Towards Secure Internet of Things Communication Through Trustworthy RPL Routing Protocols

Rui LI
Shaanxi Technical College of Finance and Economics, Xianyang 712000, China

***Abstract*—The Internet of Things (IoT) refers to a network of connected objects for autonomous data exchange and processing. With the increasing growth in IoT, ensuring data transmission integrity and security is essential, as data is subject to many attacks. Currently, the routing protocol for low-power lossy networks is RPL and finds wide deployment in IoT deployments. It also provides a framework to define characteristics related to low-power consumption and resilience to specific routing attacks. RPL trust-based routing protocols improve RPL security by introducing a threshold for Minimum Acceptable Trust, permitting only trusted nodes with a sufficient level of obtained trust to participate in routing. This mechanism is designed to reduce malicious activities and to establish secure communications. This paper will provide an overall review of trustworthy RPL routing methods in IoT and discuss the trust metrics of these approaches and their limitations. To the best of our knowledge, this is the first survey focusing on trust-based RPL protocols in IoT, offering valuable insights into the performance of protocols and possible improvements.**

***Keywords*—Internet of Things; routing; trust; data transmission**

I. Introduction

A. Context

The Internet of Things (IoT) is one of the main transformative technological developments experienced today, involving billions of devices connected, communicating, and exchanging data over different networks [1]. As it has been implemented into daily life, IoT involves general applications and particular industries, including healthcare, transportation, agriculture, and manufacturing [2]. This interdependence has forged unparalleled motivation for efficiency and innovation, where devices can analyze the collected data and make decisions in real-time [3]. On the inverse side, however, the rapid proliferation of IoT networks and billions of devices operating today motivated numerous problems, not least of which pertain to security and data privacy. This sets up a situation in which exponential growth in connected devices makes the need for integrity and safety within IoT environments increasingly central [4].

Routing protocols constitute the central heart of IoT networks, facilitating efficient and reliable data delivery across various connected devices [5]. Considering the challenge posed by the diversity of IoT deployment scenarios, which often involve several resource-constrained devices, such protocols are expected to choose optimal paths for communication while keeping energy consumption as low as possible but preserving network performance [6]. Scalability for large and dynamic networks, energy efficiency to prolong the operable life of battery-powered devices, secure communications that protect data from possible threats, and, above all, autonomy to enable them to self-manage without constant outside control are some of the critical design elements for IoT routing protocols. The Routing Protocol for Low-power and Lossy Networks (RPL) has since become the de-facto solution to these issues due to a solid framework and suitability to meet low-power and lossy network requirements. By prioritizing energy efficiency, adaptability has confidence in RPL as a significant enabler of smooth and secure operations for IoT networks, mainly in applications that feature resource scarcity [7].

B. Problem Statement

RPL is specifically designed to meet the peculiar needs of IoT networks, mainly those constrained by limited power, processing capability, and unreliable communication links [8]. RPL organizes the network into a hierarchical framework called a Destination-Oriented Directed Acyclic Graph (DODAG), wherein nodes establish paths to a common destination, typically an Internet gateway or a data sink [9]. Each node in DODAG receives a rank, reflecting its relation to others. The lower this rank, the closer the node is to the study [10]. RPL makes efficient routing decisions since rank computation is based on routing metrics like link quality, throughput, and latency. Technical adaptability and energy efficiency make the RPL useful in innumerable critical domains, ranging from healthcare monitoring systems to smart city infrastructure and industrial automation. Each of these domains needs reliable data transmission with optimum utilization.

Despite RPL's efficiency and adaptability, it is subjected to various security threats like blackhole, rank, and wormhole attacks. Under the Blackhole attack, any malicious node advertises itself with an optimum path to intercept and drop packets to disrupt communications. In Rank attacks, an adversary can alter its rank to change network topology, which might lead to inefficient routing or partitioning of the network. The wormhole attack establishes a virtual tunnel between two distant parts of the network to deceive nodes, which may result in the interception or modification of data. This attack on RPL is critical, as such vulnerabilities can compromise essential IoT applications, such as healthcare and smart city systems, leading to data loss, service disruption, or even risks to human safety. Proper security can protect data integrity, preserve smooth communication, and maintain users' confidence in such IoT systems.

C. Motivation and Contribution

Trust-based RPL routing protocols have emerged as promising to enhance RPL security. These protocols incorporate mechanisms that evaluate the trustworthiness of network nodes based on their behavior, record of communications, or reliability. By assigning a trust score, only nodes that meet predefined trust thresholds can participate in the routing process, thereby reducing the possibility of malicious activities. Essential trust metrics include packet forwarding ratios, energy consumption, and reputation scores distinguishing trusted and compromised nodes. Based on these trust metrics, the trust-based RPL protocols monitor for attacks, including blackhole or rank manipulation, to ensure data is forwarded to reliable nodes. This approach significantly improves the integrity, trust, and reliability of communications in IoT and enhances general network resilience against diverse security threats.

Kamgueu, et al. [11] presented various RPL protocol enhancements, emphasizing security and mobility. They classified existing solutions and discussed their effectiveness in mitigating RPL's inherent vulnerabilities. However, they have not discussed trust-based security mechanisms for RPL. Yang, et al. [12] presented an overview of possible RPL security vulnerabilities in RPL-based IoT networks and a discussion about possible countermeasures. While this study addresses most security-related issues, it provides only a limited discussion on trust-based routing protocols and lacks a critical analysis of trust metrics and their implementation mechanisms.

Sobral, et al. [13] presented a detailed survey of the routing protocol for Low-Power and Lossy Networks. This paper considers the evaluation of different protocols with various performance metrics like energy efficiency and scalability. The security issues are briefly discussed, but a detailed study on trust-based approaches has not been drawn. Bang, et al. [14], on the other hand, presented a thorough analysis of enhancements in security, scalability, and energy efficiency to RPL. They also discussed various attacks on RPL and their respective mitigation strategies. However, the trust-based routing protocol discussion falls short and thus demands more research into trust metrics and their impact on network performance. Shah, et al. [15] addressed the challenges and solutions of routing protocols in mobile IoT environments. They emphasized the challenges in mobility management and energy constraints but gave little attention to trust-based routing mechanisms, specifically on RPL.

Although much research has been done on RPL and its security challenges, a literature gap regarding the need for comprehensive surveys on trust-based RPL routing protocols is evident. Most related works are contributed piecemeal, leaving room for comprehensive analysis and comparison among those trust-based mechanisms. This, therefore, requires a review of the same protocols; indeed, trust-based approaches have promised a solution for improving IoT network security and preventing malicious activities while ensuring reliable communication. Such a review will shed light on the strengths and limitations of the current trust-based methods and highlight areas for further improvements to guide future research. This gap gives us a reduced understanding of the potentials available with the trust-based RPL protocols and retardation in further development of secured and resilient IoT systems.

