Security of RPL based 6LoWPAN Networks in the Internet of Things: A Review

Abhishek Verma [1] and Virender Ranga [2]

[1]National Institute of Technology Kurukshetra
[2]Affiliation not available

October 30, 2023

Abstract

Internet of Things (IoT) is one of the fastest emerging networking paradigms enabling a large number of applications for the benefit of mankind. Advancements in embedded system technology and compressed IPv6 have enabled the support of IP stack in resource constrained heterogeneous smart devices. However, global connectivity and resource constrained characteristics of smart devices have exposed them to different insider and outsider attacks, which put users' security and privacy at risk. Various risks associated with IoT slow down its growth and become an obstruction in the worldwide adoption of its applications. In RFC 6550, the IPv6 Routing Protocol for Low Power and Lossy Network (RPL) is specified by IETF's ROLL working group for facilitating efficient routing in 6LoWPAN networks, while considering its limitations. Due to resource constrained nature of nodes in the IoT, RPL is vulnerable to many attacks that consume the node's resources and degrade the network's performance. In this paper, we present a study on various attacks and their existing defense solutions, particularly to RPL. Open research issues, challenges, and future directions specific to RPL security are also discussed. A taxonomy of RPL attacks, considering the essential attributes like resources, topology, and traffic, is shown for better understanding. In addition, a study of existing cross-layered and RPL specific network layer based defense solutions suggested in the literature is also carried out.

Citation information: DOI 10.1109/JSEN.2020.2973677, URL: https://ieeexplore.ieee.org/document/8998289

Security of RPL based 6LoWPAN Networks in the Internet of Things: A Review

Abhishek Verma*, *Student Member, IEEE*, and Virender Ranga, *Member, IEEE*

***Abstract*—Internet of Things (IoT) is one of the fastest emerging networking paradigms enabling a large number of applications for the benefit of mankind. Advancements in embedded system technology and compressed IPv6 have enabled the support of IP stack in resource constrained heterogeneous smart devices. However, global connectivity and resource constrained characteristics of smart devices have exposed them to different insider and outsider attacks, which put users' security and privacy at risk. Various risks associated with IoT slow down its growth and become an obstruction in the worldwide adoption of its applications. In RFC 6550, the IPv6 Routing Protocol for Low Power and Lossy Network (RPL) is specified by IETF's ROLL working group for facilitating efficient routing in 6LoWPAN networks, while considering its limitations. Due to resource constrained nature of nodes in the IoT, RPL is vulnerable to many attacks that consume the node's resources and degrade the network's performance. In this paper, we present a study on various attacks and their existing defense solutions, particularly to RPL. Open research issues, challenges, and future directions specific to RPL security are also discussed. A taxonomy of RPL attacks, considering the essential attributes like resources, topology, and traffic, is shown for better understanding. In addition, a study of existing cross-layered and RPL specific network layer based defense solutions suggested in the literature is also carried out.**

***Index Terms*—Internet of Things, RPL, 6LoWPAN, LLN, Network Security.**

I. Introduction

INTERNET of Things[1] is realized by a large scale deployment of Low power and Lossy Networks (LLNs) which are characterized by communication links that have high packet loss and low throughput [2], [3]. LLNs restrict the use of traditional computers and communication technologies due to their strict resource constraints. Also, these networks use resource constrained devices (nodes) that operate on low power, require less energy, have small on-board memory, and low computational capabilities [4]. Moreover, characteristics like resource constraints, high packet loss, and low network throughput make state-of-the-art routing protocols like Adhoc On-Demand Distance Vector, Dynamic Source Routing, and Open Shortest Path First unsuitable for LLNs [5], [6]. To handle this issue, a set of standardized protocols has been developed [7], [8]. These protocols include IEEE 802.15.4 PHY/MAC for Physical and Data link layer, IPv6 over Low Power Wireless Personal Area Networks protocol (6LoWPAN) for Adaptation layer, Routing Protocol for Low-Power and Lossy Networks protocol (RPL) for Network layer, and Constrained Application Protocol (CoAP) for Application layer. In transport, layer the standard User Datagram Protocol [9] is used. RPL has been standardized in 2012 as RFC 6550 by Routing Over Low power and Lossy networks (ROLL) working group of Internet Engineering Task Force (IETF) [3].

RPL has been standardized as a network layer protocol for LLNs [10]. It is recommended for facilitating efficient routing in LLNs like 6LoWPAN [11]. RPL has gained much popularity in the industry as well as in academia. The reason is its capability to provide efficient routing among resource constrained smart IP enabled IoT nodes, flexibility in adapting to different network topologies, and Quality of service (QoS) support [8], [12]–[14]. RPL constructs a Destination Oriented Directed Acyclic Graph (DODAG) from the physical network topology, in which a gateway node is set as a root (destination) of DODAG. All other nodes perform sensing and data routing. RPL uses low energy consuming mechanisms to support self-organization and self-healing for handling frequent node failures [15]. It consumes very few resources while providing efficient routing of IPv6 packets. These capabilities of RPL favor its usage in IoT applications that run on LLN infrastructure [16]. In Section III, a detailed description of RPL is presented. RPL protocol based networks inherit vulnerabilities from its core technologies like IPv6 and Wireless Sensor Networks (WSN). Also, Self-organization, self-healing, open nature, and resource constrained characteristics of RPL expose it to various threats that target it for compromising users' security and privacy [17]. Also, RPL is exposed to external threats from the Internet [18], [19]. Traditional cryptography based security solutions are not suitable for securing RPL based networks (e.g., LLNs). This is because the effectiveness of traditional cryptography based security solutions (e.g. symmetric and asymmetric) relies on the secure distribution of keys. The resource constrained nature of LLNs pose many challenges to key management [20], [21]. Also, if a single legitimate node is compromised, an attacker may gain access to a large pool of pre-loaded keys [22]. This means, once pre-loaded keys are compromised, all network nodes are also compromised. The challenges related to secure key establishment, storage, distribution, revocation, and replacement in LLNs make traditional cryptography based security solutions unsuitable for LLNs [23]. The limitations of LLNs pose a severe threat to RPL security. RPL is vulnerable to various routing attacks, which can be broadly classified into two categories, i.e., attacks inherited from WSN, and RPL specific attacks. The cryptography based security mechanisms can only prevent RPL from external attacks (i.e., attack performed using a node which

* Corresponding Author

A. Verma and V. Ranga are with the Department of Computer Engineering, National Institute of Technology Kurukshetra, Haryana, India, 136119.
E-mail: abhiverma866@gmail.com, virender.ranga@nitkkr.ac.in

is not a part of the existing network) [24], [25]. Traditional security mechanisms are also incapable of detecting insider attacks (i.e., attack performed on the devices that are already part of the existing network), which are performed by the compromised nodes of the network [26]. Thus, from RPL's security point of view, it is crucial to explore the possibilities of developing energy efficient security solutions.

A. Related surveys

In the literature, some research works particular to RPL, and IoT security are present. Airehrour *et al.* [27] surveyed various attacks and defense mechanisms specific to RPL. Their study primarily focused on the utilization of trust based defense methods in RPL security. Most of the defense mechanisms, they discussed are used in WSN security and cannot be directly applied to IoT networks. Alaba *et al.* [28] presented a detailed review of IoT security issues. However, they did not focus on the RPL protocol. A detailed survey on protocols available for facilitating secure communications in IoT is done by Granjal *et al.* [12]. The authors discussed research challenges for different protocols, including RPL. However, they did not discuss attacks and defense mechanisms specific to RPL. Wallgren *et al.* [29] did a detailed study on RPL security by implementing some routing attacks and analyzing the network's performance. Also, they suggested the possible mitigation methods of such attacks. However, they only considered WSN based attacks. Mayzaud *et al.* [30] provided a survey on RPL based attacks and their countermeasures. They proposed a detailed taxonomy of attacks. However, their study did not include the latest proposed attacks and defense solutions. Moreover, the authors did not propose any taxonomy of defense solutions. Pongle *et al.* [31] performed a short study on attacks against RPL and 6LoWPAN layer. The authors only provided a short description of defense solutions and did not propose any suitable taxonomy of attacks and defense solutions specific to RPL. In our opinion, all the mentioned surveys lack effective future research directions and recent proposals. Moreover, these surveys have neglected cross-layered security solutions, which can be utilized for securing RPL as well. The key points that lacked in the previous literature are addressed in our study. The existing surveys related to RPL protocol security are summarized in Table I.

B. Motivation and contributions

With an increase in the number of resource constrained devices (LLNs nodes) and their integration with the Internet has led to severe cybersecurity risks. These risks involve users' security and privacy getting exposed to various threats. Critical applications like healthcare and smart grid, when exposed to such threats, may cause life-threatening incidents to the world population. This motivated us to explore and perform an in-depth analysis of various security issues and their available solutions specific to the RPL protocol. Since RPL is one of the most popular routing protocols for resource constrained networks hence its security aspect must be studied carefully. In this research paper, we present a comprehensive study of different attacks specific to RPL protocol and their defense solutions suggested in the literature. Our objectives include: (1) to propose a taxonomy for classifying different attacks and defense solutions specific to RPL protocol, (2) to identify open research issues, and state-of-the-art challenges related to RPL based IoT network security. The main contributions of this paper are summarized below:

- We provide a comprehensive overview of RPL protocol while focusing on its security issues.
- We present an extensive survey on RPL specific attacks and their countermeasures present in the recent literature.
- We represent the RPL security solutions into two broad categories (i.e., Secure Protocol and Intrusion Detection System) and compare their performance based on different evaluation metrics.
- We discuss cross-layered security solutions present in the literature, which can be used to leverage RPL security.
- We provide open issues, research challenges, future research directions, and potential areas for future research to promote the contribution of state-of-the-art defense solutions.

