A Review of Security Challenges and Intrusion Detection Mechanisms to Mitigate Sub-Optimization Attacks in RPL-Based 6LoWPAN IoT Networks

Angel D[1]*, and Dr. Robin Rohit Vincent[2]

***Abstract*—The Internet of Things (IoT) has transformed device connectivity with the smooth interfacing for real-time data exchange across multiple applications, from smart homes to industrial automation. Nonetheless, as networks under IoT, especially those using the routing protocol for low-power and lossy networks (RPL), continue in their expansion, the security penetration becomes much more evident. One of the major security constraints is sub-optimization attacks-they negatively affect network performance, scalability, and data integrity. These attacks impede the very efficiency of the IoT systems, thereby making it so challenging for the systems to be secured and maintained successfully. Traditional IDS and cryptographic solutions are seldom fit-for-purpose in dynamic IoT environments, which opens up the need for the ability to provide scalable and energy-aware security solutions. This review investigates and surveys existing IDS, cryptographic solutions, and machine learning techniques targeting and working against such threats. It puts forth an integrated solution where an adaptive IDS is combined with scalable, energy-efficient, real-time anomaly detection to make IoT networks more resilient to sub-optimization attacks. According to this study, dynamic, context-aware safety measures are essential, as they are capable of addressing the new challenges arising from IoT environments.**

***Index Terms*—Internet of Things, Routing Protocol for Low-Power and Lossy Networks, Intrusion Detection Systems, sub-optimization attacks, and security mechanisms.**

I. INTRODUCTION

IoT has changed how systems and devices are capable of speaking to one another seamlessly, whether in an application for a smart home or healthcare facility, in industrial automation and transport sectors, while a lot of IoT networks are also expanding with connected devices in vast numbers to the extent of billions in exchange for exchanging large data in real time [1]. However, this growth raises major security risks, as weak protection of sensitive sensor data leads to breaches with economic and safety consequences [2].

[1]* PhD scholar, Presidency School of Computer Science and Engineering Presidency University, Bengaluru, Rajanukunte, Yelahanka, Bangalore North, Karnataka. (e-mail: ANGEL.20233CSC0005@presidencyuniversity.in, Angelveena.praveena@gmail.com)

[2] Professor and Head, Nvidia - CoE
Presidency School of Computer Science and Engineering, Presidency University, Bengaluru, Rajanukunte, Yelahanka, Bangalore North, Karnataka. (e-mail: robinrohit.vincent@presidencyuniversity.in, robinrohit@gmail.com)

DOI: 10.36244/ICJ.2026.1.10

Security is difficult due to limited resources, dynamic topologies, and diverse protocols [3]. IoT networks face threats such as data manipulation, DoS, and unauthorized access, endangering critical sectors like energy, healthcare, and transport. To address this, research focuses on cryptography, authentication, IDS, and AI-driven threat detection [4]. The review emphasizes scalability, adaptability, and resource issues in IoT security. Its aims are to:

- Examine threats in RPL-based 6LoWPAN, with emphasis on sub-optimization attacks.
- Investigate IDS frameworks and their weaknesses/strengths.
- Evaluate impacts of attacks on performance, efficiency, and scalability.
- Explore solutions such as dynamic/compressive IDS.
- Recognize research gaps in IDS optimization and scalability.
- Provide recommendations to enhance RPL-based 6LoWPAN security frameworks.

II. IOT AND RPL FUNDAMENTALS

In an IoT system (illustrated in Figure 1) four distinct components exist: sensors/devices, connectivity, data processing, and user interface. Sensors, which can be simple (e.g., temperature) or sophisticated (e.g., video camera), obtain real-time data from the environment. In the case of connectivity, the sensor should transmit the gathered data to the cloud using a transmission method, which includes Bluetooth, Wi-Fi, WAN, satellite, or mobile, and is retained in the cloud for further processing, and is the key for IoT implementation and is most often overlooked. Following this, the data is processed, which can be something simple like monitoring a temperature or sophisticated like computer vision or object detection. The end user then can interact with the IoT system using the user interface of notifications, alarms or live monitoring via a web server [5].

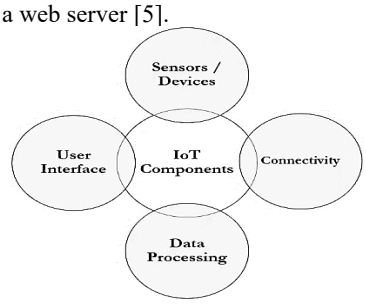

Figure 1: Components of an IoT System

A. IoT four-layer architecture

The four-layer IoT architecture consists of separate layers, with the application layer acting as a bridge between the network and devices, defining all IoT applications based on sensor data, facilitating user engagement and unique functions [6]. The perception layer sends data to the data processing layer, ensuring data safety and originates from real users. The network layer connects devices and facilitates data flow from sensors. The sensor layer detects and collects data from IoT devices, controlling their operating mechanisms for precise data gathering. These layers form a strong architecture for IoT systems, ensuring data safe and effective transmission from sensors to apps.

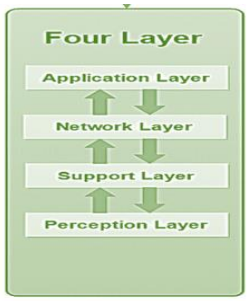

Figure 2: IoT Four-Layer Architecture

B. RPL - Network Layer Routing Protocol

RPL is a distance-vector routing protocol designed to accommodate a variety of data link layer protocols and to provide routing solutions for networks with restricted resources. RPL creates a Destination-Oriented Directed Acyclic Graph (DODAG) to ensure that each leaf node has a single path to the Root, which serves as the center for all traffic routing. The DODAG structure is established by nodes first promoting themselves as the Root by broadcasting DODAG Information Objects (DIOs), which spread throughout the network. To enable their parent nodes to make routing decisions for the destination, nodes send a Destination Advertisement Object (DAO) to them. Once the data transfer object (DTO) receives the DAO Acknowledgment (DAO-ACK), it is up to it to undertake the process to join the network. There are two modes of operation for RPL nodes: stateful and stateless. The most prevalent stateless nodes simply monitor their parent nodes, whereas the Root is fully aware of the DODAG. Stateful nodes, on the other hand, keep track of data about their parents and offspring, allowing for effective communication inside sub-trees without going via the Root. RPL is the perfect protocol for low-power and lossy situations because of its hierarchical structure and adaptable node operation.

RPL is a proactive distance-vector protocol developed by IETF for resource-constrained environments such as IoT systems running 6LoWPAN. RPL organizes nodes into a DODAG, which is rooted at a central node generally termed the gateway, acting as the destination for all traffic.

i. Key Concepts

- Rank: Indicates distance from root; exploitable for rank attacks.
- Version Number: Identifies DODAG; misuse can cause reconvergence and energy drain.
- Objective Function (OF): Guides rank/parent selection (e.g., OF0, MRHOF), affecting security and performance.

ii. RPL Control Messages

- DIO: Advertises DODAG parameters (version, rank, OF).
- DIS: Requests for DIOs for route discovery.
- DAO: Sent upstream to publish downward routes (storing mode).
- DAO-ACK: Acknowledges receipt of DAO and route advertisement.

iii. Modes of Operation

- Storing Mode: The intermediate nodes store routing tables.
- Non-Storing Mode: The root alone stores full routing information and uses source routing.

