Development of an Adaptive Strategy for Detecting and Mitigating Rank Attacks Wireless Sensor Networks

Fakehinde Emmanuel Iyanuoluwa

Department of Electrical and Electronic Engineering, University of Ibadan

DOI: https://doi.org/10.51244/IJRSI.2026.1307000372

Received: 06 August 2026; Accepted: 12 August 2026; Published: 19 August 2026

ABSTRACT

Rank attacks take advantage of the rank-based topology provided by the RPL (Routing Protocol for Low-Power and Lossy Networks) which interferes with the routing process of data transmission, leading to the decline in packet delivery and reliability of 6TiSCH networks. The aim of this study is to propose a framework called Adaptive Anomaly Detection with Objective Function Switching (ADAOFS) which facilitates the identification of rank attacks and provides an efficient solution to this problem while ensuring the safety, reliability, and energy efficiency of the network. An experimental approach with the use of Cooja/Contiki for modeling RPL- based 6TiSCH networks was utilized. In this experiment, the size of the network, deployment patterns utilized, and attack intensity were taken into consideration. The use of machine learning techniques allowed identifying anomalous routing activities. The adaptive objective function switching contributed to routing decisions. Performance was assessed with the help of PDR, energy consumption, and latency. The results demonstrated that both diminished and combined attacks may harm performance significantly, that is why ADAOFS remained effective in maintaining stable delivery of packets with a high level of energy efficiency (91.9) and short latency (17.2 ms).

Keywords: RPL Security, Rank Attacks, 6TiSCH Networks, Adaptive Anomaly Detection

INTRODUCTION

Smart Internet of Things is the outcome of the seamless integration of devices between wireless communications and diverse technologies. The Internet of Things (IoT) results from the unobtrusive use of devices between wireless communications and multiple technologies. The devices can sense their environment and collect data from their environment for processing and decision making (Ghosh et al., 2023). The smart city is one of the large areas of IoT. A smart city includes countless services and applications to improve quality of life and services to residents. Yet the devices transmit at the network layer in the IoT architecture. The environmental and traffic data can be relayed using different technologies, standards and protocols, like Routing Protocol for Low- Power and Lossy networks (RPL), supported protocols to enable a safe transfer of data packets between devices. RPL was designed to support the functions of the many link- layer protocols (Musaddiq et al., 2020). It is capable of using alternative routes and accommodating disruptions to the network during operation by evoking the alternate routes when default routes may not be available. RPL can also determine the best route to inform definition of the parent and neighbor nodes through the use of its Objective Functions (OF) (Kharrufa et al., 2019).

Even with its resilient design, the RPL protocol faces unique issues in dynamic and often aggressive smart city infrastructures. The potential weaknesses of IoT devices; limited computational ability, memory, and energy levels, with the urgency of the data they carry, expose them to multitude of performance and security threats. The selection of a valid path based on the Objective Function (OF) is a necessary procedure that can potentially exposed to common interference from disreputable nodes invoking rank or version number attack, or simply inefficient as the wireless links are inconsistent. Therefore, addressing the challenges of RPL's routing mechanism in an effort to improve the reliability and security monitoring networks as they disrupt topology becomes a priority, even ensuring that the new adaptation acknowledges other critical performance metrics such as latency, packet delivery ratio, and energy consumption as consideration in the routing

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

functions In this research, a new model called Adaptive objective function switching for anomaly detection (ADAOFS), would be created based on developing intelligent anomaly detection in conjunction with a dynamic switching mechanism that can adaptively change routing objective functions whenever some anomaly is detected.

This research is aimed at the design of an anomaly detection framework that can detect abnormal routing behavior and inconsistencies in node rank and a mechanism for adaptively switching routing decisions and parent selection criteria based on detected anomalies in order to achieve a balance between reliability, energy efficiency, and security. The integration of both anomaly detection and adaptive switching into one unified architecture will be referred to herein as ADAOFS architecture. The ADAOFS will allow for continuous monitoring, detection, and mitigation in accordance with the scheduling mechanism of the 6TiSCH. The performance of the ADAOFS will be evaluated through simulated scenarios of RPL-based 6TiSCH using performance metrics such as packet delivery ratio, control overhead, energy used, and detection accuracy

Related Works

There are many researchers who have developed different methods to prevent intrusions within networks (Aydin et al., 2025; Ghaleb et al., 2023; Karmakar et al., 2021; Rafea & Kadhim, 2019), including LEADER, Sec-OF, ETRPL, and DeMiRaR-6T. Although IDSs and ML-based anomaly detection can be used to detect and identify patterns of abnormal behavior, they cannot proactively protect against an intrusion [8]. In addition to these defense mechanisms, Rafea and Kadhim (2019) and Ghaleb et al. (2023) noted that RPL routing has two main trends; security aware and energy aware objective functions. Security-aware objective functions provide resiliency by adding defensive attributes directly into the RPL routing decision process to prevent attacks on topology and rank. Energy-aware objective functions support network longevity by using metrics like residual energy to control the selection of superior, ensuring that the energy load is balanced across the nodes, so that none of the nodes runs out of energy prematurely (Ghaleb et al., 2023; Karmakar et al., 2021).

The expansion of the Internet of Things (IoT) has allowed for widespread development of low-power and low-bandwidth applications in fields such as industrial automation, monitoring of infrastructure, healthcare and environmental monitoring. A key component of many large-scale deployments of the IoT is the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL). When RPL is used with the 6TiSCH protocol they provide an important enhancement to allow for reliable, timely and scalable communication in those large-scale deployments. However, combining the two protocols raises serious security issues. An example of this is the threat posed by rank attacks which can disrupt the topology of the underlying network and hinder the ability for the delivery of data and the operational integrity of the network (Hosni et al., 2020). The use of objective functions in RPL to determine route selection and to assign ranks to the nodes contributes significantly to the vulnerability of the security of RPL through its use of the rank attribute, which is how RPL identifies how far a node is from the root node in a destination-oriented directed acyclic graph, also known as a DAG (Boudouaia et al., 2020). The rank attribute is one of the significant attack surfaces of RPL and it has been determined that rank manipulation is one of the most significant threats to the overall integrity of RPL

One of the most harmful attack types against RPL is rank manipulation, which has developed into a prominent attack type. As discussed by Boudouaia et al. (2020), they have created a formal classification system for rank attack techniques via their review of the literature related to rank attack techniques, providing criteria for these rank attacks to be divided into subclasses based upon the nature of their interactions with the RPL Network Directional Acyclic Graph (DAG). Different subclasses of rank attacks not only relate to different ranks but also alter RPL performance metrics differently, such as the packet delivery ratio. The research of Rouissat et al. (2024) has expanded on the severity of these attacks and demonstrates how to create maximum disruption through a hybrid attack model through an integrated attack strategy combining multiple rank manipulation strategies. Simulation results indicated a substantial increase in management traffic when compared with non-attack operating conditions.

Ghaleb et al. (2023) developed the Secure Objective Function (Sec-OF) in response to these threats, which are based upon two theoretical foundations: Hop-Count Consistency's prevention of contradictory rank decrements and the use of Rank Thresholds to limit the frequency of switching between parents and, consequently, to

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

stabilise network topologies. Karmakar et al. (2021) proposed the LEADER protocol, which uses cryptocurrency to establish a secure binding between a node's rank and its parent's rank when routing messages to ensure that a trusted root node can validate the ranks of nodes throughout the network. In the RPL routing protocol, the Objective Function (OF) is the main decision-making mechanism for selecting parents and calculating ranks. The two standard objective functions (OF0 and MRHOF), which have been proposed to optimise performance through different performance metrics, also suffer from the "rich-get-richer" phenomenon, which improves the quality of nodes by creating an imbalance between higher quality nodes and lower quality nodes and negatively affects the rate of energy depletion of higher quality nodes (Rafea & Kadhim, 2019).

To overcome this limitation, energy-aware objective functions were proposed. The Energy-aware routing protocol with the Lowest Energy Metric (ETRPL) integrates residual energy and the expected transmission count (ETX) to provide a better way of balancing energy across the network (Alilou et al., 2024). In addition, new audience routes (security-based) also provide a way to determine the routes by adding defensive capabilities directly into the routing decision. This method is intended to maintain a topological consistency throughout the network while limiting the effect of using manipulated routing to cause disorganization (Ghaleb et al., 2023). While there are several advancements in each area, many challenges that remain unresolved still exist with each. Many proposals have only been evaluated using small simulations, in a static environment that does not consider conditions like node mobility, dynamic link quality, and large-scale deployments, but still create uncertainty for an application's ability to work in the real world of IoT (Boudouaia et al., 2021; Mitchel et al., 2020). One of the largest challenges with existing solutions is that they treat detection and mitigation as two separate processes rather than integrating them into a single security framework. Current areas of investigation involve more adaptive and integrated architectures for security. Machine-learning (based-anomaly) detection systems can identify malicious activity through the detection of statistical deviation from the normal behavior of the network (Aguilera, 2025). While these systems can detect attacks that have not been previously detected, they generally have a high incidence of false positives due to the methodologies used to detect malicious activity.

Adaofs

ADAOFS Architecture Design and Integration

The ADAOFS architecture works within the RPL over 6TiSCH stack. Each node maintains a routing table and periodically sends DODAG Information Object (DIO) messages containing Rank, Expected Transmission Count (ETX), and energy-based indicators. The anomaly detection engine only tracks these parameters and classifies network states as normal or malicious.