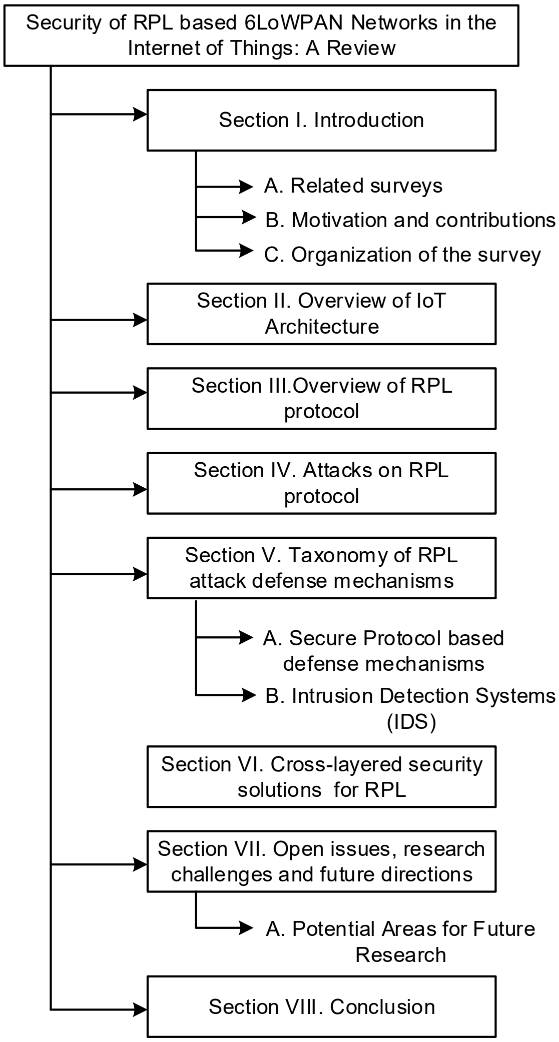
Security of RPL based 6LoWPAN Networks in the Internet of Things: A Review
Section I. Introduction
A. Related surveys
B. Motivation and contributions
C. Organization of the survey
Section II. Overview of IoT Architecture
Section III.Overview of RPL protocol
Section IV. Attacks on RPL protocol
Section V. Taxonomy of RPL attack defense mechanisms
A. Secure Protocol based defense mechanisms
B. Intrusion Detection Systems (IDS)
Section VI. Cross-layered security solutions for RPL
Section VII. Open issues, research challenges and future directions
A. Potential Areas for Future Research
Section VIII. Conclusion

Figure 1: Organization of the survey

Table I: Comparison with related survey papers

Related survey	Brief summary	Topics	Scope	Common points with our survey
Airehrour *et al.* [27]	A survey on existing routing protocols and mechanisms to secure routing communications in IoT	Security and energy consumption in IoT, Routing protocols, Vulnerabilities to routing, Secure routing protocols, Trust in secure routing	Vulnerabilities in RPL, WSN based defense methods, research challenges	Overview of RPL
Alaba *et al.* [28]	A detailed discussion on the IoT security scenario and analysis of the possible attacks	IoT overview, Classification of IoT, Threats and vulnerabilities, IoT security taxonomy, Possible attacks on IoT	State-of-the-art security threats and vulnerabilities, future directions	IoT architecture
Granjal *et al.* [12]	A detailed survey on protocols available for facilitating secure communications in IoT	IoT communication protocols, Security requirements of IoT, Security of various layers (Physical (PHY), MAC, network, application layers), Security for routing	IoT communication protocols and their security issues, protocol specific research challenges	Overview of RPL
Wallgren *et al.* [29]	A detailed study on RPL security by implementing and analyzing various routing attacks	IoT technologies and IDS, IoT protocols overview, Attacks against RPL (inherited from WSN), IDS and the IoT (lightweight heartbeat protocol)	Theoretical impact analysis of attacks inherited from WSN, defense mechanism to detect selective forwarding attack.	Overview of RPL, Attacks against RPL (inherited from WSN)
Mayzaud *et al.* [30]	A survey on RPL based attacks and their countermeasures	·RPL concepts and security concerns, Attacks against RPL protocol, Exploitation for risk management	Attacks against RPL protocol, risk management for RPL security	RPL overview and attacks
Pongle *et al.* [31]	A short study on attacks against RPL and 6LoWPAN layer	Overview of RPL and 6LoWPAN, Attacks on RPL topology, IoT and IDS, Attacks on 6LoPWAN layer	RPL and 6LoWPAN adaptation layer security	Overview of RPL, Attacks on RPL topology
Verma *et al.* (Our survey)	A detailed survey on security of RPL based 6LoWPAN Networks	IoT architectures, Overview of RPL, RPL specific attacks, Taxonomy of RPL attack defense mechanisms, Secure protocol approaches, IDS, Cross-layered security solutions	RPL specific attacks and their countermeasures , research challenges, future directions	-

C. *Organization of the survey*

The rest of this paper is consequently organized as follows. Section II describes the overview of IoT architectures. Section III presents a brief overview of the RPL protocol. Section IV presents a taxonomy of attacks specific to the RPL protocol. In Section V, the proposed taxonomy related to different defense solutions against RPL attacks present in the literature is discussed. In Section VI, cross-layered security solutions specific to RPL protocol security are discussed. Open issues, research challenges, and future directions are addressed in Section VII. Finally, the paper is concluded in Section VIII. The list of abbreviations and definitions used throughout the paper are presented in Table II. The organization of the survey is illustrated in Fig. 1.

II. Overview of IoT Architecture

Various architectures applicable to IoT have been proposed in the literature. Most popular architectures include middleware based, service-oriented based, three-layer and five-layer based [32]. Any standard IoT architecture is not yet recognized in the literature. However, the most commonly referred IoT architecture is three-layer-based architecture [33], which is shown in Fig. 2. It gains popularity because of simple nature and abstract representation of IoT that makes the implementation of applications easier. It comprises three layers, namely perception, network, and application. These layers are highlighted below.

1) Perception Layer: The perception layer is the lowest layer in three-layer IoT architecture. The main purpose of the perception layer is to collect data from the physical environment (temperature, pressure, humidity, etc.) of IoT devices. The process of perception is supported by prominent sensing technology like WSN. Besides, this layer is responsible for converting analog input to digital form and making sensed data suitable for transmission.

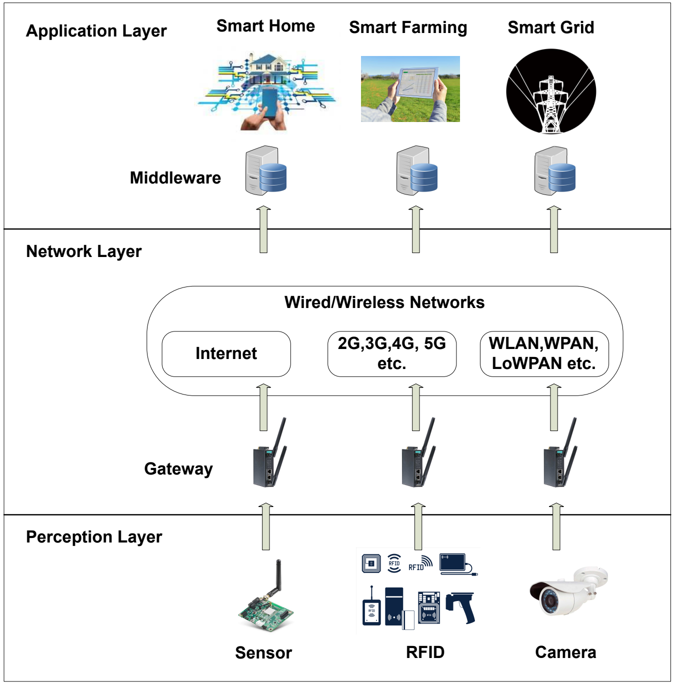

Figure 2: Three-layer architecture of IoT

2) Network Layer: The network layer is dedicated to the processing of sensed data and performing secure data transmission between the perception and application layer. It uses various wired and wireless networking technologies like WLAN, WPAN, LoWPAN, and GSM. It integrates various

Table II: List of Abbreviations

Abbreviation	Stands For
IoT	Internet of Things
IP	Internet Protocol
IPv6	Internet Protocol version 6
RPL	IPv6 Routing Protocol for Low Power and Lossy Network
IETF	Internet Engineering Task Force
ROLL	Routing Over Low power and Lossy Networks
6LoWPAN	IPv6 over Low Power Wireless Personal Area Networks
LLNs	Low power and Lossy Networks
CoAP	Constrained Application Protocol
UDP	User Datagram Protocol
QoS	Quality of Service
DODAG	Destination Oriented Directed Acyclic Graph
WSN	Wireless Sensor Networks
ML	Machine Learning
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Networks
LoWPAN	Low-Power Wireless Personal Area Networks
GSM	Global System for Mobile Communications
NFC	Near-field communication
LTE	Long-Term Evolution
OF	Objective Function
ETX	Expected Transmission Count
MRHOF	Minimum Rank with Hysteresis Objective Function
OF0	Objective Function Zero
OF-EC	OF based on combined metrics using Fuzzy Logic
DIO	DODAG Information Object
DIS	DODAG Information Solicitation
DAO	Destination Advertisement Object
DAO-ACK	Destination Advertisement Object Acknowledgment
DoS	Denial-of-Service
PDR	Packet Delivery Ratio
6BR	6LoWPAN Border Router
IDS	Intrusion Detection System
VERA	Version Number and Rank Authentication
TRAIL	Trust Anchor Interconnection Loop
SRPL	Secure-RPL
TCA	Trusted Computing Architecture
TPM	Trusted Platform Module
MRTS	Metric based RPL Trustworthiness Scheme
ERNT	Extended RPL Node Trustworthiness
TIDS	Trust based Security System
TOF	Trust Objective Function
TRU	Trust Information
AT	Adaptive Threshold
DT	Dynamic Threshold
FAM	Frequency Agility Manager
LR	Logistic Regression
MLP	Multi-layer Perceptron
NB	Naive Bayes
RF	Random Forest
SVM	Support Vector Machine
SOMIDS	Self Organizing Map Intrusion Detection System
SOM	Self Organizing Map
RSSI	Received Signal Strength Indicator
TN	True Negative
FP	False Positive
FN	False Negative
TPR	True Positive Rate
FPR	False Positive Rate
SPRT	Sequential Probability Ratio Test
InDRes	Intrusion detection and response system for IoT
FSM	Finite State Machine
EFSM	Extended Finite State Machine
SBIDS	Sink-based Intrusion Detection System
NCR	Node's current rank
NPR	Node's parent rank
NPVR	Node's previous rank
RIDES	Robust Intrusion Detection System
CUSUM	Cumulative Sum Control charts
OPFC	Unsupervised Optimum-Path Forest Clustering
NAC	Network Access Control
ETA	Encrypted Traffic Analytics
6TiSCH	IPv6 over the TSCH mode of IEEE 802.15.4e
TSCH	Time-Slotted Channel Hopping

transmission technologies like NFC, LTE, and Bluetooth. It promises unique addressing and routing of sensed data from a large number of devices, which are a part of the IoT network. 6LoWPAN is standardized for achieving unique addressing through IPv6 networking.