Even though optimal for low-power, lossy networks, RPL's management of rank, version numbers, and control messages provides weaknesses that facilitate sub-optimization attacks, reducing performance without stopping communication [7,8,9].

III. SUB-OPTIMIZATION ATTACKS ON RPL

Sub-optimization attacks refer to the routing layer attacks in RPL-based 6LoWPAN networks that use the weaknesses in design in the RPL protocol's objective functions and control mechanisms in order to deliberately degrade routing performance but not completely disrupt it. The attacks may involve manipulating metrics like rank values, suppressing DIO messages, triggering excessive DIS messages, or influencing parent selection so as to cause inefficient routing paths. Unlike conventional threats such as sinkhole or blackhole attacks that primarily capture or drop packets, sub-optimization attacks are usually covert and result, rather gradually, in higher latencies, energy burns, and congestion. Their subtlety makes it harder for an ordinary IDS to detect. Hence, emphasis must be put on security mechanisms that exploit deviations in performance rather than clear-cut malicious behaviors.

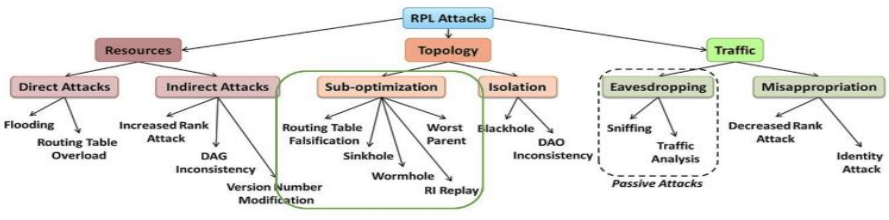

Figure 3: Classification of attacks in RPL Network

A. Routing Table Falsification

Several IoT IDS and secure routing approaches have been proposed. A hybrid SVM–Decision Tree IDS [10] achieved high accuracy with low false positives, while an ANN-based protocol [11] enhanced QoS. DETONAR [12] combined anomaly and signature detection without extra RPL overhead. A secure RPL protocol [13] mitigated DIS flooding with improved resilience, and [14] highlighted the negative impact of Hello Flood, Version Number, and Rank Reduction attacks on DODAG stability, efficiency, and scalability.

B. Sinkhole Attacks

Several solutions address sinkhole and selective forwarding in 6LoWPAN/RPL networks. A power-efficient IDS [15] achieved high detection accuracy with lightweight implementation. UVM [16] detects sinkholes via rank, power, and DIO metrics using equal voting. RFTrust [17] integrates Random Forest with trust models for reliable routing. CLS-RPL [18] uses cross-layer and overhearing mechanisms, while a multidirectional trust model [19] applies fuzzy and subjective logic with entropy-based trust weights to reduce false positives and delays.

TABLE I
COMPARISON OF SINKHOLE ATTACK DETECTION METHODS IN IOT NETWORKS

Paper	Objective	Techniques Used	Advantages	Disadvantages
[15]	Lightweight IDS for sinkhole attacks	Lightweight & Roving IDS	High performance, low energy	Limited to 6LoWPAN
[16]	Detect sinkhole nodes via behavior	UVM, Behavioral Indicators	Simple detection, effective features	Equal weight may misjudge importance
[17]	Trust-aware detection with ML	RF, SL, Trust Routing	Combines ML & trust for reliability	RF may be resource-heavy
[18]	Cross-layer sinkhole prevention	CLS-RPL, Overhearing, Secured-RPL	Stronger detection via layer integration	Overhearing adds energy cost
[19]	Multidirectional trust detection	FLS, SL, Trust Weight Adjustment	Low delay, fewer false positives	Higher complexity with adaptability

B. Wormhole Attacks

Wormhole attacks in RPL-based IoT networks create covert tunnels that disrupt routing, causing loss, delay, and integrity issues, and are harder to detect than sinkhole or blackhole attacks. Detection methods include trust models (e.g., SLF-RPL), ML frameworks using routing metrics, and traffic feature analysis. Recent solutions like MC-MLGBM [20], SLF-RPL [21], and hybrid IDSs [22] improve detection with low overhead, though wormholes remain less studied. Future work should emphasize hybrid ML–trust models for adaptive, lightweight, and scalable protection.

TABLE II
COMPARISON OF WORMHOLE ATTACK DETECTION METHODS IN RPL-BASED IOT NETWORKS

Paper	Objective	Techniques Used	Advantages	Disadvantages
[20]	To detect rank and wormhole attacks in RPL-based IoT networks	Machine Learning (MC-MLGBM Model)	Lightweight, multi-class classification, high accuracy	May require large datasets, computational overhead for training
[21]	To detect wormhole attacks using a trust model	Subjective Logic-based Trust Model (SLF-RPL)	Energy-efficient, adaptive to dynamic IoT environments	Potential delays in detecting malicious nodes, trust model sensitivity
[22]	Energy-efficient wormhole attack detection	Signal Strength, Hop Count-based Detection	Low energy overhead, suitable for constrained environments	May have detection delays in dynamic topologies

C. Other attacks

To limit IPv6 spoofing in 6LoWPAN, short-lived node addresses were suggested [23], minimizing disruption by updating addresses constantly.

An IDS based on PSO was designed [24], utilizing real-time Cooja IoT simulator information. PSO trained ML algorithms for enhanced accuracy in detecting routing threats.

A reinforcement learning (RL) agent [25] efficiently identified and prevented rank attacks in software-defined low-power IoT networks, with low latency, minimized duty cycles, and increased packet delivery ratios. An IDS model for Ping of Death attacks [26] utilized integer optimization to reduce false alarms and missed detections.

In the case of RPL routing attacks, SRPL-RP [27] resisted rank and version number tampering by ranking strategy comparison and blacklist table maintenance, supporting multiconfiguration and multiprotocol topologies.

Replay-based DoS attacks (copycat) [28] resulted in delivery degradation, energy consumption, and delay. CoSec-

RPL [30] employed Outlier Detection to counter non-spoofed copycat attacks better than baseline RPL.

To protect against DIS flooding, Secure-RPL [29] minimized control overhead and energy usage in both static and dynamic environments. In the case of version number flooding, [31] identified weaknesses in resource-constrained RPL, but only limited experiments were conducted.

