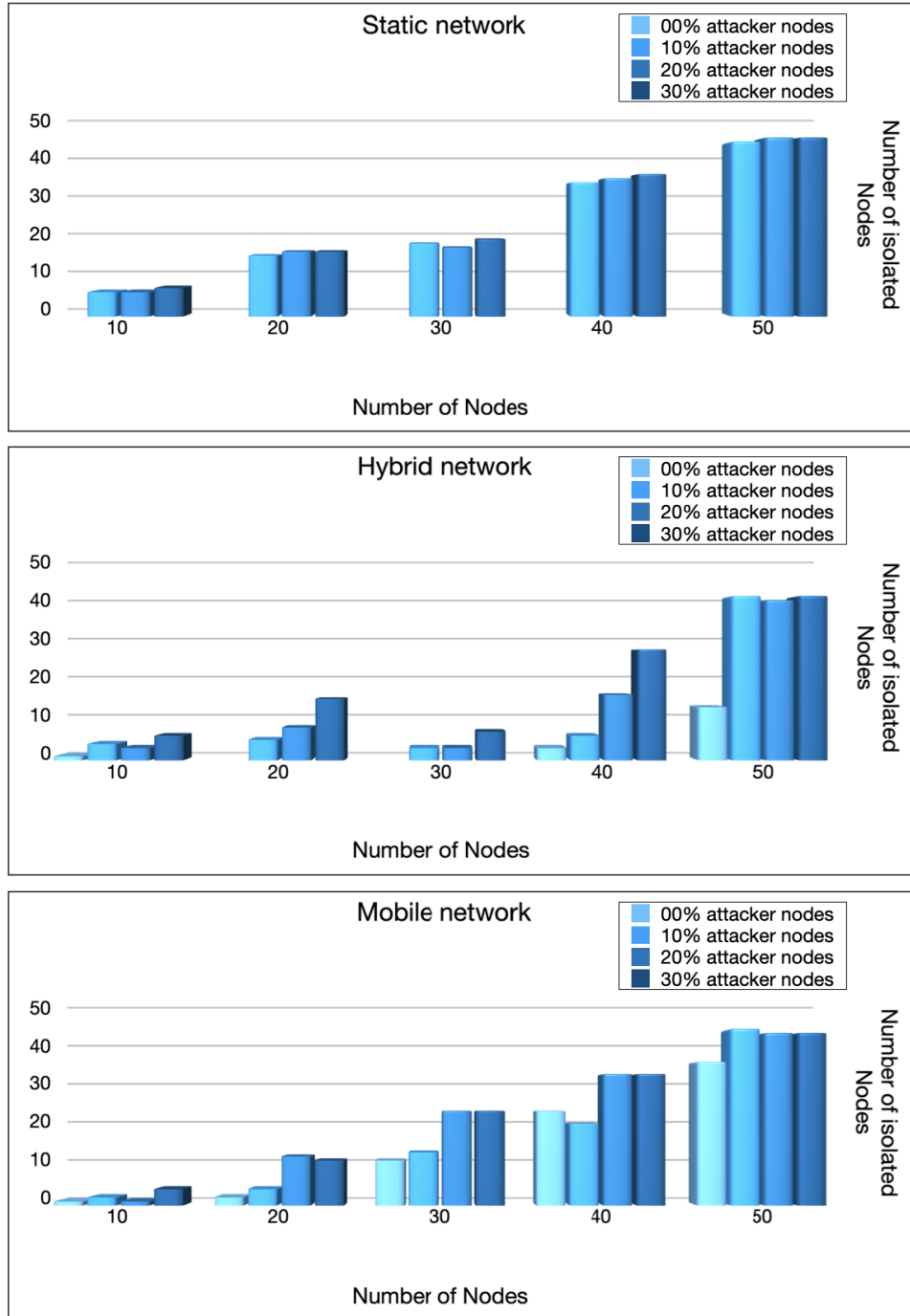


Figure 5. Number of isolated nodes.

5.2. Packet Delivery Ratio

Figure 6 illustrates the impact of a sinkhole attack on an RPL-based IoT network as the number of nodes increases, alongside the percentage of attacker nodes, in static, hybrid, and mobile networks. The effect of the attack is visible as the average PDR steadily declines with an increasing number of attackers.

In the static network, there is a dramatic drop in PDR when transitioning from a no-attack scenario to an attack scenario. However, as the number of attacker nodes continues to increase, the rate of decline in PDR slows down. This suggests that even a small number of attackers can initially isolate a significant portion of nodes, severely disrupting the network. When the number of nodes increases, the drop in PDR is less pronounced due to network congestion. Interestingly, when the network has between 20-30 nodes, the PDR improves, likely because the increased number of neighbours allows packets to be forwarded via shorter paths.

