Implementation of Rank Attack and Its Mitigation in RPL-Based IoT Networks

Madhu Yadav and Rajbir Kaur
Department of CSE, The LNMIIT, Jaipur, 302031, Rajasthan, India

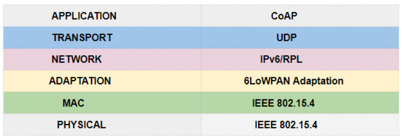
Keywords: IoT, LLN, RPL, Rank Attacks.

Abstract: The burgeoning interest in the Internet of Things (IoT) has led to the widespread deployment of Low-power and Lossy Networks (LLNs). The Routing Protocol for Low-Power and Lossy Networks (RPL) is a standard protocol designed for networks with resource-constrained devices and high packet loss rates. However, RPL is vulnerable to various attacks, particularly rank attacks, which can disrupt network performance and compromise security. This paper addresses this gap by implementing rank attacks in RPL using the Cooja Simulator in Contiki OS and analyzing their impact on network performance. While rank attacks are extensively discussed in the literature, practical implementations remain limited. To mitigate these attacks, we propose a novel trust-based mitigation strategy that integrates seamlessly with resource-constrained IoT devices. Our approach dynamically computes trust metrics to detect and isolate malicious nodes, thereby improving network security, reducing power consumption, and ensuring reliable packet transmission. Comparative analysis demonstrates the superiority of our approach over existing techniques, offering enhanced scalability and adaptability for secure IoT deployments.

1 INTRODUCTION

IoT devices operate under significant resource constraints, such as limited memory, power, and processing capabilities. Routing protocols are essential for efficient data transmission in IoT, with the *Routing Protocol for Low-Power and Lossy Networks (RPL)*—developed by the IETF RoLL working group (Baccelli and Philipp, 2013)—serving as a fundamental solution. RPL, integrated into the IoT protocol stack (Figure 1), works alongside IEEE 802.15.4 to enable interoperability and efficient communication in low-power wireless networks.

However, IoT faces significant security challenges due to its constrained nature, exposing devices and networks to various attacks that threaten data integrity and system functionality. Addressing these challenges is crucial for the secure and widespread deployment of IoT systems.



APPLICATION	CoAP
TRANSPORT	UDP
NETWORK	IPv6/RPL
ADAPTATION	6LoWPAN Adaptation
MAC	IEEE 802.15.4
PHYSICAL	IEEE 802.15.4

Figure 1: Overview of the IoT protocol stack.

The remainder of this paper is organized as follows: - Section 2 reviews related work on rank attacks and mitigation. - Section 3 introduces RPL and its role in IoT security. - Section 4 presents a taxonomy of RPL attacks with a focus on rank attacks. - Section 5 analyzes the simulation and impact of rank attacks. - Section 6 describes rank attack detection using a trust-based energy metric.

- Finally, Section 7 concludes with key findings and contributions.

2 RELATED WORK

RPL (Baccelli and Philipp, 2013) is vulnerable to rank attacks such as increase, decrease, and worst parent attacks, which degrade network performance by increasing energy consumption and reducing reliability (Mayzaud et al., 2016) (Raoof et al., 2018). Mitigation strategies include IDS (Simoglou et al., 2021), machine learning (Said et al., 2020), and trust-based methods (Liu, 2021). Approaches like SecTrust-RPL, DCTM (Hashemi and Aliee, 2019), and MRTS (Djedjig et al., 2020) improve energy efficiency and throughput. Statistical methods (Iuchi et al., 2015) and deep learning (Choukri et al., 2020) show promise

Yadav, M. and Kaur, R.
Implementation of Rank Attack and Its Mitigation in RPL-Based IoT Networks.
DOI: 10.5220/0013205100003944

In *Proceedings of the 10th International Conference on Internet of Things, Big Data and Security (IoTBDS 2025)*, pages 215-222
ISBN: 978-989-758-750-4; ISSN: 2184-4976

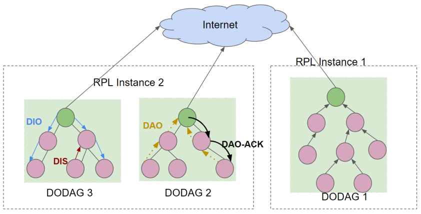


Figure 2: A network configuration with two RPL instances, and 3 DODAGs.

but face challenges. Our model focuses on energy efficiency and trust evaluation without relying on hardware or historical data, offering a lightweight solution for rank attack mitigation.