This study primarily attempts to evaluate trust-based RPL routing protocols, examine the various trust measures used, and outline their limits and issues. Additionally, the study aims to identify and propose potential future research avenues to address existing shortcomings and increase security in IoT networks. This study is distinctive as it represents the inaugural comprehensive survey focused on trust-based RPL protocols. It offers a thorough analysis that addresses a significant gap in the literature and establishes a foundation for researchers and practitioners aiming to develop secure and efficient IoT communication systems.

II. Background

This section describes the basic principles of IoT and routing protocols, including the general architecture and operation based on the protocol RPL and the principle of trust-based routing in IoT networks.

A. *Definition and Impact of IoT*

IoT is ubiquitous across virtually every aspect of human activity in modern life because of intelligent gadgets or interconnected systems. Companies, governments, and organizations increasingly employ independent devices to increase productivity, enhance quality of service, and spur economic growth [16]. IoT, in return, with its rapid advancement in various fields of health and energy management for military purposes, agriculture, and smart city infrastructure, among others, is trying to make the world much more useful and linked. It has been described by many as the "system of systems" or even a "network of networks," with IoT communication protocols capable of making devices self-configuring and strictly limiting access to authorized and trusted users [17].

However, as IoT networks scale to billions of devices, the issues of security, scalability, and resource consumption become critical. Each IoT service model differs in security, architecture, and implementation, making standardization and integration of new services even more challenging [18]. Fig. 1 illustrates the complexity of the ecosystem that needs to be managed, starting with exceptionally diverse applications and network models and proceeding to considerations about security and privacy. Security remains a significant barrier to IoT’s expansion, especially given the resource limitations of many IoT devices, making them vulnerable to various threats. These include Intrusion Detection Systems (IDS), trust-based models, and cryptographic techniques. The general idea of adapting to various IoT applications while implementing routing algorithms is highly trust-based models, which can support detecting and isolating malicious nodes.

B. *Overview of the RPL Protocol*

RPL stands for Routing Protocol for Low-power and Lossy Networks, designed to meet the unique requirements of IoT networks, which, in turn, feature limited power, processing capabilities, and unreliable communication links. The RPL protocol is one of the proactive protocols, which immediately establishes routing paths once the network becomes operative. It organizes the network into a DODAG structure, illustrated in Fig. 2. This structure has one root node that coordinates network communication. Due to such a structure, RPL can efficiently decide routing paths by ranking each node, as illustrated in Fig. 2. For the computation of the ranks, local metrics and constraints are considered so that the network has no cycle and performance is optimized.

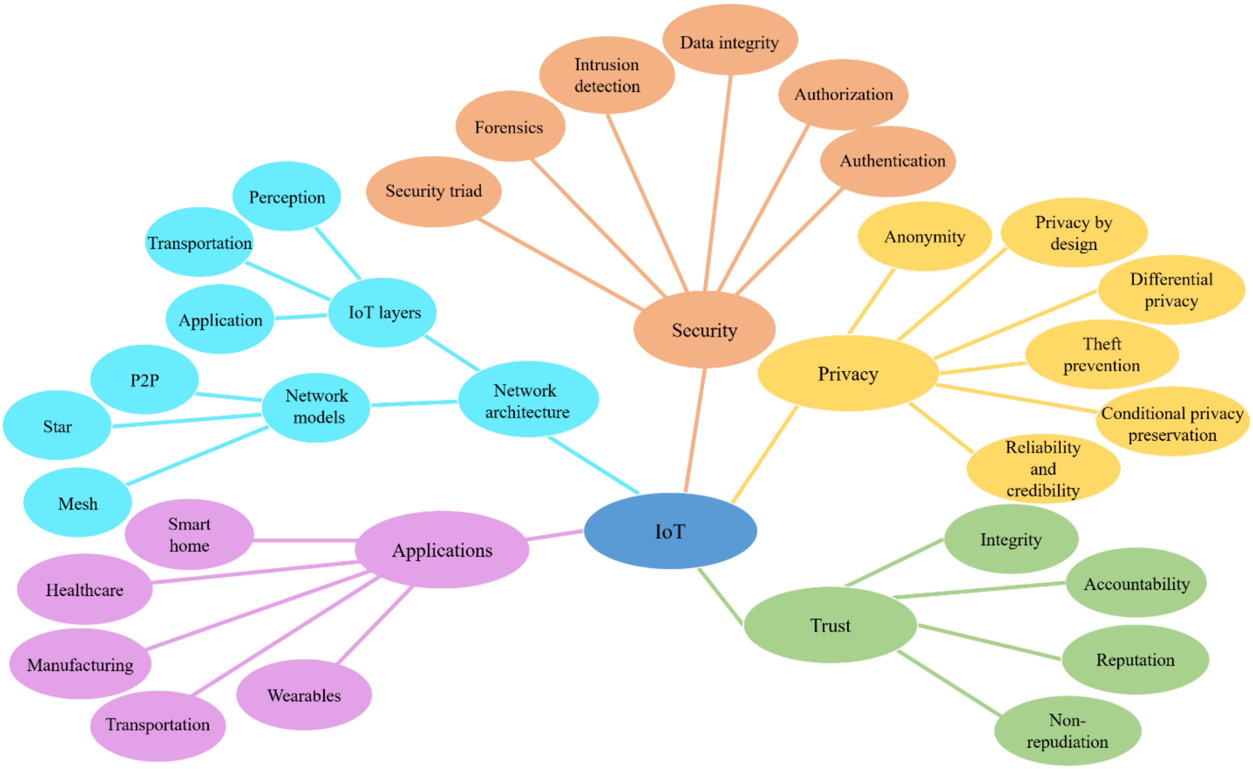

Fig. 1. An overview of IoT paradigm.

