A NOVEL ENERGY-EFFICIENT APPROACH TO DETECT AND MITIGATE RPL ROUTING ATTACKS IN IOT NETWORK

Deepak Upadhyay[1], Hiteishi Diwanji[2]

•

[1]Phd Scholar, Gujarat Technological University, Gujarat, India
[2]L. D. Government Engineering College, Gujarat, India
[1]ap_deepak@gtu.edu.in , [2]hiteishi.diwanji@gmail.com

Abstract

Communication networks are constantly at risk from routing attacks, which have the potential to disrupt the network performance, information flow and jeopardize network integrity. Network resources and Energy consumption attacks on the Internet of Things (IoT) are the main targets to bring down the services of Internet of Things devices with attacks such as Denial of Service, Jamming etc. Node mobility results in frequent changes to network topology. This increases energy consumption and reduces node lifetimes, which can disrupt overall network functionality. To overcome these problems the author has proposed a hybrid and lightweight A Novel Energy-Efficient Approach to Detect and Mitigate RPL (EEADM-RPL) protocol considering control messages with route metrics in different detection and mitigation algorithm to mitigate the Blackhole attack, Rank attack and Sybil attacks under mobility environment at a time. An attack scenario created with the algorithms for all attacks using control messages and attributes of packets. The EEADM-RPL protocol uses basic RPL control messages, neighbor table, trust calculation, and a minimum rank hysteresis objective function to detect and eliminate the attacks. This protocol is suitable for industrial systems to handle cyber-attack and for the Vulnerability Assessment and Penetration Testing audit. The Cooja simulator, part of the Contiki operating system, simulates the attacks without mobility and with mobility demonstrates the effectiveness affecting the network and the resources. The outcomes of the simulation are compared with those of current protocols. According to the data, the proposed protocol demonstrates improvements over the conventional RPL protocols in several metrics: the average parent change ratio by 87.94%, the average packet loss ratio by 69.17%, end-to-end latency by 67.85%, and both energy consumption and end-to-end delay by 13.07%.

Keywords: IoT Network Attacks, Sybil Attack, Rank Attack, Blackhole Attack, EEADM-RPL

I. Introduction

The widespread adoption of Internet of Things (IoT) devices has significantly transformed various sectors, ranging from residential smart homes to industrial automation. With the rapid rise in IoT device deployment, there is a heightened risk landscape with multiple security threats. Laghari [1] introduces one of the major concerns for the hybrid attacks in this area is Sybil attacks, which present serious challenges to the reliability and operation of IoT networks. Deceptive tactics are used by adversaries to create multiple fake identities to deceive systems and gain unauthorized access or

control. With the increasing number of IoT devices, the risk of Sybil attacks disrupting operations and compromising sensitive data also rises. Sasi et al. [2] referenced conventional approaches for identifying Sybil attacks in IoT environments frequently prove inadequate because of the ever-changing and intricate structure of these networks. Recent advancements in deep learning show promising potential for improving Sybil attack detection capabilities. Alfriehat et al. [3] utilized advanced learning methods, these techniques can effectively detect unusual behaviors that may signal security threats in IoT environments.

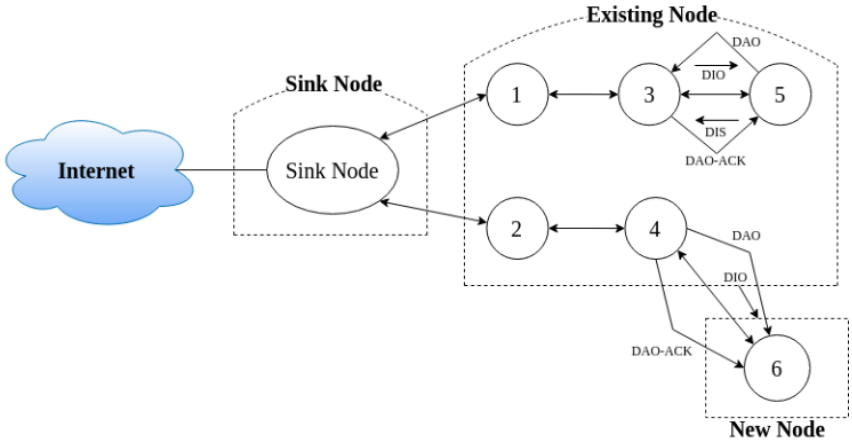

Figure 1: *RPL Graph*

Exploring the growing threat of Sybil attacks on IoT devices and investigating the use of deep learning tools for detection. Utilizing neural networks and sophisticated machine learning algorithms, our goal is to create a defense system that can detect and prevent Sybil attacks in real-time. Aldhaheri [4] study adds to the continuous work aimed at enhancing the security of IoT infrastructures, protecting them from advancing cyber threats in a world that is becoming more interconnected.

I. Motivation of EEADM-RPL Protocol

The dynamics within networks influence the convergence of routing protocols, as well as their organization and configuration, potentially compromising network operations. Considering node mobility, existing methods and protocols use cryptography, encryption, mathematical, decryption, rule-based, blockchain, and intrusion detection system (IDS) algorithms to identify and eliminate threats, primarily in a static environment. These techniques create overhead with the message and affect the performance to counter the mobility with high detection and mitigation solutions. This results in several challenges, including reduced throughput and packet delivery ratios, increased end-to-end delay, and ultimately diminishing the network's overall lifespan. These factors contribute to the potential failure of the entire network. In order to address these issues, the EEADM-RPL protocol is put out, which uses tiny byte-fag values, MRHOF, trickling timers, and basic RPL control messages to identify and lessen the threats. The primary objective of the proposed DE2RA-RPL protocol is to conserve energy.

II. Contribution of the EEADM-RPL Protocol

This EEADM-RPL protocol is proposed to handle the Blackhole attack, Rank attack and Sybil attack in a dynamic environment considering mobility of the nodes as malicious nodes for attacks. Majorly it affects more degradation of the performance of the network and more consumption of power can lead to failure of the network.