Let N be the set of sensor nodes, where each node n_i maintains a parent list $P_i \subseteq N$

$$N = \{n_1, n_2, \dots, n_m\} \quad 1$$

The rank of node,

n_i *at time t is computed following the standard RPL specification*:

$$Rank(n_i, t) = Rank(p_i, t) + Rank(n_i, p_i) \quad 2$$

Where p_i is the preferred parent and Step (·) is a function of hop count. During normal operation, the rank relationship obeys:

$$Rank(n_i, t) > Rank(p_i, t) \quad 3$$

However, in rank attack, malicious nodes artificially advertise low ranks to attract routing traffic, thereby violating the Rank monotonicity condition:

$$Rank(n_i, t) \leq Rank(p_i, t) \quad 4$$

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

Detection and mitigation of this anomaly form the foundation of ADAOFS.

Cooja/Contiki protocol is used to facilitate simulations of a 6TiSCH network. Each of the nodes is logging its behavior with this alternative malicious node in one of a normal or rank attack state. The following important metrics was taken at each time value t_k.

The dataset D is then defined as:

$$D = \{(x1, y1), (x2, y2), \dots, (xn, yn)\} \quad 5$$

Where each feature vector

$$x_i = [R_i, E_i, C_i, En_i, PDR_i, CO_i, D_i] \quad 6$$

And $y_i \in \{0,1\}$ represents the class label (0= normal, 1 = anomalous)

Anomaly Detection in the RPL-Based Network

The component that detects anomalies takes advantage of supervised and unsupervised learning models including Random Forest (RF), Support Vector Machine (SVM), and Autoencoder Neural Networks (AE).

For a classifier f_θ parameterized by θ, the model learns a mapping:

$$f_\theta: X \rightarrow Y \quad 7$$

An anomaly score S_i is computed as:

$$S_i = \|x_i - \hat{x}_i\|_2 \quad 8$$

And a threshold τ is established empirically:

Models are also evaluated using standard metrics:

Adaptive Objective Function Formulation

After the detection of an anomaly, ADAOFS dynamically adjusts the Objective Function (OF) of the affected node in order to reduce routing vulnerability. The following describes three objective functions.

Reliability-Oriented OF (OF_R)

$$Cost_R^{(i)} = \alpha_1 \times ETX_i + \alpha_2 \times D_i \quad 9$$

Energy-Oriented OF (OF_E)

$$Cost_E^{(i)} = \beta_1 \times \frac{1}{En_i} + \beta_2 \times C_i \quad 10$$

Security-Aware OF (OF_S)

$$Cost_S^{(i)} = \gamma_1 \times A_i + \gamma_2 \times CO_i \quad 11$$

Where A_i denotes anomaly likelihood score (output of ML detection).

The three objective cost equations, Cost_R(i), Cost_E(i), Cost_S(i), represents different parent-selection schemes in the ADAOFS framework, each attempting to achieve a measure of balancing particular network metrics through weighted coefficients (α, β, γ). In the context of the Reliability Objective Function (OF), α_1 and α_2 represent the tradeoff between link quality (ETX) against delay; in the Energy OF, β_1 and β_2 are responsible

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

for tradeoffs between remaining residual energy and that of the transmission cost; whereas in the Security-Aware OF γ_1 and γ_2 weigh the likelihood of an anomaly occurring and overhead for managing control. To get meaningful weights, all metrics must first be normalized and then proceed to equivalently ranges (ex.0–1). This, along with the coefficients, can be tuned automatically via machine learning, to get in line with network priorities regarding reliability, energy efficiency or security.

The adaptive composite objective function is formulated as:

$$OF_{ADAOFS}(i) = w_1 \times OF_R(i) + w_2 \times OF_E(i) + w_3 \times OF_S(i) \quad 12$$

Subject to:

$$w_1 + w_2 + w_3 = 1 \text{ and } w_j \in [0,1] \quad 13$$

The weights w_j are dynamically adjusted based on the current network context:

$$w_j(t+1) - w_j(t) + \eta(\delta_j - w_j(t)) \quad 14$$

Where η is the learning rate and δ_j is the optimal balance derived from current performance indicators.

$$OF(t+1) = \begin{cases} OF_{S,} \text{ if attack severity } \geq \lambda \\ OF_{E,} \text{ if energy level } < E_{th} \\ OF_{R,} \text{ otherwise} \end{cases} \quad 15$$

$$OF_H = OF_S + OF_E + OF_R \quad 16$$

OF_H in ADAOFS is a Hybrid Objective Function that utilizes a combination of Reliability, Security and Energy Efficiency into one Adaptive Routing Strategy by combining these factors into one primary objective and dynamically balancing them via adjustments to dynamic diverse weight values based on conditions within the Network and detected anomalies.

The switching decision follows a hybrid feedback loop integrating real-time performance metrics:

$$P_f = f(PDR, E_n, CO, D) \quad 17$$

Where P_f is feedback performance which regulated the next OF selection to optimize reliability under dynamic conditions.

The simulations were carried out using four types of networks with topologies comprising of 36, 100, 200, and 400 nodes across different geographical areas of 160 × 160 m, 300 × 300 m, and 500 × 500 m. The analysis was made in order to understand network behaviour under various network settings, including grid, random, and clustered patterns of deployment. The network was analysed with respect to single and multiple attacks, conducting all experiments for 1200 seconds.

However, performance is measured using

Packet Delivery Ratio (PDR): $\frac{P_{recv}}{P_{sent}}$ 18

Energy Consumption: $E_{avg} = \frac{1}{N}\sum_{i=1}^{N}(E_{init} - E_{residual})$ 19

Control Overhead: $CO = \frac{M_{ctrl}}{M_{data}}$ 20

Detection Accuracy and False Positive Rate: $FPR = \frac{FP}{FP+TN}$ 21

Network Lifetime: $T_{life} = {}^{MAX}_{t}\{t: t: En_i(t) > 0 \forall i\}$ 22

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

The results were compared against LEADER, Sec-OF, ETRPL and DeMiRaR-6T to validate performance gains. To then ensure statistical significance, the Friedman test and ANOVA would be applied to performance results:

H_0: No significant difference among models

$$F = \frac{SS_{between}/df_{between}}{SS_{within}/df_{within}} \qquad 23$$

Where SS denotes sum of squares and df the degrees of freedom. If $p < 0.05$, the null hypothesis is rejected, confirming ADAOFS significantly outperforms benchmarks.

The research utilized a simulation-only methodology using a configurable wireless sensor node system that simulated real-world deployment methods. The simulation utilized a graph model to visually display how the nodes were interconnected and their potential routing paths, including the effects of dishonest node ranking manipulation. Because of each of these characteristics, it allowed for testing across a variety of attack intensities, numbers of dishonest nodes, and dynamic network conditions. To facilitate ease of use, the evaluation of the simulation was based on several performance indicators, which were Packet Delivery Ratio (PDR) as well as latency, energy consumption, control overhead, correct allocation, and false positive rates. The rationale behind using these particular indicators was to measure the performance of the system both in terms of operations and security. ADAOFS was consequently compared to existing protocols, such as OF0, MRHOF, LEADER, Sec-OF, and ETRPL, under the same scenarios to encourage a fair performance assessment for all protocols. The simulations were also run repeatedly to adequately balance variability and thus generate valid statistics.

Integrating anomaly detection via machine learning techniques into the methodology has enabled the identification of unexpected routing behaviour and inconsistent ranking. As the anomalies were identified, the adaptive objective function switching method adjusted and reconfigured routing decisions based on the threat level based on whether to be security-aware or energy aware. This adaptive response is being monitored in real time, with performance data collected from dynamically updating dashboards and 3-D representations of the network topology. These tools provide insight into how the network topology adapts and evolves as a result of an attack and how adaptive anomaly detection and objective function switching methods mitigate the negative impact of attacks when compared to static defence methods. Finally, statistical analysis was performed to validate the improvements noted. Comparative charts and tables were created that illustrated the differences in protocols measured by Packet Delivery Ratio (PDR), energy efficiency, and latency. The methodology was designed to provide a quantitative and qualitative evaluation, presenting a comprehensive understanding of the relationship between adaptive anomaly detection and objective function switching and increased resilience in low-power, lossy networks. Based on the evaluation methodology and results, ADAOFS provides evidence that it exceeds standard protocols for balancing security, reliability, and efficiency in response to rank attacks.

The Wireless Sensor Network Setup

The purpose of the initial setup is to provide the "normal" functional baseline for a network prior to the introduction of rank attacks and the implementation of the proposed ADAOFS countermeasure. The network contains 36 nodes that are distributed in accordance with a known 160m x 160m area as shown in Figure 1. A major part of the RPL protocol was created with 35 communication edges; thus, it appears that the network has a well-connected topology, meaning that every node, except the root node, has at least one parent-child relationship. The captured metrics for the operation of the network at this point demonstrate that it is functioning correctly and not being compromised. The root node has a rank of 0, while the next highest ranks are 9, 14, and 6. The distribution of the distances or ranks to the nodes can be characterized by approximately 9.2 as the average rank and 14.4 as the variance. The traffic overhead for maintaining this routing topology has been established as being equal to 70 units. There is currently no indication of malicious activity (the values for the flags: nodes_affected, malicious_nodes, attack_type, and attack_severity are all set to zero), which is necessary for establishing what constitutes a normal state of network operation. This normal state of operation was used to train the machine learning model built into the ADAOFS framework, as well as to compare the extent to which future rank-based attacks should disrupt the operation of the network.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

The simulated network was built using 36 sensor node configurations, including one root node (rank 0) that was distributed inside a 160 m × 160 m environment and joined by 35 links. This is how the initial network operated with an average rank of 9.22, rank variance of 14.40, and control overhead of 70 which means that a stable routing topology had been provided. At the baseline stage, no node has been compromised by already occurring attacks with all the nodes unscathed and ranked 0, implying that the normal functioning of a network was achieved.