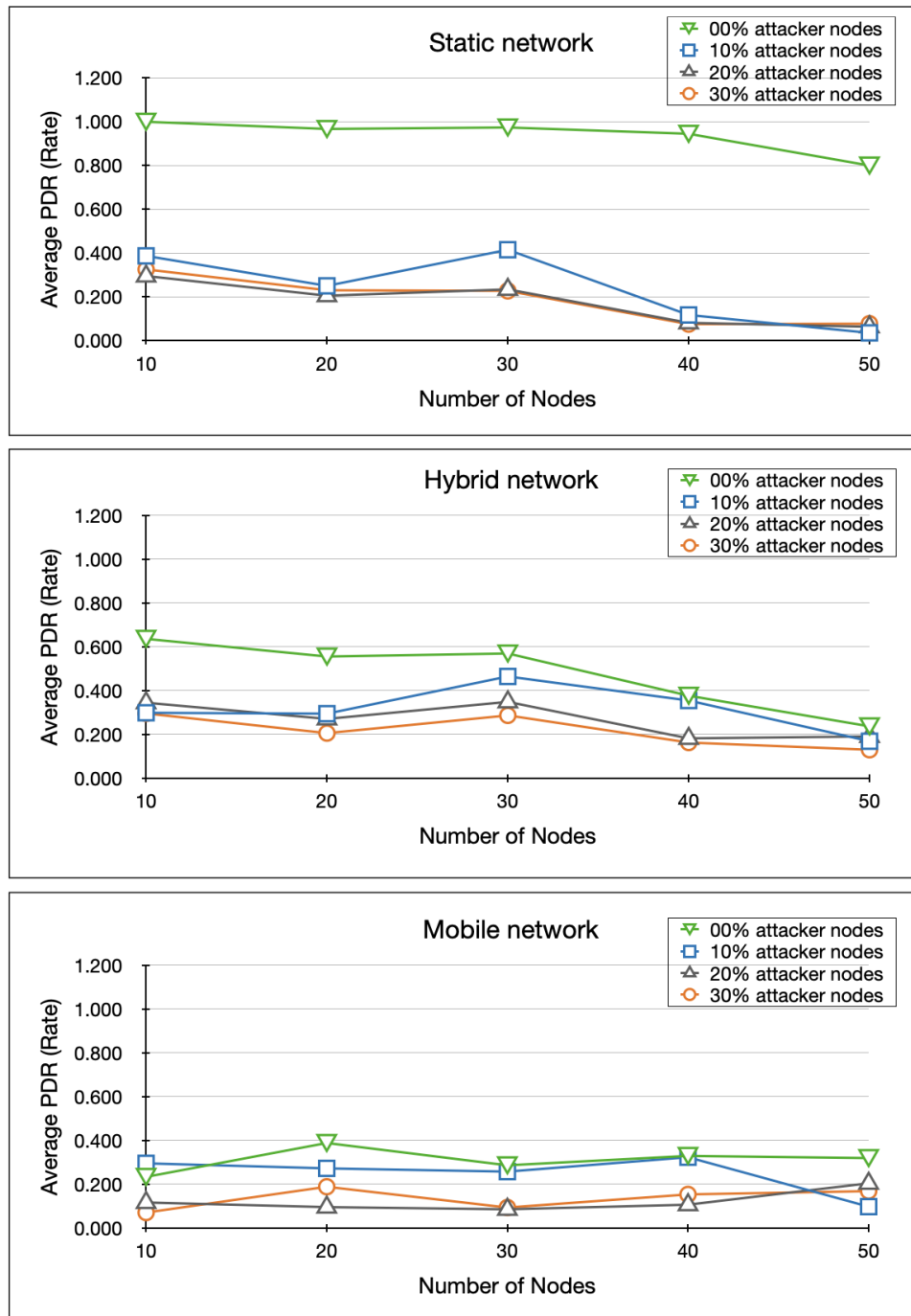


Figure 6. Average packet delivery ratio.

In the hybrid network, even in the no-attack scenario, the average PDR is already reduced by 37% due to mobility, which introduces instability in the network. As the percentage of attacker nodes rises, the average PDR continues to drop, indicating that as more nodes are isolated, the PDR decreases. Nodes 20 to 30, PDR improves because additional neighbours provide shorter paths for packet forwarding. However, further increases in nodes lead to a decrease in PDR due to congestion.

In the mobile network, the no-attack scenario already shows a significant 70% drop in PDR, largely due to the mobility of the nodes, which causes frequent disconnections and route changes. As the number of attackers increases, the PDR drops further but eventually shows a slight improvement. This indicates that congestion is reduced as the attacker nodes increase, possibly because the network becomes less dense, making it easier for packets to find a clear path. When the number of nodes increases, PDR initially improves due to the availability of more neighbours, enabling packets to be forwarded via shorter paths. However, as the network becomes more congested, the PDR drops again, showing that congestion

eventually outweighs the benefits of having more neighbours. In conclusion, this analysis shows that in a mobile network, two factors significantly impact PDR as the number of nodes increases: congestion and the availability of shorter paths. As congestion increases, PDR decreases, but when more neighbours are available to forward packets via shorter paths, PDR improves.

5.3. Inter-Packet Time

The IPT metric is minimally affected by the presence of attackers but is highly sensitive to mobility, as shown in Figure 7.