3) Application Layer: The main purpose of the application layer is to provide personalized services or interface (front end) to the IoT application users. It uses processed data from the network layer and delivers it as per the user's need. It fills the gap between users and IoT applications. The application layer provides tools to the application developers in order to realize IoT insights. It specifies various applications in which IoT can be exploited, e.g., smart homes, smart power grid, industrial monitoring, surveillance systems, healthcare monitoring, and logistics management [32], [34], [35]

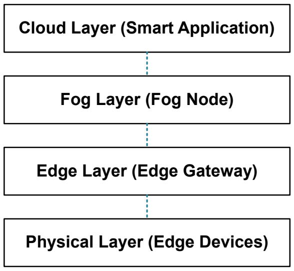
Cloud Layer (Smart Application)
Fog Layer (Fog Node)
Edge Layer (Edge Gateway)
Physical Layer (Edge Devices)

Figure 3: Fog computing based four-layer IoT architecture

Currently, IoT devices generate a large volume of data that needs to be processed at cloud servers for various purposes like business insights and security monitoring. However, the rate at which data is generated by IoT devices, requires good bandwidth connections for data transmission to the cloud servers. The limited bandwidth connections cause a significant delay in data transmission and processing, which affects the overall performance of smart applications. Three-Layer based architecture is not capable enough to solve such issues [32]. To address these issues, Edge and Fog computing paradigms [36] are emerged as possible solutions and are being used nowadays. The four-layered Fog computing based IoT architecture is shown in Fig. 3. The physical layer includes IoT devices or edge devices which sense and send data to edge gateways. The edge layer consists of edge gateways (border routers), which either perform real-time data preprocessing at source/on-premises or forward the received data to the fog node. The fog layer consists of powerful servers that collect data from edge gateways and perform the task of data preprocessing, and transmission to the cloud servers. At the cloud layer, smart applications are deployed, which perform critical tasks like business insights and security monitoring. Fog nodes can process and act on a large volume of data, reduce bandwidth and latency, and can perform security monitoring. Whereas edge nodes can apply local security policies and make real-time decisions locally to control and monitor many IoT devices at a time. With fog and edge layer, the security of IoT application and involved protocols can be improved significantly [37]–[39].

III. Overview of RPL protocol

RPL is IPv6 based Distance Vector and Source Routing protocol that specifies how to build a DODAG using a *Objective Function (OF)*, set of metrics and constraints. In RPL, the IoT devices are interconnected using mesh and tree topology in order to build a DODAG graph starting from a root (sink or gateway) node that acts as an interface between LLN nodes and the Internet. A network may contain more than one DODAG, which collectively form an RPL Instance. In a network, more than one RPL Instance can run in parallel, and every RPL Instance is identified by a unique *RPLInstanceID*. An RPL node can belong to only one DODAG of every RPL Instance running in the network. Each node in DODAG is assigned a rank (16-bit value), which represents "the node's individual position relative to other nodes with respect to a DODAG root" [3]. The rank stringently increases in DODAG's downward direction (root to leaves) and decreases in the upward direction (leaf nodes to root). The rank concept is used: (1) to detect and avoid routing loops, (2) to build parent-child relationship, (3) to provide a mechanism for nodes to differentiate between parent and siblings, and (4) to enable nodes to store a list of preferred parents and siblings which can be used in case a node loses its link with the parent node. DODAG is built during the network topology setup phase, where each node uses RPL control messages to find the optimal set of parents towards the root and link itself with the preferred parent, i.e., parent on the most optimal path. The selection of preferred parent is based on a *OF* that defines how to compute a rank based on routing metrics while considering routing constraints and optimization objectives. RPL may use different *OF* [40] which includes ETX Objective function [41], *Minimum Rank with Hysteresis Objective Function (MRHOF)* [42], *Objective Function Zero (OF0)* [43], and objective function based on combined metrics using fuzzy logic *(OF-EC) [44]*. RPL control messages include DODAG Information Object (DIO), DODAG Information Solicitation (DIS), Destination Advertisement Object (DAO), and Destination Advertisement Object Acknowledgment (DAO-ACK). RPL uses an adaptive timer mechanism called as "Trickle timer" in order to limit the control traffic in the network [45].

IV. Attacks on RPL protocol

RPL protocol is susceptible to a wide range of insider and outsider attacks. These attacks are difficult to detect and mitigate because of the vulnerable nature of nodes and wireless network, easily tamperable nature of nodes, mobility of nodes, and resource constraints. Many authors have proposed various security mechanisms specific to RPL, which include control message encryption and security modes [46]. However, most of the RPL implementations do not consider the security measures due to incomplete specification of mechanisms, and implementation overheads [47]. These security mechanisms are effective in defending against outsider attacks. However, they fail in case of insider attacks. An insider attacker may bypass the applied RPL security mechanisms and disrupt network functionality. A taxonomy of attacks, is shown in Fig. 4, where attacks are classified on the basis of their primary target. We have extended the taxonomy presented in [30] by adding recently proposed attacks, and categorizing some similar kind of attacks for better understanding. RPL control messages can be illegitimately manipulated to disrupt routing operations. Similarly, fault tolerance mechanisms can be exploited to target network resources by performing a Denial of Services attack (DoS). In this section, attacks specific to the RPL protocol are listed and briefly discussed.

Rank attacks: The rank field or rules can be exploited for performing various rank based attacks [48]. In RPL, there is no specific mechanism to monitor the integrity of control messages and routing metric values received from the parent node. In fact, a child node receives all the routing information through control messages without verifying its parent trustworthiness. Thus, if the parent node is malicious, the child node still believes that all the information coming from its parent is genuine. Hence, this condition may lead to the formation of unoptimized routes and show poor network performance. An attacker node performs the Rank attack by illegitimately changing its rank value, thus, attracting neighbor nodes to select it as their parent, assuming that the malicious node leads to the root node in the shortest path cost. Different variants of Rank attack have been proposed in the literature by the researchers, which include increased rank, decreased rank, worst parent attacks.

Neighbor or replay attack: In neighbor attack [49], an attacker node duplicates and multicast all DIO messages received from its parent. In such a case, all the neighbor nodes which receive replayed DIO messages may think that the message is received from a new neighbor. Further, if the replayed DIO message contains favorable routing information like rank, the victim neighbor node may add out of range node as its preferred parent. Another variant of this attack is proposed in [30] and termed as DIO replay attack. In this variant, an attacker nodes multicast the outdated DIO messages containing old routing information. This attack forces a victim node to follow the stale and unoptimized paths.

DAO attacks: An adversary can exploit the storing mode of the RPL protocol. It can manipulate the DAO messages to perform DAO related attacks. These types of attacks include DAO inconsistency and routing table falsification. Both of these are highlighted below.

DAO inconsistency: RPL uses some flags which are carried out in IPv6 hop-by-hop option to manage important topological mechanisms. Down 'O' flag represents the expected direction of packet, Rank-Error 'R' flag indicates rank error in topology, and Forwarding-Error 'F' flag represents that the node is not capable of forwarding packet to the set destination [3]. DAO inconsistency is reported by a node when its child node is unable to forward the data to a specified destination, due to unavailability of a route that is learned from fake DAO message (DAO with fake routing information) during topology creation. The attacker exploits this mechanism to perform an attack by setting 'F' flag to 1 in the packets and sending it back to its parent. This forces the parent node to discard legitimate available downward routes. DAO inconsistency attack leads to an increase in end-to-end delay, unoptimized topology, and isolation of nodes.