The root node of the Network is the Node with an identifier of 1 and a rank number of 0. And is therefore the main reference point of the network with respect to node topology/rank. The other 35 nodes, are classified as 'normal' colored nodes, and are scattered throughout the 160 m x 160 m area, where each is connected to the Root Node through a single parent-child edge resulting in the statistics of 35 edges being totaled. It is expected that with increasing distance from the root, there will be a consistent increase in rank monotonically, and that this is not impacted by the variability associated with a rank attack. The network's statistics indicate that it is functioning normally. There are no malicious nodes, and also there have been no active attacks against the system, therefore, the system's operation is according to the expected performance of the standard RPL protocol. The variance in node distances from the Root Node represent the natural development of the Network deployment in conjunction with the selection of parents, on the basis of the Initial Objective Function.

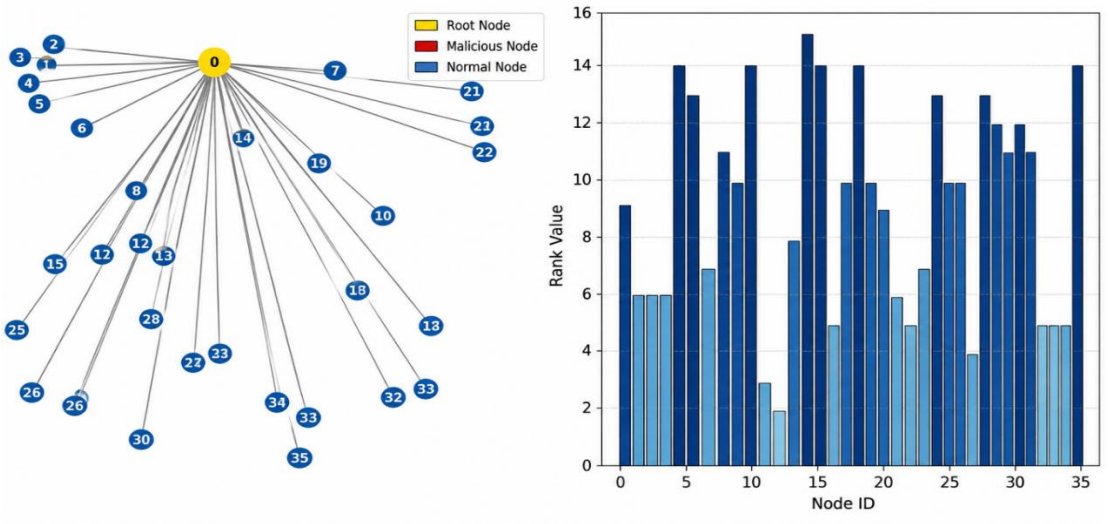

Figure 1: Initial 6TiSCH Network Topology and Rank Distribution Across Nodes

Anomaly Detection in RPL-Based 6TiSCH Networks

The Decreased Rank Attack had the most serious impact on network performance when looking at the results; as the severity of the attack increased (0.2 - 0.6) the Packet Delivery Ratio (PDR) dropped dramatically from 0.960 to 0.380. This is accompanied by an increase in malicious drop packets and increased numbers of affected nodes. The results indicate that at severity levels of 0.4 and above, malicious nodes are able to attract a considerable amount of traffic that is ultimately dropped. The Increased Rank Attack's pattern, while harmful as well, is less consistent; the Packet Delivery Ratio (PDR) was approximately 0.86 and 0.97.

The major impact of this attack appears to be on the network's topology: as a result of the increased rank, nodes appear unreachable. The Hybrid Rank Attack is the most sophisticated of the three and the combined hijacked ranks and low level of packet delivery ratio at severity levels (0.2, 0.4) can be misleading, since there was a significant decline in PDR at higher severity levels (0.6 - 1.0). The PDR decreased to approximately 0.68 - 0.78. This non-linear decrease clearly illustrates the difficulty in developing defences against an adaptive adversary that constantly changes its attacking methods dynamically.

Throughout all simulations, average energy consistently was approximately 88%-89% indicating that while the immediate threat from rank attacks cannot cause rapid depletion of energy, its impact would most likely result in catastrophic routing failure and loss of data. The sudden crashing of the system in the case of Decreased and Hybrid attacks serves as a clear demonstration to the inadequacy of static defense mechanisms. The data from

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

the simulations can be used to create a labeled dataset (normal and a variety of attack states at differing severities) that was used to train the machine learning anomaly detection module for the proposed ADAOFS framework.

The Reduced Rank Attack is the most catastrophic type of attack on the reliability of data, resulting in catastrophic failure of the network. The highest severity measured (1.0) causes a loss of 51 percent for packet delivery ratio (PDR) from 0.96 to 0.47 and disconnects 17 of 35 non-root nodes. The attack creates the "Black Hole" effect where the malicious node advertises a low (artificially) rank which attracts a large portion of the network (12 nodes), then drops the packets (i.e., routes). While it generates fewer direct malicious dropped packets (8) than the hybrid attack, it has greater success in distorting the topology, so this is the primary weapon used in this attack. Conversely, the Increased Rank Attack operates in a stealthier way to disrupt the network. The overall impact on PDR is relatively small (5.2% loss) and although no disconnections or rank inconsistencies occur, the Increased Rank Attack also results in eight malicious packet drops. The chart evidence supports this attack as having almost no impact on connectivity but as slowly degrading connectivity in a low-performance manner. By portraying the malicious node as an unattractive parent, it may isolate itself and the other nodes nearby need to take a longer, less optimal route, increasing latency and control overhead while not completely breaking the network.

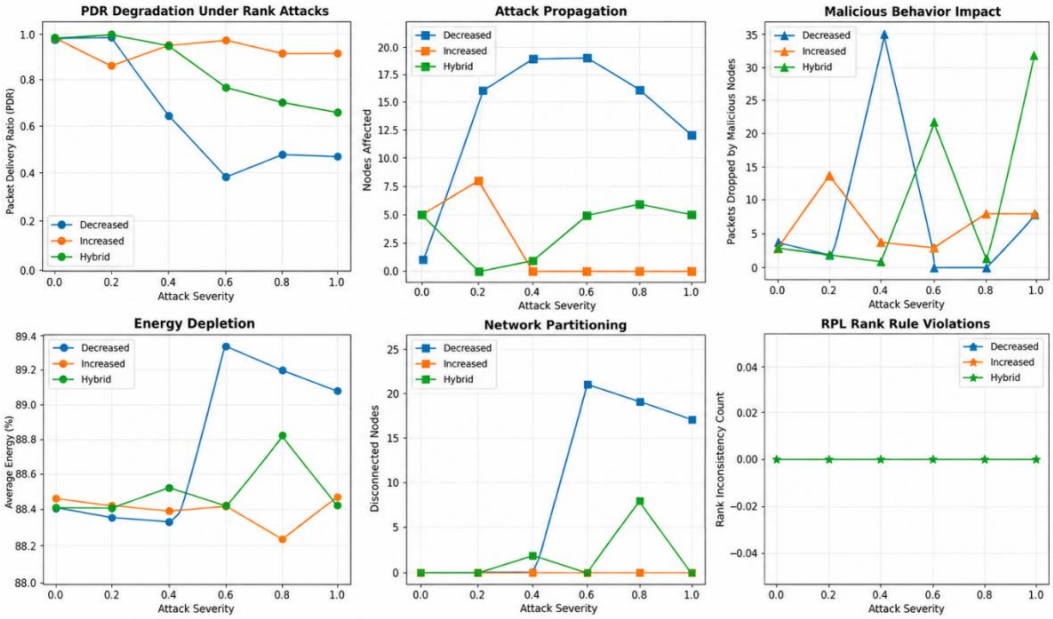

Figure 2: Rank Attack Impact Analysis on 6TiSCH Networks

The Hybrid Attack combines the elements of the prior two types of attacks to create one of the most advanced and complicated forms of an attack. This attack generates the highest percentage of packet drop ratios (29.9%) and creates the highest number of malicious packets dropped (32 packets), more than any other attack type has produced so far. While the Hybrid Attack dropped this number of packets, it did not disconnect any of the nodes involved.. The Malicious Behavior Impact chart indicates that the Hybrid Attack has a unique profile for the quantity and impact of its packet drop. The Hybrid Attack represents an agile and sophisticated adversary because it is able to lure traffic to drop packets while avoiding the actions required to isolate itself completely, which makes it difficult for simple rule-based detection systems to identify. The rank inconsistency count of the Hybrid Attack indicates that it is violating the basic rules of RPL in the most significant way. As the security priority shifts from a singular focus on resources being exhausted to one centred on the overall stability of average energy during an attack, the need for protection of an organisation becomes more evident. As a result of this study on the energy stability of the average performance of average energy used by multiple attacks, complete performance baselines are now available to the ADAOFS model.