TABLE III
COMPARISON OF IOT NETWORK SECURITY PAPERS

Paper	Objective	Techniques Used	Advantages	Disadvantages
[25]	Prevent rank attacks using SDN & RL	RL for route optimization, SDN for QoS	Cost-efficient, improved forwarding & latency	Higher complexity due to RL-SDN integration
[26]	Prevent Ping of Death via oversized packet filtering	Integer optimization, packet filtering	Low false alarms, reduced missed detections	Limited to DoS packet-size attacks
[27]	Detect & isolate rank/version number attacks in RPL	Secure RPL protocol	Supports multiple topologies	Focused only on rank/version threats
[28]	Study & mitigate copycat (replay) DoS attacks	Experimental analysis (delivery ratio, delay, power)	Detailed impact analysis of copycat attacks	Narrow focus, not generalizable
[29]	Mitigate DIS flooding in 6LoWPAN	Secure-RPL detection method	Reduces overhead & power drain	Attack-specific, not broadly applicable
[30]	Detect replay-based attacks with anomaly methods	Outlier Detection, CoSec-RPL IDS	Reduces replay attack effects	May miss varied replay/DoS attacks
[31]	Analyze flooding via version manipulation in RPL	Experimental performance study	Shows vulnerabilities in RPL versioning	Limited topologies, results not generalizable

IV. CURRENT SECURITY APPROACHES

A. Intrusion Detection Systems (IDS)

RPL, though widely adopted in IoT, remains vulnerable due to open environments and node constraints [32],[33]. Several IDS solutions have been proposed: a hybrid IDS with incremental ML for detecting DIO Suppression, Worst Parent, and Rank attacks [34]; an energy-aware cooperative IDS for host/edge devices [35]; and a heterogeneous IDS for dynamic 6LoWPAN environments [36]. Other works include KNN-based IPv6-IDS for WSNs [37], a Zigbee hybrid rule/ML IDS [38], and optimized RPL IDSs targeting routing and DoS attacks [39]. ASSET [40], a softwarized IDS, further detects 13 attack types with adaptive monitoring.

TABLE IV
COMPARISON OF IDS FOR IOT NETWORKS

Paper	Objective	Techniques Used	Advantages	Disadvantages
[36]	Adaptive IDS for RPL attacks in dynamic IoT.	Hybrid IDS, mobility- & attack-aware.	Works well in dynamic/heterogeneous settings.	High resource use, complex deployment.
[37]	Secure framework & IDS for IPv6 WSNs.	K-NN, profile-based detection.	Fast detection, easy integration.	Not scalable; K-NN is costly.
[38]	Hybrid IDS for Zigbee IoT.	ML anomaly detection + rule-based IDS.	Detects known & unknown attacks.	Rule creation hard; complex upkeep.
[39]	IDS for RPL IoT (routing & DoS attacks).	Multi-technique detection.	Detects many attacks (version, blackhole, grayhole, flooding).	Needs tuning for different networks.
[40]	Softwarized IDS (ASSET) for RPL IoT.	Multi-mechanism, configurable IDS.	Flexible, expandable, good trade-offs.	Complex setup; may add overhead.

B. Trust-based models

The rapid growth of IoT has amplified security risks, leading to increasing focus on trust-based IDS models for RPL networks. TIDSRPL [43] forwards node trust evaluations to the root, improving efficiency and outperforming MRHOF-RPL against Sybil, Sinkhole, and Selective Forwarding attacks. DSTIDS [44] strengthens sinkhole resistance and maintains QoS under attack through direct neighbor reputation. A behavioral trust model [45] mitigates version spoofing and hello flooding, analyzing both localized and global energy impacts. SMTrust [46] leverages mobility-aware trust to enhance resilience against rank and blackhole threats. SRF-IoT [47] integrates trust with an external IDS to isolate attackers in Contiki-NG. More advanced, a hybrid deep learning approach [48] combining RNN and stacked LSTM autoencoders predicts routing behaviors and mitigates blackhole, DIS flooding, rank, and version number attacks, showcasing the synergy between deep learning and trust mechanisms.

TABLE V
COMPARISON OF TRUST-BASED MODELS FOR RPL NETWORK SECURITY

Paper	Objective	Techniques Used	Advantages	Disadvantages
[43]	TIDSRPL: trust-based IDS to spot malicious nodes.	Trust eval, root-node offload; detects Sybil, Sinkhole, Selective Forwarding.	Efficient trust use; multi-attack detection.	Heavy root-node reliance, bottleneck risk.
[44]	DSTIDS to block sinkhole attacks in RPL IoT.	Trust-based, tested on Contiki 3.0 & Cooja.	Prevents sinkhole, improves QoS.	Limited to sinkhole only.
[45]	Trust-based RPL to curb energy fatigue (version/hello flooding).	Trust vs. version tampering & hello flooding.	Reduces energy drain, local mitigation.	Handles only two attacks, limited scope.
[46]	SMTrust for secure IoT routing, Rank & Blackhole prevention.	Security-Mobility-Trust model, trust metrics.	Better security, works for mobile/static nodes.	Needs parameter tuning for diverse nets.
[47]	SRF-IoT IDS for Rank & Blackhole detection.	Trust + IDS framework, external IDS.	Isolates malicious nodes well.	Extra IDS integration adds overhead.
[48]	Hybrid DL trust model for anomaly detection.	LSTM seq2seq autoencoder + trust.	Detects multiple RPL attacks via DL.	High complexity, tough for low-power IoT.

C. Anomaly-based detection techniques

In RPL networks, attackers can exploit the lack of parent monitoring by advertising falsely low rank values, drawing excessive traffic and enabling Rank Attacks such as sinkhole or selective forwarding (RA1) and topological instability (RA2) that degrade network performance [49]. To address these, SARPL applies statistical anomaly detection to identify and counter RA1 and RA2 effectively. Another approach, GAIDS [50], introduces an anomaly-based IDS leveraging stochastic games for attack detection and evolutionary games to confirm malicious intent. Since RPL's constraints may lead to false positives by misclassifying honest nodes, GAIDS employs an adaptive game-theoretic framework and clustered network design to improve verification accuracy, reliability, and robustness.

D. Cryptographic solutions

In [51], a lightweight Authentication and Key Exchange (AKE) framework was proposed for 6LoWPAN, using hashing and authenticated encryption to establish keys securely between sensor nodes and a server with low cost, avoiding IP security protocols. In [52], SRUA-IoT, a resource-efficient remote user authentication scheme, applied symmetric encryption, XOR, and hashing to generate secure session credentials, resisting multiple threats through formal and informal analysis. In [53], DSHRPL integrated encryption with node rating to secure RPL in 6LoWPAN through four stages: building trusted RPL, detecting sinkhole attacks, quarantining malicious nodes, and encrypting transmissions.

