Trust-Aware Distributed and Hybrid Intrusion Detection for Rank Attacks in RPL IoT Environments

Bruno Monteiro * and Jorge Granjal *

Posted Date: 31 October 2025

doi: 10.20944/preprints202510.2471.v1

Keywords: RPL; IoT security; Intrusion Detection System; rank attack; trust model; LLN; mobility; Cooja; Contiki-NG

Article

Trust-Aware Distributed and Hybrid Intrusion Detection for Rank Attacks in RPL IoT Environments

Bruno Monteiro * and Jorge Granjal *

University of Coimbra, CISUC Centre - for Informatics and Systems of the University of Coimbra, Department of Informatics Engineering, Coimbra Portugal

* Correspondence: uc2012178617@student.uc.pt (B.M.); jgranjal@dei.uc.pt (J.G.)

Abstract

The rapid expansion of Internet of Things (IoT) systems in critical infrastructures has raised significant concerns regarding network security and reliability. In particular, RPL (Routing Protocol for Low-Power and Lossy Networks), widely adopted in IoT communications, remains vulnerable to topological manipulation attacks such as Decreased Rank, Increased Rank, and the less-explored Worst Parent Selection (WPS). While several RPL security approaches address rank manipulation attacks, most assume static topologies and offer limited support for mobility. Moreover, trust-based routing and hybrid IDS (Intrusion Detection System) approaches are seldom integrated, which limits detection reliability under mobility. This study introduces a unified IDS framework that combines mobility awareness with trust-based decision-making to detect multiple rank-based attacks. We evaluate two lightweight, rule-based IDS architectures: a fully distributed model and a hybrid model supported by designated monitoring nodes. A trust-based mechanism is incorporated into both architectures, and their performance is assessed under static and mobile scenarios. Results show that while the distributed IDS provides rapid local responsiveness, the hybrid IDS maintains more stable latency and packet delivery under mobility. Additionally, incorporating trust metrics reduces false alerts and improves detection reliability while preserving low latency and energy usage, supporting time-sensitive applications such as healthcare monitoring.

Keywords: RPL; IoT security; Intrusion Detection System; rank attack; trust model; LLN; mobility; Cooja; Contiki-NG

1. Introduction

As Internet of Things (IoT) devices become increasingly prevalent in domains such as industrial automation, smart healthcare, and energy distribution, the resilience and security of underlying communication protocols face growing demands. Among these, the Routing Protocol for Low-Power and Lossy Networks (RPL) has emerged as a standard for constrained network environments. However, its reliance on self-organizing topologies makes it susceptible to various rank-based attacks that compromise route consistency, degrade performance, and threaten system availability.

Although several solutions have been proposed to detect rank manipulation attacks in RPL networks, most rely on static assumptions or centralized coordination, which limits their effectiveness in dynamic IoT environments. Trust-based routing strategies have shown potential to improve decision reliability, but are rarely integrated with intrusion detection mechanisms, and existing hybrid IDS models do not account for node mobility. Consequently, current approaches struggle to maintain stable network performance and detection accuracy under changing topologies. This gap highlights the need for lightweight IDS architectures that can combine trust evaluation with both distributed and coordinated detection while operating effectively in mobile scenarios.

This work investigates the design and performance of IDS strategies tailored to detect and mitigate three critical types of RPL attacks: Decreased Rank, Increased Rank, and Worst Parent Selection (WPS).

 doi:10.20944/preprints202510.2471.v1

We consider two IDS approaches: a distributed model, in which every node independently monitors its local neighborhood, and a hybrid model, where monitoring responsibilities are partially centralized through designated Global IDS nodes. In addition, we embed a trust-based evaluation mechanism that leverages dynamic network metrics to improve decision accuracy.

Two IDS models were designed and implemented in this study: the distributed and the hybrid architectures, both specifically adapted for RPL-based IoT networks. These models aim to provide robust protection against topological attacks while preserving the low-resource nature of such environments. The main contributions of this work can be summarized in three points. First, we integrate a trust index that enhances decision-making by incorporating key dynamic parameters such as communication success rate, node mobility, link stability, and residual energy levels.

Second, a comparative evaluation is conducted to assess the behavior of both IDS architectures in scenarios with and without node mobility. This analysis enables us to examine how various network dynamics affect detection performance and resource utilization. Lastly, we perform a detailed examination of each model in terms of detection efficacy, resource consumption, communication overhead, and end-to-end delay. These results provide a comprehensive understanding of the trade-offs involved and support informed decisions on deploying lightweight security mechanisms in critical IoT infrastructures.

2. Technical Background

A concise overview of the core technologies supporting the proposed IDS models is presented, with emphasis on communication protocols and architectural models relevant to constrained IoT environments.

2.1. RPL and LLN Architectures

The Routing Protocol for Low-Power and Lossy Networks (RPL), defined in RFC 6550, is the standard for routing in constrained IoT environments. It organizes the network into a Destination-Oriented Directed Acyclic Graph (DODAG), where each node determines its position through a scalar metric known as rank. Routing decisions are influenced by an Objective Function (OF) and routing metrics such as hop count, Expected Transmission Count (ETX), and energy [16].

RPL operates on top of IPv6 and is optimized for 6LoWPAN networks, enabling IP-based communication over IEEE 802.15.4 links [16]. Its lightweight design, however, makes it susceptible to topological manipulation attacks, particularly those exploiting the rank metric to distort routing paths or isolate nodes.

2.2. IEEE 802.15.4e and 6TiSCH

IEEE 802.15.4e introduces the Time Slotted Channel Hopping (TSCH) mode to improve reliability and energy efficiency in LLNs. TSCH mitigates interference and multipath fading by combining time synchronization and frequency hopping. The 6TiSCH stack integrates TSCH with IPv6 networking, enabling deterministic and low-latency communication in industrial and critical applications [3].