3 THE RPL PROTOCOL

The Routing Protocol for Low-Power and Lossy Networks (RPL) (Baccelli and Philipp, 2013) is a distance-vector protocol designed for resource-constrained devices in environments with high packet loss. It constructs Destination Oriented Directed Acyclic Graphs (DODAGs) combining tree and mesh structures, with multiple instances optimized for metrics like energy consumption. RPL uses four ICMPv6 control messages (DIS, DIO, DAO, DAO-ACK), and the trickle algorithm updates DIOs. Security is provided in three modes: Unsecured, Pre-Installed, and Authenticated. Despite these measures, security challenges persist, emphasizing the need for lightweight monitoring solutions. Figure 2 illustrates a network configuration with two RPL instances and three DODAGs.

4 RPL ATTACKS

The attacks are categorized into resource depletion, topology disruption, and traffic manipulation depending on the attacks' effect on the IoT network (Mayzaud et al., 2016). This taxonomy provides a concise overview of RPL attacks, aiding in understanding and mitigating potential threats to network security.

4.1 Resource Depletion Attacks

Resource depletion attacks aim to exhaust network resources such as bandwidth, memory, and energy. These attacks can disrupt normal network operations.

Rank Increase Attack increases energy consumption by influencing nodes to choose more distant nodes as parents. This is shown in (Figure 3(I)). Here, a malicious node 4 advertises a rank higher than node 2 and node 3, causing nodes 6, 7 and 8 to select a distant node 4 as their parent (Raoof et al., 2018).

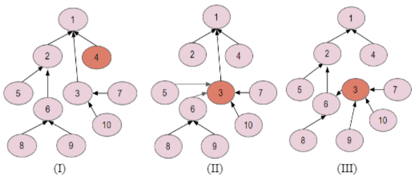


Figure 3: RPL attacks (I).Rank Increase Attack (II).Rank Decrease Attack (III).Worst Parent Attack

4.2 Traffic Manipulation Attacks

Traffic manipulation attacks in Low-Power and Lossy Networks (LLNs) occur when malicious entities disrupt data flow by creating fake identities or injecting malicious traffic.

Decrease Rank Attack involves advertising lower ranks to disrupt the normal traffic flow, causing suboptimal or incorrect routes. This manipulation can isolate nodes, impair communication, and potentially lead to network partitioning, resulting in traffic disruptions and degraded overall network performance. In (Figure 3(II)), a malicious node 3 advertises a lower rank than node 2 and node 4, causing one-hop neighbors of nodes 2 and 4 to choose the adversary as their preferred parent (Raoof et al., 2018).

4.3 Topology Disruption Attacks

Topology disruption attacks target the RPL network's structure, affecting the routing paths and overall communication within the network. Malicious nodes hinder optimal convergence and render nodes communication-incapable.

In **Worst Parent Attack**, malicious nodes manipulate parent selection, leading to suboptimal routing and disrupting the network's topology. In (Figure 3(III)), a malicious node 3 advertises its unmodified rank or a lower rank than its neighbors. The child nodes forward the data traffic to 3. Instead of forwarding the traffic to its legitimate parent (node 1), the malicious node 3 forwards the traffic to the adversary's worst parent 6 (assuming node 6 has the highest rank among node 3's neighbors) (Raoof et al., 2018).

5 RANK ATTACKS: SIMULATION AND ANALYSIS

We implement rank attacks using the Cooja simulator on Contiki OS, which supports TCP/IP, multithreading, and hardware abstraction. C programming and protothreads are used, with Cooja enabling code development. Java handles mote configuration, log analysis, and visualization, while XML configures simulations.

To evaluate the impact of rank attacks on network performance, we use several performance metrics that provide a comprehensive assessment of resource consumption within the Contiki OS and Cooja simulation environment.

Packet Delivery Ratio (PDR): Measures network reliability by calculating the ratio of received data packets to the total generated packets.

$$PDR = \left(\frac{\sum \text{packet received}}{\sum \text{packet sent}} \right) \times 100\%$$

Power Consumption: Quantifies the amount of energy consumed by a device in performing various operations in the network. We calculated power consumption using the Powertrace tool in Contiki OS, considering transmission, listening, CPU usage, and low-power mode.

Energy(mJ) = (Transmit × 19.5mA + Listen × 21.5mA + CPU × 1.8mA + LPM × 0.0545mA) × 3V / 32768

$$PowerConsumption(mW) = Energy(mJ)/Time(sec)$$

Our analysis includes the implementation of rank increase, rank decrease, and worst parent attacks. The simulation parameters configured in InstantContiki3.0/Cooja are detailed in Table 1.