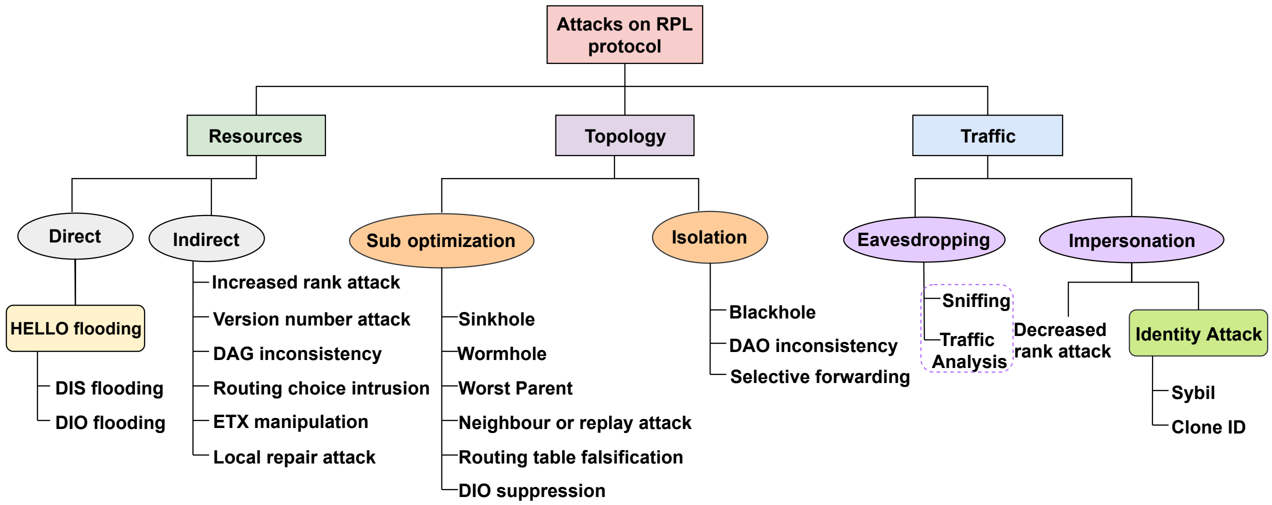

Figure 4: Detailed taxonomy of attacks specific to RPL protocol

Routing table falsification: Mayzaud *et al.* [30] proposed a methodology to perform the attacks that lead the nodes to learn fake routes which do not exist. Such attacks can create unoptimized topology due to increased end-to-end packet delay and decreased packet delivery ratio (*PDR*). An attacker may perform the attack by forging the routing information contained in DAO messages, which forces the legitimate nodes to build false downward routes, i.e., non-existing routes. Thus, when legitimate nodes try to forward the data to non-existing nodes, this situation leads to DAO inconsistency, unnecessary packet delay, and increased control overhead. In a variant of routing table falsification attack termed as routing table overload, the attacker forges a DAO message with false routing information and sends it to the parent node. It leads to the victim node's routing table buffer getting full. Thus, further creation of legitimate optimized routes is entirely blocked.

Routing choice intrusion: Zhang *et al.* [50] proposed a new internal routing attack known as Routing choice intrusion. The main idea is to learn the current routing conditions used by the nodes for choosing optimal paths. Then capturing the DIO messages, and later multicast the forged DIO messages by its legitimate identity. This attack requires a node to be reprogrammed in such a manner that it ignores the internal misbehavior detection and operates normally, thus, makes it hard to be detected. This attack may involve one or more compromised nodes. Routing choice intrusion attack leads to an increase in end-to-end delay, routing loops, energy consumption, and creation of unoptimized paths.

DIS attack: In DIS attack, an attacker node periodically sends DIS messages to neighbors within its transmission range. In return, the victim node resets its trickle timer and replies with DIO messages (RPL specific mechanism for allowing new nodes to join DODAG) [51], [52]. This attack can be performed either by sending unicast DIS messages to a single node or by multicasting DIS messages in order to target multiple nodes at a time. DIS attacks can be termed as flooding attack as it involves the flooding of DIS messages in the network [30]. It leads to an increase in control packet overhead, node energy exhaustion, and routing disruption.

Version number attack: In RPL, only border router (6BR) is responsible for initiating the propagation and updation (increase) of version number [3]. Whenever a border router or gateway (6BR) needs to rebuild the whole DODAG, it initiates a global repair process by incrementing the version number value present in the version number field of DIO message and sends it to child nodes. Upon receiving a DIO with a different version number than it has, the child node starts the process for updating its routing state (preferred parent, preferred parent, and links) by resetting its trickle timer. This process iterates until all the nodes update their routing state. RPL defines no mechanism to prevent nodes (other than 6BR) from illegitimate modification of version number [53]–[55]. Hence, an attacker can modify the version number field of the DIO message and forwards it to the neighbors. This leads to the unnecessary rebuilding of complete DODAG. It results in an increase in control packet overhead, end-to-end delay, rank inconsistencies, routing loops, and energy consumption.

Local repair attack: In RPL, a local repair mechanism is triggered by a node after it loses the link with its preferred parent [3]. A node can initiate a local repair mechanism either by changing the value in the DODAG ID field of DIO or by updating its rank to infinite and multicast the DIO to all its neighbors. Both the methods force neighbor nodes to search for a new preferred parent. Local repair enables an RPL network to converge once again in minimum time. This mechanism is supposed to be called only when a node does not have any connection with its parent. However, an attacker may deliberately use both the methods to trigger unnecessary local repairs even if it is still connected to its parent [56]–[58]. This is possible because RPL does not define any method that can be used by a node to verify the authenticity of local repair initiated by their neighbor nodes [23]. Wherever a local repair is triggered, the network topology is forced to be restructured. This leads to an increase in energy consumption of victim nodes as well as disruption of the routing process.

DODAG inconsistency: RPL specifies the data path validation method to detect and repair rank related inconsistencies (loops) in DODAG. RPL uses different flags of RPL IPv6 header options of multi-hop data packets [59] for tracking inconsistencies (routing loops) in the network. As per [3], DODAG is inconsistent if the direction flag of the data packet represented by the 'O' does not follow the strict rank relation with the node that has sent/forwarded the packet. When such a situation is encountered, the 'R' flag is used to perform topology repair, i.e., 'R' flag is set to 1 by the node which encountered forwarding error, and the packet is forwarded. Further, when another node receives a packet with 'R' flag set (detects inconsistency), it discards the packet and resets its trickle timer to perform local repair [45]. An attacker can exploit these flags to perform various attacks that are collectively termed as a DODAG inconsistency attack, which includes Direct and Forced blackhole attack [60], [61].

DIO suppression: In [62], a novel attack against RPL protocol was proposed and termed as a DIO suppression attack. The idea behind this attack is to suppress the transmission of fresh DIO control messages required by the IoT nodes for exploring new optimized routing paths and removal of stale paths. This leads to the creation of unoptimized routes, which further leads to a partition problem in the network. An attacker only needs to sniff DIO message from any legitimate node and then, multicast that message for at least k times (suppression threshold) periodically. This makes victim node believe that the consistent DIOs [45] are received from its parent node irrespective of any legitimate change in network's current state. Thus, there won't be any change in victim's current state, i.e., preferred parent set, parent, and relative distance from the root. In Fig. 5, I_{min} represents the starting time period set by trickle algorithm, which is doubled every time k consistent DIO's are received. I_{min} is initiated again when DIO's less than k are received or when any inconsistent DIO is received.

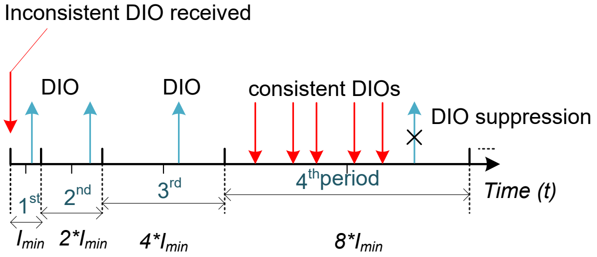

Figure 5: DIO suppression with suppression threshold ($k = 5$)[62]

ETX manipulation: In RPL, the Expected transmission count (ETX) objective function uses the ETX parameter as a metric for selecting the optimal routing path between two nodes. RPL follows a simple thumb rule, i.e., the ETX value of any parent node must be lower than that of a child node. This rule must be followed throughout the network. An attacker exploits this rule by deliberately manipulating nodes ETX value in order to gain a better position in the network [63]. This allows the attacker to attract a large part of network traffic and then launch other attacks like Blackhole and Grayhole attacks.

Table III presents a classification of attacks based on their type (insider or outsider), prerequisites, and their impact on the network's performance. RPL is also vulnerable to attacks inherited from WSN. These attacks include HELLO flood or DIO flood, Sinkhole, Wormhole [64], Blackhole, Selective forwarding, Sybil, Clone ID, etc. These attacks disrupt the network's performance drastically, which decreases the network's lifetime. Since many surveys are already available in the literature that present WSN based attacks hence we do not discuss them in this paper [65], [66].

V. Taxonomy of RPL attack defense mechanisms

In this section, different solutions proposed for the detection and mitigation of RPL attacks are discussed. The solutions present in the literature are divided into two categories: Secure Protocol and Intrusion Detection System (IDS). Secure Protocol based solutions refer to defense mechanisms that are incorporated in the RPL protocol itself, thus, making it secure against various attacks. These mechanisms are further categorized into Cryptography, Trust, and Threshold based solutions. Cryptography mechanisms make the use of traditional cryptography methods to provide security and defense against various attacks, whereas trust based mechanisms involve computation of trustworthiness of nodes for facilitating routing decisions. Threshold based defense solutions exploit the inbuilt feature of RPL and provide an enhancement in order to decide the way trickle timer is reset. These mechanisms are embedded into RPL protocol, making it more robust in terms of defensive behavior while maintaining desirable network performance. Traditional IDS solutions cannot be directly applied to IoT [90]. It is because of resource constrained nodes used in the network, different network topologies, and IP based connectivity, which makes traditional IDS solutions infeasible. This demands for lightweight IDS solutions in terms of computational, communication, memory and energy overhead. In particular to RPL protocol, IDS refers to the second line of defense, which is responsible for the detection of anomalies in RPL operation. These defense solutions can be further classified into Signature, Anomaly, Specification, and Hybrid.

In this section, a brief review of security solutions available in the literature for detecting various attacks in IoT (i.e., typically DoS and RPL based attacks) is presented. Fig. 6 shows the taxonomy of various defense solutions, in particular to the RPL protocol.

A. *Secure Protocol Based Defense Mechanisms*

This section presents various secure protocol based defense solutions for defending the RPL protocol against routing attacks. Summary of Secure Protocol solutions is presented in Table IV.

1) Cryptography Based Solutions:

Version Number and Rank Authentication (VeRA): In [53], a security scheme called VeRA is proposed. The proposed scheme provides defense solutions against attacks related to illegitimate version number and rank change. The key idea is to use hash chains for authenticating those nodes whose rank or version number is changed. VeRa incorporates an authentication mechanism based on hash operations having small time complexity. The main drawback of VeRA is that it can be bypassed using rank forgery and replay attacks.