There are three algorithms in the proposed EEADM-RPL, including Detection and Mitigation of Blackhole Attack, Rank Attack and Sybil Attack for detecting and mitigating of Network Resource and Energy Consumption related attacks. The hybrid lightweight EEADM-RPL protocol comprises six algorithms that are distributed to every node within the DODAG environment. The EEADM-RPL protocol utilizes MRHOF, small byte flag values, a trickling timer, and standard RPL control messages to facilitate node mobility and mitigate potential attacks. The root node will not encounter any overhead. Additionally, nodes within the DODAG environment will not face any overhead, as the algorithms utilize lightweight packets that integrate with the existing RPL control messages. The Cooja simulation environment highlights two scenarios. In one, the EEADM-RPL protocol outperforms existing RPL-based protocols with immobile nodes. In the other, it shows superior performance with mobile malevolent nodes. Paganraj [5] aims the comparative results with existing protocols indicate that the EEADM-RPL protocol enhances throughput, reduces energy consumption, improves packet delivery ratio, and decreases end-to-end latency.

The structure of this document is as follows: Section 2 of the Attack Methodology presents an overview of the key concepts related to the Blackhole Attack, Rank Attack, and Sybil Attack. Section 3 offers an explanation of the Literature Survey. Section 4 contains a detailed discussion on the proposed EEADM-RPL protocol. Section 5 provides an analysis of the performance and simulation results. The document concludes with future work outlined in Section 6.

II. Attack Methodology

I. Blackhole Attack

In a Black Hole Attack, a malicious node within the network falsely advertises itself as possessing the optimal path to the target. This deceitful tactic causes other nodes to forward their packets to the attacker. Consequently, the data is effectively absorbed or discarded, hence the term "black hole". The malicious node exploits the RPL's route advertisement mechanism to inject incorrect routing information into the network. By manipulating control messages such as DODAG Information Objects (DIOs), the attacker can convince adjacent nodes to select it as their preferred parent node.

Algorithm	Black Hole Attack

Step 1: Let N represent the total number of nodes in the network.

Step 2: The malicious node as $M \in N$.

Step 3: Modify the DIO (DODAG Information Object) message such that:

- Rank(M) → ∞, where M advertises itself with a lower rank compared to legitimate nodes.
- The rank value for legitimate nodes, R, will satisfy the condition: $R_{legitimate} < R_M$ (where R_M is the rank of malicious node)
- $R_{legitimate} < R_M$ $R_{legitimate} < R_M$ The malicious node M sends a fake DIO advertisement with: $Rank_M \rightarrow 0$, $cost_M \rightarrow 0$
- For legitimate node L, $cost_L = 0$ and $Rank_L = 0$

Step 4: Alter packet forwarding logic Packet P arrives at node M,

P_M = Drop(P), if M is malicious; Forward(P), if M is legitimate

Step 5: Compile and flash the firmware

Step 6: M node behavior: ∀P, M, Drop(P)

$P_{dropped}$ = {P | Received by M, M drops P}

Step 7: M advertises itself with rank R_M and cost C_M.

$$P_{dropped} = \sum_{i=0}^{N} P_i \quad (1)$$

$$P_{loss} = \frac{P_{dropped}}{P_{total}} \quad (2)$$

$$\text{Throughput}_{attack} = \frac{P_{received}}{T_{total}}, \quad (3)$$

T_{total} is total simulation time

II. Rank Attack

Increasing Rank Attacks: Within the RPL protocol, the rank value increases from the root node to the child node. An attacker can manipulate this metric to attract significant traffic toward the root and induce child nodes to select malicious nodes as parents by altering the Rank value. Reduced Rank Attacks: In a destination-oriented directed acyclic graph (DODAG), nodes with lower ranks are responsible for handling greater traffic as they are positioned closer to the root. A malicious node may falsely claim superior performance by advertising a lower rank value than its actual capability.

Algorithm Rank Attack

Step 1: Initialize Simulator
S ← Start Simulator()
Step 2: Manipulate RPL protocol packets
Modify: Modules: {rpl_dag, rpl_icmp6, rpl_dio}
Step 3: Falsify Rank Value
$R_{falsified} \leftarrow R_{current} \pm \Delta R$
Step 4: Tamper DIO Rank
DIO_{Rank} = Replace ($Rank_{actual}$, $R_{falsified}$)
Step 5: Alter Sequence Numbers
$Seq_{modified} = Seq_{oroginal} + \in$
Step 6: Manipulate Neighbour Table
$N_{table} \leftarrow$ f ($N_{entries}$, Tampered Data)
Step 7: Deceive Nodes about Topology
$T_{misleading} \leftarrow$ g(Topology Info, False Metrics)
Step 8: Compile and Flash Firmware
$F_{compiled}$ = Compile(Modified Code) Deploy($F_{compiled}$)
Step 9: Execute Attack
$A_{execute} \leftarrow$ Run (Rank Attack Simulation)

III. Sybil Attack

A sybil attack involves the use of multiple logical entities on a single physical node, similar to a clone ID attack. Kumari et al. [6] experimented the type of attack which can take control of large portions of a network without requiring additional physical nodes.

Algorithm Sybil Attack

Step 1: Initialize Simulator
S ← Start Simulator()
Step 2: Implement Selective Forward Logic
Modify: Modules: {rpl_dag, rpl_icmp6, rpl_dio, rpl_neighbor, rpl_forward}
Step 3: Spoof Node Identity
$NodeID_{spoofed} \leftarrow$ Generate(FakeID)
$MAC_{spoofed} \leftarrow$ Generate(FakeMAC)
Step 4: Manipulate Neighbour Table
$N_{table} \leftarrow$ f ($N_{entries}$, Spoofed Nodes)

Step 5: Forge Routing Advertisements

Fake DIO:

DIO_{fake} ← Create (False Rank, False Routes)

Fake DAO:

DAO_{fake} ← Create (False Destinations)

Step 6: Compile and Flash Firmware

$F_{compiled}$ = Compile (Modified Code) Deploy(Fcompiled)

Step 7: Start Session in Simulator

$S_{session}$ ← Start(S)

Step 8: Execute Attack

$A_{execute}$ ← Run (Sybil Attack Simulation)

III. Literature Survey

This section reviews the methodologies proposed by various researchers for the identification and mitigation of Blackhole, DIS Flooding, Rank, Selective Forwarding, Sybil, and Version attacks.