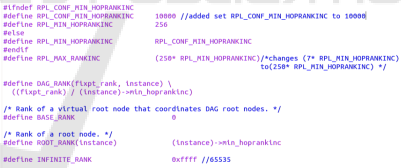
5.1 Rank Increase Attack

Specific modifications are needed in the source code to execute a rank increase attack in Contiki's RPL implementation, focusing on files in the ”contiki/core/net/rpl/” directory. In the ”rpl-private.h” file (Figure 4), which contains declarations and constants pertinent to the calculation of Directed Acyclic Graph (DAG) ranks, modifications need to be made to compromise the protective measures within the rank computation algorithm.

Moreover, within ”rpl-timers.c” (Figure 5), which oversees RPL timer functions, the segment of code responsible for managing node rank recalculations requires modifications to deactivate this process, thus maintaining the impact of the rank increase attack.

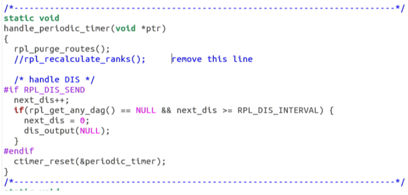
Table 1: Simulation Parameters.

Parameter	Value
Coverage Area	110m x 110m
Number of Nodes	8 normal and 1 Malicious in rank decrease attack, 12 normal and 1 malicious in rank increase and worst parent attack
Number of Nodes mitigation simulation	7 normal and 3 attacker, 3 malicious, 3 mitigation nodes
Node Placement	Random
Transmission Range	50m
Interference Range	60m
Transmission Ratio	100
Reception Ratio	30-100 (variable)
Routing Protocol	RPL
Network Protocol	IPv6
Simulation Start Delay	500 milliseconds
Radio Medium	UGDM Distance Loss
Simulation Duration	60 minutes for rank increase and rank decrease attack, 20 minutes for worst parent attack, 1 hour 12 minutes for rank attack mitigation



```
#ifndef RPL_CONF_MIN_HOPRANKINC
#define RPL_CONF_MIN_HOPRANKINC     10000 //added set RPL_CONF_MIN_HOPRANKINC to 10000
#define RPL_MIN_HOPRANKINC          256
#else
#define RPL_MIN_HOPRANKINC          RPL_CONF_MIN_HOPRANKINC
#endif
#define RPL_MAX_RANKINC             (250* RPL_MIN_HOPRANKINC)/*changes (7* RPL_MIN_HOPRANKINC)
                                                         to(250* RPL_MIN_HOPRANKINC) */

#define DAG_RANK(fixpt_rank, instance) \
  ((fixpt_rank) / (instance)->min_hoprankinc)

/* Rank of a virtual root node that coordinates DAG root nodes. */
#define BASE_RANK                       0

/* Rank of a root node. */
#define ROOT_RANK(instance)             (instance)->min_hoprankinc

#define INFINITE_RANK                   0xffff //65535
```

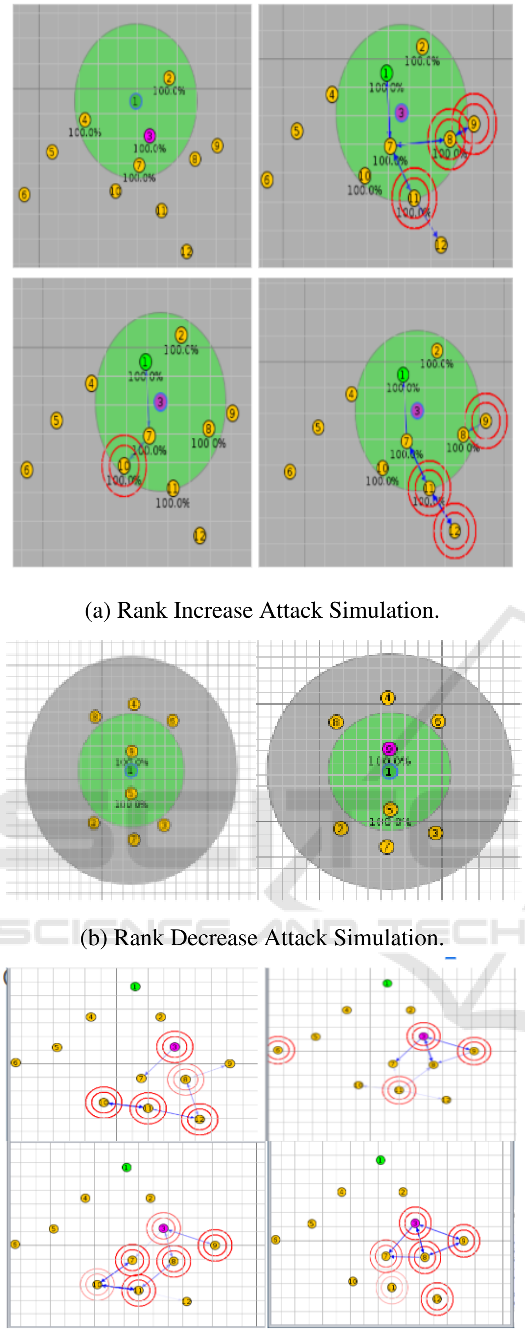
Figure 4: rpl private.h code modification.



```
/*---------------------------------------------------------------------------*/
static void
handle_periodic_timer(void *ptr)
{
  rpl_purge_routes();
  //rpl_recalculate_ranks();     remove this line

  /* handle DIS */
#if RPL_DIS_SEND
  next_dis++;
  if(rpl_get_any_dag() == NULL && next_dis >= RPL_DIS_INTERVAL) {
    next_dis = 0;
    dis_output(NULL);
  }
#endif
  ctimer_reset(&periodic_timer);
}
/*---------------------------------------------------------------------------*/
```