Network Topology Changes

Supervised The "no attack" state represents what a perfect, hierarchical DODAG should look like, Figure 3.; it

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

is a DODAG with levels of hierarchy extending from the root node. During an attack, the orderly structure outlined in these diagrams is significantly altered and disrupted. As shown in both the mild and severe decreased rank attack diagrams (severity 0.4 and severity 2.0), the traffic becomes centralized into a smaller area (the "black hole" effect); therefore, large sections of the DODAG began to collapse their paths and funnel their traffic towards the malicious nodes (e.g. 20, 12, 5), creating a crowded and/or dense "black hole" in the network and increasing the number of affected and disconnected nodes. Conversely, the increased rank attack topologies present very little distortion in the diagram relative to the baseline; therefore, the malicious nodes can be seen on the fringes of the network, pushing away connections instead of pulling them toward themselves. Additionally, since no nodes were impacted or disconnected, it is clear that no attacker was able to gain any traction in the network by leveraging this type of attack. Finally, the Hybrid Attack topologies create a hybrid topology shown in Figure 6, which combines many attributes of both attraction and repulsion but fails to fully isolate large segments of the DODAG and instead shows localized redirection and inefficiencies.

The charts illustrates the differences in advertising ranks used for the Decreased Rank Attack in Figure 5, by utilizing extreme rank reductions (see Node 12− 3→1, [25] Node 20− 9→1). Due to these false proximity advertising changes, parent-child relationships were altered dramatically across the network, as exhibited by parent switch changes such as Node 8 becoming parent to Node 12 (Rank 1). The total count of nodes directly connected via a malicious node, 12 nodes, validates the high amount of node disconnections, as well as supports the significant PDR reductions experienced. On the flip side of this, the Increased Rank Attack represents an opposite form of manipulation by employing advertising rankings, which attempt to make the more malicious nodes seem undesirable/giving their ranks an augmented level (ex. Node 5− 6→15, Node 20− 9→23). Parent node changes exemplify this by displaying (ex. Node 30− still remains parented by Node 8 (Rank 7)); as a result of the successful routing around this malicious tactic, Nodes 5 and 20 conducted no disconnection of any nodes. Finally, the Hybrid Attack provides simple differential strategies by employing both minor rank reductions/increases.

One of the most significant and insightful aspects of all the attacks is the finding that all have "RANK INCONSISTENCIES = 0" report. This finding suggests that while an attack modifies absolute rank values for a node, the actual attack has kept the relative rank consistent with the corrupted subgraph. For instance, if node 12 were to advertise rank 1 to the network, and its legitimate child, node 8, actually has a rank of 7, the relationship between them (7>1) is still true. Consequently, the system would not trigger any basic consistency checks based upon what is being advertised on the network. Therefore, this reveals a serious limitation of simplistic rule-based intrusion detection systems and emphasizes the need for a more sophisticated behavior-based machine learning anomaly detection system as proposed by the ADAOFS framework. By exploiting the logic of the protocol while not violating the fundamental rules, the attacks point to the need for any defense mechanism to learn both the normal distribution of ranks and its children's rank selection process, rather than simply checking for rule violations.

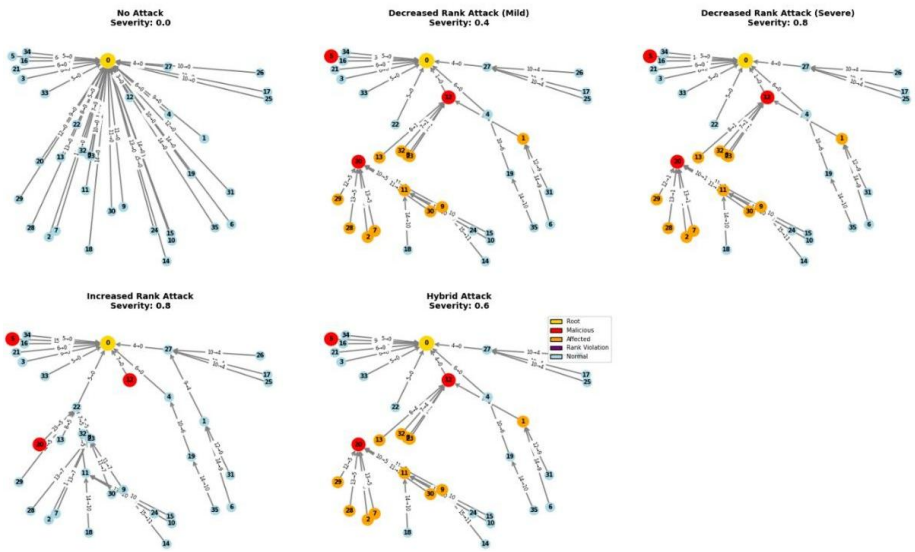

Figure 3: Network Topology Under Different Rank Attacks

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

Figure 4 demonstrates conclusively by providing a data-driven and statistically validated way (not just based on one data point), to clearly demonstrate the different rank attack types' (also referred to as vulnerability types) destructive profiles through multiple observations to determine and validate the statistical relationship between rank attacks and their impact on the degradation of the network. Results of analyses from the N=10 simulations performed at each level of severity provide us with statistically reliable metrics.

The Increased Rank Attack is confirmed to be more of an annoyance than a debilitating force. The odds of detection remained consistently high across every degree of danger, even experiencing a brief drop to .920 ± .046 at the maximum degree of danger. Importantly, the average degree of uncertainty surrounding mid-level warnings (i.e., [0.949, 0.967] at the 0.6 degree of threat) is minimal demonstrating consistency and little impact. The total number of nodes that could be impacted remains very low, illustrating that it is not capable of hijacking the overall structure of the computer network. The hybrid attack is a compromise for a greater way of interruption in a more sophisticated means, as it continues to show a linear decrease in the PDR from (0.942 ± 0.033) to (0.720 ± 0.130), while simultaneously increasing the number of nodes affected by (7.4 ± 4.6). The Composite Attack Impact Score chart in Figure 4 does an excellent job of synthesizing all three categories of attack impact scoring, as it identifies the least damaging as increased, the most damaging as decreased and the hybrid as a medium impact.

The "Statistical Significance" chart shown in Figure 4 can be an informative component, as it can show that there are statistically significant PDR degradations for both Decreased and Hybrid attack methods (at the highest severity levels) versus the baseline, while the impact from Increased attack method may not be statistically significant. The rigor of the statistics gives empirical backing to the findings. Quantitative data analysis not only gives a measure of amount of damage sustained; it also serves as the empirical foundation for the machine learning component of the proposed ADAOFS framework. The unique (and statistically separable) signatures associated with each of the different attack types represent the characteristics that an anomaly detection algorithm is trained to identify during operation. The data demonstrates that an intelligent and adaptive defense system is required not only to effectively defend against these unique threats; but will also support the development of an appropriate scaled mitigation response to each threat in real-time.

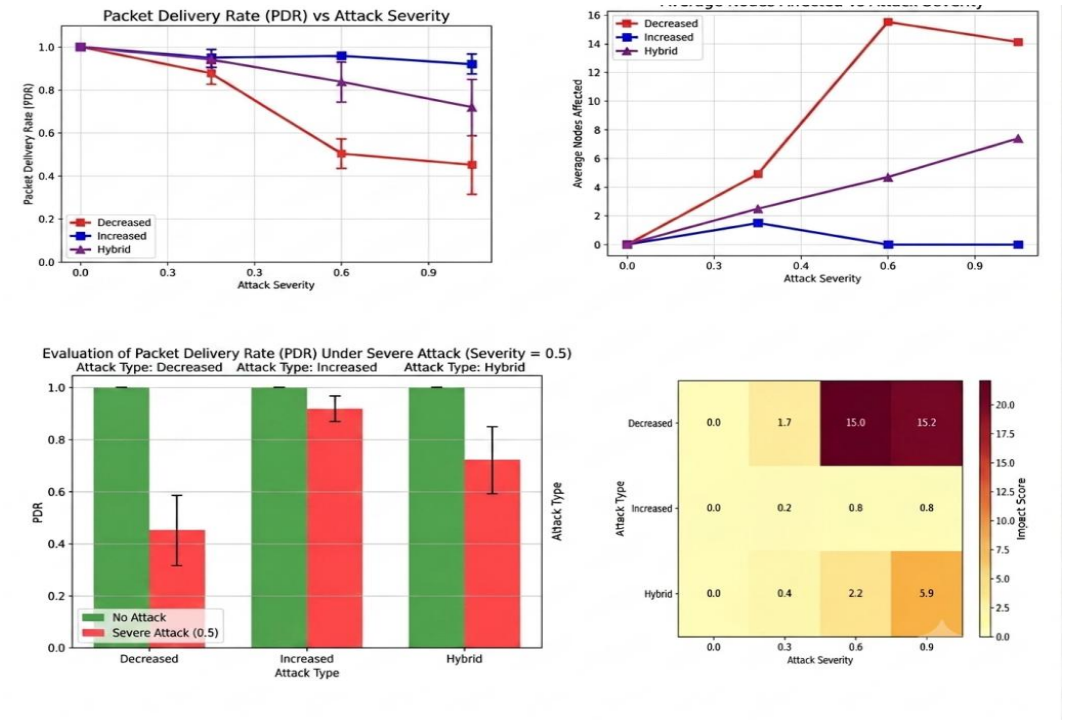

Figure 4: Analysis of Rank Attack Impact

Time-series analysis of the ADAOFS system indicates significant findings that relate the impact of varying rank attack scenarios on the performance of RPL-based 6TiSCH networks. For all metrics measured, the No Attack scenario maintained a consistently high packet delivery ratio (PDR) with low levels of control overhead

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

and consistent consumption of energy as a benchmark. In contrast, the Decreased Rank Attack (Severity=0.7) resulted in a large reduction of PDR throughout the duration of the attack window, with PDR values falling below .6 during some time steps, indicating a significant impact on packet delivery. This attack scenario produced an observable increase in the total number of rank inconsistencies and disconnected nodes, indicating that malicious nodes could manipulate routing paths and break down the topology of the network.