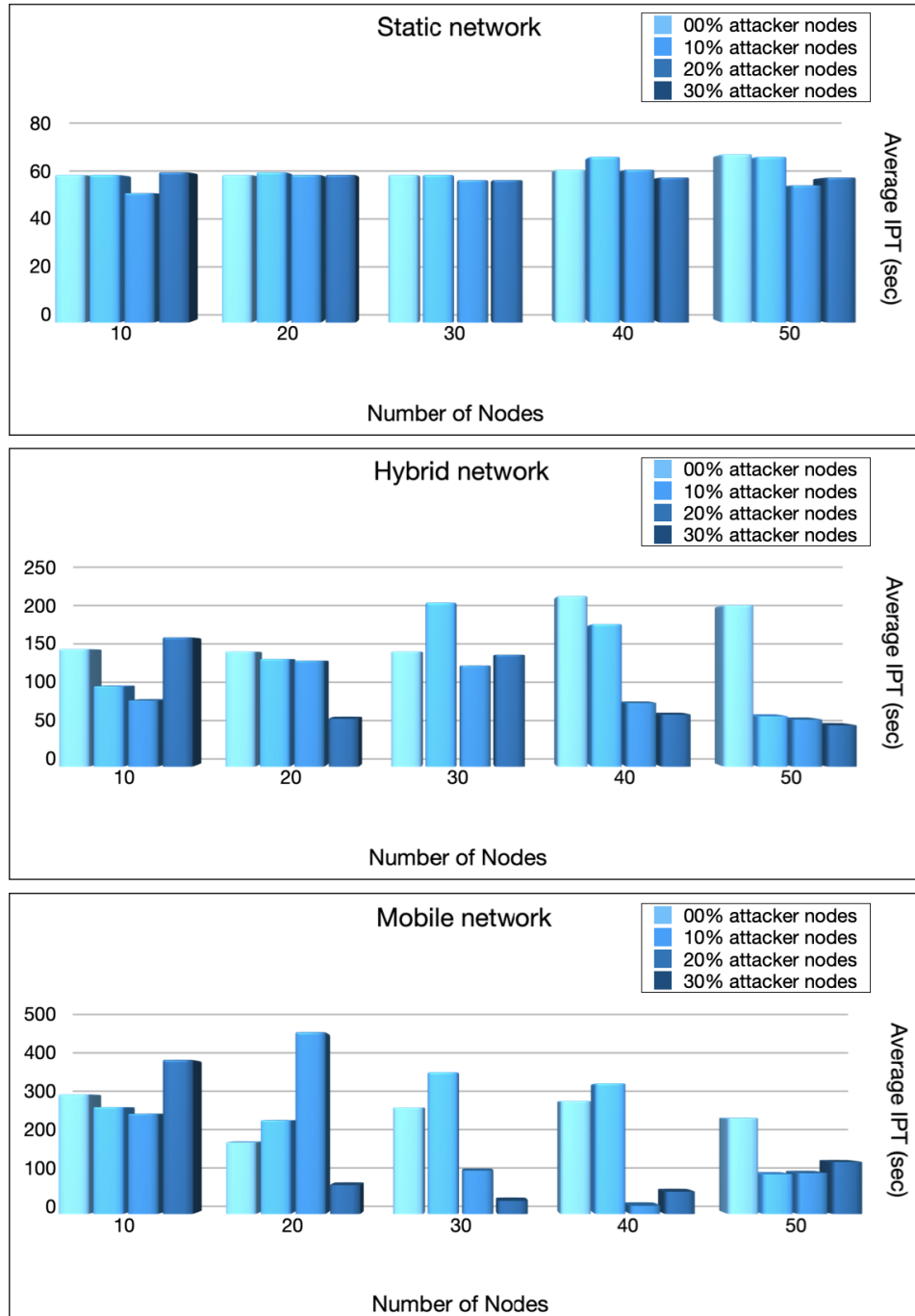


Figure 7. Average inter-packet time.

In a static network, increasing the percentage of attacker nodes results in little to no change in the average IPT. This indicates that when attacker nodes isolate sensor nodes, IPT remains largely unaffected. Interestingly, in some cases, IPT decreases with a higher percentage of attackers due to the reduced congestion in the network caused by the isolation of nodes. When the number of nodes in the static

network increases, there is also no significant change in IPT. Since the positions of the nodes are fixed, packets reach the gateway without delay, leading to a stable IPT. Occasionally, IPT decreases as the number of attacker nodes increases, again due to less congestion as more nodes become isolated.

In the hybrid network, IPT increases by approximately 90 seconds due to mobility as compared to the static network. As attacker nodes increase, IPT generally decreases, which can be attributed to reduced congestion from the isolation of more nodes. When the number of nodes in the hybrid network are 30, IPT first rises and then falls, reflecting the network's instability caused by mobility. The initial increase in IPT indicates that mobility is causing delays, while the subsequent decrease suggests that isolated nodes reduce congestion, making packet delivery more efficient.

In the mobile network, IPT decreases further as the proportion of mobile nodes grows, continuing the trend observed from the static to the hybrid network. When the number of attacker nodes increases, IPT initially rises, then falls, and sometimes rises again. This pattern occurs because mobile attacker nodes disrupt the packet forwarding routes, leading to delays and increased IPT. However, if attackers do not significantly disrupt the routes, IPT may decrease. As the number of nodes in the mobile network increases, IPT first decreases and then increases. Initially, the presence of more neighbours allows packets to take shorter paths, reducing IPT. However, as the number of nodes continues to rise, congestion begins to outweigh the benefits of these shorter paths, leading to an increase in IPT. This demonstrates that in mobile networks, congestion can eventually dominate the efficiency gains provided by additional neighbours, leading to an overall increase in IPT.