Figure 5: rpl timers.c code modification.

Figure 6a depicts the simulated network network for a rank increase attack in the Contiki/COOJA simulator. A green circle represents the transmission range of a node. Node 1 is designated as the sink node, while the remaining nodes act as normal sender nodes. Node 3 is identified as a malicious node. The blue lines connecting the nodes indicate potential radio communication. Double-outlined pink circles illustrate nodes sensing their neighboring nodes within the transmission range.



(a) Rank Increase Attack Simulation.

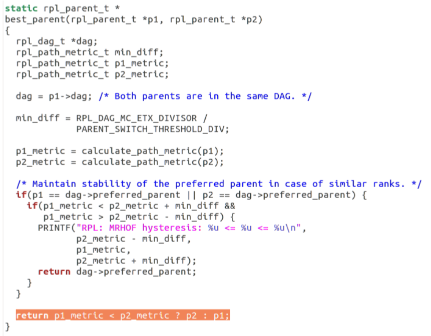
(b) Rank Decrease Attack Simulation.

(c) Worst Parent Attack Simulation.

Figure 6: Simulation Network.

5.2 Decrease Rank Attack

Similar changes are required in the files as mentioned above 5.1, to execute the rank decrease attack. The process is identical, involving modifications to constants declared in ”rpl-private.h” and disabling rank recalculation in ”rpl-timers.c”.



```
static rpl_parent_t *
best_parent(rpl_parent_t *p1, rpl_parent_t *p2)
{
  rpl_dag_t *dag;
  rpl_path_metric_t min_diff;
  rpl_path_metric_t p1_metric;
  rpl_path_metric_t p2_metric;

  dag = p1->dag; /* Both parents are in the same DAG. */

  min_diff = RPL_DAG_MC_ETX_DIVISOR /
             PARENT_SWITCH_THRESHOLD_DIV;

  p1_metric = calculate_path_metric(p1);
  p2_metric = calculate_path_metric(p2);

  /* Maintain stability of the preferred parent in case of similar ranks. */
  if(p1 == dag->preferred_parent || p2 == dag->preferred_parent) {
    if(p1_metric < p2_metric + min_diff &&
       p1_metric > p2_metric - min_diff) {
      PRINTF("RPL: MRHOF hysteresis: %u <= %u <= %u\n",
             p2_metric - min_diff,
             p1_metric,
             p2_metric + min_diff);
      return dag->preferred_parent;
    }
  }

  return p1_metric < p2_metric ? p2 : p1;
}
```

Figure 7: Modifications in rpl-mrhof.c.

Figure 6b illustrates the simulated network for a rank decrease attack in the Contiki/COOJA simulator. The left side of the figure represents the normal scenario with no malicious node. Node 1 is assigned as the sink node, and the remaining nodes function as normal sender nodes. Node 9 is identified as a malicious node on the right side of the figure. It intentionally discards packets originating from nodes 4, 6, and 8, leading to the isolation of these nodes and disruption of the network topology.