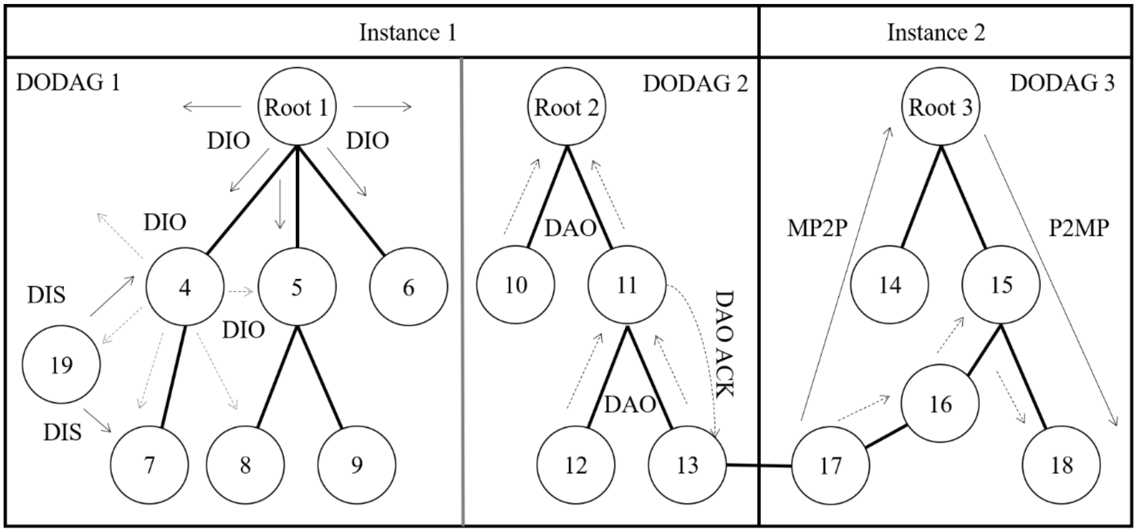

Fig. 2. DODAG structure.

The formation of DODAG in RPL starts with the root node broadcasting DIO messages. The nodes hear these messages, calculate their rank, and choose a parent node based on routing metrics. The nodes ensure the acyclicity of the DODAG by ensuring that the rank of its parent is less than that of itself. Techniques like trickle timers prevent extra overhead by controlling message traffic. The nodes can join the network by sending the DODAG Information Solicitation message. RPL also has different modes of operation for root to upward routes and downward routes based on Destination Advertisement Object (DAO) messages to communicate efficiently in the network.

C. *Trust-based Routing in IoT*

The widespread deployment of IoT devices in diverse environments increases the risk of security breaches, such as attacks that drain a device’s energy or disrupt network operations. Given these threats, designing adequate safeguards is crucial, particularly considering the limited resources of many IoT devices. A promising approach is trust-based routing, which detects and isolates malicious nodes using appropriate trust assessment strategies. Trust among network nodes builds up over time, allowing the system to discriminate effectively between honest and malicious participants. However, attackers can manipulate trust metrics either by falsely downgrading reliable nodes or by falsely promoting threatening ones, undermining the effectiveness of trust-based solutions and disrupting the stability of networks.

In other words, trust-based routing protocols ensure participation in route formation and data exchange through nodes that can be adjudged trusted depending on their behavior and past interactions. Isolation strategies will be applied to protect the network against malicious or selfish behavior by nodes. Trust attributes assessment is one of the most challenging barriers at the network level. Thus, trust-based approaches are recommended for several IoT applications.

D. *Performance Metrics*

This section presents some of the most essential metrics considered in the literature to evaluate the performance and security of RPL-based IoT networks. Each metric is briefly explained, and the relevant equations are presented.

Malicious node containment: This evaluates the protocol's effectiveness in isolating malicious nodes, expressed as follows.

$$Acc = \frac{No. of\ detected\ malicious\ nodes}{Total\ no. of\ malicious\ nodes} \tag{1}$$

Where Acc represents the detection accuracy of the proposed solution.

Network throughput: Measured in kilobits per second, indicates the data transmission rate over a given period.

$$Throughput = \frac{Total\ data\ transmitted\ (in\ kilobits)}{Total\ time\ (in\ seconds)} \tag{2}$$

Where Total Data Transmitted is the amount of data successfully sent over the network, and Total Time is the duration over which the data transmission occurs. This formula provides the data transmission rate in kilobits per second (kbps).

Storage cost: Nodes maintain lists of neighbors' behaviors, increasing storage requirements at the node level.

$$SC = N \times S_b \tag{3}$$

Where N represents the number of neighboring nodes for which behavior information is maintained, and S_b is the storage size required (in bytes) to store the behavior information of a single node.

Median packets dropped: This metric indicates the percentage of packets dropped during attacks, calculated as:

$$D_r = \frac{Drop_r}{\sum_{k=1}^{n} TAk} \tag{4}$$

$$E[Dpkt] = Median\ (D) \tag{5}$$

Packet Delivery Ratio (PDR): PDR is the median value of the packet delivery ratio across multiple repetitions, calculated as:

$$S_r = \frac{Rcvd}{\sum_{k=1}^{n} P_k} \tag{6}$$

$$E[DRpkt] = Median\ (S) \tag{7}$$

Communication overhead: This metric assesses the additional communication costs due to control messages exchanged during security events.

$$CO = \frac{CM}{TD} \times 100 \tag{8}$$

Where *CM* is the number of control messages transmitted during security events, and *TD* denotes the total data packets transmitted over the network.

Misdetection rate: This rate measures the error in detecting malicious nodes, accounting for false positives and negatives.

$$MR = \frac{FP + FN}{TP + TN + FP + FN} \tag{9}$$

Where *FP* denotes the number of false positives (benign nodes incorrectly identified as malicious), FN represents the number of false negatives (malicious nodes incorrectly identified as benign), *TP* is the number of true positives (malicious nodes correctly identified), and *TN* is the number of true negatives (benign nodes correctly identified).

Trust values: A trust value is a feeling of confidence in a node's predictable behavior and honesty. Trust values are essential for routing to ensure that only trustworthy nodes participate in packet forwarding, especially faraway nodes. The trust can be computed as follows:

$$RT(N_i, N_m) = DT(N_i, N_j) \times DT(N_j, N_m) \tag{10}$$

Where $RT(N_i, N_m)$ is the recommended trust value from node *i* to node *m*, and $DT(N_i, N_j)$ and $DT(N_j, N_m)$ are the direct trust values between nodes.

Reliability: Reliability is based on a predefined trust threshold. It assesses the trustworthiness and dependability of nodes, ensuring only reliable nodes participate in routing. Trust ratings are similar to assigning ranks to nodes based on trust indices.

$$R = \frac{N_t}{N} \tag{11}$$

Where R is the Reliability of the network, N_t represents the number of nodes with trust values above the trust threshold, and N is the total number of nodes in the network.

Key generation time: It calculates the time a key is generated for secure data transmission. High key generation times cause IoT devices to consume extra resources and experience delays. Thus, reducing them is critical for efficient data communication.

$$KGT = E_t - S_t \tag{12}$$

Where E_t denotes the end time when the key generation process is completed and S_t represents the start time when the key generation process begins.