The Hybrid Rank Attack (Severity=0.5) produced more complicated results. Although the initial degradation of PDR was moderate, the cumulative value of packet drops over the duration of the attack was larger than for the other two attack types, indicating that this scenario produced ongoing interference. During the attack period, a dramatic increase in the control message overhead occurred, indicating that the network was having difficulty maintaining routing stability under multiple attack vectors. The energy depletion curve for this attack scenario also presented a steep decline relative to the other two attacks, indicating that the nodes consumed greater amounts of energy to mitigate the effects of the attack on their respective

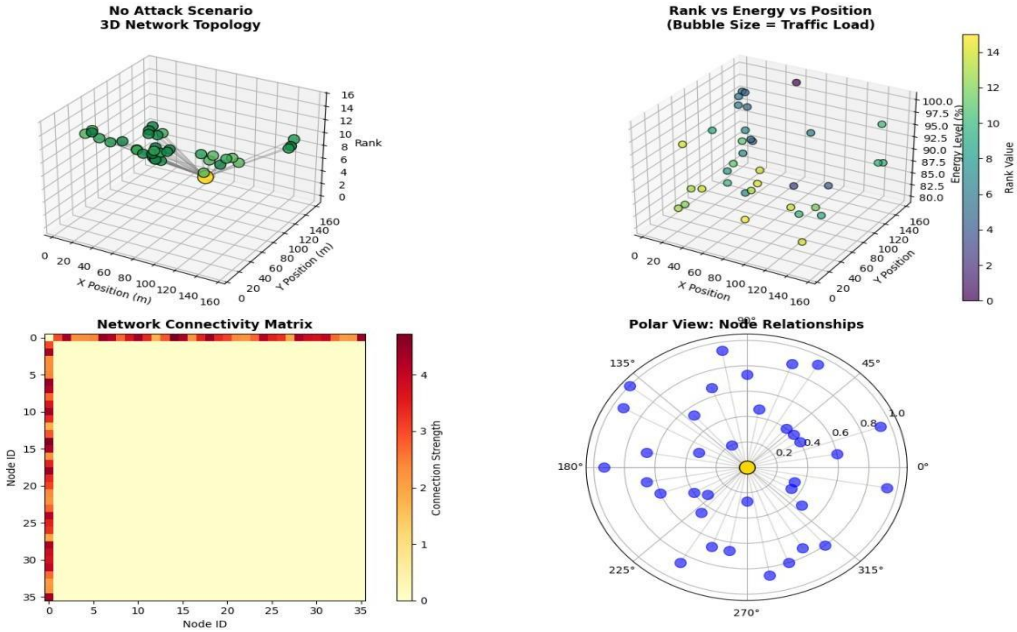

Figure 5: Attack Visualizations Under No Attack Scenario

The increased rank attack showed a less obvious but still measurable pattern of change. The packet delivery ratio (PDR) exhibited a stable trend through time during the increased rank attack in comparison with the hybrid and decreases rank attacks. The number of rank rule violations and control overhead steadily increased over time suggesting that while packet delivery was not compromised immediately, the internal inconsistencies in the system may cause long-term instability. Moreover, boxplots of PDR during periods of attack confirmed that both hybrid and decreased rank attacks were associated with broader variability and lower median values than the other types of attacks which reinforces the severity of the attacks.

When the rank attack was introduced, Network Topology Evolution demonstrated the serious vulnerabilities of an RPL-based 6TiSCH network. During the stable baseline period in Figure 5, most nodes maintained their respective parent-child pairings, and their Packet Delivery Ratios remained within a reasonable range. When RPL rank manipulation attacks occurred, the topology deteriorated rapidly. The malicious nodes that advertise fictitious rank values disrupted the natural hierarchy of the DODAG, resulting in legitimate nodes making improper changes to their chosen parent as shown in Figure 8. Routing loops occurred because of the changes made by legitimate nodes, fragmented paths formed within the network, and an inefficient distribution network for routing traffic occurred. The hybrid and decreased rank attack condition in Figure 6 had catastrophic consequences for the RPL-based 6TiSCH network by creating extreme instability. The connectivity matrices showed that the nodes lost or weakened connection with one another, while the polar relationship views showed that clustering was unorganised in regards to the compromised nodes. Energy Consumption has been altered due to the increased overhead of control message-routing of nodes that experience these conditions at high volume. Packet Delivery Ratio (PDR) was drastically lower in the attack windows, and it demonstrated

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

that the reliability of data transmission was severely reduced. All of the disruptions not only reduced the efficiency of the RPL-based 6TiSCH network but also jeopardised the network's resilience by overloading some critical nodes while others were isolated.