5.3 Worst Parent Attack

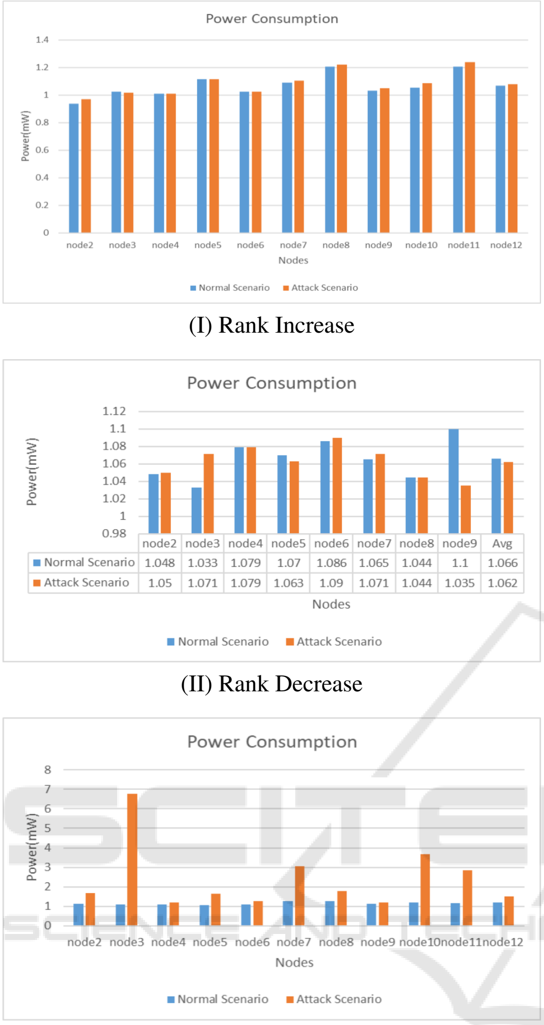
To simulate rank attacks in Contiki OS, we modified the metric evaluation function in the ”rpl-mrhof.c” (Figure 7) file. Specifically, we modified the ’best-parent’ function in the file. The parameters of the function are two nodes that are candidates for becoming the parent of a node. We modified the code to select the weakest candidate as the preferred parent. The ’rpl-select-parent()’ in ”rpl-dag.c” uses the outcome of the ’best-parent()’ function to determine the preferred parent in the DODAG structure.

Figure 6c presents the simulation network depicting a worst-parent attack in the Contiki/COOJA simulator. Node 1 is designated as the sink node, and the remaining nodes operate as normal sender nodes. Node 3 is marked as a malicious node. Instead of directing the packets toward the sink node, it intentionally routes them through the worst path, leading to delays and potential routing loops.

5.4 Analysis of the Effects of Rank Attacks

In this section, we analyze the effects of rank attacks on network performance parameters, such as the packet delivered at the sink and power consumption.

1. In a rank increase attack, malicious nodes intentionally manipulate the RPL (Routing Protocol



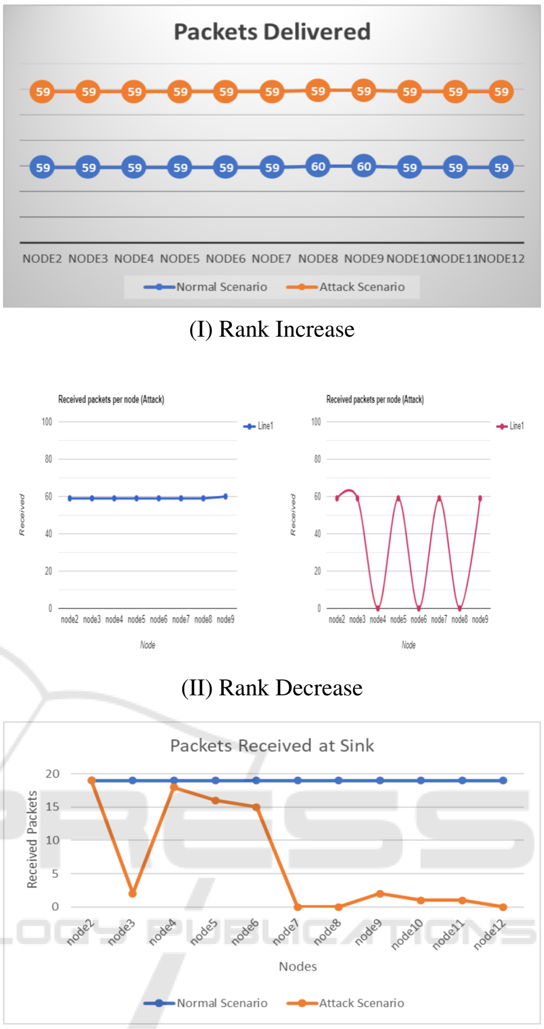
(I) Rank Increase

	node2	node3	node4	node5	node6	node7	node8	node9	Avg
Normal Scenario	1.048	1.033	1.079	1.07	1.086	1.065	1.044	1.1	1.066
Attack Scenario	1.05	1.071	1.079	1.063	1.09	1.071	1.044	1.035	1.062

(II) Rank Decrease

(III) Worst Parent

Figure 8: Power Consumption.



(I) Rank Increase

(II) Rank Decrease

(III) Worst Parent

Figure 9: Packet Delivered at Sink.

for Low-Power and Lossy Networks) by choosing suboptimal parents based on the objective function. This strategy increases energy consumption (Figure 8(I)) and overhead traffic in the network.(Figure 9 (I)) represents the packets delivered at the sink during the 60-minute simulation period in both normal and attack scenarios.