6TiSCH defines a minimal configuration for scheduling communication slots and introduces the concept of cells, which are time/frequency resources allocated for communication. The presence of a schedule manager allows dynamic adjustment of communication resources, critical for adapting to traffic variations and maintaining QoS guarantees [3].

2.3. CoAP

The Constrained Application Protocol (CoAP) is a lightweight RESTful protocol designed for constrained devices and low-bandwidth networks. It supports asynchronous communication and integrates with the UDP transport layer, enabling minimal overhead[1].

The communication protocols and architectural models outlined above form the foundation of constrained IoT networks, but also expose inherent vulnerabilities. In particular, the rank-based operation of RPL and the reliance on lightweight protocols such as IEEE 802.15.4e/6TiSCH and CoAP,

 doi:10.20944/preprints202510.2471.v1

while enabling scalability and efficiency, leave the network susceptible to topological manipulation and resource exhaustion attacks. These vulnerabilities have motivated a wide range of research efforts seeking to enhance resilience, improve routing reliability, and design intrusion detection mechanisms tailored to the limitations of LLNs. The following section reviews these studies, highlighting existing approaches to securing RPL against rank-related threats and identifying the gaps that guide the contributions of this work.

3. Related Work

The vulnerability of the RPL protocol to topological manipulation has been thoroughly analyzed in several studies.

Ambarkar et al. [6] investigate the impact of Increased Rank and Decreased Rank attacks in RPL-based 6LoWPAN networks, employing Contiki and Cooja for simulation. Their work demonstrates that such attacks lead to energy overhead, reduced packet delivery ratio (PDR), and increased control traffic, ultimately impairing RPL's self-healing mechanisms.

Similarly, Hkiri et al. [7] evaluate the effects of Decreased Rank attacks under both static and mobile scenarios using the Random Direction Mobility (RDM) model. They show that such attacks significantly degrade throughput and increase average end-to-end delay (AE2ED) and energy consumption.

Bang et al. [8] further extend this analysis by incorporating node mobility and different attacker placements. Their findings indicate that attackers positioned closer to the sink node cause a more severe drop in PDR and induce higher control message overhead, making attack positioning a critical factor in network degradation.

Nandhini et al. [9] review the limitations of existing rank attack mitigation techniques in resource-constrained IoT environments. The authors highlight that while cryptographic and trust-based approaches are promising, they often struggle to adapt to dynamic topologies, revealing a gap that motivates hybrid and adaptive detection architectures.

Althubaity et al. [5] proposed FORCE, which introduces a distributed, rule-based IDS for detecting multiple types of rank-related attacks, including Worst Parent Selection (WPS). Each node independently monitors parent-child relationships in DIO and DAO messages, triggering isolation procedures upon detecting anomalies.

Bang et al. [10] propose EMBOF-RPL, which introduces a new "echelon" metric into the DIO message structure and modifies the objective function to ensure rank consistency. The method allows for early detection and isolation of malicious nodes, outperforming existing solutions in both precision and energy consumption.

Verma et al. [11] present a comprehensive taxonomy of RPL threats and countermeasures, emphasizing hybrid IDS architectures that combine centralized coordination with local monitoring. Their work underscores the importance of balancing detection accuracy with energy and latency constraints.

Muzammal et al. [15] introduce SMTrust, a trust-based model for RPL security that incorporates multiple metrics such as energy level, historical behavior, mobility, and link stability. Implemented in Contiki-NG with the BonnMotion mobility plugin, SMTrust achieves superior performance in packet loss reduction and topological stability, even under dynamic conditions.

Ioulianou et al. [12] propose SRF-IoT, a framework that integrates trust-based parent selection (SRF-OF) and a reactive IDS (SRF-IDS). Their system operates in a decentralized fashion and achieves significant improvement in packet delivery ratio by avoiding untrusted nodes.

Remya et al. [13] present TIDSRPL, a centralized trust-based IDS capable of detecting rank, sinkhole, and Sybil attacks. It leverages behavioral and location-based metrics to isolate malicious nodes with minimal performance overhead.

Mohajerani et al. [14] develop MCTE-RPL, which combines trust evaluation and IDS mechanisms in a distributed RPL extension. The protocol enhances routing decisions through a new objective

 doi:10.20944/preprints202510.2471.v1

function (TQAOF) and shows notable improvements in throughput and energy consumption under adversarial conditions.

While existing solutions have significantly advanced the state of the art in RPL attack detection, most approaches remain either purely centralized or lack adaptability in mobile topologies. Specification-based systems such as FORCE [5] and EMBOF-RPL [10] offer high detection accuracy but are limited in scalability. Conversely, trust-based models like SMTrust [15] and SRF-IoT [12] provide improved adaptability but often rely on centralized architectures or incur additional computational cost.

None of the reviewed works simultaneously addresses the combination of mobility, trust-based decision-making, and the usage of hybrid detection approaches while targeting a wide spectrum of rank-based attacks, including the less-explored Worst Parent Selection. This motivates the development of the lightweight, rule-based IDS models proposed in this investigation, designed to improve detection reliability and maintain communication performance in critical IoT infrastructures.

4. System Model and Assumptions

The system model is defined by a set of underlying assumptions, including the network topology, attacker model, and trust metric composition adopted in the proposed evaluation framework.

The simulated network follows a low-power and lossy network (LLN) architecture designed to support critical IoT applications that demand reliable communication, low latency, and energy efficiency. Such environments, including industrial automation, healthcare monitoring, and smart grid infrastructures, require routing protocols that can operate effectively under constrained resources while maintaining resilience against failures and attacks. To this end, the network is structured using the RPL protocol operating over IEEE 802.15.4e TSCH, with support from 6LoWPAN and 6TiSCH to enable IPv6-based communications. As a representative case, the framework is aligned with smart health deployments, where timely and secure data delivery is fundamental for patient monitoring and medical decision-making.