Energy consumption: This metric quantifies the energy used during data transmission in the network. It is determined by the difference between the total energy T_e and the remaining energy R_e, given by:

$$EC = T_e - R_e \tag{13}$$

Delay: It refers to the time taken for data packets to travel from the source nodes to the root destination node in the network. Thus, it can be measured as a difference between packet transmission time, $\mathrm{P}_{\mathrm{r,t}}$, and packet received time, $\mathrm{P}_{\mathrm{t,t}}$, given as:

$$D = \sum_{i=0}^{n} \left(P_{r,t} - P_{t,t}\right) \tag{14}$$

III. Trust-based RPL Routing Protocols

The taxonomy of trust-based RPL protocols can be divided into: 1) Trust-based detection and isolation mechanisms, which primarily detect and isolate malicious nodes by relying on trust scores generated from node behavior and recorded communications; 2) Energy-efficient and lightweight models of trust, which essentially reduce computational and energy overhead due to trust evaluations-small enough for resource-constrained IoT devices; 3) Advanced models of trust for dynamic environments for the adaptation of trust mechanisms to the respective mobility, heterogeneity, and time-varying conditions in IoT networks; 4) Attack-specific mitigation strategies that aim to identify unique trust metrics coupled with countermeasures developed for particular threats, such as blackhole, rank, and wormhole attacks. Together, these categories provide solutions for crucial challenges to RPL security by enhancing detection, reducing resource consumption, and improving network resilience against various threats.

A. *Trust-Based Detection and Isolation Mechanisms*

Airehrour, et al. [19] proposed SecTrust-RPL, which uses trust assessments to segregate malicious nodes from the network while determining optimal routing paths. Successful packet exchanges thus contribute to node reliability and build-up throughput. However, complex attacks like combinations of rank, blackhole, and Sybil would not be defended, and the integration of trustworthy nodes into the network needs to be addressed. Airehrour, et al. [20] developed a trust-based routing protocol for low-power networks whose efficiency was checked with RPL classic through Minimum Rank with Hysteresis Objective Function (MRHOF).

Rakesh [21] introduced the concept of SecRPL-MS to secure RPL-based IoT networks through authentication and security measures. This minimizes energy consumption in rank, Sybil, blackhole, and man-in-the-middle attacks. However, it also has some disadvantages since it neglects DoS/DDoS threats entirely and provides no satisfactory trust-based verification process. Ioulianou, et al. [22] presented SRF-IoT, which was developed by integrating external IDS and trust-based methods against rank and blackhole attacks. Decreasing the extra parent switches to the minimum will provide higher network efficiency, though it suffers from limitations in identifying unidentified attacks and indentation.

Patel, et al. [23] proposed a trust-based intrusion detection solution, FSTIDS, to reduce the impact of topology-based selective forwarding attacks against RPL networks. Selective forwarding is a hard attack to detect because it manifests by merely dropping control or data packets. FSTIDS performs computation at the sink node for trust values to reduce overhead, embedding a threshold and uncertainty factor to maintain accuracy.

Airehrour, et al. [24] proposed a trust-based routing protocol that efficiently protected against blackhole attacks and improved network efficiency without extra traffic overhead. This scheme addresses the challenge caused by compromised sensor nodes in IoT networks. Compromised nodes affect routing integrity by issuing false control information, dropping packets, and even introducing false data during aggregation or obstructing data forwarding.

Djedjig, et al. [25] analyzed the problem of trust management in RPL networks, illustrating that trusting only the Trusted Platform Module (TPM) is not enough to make nodes reliable. They pointed out that nodes may be infected internally or selfishly and thus still build the RPL topology. Their solution proposes trust values as a main routing criterion derived from a node's behavior to create a robust trust mechanism. Airehrour, et al. [26] proposed a comprehensive trust-based RPL protocol that could efficiently prevent black hole attacks. The authors evaluated the performance of the proposed protocol with standard RPL using the MRHOF and IETF's Contiki RPL implementation to analyze its capability in mitigating black hole threats.

These protocols enhance the security of RPL networks, which expose malicious nodes through trust evaluations and isolate them. Some protocols, such as SecTrust-RPL and SecRPL-MS, as shown in Table I, detect dangerous nodes based on trust metrics for their isolation to perform secure routing. However, their procedures are different when various types of attacks need to be handled.

Though SecTrust-RPL is efficient at threat node isolation without dealing with sophisticated attacks, SecRPL-MS detects many threats but cannot mitigate DDoS attacks. Similarly, RPL SRF-IoT maintains an external IDS to provide additional security features against rank and blackhole attacks. However, again, it fails to identify undetected threats. In addition, protocols like FSTIDS and TrustedRPL are more focused on efficient computation of trust and self-organization, ignoring factors related to node mobility and energy consumption in IoT.

B. *Energy-Efficient and Lightweight Trust Models*

Subramanian, et al. [27] has proposed HTmRPL++, which enhances the trust between fog nodes without compromising network speed. Though effective against BSA, it does not consider node mobility and addresses only one attack type. Mehta and Parmar [28] have proposed an energy-efficient strategy against wormhole and gray hole attacks using lightweight trust mechanisms. The technique is practical, yet extra or combined attacks are not considered.

Ul Hassan, et al. [29] suggested CTrust-RLP, which introduced a control layer that detects and isolates blackhole attacks with efficient energy conservation. Still, it reduces the processing overhead without scalability and cannot cope with multiple threats, such as Sybil and rank attacks.

TABLE I. AN OVERVIEW OF TRUST-BASED DETECTION AND ISOLATION MECHANISMS

Reference	Key features	Strengths	Limitations
[19]	Uses trust to isolate malicious nodes and optimize routing by examining successful packet exchanges	High throughput, effective at detecting and isolating suspicious nodes	Does not account for complex collusive attacks (e.g., rank/blackhole, rank/Sybil) and lacks strategies for integrating trustworthy nodes
[20]	Secures against black hole and selective forwarding attacks without adding traffic overhead	Effective against critical attacks and maintains network efficiency	Ignores energy consumption and does not address a broader range of attacks
[21]	Employs authentication and security to mitigate rank, Sybil, blackhole, and man-in-the-middle attacks, with a focus on delay and energy reduction	Comprehensive attack defense reduces packet loss and delay	Overlooks DDoS/DoS threats and lacks a robust trust verification mechanism
[22]	Combines external IDS and trust-based mechanisms to counter rank and blackhole attacks	Reduces parent switches and enhances network efficiency	Limited in detecting additional threats and lacks a solution for indentation attacks
[23]	Uses trust-based intrusion detection for selective forwarding attacks, computing trust at the sink node to reduce overhead	Efficient in minimizing processing load and precise trust computation	Does not consider mobility scenarios, restricting effectiveness in dynamic environments
[24]	Protects against black hole attacks without increasing network traffic using a trust-based mechanism	Secures against compromised nodes and maintains traffic efficiency	Does not consider energy criteria or other types of attacks
[25]	Uses trust values as the primary routing criterion to create a self-organized network	Focuses on internal threats and enables trust-based self-organization	Lacks simulation for empirical validation and does not analyze energy or routing overhead
[26]	Compares trust-based RPL to standard RPL and IETF Contiki RPL, focusing on mitigating black hole attacks	Strong protection against black hole attacks, validated through comparison	Insufficient focus on selective forwarding, ranking, and Sybil attacks; does not address energy and network lifespan