Table III: Classification of attacks on RPL and their impact on network's performance

Attack	Type	Prerequisites	Description	Impact on network performance
Rank	Insider	-	Rank field and strict rank rules are exploited.	Generates routing loops. Increases end-to-end delay, *PDR*, control packet overhead, congestion, and energy consumption. Introduces unoptimized routes.
Neighbor /replay	Insider	-	Attacker node eavesdrops the DIO messages of legitimate neighbors and later send it to its neighbors	Increases packet loss (low *PDR*), disrupted routes, network congestion, and unwanted interference.
DAO inconsistency	Insider	Storing mode, Option Header	DAO loop recovery mechanism is exploited by the attacker.	Increases end-to-end delay. Leads to unoptimized topology and isolation of nodes.
Routing table falsification	Insider	Storing mode, Option Header	Attacker overloads the routing table of legitimate nodes with false routing information.	Routing table buffer of victim nodes gets filled, which further blocks the building of legitimate optimized routes.
Routing choice intrusion	Insider	-	Attacker node learns the current routing rules. Then, it captures real DIO messages and multicast the forged DIO messages.	Increases end-to-end delay and energy consumption. Generates routing loops and introduces unoptimized paths.
DIS	Insider /Outsider	-	Legitimate nodes are flooded with DIS messages, which forces them to reset their trickle timer and reply with new DIO messages.	Increases control packet overhead and energy consumption, and causes routing disruption.
Version number	Insider	-	Attacker node deliberately increments the version number, which triggers global repair of the network.	Increases control packet overhead, end-to-end delay, and energy consumption. Introduces rank inconsistencies and routing loops.
Local repair	Insider	-	Local repair mechanism is exploited, i.e., by changing the rank value to infinite or changing DODAG ID value to trigger unnecessary local repairs.	Disrupts the routing process and increases energy consumption.
Direct DODAG inconsistency	Insider /Outsider	Option Header	Local repair mechanism is exploited, i.e., attacker multicast the packets after setting 'O' and 'R' flags.	Traffic congestion. Increases packet loss ratio, control packet overhead and energy consumption.
Forced blackhole	Insider	Option Header	Attacker node sets 'O' and 'R' flags of received data packets and forwards them to its neighbors.	Increases control packet overhead and energy consumption. Decreases *PDR*.
DIO suppression	Insider /Outsider	-	Previously eavesdropped DIO messages are sent, which leads to suppression of new DIO transmission.	Introduces unoptimized routing paths, which leads to network partition.
ETX manipulation	Insider	ETX objective function	Manipulation of ETX value in order to gain a better position in the network and attract network traffic.	Introduces unoptimized routing paths.
HELLO/DIO flood	Insider /Outsider	-	DIO messages with favorable routing metrics are multicast with strong signal strength.	Leads to network congestion and saturation of RPL nodes. Increases packet loss ratio and control packet overhead.
Sinkhole	Insider	-	Malicious node decreases its rank in order to become the preferred parent of its neighbors.	Degrades the overall network performance due to unoptimized routes.
Blackhole	Insider	-	Malicious node drops all the packets it receives from its children nodes.	Decreases *PDR*, increases end-to-end delay, unstabilizes topology.
Selective forwarding/grayhole	Insider	-	Malicious node selectively drops packets, i.e., forwards control packets and drops data packets.	Negatively affects topology construction, which leads to disrupted routing. Decreases *PDR*.
Wormhole	Insider	Minimum two malicious nodes.	Two or more nodes create a high bandwidth tunnel between them in order to transmit data in long range.	Creates unoptimized paths.
Sybil	Insider	-	Single node posses multiple logical identity.	Overcomes voting schemes, compromises transmission routes by taking control of network.
Clone ID	Insider /Outsider	-	Single logical identity is copied to multiple nodes.	Compromises transmission routes by taking control of the network, eavesdrop on transmission links.
Jamming	Outsider	-	Attacker transmit with high power radio signals to introduce heavy interference.	Decreases *PDR* and increases energy consumption.
Sniffing	Insider /Outsider	-	Network traffic is eavesdropped for obtaining routing information from packets.	Introduces privacy concerns.
Traffic analysis	Insider /Outsider	-	Radio transmissions are eavesdropped to analyze traffic patterns for obtaining routing/topology information.	Introduces privacy concerns.

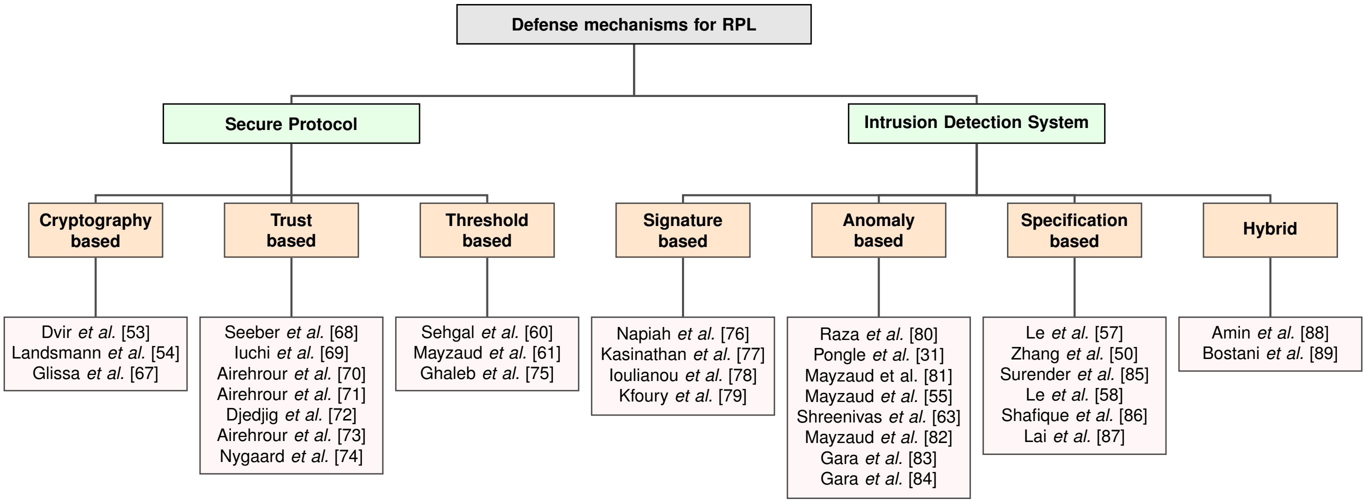

Figure 6: Taxonomy of defense mechanisms for RPL protocol

Enhanced VeRA and Trust Anchor Interconnection Loop (TRAIL): To counter Decreased rank attack, Landsmann *et al.* [54] proposed a novel security mechanism that uses a nested encryption chain to prevent an attacker from multicasting altered hash chains and maintains rank integrity. The encryption chain links both version number hash chain with rank hash chain. The proposed security mechanism does not provide defense against rank-replay attack. Perrey *et al.* [91] proposed an extension to [54] for detecting and preventing topological inconsistencies. A generic security scheme called Trust Anchor Interconnection Loop (TRAIL) is proposed to facilitate topology authentication in RPL. In TRAIL, each node can validate its upward routing path towards the root and can detect any rank spoofing without relying on encryption chains. TRAIL can search and remove illegitimate nodes from the network topology. Both VeRA and TRAIL maintain the node's states which incurs memory overhead on resource constrained nodes.

Secure-RPL (SRPL): Glissa *et al.* [67] proposed a secure version of the RPL known as SRPL. The main aim of SRPL is to stop compromised nodes from illegitimately manipulating control message information, which may lead to network disruption, i.e., rank manipulation for gaining a better position in the DODAG. SRPL incorporates a security mechanism to maintain a suitable rank threshold such that any change in the rate of rank change leads to the detection of the attack. The rank threshold is implemented with a hash chain authentication of every node in the network. The main advantage of using the proposed solution is that it does not put any limit on node movement from one DODAG to another. When a node moves from one DODAG to another or changing rank, it needs to be validated using secured hashed values at first. SRPL mainly aims to defend Sinkhole, Blackhole, Selective forwarding, and Rank attacks. SRPL involves three phases, namely the initiation phase, the verification phase, and the rank update phase. In the initiation phase, all the nodes in the network compute their rank, threshold values, and respective hashed values. In the verification phase, parents of a respective child node, other nodes check, or verify the hashed rank and thresholds. The rank update is triggered when any node wants to change its rank, and this change is verified against old information and acceptable rank change. The major limitation of SRPL is that it uses computationally expensive operations that consume a lot of node's resources.

Summary and Insights: This section discussed the various cryptography based defense solutions for securing RPL protocol. It has been observed that the proposed approaches are not sufficient enough to provide the desired security in 6LoWPAN networks. The proposed solutions face many challenges that need to be addressed. For example, the solution proposed in [53] is vulnerable to rank forgery and replay attacks. Similarly, [54], [67], [91], [92] introduce resource overhead (memory, processing), which inhibits their usage in real 6LoWPAN networks. The approach proposed in [93] introduces significant communication overhead. In order to leverage the use of cryptography based solutions, further investigation into IoT constraints is needed. Lightweight cryptography solutions can also be explored for developing IoT based security solutions.

2) Trust Based Solutions:

Trusted Computing Architecture (TCA): In [68], a TCA is proposed for establishing trust and facilitating secure key exchange among nodes using a trusted platform module (TPM). Authors have focused on making the use of low-cost TPM module to incorporate security in resource constrained nodes. The proposed architecture is capable of defending against node tampering, DoS, and routing attacks targeting availability and integrity. TPM plays a significant role in the proposed architecture as it is responsible for providing keys among authenticated nodes for establishing secure communication. TPM acts as a single point of failure, and if it is tampered or fails, it leads to network performance degradation and security breaches. No extensive evaluation and simulation results have been discussed for validating the effectiveness of TCA.