Two architectural variants are explored:

- **Distributed IDS model -** Each node individually monitors neighbor behavior and makes local decisions.
- **Hybrid IDS model -** Local detection nodes generate alerts that are then processed by a subset of designated global nodes responsible for security decisions (e.g., isolation of suspicious nodes).

The simulated network consists of one root node, multiple regular nodes with local IDS capabilities, a smaller set of global IDS nodes (only in the hybrid model), and a subset of malicious nodes. In certain experiments, node mobility is introduced using a Random Waypoint model to reflect dynamic environments.

Each node is assumed to have constrained resources, limited energy, and low processing capacity, as is typical in LLN scenarios. Communication follows the DODAG structure defined by RPL, where each node selects preferred parents based on routing metrics and trust evaluations.

4.1. Attacker Model

The system considers three primary topological manipulation attacks targeting the RPL protocol [4]:

- **Decreased Rank Attack -** Malicious nodes advertise artificially low rank values to attract child nodes, thereby disrupting the routing structure and potentially intercepting traffic.
- **Increased Rank Attack -** Attackers announce artificially high ranks to avoid participation in forwarding, effectively reducing network reliability.
- **Worst Parent Selection (WPS) -** Attackers continuously advertise poor link metrics to legitimate nodes, causing them to make suboptimal parent selections.

 doi:10.20944/preprints202510.2471.v1

Malicious nodes are capable of emitting crafted DIO messages and manipulating rank and routing metric fields. These nodes do not cooperate with the IDS mechanism and attempt to evade detection by limiting the frequency or visibility of malicious behavior. Attacks may target both static and mobile environments.

4.2. Trust Metric Composition

To enhance detection reliability and reduce false positives in dynamic environments, a trust-based decision-making mechanism is integrated into the IDS logic. Trust evaluation is based on six distinct metrics:

- **Historical Success Rate (HSR) -** Ratio of successfully forwarded packets.
- **Current Energy Level (CEL) -** Remaining energy level as a percentage.
- **Stability (STB) -** Frequency of parent changes in recent time windows.
- **Mobility (MOB) -** Variation in node position over time (only in mobile scenarios).
- **Recommendation (REC) -** Trust information received from neighboring nodes.
- **Link Quality (LQ) -** Communication metrics such as ETX and RSSI derived from DIO exchanges.

Each metric is normalized and assigned a corresponding weight to reflect its relevance in the current network context. These values are then combined to compute the final *Trust Index (TI)* using the following formula:

$$\begin{aligned} TI = \; & w_1 \cdot HSR + w_2 \cdot CEL + w_3 \cdot STB \\ & + w_4 \cdot MOB + w_5 \cdot REC + w_6 \cdot LQ \end{aligned}$$

where $w_1, w_2, \ldots, w_6$ are the weights associated with each trust metric, such that $\sum_{i=1}^{6} w_i = 1$.

The computed TI is applied in two critical RPL operations: (i) guiding the parent selection process during routing, and (ii) assessing the legitimacy of neighbor behavior in the IDS context. In standard RPL, parent selection is performed according to the Objective Function (OF), which typically prioritizes rank values and routing metrics such as ETX. In our framework, this process was extended through a customized function, where the trust index of candidate neighbors is evaluated prior to rank.

Nodes whose trust index falls below a predefined threshold ($TI < 0.5$) are marked as suspicious. If the condition persists over successive observation windows, the node is classified as malicious and subject to isolation by the IDS. This threshold was selected to balance detection sensitivity and false positive mitigation, as demonstrated in the experimental validation.

This trust-based evaluation helps stabilize parent selection decisions by adapting to temporary performance fluctuations, reducing the risk of misclassifying benign nodes during mobility.

4.3. Parent Selection

An extended mechanism for trustworthy parent selection was implemented to incorporate the proposed trust model. In this version, the parent selection process prioritizes the trust index of candidate nodes, while the RPL Rank is used solely as a secondary criterion in the case of a tie. This adjustment aims to enhance the reliability of routing decisions by favoring nodes that demonstrate consistent and trustworthy behavior over time.

During the selection process, a candidate node is considered valid only if it is not included in the blacklist and does not correspond to the sink node. Furthermore, its trust index must exceed a predefined threshold to qualify for consideration. Among the valid candidates, the node with the highest trust index is selected as the preferred parent. In scenarios where two or more candidates present the same trust index, the node with the lowest Rank is chosen, ensuring that routing efficiency is preserved while maintaining a high level of trustworthiness in the network topology.

In terms of RPL control message exchange, this strategy primarily impacts the interpretation and propagation of existing control messages:

 doi:10.20944/preprints202510.2471.v1

- **DIO (DODAG Information Object)** messages remain the main vehicle for disseminating topology information. In the proposed approach, whenever the preferred parent changes due to trust index variations, the Trickle Timer is reset, prompting the immediate dissemination of updated DIOs. The Rank field contained in the DIO continues to serve its original role, but it is now subordinated to the trust index in the decision-making process. Additionally, before accepting a DIO, the receiving node checks whether the sender is present in the blacklist, discarding its information if so.
- **DAO (Destination Advertisement Object)** messages are not directly modified. However, the downward routes they establish naturally reflect the trusted parent relationships, as only nodes surpassing the trust threshold are allowed to propagate routing information.
- **DIS (DODAG Information Solicitation)** messages also remain unchanged. Their role in requesting new DIOs is preserved, while the trust-based filtering is exclusively applied during the processing of the received DIOs.