Djedjig, et al. [30] developed a Management Trust Scheme (MRTS) to enhance the security of RPL networks through a distributed and collaborative trust model. This model evaluates nodes' behavior to compute a trust-based value called the Extended RPL Node Trustworthiness (ERNT) measure. MRTS leverages these trust assessments to ensure that only reliable nodes participate in routing, enabling the self-organization of a secure network based on trust status.

Sisodiya, et al. [31] proposed a multicast trust-based RPL management scheme to enhance network security. This approach achieves its goal by continuously monitoring and isolating untrusted nodes that would destroy data integrity or delay and corrupt messages in the protocol. The protocol enables nodes to infer the degree of trust of neighboring nodes in establishing a network topology. It is more effective than broadcast-based transmissions. It provides greater energy efficiency, high throughput, and low dead node ratios. This schema detects malicious nodes before route establishment, allowing only trustworthy nodes to participate in secure multicast.

All these protocols target the optimization of the RPL security mechanism, not to compromise network performance for energy conservation. Most protocols listed in Table II, such as HTmRPL++ and CTrust-RPL, target lightweight design and will be suitable for application in resource-constrained environments. HTmRPL++ addresses specific attacks, such as Ballot Stuffing Attacks, without considering the node's mobility. As a result, it presents robust mutual trust among fog nodes. CTrust-RPL detects a suspicious node or source that can create an attack by using a control layer to reduce overhead processing efficiently; this technique has poor scalability and resistance against sophisticated threats.

TABLE II. AN OVERVIEW OF ENERGY-EFFICIENT AND LIGHTWEIGHT TRUST MODELS

Reference	Key features	Strengths	Limitations
[27]	Trust mechanism tailored for fog nodes, designed to maintain network speed and performance; tested for reliability, delay, and ballot stuffing attacks	Efficient communication for resource-constrained fog nodes and lightweight design	Does not account for node mobility, limited to testing against a single attack
[28]	Defends against wormhole and grayhole attacks using an energy-efficient trust-based approach	Reduces packet loss, isolates rogue nodes and improves performance	Fails to address combined or additional attacks beyond wormhole and grayhole
[29]	Control layer-based trust mechanism that conserves energy while stopping black hole attacks; calculates trust based on packet exchanges	Low processing and storage overhead, improved network longevity, and effective against black hole attacks	Not scalable or distributed, lacks defenses against threats like Sybil and ranking attacks, and limited evaluation of trust mechanism
[30]	Distributed trust model using extended RPL node trustworthiness for secure routing; allows self-organization based on trust status	Enables secure, self-organized network, and behavior-based trust evaluation	Overlooks energy consumption and routing/security overhead, not tested with Cooja-Contiki simulator
[31]	Uses a trust-based approach to identify and isolate malicious nodes, enabling efficient multicast transmission	More energy-efficient and reliable compared to Broadcast RPL, enhances network longevity and throughput	Does not address performance under various attack types, limited platform testing restricts versatility

C. Advanced Trust Models for Dynamic Environments

Muzammal, et al. [32] offered SMTrust, a mobility-based trust model that mitigates attacks such as black holes, rank, and gray holes. It provides optimization of routing in both static and mobile environments but needs to address energy consumption and other potential threats comprehensively. Al-Jumeily, et al. [33] came up with a hybrid trust approach against Sybil attacks, which they called THC-RPL. While this can help with network longevity, reducing packet loss significantly, this protocol has yet to be tested in practical situations, the relevance of which is thus limited.

Addressing one of the biggest challenges in military usage of COTS IoT devices, Thulasiraman and Wang [34] produced a lightweight trust-based per-node secure data transmission architecture based on routing in mobile IoT networks. This design enhanced security for the RPL IoT routing algorithm by bringing in nonce identity values, timestamps, and whitelisting. The modified protocol selects routing paths based on computed node trust values and the Average Received Signal Strength Indicator (ARSSI).

Hassan, et al. [35] introduced the Jini Index approach, a trust-based security framework designed to effectively detect and manage Sybil attacks, one of the most challenging internal threats in IoT networks. Their architecture employs a tiered design comprising layers of devices and fog nodes, enhancing overall network security and energy efficiency by offloading processing tasks from individual nodes. This approach significantly improves Sybil attack detection, reducing latency and energy consumption.

Savitha and Basarkod [36] introduced TEMGTO-RPL, which applies Gorilla Forces Optimization for node selection while balancing trust and energy efficiency. According to the simulation results, the protocol performs well but needs to consider various attack methods. Therefore, the TEMGTO-RPL protocol has an improvement space.

Muzammal, et al. [37] proposed the SMTrust model, which involves an extension of RPL with a trust factor criterion based on mobility in IoT networks. The SMTrust approach resists general RPL attacks such as Blackhole, grey hole, rank, and version number attacks. It considers the sink and sensor node mobility and only allows trustworthy nodes to participate in the network. It is designed for sensor nodes to provide confidentiality, integrity, and availability during routing and communicating data.

Jiang and Liu [38] proposed a defensive technique that effectively addresses sophisticated selective forwarding attacks in RPL-based IoT networks. They design and implement a set of energy-efficient attacks that can flexibly select the type and proportion of packets to be broadcast to maximize the impact, increasing the number of missed packets while keeping stealthy. They brought the right to neutralize these threats, a simple trust-based security mechanism using a beta trust model with asymmetric forgetting rates and decaying trust values.