The research expands the network scale to 50 nodes and evaluates performance metrics via Contiki Cooja, providing comprehensive insights. Sharma et al. [7] work compared with existing security solutions often ignore node mobility, which this study highlights as critical for realistic IoT scenarios. Verma [8] introduced the Li-MSD approach, a distributed, threshold-based detection algorithm that maintains neighbor and blacklist tables to identify and block attacker nodes efficiently. This research focuses on the impact of black hole attacks in lossy and low-power networks using the RPL protocol. Kumar et al. [9] demonstrates simulation-based analysis of attack behaviors and detection capabilities. Rank attacks are most harmful in network areas with many attacker nodes or heavy forwarding loads.

Le et al. [10] and Djedj ig et al. [11] study aims to find out the key indicators of rank attack effects include affected node count, end-to-end delay, and delivery ratio. MRTS incorporates a trust management scheme that evaluates nodes' behaviors to assign trust values. Simulation results show MRTS outperforms standard RPL in trustworthiness and security, especially as the number of malicious nodes grows.

The Routing Protocol for Low-Power and Lossy Networks (RPL), which is extensively utilized in Internet of Things (IoT) contexts, has security flaws that are addressed in this paper. Rouissat [12] experiment by promoting a fake low rank, the authors present a brand-new "silent decreased rank attack" that tricks the RPL's routing system and directs data traffic to a malicious node.

The study examines IoT security flaws, focusing on Sybil attacks where a malicious node uses multiple identities to disrupt network functions. Thuluva [13] aims to counter these attacks in IoT-based health monitoring systems, the authors propose a hybrid security framework using Caesar Cipher Algorithm (CCA), Lightweight Encryption Algorithm (LEA), and Received Signal Strength Indicator (RSSI).

IV. Proposed EEADM-RPL Protocol

Detection and Removal of DR Incidents:

The malicious node attracts additional nodes by broadcasting a DIO message with a low rank value. Upon receiving this message, new nodes calculate their rank using the Objective Function (OF). A node will select the parent with the lowest rank if it receives multiple DIO messages based on OF.

Operational functions are available in two distinct types.

1. This objective function is predicated on the minimal number of hops to the root and does not account for the reliability of the path links.
2. MRHOF, or the Minimum Rank Hysteresis Objective Function, aims to reduce the cost of the path by using either the link metric anticipated transmission count (ETX) or the node metric energy.

The rank value is determined by employing the MRHOF objective function. This approach involves two main actions: first, identifying the malicious nodes, and second, eliminating them. The non-storing mode technique serves as the basis for this procedure, ensuring that the root node maintains current information on every node.

I. Detection and Mitigation of Blackhole Attack

Algorithm	Black Hole Attack Mitigation

Step 1: Start
Step 2: Capture PCAP network traffic
Step 3: Extract Rank, Objective Function Code Position
Step 4: For all P_{node} and C_{node}, traverse F(flow) from R_{root} to L_{leaf}.
Step 5: Parse each packet P.
Step 6: Extract D_{RPL}, D_{ICMP6}, D_{IPv4}, $D_{6LoWPAND}$
Step 7: Perform StatAnalysis (LQI, RSSI, SensorRead, PktLen, PktType, PktLossRate, SeqNo, NeighborTbl)
Step 8: Wait for ΔStat.
If ΔStat=0: Activity=Normal
If ΔStat ≠ 0 : RaiseAalert.
Step 9: Detect Ablackhole using DDIS, PktSeqNo, NeighborTblUpdates, RSSI, LQI, Latency, RTT
Step 10: Set $T_{interval}$ = 1 min
Step 11: Check DDIS, PktSeqNo, NeighborTblUpdates, RSSI, LQI, Latency, RTT
If Δvalues=0: Add to T_{trust}
If Δvalues ≠ 0 : Add to $T_{malicious}$

II. Detection and Mitigation of Rank Attack

Algorithm	Rank Attack Mitigation

Step 1: Start
Step 2: Capture PCAP traffic.
Step 3: Extract Rank, Objective Function Code, Position For all P_{node} and C_{node} traverse F_{flow} from R_{root} to L_{leaf}.
Step 4: Parse each packet P.
Step 5: Extract DRPL, DICMP6, DIPv4, D6LoWPAND.
Step 6: Perform StatAnalysis (LQI, RSSI, Sensor Read, PktLen, PktType, PktLoss Rate, SeqNo, Neighbour Table)
Step 7: Wait for ΔState.
If ΔStat=0 : Activity=Normal.
If ΔStat ≠ 0 : Raise A_{alert}.
Step 8: Detect_ARankAttack using DRank, DDIOSQ.

Step 9: Set $T_{interval}$ = 1 min.
Step 10: Check D_{Rank}, D_{DIOSQ}.
If Δvalues=0: Add to T_{trust}.
If Δvalues ≠ 0 : Add to $T_{malicious}$

III. Detection and Mitigation of Sybil Attack

Algorithm Sybil Attack Mitigation

Step 1: Start
Step 2: Capture PCAP traffic.
Step 3: Extract Rank, Objective Function Code, Position For all P_{node} and C_{node} traverse F_{flow} from R_{root} to L_{leaf}.
Step 4: Parse each packet P.
Step 5: Extract D_{RPL}, D_{ICMP6}, D_{IPv4}, $D_{6LoWPAND}$.
Step 6: Perform StatAnalysis (LQI, RSSI, Sensor Read, PktLen, PktType, PktLoss Rate, SeqNo, Neighbour Table, Node IDs)
Step 7: Detects duplicate Node IDs in Neighbor Tbl.
Step 8: Identify nodes with:
- Same NodeID but different RSSI, LQI, or Pos.
- Multiple NodeIDs RSSI, LQI, or Pos.