Secure Parent Selection: Iuchi *et al.* [69] proposed a Trust based threshold mechanism for securely selecting a legitimate node as a preferred parent and defending against Rank attacks. In the proposed mechanism, every node in the network selects its preferred parent by assuming the fact that illegitimate node claims a much lower rank than legitimate nodes. All the nodes in the network are capable of finding the illegitimate ranked node by computing the maximum and average rank of its neighbor nodes. A legitimate node then selects its parent node by excluding the node that shows a deficient rank and avoids forwarding packets to illegitimate nodes. The proposed mechanism shows two major limitations. First, it may sometime lead to the creation of unoptimized routes because the legitimate nodes are not selected as a parent in some cases. Second, the proposed approach is vulnerable to Sybil and Blackhole attacks.

Lightweight Trust-Aware RPL: Ariehrour *et al.* [70] proposed a Trust-Aware RPL routing protocol to detect Blackhole and Selective forwarding attacks. The primary idea behind the proposed work is that the packet drop rate of malicious nodes is higher compared to non-malicious nodes when an attacker is performing a Blackhole or Selective forwarding attack. This behavior of nodes is used to evaluate their trustworthiness. The proposed RPL enhancement uses trust values to evaluate the trustworthiness of nodes for facilitating optimal routing decisions. In Trust-Aware RPL initially, all the nodes perform normal path selection operations, i.e., computing route quality over different neighbors based on MRHOF. Trust-Aware RPL shows better performance as compared to MRHOF-RPL in terms of attacks detected, the frequency of node rank changes, throughput, and packet loss. Several drawbacks of the proposed protocol are: (1) promiscuous mode operation increases energy consumption; (2) a legitimate node may begin to drop packets due to unintentional errors that would resemble it as a blackhole attacker.

SecTrust-RPL: In [73], a time based trust aware variant of RPL protocol known as *SecTrust*-RPL is proposed. The proposed RPL variant incorporates a secure trust system that promotes secure communication, detection, and isolation of malicious nodes performing rank and Sybil attacks. The proposed trust mechanism defines a way so that each node in the network computes the trustworthiness of its neighbors by using direct and recommended trust values. *SecTrust*-RPL incorporates five modules. Trust calculation module is responsible for calculating the trust values of nodes. Trust monitoring module is responsible for updating the trust values of nodes in a periodic and reactive manner. The trust rating process is responsible for sorting trust values in descending order. Detection and isolation of attacks process responsible for selecting high-quality routes and detecting malicious and misbehaving nodes using trust values for ensuring the CIA as well as authenticity. Trust backup and recuperation process take care of the selfish nodes, i.e., nodes which aim to preserve their resources and considered malicious. *SecTrust*-RPL is compared with MRHOF-RPL, and it is shown that the proposed mechanism performs better in terms of attack detected, packet loss, throughput, and frequency of node rank changes. *SecTrust*-RPL requires nodes to operate in a promiscuous mode, which consequently leads to heavy energy consumption and decreased network lifetime.

Metric based RPL Trustworthiness Scheme (MRTS): A trust based security scheme named as MRTS is proposed in [72] for setting up secure routing paths. It works during RPL topology construction and management by incorporating trustworthiness among nodes. In order to perform a secure operation, MRTS defines a new trust based metric named as Extended RPL Node Trustworthiness (ERNT) and a new trust based objective function named as Trust Objective Function (TOF). ERNT is incorporated in DIO messages and exchanged with neighbor nodes. It is responsible for evaluating the trust value of each node and then quantifies the cost of routing paths. TOF defines a way for nodes to use ERNT and constraints for selecting the preferred parent, and compute their own rank. TOF finds the best routing paths while avoiding the paths with less trustable nodes. MRTS requires TPM for securing RPL control messages and performs all the security-related computations. MRTS shows better performance as compared to traditional RPL. However, the main limitations of MRTS are that it uses TPM, which introduces a single point of failure in the network and adds extra hardware cost to the network.

Trust based Security System (TIDS): Nygaard *et al.* [74] proposed a novel trust-based security system named as TIDS for detecting Sinkhole and Selective forwarding attacks. TIDS enables the normal node to monitor and evaluate its neighbors in order to find anomalies in the normal RPL operation. The observed data by the node is sent to root (gateway) using Trust Information (TRU) messages for further analysis. The main functionality of TIDS is based on computing trust values using subjective logic. These values are categorized into belief, disbelief, and uncertainty. The trust values are used to analyze the monitored data received from nodes. TIDS is able to detect all the attackers in the network on the cost of heavy energy consumption by the root node and false positives. TIDS requires approximately 5Kb-6.4Kb of ROM and 0.7Kb-1Kb of RAM. The main advantage of the TIDS scheme is that the normal nodes with IDS implemented on it consume very little energy while showing approximately 100% detection rate.

Summary and Insights: It is observed that some solutions present in the literature face a single point of failure issue [68], [72]. The solution proposed in [69] is vulnerable to frequent attacks like Sinkhole and Blackhole. Several works [70], [73], [74] require nodes to operate in a promiscuous mode which leads to substantial energy consumption. The energy consumption parameter must be considered as the most critical metric while designing any security algorithm for RPL. Also, the assumption of static networks also adds to one of the essential limitations of work proposed in the literature. These challenges must be addressed before the utilization of proposed solutions in the real network.

3) Threshold Based Solutions:

Adaptive Threshold (AT): In [60], a mechanism named as Adaptive Threshold (AT) is presented for countering DODAG inconsistency attacks in RPL. The default mechanism (Fixed Threshold) embedded in RPL has a threshold value of 20. After receiving a packet with ‘O’ and ‘R’ flags set, a node drops the packet and resets the trickle timer. When this number reaches up to a threshold limit of 20, all such incoming packets are dropped, but the trickle timer is not reset in order to limit the effect of an attack. This counter is reset after every hour, and in this way, RPL counters the DODAG inconsistency attack. However, a smart attacker can send 20 malformed packets every hour and affect the network performance gradually. An attacker can also use different attack patterns to degrade network's performance without getting detected. AT mechanism considers the current network state to update the threshold based on the rate of receiving packets. The value of threshold decreases when an attacker sends malformed packets very quickly, and increases when an attacker stops sending malformed packets. AT requires prior calculation of optimal configuration parameter values in the arbitrary way (i.e., α, β and γ) and does not consider the node mobility.

Dynamic Threshold (DT): Mayzaud *et al.* [61] proposed an improvement to their previous DODAG inconsistency mitigation mechanism [60]. The proposed defense mechanism is known as Dynamic Threshold (DT). It is a fully dynamic threshold mechanism that takes into account the dynamic characteristics of the network to set a threshold for mitigating the DODAG inconsistency attack efficiently. DT does not require any prior calculation of optimal value of configuration parameters like that of AT mechanism because all required information is gathered from network characteristics itself. It takes into account the convergence time of the network, i.e., the time required by the RPL network to converge. DT approach avoids unnecessary resetting of trickle timer, which consequently suppresses extra DIO transmissions. DT mechanism outperforms AT mechanism in terms of energy consumption, *PDR*, and end-to-end delay. In addition, the DT mechanism is capable of mitigating the Forced blackhole problem efficiently.

SecRPL: Ghaleb *et al.* [75] proposed SecRPL to address the DAO falsification attack. The proposed defense mechanism is based on putting a threshold on the number of DAO packets forwarded to each destination. In SecRPL, each parent node maintains a table that contains a counter, specific to every child node in its sub-DODAG. Once the number of DAOs from any child node exceeds the fixed threshold, then that child is marked as malicious. The parent node drops any further DAO containing the prefix of that malicious child. In order to avoid the situation where any child is permanently blocked, the counter table is reset on every DIO multicast. SecRPL shows significantly good results in terms of the number of DAOs forwarded, control packet overhead, average power consumption, upward, and downward latency. SecRPL requires the selection of optimal threshold limit for efficient operation, which incurs overhead to the security scheme.

Summary and Insights: As far as the literature is concerned, only a few works [60], [61], [75] focus on using threshold based solutions are available. Moreover, the proposed solutions address only DODAG inconsistency, Forced blackhole, and DAO falsification attacks, which leaves a big gap to be filled in this field. In addition, the proposed solutions do not consider node mobility, which may hinder the overall system's performance. The key to threshold based solutions lies in the optimal selection of thresholds, i.e., parameters while considering the network environment. This assumption makes such solutions challenging to be developed for other routing attacks. The standard RPL parameters can be used in the optimal selection of thresholds for the development of lightweight threshold based defense solutions [51], [52].

B. Intrusion Detection System (IDS)

This section discusses various IDS based defense solutions for detecting routing attacks against RPL protocol. IDS based RPL defense mechanisms are summarized in Table V.

1) Signature Based IDS:

Intrusion Detection System for 6LoWPAN networks: Kasinathan *et al.* [77] proposed an IDS to detect DoS attacks in 6LoWPAN network . An open-source IDS Suricata is used for pattern matching and attack detection. An IDS probe node is used to sniff all the packet transmissions in the network, and transfer information to Suricata IDS (Open source IDS) for further analysis and attack detection. To prevent communication overhead, the IDS probe node is connected directly to Suricata IDS using a wired link. In addition, a Frequency Agility Manager (FAM) is incorporated to make the network aware of channel occupancy in real-time and operates when the interference level exceeds the set threshold. In this situation, FAM changes the operating channel to the best available one, thus, providing uninterpreted network operations. No simulation study is done in support of IDS performance and its usability.