2. The rank decrease attack overloads the network, causing resource consumption attacks that drain node batteries(Figure 8 (II)) and congest the RPL network. The consequences include significant disruption in traffic and the RPL's DODAG (Destination Oriented Directed Acyclic Graph), with legitimate nodes connecting to the DODAG via the attacker. This diverts much traffic, disrupting the network's topology and reducing the packet delivery ratio(Figure 9 (II)).

3. The attacker's systematic selection of the least-preferred parent results in suboptimal paths and poor overall network performance, including high power consumption(Figure 8 (III)) and a low number of packets delivered at the sink(Figure 9 (III)). Furthermore, the attacker may use the decreased rank method to attract more nodes as parents, resulting in increased delays or routing loops. To summarize, the worst parent attack leads to network sub-optimization and heightened end-to-end delays.

Table 2: Comparison of Rank Attack Analysis and Mitigation Approaches in RPL-Based IoT Networks.

Criteria	**Our Approach**	**(Rouissat et al., 2023)**	**(Algahtani et al., 2021)**	**(A. Hkiri and Machhout, 2024)**
Attack Types Covered	Three rank-based attacks: rank increase, decrease, worst-parent.	Silent decreased rank attack only.	Covers multiple RPL attacks, no focus on rank-based attacks.	Decreased rank attack only.
Mitigation Strategy	Trust-based real-time mitigation to detect and isolate malicious nodes.	Lightweight countermeasure for silent decreased rank attack.	Simulation framework, no specific mitigation strategies.	No mitigation or real-time defense proposed.
Performance Metrics Evaluated	Energy, PDR, latency, overhead, and other metrics.	Energy, latency, and overhead only.	Focuses on generating data, not defense analysis.	PDR, throughput, and power consumption.
Attack Analysis and Mitigation Integration	Comprehensive analysis and integrated mitigation in real-world IoT scenarios.	Focus on single attack and countermeasure.	Attack simulation tools only, no integration of mitigation.	Focus on attack impact without practical defenses.

6 PROPOSED APPROACH: RANK ATTACKS MITIGATION

To enhance the security of the Routing Protocol for Low-Power and Lossy Networks (RPL) against rank attacks, we propose a Trust Energy-based countermeasure. We introduce a novel metric called ”Trust Energy” to assess the trustworthiness of nodes within the RPL network. The Trust Energy metric is calculated based on behavioral, communication, and security-related parameters. The block diagram in Figure 10 shows the steps of our proposed approach.

The following description outlines the steps:

1. Trust Energy Estimation:
   The Trust Energy ($Trust_i$) of a node is calculated as follows (Zhou and Gong, 2014):

   $$Trust_i = (1-\alpha)\cdot Energy_i + \beta \cdot PDR_i + \alpha \cdot Behavior_i + (1-\beta)\cdot Trustneighbor_{avg} \quad (1)$$

   Here, $Energy_i$ represents the energy level associated with node ’i’.
   $Trustneighbor_{avg}$ is average trust value recommended by neighboring nodes. This introduces a collaborative aspect where a node’s trust is influenced by the collective trustworthiness of its neighbors.

   The behavior of a node ($Behavior_i$) is calculated using the following parameters.

   - Successful Packet Delivery (PDRi): Reflects a node’s reliability in delivering packets. Higher success rates contribute positively to trust energy.
   - Adherence to Protocols (Behaviori): Nodes conforming to communication protocols and standards are deemed more trustworthy, emphasizing expected protocol behavior.
   - Reliability in Task Execution: Nodes consistently fulfilling responsibilities enhance trust energy.
   - Communication Analysis:
   - Communication Responsiveness: Swift responses to communication requests positively impact trust energy (Dahal and Shrestha, 2020).
   - Consistency in Communication Patterns: Monitoring and analyzing consistent communication patterns contribute to trust energy.
   - Communication Security Measures: Robust security measures, such as encryption and authentication, positively influence trust energy.
   - Security Credential Assessment:
   - Authentication and Authorization: Nodes with valid credentials and a clean security history boost trust energy.
   - History of Security Incidents: A node’s security incident history affects trust energy. The parameters α and β serve as weighting factors, allowing the adjustment of each factor’s influence on the overall trust computation. This comprehensive approach aims to create a nuanced evaluation of node trustworthiness, considering both individual and collective performance metrics.