To support these decisions, each node maintains a trust index for its neighbors, updated locally according to the selected metrics. This value is stored together with the neighbor's routing information, ensuring that parent selection integrates both the trust evaluation and the RPL rank. Furthermore, a blacklist structure is maintained to register malicious or suspicious nodes. During parent selection, any neighbor present in the blacklist or with a trust index below the defined trust threshold is disregarded, regardless of its advertised Rank.

Finally, the implemented strategy also includes an adaptive and periodic reaction mechanism. A local event timer triggers regular evaluations of neighbors' trust indices to ensure that parent selection remains aligned with the most recent observations. Whenever the preferred parent changes, the reset of the Trickle Timer ensures that updated routing information is promptly disseminated across the network, reinforcing stable and secure routes.

5. Implementation

The operational logic of the two IDS models proposed in this work is described, namely the distributed IDS and the hybrid IDS. Both models were designed to detect and mitigate topological manipulation attacks in RPL-based IoT networks, particularly targeting the rank attacks. The core difference lies in the distribution of detection and response responsibilities, as illustrated in the flow diagrams provided by Figure 1 and 2.

 doi:10.20944/preprints202510.2471.v1

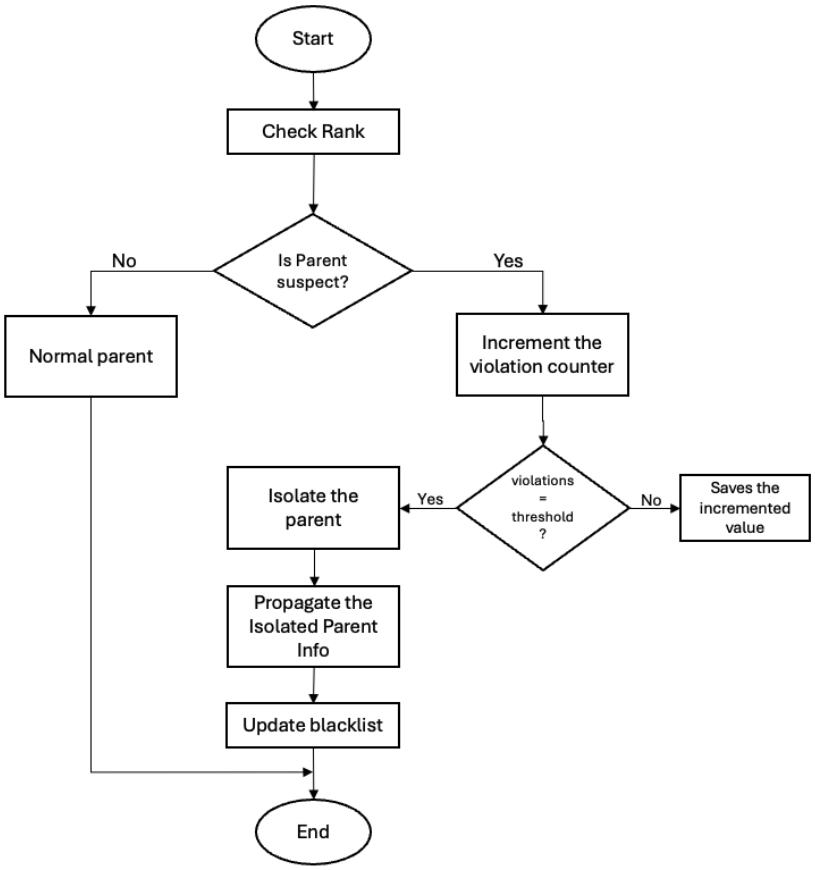

Figure 1. Distributed IDS operation at node level.

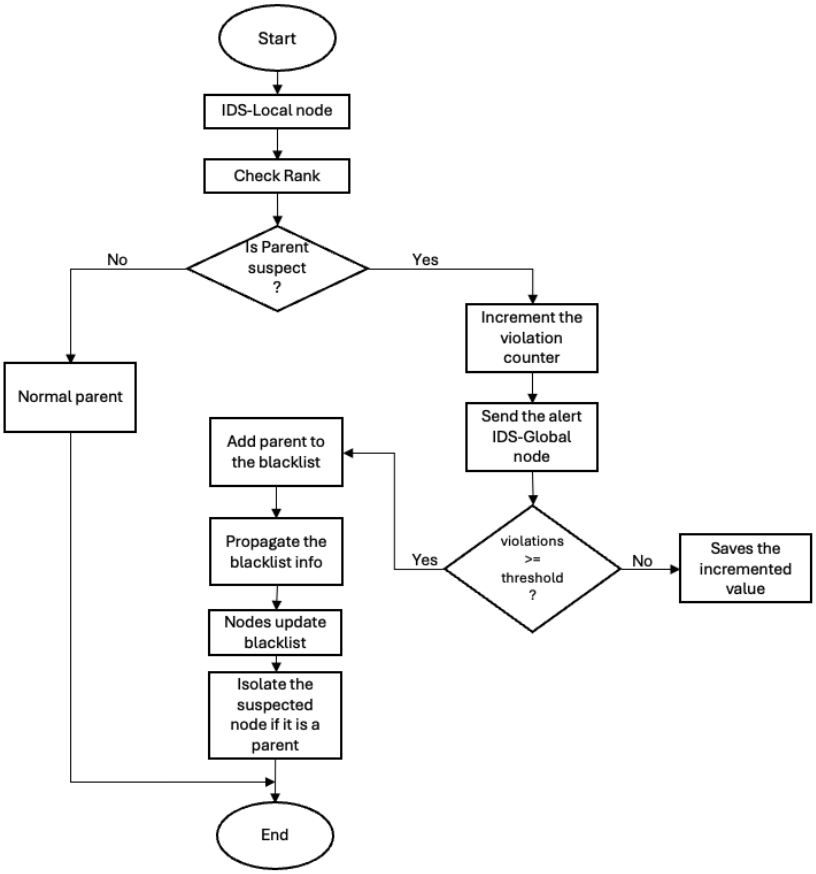

Figure 2. Hybrid IDS operation at node level.

 doi:10.20944/preprints202510.2471.v1

5.1. Distributed IDS

In the distributed IDS architecture, each node is equipped with full detection and response capabilities. The operational flow begins with the periodic verification of the parent node's RPL rank. If the parent node exhibits suspicious behavior, such as a significant drop in rank or inconsistencies with previous observations, the local node increments a violation counter associated with that parent.