E. IDS using optimization techniques

In [54], a mobility management framework based on firefly algorithm (mRPL+firefly optimizer) was presented to improve RPL routing protocol in 6LoWPAN networks, realizing improvements in Packet Delivery Ratio (PDR), hop count, end-to-end latency, and energy consumption over available systems. To meet data dissemination overhead in IoT-enabled systems, [55] proposed Tabu RPL, which incorporates Tabu Search Routing (TSR), an adaptive routing that constantly optimizes data distribution according to network conditions and device capabilities, efficiently balancing routing options for enhanced efficiency. In the same vein, [56] introduced an equilibrium optimizer-based RPL (EO-RPL) protocol specifically designed for smart city structural health monitoring, where the EO algorithm optimizes parent node selection by weighing various routing metrics together, breaking the constraint of conventional RPL methods depending on single or composite rigid metrics.

F. Recent Studies on Sub-Optimization Attacks in RPL-Based IoT Networks (2025)

Rank attacks on RPL were first deployed in the Cooja Simulator in order to assess their impact. Subsequently, a new trust-based mitigation strategy was put forward [57] that catered to the requirements of IoT systems with limited resources. Meanwhile, an MLP trained on simulated data was put to use in a combined deep learning and machine learning framework [58] so as to improve the detection and classification of 10 types of RPL routing attacks. To effectively counter rank attacks, a lightweight ensemble IDS was introduced in [59], integrating SVM and XGBoost. This system, feature selection of which was carried out using RFE and Mutual Information, was evaluated under static and dynamic conditions. While the attacks in were addressed, attention in [60] was given to the version number attacks, conducting an in-depth study of the attacks and existing detection and prevention methods, and outlining the burning challenges in the research of RPL security. Edge-layer scrutiny of traffic patterns for the detection of Clone ID attacks was enhanced with the proposal of [61] through a DNN-based approach, bolstering the security, robustness, and efficiency of RPL IoT networks.

G. Comparison of Intrusion Detection Techniques

The earlier section presented various IDS and security mechanisms for RPL-based 6LoWPAN IoT networks;

however, for a practical application perspective, it is important to have a critical comparison. Table 6, given below, contrasts the prominent techniques according to detection accuracy, energy efficiency, scalability, and readiness for real-world deployment. Such an analysis facilitates identifying the solutions best suited for the context of an IoT setup with varied constraints.

TABLE VI
Comparative Analysis of IDS Techniques for RPL-Based 6LoWPAN IoT Networks

Technique / Model	Attack Type(s) Detected	Detection Accuracy	Energy Efficiency	Scalability	Real-World Readiness
Adaptive Hybrid IDS [36]	DIO Suppression, Worst Parent, Rank	High (90–98%)	Moderate	Moderate	Tested in dynamic data settings
RFTrust [17]	Sinkhole	High	Low–Moderate	High	Lightweight, trust-aware
DETONAR [12]	Routing Attacks (DIS, DAO, etc.)	Medium–High	High	Moderate	Packet-sniffing-based, tested
LSTM Autoencoder + RNN [48]	Blackhole, DIS Flooding, Rank, Version	Very High	Low	Low (high overhead)	High accuracy but resource-heavy
KNN-based IDS [37]	General routing anomalies	Moderate	Low	Low	Simple but not scalable
SM Trust Framework [46]	Rank, Blackhole (with node mobility)	High	Moderate	High	Suitable for mobile/static IoT
GAIDS (Game-Theoretic Anomaly IDS) [50]	Rank-based statistical anomalies	Moderate–High	Moderate	Moderate	Realistic with clustered topology
PSO-Optimized IDS [52]	Multiple attacks (ML-based)	High	Moderate	High	Efficient but setup-sensitive

The study reveals that intrusion detection techniques for RPL-based 6LoWPAN networks vary significantly in terms of accuracy, resource consumption, scalability, and practical applicability. Deep learning models, like LSTM autoencoders, have the best detection rates but are not suitable for resource-constrained IoT settings. Trust-based models like RFTrust and SMTrust offer a balanced trade-off, with high detection accuracy and good scalability. PSO-based IDSs compromise adaptability and efficiency, while KNN-based methods lack scalability and real-time applicability. The study emphasizes that no IDS solution is universally best, but its selection depends on deployment criteria.

H. Comparative Analysis of Detection Techniques

Detection techniques currently vary in terms of cost, scalability, and deployment readiness. A hybrid IDS model balances energy efficiency and scalability, ensuring reliable detection of diverse attack types. Deep learning-based architectures show better detection accuracy but have high computational costs. Rule-based and lightweight IDS approaches are practical but lack resilience against adaptive or sophisticated attack patterns. There is a need for an integrated framework that combines these approaches while keeping computational and energy costs low. The framework should adapt to IoT traffic drift and be scalable and fault-resilient for heterogeneous and large-scale environments.

I. Critical Evaluation of Existing Studies

Despite studies presenting effective measures against sub-optimization attacks in RPL-based 6LoWPAN networks, most do not address their limitations in real-world scenarios. Techniques like deep learning-based IDS have limitations in scalability and energy consumption, while lightweight alternatives can improve energy consumption but compromise detection rates. Trust-based and rule-based mechanisms offer balanced tradeoffs but are still limited in their ability to detect evolving or hybrid attacks. There is a lack of an honest comparative evaluation considering detection accuracy, energy efficiency, scalability, and deployability for RPL-based IoT networks.

V. TRENDS AND CHALLENGES

Extending This section explores emerging trends and challenges in IoT security for RPL-based 6LoWPAN networks. Key trends include the use of machine learning and artificial intelligence in IDS for real-time threat detection, decentralized security systems like trust-based and blockchain, and energy efficiency. Context-based security solutions are needed to support network morphisms due to network size and complexity. Privacy issues remain a challenge, requiring scalable, adaptive, and energy-efficient solutions to safeguard sensitive information while adhering to privacy regulations.

i) AI and machine learning for dynamic threat detection

ML/DL development is limited by the resources of the devices, but deployment at RPL, fog/edge, and cloud layers facilitates AI-based security. A hybrid IDS [63] addressed Flooding, Black Hole, DODAG Version Number, and Reduced Rank attacks employing ROUT-4-2023 and compared ML and DL through confusion matrices and processing time. To improve RPL security and QoS, [64] presented a mixed solution with varying OF, random forest classification, and RL-based adaptive routing against rank, sinkhole, and wormhole attacks. A hybrid DL IDS [65] integrating semi-supervised and supervised learning with IoTR-DS dataset was able to detect

DIS, Rank, and Wormhole attacks more accurately than current models. A GRU-based DL model [66] performed better than SVM and logistic regression in detecting HF attacks, enhancing efficiency, accuracy, and energy savings.

ii) Lightweight solutions for constrained devices

In [67], a distributed and collaborative RPL-based security mechanism (CDRPL) was proposed to detect and counteract Version Number (VN) attacks in order to efficiently identify and achieve fast topology convergence. To address flooding-based threats, [68] exhibited a Destination Information Object Flooding (DIOF) attack model in Cooja and suggested an easy-to-implement countermeasures. An energy-efficient ML-based trust-based IDS [69] for Rank, Sybil, and Wormhole attacks was proposed with dynamic trust estimation and low memory consumption. The Hatchet Man attack in RPL was investigated in [70], where low-complexity game-theoretic defense mechanism mitigated denial-of-service effects in 6LoWPAN IoT networks.