5.4. Power Consumption

Since IoT networks are composed of resource-constrained devices, efficient power consumption is essential for maintaining device connectivity. Therefore, average power consumption is one of the most important metrics to evaluate in such networks. The analysis of this metric is shown in Figure 8, where the effect of increasing the percentage of attacker nodes on power consumption is examined.

In the static network, it is evident from the graph that power consumption generally increases as the number of attacker nodes rises. This happens because attacker nodes isolate sensor nodes, reducing the number of neighbouring nodes available to forward packets. As a result, the network often fails to find the shortest paths, leading to increased power consumption. The graph also shows that power consumption tends to increase as the number of nodes grows, likely due to network congestion. However, in some instances, power consumption decreases, which may be due to the availability of more neighbours that help forward packets along shorter paths, thereby reducing energy usage.

The hybrid network exhibits a similar trend to the static network. However, the gap in power consumption between different percentages of attacker nodes is narrower in the hybrid network compared to the static network. This reduced gap is attributed to the mobility of nodes, which introduces a level of dynamism in the network. Despite this, overall power consumption continues to increase as attacker nodes are added, similar to what is observed in the static network.

When examining the mobile network, the graph shows that power consumption increases even more compared to the hybrid network. This confirms that as the number of mobile nodes increases, power consumption also rises. In the mobile network, as the number of attacker nodes increases, power consumption initially rises, then decreases. This pattern can be explained by two factors previously discussed: congestion and the availability of shorter paths in the network. As attacker nodes isolate others, congestion may decrease, but the availability of shorter paths plays a crucial role. If the network can still find shorter paths despite the attack, power consumption may decrease. However, if shorter paths are not available, power consumption will increase. Finally, as the number of nodes in the mobile network increases, power consumption initially rises and then falls. This indicates that the same two factors, congestion and the availability of shorter paths are at play. Initially, congestion causes power consumption to increase, but as more neighbours become available and shorter paths are found, power consumption decreases. However, if congestion becomes too severe, power consumption rises again, demonstrating the complex interplay between these factors in a mobile IoT network.

The results indicate that sinkhole attacks can cause substantial degradation in RPL-based IoT networks, particularly when attacker density increases. In the literature, mitigation approaches such as INTI [51], SoS-RPL [52], RFTRUST [53], InDReS [54], and NADSA [55] have been shown to improve detection accuracy and reduce false alarms to varying degrees, but their reported performance is generally dependent on network conditions such as node density, traffic pattern, and mobility. The attack effects observed in this study are consistent with those findings, showing that malicious nodes can significantly lower packet delivery reliability while increasing routing disruption and false forwarding behavior. This suggests that any mitigation strategy must be robust enough to maintain stable detection performance under changing network conditions, especially in dense and dynamic IoT deployments. Therefore, the present results provide a useful baseline for comparing the severity of sinkhole attacks against the

effectiveness of existing defense mechanisms reported in the literature.