Step 9: Check for ΔStat in:
- Packet frequency for the same NodeID.
- TrustScore inconsistencies.

If ΔStat=0: Activity=Normal.
If ΔStat ≠ 0 : Raise A_{alert}.

Step 10: Detect A Sybil Attack using:
- Duplicate NodeID with differing physical characteristics.
- Multiple NodeIDs sharing identical physical characteristics.

Step 11: In $T_{interval}$=1 min:
- Verify NodeID uniqueness with RSSI, LQI, SeqNo, PktFlowPath, TrustScore.

If Δvalues=0: Add to T_{trust}.
If Δvalues ≠ 0 : Add to $T_{malicious}$.

Step 12: Mitigation:
- Isolate nodes flagged in $T_{malicious}$.
- Update network routes to exclude flagged nodes.

V. Simulation Results and Performance Analysis

I. Simulation Environment

Simulations are employed to evaluate the performance of EEADM-RPL. For this purpose, Cooja, a simulator integrated within the Contiki operating system, is utilized. Triantafyllou et al. [14] study is compared with the evaluation as conducted under the environment and conditions specified in this study.

Table 1 presents the details of the simulation parameters.

Table 1: *Simulation Parameters*

Simulation Parameters	Value
Simulation tool	Contiki /Cooja 3.0
Simulation coverage area	100 m * 100 m
Deployment Type	Random position (based on smart home)
Total number of nodes	30
Emulated nodes	T-mote Sky
Malicious nodes	1:10
TX range	50 m
TX ratio	100%
RX ratio	30-100%
Link failure model	UDGM
Interference range	50 m
Routing protocols	THC-RPL
Mobility speed	0-6.23 km/h
Simulation time	60 min

Network internal security cannot be ensured by relying solely on the single metric used in standard RPL. Ferreira [15] and Singhal [16] studies have employed multiple matrices to integrate a security mechanism into the standard RPL. One internal security threat is the Sybil attack, which is addressed by methods that use matrices in the trust computation model. These methods employ node-level computation to determine the trust value. One consequence of node-level computation is high energy consumption, which affects low power and lossy IoT network devices.

The EEADM-RPL aims to minimize node-level computations and delegate trust computations to the Root node, which is a resourceful IoT device. The primary objective is to extend the operational lifespan of low-power lossy network devices by optimizing their energy consumption. Secondly, it performs these trust-related computations independently, without relying on any external devices. The simulation is conducted over a 20-minute duration, involving 30 nodes-one of which is malicious and another is mobile-utilized in the testing process.

The metrics used to evaluate EEADM-RPL include the number of Sybil attacks detected, the Packet Delivery Ratio (PDR), the average energy consumption of nodes, and the average energy consumption of the network.

To evaluate the performance of the work, a simulation was conducted in a smart home environment where various nodes may be mobile while one border router remains static.

II. Performance Analysis

i) Parent Change Ratio, ii) Packet Loss Ratio, iii) End-to-End Delay, iv) Energy Consumption, v) Network Lifetime, vi) Packet Delivery Ratio

The overall energy consumption of a node can be determined by summing the energy used for processing (CPU), low power mode (LPM), listening, and transmitting data. Therefore, the total energy consumption of a node is the aggregate of its energy usage during data transmission, data listening, CPU operation in low-power mode, and CPU operation in active mode.

VI. Experimental Results and Analysis

The Cooja simulator operating on the Contiki OS was utilized to conduct extensive simulations to evaluate the efficacy of the proposed EEADM-RPL protocol. In conditions with node mobility, the experimental setup included Sybil, Rank, and Blackhole attacks. Six critical network performance

metrics: Parent Change Ratio, Packet Loss Ratio, End-to-End Delay, Energy Consumption, Network Lifetime, and Packet Delivery Ratio -were employed to evaluate and compare the performance of EEADM-RPL with traditional RPL protocols (OF0, MRHOF, and DCTM-RPL).

I. Parent Change Ratio

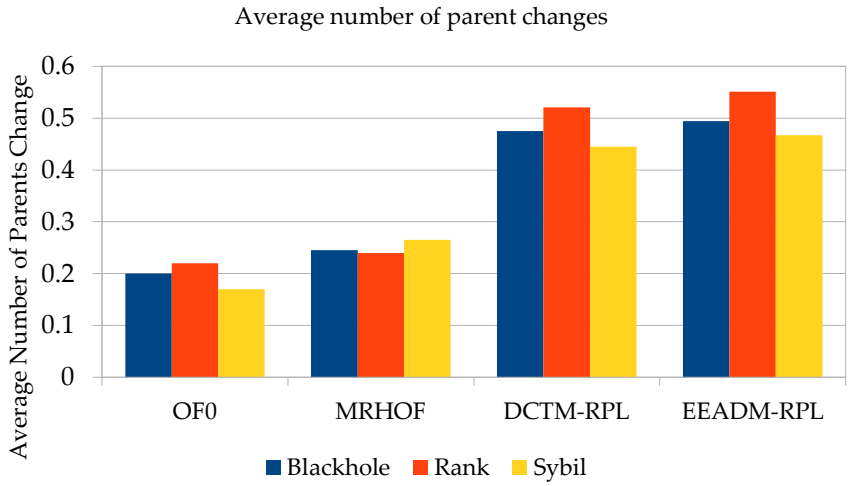

Figure 2: *Parent Change Ratio*

The Parent Change Ratio measures the frequency of switching parent nodes during data routing. Frequent parent changes indicate the instability of the routing protocol in dynamic conditions, such as during attacks or node mobility.