VI. KEY CHALLENGES

The key challenges of the review are listed as,

- **Resource Constraints:** Limited power, memory, and computing capacity demand lightweight solutions.
- **Dynamic & Scalable Networks:** Constantly changing and expanding devices make stable security difficult.
- **Energy-Efficient Security:** Battery limits require strong yet low-energy mechanisms.
- **False Positives & Latency:** Diverse traffic causes false alarms; real-time detection must balance resource limits.
- **Advanced Attacks:** Sinkhole, wormhole, and rank attacks exploit protocol flaws, needing multi-layered defenses.
- **Dataset Limitations:** Lack of large, realistic datasets hinders ML/AI-based IDS accuracy.
- **Interoperability:** Security must span heterogeneous IoT protocols (RPL, Zigbee, LoRaWAN, 6LoWPAN).
- **Privacy & Data Protection:** Safeguarding sensitive IoT data against misuse is challenging.
- **Concept Drift:** Changing traffic/attack patterns require adaptive models.
- **Centralized vs. Decentralized Trade-off:** Centralized models risk single-point failures; decentralized ones add overhead.
- **Real-time Adaptation:** Rapidly evolving threats reduce detection accuracy if systems cannot adapt.

VII. RESEARCH GAPS

Although there has been significant work toward resolving RPL-based 6LoWPAN security, numerous important research gaps remain [32]– [48]. IDS solutions today are not advanced or scalable enough to accommodate future threats like wormhole and rank manipulation in dynamic IoT networks. Lightweight methods that support security in conjunction with energy and computational constraints are still insufficient, while the majority of frameworks are based on centralized architectures with single points of failure and poor resilience. There is also the requirement for topology-aware and traffic-aware security systems that would evolve with topology and traffic changes, and privacy-aware methods in conformance with regulatory needs. Additionally, the incorporation of emerging technologies like machine learning and blockchain into IoT security solutions presents the potential to advance detection, data integrity, and scalability but remains untapped.

A significant challenge is the unavailability of realistic IoT attack datasets. Available datasets tend to be either synthetic or simulated, and this confines the strength of IDS models upon deployment in realistic settings. Much research has concentrated on classic attacks such as sinkhole and rank manipulation, with little investigation into hybrid, multi-layered, or adaptive threats. The majority of IDS solutions are static and do not learn adaptability against concept drift in IoT traffic, leading to greater false positives and lower accuracy. Scalability is also not addressed, as most methods are tested only on controlled or small networks and not on large, heterogeneous deployments.

Privacy is also an open gap, as most solutions focus on protecting communications and intrusion detection but fail to anonymize data and ensure secure handling of data. Most IoT security models also are not real-time adaptive and cannot automatically respond dynamically to changing threats without human action. Excessive use of single-layer defenses omits cross-layer vulnerabilities almost completely. To address these challenges, future work should emphasize scalable, lightweight, multi-layered, and adaptive security solutions that incorporate AI, blockchain, and context-awareness to provide strong and resilient IoT security.

VIII. PROPOSED ROADMAP FOR FUTURE RESEARCH

This article suggests a hybrid evaluation matrix as a method for systematically comparing intrusion detection and protection mechanisms across four key axes:

- Detection Performance – identifying different/novel attack types as they evolve while minimizing false positives.
- Resource Efficiency – ensuring low utilization of resources such as CPU or memory space suitable for constrained IoT devices.
- Scalability – potential for supporting large scale, dynamic, heterogeneous IoT networks depending on the size of the IoT ecosystem.
- Deployment Maturity – practical integration within the real world IoT ecosystem beyond simulation environments.

Furthermore, it suggests a multi-layer integrated solution integrating anomaly detection (e.g. ML/DL), trust management, and lightweight cryptography, where old adversaries are still relevant in the evolving threats space (i.e. concept drift) while maintaining energy consumption for resilient and feasible IoT solution designs. A single ecosystem that can also reduce the number of false alarms.

IX. CONCLUSION AND FUTURE DIRECTIONS

Though research in the field of IoT security has made progress in addressing vulnerabilities, there are still serious limitations. Many currently existing solutions are resource-heavy thus are not a feasible solution for low resource IoT devices. Moreover, most intrusion detection systems (IDS) are static, meaning their modifications are limited, which makes it unsuitable to address the dynamic and evolving nature of IoT

environments. The privacy concerns you can attack with a scalable prototype that has been tested in the real world are still serious issues. While there has been much done about countering known attacks, such as sinkhole, rank and wormhole attacks, there are sophisticated and emerging threats that still create challenges to IoT Security. To address these gaps, there is posting future research on efficient and adaptive frameworks, with promising avenues including AI/ML driven IDS capable of detecting and responding in real-time, blockchain integration for data integrity and decentralized trust, and post quantum cryptography can be utilized to mitigate the risks associated with quantum computing's threats to secure IoT. Another key area of interest is using decentralized security models, eliminating a single point of failure, to encourage resilience in a diverse IoT ecosystem. Furthermore, the future of IoT security ultimately resides in a state of development that is scalable, lightweight, and adaptive, capable of securing heterogeneous and large-scale networks against evolving and complex threats.

REFERENCES

[1] A. Seyfollahi, M. Mainuddin, T. Taami, and A. Ghaffari, "RM-RPL: reliable mobility management framework for RPL-based IoT systems,"*Clust. Comput.*, vol. 27, no. 4, pp. 4449–4468, 2024, DOI: 10.1007/s10586-023-04199-0.

[2] S. Gonen, "A methodical examination of single and multi-attacker flood attacks using RPL-based approaches," *Comput. Ind. Eng.*, vol. 194, p. 110 356, 2024, DOI: 10.1016/j.cie.2024.110356.

[3] S. Sahraoui and N. Henni, "SAMP-RPL: secure and adaptive multipath RPL for enhanced security and reliability in heterogeneous IoT-connected low power and lossy networks," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. 1, pp. 409–429, 2023, DOI: 10.1007/s12652-021-03303-9.

[4] B. Isong, O. Kgote, and A. Abu-Mahfouz, "Insights into Modern Intrusion Detection Strategies for Internet of Things Ecosystems," *Electron. Switz.*, vol. 13, no. 12, 2024, DOI: 10.3390/electronics13122370.

[5] M. Kamal, I. Rashid, W. Iqbal, M. H. Siddiqui, S. Khan, and I. Ahmad, "Privacy and security federated reference architecture for Internet of Things," *Front. Inf. Technol. Electron. Eng.*, vol. 24, no. 4, pp. 481–508, 2023, DOI: 10.1631/FITEE.2200368.

[6] M. Ghaleb and F. Azzedin, "Towards Scalable and Efficient Architecture for Modeling Trust in IoT Environments," *Sensors*, vol. 21, Apr. 2021, DOI: 10.3390/s21092986.