Compression Header Analyzer Intrusion Detection System (CHA-IDS): Napiah *et al.* [76] proposed a centralized IDS named CHA-IDS for detecting HELLO flood, Sinkhole and Wormhole attacks. It uses compression header data to extract certain important network features that are used for detecting individual and combined attacks. The proposed IDS uses the best first and greedy stepwise strategy with correlation-based feature selection to determine the significant features. Then the selected features are evaluated using six Machine Learning (ML) algorithms (Decision Trees (J48), Logistic Regression (LR), Multi-layer Perceptron (MLP), Naive Bayes (NB), Random Forest (RF), and Support Vector Machine (SVM)) which are used to perform classification of normal and benign traffic. CHA-IDS outperforms SVELTE and the IDS proposed in [31]. The main limitations of CHA-IDS include high memory and energy consumption. Moreover, it is incapable of identifying the attacker.

Signature-based Intrusion Detection System: A framework for a signature-based IDS to detect DIS and Version number attack is proposed in [78]. The proposed IDS requires detection and monitoring modules to be placed on nodes itself, as in the case of hybrid detection schemes. However, the authors consider two types of additional nodes in the proposed scheme. The first type of nodes are IDS routers, which carry detection and firewall modules. The second type of nodes are sensors or IDS detectors which are responsible for monitoring and sending malicious traffic information to the router nodes. IDS router checks all the passing traffic to decide whether the packet source is malicious or not. The job of the IDS detector is to monitor sensor traffic and calculate the metric of interest , i.e., Received Signal Strength Indicator (RSSI), packet drop rate, and packet sending rate. The final decision of classifying a node as malicious or not is taken by detection module running on 6BR, based on the data received from each node. The proposed framework is not validated, which is its major limitation.

Table IV: Summary of Secure Protocol based defense mechanisms

Reference	Defense Mechanism	Relevant Attack	Limitations	Mobility	Validation	Tools/Motes	Performance metrics
Dvir *et al.* [53]	VeRA	Version number and Decreased rank	Vulnerable to Rank-replay attack, Hash chain forgery attack, adds memory and computational overhead.	No	-	-	-
Landsmann *et al.* [54]	Enhanced VeRA	Version number and Decreased rank	Vulnerable to Rank-replay attack, adds memory overhead, child node might select attacker as a parent.	No	-	-	-
Perrey *et al.* [91]	TRAIL	Version number, Decreased rank, Rank-replay	Adds memory overhead.	No	Testbed	DES Mesh/RIOT OS	Routing convergence time, Average message size
Seeber *et al.* [68]	Trusted Computing Architecture	RPL routing attacks targeting availability and integrity, node tampering	TPM is a single point of failure, adds computational overhead due to cryptography processing.	No	-	-	-
Sehgal *et al.* [60]	Adaptive Threshold	DODAG inconsistency	Requires prior calculation of configuration parameters (optimal values).	No	Simulation	Contiki OS/Cooja	*PDR*, Energy consumption and Control packet overhead
Mayzaud *et al.* [61]	Dynamic Threshold	DODAG inconsistency	Increases energy consumption.	No	Simulation		Control packet overhead, *PDR*, Energy consumption
Ghaleb *et al.* [75]	SecRPL	DAO falsification	Increases Average power consumption, Control packet Overhead and Latency. Decreases *PDR* and degrades network reliability.	No	Simulation	Contiki OS/Cooja	Control Packet Overhead, *PDR*, Energy consumption, DAO forwarding overhead, Upward and downward Latency
Iuchi *et al.* [69]	Secure Parent Selection	Rank	Susceptible to Sybil and Blackhole attacks, may result in longer paths (unoptimized).	No	Simulation	Contiki OS/Cooja	Total number of child nodes attached to attacker nodes.
Glissa *et al.* [67]	Secure-RPL (SRPL)	Rank, Sinkhole and Selective forwarding attacks	Computationally expensive.	No	Simulation	Contiki OS/Cooja	Average power consumption, Control message overhead, and Packet reception rate
Djedjig *et al.* [72]	Metric-based RPL Trustworthiness Scheme (MRTS).	Insider attacks	Adds computation and communicate overhead and increases energy consumption.	No	-	-	-
Ariehrour *et al.* [70]	Trust-Aware RPL	Blackhole and Selective forwarding	Nodes need to operate in promiscuous mode to overhear neighbor transmissions which adds energy overhead.	No	Simulation	Contiki OS/Cooja	Detection rate, Throughput, Packet loss and Frequency of node rank changes.
Ariehrour *et al.* [71]	Trust-Aware RPL for detecting Blackhole	Blackhole	Nodes need to operate in promiscuous mode which adds energy overhead.	No	Testbed	Contiki/ XM1000 motes	Detection rate, Throughput, Packet loss and Frequency of node rank changes.
Ariehrour *et al.* [73]	SecTrust-RPL	Rank and Sybil	Considers static network topology, nodes need to operate in promiscuous mode which increases energy consumption.	No	Simulation and Testbed	Contiki/ XM1000 motes	Detection rate, Throughput, Packet loss and Frequency of node rank changes.
Nygaard *et al.* [74]	TIDS	Sinkhole and Selective forwarding	Considers static network topology, requires 6BR (root) to remain constantly ON which consequently increases energy consumption, high *FPR*.	No	Simulation	Contiki OS/Cooja	*Detection rate, FN, FP*, Energy consumption

Self Organizing Map Intrusion Detection System (SOMIDS): Kfoury *et al.* [79] proposed SOMIDS for detecting Sinkhole, Version number, and HELLO flooding attacks. SOMIDS uses Self Organizing Maps (SOM) for clustering attacks and normal traffic. SOMIDS uses a Pcap file from a cooja simulator for extracting data and performing clustering of traffic classes. SOMIDS consists of three major components. The first component is an aggregator module that is responsible for aggregating the data (ICMPv6 code, IPv6 destination, IPv6 source, ICMPv6 DIO version, ICMPv6 DIO rank, Timestamp) contained in captured PCAP file. Traffic data is aggregated into six variables, i.e., number of DIS, DIO, DAO messages, the ratio of version number changes, the ratio of rank changes, and average mote power. The second component is normalizer, which performs the task of normalizing the aggregated data. Third component is a trainer module which is responsible for training SOM. The result of the IDS is a matrix that is converted into a 2D image for better visualization of clusters. SOMIDS is not evaluated in terms of the implementation overhead and does not consider node mobility.

Summary and Insights: It is analyzed that some of the proposed approaches [77], [94] rely on the outdated signatures (traffic patterns) for classifier training which makes these approach ineffective for securing RPL networks. The solutions proposed in [76], [79], [95] used signatures collected from the simulated attacks. These approaches show promising results in terms of prominent metrics. However, signatures collected from the real network can be more effective in classifier training. The development of RPL based real traffic dataset containing traces of common routing attacks needs to be done [96], [97]. The signature based IDS proposed in [76] can be improved in terms of energy consumption.

2) Anomaly Based IDS:

SVELTE: Raza *et al.* [80] proposed a real-time IDS named SVELTE for 6LoWPAN. The proposed IDS consists of anomaly based detection engine which uses RPL specifications for detecting spoofed information, Sinkhole, and Selective forwarding attacks. It consists of three centralized modules that are placed on 6BR: Mapper, Analyzer and Detector, and a Mini-firewall. Every child node sends RPL information to 6BR for illegitimate traffic filtering. Intrusion detection in SVELTE involves network graph inconsistency detection, node availability detection, and routing graph validation. SVELTE imposes very less memory, computational, and energy overhead on the resource constrained nodes. Moreover, it shows a good performance in terms of *PDR* and control packet overhead. The limitations of SVELTE include strategic placement of IDS modules, timing inconsistency in rank measurements, which consequently leads to inaccurate topology creation at 6BR, and high false positive rate (*FPR*). In addition, SVELTE does not provide defense against coordinated attacks.

Real Time Intrusion and Wormhole Detection: A novel IDS for the detection of Wormhole attack in IoT is proposed in [31]. It detects the packet relay and encapsulation types of Wormhole attack. The proposed IDS uses the node's location and neighbor information to identify the attack and received signal strength indicator (RSSI) to identify attacker nodes. A hybrid deployment strategy on a static network is considered for placing IDS modules, where a centralized module is placed on 6BR, and distributed modules are placed on resource constrained nodes. Distributed modules are responsible for sending and monitoring RSSI values, sending neighbor information to 6BR, and packet forwarding. Centralized modules collect RSSI values, compute the distance from the node's RSSI value, and perform validation of neighbors from collected information and detect attack with its location. The main drawback of the proposed IDS is that it puts much communication and computational burden on resource constrained nodes.

Distributed Monitoring Architecture: Mayzaud *et al.* [81] proposed a distributed monitoring architecture for detecting DODAG inconsistency attacks. The proposed architecture makes the use of RPL multi-instance feature and dedicated monitoring nodes for facilitating energy efficient network events observation (passively). Two types of nodes are considered in the network, i.e., regular (monitored) and monitoring nodes. The multi-instance feature of RPL is used for creating regular (the network of regular nodes) and monitoring network (the network of monitoring nodes). The monitoring nodes contain local anomaly detection (algorithm) modules that analyze the collected data and detect possible attacks in a distributed manner. The main limitations of the proposed architecture are: it assumes a single attacker case and fails in case of multiple attackers which are operating in a collaborative manner, monitoring nodes need to operate in promiscuous modes for anomaly detection, depends on the coverage of regular nodes by monitoring nodes (strategic placement), relies on high order devices for monitoring which adds cost overhead, architecture relies on local detection.