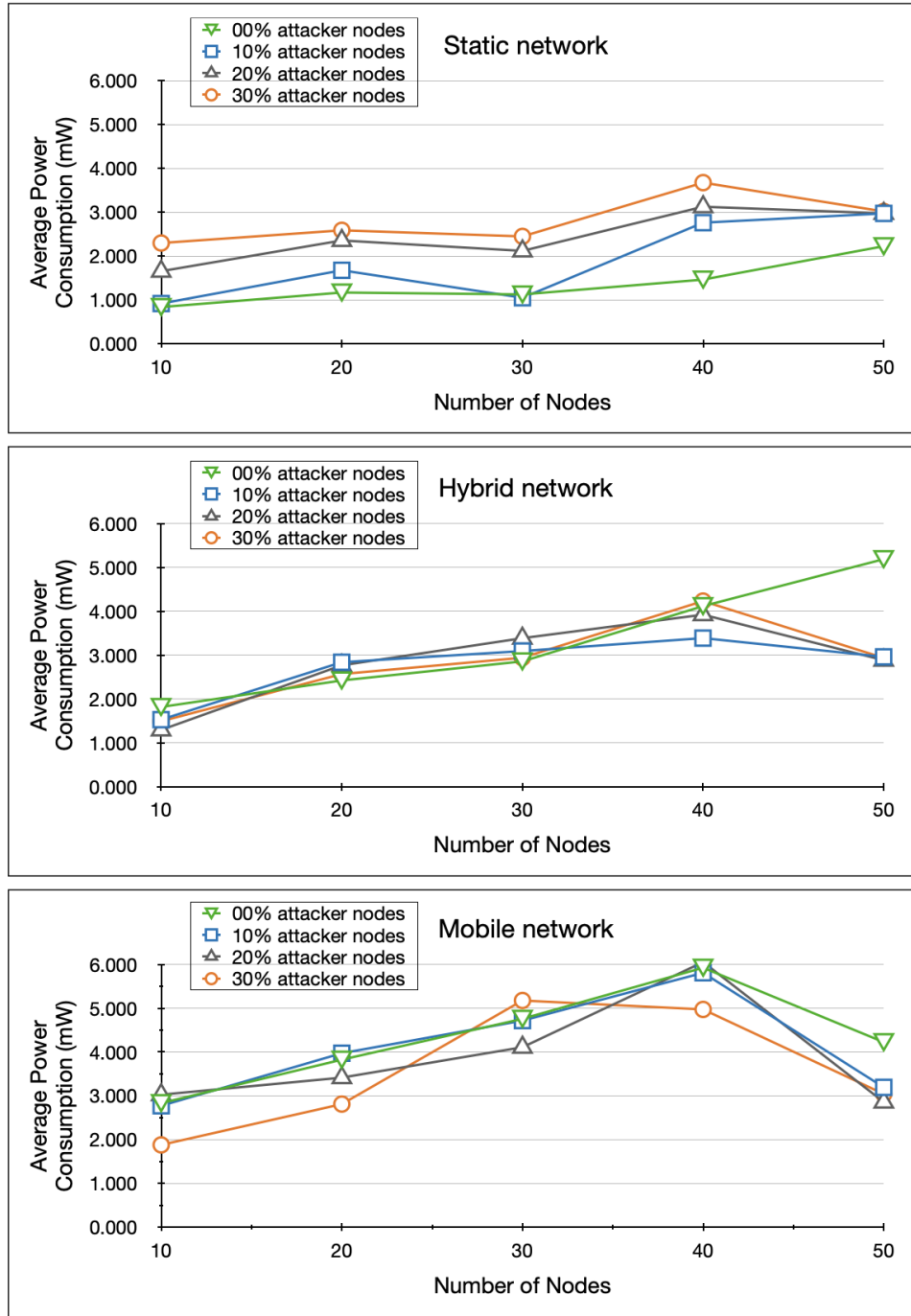


Figure 8. Average power consumption.

6. Discussions

The results of the experiment clearly show that mobility causes an increase in resource consumption in terms of power. Therefore, researchers should include mobility in their analysis and mitigation strategies, which many have not done. Some have considered mobility but haven't used fully mobile networks where all nodes are mobile. The goal of this paper was to understand the impact of mobility and sinkhole attacks on RPL-based IoT networks. It shows the effect of sinkhole attacks on static, hybrid, and mobile networks, which is important to understand how both attacks and mobility influence the network.

The results demonstrate that both the attack and mobility cause the PDR to drop significantly. Therefore, it is crucial to find ways to address the drop in PDR caused by both the attack and mobility.

The findings also reveal a significant increase in the number of isolated nodes due to both factors. Increasing the number of nodes in the network also affects performance. Adding more nodes has two impacts: it can lead to network congestion, which reduces performance, and it can provide shorter paths due to more neighbors, which can improve performance.

In conclusion, the analysis from this paper highlights the importance of considering mobility, attacks, and the number of nodes when implementing IDS. The following sub-section will discuss the implementation overload in more detail.

6.1. Implementation Overhead

In this analysis, a sinkhole attack was applied to an RPL-based IoT network. The attacker nodes, sensor nodes, and gateway nodes used for implementation were all of the Zolertia Z1 mote type. As shown in Figure 9, it is evident that the sinkhole attack was implemented with minimal overload because both ROM and RAM usage were lower than the standard Zolertia Z1 node. This allows us to conclude that the sinkhole attack can be implemented with less overload in static, hybrid, and mobile networks.

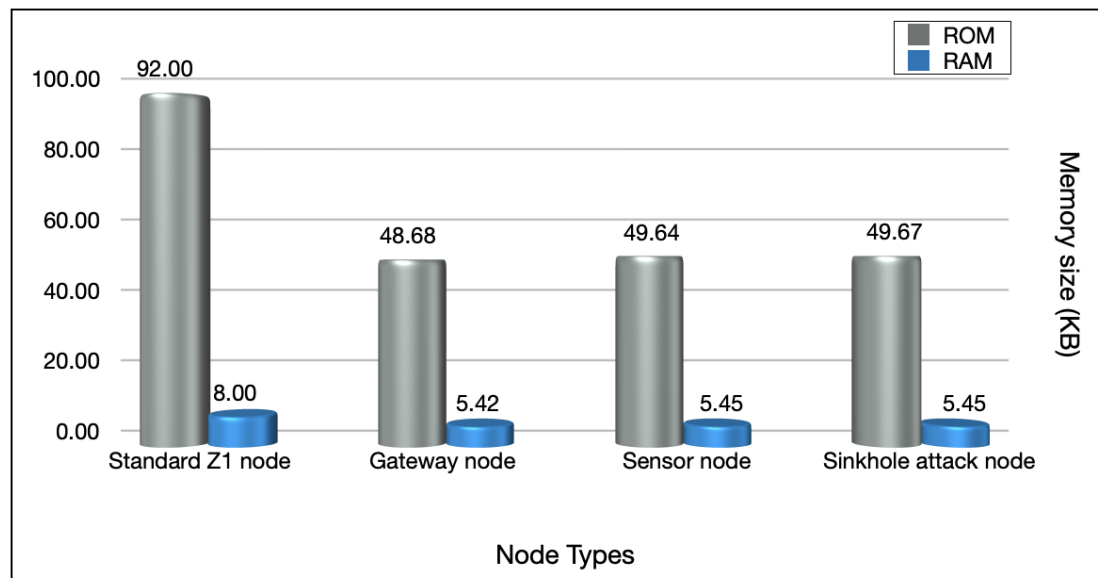


Figure 9. Memory requirement.