Our proposed EEADM-RPL protocol shows a substantial 87.94% increase in the average number of parent changes compared to traditional RPL protocols. This increase signifies better adaptability of the proposed protocol in mitigating attacks and re-establishing stable routes dynamically. The proactive parent selection helps maintain connectivity even in the presence of disruptive attacks like Blackhole and Sybil.

Table 2: *Parent Change Ratio*

Average number of parent changes	OF0	MRHOF	DCTM-RPL	EEADM-RPL
BLACKHOLE	0.2	0.245	0.475	0.494
RANK Attack	0.22	0.24	0.521	0.551
SYBIL	0.17	0.265	0.445	0.467

II. Packet Loss Ratio

The percentage of data packets that do not arrive at their destination is shown by the packet loss ratio. Poor dependability and heightened network vulnerability to attacks are indicated by a greater ratio.

The EEADM-RPL protocol demonstrates a 69.17% reduction in the average packet loss ratio. This significant improvement indicates the enhanced robustness and reliability of EEADM-RPL in securing data delivery. The detection and isolation mechanisms against malicious nodes help ensure that legitimate packets follow secure and verified routes.

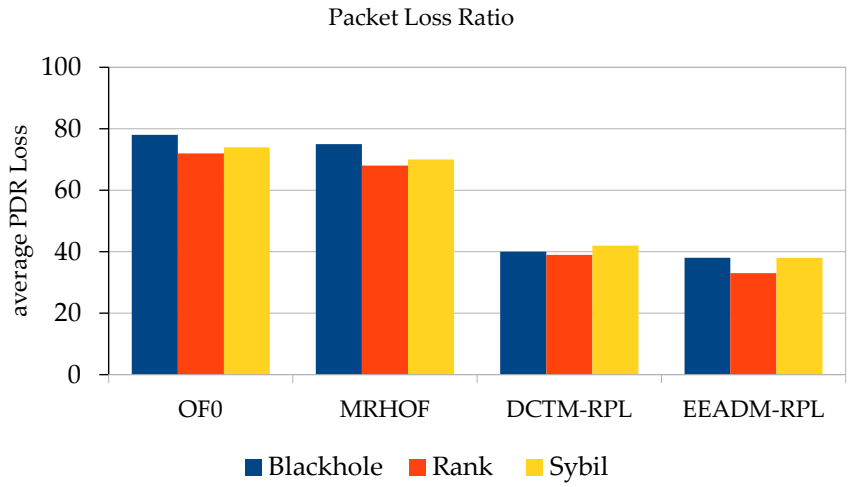

Figure 3: *Packet Loss Ratio*

Table 3: *Packet Loss Ratio*

Average Packet Loss Ratio	OF0	MRHOF	DCTM-RPL	EEADM-RPL
BLACKHOLE	78	75	40	38
RANK Attack	72	68	39	33
SYBIL	74	70	42	38

III. End-to-End Delay

Completely The amount of time it takes for a packet to go from its source to its destination is referred to as its delay. Delay reduction is essential for industrial and real-time Internet of Things applications. Simulation results show that EEADM-RPL achieves a 67.85% reduction in end-to-end delay. This drastic decrease is due to the optimized routing decisions and early detection of malicious behaviors, allowing for faster route recovery and minimal retransmissions. Additionally, this leads to improved quality of service (QoS) in dynamic IoT environments.

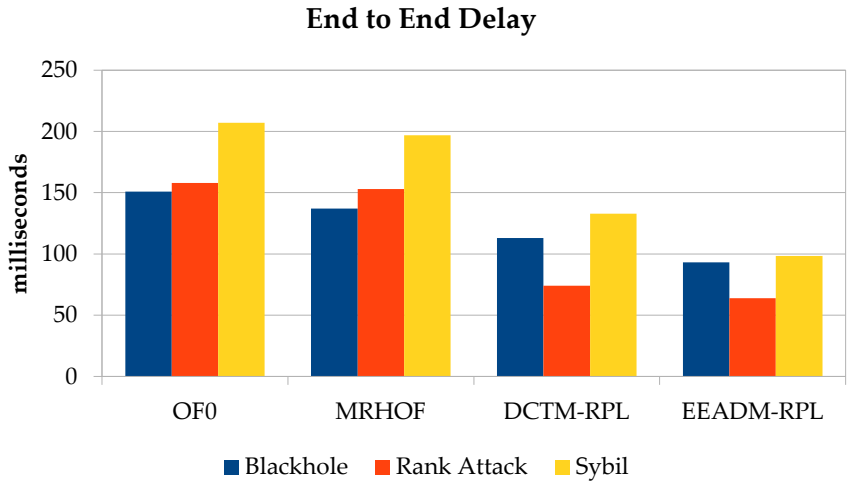

Figure 4: *End-to-End Delay*

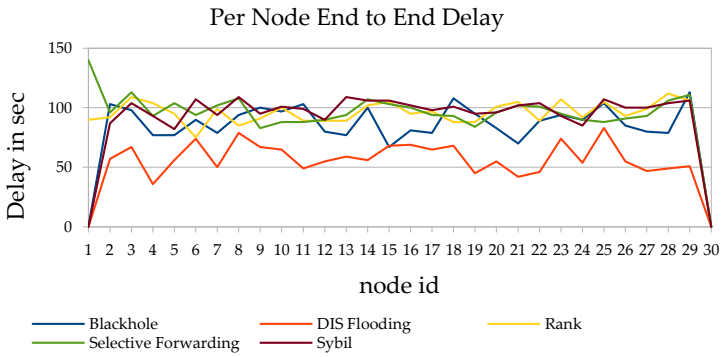

Figure 5: *Per node End-to-End Delay with mobility*

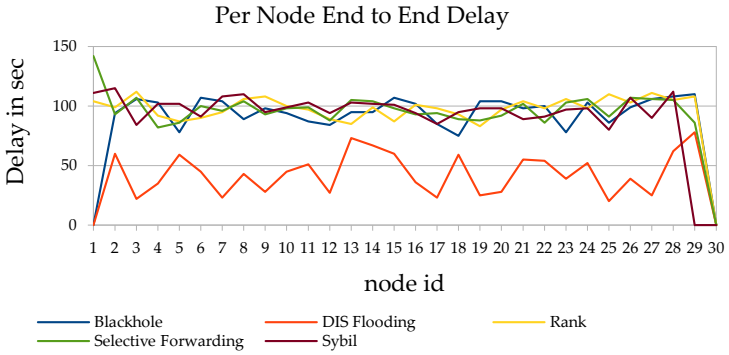

Figure 6: *Per node End-to-End Delay without mobility*

Table 4: *End-to-End Delay*

End-to-End Delay	OF0	MRHOF	DCTM-RPL	EEADM-RPL
BLACKHOLE	151	137	113	93.07
RANK Attack	158	153	74	63.79
SYBIL	207	197	133	98.36