The protocols reviewed address securing RPL networks in highly mobile or dynamic scenarios. According to Table III, protocols like SMTrust and THC-RPL integrate mobility-based trust metrics into their trust computations to ensure both fixed and mobile nodes. SMTrust can protect against various RPL attacks and perform better than the existing schemes. The significant drawbacks of this protocol lie in its failure to focus on energy consumption and protection against a wide range of threats. THC-RPL adopts a hybrid approach to Sybil attack detection to extend the network lifetime, yet it is waiting for validation in a natural environment.

In Thulasiraman and Wang's Lightweight Security Architecture, countermeasures against DoS and Sybil attacks are robustly provided in mobile IoT networks. Energy efficiency problems may be shown when the number of mobile nodes increases. The proposed Jini Index method by Hassan and Tariq detects Sybil attacks with minimum latency and energy utilization efficiently. However, more is needed to cover broader recognition of attacks using machine learning. TEMGTO-RPL proposes a trust model based on optimization that strikes a balance between energy and trust considerations without concerns about multiple attack vectors. These models show how trust mechanisms will adapt to IoT environments, which will be dynamic and balance mobility, energy efficiency, and security.

D. Attack-Specific Mitigation Strategies

Kim, et al. [39] proposed PITrust, which utilizes the RSSI and a centralized mechanism for trust to enhance the detection accuracy of Sybil attacks. While this method is effective, it targets only one type of attack with no extensive security scope. Lahbib, et al. [40] have proposed LT-RPL, which secures RPL networks under blackhole and grayhole attacks while still assured QoS guarantees. While this is efficient, it does not consider other types of attacks and protocol testing in various application settings. Karkazis, et al. [41] contributed to TXPFI by enhancing the routing with minimal transmission to enhance efficiency.

These approaches focus their contribution on protocols developed for targeted threats to optimize security measures against certain kinds of attacks in RPL networks. As summarized in Table IV, PITrust uses RSSI and a centralized trust mechanism to find Sybil attacks with high accuracy, but it does not cover other attack types. LT-RPL uses an ETX-based trust model to prevent black and gray hole attacks and ensure efficient and energy-conscious routing.

However, it is not validated in diverse application scenarios and does not cancel additional threats. TXPFI proposes a metric that minimizes message transmissions, considering retransmissions and lost links, and significantly reduces communication overhead. It provides a deficiency in performance evaluation during an attack and does not provide comprehensive security.

TABLE III. AN OVERVIEW OF ADVANCED TRUST MODELS FOR DYNAMIC ENVIRONMENTS

Reference	Key features	Strengths	Limitations
[32]	Incorporates mobility-based trust metrics for both fixed and mobile nodes; defends against blackhole, rank, and version number attacks	Outperforms MRHOF, SecTrust, and MRTS; improves performance for mobile and static nodes	Does not address energy efficiency or consider additional attack types
[33]	Hybrid trust model that uses Direct Trust (DT) and Indirect Trust (IDT) to detect Sybil nodes; relays trust data to the root node	Reduces packet loss, extends network lifespan, effective against Sybil attacks	Not tested in real-world environments, limiting practical applicability
[34]	Trust-based routing for mobile IoT using nonce, timestamp, and ARSSI; designed for COTS IoT devices	Protects against DoS and Sybil attacks, high PDR, lightweight and efficient	Does not consider energy consumption or handle a large number of mobile nodes efficiently
[35]	Layered trust model using fog devices to manage Sybil attacks; reduces detection latency and energy consumption	Effectively detects Sybil attacks, reduces energy use and latency	Does not integrate ML algorithms for broader attack mitigation, limited to Sybil attack recognition
[36]	Uses Gorilla Forces Optimization (GTO) for trust and energy-efficient routing; considers trust value, energy ratio, node distance, and PDR	Balances trust and energy efficiency, selects optimal nodes for routing	Does not address multiple attack types, lacks comprehensive security measures
[37]	Focuses on mobility and trust criteria to secure RPL networks against blackhole, greyhole, and rank attacks	Ensures confidentiality, integrity, and availability of sensor nodes; energy-efficient design	Limited in addressing combined attacks, needs efficiency improvements in detection and data transfer
[38]	Uses a beta trust model with asymmetric forgetting rates to detect and mitigate selective forwarding attacks	Efficient against selective forwarding, energy-efficient attack model	Ignores mobile node dynamics, does not address other attack vectors

IV. FUTURE RESEARCH DIRECTIONS

Although several trust-based RPL routing protocols have recently been developed for securing IoT networks, several research gaps and challenges remain to be addressed. Below are future research directions to enhance these protocols' effectiveness, scalability, and robustness.

Most protocols proposed to date target specific attacks, like black holes, Sybil, and rank attacks. Sophisticated and combined attack strategies will attack IoT networks. Future research should develop comprehensive solutions to guard against multiple and simultaneous attack types, such as DDoS, wormhole, and other advanced collusive attacks. Hybrid approaches using machine learning-based anomaly detection and trust evaluation mechanisms may be promising.

These trust-based protocols should take advantage of energy consumption in IoT environments when the resources are constrained. Novel approaches to be explored that tend to minimize energy consumption while sustaining a high level of security. Adaptive computation of trust, energy-aware routing decisions, and lightweight cryptographic methods may lead to less energy-consuming solutions. The protocol design should embed energy consumption models so that a careful evaluation of trade-offs involving security against resource management can be estimated.

IoT networks are highly dynamic, with nodes frequently joining and leaving a network. Most protocols still lack adaptiveness in large-scale or high-mobility scenarios. Trust mechanisms to handle node mobility, changing network topology, and variable device densities using scalable and efficient methods need more research attention. The development of distributed systems for trust management or decentralized usage of blockchain might allow increased scalability and resilience of RPL networks.

Most proposed protocols have been tested only with simulations with minimal scenarios or synthetic datasets. Implementation and testing in diverse and realistic real-world environments are essential in studying practical applicability and effectiveness. Field tests and experiments in intelligent cities or industrial automation based on these solutions may reveal unforeseen challenges and performance issues that might not become evident at a simulation level.

The selection and computation of appropriate trust metrics are critical factors in accurately detecting malicious nodes. In the future, refinement in trust evaluation methods should incorporate context-aware metrics, analysis of historical data, and adaptive trust thresholds. Machine learning algorithms improve trust evaluations by recognizing complex patterns and making better decisions in trust-based routing, making even more enhancement possible.