Once the number of violations exceeds a predefined threshold, the node autonomously isolates the malicious parent by removing it from the preferred parent list and updating its local blacklist. This action is followed by the propagation of a notification through the RPL control plane, typically via modified DIO messages. The process ensures that isolated nodes are no longer selected as valid parents by other nodes. Metrics related to energy, latency, and detection performance are then updated locally.

The distributed IDS approach enables a fast and autonomous response to attacks, enhancing resilience in dynamic topologies. However, the absence of global coordination may lead to inconsistent detection thresholds across the network.

5.2. Hybrid IDS

The hybrid IDS architecture introduces a division of roles between IDS-Local and IDS-Global nodes. In this model, all nodes perform rank verification locally and maintain a local counter of suspicious behavior. When an anomaly is detected, an IDS-Local node sends an alert message via UDP to all IDS-Global nodes, including the suspect's identifier and the updated violation count.

IDS-Global nodes aggregate these alerts and evaluate whether the accumulated violations for a given node exceed a central threshold. If confirmed, the node is marked as malicious and added to a global blacklist. The blacklist is then propagated through a UDP multicast to the entire network. Upon receiving this update, each node checks if its current parent is blacklisted and, if so, initiates isolation procedures.

This collaborative mechanism enables cross-verification among multiple IDS-Local reports before enforcing isolation, thereby reducing false positives and improving detection accuracy. The hybrid IDS model also offers improved scalability and communication efficiency, particularly in mobile environments.

This comparison highlights that the distributed IDS prioritizes rapid and autonomous responses, offering robustness in highly dynamic scenarios but lacking global coordination, which may lead to inconsistent decisions. Conversely, the hybrid IDS leverages collaborative validation and centralized blacklisting, improving detection accuracy and scalability at the cost of additional communication overhead. These complementary characteristics motivate the experimental evaluation presented in the next section, where both models are systematically assessed under diverse attack and mobility scenarios.

6. Evaluation

The evaluation phase is essential to assess the effectiveness and feasibility of the proposed IDS models under realistic IoT networking conditions. The analysis considers both static and mobile environments, with and without the integration of trust metrics, enabling a comprehensive comparison of the distributed and hybrid architectures in terms of energy efficiency, latency, detection accuracy, packet delivery reliability, and communication overhead.

6.1. Experimental Setup

To validate the proposed IDS models, a series of simulations was conducted using the Contiki-NG operating system and the Cooja network simulator. Each simulation scenario included 30 nodes randomly deployed in a 100m × 100m area, operating over IPv6 with IEEE 802.15.4e TSCH and 6TiSCH stack. Simulations were executed for a total duration of 600 seconds per run.

 doi:10.20944/preprints202510.2471.v1

To emulate dynamic conditions, node mobility was introduced in specific scenarios using the Random Waypoint mobility model. This mobility trace was generated using the BonnMotion tool [2]. Table 1 summarizes the parameters used in the mobility trace generation.

Table 1. Random Waypoint mobility model parameters.

Parameter	Value
Output file name (-f)	randomwaypoint-ids
Number of mobile nodes ($-n$)	7
Simulation duration ($-t$)	600 s
Simulation area ($-x$, $-y$)	100 m $\times$ 100 m
Node distribution ($-d$)	Uniform random
Pause time ($-R$)	0 (continuous movement)
Mobility model	Random Waypoint

The output was converted to a format compatible with Cooja using the cooja-mobility extension, allowing realistic mobility patterns to be applied to the selected nodes while preserving time synchronization across the simulation.

Additionally, the CoAP protocol was deployed on two dedicated nodes (client and server) to simulate application-layer traffic representative of real-time monitoring tasks. This setup enabled the evaluation of end-to-end latency in the presence of both mobility and topological attacks, from the perspective of the application layer. In particular, this allows assessing how fluctuations in routing stability can affect time-sensitive IoT services such as remote patient monitoring and other medical applications, where delayed data delivery can compromise system reliability.

Each simulation run tested both the distributed and hybrid IDS models under three attack types: Decreased Rank, Increased Rank, and Worst Parent Selection (WPS). Metrics were collected to assess energy consumption (CPU, LPM, TX, RX), RPL control message overhead (DIO, DAO, DIS), CPU load, packet delivery ratio (PDR), average latency, and IDS detection efficiency (true positives, false positives, false negatives). All simulations were repeated five times per scenario to ensure statistical significance.

6.2. Results and Discussion

The experimental results obtained from the implementation and simulation of the proposed IDS models are analyzed by evaluating both the distributed and hybrid IDS under identical scenarios, considering static and mobile environments, with and without the integration of trust metrics. The evaluation not only targets the measurement of overhead on resource-constrained IoT devices but also examines the effectiveness of the detection strategy under varying network conditions. The comparison focuses on five key performance indicators: energy consumption, latency, detection rate, packet delivery ratio (PDR), and communication overhead. The results presented in this section are derived from extensive simulations encompassing multiple scenarios — both static and mobile — with and without the integration of trust metrics. To guarantee the reliability and consistency of the obtained results, each simulation scenario was repeated five times, and the average and standard deviation values were computed. For clarity, the discussion is supported by selected representative graphs that illustrate the most relevant trends observed across the experiments. These visualizations focus on key aspects such as detection accuracy and packet delivery ratio under Increased Rank attacks, contrasting the behavior of distributed and hybrid IDS configurations.