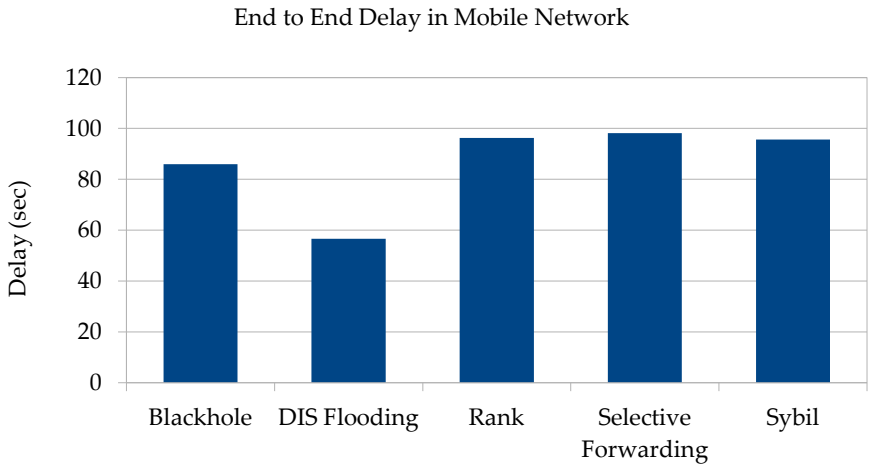

Figure 7: *End to End delay in mobile networks*

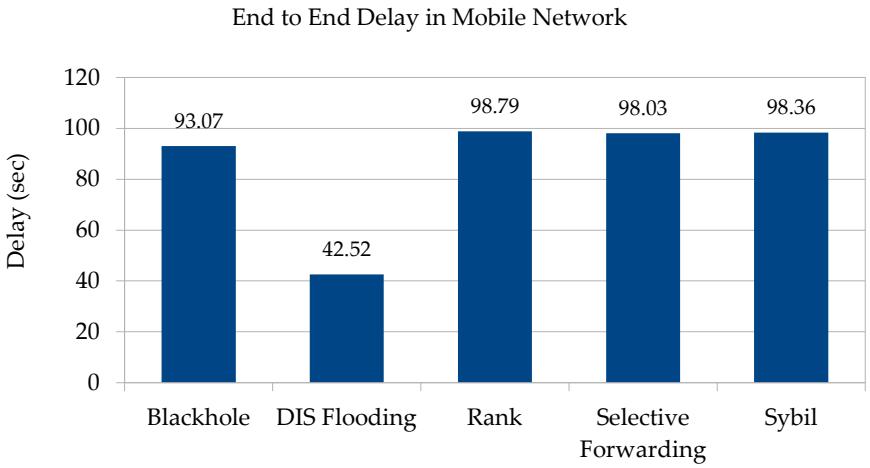

Figure 8: *End-to-End Delay in immobile networks*

IV. Energy Consumption

Energy efficiency is a key requirement in IoT environments where devices often operate on battery power. EEADM-RPL results in a 13.07% reduction in overall energy consumption compared to existing protocols. This improvement is achieved through the lightweight design of detection mechanisms, reduced retransmissions due to lower packet loss, and optimized control message exchanges.

By effectively mitigating attacks, the protocol reduces unnecessary energy usage caused by unstable routing paths.

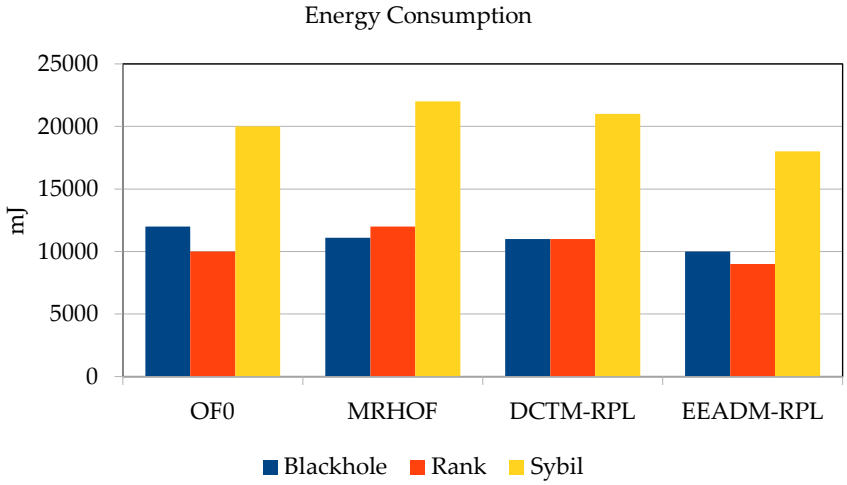

Figure 9: *Energy Consumption*

Table 5: *Energy Consumption*

Energy Consumption	OF0	MRHOF	DCTM-RPL	EEADM-RPL
BLACKHOLE	12000	11111	11000	10000
RANK Attack	10000	12000	11000	9000
SYBIL	20000	22000	21000	18000

V. Network Lifetime

A notable threat to mobile RPL is the Sybil attack, which can affect performance by significantly increasing control overhead transfer, thereby reducing the network's lifespan. Sybil attacks notably impact the network lifespan in mobile RPL-based IoT networks. These attacks lead to a substantial increase in node computation and control overhead traffic.