6.2. Limitation and Future Work

This study has some limitations. First, the evaluation is based solely on simulations conducted in the Cooja environment and does not include validation using real-world IoT testbeds. Second, node mobility is modeled using only the Random Waypoint mobility model, and different mobility patterns may lead to variations in network behavior. Finally, the scope of this work is limited to analyzing the impact of sinkhole attacks on mobile RPL-based IoT networks; therefore, no attack detection or mitigation mechanism is proposed or evaluated. Future work will address these limitations through real-world experimentation, the use of additional mobility models, and the investigation of suitable mitigation strategies.

7. Conclusion

This work evaluated the performance of mobile RPL-based IoT networks in the presence of a sinkhole attack. Through extensive simulations and analysis, it was observed that mobility significantly impacts the network's performance, particularly in terms of IPT and power consumption. The results demonstrated that the combination of mobility and sinkhole attacks leads to a considerable degradation in network performance, causing an increase in the number of isolated nodes and a sharp decline in PDR. The findings highlight the importance of considering mobility in the design and implementation of security mechanisms for RPL-based IoT networks, as ignoring it could lead to underestimating the impact of such attacks.

Author Contributions

Conceptualization, M.A. and N.C.; methodology, M.A. and N.C.; software, M.A.; validation, M.A. and N.C.; formal analysis, M.A.; investigation, M.A. and N.C.; resources, M.A. and N.C.; data curation, M.A.; writing—original draft preparation, M.A.; writing—review and editing, M.A. and N.C.; visualization, M.A. and N.C.; supervision, N.C..

Funding

This research received no external funding.

Conflict of Interest Statement

The authors declare no conflict of interest.

Data Availability Statement

Available from the authors upon reasonable request.

Acknowledgment

The authors would like to express their sincere gratitude to the National Institute of Technology (NIT) Hamirpur, Himachal Pradesh, India, for providing the computational facilities, research infrastructure, and academic environment necessary to carry out this research.

References

- 1 N. Khelifi, E. Nataf, S. Oteafy, and H. Youssef. “Rescue-sink: dynamic sink augmentation for rpl in the internet of things”, *Transactions on emerging telecommunications technologies*, XXIX (4), p. e3278, 2018.
- 2 A. Verma and V. Ranga. “Mitigation of dis flooding attacks in rpl-based 6lowpan networks”, *Transactions on emerging telecommunications technologies*, XXXI (2), p. e3802, 2020.
- 3 A. A. R. A. Omar, B. Soudan, and A. Altaweel. “Uos iotsh 2024: A comprehensive network traffic dataset for sinkhole attacks in diverse rpl iot networks”, *Data in Brief*, LV, p. 110650, 2024.
- 4 A. Hkiri, M. Karmani, O. B. Bahri, A. M. Murayr, F. H. Alasmari, and M. Machhout. “Rpl-based iot networks under decreased rank attack: Performance analysis in static and mobile environments”, *Computers, Materials & Continua*, LXXVIII (1), pp. 227–247, 2024.
- 5 G. Sharma, J. Grover, and A. Verma. “Performance evaluation of mobile rpl-based iot networks under version number attack”, *Computer Communications*, CXCVII, pp. 12–22, 2023.
- 6 F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt. “Cross-level sensor network simulation with cooja”. In *Proceedings of the 31st IEEE conference on local computer networks*, pp. 641–648, 2006.
- 7 A. Dunkels, B. Gronvall, and T. Voigt. “Contiki-a lightweight and flexible operating system for tiny networked sensors”. In *Proceedings of the 29th annual IEEE international conference on local computer networks*, pp. 455–462, 2004.
- 8 B. Safaei and M. Khodabandelou. “Dpm-rpl: Routing-based distributed dynamic power management for nvp iot networks”, *IEEE Transactions on Green Communications and Networking*, X, pp. 2262–2280, 2026.
- 9 D. Manivannan. “Recent endeavors in machine learning-powered intrusion detection systems for the internet of things”, *Journal of Network and Computer Applications*, CCXXIX, p. 103925, 2024.
- 10 T. ul Hassan, M. Asim, T. Baker, J. Hassan, and N. Tariq. “Ctrust-rpl: A control layer-based trust mechanism for supporting secure routing in routing protocol for low power and lossy networks-based internet of things applications”, *Transactions on Emerging Telecommunications Technologies*, XXXII (3), p. e4224, 2021.
- 11 J. T. Ibibo and B. R. Japheth. “Rpl protocol using contiki operating systems: A review”. In *Proceedings of the International Conference on Safety and Security in IoT*. Springer, pp. 17–34, 2023.
- 12 A. Wakili, S. Bakkali, and N. Faruk. “Ai-enhanced context-aware optimization of rpl routing protocol for iot environments”. In *Proceedings of the IEEE 2nd International Conference on Multi-disciplinary Engineering and Applied Science (ICMEAS)*, pp. 1–6, 2023.
- 13 J. Knies and V. de Figueiredo Marques. “Marpl: A crosslayer approach for internet of things based on neighbor variability for mobility support in rpl”, *Transactions on Emerging Telecommunications Technologies*, XXXI (12), p. e3931, 2020.