6.2.1. Energy Consumption

The distributed IDS consistently exhibited higher CPU usage across all scenarios due to the decentralized nature of its detection mechanism, which forces all nodes to execute complex monitoring and decision logic. The hybrid IDS demonstrated more efficient energy usage, especially in Local nodes, which are only responsible for monitoring and forwarding alerts. The inclusion of trust metrics

 doi:10.20944/preprints202510.2471.v1

introduced a slight increase in processing load, particularly in the distributed IDS. However, this additional consumption did not compromise the operational feasibility of battery-powered devices, as the overall resource usage remained below thresholds typically associated with significant reductions in node lifetime.

6.2.2. Latency

The latency was extensively assessed across all simulated scenarios. The results indicate that the hybrid IDS model consistently outperforms the distributed IDS in terms of latency, regardless of the attack type or the presence of node mobility. In static environments, the hybrid architecture achieved lower average latencies, benefiting from centralized decision-making and reduced local processing delays. In contrast, the distributed model exhibited slightly higher latencies, attributed to the overhead of decentralized alert generation and immediate response mechanisms.

Under mobility conditions, both architectures experienced a marginal increase in latency due to route rediscovery and node repositioning. However, the hybrid model demonstrated greater resilience, maintaining more stable latency values compared to the distributed model, which showed greater variability and occasional delays. Importantly, the integration of the trust-based decision mechanism had no significant negative impact on latency. In some cases, it contributed to a modest improvement by filtering false positives and enhancing route stability. These findings confirm that the proposed IDS models, particularly the hybrid configuration, are suitable for deployment in latency-sensitive IoT infrastructures.

6.2.3. Detection Performance

The detection rate was evaluated through true positives, false positives, and false negatives. While the distributed IDS offered immediate detection capabilities, its lack of global consensus sometimes led to premature, incorrect, or late isolation decisions. In contrast, the hybrid IDS achieved superior accuracy by relying on corroborated alerts received from multiple nodes, enabling more informed decisions. The integration of trust metrics further enhanced detection precision in both models by filtering out transient anomalies and reinforcing alerts based on multi-dimensional trust evaluation. This significantly reduced false positives, particularly in mobile scenarios. Figures 3 and 4 illustrate the detection performance of the hybrid IDS under Increased Rank attacks, highlighting its superior resilience in mobile scenarios compared to the distributed IDS.

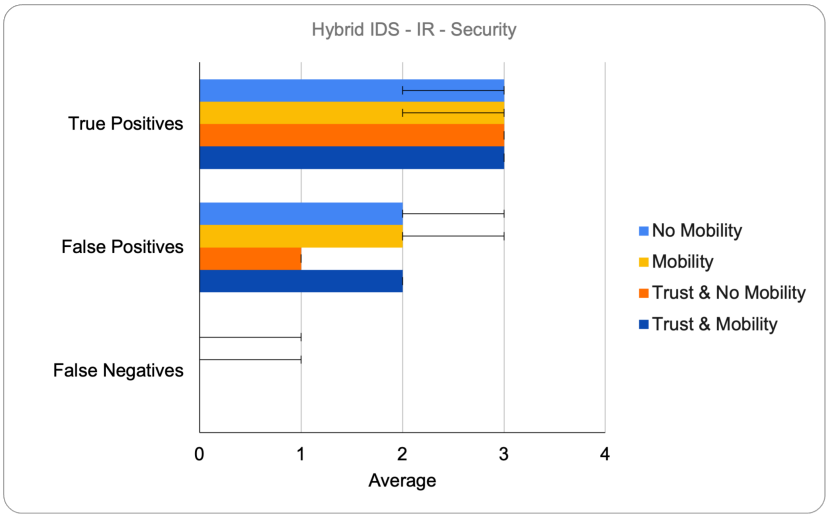

Figure 3. Hybrid IDS - Increased Rank attack - Detection Accuracy.

 doi:10.20944/preprints202510.2471.v1

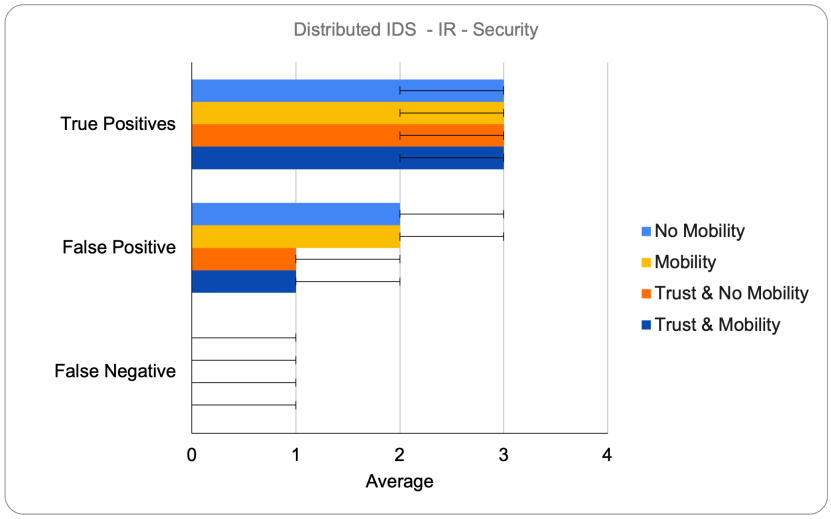

Figure 4. Distributed IDS - Increased Rank attack - Detection Accuracy.