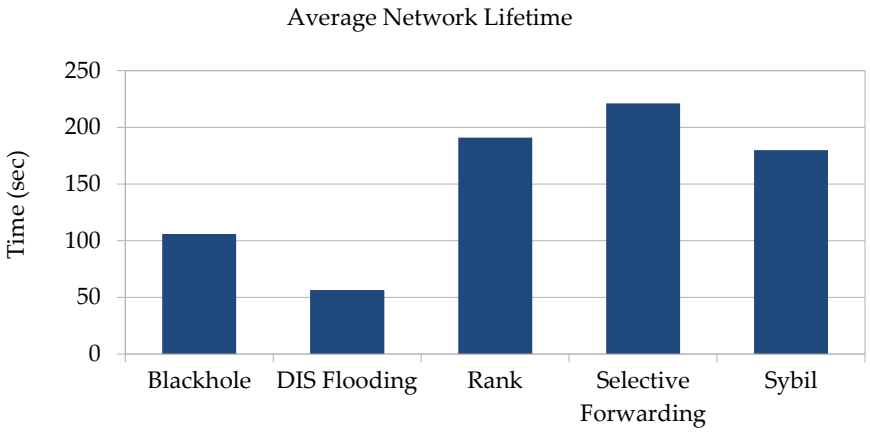

Figure 10: *Average Network Lifetime with mobility*

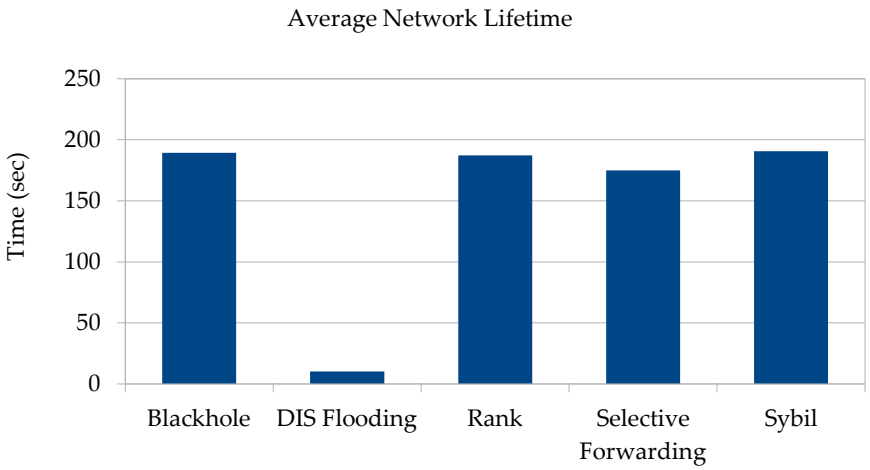

Figure 11: *Average Network Lifetime without mobility*

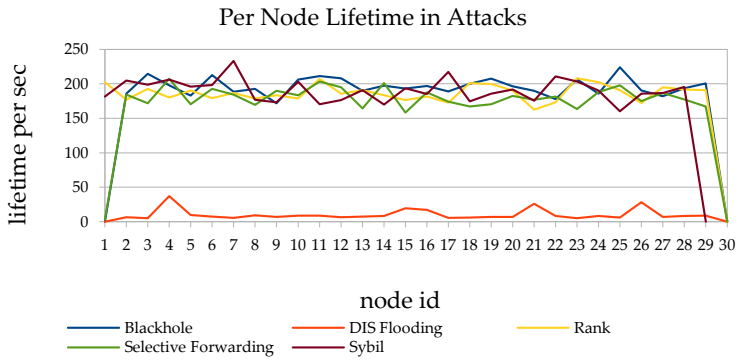

Figure 12: Per *Node Lifetime in Attacks with Mobility*

VI. Packet Delivery Ratio

Simulation scenarios indicate that Packet Delivery Ratio (PDR) can achieve up to 99% in networks with fewer nodes and a higher number of anchor connections. However, in denser network configurations, PDR values may be reduced to approximately 90%, due to increased congestion and transmission overlaps. Effective strategies for enhancing Packet Delivery Ratio (PDR) in mobile environments encompass selecting optimal parent nodes, minimizing disconnections, and ensuring consistent communication linkages.

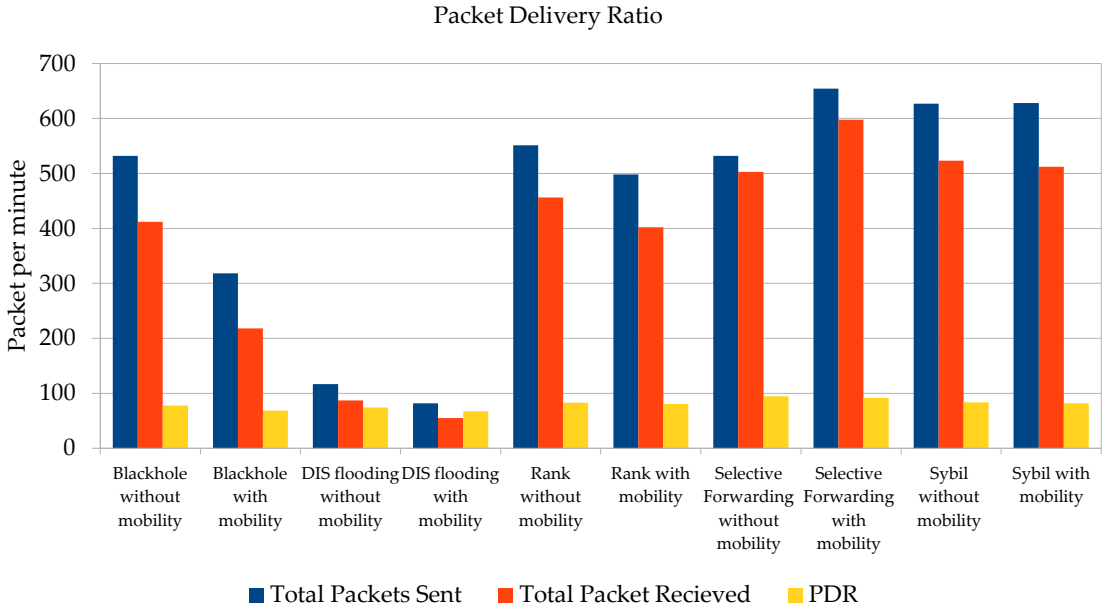

Figure 13: *Attack Types Parameter Packet Delivery Ratio with and without mobility*