TABLE IV. AN OVERVIEW OF ATTACK-SPECIFIC MITIGATION STRATEGIES

Reference	Key features	Strengths	Limitations
[39]	Trust-based mechanism using RSSI and a centralized trust model for Sybil attack detection	High detection accuracy, improved routing performance compared to conventional protocols	Limited to addressing only Sybil attacks; does not consider other types of security threats
[40]	Trust management method integrated with ETX-based MRHOF to secure routing topology from black hole and gray hole attacks	Effective at identifying and isolating malicious nodes, provides QoS for energy-efficient routing	Does not address other attack types, lacks validation across various application scenarios and platforms
[41]	Routing metric that minimizes message transmissions by considering frame retransmissions and authenticating lost links	Reduces the number of messages transfers, improves efficiency in data delivery	Does not evaluate protocol under attack conditions, lacks comprehensive security measures and analysis of network lifetime impact

Limited computing and storage resources characterize most IoT devices. Thus, lightweight, efficient security architecture developments are of prime importance. Future research should investigate novel architectures that combine low overhead with solid security features. For example, offloading trust-related intensive computational tasks to fog or edge computing could achieve a good trade-off between performance and security in resource-constrained environments.

Integrating the IoT with blockchain, edge computing, and AI opens a new avenue for IoT network security. Blockchain will offer trust management in a decentralized and tamper-proof way, whereas AI can enhance features related to anomaly detection and adaptive security responses. The research study will focus on integrating such emerging technologies with trust-based RPL protocols to achieve secure and intelligent IoT ecosystems.

In light of the diverse IoT devices and networks, interoperability within the variant trust-based protocols poses a challenge. Any future work, therefore, should seek to develop standardized frameworks and protocols for easy interoperability across different platforms and communication standards. Industry, academia, and standardization bodies are encouraged to work together to enable the adoption of secure and interoperable mechanisms of trust.

Finally, there are issues regarding user data, which could raise some privacy concerns. It is essential to consider techniques during the design of research that will maintain users' privacy while still allowing trust evaluations. This might be a balance between security, trust management, and data privacy using techniques like differential privacy, homomorphic encryption, or federated learning.

Future protocols can adapt to changes in network conditions, such as varying device behavior, environmental factors, or application-specific requirements. Adaptive trust models will adjust the parameters of trust computation on the fly and enhance the robustness of RPL Networks. In this regard, context-aware security mechanisms can ensure that protection is appropriate for the current network state and the criticality of the data transmitted.

V. Conclusion

Despite increasing and diversifying cyber threats, IoT network security remains an open challenge. This review has presented a critical analysis of several trust-based RPL routing protocols proposed to enhance network security. The protocols discussed in this study utilize trust-based mechanisms to detect and isolate malicious nodes to ensure data integrity and optimize routing efficiency. Whereas some have been quite effective in eliminating specific attacks, such as blackhole, Sybil, and rank attacks, there are significant lacunae concerning their comprehensively addressing complex, multifaced threats and adaptation issues related to dynamic network environments. The evaluation of performance metrics across protocols presented a variety of tradeoffs between security and energy efficiency versus network performance. For example, some have high detection accuracy with low communication overhead; however, energy consumption and scalability in large networks should be considered. While designed for energy efficiency, others do not offer protection against complex or combined attacks. These observations clearly dictate why future research should concentrate on holistic and adaptive solutions, including performance and resource constraints. Others pertain to real-world validation and the introduction of cutting-edge technologies such as AI, blockchain, and edge computing. When the IoT network becomes widely adopted, most challenges in energy management, scalability, and user privacy will be resolved.

References

[1] B. Pourghebleh and N. J. Navimipour, "Data aggregation mechanisms in the Internet of things: A systematic review of the literature and recommendations for future research," Journal of Network and Computer Applications, vol. 97, pp. 23-34, 2017.

[2] F. Kamalov, B. Pourghebleh, M. Gheisari, Y. Liu, and S. Moussa, "Internet of medical things privacy and security: Challenges, solutions, and future trends from a new perspective," Sustainability, vol. 15, no. 4, p. 3317, 2023.

[3] M. Soori, B. Arezoo, and R. Dastres, "Internet of things for smart factories in industry 4.0, a review," Internet of Things and Cyber-Physical Systems, vol. 3, pp. 192-204, 2023.

[4] A. Morchid, R. El Alami, A. A. Raezah, and Y. Sabbar, "Applications of internet of things (IoT) and sensors technology to increase food security and agricultural Sustainability: Benefits and challenges," Ain Shams Engineering Journal, vol. 15, no. 3, p. 102509, 2024.

[5] B. Pourghebleh and V. Hayyolalam, "A comprehensive and systematic review of the load balancing mechanisms in the Internet of Things," Cluster Computing, vol. 23, no. 2, pp. 641-661, 2020.

[6] W. Mao, Z. Zhao, Z. Chang, G. Min, and W. Gao, "Energy-efficient industrial Internet of Things: Overview and open issues," IEEE transactions on industrial informatics, vol. 17, no. 11, pp. 7225-7237, 2021.

[7] V. Hayyolalam, B. Pourghebleh, and A. A. Pourhaji Kazem, "Trust management of services (TMoS): investigating the current mechanisms," Transactions on Emerging Telecommunications Technologies, vol. 31, no. 10, p. e4063, 2020.

[8] A. Verma and V. Ranga, "Security of RPL based 6LoWPAN Networks in the Internet of Things: A Review," IEEE Sensors Journal, vol. 20, no. 11, pp. 5666-5690, 2020.

[9] E. Bozorgi, S. Soleimani, S. K. Alqaiidi, H. R. Arabnia, and K. Kochut, "Subgraph2vec: A random walk-based algorithm for embedding knowledge graphs," arXiv preprint arXiv:2405.02240, 2024, doi: https://doi.org/10.48550/arXiv.2405.02240.

[10] P. Chithaluru et al., "An enhanced opportunistic rank-based parent node selection for sustainable & smart IoT networks," Sustainable Energy Technologies and Assessments, vol. 56, p. 103079, 2023.

[11] P. O. Kamgueu, E. Nataf, and T. D. Ndie, "Survey on RPL enhancements: A focus on topology, security and mobility," Computer Communications, vol. 120, pp. 10-21, 2018.

[12] W. Yang, Y. Wang, Z. Lai, Y. Wan, and Z. Cheng, "Security Vulnerabilities and Countermeasures in the RPL-based Internet of Things," in 2018 international conference on cyber-enabled distributed computing and knowledge discovery (CyberC), 2018: IEEE, pp. 49-495.

[13] J. V. Sobral, J. J. Rodrigues, R. A. Rabêlo, J. Al-Muhtadi, and V. Korotaev, "Routing protocols for low power and lossy networks in internet of things applications," Sensors, vol. 19, no. 9, p. 2144, 2019.