- 14 J. Jaisooraj and S. Madhu Kumar. "Energy-efficient routing in low power and lossy networks with concurrent overlapping rpl instances", *Transactions on Emerging Telecommunications Technologies*, XXXIII (11), p. e4590, 2022.
- 15 S. Budania and M. V. Shenoy. "Rpl*: An explainable ai-based routing protocol for internet of mobile things", *Internet of Things*, XXVII, p. 101283, 2024.
- 16 A. Patel, D. Patel, R. Kakkar, P. Oza, S. Agrawal, S. Tanwar, R. Sharma, and N. Yamsani. "Safeguarding the iot: Taxonomy, security solutions, and future research opportunities", *Security and Privacy*, VII (2), p. e354, 2024.
- 17 S. Yilmaz, S. Sen, and E. Aydogan. "Exploring and enhancing placement of ids in rpl: A federated learning-based approach" *IEEE Internet of Things Journal*, XII (13), 2025.
- 18 M. Belkheir, M. Rouissat, A. Mokaddem, D. Ziani, and P. Lorenz. "Lightweight novel approach for collaborative packet-based mitigation of blackhole attacks in rpl-based iot", *Journal of Network and Systems Management*, XXXIII (2), p. 34, 2025.
- 19 M. N. Parizi, S. H. Ghafouri, and M. S. Hajmohammadi. "Tarrp: Trust aware rpl routing protocol for iot", *International Journal of Communication Systems*, XXXVIII (4), p. e6124, 2025.
- 20 H. Sharma and G. S. Yadav. "Privacy-preserving intrusion detection with federated learning: enhancing privacy and efficiency in iot networks", *International Journal of Machine Learning and Cybernetics*, XVI (9), pp. 5821-5839, 2025.
- 21 I. S. Alsukayti, M. Alreshoodi, and M. Rouissat. "A lightweight mitigation technique against a modified version number attack in iot networks", *IEEE Access*, XIII, pp. 20472-20490, 2025.
- 22 S. Hamrioui, A. Ali Cherif, and P. Lorenz. "Sarp: A secure and adaptive machine learning-driven routing protocol for dynamic iot networks", *Journal of Network and Systems Management*, XXXIV (1), p. 32, 2026.
- 23 P. Therasa, P. S. Kumar, and D. K. Selvi. "Fortifying internet of things security: Employing deep learning for privacy-preserving data transmission in clustered environments", *International Journal of Communication Systems*, XXXIX (4), p. e70411, 2026.
- 24 P. K. Verma, M. Kumar, A. Gupta, A. K. Saini, A. K. Sharma, and N. Rakesh. "Enhanced detection and mitigation of hello flood attacks in iot networks using modified deep neural networks and optimization algorithms", *Discover Internet of Things*, 2026.
- 25 M. Z. Hasan, Z. M. Hanapi, Z. A. Zukarnain, F. H. Huyop, and M. D. H. Abdullah. "An efficient detection of sinkhole attacks using machine learning: Impact on energy and security", *Plos one*, XX (3), p. e0309532, 2025.
- 26 N. Sinha and A. K. Mishra. "Impact assessment of sinkhole attack in iot networks: a mathematical modeling approach", *Peer-to-Peer Networking and Applications*, XVIII (5), p. 279, 2025.
- 27 J. Hassan, A. Sohail, A. I. Awad, and M. A. Zaka. "Letm-iot: A lightweight and efficient trust mechanism for sybil attacks in internet of things networks", *Ad Hoc Networks*, CLXIII, p. 103576, 2024.
- 28 A. Verma, S. K. Verma, A. C. Pandey, J. Grover, and G. Sharma. "Li-msd: A lightweight mitigation solution for dao insider attack in rpl-based iot", *Future Generation Computer Systems*, CLIX, pp. 327-339, 2024.
- 29 A. Rullo, D. Midi, A. Mudjerikar, and E. Bertino. "Kalis2. 0-a secaas-based context-aware self-adaptive intrusion detection system for the iot", *IEEE Internet of Things Journal*, XI (7), pp. 12 579-12 601, 2024.
- 30 V. R. Vijaykumar, S.R. Sekar, R. Jothin, V. C. Diniesh, S. Elango, and S. Ramakrishnan. "Novel light weight hardware authentication protocol for resource constrained iot based devices", *IEEE Journal of Radio Frequency Identification*, VIII, pp. 31-42, 2024.
- 31 S. Bilgili, A. K. Demir, and S. Alam. "Ifnot: An approach towards mitigating interest flooding attacks in named data networking of things", *Internet of Things*, XXV, p. 101076, 2024.