6.2.4. Packet Delivery Ratio (PDR)

PDR analysis revealed that the distributed IDS experienced greater packet loss in mobile scenarios, primarily due to excessive route recalculations following false or unnecessary isolations. These disruptions frequently originated from transient topology changes being misinterpreted as attacks. The hybrid IDS maintained more stable routing structures, benefiting from centralized isolation decisions and reduced network churn. The use of trust-based parent selection—favoring nodes with stable behavior, low mobility, and consistent forwarding success—helped both architectures sustain higher PDR values by promoting reliable and less disruptive routing paths. Figures 5 and 6 present representative PDR results for both hybrid and distributed IDS models under Increased Rank attacks. The graphs show that the hybrid architecture sustains higher delivery ratios, even in mobile scenarios, while the distributed model exhibits greater degradation due to excessive isolation.

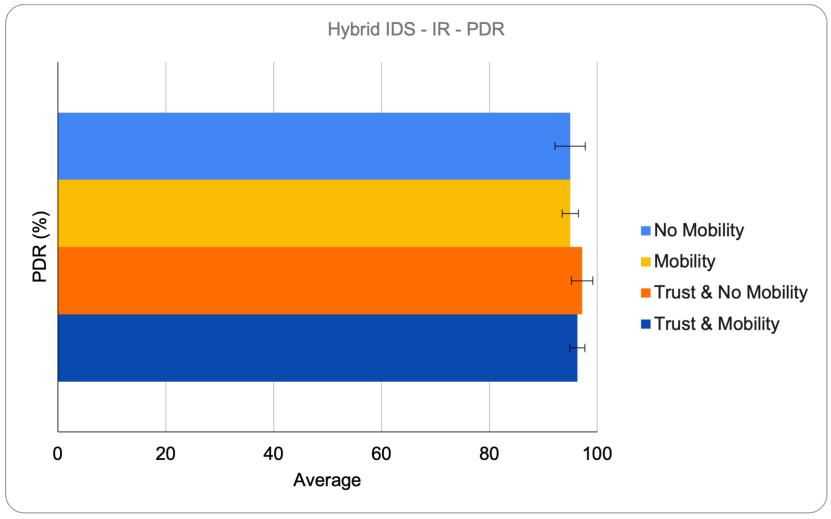

Figure 5. Hybrid IDS - Increased Rank attack - PDR.

 doi:10.20944/preprints202510.2471.v1

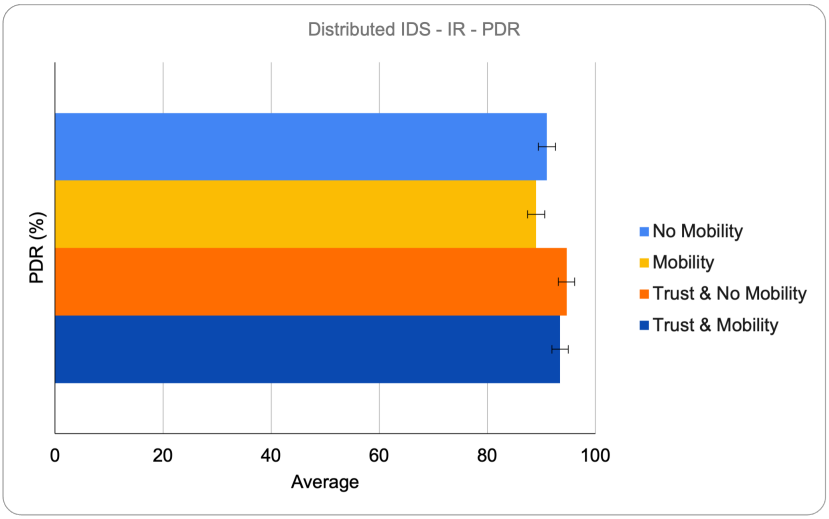

Figure 6. Distributed IDS - Increased Rank attack - PDR.

6.2.5. Communication Overhead

The distributed IDS generated a higher number of control messages due to the active participation of all nodes and the reactive propagation of DIO messages upon isolation. In contrast, the hybrid IDS required UDP-based communication for alert propagation and blacklist coordination, but maintained a more predictable and controlled message exchange profile. Furthermore, the integration of the trust-based mechanism reduced redundant control traffic in both models by suppressing alerts triggered by temporary rank fluctuations. This selective filtering minimized unnecessary communication and contributed to lower overhead, especially in dynamic topologies where mobility could otherwise induce spurious detections.

Overall, the graphs included are representative examples extracted from the broader set of experiments conducted. They were selected to emphasize the main findings, particularly regarding detection accuracy and packet delivery under Increased Rank attacks, and are consistent with the trends observed across all scenarios.

7. Conclusions and Future Work

This work presented and evaluated two lightweight, rule-based Intrusion Detection System (IDS) architectures tailored for securing RPL-based IoT networks against rank manipulation attacks. Through comprehensive simulations conducted in Contiki-NG and Cooja, we assessed the performance of a fully distributed IDS and a hybrid IDS model under various conditions, including node mobility and the presence of sophisticated topological attacks.

The experimental evidence shows that, although the distributed IDS delivers swift local reactions, its decentralized alert propagation entails higher and less predictable end-to-end delays, particularly when nodes are mobile, and it remains prone to false positives and control-traffic bursts. By contrast, the hybrid IDS, despite requiring inter-node coordination, achieves consistently lower and more stable latency across all attack scenarios, while also improving detection accuracy and curbing control overhead. Crucially, the integration of the trust-based decision mechanism does not penalize latency; instead, it slightly enhances route stability by suppressing spurious alerts. These results position the hybrid IDS as the more suitable architecture for latency-sensitive and mobile IoT environments.