VII. Conclusion

The Novel Energy-Efficient Approach to Detect and Mitigate RPL (EEADM-RPL) protocol presents a significant advancement in securing IoT networks against routing attacks while maintaining operational efficiency. Our comprehensive evaluation using the Cooja simulator demonstrates that the proposed protocol substantially outperforms traditional RPL implementations across all measured performance parameters. The hybrid approach effectively balances robust security mechanisms with network performance optimization and energy efficiency considerations. By increasing the average number of parent change ratio by 87.94%, decreasing the average packet loss ratio by 69.17%, decreasing the end-to-end delay by by 67.85%, and lowering energy consumption by 13.07%, EEADM-RPL addresses critical challenges in securing mobile IoT environments. The protocol's unique ability to handle multiple attack types simultaneously (Black Hole, Rank, and Sybil attacks) while maintaining performance under mobility conditions makes it particularly valuable for industrial IoT deployments where security and reliability are paramount concerns. Future research directions could explore further optimization of energy consumption for ultra-low-power applications, extension of attack detection capabilities to address emerging threat vectors, integration of machine learning-based anomaly detection mechanisms to enhance adaptability, and evaluation of protocol performance in larger-scale deployments with heterogeneous device types

and varying mobility patterns.

References

[1] Laghari, A. A., Li, H., Khan, A. A., Shoulin, Y., Karim, S., & Khani, M. A. K. (2024). Internet of Things (IoT) applications security trends and challenges. *Discover Internet of Things*, 4(1), 1–22.

[2] Sasi, T., Lashkari, A. H., Lu, R., Xiong, P., & Iqbal, S. (2024). A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges. *Journal of Information and Intelligence*, 2(6), 455–513.

[3] Alfriehat, N., Anbar, M., Aladaileh, M., Hasbullah, I., Shurbaji, T. A., Karuppayah, S., & Almomani, A. (2024). RPL-based attack detection approaches in IoT networks: review and taxonomy. *Artificial Intelligence Review*, 57(9), 1–56.

[4] Aldhaheri, A., Alwahedi, F., Ferrag, M. A., & Battah, A. (2024). Deep learning for cyber threat detection in IoT networks: A review. *Internet of Things and Cyber-Physical Systems*, 4, 110–128.

[5] Paganraj, D., & Chelliah, M. (2024). DE2RA-RPL: detection and elimination of resource-related attacks in IoT RPL-based protocol. *Journal of Supercomputing*, 80(15), 22397–22427.

[6] Kumari, D., Singh, K., & Manjul, M. (2020). Performance Evaluation of Sybil Attack in Cyber Physical System. *Procedia Computer Science*, 167, 1013–1027.

[7] Sharma, G., Grover, J., & Verma, A. (2023). Performance evaluation of mobile RPL-based IoT networks under version number attack. *Computer Communications*, 197, 12–22.

[8] Verma, A., Verma, S. K., Pandey, A. C., Grover, J., & Sharma, G. (2024). Li-MSD: A lightweight mitigation solution for DAO insider attack in RPL-based IoT. *Future Generation Computer Systems*, 159, 327–339.

[9] Kumar, A., Matam, R., & Shukla, S. (2016). Paper_23 Impact of packet dropping attacks on RPL. 2016 4th International Conference on Parallel, Distributed and Grid Computing, PDGC 2016, 694–698.

[10] Le, A., Loo, J., Lasebae, A., Vinel, A., Chen, Y., & Chai, M. (2013). The impact of rank attack on network topology of routing protocol for low-power and lossy networks. *IEEE Sensors Journal*, 13(10), 3685–3692.

[11] Djedjig, N., Tandjaoui, D., Medjek, F., & Romdhani, I. (2017). New trust metric for the RPL routing protocol. 2017 8th International Conference on Information and Communication Systems, ICICS 2017, 328–335.

[12] Rouissat, M., Belkheir, M., Belkhira, H. S. A., Mokaddem, A., & Ziani, D. (2023). Implementing and evaluating a new Silent Rank Attack in RPL-Contiki based IoT networks. *Journal of Electrical Engineering*, 74(6), 454–462.

[13] Thuluva, A. S. S., Somanathan, M. S., Somula, R., Sennan, S., & Burgos, D. (2021). Secure and efficient transmission of data based on Caesar Cipher Algorithm for Sybil attack in IoT. *Eurasip Journal on Advances in Signal Processing*, 2021(1), 1–23.

[14] Triantafyllou, A., Sarigiannidis, P., & Lagkas, T. D. (2018). Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges, and Trends. *Wireless Communications and Mobile Computing*, 2018(1), 5349894.

[15] Ferreira, A. M. A., Azevedo, L. J. de M. de, Estrella, J. C., & Delbem, A. C. B. (2023). Case Studies with the Contiki-NG Simulator to Design Strategies for Sensors' Communication Optimization in an IoT-Fog Ecosystem. *Sensors* 2023, Vol. 23, Page 2300, 23(4), 2300.

[16] Singhal, P., Singhal, P., Sharma, P., & Arora, D. (2018). An approach towards preventing iot based sybil attack based on contiki framework through cooja simulator. *International Journal of Engineering and Technology*, 7(2.8), 261–267.