[7] M. Asim, T. Baker, J. Nisar, and N. Tariq, "CTrust-RPL: A control layer-based trust mechanism for supporting secure routing in routing protocol for low power and lossy networks-based Internet of Things applications," *Trans. Emerg. Telecommun. Technol.*, vol. 32, Mar. 2021, DOI: 10.1002/ett.4224.

[8] A. Idrees and A. Witwit, "Energy-efficient Load-balanced RPL routing protocol for Internet of Things (IoTs) Networks," *Int. J. Internet Technol. Secur. Trans.*, vol. 11, pp. 286–306, Apr. 2021, DOI: 10.1504/IJITST.2020.10030144.

[9] T. Winter et al., RFC 6550: RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. USA: RFC Editor, 2012.

[10] A. Alazab, A. Khraisat, S. Singh, S. Bevinakoppa, and O. Mahdi, "Routing Attacks Detection in 6LoWPAN-Based Internet of Things," *Electronics*, vol. 12, p. 1320, Mar. 2023, DOI: 10.3390/electronics12061320.

[11] J. Lu, D. Li, P. Wang, F. Zheng, and M. Wang, "Security-Aware Routing Protocol Based on Artificial Neural Network Algorithm and 6LoWPAN in the Internet of Things," *Wirel. Commun. Mob. Comput.*, vol. 2022, pp. 1–8, Jan. 2022, DOI: 10.1155/2022/8374473.

[12] A. Agiollo, M. Conti, P. Kaliyar, T.-N. Lin, and L. Pajola, "DETONAR: Detection of Routing Attacks in RPL-Based IoT," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 2, pp.1178–1190, 2021, DOI: 10.1109/TNSM.2021.3075496.

[13] E. V Abhinaya and B. Sudhakar, "A secure routing protocol for low power and lossy networks based 6LoWPAN networks to mitigate DIS flooding attacks," *J. Ambient Intell. Humaniz. Comput.*, 2021, DOI: 10.1007/s12652-020-02804-3.

[14] S. Sharma and V. K. Verma, "Security explorations for routing attacks in low power networks on internet of things," *J. Supercomput.*, vol. 77, no. 5, pp. 4778–4812, 2021, DOI: 10.1007/s11227-020-03471-z.

[15] P. Bhale, S. Dey, S. Biswas, and S. Nandi, "Energy Efficient Approach to Detect Sinkhole Attack Using Roving IDS in 6LoWPAN Network BT – Innovations for Community Services," S. S. Rautaray, G. Eichler, C. Erfurth, and G. Fahrnberger, Eds., Cham: Springer International Publishing, 2020, pp. 187–207.

[16] S. Al-Sarawi, M. Anbar, B. A. Alabsi, M. A. Aladaileh, and S. D. Ahmed Rihan, "Unweighted Voting Method to Detect Sinkhole Attack in RPL-Based Internet of Things Networks," *Comput. Mater. Contin.*, vol. 77, no. 1, pp. 491–515, 2023, DOI: 10.32604/cmc.2023.041108.

[17] K. Prathapchandran and T. Janani, "A trust aware security mechanism to detect sinkhole attack in RPL-based IoT environment using random forest – RFTRUST," *Comput. Netw.*, vol. 198, p. 108 413, 2021, DOI: 10.1016/j.comnet.2021.108413.

[18] A. Jamil, M. Ali, and M. Tharwat, "Sinkhole Attack Detection and Avoidance Mechanism for RPL in Wireless Sensor Networks," *Ann. Emerg. Technol. Comput.*, vol. 5, pp. 94–101, Mar. 2021, DOI: 10.33166/AETiC.2021.05.011.

[19] S. Khoeurt, C. So-In, P. Musikawan, and P. Aimtongkham, "Multidirectional Trust-Based Security Mechanisms for Sinkhole Attack Detection in the RPL Routing Protocol for Internet of Things," *J. Wirel. Mob. Netw.*, vol. 14, pp. 48–76, Sep. 2023, DOI: 10.58346/JOWUA.2023.I3.005.

[20] F. Zahra, N. Z. Jhanjhi, S. N. Brohi, N. A. Khan, M. Masud, and M. A. AlZain, "Rank and Wormhole Attack Detection Model for RPL-Based Internet of Things Using Machine Learning," *Sensors*, vol. 22, no. 18, 2022, DOI: 10.3390/s22186765.

[21] S. Javed *et al.*, "A Subjective Logical Framework-Based Trust Model for Wormhole Attack Detection and Mitigation in Low-Power and Lossy (RPL) IoT-Networks," *Information*, Aug. 2023, DOI: 10.3390/info14090478.

[22] S. A. Bhosale and S. S. Sonavane, "Wormhole Attack Detection System for IoT Network: A Hybrid Approach," *Wirel. Pers. Commun.*, vol. 124, no. 2, pp. 1081–1108, 2022, DOI: 10.1007/s11277-021-09395-y.

[23] M. Mavani and K. Asawa, "Resilient against spoofing in 6LoWPAN networks by temporary-private IPv6 addresses," *Peer--Peer Netw. Appl.*, vol. 13, no. 1, pp. 333–347, Jan. 2020, DOI: 10.1007/s12083-019-00792-6.

[24] M. Belaissaoui and Y. Maleh, "Machine Learning techniques optimized by Practical Swarm optimization for Intrusions Detection in IoT".

[25] C. Miranda, G. Kaddoum, A. Boukhtouta, T. Madi, and H. A. Alameddine, "Intrusion Prevention Scheme Against Rank Attacks for Software-Defined Low Power IoT Networks," *IEEE Access,* vol. 10, pp. 129 970–129 984, 2022, DOI: 10.1109/ACCESS.2022.3228170.

[26] A. Abdollahi and M. Fathi, "An Intrusion Detection System on Ping of Death Attacks in IoT Networks," *Wirel. Pers. Commun.*, vol. 112, no. 4, pp. 2057–2070, 2020, DOI: 10.1007/s11277-020-07139-y.

[27] Z. Almusaylim, N. Jhanjhi, and A. Alhumam, "Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP," *Sensors*, vol. 20, p. 5997, Oct. 2020, DOI: 10.3390/s20215997.

[28] A. Verma and V. Ranga, "The impact of copycat attack on RPL based 6LoWPAN networks in Internet of Things," *Computing*, vol. 103, no. 7, pp. 1479–1500, 2021, DOI: 10.1007/s00607-020-00862-1.

[29] A. Verma and V. Ranga, "Mitigation of DIS flooding attacks in RPL-based 6LoWPAN networks," *Trans. Emerg. Telecommun. Technol.*, pp. 1–25, Feb. 2020, https://doi.org/10.1002/ett.3802.

[30] A. Verma and V. Ranga, "CoSec-RPL: detection of copycat attacks in RPL based 6LoWPANs using outlier analysis," *Telecommun. Syst.*, vol. 75, no. 1, pp. 43–61, 2020, DOI: 10.1007/s11235-020-00674-w.