[14] A. O. Bang, U. P. Rao, P. Kaliyar, and M. Conti, "Assessment of routing attacks and mitigation techniques with RPL control messages: A survey," ACM Computing Surveys (CSUR), vol. 55, no. 2, pp. 1-36, 2022.

[15] Z. Shah, A. Levula, K. Khurshid, J. Ahmed, I. Ullah, and S. Singh, "Routing protocols for mobile Internet of things (IoT): A survey on challenges and solutions," Electronics, vol. 10, no. 19, p. 2320, 2021.

[16] B. Pourghebleh, N. Hekmati, Z. Davoudnia, and M. Sadeghi, "A roadmap towards energy-efficient data fusion methods in the Internet of Things," Concurrency and Computation: Practice and Experience, vol. 34, no. 15, p. e6959, 2022.

[17] M. Shoeibi, A. E. Oskouei, and M. Kaveh, "A Novel Six-Dimensional Chimp Optimization Algorithm—Deep Reinforcement Learning-Based Optimization Scheme for Reconfigurable Intelligent Surface-Assisted Energy Harvesting in Batteryless IoT Networks," Future Internet, vol. 16, no. 12, p. 460, 2024, doi: https://doi.org/10.3390/fi16120460.

[18] B. Pourghebleh, K. Wakil, and N. J. Navimipour, "A comprehensive study on the trust management techniques in the Internet of Things," IEEE Internet of Things Journal, vol. 6, no. 6, pp. 9326-9337, 2019.

[19] D. Airehrour, J. A. Gutierrez, and S. K. Ray, "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things," Future Generation Computer Systems, vol. 93, pp. 860-876, 2019.

[20] D. Airehrour, J. Gutierrez, and S. K. Ray, "A trust-aware RPL routing protocol to detect blackhole and selective forwarding attacks," Journal of Telecommunications and the Digital Economy, vol. 5, no. 1, pp. 50-69, 2017.

[21] B. Rakesh, "Novel authentication and secure trust based RPL routing in mobile sink supported Internet of Things," Cyber-Physical Systems, vol. 9, no. 1, pp. 43-76, 2023.

[22] 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," Journal of Cybersecurity and Privacy, vol. 2, no. 1, pp. 124-153, 2022.

[23] B. Patel, J. Vasa, and P. Shah, "Forwarding Neighbor Based Sink Reputed Trust Based Intrusion Detection System to Mitigate Selective Forwarding Attack in RPL for IoT Networks," SN Computer Science, vol. 4, no. 4, p. 420, 2023.

[24] D. Airehrour, J. Gutierrez, and S. K. Ray, "Securing RPL routing protocol from blackhole attacks using a trust-based mechanism," in 2016 26th International telecommunication networks and applications conference (ITNAC), 2016: IEEE, pp. 115-120.

[25] N. Djedjig, D. Tandjaoui, and F. Medjek, "Trust-based RPL for the Internet of Things," in 2015 IEEE Symposium on Computers and Communication (ISCC), 2015: IEEE, pp. 962-967.

[26] D. Airehrour, J. Gutierrez, and S. K. Ray, "A testbed implementation of a trust-aware RPL routing protocol," in 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), 2017: IEEE, pp. 1-6.

[27] N. Subramanian, S. M. GB, J. P. Martin, and K. Chandrasekaran, "HTmRPL++: a trust-aware RPL routing protocol for fog enabled Internet of Things," in 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), 2020: IEEE, pp. 1-5.

[28] R. Mehta and M. M. Parmar, "Trust based mechanism for securing iot routing protocol rpl against wormhole &grayhole attacks," in 2018 3rd International Conference for Convergence in Technology (I2CT), 2018: IEEE, pp. 1-6.

[29] T. ul Hassan, M. Asim, T. Baker, J. Hassan, 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," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 3, p. e4224, 2021.

[30] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, "New trust metric for the RPL routing protocol," in 2017 8th International Conference on Information and Communication Systems (ICICS), 2017: IEEE, pp. 328-335.

[31] M. Sisodiya, V. Dahima, and S. Joshi, "Trust based Mechanism using Multicast Routing in RPL for the Internet of Things," in 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN), 2020: IEEE, pp. 392-397.

[32] S. M. Muzammal, R. K. Murugesan, N. Z. Jhanjhi, M. Humayun, A. O. Ibrahim, and A. Abdelmaboud, "A trust-based model for secure routing against RPL attacks in internet of things," Sensors, vol. 22, no. 18, p. 7052, 2022.

[33] D. Al-Jumeily, D. Arshad, N. Tariq, T. Baker, H. Tawfik, and M. Asim, "A Lightweight Trust-enabled Routing in RPL-based IoT Networks Against Sybil Attack," PLoS One, vol. 17, no. 7, 2022.

[34] P. Thulasiraman and Y. Wang, "A lightweight trust-based security architecture for RPL in mobile IoT networks," in 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2019: IEEE, pp. 1-6.

[35] M. Hassan et al., "Gitm: A gini index-based trust mechanism to mitigate and isolate sybil attack in rpl-enabled smart grid advanced metering infrastructures," IEEE Access, vol. 11, pp. 62697-62720, 2023.

[36] M. Savitha and P. Basarkod, "A Trust and Energy based Routing using Gorilla Troops Optimization in RPL Networks," in 2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), 2023: IEEE, pp. 1-7.

[37] S. M. Muzammal, R. K. Murugesan, N. Z. Jhanjhi, and L. T. Jung, "SMTrust: Proposing trust-based secure routing protocol for RPL attacks for IoT applications," in 2020 International Conference on Computational Intelligence (ICCI), 2020: IEEE, pp. 305-310.

[38] J. Jiang and Y. Liu, "Secure IoT routing: selective forwarding attacks and trust-based defenses in RPL network," arXiv preprint arXiv:2201.06937, 2022.

[39] J.-D. Kim, M. Ko, and J.-M. Chung, "Physical identification based trust path routing against sybil attacks on RPL in IoT networks," IEEE Wireless Communications Letters, vol. 11, no. 5, pp. 1102-1106, 2022.

[40] A. Lahbib, K. Toumi, S. Elleuch, A. Laouiti, and S. Martin, "Link reliable and trust aware RPL routing protocol for Internet of Things," in 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), 2017: IEEE, pp. 1-5.

[41] P. Karkazis, I. Papaefstathiou, L. Sarakis, T. Zahariadis, T.-H. Velivassaki, and D. Bargiotas, "Evaluation of RPL with a transmission count-efficient and trust-aware routing metric," in 2014 IEEE International Conference on Communications (ICC), 2014: IEEE, pp. 550-556.