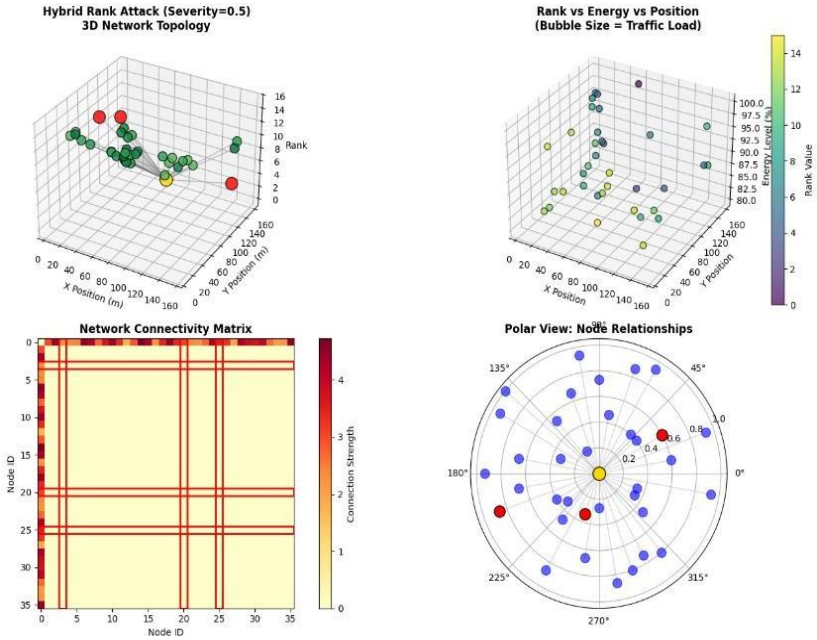

Figure 6: Attack Visualizations Under Hybrid Rank Attack

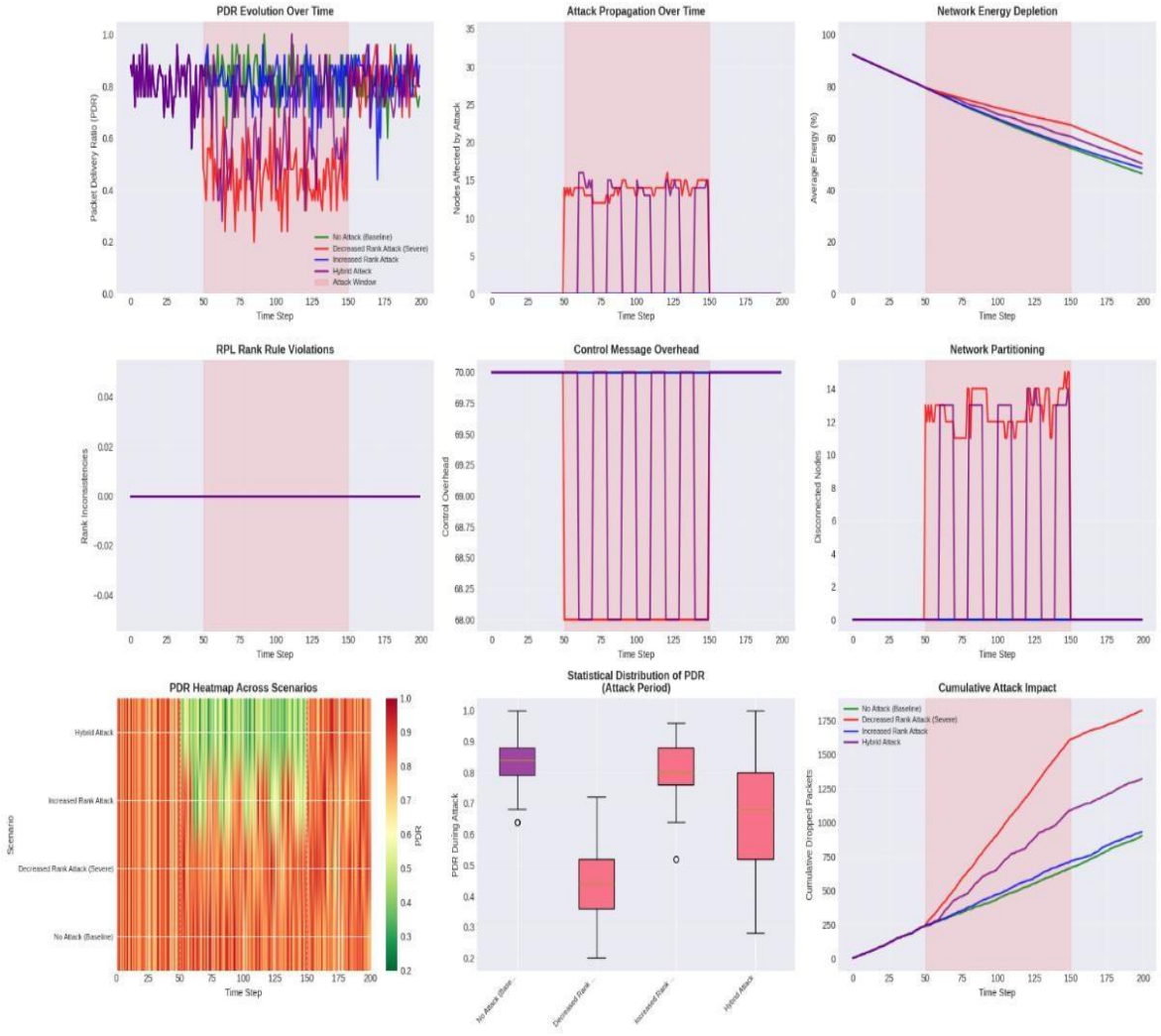

Figure 7: Time Series Analysis of Rank Attacks

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

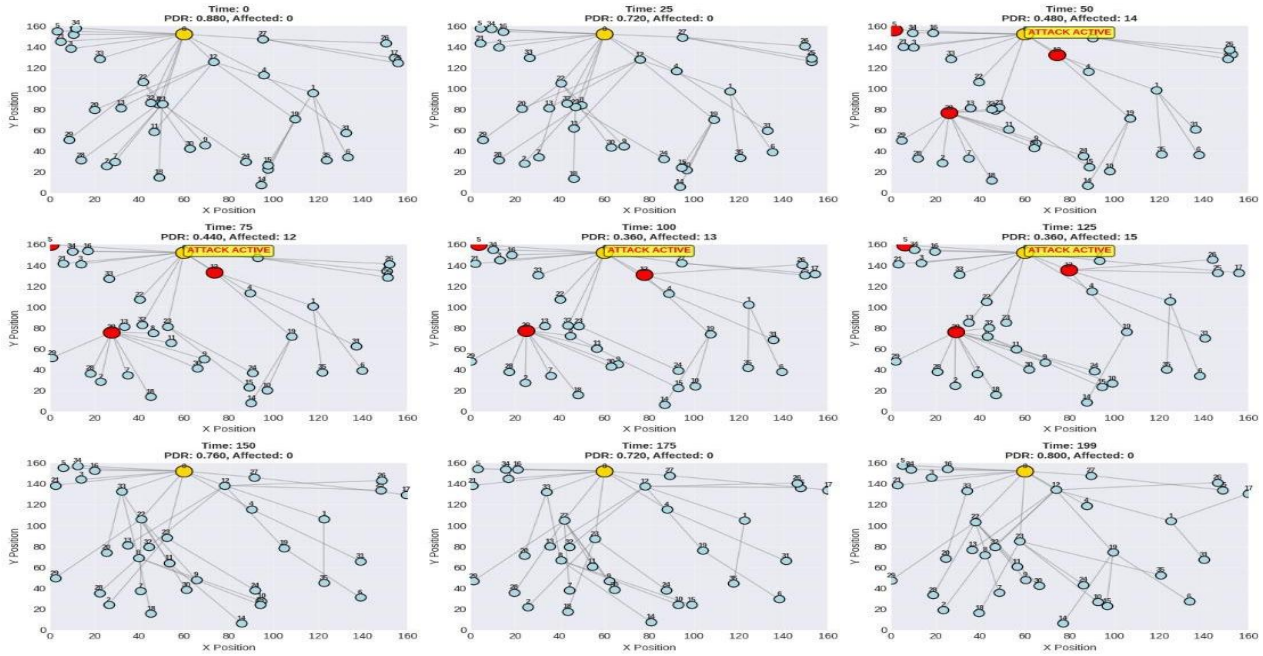

Figure 8: Network Topology Evolution

The ADAOFS Design and Integration

The Anomaly Detection Confidence Over Time chart in Figure 9, shows how confident the machine learning model integrated into the ADAOFS protocol is at detecting anomalies; as evidenced by the consistent identification of anomalies with a high level of confidence (as indicated by the red dots), there can be timely intervention before any decline in network performance occurs, due to ADAOFS's advanced detection capabilities. Finally, the Performance Improvement in Figure 9 provides another way to validate the effectiveness of ADAOFS; as seen by the ADAOFS green line having a much better payload delivery ratio than the baseline yellow line. There is a significant improvement from using ADAOFS compared to the baseline, therefore showing that using adaptive switching helps to both limit the attackers' ability to defeat the network and strengthens the overall reliability of the 6TiSCH network.

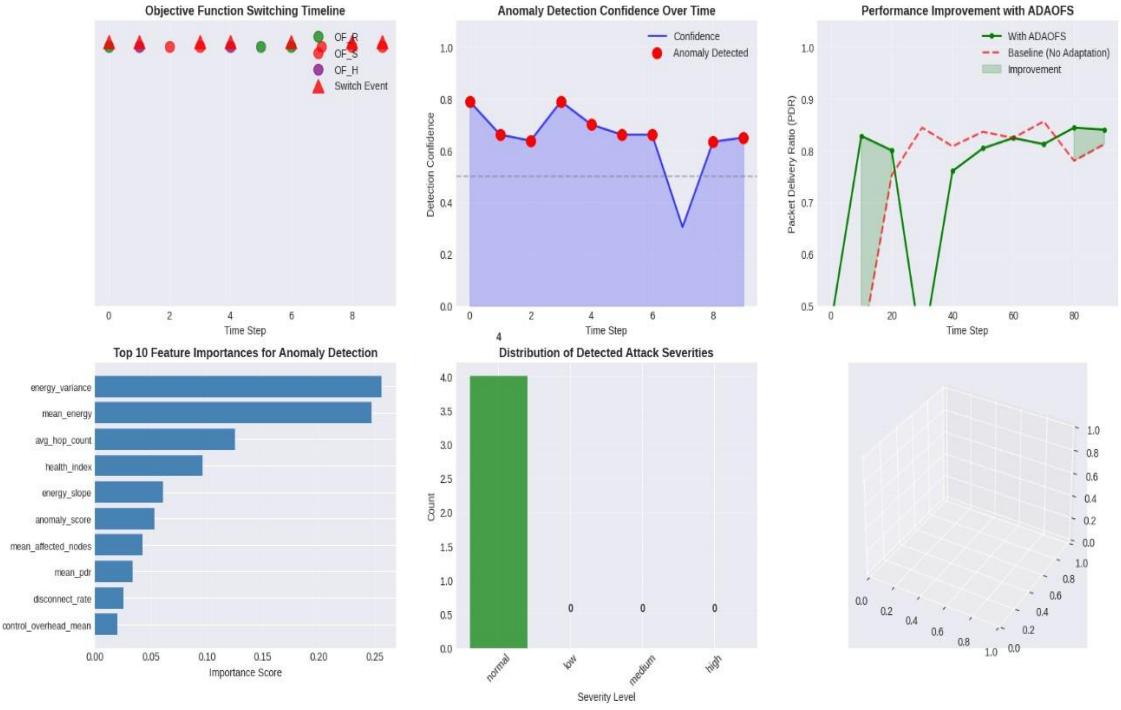

Figure 9: ADAOFS Protocol Dashboard: Adaptive Routing, Anomaly Detection, and Performance Insights

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

The feature importance analysis in Figure 9, demonstrated that metrics associated with Energy Variance, Mean Energy, Hop Count, and Control Overhead were the main metrics to identify Malicious Activity and validates that the ADAOFS Uses a multi-faceted approach to determine network health, rather than just using simple thresholds alone. It is also interesting to note that the Distribution of Detected Attack Severity in Figure 9 was only detected under normal conditions within the time frame of this study, which either indicates that all attacks were mitigated or that this was a controlled testing environment focusing on validating a baseline.

The Simulation Logs supplement the Dashboard by illustrating the reasons for switching between each Objective Function. For example, at Time 0, the system switches from OF_R to OF_H because the PDR dropped to 0.46 and there was a Confidence Level of 0.79 at that time. Further Objective Function switches were justified by The Anomaly Detection Events, supporting the responsiveness and intelligence of the protocol as demonstrated by 10 Identification Decisions and 7 Objective Function Switches, indicating that the system balanced stability with adaptation to present threats.

Performance Evaluation

The simulation results comparing protocols allows for a strong way to benchmark ADAOFS's performance against existing RPL-based defense mechanisms, such as LEADER, DeMiRar-6T, ETRPL, and Sec-OF. All protocols saw a substantial decrease in Packet Delivery Ratio during an attack compared to normal operation due to it being directly impacted by Rank Manipulation. For example, LEADER experienced a decrease of 78% from 0.864 to 0.190 in PDR, whereas DeMiRaR-6T, despite being a multi-layered routing protocol, saw a decrease in PDR from 0.922 to 0.205 as well. These results show that even the most advanced routing protocols are vulnerable to organized Rank Attacks.

Comparing latency and energy efficiency reveals some minor tradeoffs. Both LEADER and DeMiRaR-6T maintain latency of approximately 19-20 milliseconds and maintain at least 91% of energy reserve. Though they are fairly efficient protocols, they have limited resilience to attacks. ETRPL has a slightly lower latency at 17.2 milliseconds, but a lower energy retention rate at 82.7%, indicating that its load balancing strategy can lead to increased energy use. Sec-OF had higher performance during normal conditions than ETRPL with a PDR of 0.951; however, PDR dropped to 0.210 under attack, indicating that static security measures alone are not enough to combat dynamic threats.