2. Trust-based Route Selection: Nodes prioritize routes with higher trust energy to avoid compro-

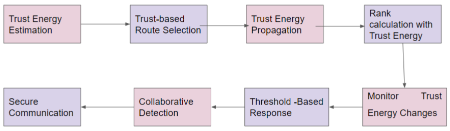

Trust Energy Estimation
Trust-based Route Selection
Trust Energy Propagation
Rank calculation with Trust Energy
Monitor Trust Energy Changes
Threshold -Based Response
Collaborative Detection
Secure Communication

Figure 10: Steps of Proposed Rank Attack Mitigation.

mised nodes, integrating trust metrics with standard Objective Function metrics.

3. Trust Energy Propagation: Nodes exchange trust energy values with neighbors (one-hop or two-hop), using secure protocols to prevent malicious activity.
4. Rank Calculation with Trust Energy: The Trust Energy Factor (TEF) is integrated into the RPL rank calculation (Santos-Boada and Hesselbach, 2019):

$$R = (DODAGRank \times mHRI) + minRankIncrease + \alpha \cdot TEF$$

5. Monitor Trust Energy Changes: Rapid drops in trust energy indicate attacks, and nodes with suspicious changes are isolated or rerouted (Airehrour et al., 2019).
6. Trust Energy Exchange: Nodes exchange trust energy values securely with neighbors (Gelogo et al., 2011).
7. Threshold Based Response: Nodes below a trust energy threshold trigger isolation and rerouting actions.
8. Collaborative Detection: Nodes detect and share rapid trust energy drops to improve attack detection (Airehrour et al., 2019).
9. Secure Communication: Secure protocols, including AES encryption and authentication, protect trust energy data (Ioulianou et al., 2022) (Raghavendra et al., 2022).

While Trust Energy-based countermeasures enhance security in RPL networks, a multi-layered strategy combining cryptographic methods, intrusion detection, and anomaly detection is vital for comprehensive protection (Zhang and Chen, 2018).

6.1 Simulation of Rank Attack Mitigation

- Figure 11 (I) depicts the simulated node network designed for detecting rank attacks. The network comprises four types of nodes: green nodes numbered from 1 to 7 serve as result nodes, acting as UDP sender nodes during bootstrapping. Following them are the rank attacker nodes (numbered 7 to 10) and malicious nodes (numbered 11 to 13), which attempt to manipulate rank values. However, mitigation nodes (numbered 14 to 16) isolate these attackers and redirect traffic through normal nodes. .

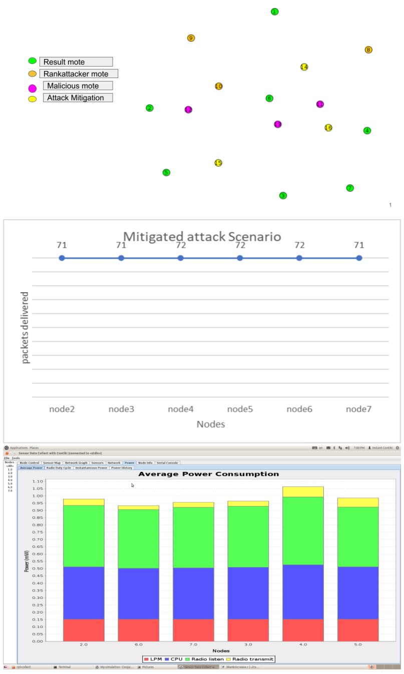


Figure 11: I.Simulation Network II.PDR III.Power Consumption.

- The proposed work aims to address attacker access and isolate them, leading to improved network packet transmissions (Figure 11 II). A collect view is initiated for node ID 1, and the snapshot (Figure 11 III) illustrates the power consumption of nodes, including CPU power, LPM power, Listen power, and Transmit power. This mitigation method boasts low power consumption and minimal computation time, thereby enhancing the security of the RPL network and ensuring proper packet transmission.

6.2 Comparative Analysis of Rank Attacks and Mitigation

This section compares various approaches to addressing rank-based attacks in RPL-based IoT networks, including **Our Approach**, (Rouissat et al., 2023), (Algahtani et al., 2021), and (A. Hkiri and Machhout, 2024).Our Approach provides a comprehensive solution for securing IoT networks by analyzing three rank-based attacks (increase, decrease, and worst-parent). It features a real-time dynamic trust-based mitigation strategy that ensures network security during attacks. Additionally, it evaluates multiple performance metrics, such as energy, PDR, and latency, to demonstrate how mitigation improves network performance. Furthermore, our Approach integrates both attack analysis and mitigation into a cohesive framework, offering a holistic solution for securing IoT networks. Table 2 provides a comparison of the discussed approaches.