- 32 M. Osman, J. He, N. Zhu, and F. M. M. Mokbal. "An ensemble learning framework for the detection of rpl attacks in iot networks based on the genetic feature selection approach", *Ad Hoc Networks*, CLII, p. 103331, 2024.
- 33 P. Bhale, S. Biswas, and S. Nandi. "A hybrid ids for detection and mitigation of sinkhole attack in 6lowpan networks", *International Journal of Information Security*, XXIII (2), pp. 915–934, 2024.
- 34 L. Sadineni, E. S. Pilli, and R. B. Battula. "Provlink-iot: A novel provenance model for link-layer forensics in iot networks", *Forensic Science International: Digital Investigation*, XLVI, p. 301600, 2023.
- 35 S. Goel, A. Verma, and V. K. Jain. "Cra-rpl: A novel lightweight challenge-response authentication-based technique for securing rpl against dropped dao attacks", *Computers & Security*, CXXXII, p. 103346, 2023.
- 36 Kamaldeep, M. Malik, and M. Dutta. "Feature engineering and machine learning framework for ddos attack detection in the standardized internet of things", *IEEE Internet of Things Journal*, X (10), pp. 8658–8669, 2023.
- 37 Z. Najafi and S. Babaie. "A lightweight hierarchical key management approach for internet of things", *Journal of Information Security and Applications*, LXXV, p. 103485, 2023.
- 38 W. Zhao, Y. Wang, W. Zhai, L. Liu, and Y. Liu. "Efficient time-delay attack detection based on node pruning and model fusion in iot networks", *Peer-to-Peer Networking and Applications*, XVI (2), pp. 1286–1309, 2023.
- 39 G. Sharma, J. Grover, and A. Verma. "Qsec-rpl: detection of version number attacks in rpl based mobile iot using q-learning", *Ad Hoc Networks*, CXLII, p. 103118, 2023.
- 40 F. K. "Ors and A. Levi. "Data driven intrusion detection for 6lowpan based iot systems", *Ad Hoc Networks*, CXLI, p. 103120, 2023.
- 41 J. H"oglund, M. Furuheid, and S. Raza. "Lightweight certificate revocation for low-power iot with end-to-end security", *Journal of Information Security and Applications*, LXXIII, p. 103424, 2023.
- 42 R. Alghamdi and M. Bellaiche. "A cascaded federated deep learning based framework for detecting wormhole attacks in iot networks", *Computers & Security*, CXXV, p. 103014, 2023.
- 43 S. Goel, A. Verma, and V. K. Jain. "A lightweight mitigation approach for addressing ddao attacks in rpl-based internet of things". In *Proceedings of the Fifteenth International Conference on Contemporary Computing*. ACM, pp. 580–586, 2023.
- 44 V. Rajasekar and S. Rajkumar. "A study on impact of dis flooding attack on rpl-based 6lowpan network", *Microprocessors and Microsystems*, XCIV, p. 104675, 2022.
- 45 P. Nandhini, S. Kuppuswami, S. Malliga, and R. DeviPriya. "A lightweight energy-efficient algorithm for mitigation and isolation of internal rank attackers in rpl based internet of things", *Computer Networks*, CCXVIII, p. 109391, 2022.
- 46 M. M. Sithik and B. M. Kumar. "Intelligent agent based virtual clustering and multi-context aware routing for congestion mitigation in secure rpl-iot environment", *Ad Hoc Networks*, CXXXVIII, p. 102972, 2022.
- 47 A. Bilal, S. M. N. Hasany, and A. H. Pitafi. "Effective modelling of sinkhole detection algorithm for edge-based internet of things (iot) sensing devices", *IET Communications*, XVI (8), pp. 845–855, 2022.
- 48 S. S. Dhanda, B. Singh, and P. Jindal. "Lightweight cryptography: a solution to secure iot", *Wireless Personal Communications*, CXII (3), pp. 1947–1980, 2020.
- 49 M. Ataulloh and N. Chauhan. "Exploring security and privacy enhancement technologies in the internet of things: A comprehensive review", *Security and Privacy*, VII (6), p. e448, 2024.
- 50 A. Rashid and T. Pecorella. "Is 6LoWPAN-ND necessary? (Spoiler alert: Yes)", *Computer Networks*, CCL, p. 110535, 2024.
- 51 C. Cervantes, D. Poplade, M. Nogueira, and A. Santos. "Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things". In *Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management (IM)*. IEEE, pp. 606–611, 2015.

- 52 M. Zaminkar and R. Fotohi. “Sos-rpl: securing internet of things against sinkhole attack using rpl protocol-based node rating and ranking mechanism”, *Wireless Personal Communications*, CXIV (2), pp. 1287–1312, 2020.
- 53 K. Prathapchandran and T. Janani. “A trust aware security mechanism to detect sinkhole attack in rpl-based iot environment using random forest–rfrtrust”, *Computer Networks*, CXCVIII, p. 108413, 2021.
- 54 M. Surendar and A. Umamakeswari. “Indres: An intrusion detection and response system for internet of things with 6lowpan”. In *Proceedings of the International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. *IEEE*, pp. 1903–1908, 2016.
- 55 A. Shiranzaei, E. Alizadeh, M. Rabbani, S. B. B. Ahmadi, and M. Tajgardan. “Nadsa: A novel approach for detection of sinkhole attacks based on rpl protocol in 6lowpan network”, *Computers, Materials & Continua*, LXXXIV (3), 2025.