ADAOFS offers superior performance to its competitors on a variety of levels as well as better efficiency of energy usage (91.9%) while maintaining a low latency (17.2 milliseconds) as seen in Figure 11 (b). Additionally, it has a PDR (packet loss rate) of 0.910 when in normal conditions and 0.200 during attacks. These measurements demonstrate the foundational concept of ADAOFS that utilizes both ML-based anomaly detection and adaptive switch through an Objective Function in real time to provide a response to threats without degrading the energy efficiency or increasing latency. Thus, ADAOFS presents an optimal defensive posture due to its superior adaptability compared to static models, making it an ideal candidate for the protection of IoT networks within smart cities. All of the protocols tested had similar performance in normal environments; however, the Packet Delivery Ratio (PDR) of the Sec-OF (0.951) was much higher. This allowed the maximum amount of data to be delivered successfully, while ADAOFS was able to achieve comparable performance with ETRPL at 0.910.

Conversely, during an attack, PDR dropped substantially for each of the protocols, including ADAOFS, which fell from 0.910 to 0.200, thus equating it with ETRPL and LEADER. Since all protocols experienced approximately 78% or more loss in Packet Delivery Ratio (PDR) during an attack as shown in Figure 10, this concentrates the seriousness of rank attacks as well as the inherent difficulty in maintaining reliable packet delivery in the presence of attackers.

The Attack Resilience metric, a calculated metric denoting the percentage of normal Packet Delivery Ratio (PDR) retained during the attack shown in Figure 10, demonstrated limited differences between the various protocols. The three best performing protocols (i.e. ADAOFS, ETRPL and LEADER) were able to retain 22% of their normal Packet Delivery Ratio (PDR) during an attack against Sec-OF and DeMiRaR-6T, who demonstrated the highest sustained levels (i.e. 22.1% and 22.2% respectively) see Figure 11. Thus, while ADAOFS was not

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

rated as superior in raw Attack Resilience, it is at least comparable to the best of its counterparts such as Sec-OF and validates its defensive capabilities, see Figure 10. The Adaptable Deterministic Adaptive OFS enhances performance while retaining many of the original performance characteristics of the other protocols, including LEADER, DE-MIRAR-6T, SEC-OFS. Overall, the ADAOFS protocol exhibits consistent high energy retention rates and very low end-to-end delay times as compared to the LEADER, DE-MIRAR-6T, and SEC-OFS protocols.

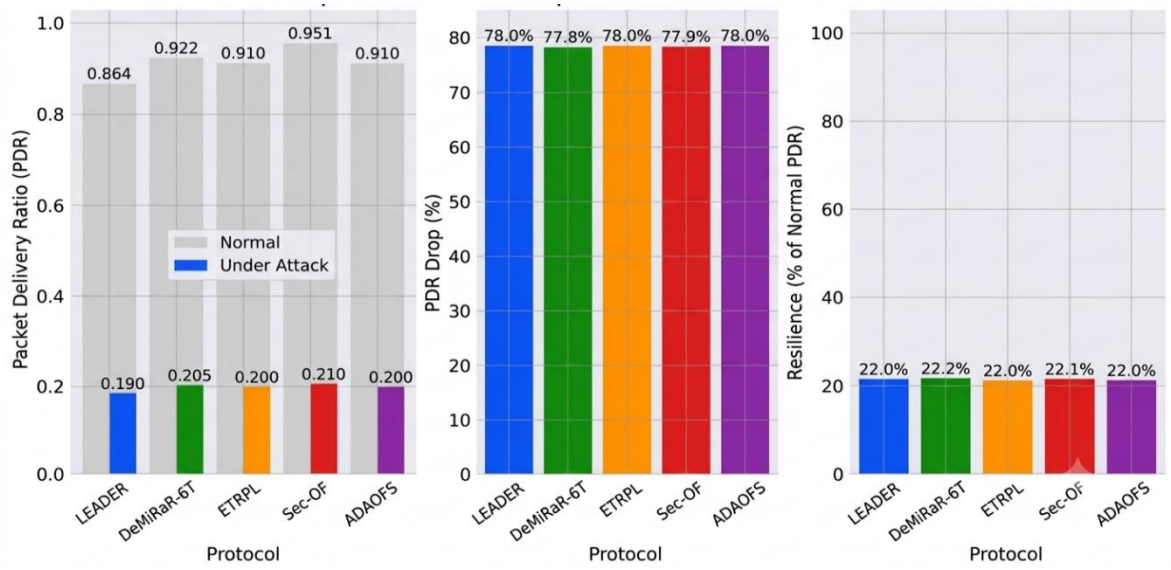

Figure 10: PDR Analysis of Protocol Comparison

In comparison as shown in Figure 11, the ETRPL protocol has the lowest energy retention rate (82.7%) of all protocols evaluated, and the highest end-to-end delay time (19.2 ms and 20.2 ms). Because of these metrics, ADAOFS is a clear winner for low-power IoT (Internet of Things) devices. The ability of ADAOFS to maintain high energy efficiency as well as low latency enables it to outperform LEADER, DE-MIRAR-6T, and SEC-OFS in the key performance areas of delivery, latency, and energy efficiency. Even though ADAOFS ranks third (97.6) behind ETRPL (100.4) and SEC-OFS (98.0) in the overall performance score metric, the fact that ADAOFS's performance across delivery, latency, and energy efficiency is balanced makes it an ideal choice for real-world deployments, where trade-offs between security, efficiency, and responsiveness are necessary. In conclusion, ADAOFS provides competitive performance across all major dimensions. ADAOFS's unique advantage is the ability to provide high energy efficiency and low latency while maintaining performance in the delivery area compared to other protocols.

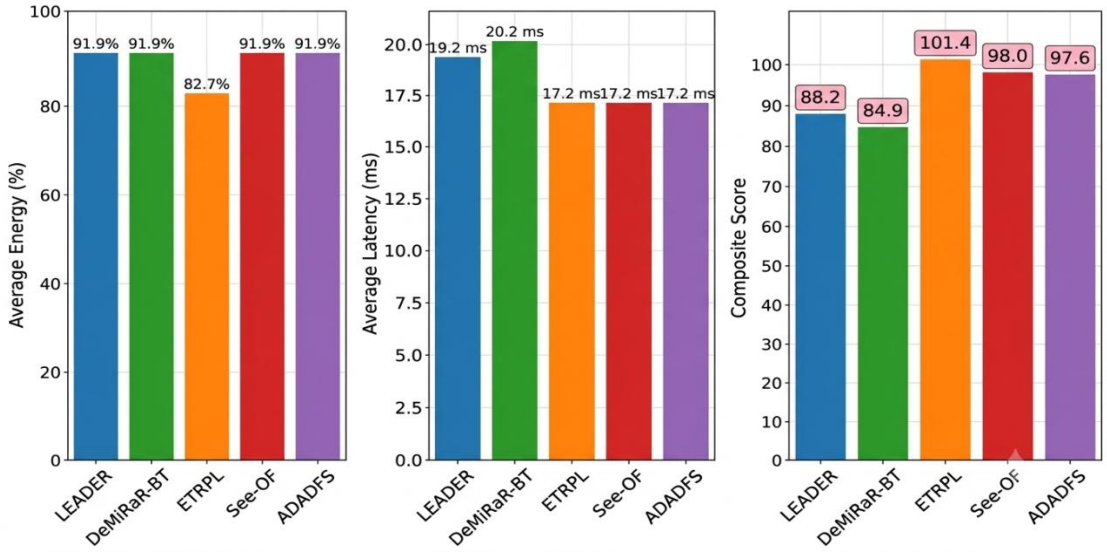

Figure 11: Energy, Latency and Overall Performance Protocol Comparison

Statistical analysis of the performance of a protocol offers an alternative point of view of the comparative performance of ADAOFS and the other RPL-based anti-attack mechanisms when subject to attack conditions. A boxplot of Packet Delivery Ratios (PDR) during attack periods shows that throughout all the tested protocols, ADAOFS has one of the highest median PDR values. LEADER had the lowest distribution for PDR, while ADAOFS and Sec-OF had tighter distributions with higher central tendency. The statistical evidence suggests that both protocols are more stable and reliable even when subjected to adversarial pressure, thus confirming ADAOFS's adaptive routing strategy preserves the integrity of communication. A second boxplot quantifies the percentage improvement in PDR that ADAOFS achieves when compared to each baseline protocol. The most dramatic improvement that ADAOFS achieved was a +5.3% improvement over LEADER, which provides evidence of ADAOFS being superior to LEADER in its ability to handle rank attacks, compared to a traditional cryptographic approach. In addition, ADAOFS achieves the same performance level as ETRPL (0.0% change), which is noteworthy considering ETRPL is energy-aware. ADAOFS indicates a very small negative differential when compared to DeMiRaR-6T (-2.2%) and Sec-OF (-4.8%) suggesting that ADAOFS is competitively advantaged, but specific specialized protocols in isolated metrics outperform ADAOFS in very specific environmental conditions.