[31] M. Rouissat, B. Mohammed, and B. Sid Ahmed Hichame, "A potential flooding version number attack against RPL based IOT networks," *J. Electr. Eng.*, vol. 73, 2022, pp. 67–275, Sep. 2022, DOI: 10.2478/jee-2022-0035.

[32] G. Simoglou, G. Violettas, S. Petridou, and L. Mamatas, "Intrusion detection systems for RPL security: A comparative analysis," *Comput. Secur.*, vol. 104, p. 102 219, May 2021, DOI: 10.1016/j.cose.2021.102219.

[33] A. Verma and V. Ranga, "Security of RPL Based 6LoWPAN Networks in the Internet of Things: A Review," *IEEE Sens. J.*, vol. 20, no. 11, pp. 5666–5690, Jun. 2020, DOI: 10.1109/JSEN.2020.2973677.

[34] A. M. Pasikhan, J. A. Clark, and P. Gope, "Incremental hybrid intrusion detection for 6LoWPAN," *Comput. Secur.*, vol. 135, p. 103 447, 2023, DOI: 10.1016/j.cose.2023.103447.

[35] J. Arshad, M. A. Azad, M. M. Abdeltaif, and K. Salah, "An intrusion detection framework for energy constrained IoT devices," *Mech. Syst. Signal Process.*, vol. 136, p. 106 436, 2020, DOI: 10.1016/j.ymssp.2019.106436.

[36] A. Pasikhani, J. Clark, and P. Gope, Adaptive Hybrid Heterogeneous IDS for 6LoWPAN. 2022. DOI: 10.48550/arXiv.2205.09170.

[37] M. Wei, C. Rong, E. Liang, and Y. Zhuang, "An intrusion detection mechanism for IPv6-based wireless sensor networks," *Int. J. Distrib. Sens. Netw.*, vol. 18, p. 155013292210779, Mar. 2022, DOI: 10.1177/15501329221077922.

[38] F. Sadikin, T. van Deursen, and S. Kumar, "A ZigBee Intrusion Detection System for IoT using Secure and Efficient Data Collection," *Internet Things*, vol. 12, p. 100 306, 2020, DOI: 10.1016/j.iot.2020.100306.

[39] E. Garcia Ribera, B. Martinez Alvarez, C. Samuel, P. P. Ioulianou, and V. G. Vassilakis, "An Intrusion Detection System for RPL-Based IoT Networks," *Electron. Switz.*, vol. 11, no. 23, 2022, DOI: 10.3390/electronics11234041.

[40] G. Violettas, G. Simoglou, S. Petridou, and L. Mamatas, "A Softwarized Intrusion Detection System for the RPL-based Internet of Things networks," *Future Gener. Comput. Syst.*, vol. 125, pp. 698–714, 2021, DOI: 10.1016/j.future.2021.07.013.

[41] K. Avila, D. Jabba, and J. Gomez, "Security Aspects for Rpl-Based Protocols: A Systematic Review in IoT," *Appl. Sci.*, vol. 10, no. 18, Art. no. 18, Jan. 2020, DOI: 10.3390/app10186472.

[42] A. Kamble, V. S. Malemath, and D. Patil, "Security attacks and secure routing protocols in RPL-based Internet of Things: Survey," in *2017 International Conference on Emerging Trends & Innovation in ICT (ICEI)*, Feb. 2017, pp. 33–39. DOI: 10.1109/ETIICT.2017.7977006.

[43] S. Remya, M. J. Pillai, C. Arjun, S. Ramasubbareddy, and Y. Cho, "Enhancing Security in LLNs Using a Hybrid Trust-Based Intrusion Detection System for RPL," *IEEE Access*, vol. 12, pp. 58 836–58 850, 2024, DOI: 10.1109/ACCESS.2024.3391918.

[44] B. Patel and P. Shah, "Direct Neighbour Sink Reputed Trust Based Intrusion Detection System to Mitigate Sinkhole Attack in RPL for IoT Networks," *J. Eng. Sci. Technol. Rev.*, vol. 14, pp. 35–38, Feb. 2021, DOI: 10.25103/jestr.141.03.

[45] F. Azzedin, "Mitigating Denial of Service Attacks in RPL-Based IoT Environments: Trust-Based Approach," *IEEE Access*, vol. PP, p. 1, Jan. 2023, DOI: 10.1109/ACCESS.2023.3331030.

[46] S. M. Muzammal, R. K. Murugesan, N. Jhanjhi, M. Humayun, A. Osman, and A. Abdelmaboud, "A Trust-Based Model for Secure Routing against RPL Attacks in Internet of Things," *Sensors*, vol. 22, p. 7052, Sep. 2022, DOI: 10.3390/s22187052.

[47] P. P. Ioulianou, V. G. Vassilakis, and S. F. Shahandashti, "A Trust-Based Intrusion Detection System for RPL Networks: Detecting a Combination of Rank and Blackhole Attacks," *J. Cybersecurity Priv.*, vol. 2, no. 1, pp. 124–153, 2022, DOI: 10.3390/jcp2010009.

[48] K. Ahmadi and R. Javidan, "A Trust Based Anomaly Detection Scheme Using a Hybrid Deep Learning Model for IoT Routing Attacks Mitigation," *IET Inf. Secur.*, vol. 2024, no. 1, p. 4 449 798, Jan. 2024, DOI: 10.1049/2024/4449798.

[49] M. A. Alqarni and S. H. Chauhdary, "A Security Scheme for Statistical Anomaly Detection and the Mitigation of Rank Attacks in RPL Networks (IoT Environment)," *Eng. Technol. Appl. Sci. Res.*, vol. 13, no. 6, pp. 12 409–12 414, 2023, DOI: 10.48084/etasr.6433.

[50] D. B. Gothawal and S. V Nagaraj, "Anomaly-Based Intrusion Detection System in RPL by Applying Stochastic and Evolutionary Game Models over IoT Environment," *Wirel. Pers. Commun.,* vol. 110, no. 3, pp. 1323–1344, 2020, DOI: 10.1007/s11277-019-06789-x.

[51] M. Tanveer, G. Abbas, Z. Abbas, M. Waqas, F. Muhammad, and S. Kim, "S6AE: Securing 6LoWPAN using Authenticated Encryption Scheme," *Sensors*, vol. 20, May 2020, DOI: 10.3390/s20092707.

[52] G. Abbas, M. Tanveer, Z. Abbas, M. Waqas, T. Baker, and D. OBE, "A secure remote user authentication scheme for 6LoWPAN-based Internet of Things," *PLOS ONE*, vol. 16, p. e0258279, Nov. 2021, DOI: 10.1371/journal.pone.0258279.

[53] M. Zaminkar, F. Sarkohaki, and R. Fotohi, "A method based on encryption and node rating for securing the RPL protocol communications in the IoT ecosystem," *Int. J. Commun. Syst.*, vol. 34, Nov. 2020, DOI: 10.1002/dac.4693.