A key innovation in this study was the integration of a trust-based decision-making mechanism, which improved the reliability of intrusion detection and contributed to more stable parent selection under mobility. By incorporating multi-metric trust indices—reflecting energy, mobility, communication reliability, and historical behavior—both systems were able to reduce false alerts and maintain higher packet delivery ratios, particularly in mobile scenarios.

Overall, the proposed IDS models offer effective lightweight protection for RPL-based IoT networks while respecting the latency and energy constraints of time-sensitive IoT applications. Future

 doi:10.20944/preprints202510.2471.v1

work may explore adaptive thresholding, lightweight consensus schemes, and real-world testbed validation to further strengthen the applicability of trust-enhanced hybrid detection mechanisms in critical IoT infrastructures.

As future work, the experimental environment can be expanded with a larger number of malicious nodes to evaluate the scalability and robustness of the proposed models under more intensive or coordinated attack scenarios. Another promising direction is the validation of the IDS architectures in real platforms or testbeds with physical devices, thereby bridging the gap between simulation and practical deployments. Furthermore, adapting the IDS models to address other RPL attack vectors, such as Hello Flood, Sinkhole, or Selective Forwarding, will be relevant to assess the effectiveness of the distributed and hybrid detection strategies across a broader spectrum of threats.

Author Contributions: B.M. and J.G. contributed equally to the paper except for the development of the experimental scenario, which was made by B.M. All authors have read and agreed to the published version of the manuscript.

Funding: This work is funded by national funds through FCT – Foundation for Science and Technology, I.P., within the scope of the research unit UID/00326 - Centre for Informatics and Systems of the University of Coimbra.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shelby, Z.; Hartke, K.; Bormann, C. (2014). *The Constrained Application Protocol (CoAP)*. RFC 7252, RFC Editor. Available online: https://www.rfc-editor.org/info/rfc7252 (accessed on 10 October 2024). DOI: 10.17487/RFC7252.
2. BonnMotion. (2016). *A Mobility Scenario Generation and Analysis Tool*. Available online: https://sys.cs.uos.de/bonnmotion/ (accessed on 10 October 2024).
3. Watteyne, T.; Palattella, M.R.; Grieco, L.A. (2015). *Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement*. RFC 7554, RFC Editor. Available online: https://www.rfc-editor.org/info/rfc7554 (accessed on 10 October 2024). DOI: 10.17487/RFC7554.
4. 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), 248. Springer.
5. Althubaity, A.; Gong, T.; Raymond, K.-K.; Nixon, M.; Ammar, R.; Han, S. (2020). Specification-based distributed detection of rank-related attacks in RPL-based resource-constrained real-time wireless networks. In *2020 IEEE Conference on Industrial Cyberphysical Systems (ICPS)*, 1, 168–175. IEEE.
6. Ambarkar, S.S.; Shekokar, N. (2021). Impact Analysis of RPL Attacks on 6Lo WPAN based Internet of Things network. In *2021 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, 1–5. IEEE.
7. Hkiri, A.; Karmani, M.; Bahri, O.B.; Murayr, A.M.; Alasmari, F.H.; Machhout, M. (2024). RPL-Based IoT Networks under Decreased Rank Attack: Performance Analysis in Static and Mobile Environments. *Computers, Materials & Continua*, **78**(1).
8. Bang, A.; Rao, U.P. (2023). Impact analysis of rank attack on RPL-based 6LoWPAN networks in Internet of Things and aftermaths. *Arabian Journal for Science and Engineering*, **48**(2), 2489–2505. Springer.
9. Nandhini, P.S.; Kuppuswami, S.; Malliga, S. (2023). Energy efficient thwarting rank attack from RPL based IoT networks: a review. *Materials Today: Proceedings*, **81**, 694–699. Elsevier.
10. Bang, A.O.; Rao, U.P. (2022). EMBOF-RPL: Improved RPL for early detection and isolation of rank attack in RPL-based internet of things. *Peer-to-Peer Networking and Applications*, **15**(1), 642–665. Springer.
11. Verma, A.; Ranga, V. (2020). Security of RPL based 6LoWPAN Networks in the Internet of Things: A Review. *IEEE Sensors Journal*, **20**(11), 5666–5690. IEEE.
12. Ioulianou, P.P.; Vassilakis, V.G.; Shahandashti, S.F. (2022). A trust-based intrusion detection system for RPL networks: Detecting a combination of rank and blackhole attacks. *Journal of Cybersecurity and Privacy*, **2**(1), 124–153. MDPI.
13. Remya, S.; Pillai, M.J.; Arjun, C.; Subbareddy, S.R.; Cho, Y. (2024). Enhancing Security in LLNs using a Hybrid Trust-Based Intrusion Detection System for RPL. *IEEE Access*. IEEE.

 doi:10.20944/preprints202510.2471.v1

14. Mohajerani, J.; Ghanatghestani, M.M.; Hashemipour, M. (2024). MCTE-RPL: A Multi-Context Trust-based Efficient RPL for IoT. *Journal of Network and Computer Applications*, 103937. Elsevier.
15. Muzammal, S.M.; Murugesan, R.K.; Jhanjhi, N.Z.; Humayun, M.; Ibrahim, A.O.; Abdelmaboud, A. (2022). A trust-based model for secure routing against RPL attacks in internet of things. *Sensors*, **22**(18), 7052. MDPI.
16. Alexander, R.; Brandt, A.; Vasseur, J.P.; Hui, J.; Pister, K.; Thubert, P.; Levis, P.; Struik, R.; Kelsey, R.; Winter, T. (2012). RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. *RFC 6550*, RFC Editor, 157 pages. Available online: https://www.rfc-editor.org/info/rfc6550.