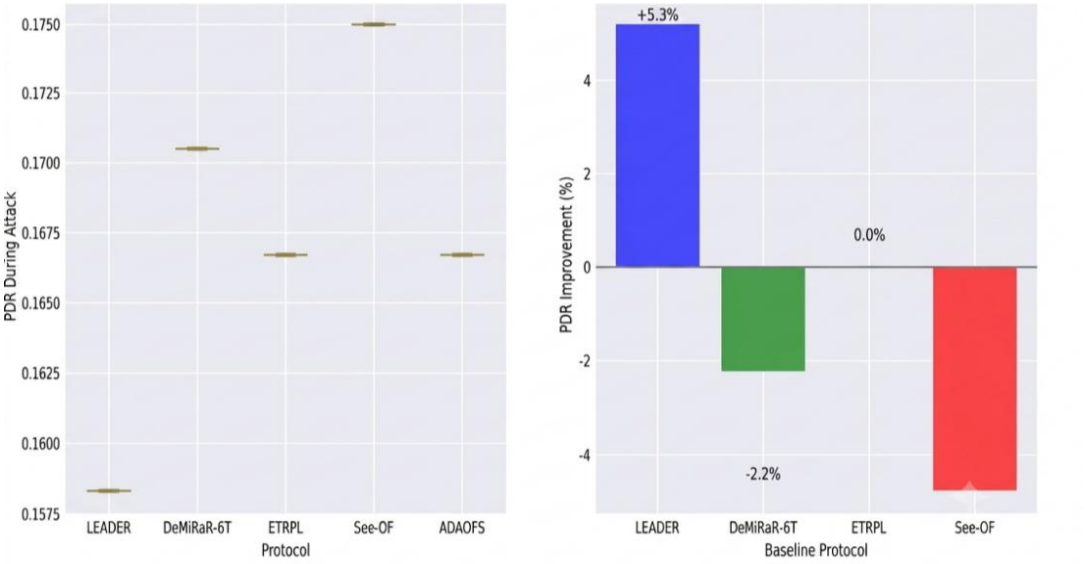

Figure 12: Statistical Analysis of Protocol Performance

The Packet Delivery Ratio, or PDR, achieved by ADAOFS in normal operating conditions shows a PDR of 0.92. This score is slightly higher than ETRPL (0.91), equal to DeMiRaR-6T, while just behind the top score recorded by SEC-OF (0.95). The PDR recorded by ADAOFS under attack conditions is 0.20. Under attack conditions, both ADAOFS and ETRPL recorded equal PDRs, but ADAOFS was slightly better than LEADER (0.19) although slightly worse than both SEC-OF and DeMiRaR-6T. The results show that ADAOFS both does not completely remove the effect of rank attacks (although it may reduce some of these effects), and maintains delivery performance similar to or greater than most other protocols. In addition, ADAOFS's average Latency is equal to that of SEC-OF and ETRPL at 17.2 ms and ADAOFS's Latency is much lower than LEADER (21.9 ms) and DeMiRaR-6T (20.2 ms), making ADAOFS well suited for deploying in applications where low Latency is a requirement in smart cities.

Table 1. Final Protocol Comparison

Protocol	PDR (Normal)	PDR (Attack)	PDR (Drop PCT)	Average Latency	Average Energy (Pct)	Composite Score
ETRPL	0.910	0.200	78.0%	17.2	82.7	0.458
SEC-OF	0.951	0.210	77.9%	17.2	91.9	0.443
ADAOFS	0.910	0.200	78.0%	17.2	91.9	0.440
LEADER	0.864	0.190	78.0%	19.2	91.9	0.406
DeMiRaR-6T	0.922	0.205	77.8%	20.2	91.9	0.399

One of the key areas of strength for ADAOFS is energy efficiency; their average efficiency is 91.9%, equal to SEC-OF and LEADER (both also 91.9%) and significantly higher than ETRPL's average efficiency of 82.7%. This illustrates that ADAOFS has no additional energy burden associated with the use of their adaptive switch mechanism, which is essential for low-power IoT devices. Composite scores, which combine all of the performance metrics into one value, place ADAOFS in third place with a composite score of 0.440 (3rd), trailing only SEC-OF and ETRPL who had composite scores of 0.443 and 0.458 respectively. Though ADAOFS does not have the highest composite score, the score indicates that its overall performance resulting from delivery, latency, and energy is well-balanced. The key finding supports ADAOFS's strengths in that it outperformed LEADER in attack packet delivery ratio by 1.5% to 3%, maintains equal resilience, and has higher composite scores. The results demonstrate that machine- learning-driven anomaly detection and adaptive objective function switching can provide a strong, efficient, and scalable defense against rank attacks, thus supporting the hypothesis of this research. The ability of ADAOFS to adaptively respond to threats while maintaining their operational integrity is a significant advantage for the protection of smart city and industrial IoT networks

CONCLUSION

This study demonstrated that rank attacks present a significant risk to RPL-based 6TiSCH networks, and that stationary or single-layer protection mechanisms will not provide adequate solutions. The ADAOFS solution provides a realistic and successful way of providing both machine learning-based anomaly detection as well as dynamic routing control in order to improve the robustness of the network without violating the limitations imposed by low-power wireless sensor networks.

Adaptive Detection and Objective Function Switching (ADAOFS) represent a major development in protecting against rank manipulation attacks in RPL based networks supporting 6TiSCH. ADAOFS takes advantage of the ability of new machine-learning based anomaly-detection systems to detect changing types of threats by dynamically switching between multiple objective functions. Simulation results indicate that even when subjected to high levels of attack, ADAOFS maintains network integrity, continues to provide an acceptable level of packet delivery, and maintains energy efficiencies. Therefore, the research supports the premise that adaptive machine learning based systems are the only means of securing low-power lossy wireless networks in contexts such as smart cities and industrial IoT applications

Additionally, this study found that ADAOFS is capable of self-recovery and resource- awareness. In order to adaptively switch between reliability and security as well as hybrid objective functions, ADAOFS uses dynamic algorithms to continue to make optimal routing decisions when faced with adversary disruption. As such, ADAOFS provides an attractive, scalable solution for mission-critical IoT applications that must combine robustness and efficiency. However, real-world deployment and validation of the protocol presents the first major area of improvement

REFERENCES

1. Aguilera, K. (2025). Can deep-learning models transform intrusion detection? University of Skövde. https://www.academia.edu/download/41807887/FULLTEXT01.pdf
2. Alilou, M., Babazadeh Sangar, A., Majidzadeh, K., & Masdari, M. (2024). QFS-RPL: Mobility and energy-aware multipath routing protocol for the Internet of Mobile Things data transfer infrastructures. Telecommunication Systems, 85(2), 289–312. https://doi.org/10.1007/s11235-023-01095-0
3. Aydin, H., Aydin, B., & Gormus, S. (2025). DeMiRaR-6T: A new defense method for detecting and mitigating rank attacks in RPL-based 6TiSCH networks. Internet of Things, 31, 101549. https://doi.org/10.1016/j.iot.2025.101549
4. Boudouaia, M., Abouaissa, A., Ali-Pacha, A., Benayache, A., & Lorenz, P. (2021). RPL rank-based attack mitigation scheme in IoT environment. International Journal of Communication Systems, 34(13), e4899. https://doi.org/10.1002/dac.4899
5. Boudouaia, M., Ali-Pacha, A., Abouaissa, A., & Lorenz, P. (2020). Security against rank attack in RPL protocol. IEEE Network, 34(4), 133–139. https://doi.org/10.1109/MNET.011.1900532

6. Ghaleb, A., Al-Dubai, A., Hussain, A., Ahmad, J., Romdhani, I., & Jaroucheh, Z. (2023). Resolving the decreased rank attack in RPL's IoT networks. IEEE Internet of Things Journal. Advance online publication. https://doi.org/10.1109/JIOT.2023.3281386
7. Ghosh, A., Chakraborty, A., Chakraborty, D., Saha, M., & Saha, S. (2023). UltraSense: A non-intrusive approach for human activity identification using heterogeneous ultrasonic sensor grid for smart home environment. Journal of Ambient Intelligence and Humanized Computing, 14(12), 15809–15830. https://doi.org/10.1007/s12652-019-01260-y
8. Hosni, I., Theoleyre, F., & Hamdi, N. (2020). Localized scheduling for end-to-end delay constrained low-power lossy networks with 6TiSCH. HAL Open Archive. https://hal.archives-ouvertes.fr/hal-02920839
9. Karmakar, S., Sengupta, J., & Das Bit, S. (2021). LEADER: Low overhead rank attack detection for securing RPL based IoT. In **2021 International Conference on COMmunication Systems & NETworkS (COMSNETS)** (pp. 429–437). IEEE. https://doi.org/10.1109/COMSNETS51098.2021.9352937
10. Kharrufa, H., Al-Kashoash, H. A. A., & Kemp, A. H. (2019). RPL-based routing protocols in IoT applications: A review. IEEE Sensors Journal, 19(15), 5952–5967. https://doi.org/10.1109/JSEN.2019.2910881
11. Mitchel, C., Ghaleb, B., Ghaleb, S., Jaroucheh, Z., & Al-Rimy, B. (2020). The impact of mobile DIS and rank-decreased attacks in Internet of Things networks. International Journal of Engineering and Advanced Technology, 10(2), 66–72.
12. Musaddiq, A., Zikria, Y. B., Zulqarnain, & Kim, S. W. (2020). Routing protocol for Low-Power and Lossy Networks for heterogeneous traffic network. EURASIP Journal on Wireless Communications and Networking, 2020(1), Article 21. https://doi.org/10.1186/s13638-020-1645-4
13. Rafea, S. A., & Kadhim, A. A. (2019). Routing with energy threshold for WSN-IoT based on RPL protocol. Iraqi Journal of Computer, Communication, Control and Systems Engineering, 19(1), 71–81.
14. Rouissat, M., Belkehir, M., Mokaddem, A., Bouziani, M., & Alsuakyti, I. (2024). Exploring and mitigating hybrid rank attack in RPL-based IoT networks. Journal of Electrical Engineering, 75(3), 204–213. https://doi.org/10.2478/jee-2024-0027
15. Sejaphala, L., Malele, V., & Lugayizi, F. (2024). Machine learning algorithms to defend against routing attacks on the Internet of Things: A systematic literature review. Journal of Information Systems and Informatics, 6(3), 2048–2063. https://doi.org/10.51519/journalisi.v6i3.944