7 CONCLUSION

This work analyzes the vulnerabilities of the Routing Protocol for Low-Power and Lossy Networks (RPL), focusing on rank-based attacks like rank increase, rank decrease, and worst-parent attacks. We find that rank-increase attacks raise energy consumption and overhead, leading to network overload, while rank-decrease attacks disrupt traffic and the RPL's Directed Acyclic Graph (DODAG), affecting packet delivery.

To improve security in low-power networks like IoT, we propose a trust energy-based mitigation for RPL, using trust energy for routing, anomaly detection, and defense. This approach enhances network resilience against rank-based attacks, providing dynamic security that adapts to evolving threats. Future work is necessary to refine and address emerging challenges.

REFERENCES

A. Hkiri, M. Karmani, O. B. B. A. M. M. F. H. A. and Machhout, M. (2024). Rpl-based iot networks under decreased rank attack: Performance analysis in static and mobile environments. *Faculty of Sciences of Monastir, Tunisia, and Taif University, Saudi Arabia*.

Airehrour, D., Gutierrez, J., and Ray, S. (2019). Sectrust-rpl: A secure trust-aware rpl routing protocol for internet of things. *Future Generation Computer Systems*, 93:860–876.

Algahtani, F., Tryfonas, T., and Oikonomou, G. (2021). A reference implementation for rpl attacks using contiking and cooja. In *Proceedings of the 2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pages 280–286, Pafos, Cyprus.

Baccelli, E. and Philipp, M. (2013). The rpl routing protocol for low-power and lossy networks. Technical report, IETF RFC 6550.

Choukri, W., Lamaazi, H., and Bena, N. (2020). Rpl rank attack detection using deep learning. In *3rd ICT International Conference*, pages 1–6.

Dahal, S. and Shrestha, P. (2020). A comprehensive survey of trust management systems in low-power and lossy networks. *IEEE Access*, 8:148484–148514.

Djedjig, N., Tandjaoui, D., Medjek, F., and Romdhani, I. (2020). Trust-aware and cooperative routing protocol for iot security. *Journal of Information Security Applications*, 52:102467.

Gelogo, Y., Caytiles, R., and Park, B. J. (2011). Threats and security analysis for enhanced secure neighbor discovery protocol (send) of ipv6 ndp security. *International Journal of Security*, 4:179–184.

Hashemi, S. and Aliee, F. S. (2019). Dynamic and comprehensive trust model for iot and its integration into rpl. *Journal of Supercomputing*, 75:3555–3584.

Ioulianou, P., Vassilakis, V., and Shahandashti, S. (2022). A trust-based intrusion detection system for rpl networks: Detecting a combination of rank and blackhole attacks. *Journal of Cybersecurity and Privacy*, 2:124–152.

Iuchi, K., Matsunaga, T., Toyoda, K., and Sasase, I. (2015). Secure parent node selection scheme in route construction to exclude attacking nodes from rpl network. In *Proc. 21st Asia–Pac. Conf. Commun. (APCC)*, pages 299–303.

Liu (2021). A detection framework against cpma attack based on trust evaluation and machine learning in iot network. *IEEE Internet of Things Journal*, 8:15249–15258.

Mayzaud, A., Rémi, B., and I., C. (2016). A taxonomy of attacks in rpl-based internet of things. *18*.

Raghavendra, T., Anand, M., Munuswamy, S., Kalidoss, T., Svn, S. K., and Arputharaj, K. (2022). An intelligent rpl attack detection using machine learning-based intrusion detection system for internet of things. *Procedia Computer Science*, 215:61–70.

Raoof, A., Ashraf, M., and Horng, L. C. (2018). Routing attacks and mitigation methods for rpl-based internet of things. *IEEE Communications Surveys Tutorials*, pages 1–11.

Rouissat, M., Belkheir, M., Belkhira, S. A. H., Mokaddem, A., and Ziani, D. (2023). Implementing and evaluating a new silent rank attack in rpl-contiki based iot networks. *Journal of Electrical Engineering*, 74:454–462.

Said, A., Aymen, Y., Faicel, Y., and Takoua, A. (2020). Machine learning-based rank attack detection for smart hospital infrastructure. In *Proceedings of the International Conference*.

Santos-Boada, G. and Hesselbach, X. (2019). Trust management for rpl-based networks: A comprehensive survey. *Sensors*, 19(24):5385.

Simoglou, G., Violettas, G., Petridou, S., and Mamatas, L. (2021). Intrusion detection systems for rpl security: A comparative analysis. *Computers Security*, 104:102219.

Zhang, Z. and Chen, H. (2018). A survey of trust management in the internet of things. *IEEE Access*, 6:76007–76020.

Zhou, L. and Gong, H. (2014). Trust-based secure routing for rpl in low-power and lossy networks. *IEEE Transactions on Parallel and Distributed Systems*, 25(9):2297–2306.