[54] K. Manikannan and V. Nagarajan, "Optimized mobility management for RPL/6LoWPAN based IoT network architecture using the firefly algorithm," *Microprocess. Microsyst.*, vol. 77, p. 103 193, 2020, DOI: 10.1016/j.micpro.2020.103193.

[55] V. K. Prajapati, T. P. Sharma, and L. K. Awasthi, "Data Dissemination Framework for Optimizing Overhead in IoT-Enabled Systems Using Tabu-RPL," *SN Comput. Sci.*, vol. 5, no. 4, p. 343, 2024, DOI: 10.1007/s42979-024-02694-8.

[56] K. A. Darabkh, H. H. AlAdwan, M. Al-Akhras, F. Jubair, and S. Rahamneh, "A revolutionary RPL-based IoT routing protocol for monitoring building structural health in smart city domain utilizing equilibrium optimizer algorithm," *Soft Comput.*, vol. 28, no. 17, pp. 10 099–10 138, 2024, DOI: 10.1007/s00500-024-09677-0.

[57] M. Yadav and R. Kaur, "Implementation of Rank Attack and Its Mitigation in RPL-Based IoT Networks:," in *Proceedings of the 10th International Conference on Internet of Things, Big Data and Security, Porto, Portugal: SCITEPRESS - Science and Technology Publications*, 2025, pp. 215–222. DOI: 10.5220/0013205100003944.

[58] A. Krari, A. Hajami, A. Toubi, and M. A. Said, "Securing IoT Networks: Multi-Attack Detection of RPL Routing Threats Using Deep Learning," *J. Comput. Sci.*, vol. 21, no. 4, pp. 836–850, Mar. 2025, DOI: 10.3844/jcssp.2025.836.850.

[59] S. Kalyani and D. Vydeki, "A Resource-Efficient Ensemble Learning Framework for Detecting Rank Attacks in RPL-Based IoT Networks," *J. Econ. Technol.*, Jul. 2025, DOI: 10.1016/j.ject.2025.06.003.

[60] M. Boudouaia, V. Tournois, S. Ouchani, and A. Abuarqoub, "Version Number Attacks in RPL based IoT Networks State of the Art and Future directions," in *Proceedings of the 8th International Conference on Future Networks & Distributed Systems, in ICFNDS '24*. New York, NY, USA: Association for Computing Machinery, Jul. 2025, pp. 276–282. DOI: 10.1145/3726122.3726163.

[61] F. Al-Quayed, S. R. Awan, N. Tariq, M. Humayun, T. S. Alnusairi, and T. Rehman, "CID-RPL: Clone ID Attack Detection Using Deep Neural Network for RPL-Based IoT Networks," *IET Commun.*, vol. 19, no. 1, p. e70067, 2025, DOI: 10.1049/cmu2.70067.

[62] M. Belaissaoui and M. Yassine, "Machine Learning techniques optimized by Practical Swarm optimization for Intrusions Detection in IoT. In *Journal of Information Assurance and Security*. ISSN 1554-1010," vol. 16, pp. 105–116, Jul. 2021.

[63] U. Shahid, M. Z. Hussain, M. Z. Hasan, A. Haider, J. Ali, and J. Altaf, "Hybrid Intrusion Detection System for RPL IoT Networks Using Machine Learning and Deep Learning," *IEEE Access*, vol. PP, p. 1, Jan. 2024, DOI: 10.1109/ACCESS.2024.3442529.

[64] A. Wakili, S. Bakkali, and A. E. H. Alaoui, "Machine learning for QoS and security enhancement of RPL in IoT-Enabled wireless sensors," *Sens. Int.*, vol. 5, p. 100 289, 2024, DOI: 10.1016/j.sintl.2024.100289.

[65] N. W. Khan et al., "A hybrid deep learning-based intrusion detection system for IoT networks," *Math. Biosci. Eng.*, vol. 20, no. 8, pp. 13 491–13 520, 2023, DOI: 10.3934/mbe.2023602.

[66] S. Çakır, S. Toklu, and N. Yalçın, "RPL Attack Detection and Prevention in the Internet of Things Networks Using a GRU Based Deep Learning," *IEEE Access*, vol. 8, pp. 183 678–183 689, Oct. 2020, DOI: 10.1109/ACCESS.2020.3029191.

[67] I. S. Alsukayti and A. Singh, "A Lightweight Scheme for Mitigating RPL Version Number Attacks in IoT Networks," *IEEE Access*, vol. 10, pp. 111 115–111 133, 2022, DOI: 10.1109/ACCESS.2022.3215460.

[68] M. Rouissat, B. Mohammed, I. Alsukayti, and A. Mokaddem, "A Lightweight Mitigation Approach against a New Inundation Attack in RPL-Based IoT Networks," *Appl. Sci.*, vol. 13, Sep. 2023, DOI: 10.3390/app131810366.

[69] A. Burange and V. Deshmukh, "Securing IoT Attacks: A Machine Learning Approach for Developing Lightweight Trust-Based Intrusion Detection System," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 11, pp. 14–22, Sep. 2023, DOI: 10.17762/ijritcc.v11i7.7788.

[70] G. Sharma, J. Grover, and A. Verma, "A Lightweight Security Solution for Mitigation of Hatchetman Attack in RPL-based 6LoWPAN," in *2023 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2023, pp. 750–755. DOI: 10.1109/ANTS59832.2023.10469481.

Angel D is an experienced Information Technology Senior Lecturer with over 12 years in academia and industry, specializing in curriculum development, innovative teaching methodologies, and research. She is currently pursuing a Ph.D. in Computer Science Engineering at Presidency University and holds a master's degree in computer application. Her research interests include Machine Learning, AI, IoT, and Data Analytics. Angel has also contributed to international conferences, authored academic articles, and led workshops on emerging IT trends. She also held senior roles in the IT industry, as Senior Programmer Analyst at Cognizant and Infosys, specialized in BI applications and data reporting, working with clients such as Royal Bank of Scotland, AstraZeneca, Philips, and British Gas. She been recognized with several awards from the Ministry of Higher Education, Oman, and had the privilege of speaking at various academic institutions on the importance of strengthening soft skills.

Dr. Robin Rohit Vincent is a distinguished academician and researcher in the field of Computer Science and Engineering. He currently serves as Professor and Head of the NVIDIA Centre of Excellence (CoE) at Presidency School of Computer Science and Engineering, Presidency University, Bengaluru. He holds B.E., M.E., and Ph.D. degrees, along with a Postdoctoral Fellowship (PDF) from the UK, reflecting his strong academic and research background.

With extensive experience in teaching, research, and academic leadership, Dr. Vincent has contributed significantly to emerging areas of technology, mentoring students and guiding innovative projects. His work focuses on advancing knowledge in cutting-edge domains and fostering industry– academia collaboration through initiatives like the NVIDIA CoE.