Extension to Distributed Monitoring Architecture: Mayzaud *et al.* extended their previous proposed approach [81] in [55] to detect Version number attacks. Authors considered the fact that an incremented version number is propagated in the entire graph, and a monitoring node cannot decide by itself if this is the result of an attack or not, and they must share monitoring information to identify the malicious node more efficiently. Thus, they extended the distributed monitoring architecture such that monitoring nodes can collaborate together using a multi-instance network and facilitate global detection. Only one attacker case is assumed, and mobility is not considered in this defense architecture. An extension to [55] is presented in [82]. In this work, detection and localization algorithms are presented. The *"LOCAL_ASSESSMENT"* algorithm is deployed on monitoring nodes except the root, which allows monitoring nodes to report to the root the sender of an incremented version number in their neighborhood. The *"DISTRIBUTED_DETECTION"* algorithm is deployed on the sink to detect the attack and gather all monitoring node information into tables. The *"LOCALIZATION"* algorithm is deployed on the sink node and performs attacker identification by analyzing the collected information. This framework inherits the limitations of Mayzaud *et al.* [81].

Extended SVELTE based on ETX metric: An extension to SVELTE is proposed in [63]. In addition to SVELTE IDS modules, an extra intrusion detection module which uses the ETX metric is incorporated for the detection of ETX manipulation attacks in ETX metric based RPL networks.

The authors have also proposed an intrusion detection method which uses geographical parameters (node's location and transmission limits) for handling a case when both rank and ETX based detection methods fail. The main idea behind ETX based intrusion detection method is that ETX value of the parent node must be lower than that of its children node, and if any node's ETX value is found to be inappropriate or unusual, then the node reported as malicious. The main advantage associated with the proposed solution is that the ETX based IDS can defend against ETX and rank based attacks. In contrast, the geographical parameter based method can locate the nodes and test their authenticity. The proposed IDS solutions consume less power when nodes operate in duty cycling mode and require only $5,570$ and 6 Bytes of RAM and ROM, respectively. A high true positive rate (*TPR*) is achieved when both the proposed solutions are combined together. The proposed solution does not consider node mobility in the network.

Hybrid IDS based on the Sequential Probability Ratio Test with an Adaptive Threshold: A hybrid IDS that combines the Sequential Probability Ratio Test (SPRT) with an Adaptive Threshold to detect Selective forwarding attack is proposed in [83]. It uses two types of modules, a centralized module deployed on the gateway node and a distributed module deployed on resource constrained nodes. The proposed IDS involves three steps, i.e., data gathering, data analysis, decision, and elimination of compromised node. The data gathering step involves each routing node to collect the neighbor's information, storing it in the form of a table, and then send it to the centralized node using HELLO messages. The data analysis step involves the computation of the number of dropped packets and the probability of dropped packet for each node using data gathered from HELLO messages. The decision step is responsible for detecting malicious nodes and minimizing *FAR* by utilizing SPRT. The elimination of the compromised node step involves informing legitimate nodes about the compromised nodes by initiating a global repair and sending the compromised node's identifier in fresh DIO messages to all other legitimate nodes in the network. The proposed IDS achieves 100% detection rate. However, the communication overhead of the network increases with the increase in node mobility.

Summary and Insights: Many of the anomaly based IDS solutions present in the literature show acceptable performance, which favors their utility in IoT applications. However, it is observed that the proposed solutions achieve high performance (accuracy, *TRP, FPR*, etc.) while imposing an additional cost to the nodes in terms of communication, computation, memory, and energy consumption. The solutions proposed in [31], [55], [81], [83], [84], [98], [99] impose extra network deployment cost which is undesirable for resource constrained networks. Similarly, the security approach proposed in [80] requires the strategic placement of IDS monitoring modules, which add an implementation complexity to the network. Moreover, it is also observed that the proposed anomaly based IDS are still vulnerable to the coordinated attacks. These critical challenges must be addressed for the advanced development of anomaly based IDS for IoT.

3) *Specification Based IDS:*

Intrusion detection and response system for Internet of things (InDReS): In [85], a distributed IDS named InDReS to detect Sinkhole attack in RPL is proposed. The proposed IDS is based on cluster tree topology, where cluster head acts as a monitoring node that observes packet drop count of its adjacent nodes. The monitoring nodes compute the rank of every adjacent node to it and compare that rank with the threshold value for finding a malicious node. InDReS is implemented on NS-2, and performance results are compared with that of INTI. The results show that the proposed IDS performs well compared to INTI in terms of packet drop ratio, *PDR*, control packet overhead, and average energy consumption. The limitations of InDReS include: only homogeneous nodes are considered, the dynamic network is not considered, and it may fail if the leader node itself gets compromised.

Specification-Based IDS for Detecting Topology Attacks: Le *et al.* in their previous work [57] proposed a specification based IDS architecture which lacks implementation and performance analysis. In [58], the authors extended the previous architecture and evaluated it in terms of prominent evaluation metrics. They proposed a specification based IDS consisting of Extended Finite State Machine (EFSM) that is generated from a semi-auto profiling technique. Firstly, EFSM is created from RPL specification using ILP (Integer Linear Programming) technique to define stable states and transitions among them. Secondly, RPL knowledge of the RPL profile of detection algorithms is translated to form more concrete states and transitions, i.e., utilizing trace files generated from RPL normal operation in the Cooja simulator. This specification defines all the legitimate states and transitions which a node must follow while operating in a normal manner. EFSM is implemented as a set of rules on intrusion detection agents for detecting various attacks, including Rank, Local Repair, Neighbor, DIS, and Sinkhole. The proposed IDS is shown to achieve *TPR* of 100% with *FPR* up to 6.78%. The proposed IDS introduces communication overhead, requires a good network trace for the creation of effective specification, and shows less accuracy when it works for a long time.

RPL-Based Wormhole Detection: Lai *et al.* [87] proposed a distributed wormhole detection method which applies the rank information to estimate the relative distance from the root node. The proposed method uses the hop count metric for rank calculation. To detect malicious nodes, the proposed detection method checks for the nodes with unreasonable rank values. It defines *Rank_Threshold* and *Rank_Diff* attributes for the detection of illegitimate DIO messages. *Rank_Threshold* is defined as the difference between the rank values of parent and node itself, whereas *Rank_Diff* is the difference between the rank values of the source node and node itself. DIO message is considered as abnormal, when *Rank_Diff*>*Rank_Threshold* condition is not met. The proposed wormhole detection method shows a 100% output in terms of precision, recall, and accuracy. The main advantages of this approach are its easy implementation and no additional requirement for Wormhole attack detection. However, node mobility is node considered, which can severely affect the detection results. In addition, critical parameters like *PDR*, end-to-end delay, and energy consumption are not analyzed.

Specification based IDS based on Finite State Machine: In [57], a specification based IDS is proposed for detecting rank and local repair attacks. The proposed IDS uses a finite state machine (FSM) for monitoring the node's state, i.e., normal or malicious. A backbone architecture is used for placing monitoring nodes containing FSM modules. Monitoring nodes sniff neighbor transmissions, including its parent and child nodes. The parameters like node id, the preferred parent with their respective rank, state changes in a specific period are monitored and extracted from sniffed DIO messages in order to analyze the node's behavior. Monitoring nodes collaborate and share information for detecting attacker nodes. FSM specifies normal and malicious states. FSM state specifies the strict rank rule which nodes must follow, i.e., parent-child relationship, and an acceptable threshold for the number of times a topology can be set up or updated. Any deviation from the specified rules and threshold consequently changes the node's state from normal to suspicious and detects the possible attacker node.

IDS to defense Routing choice intrusion Intrusion: An IDS to defend against Routing choice intrusion (ETX metric) is proposed in [50]. The proposed IDS is based on specification methodology that uses a stand alone architecture with distributed monitoring nodes. Authors consider attack defense only against a single intruder case. The proposed IDS requires monitoring nodes containing FSM with normal and malicious states. Network behaviors are matched with FSM states, and any deviation from normal state leads to attack detection. Routing choice intrusion is detected in the case when any malicious node multicast the DIO with lower ETX value, which consequently leads to a large fluctuation in the number of its child nodes than a set threshold, this node is marked as an attacker node. The authors consider certain assumptions like secure network initialization, homogeneous nodes, monitoring nodes with more resources, and static environment, which limits the practicality of the proposed IDS.

Sink-based Intrusion Detection System (SBIDS): In [86], a centralized specification based IDS known as SBIDS is proposed to address rank attacks in RPL based IoT networks. SBIDS uses information contained in the DAO message received from child nodes in its sub-DODAG. SBIDS utilizes RPL parameters, including node's current rank (NCR), node's parent rank (NPR), node's previous rank (NPVR), and parent switching threshold (PST) for detecting whether a node is malicious or not. SBIDS achieves 100% accuracy in case of a static network. The accuracy decreases in the presence of mobile nodes in the network. SBIDS adds a communication overhead to RPL protocol as it requires an extra 48-bit information to be added by the nodes in the DAO packets they send. SBIDS shows better results for a static network as compared to the mobile network. The average power consumption of nodes increases in the case of SBIDS.

Summary and Insights: The effectiveness of specification based IDS solutions can be observed from their performance. The only key challenge in the development of specification based IDS is the availability of quality traffic trace required for generating adequate specifications [58]. It is observed that several approaches [86], [87] have not performed power consumption analysis, hence there exists an open research gap to be considered for future research. Moreover, the integration of mobility support in the proposed solutions is a challenging task and needs further investigation.

4) Hybrid IDS:

Robust Intrusion Detection System (RIDES): Amin *et al.* [88] proposed a novel IDS named RIDES for detecting DoS attacks in IP based WSN. It is a hybrid of signature and anomaly based IDS. The signature based intrusion detection component uses a distributed pattern matching using bloom filters to match signature codes. To reduce the overhead to long signature codes, a coding scheme is used which converts signatures into short attack identifiers. The anomaly based intrusion detection component uses Cumulative Sum Control charts (CUSUM) with upper and lower threshold limits to detect anomalies in the network pattern. A distributed approach is used to place the intrusion detection components for decreasing the communication, memory, and computational overhead on nodes. The main limitation of this work is interpacket delay that leads to delayed intrusion detection by RIDES. In addition to it, energy consumption by the resource constrained nodes is not studied.

Hybrid of Anomaly and Specification based on optimum-path forest clustering: A novel real-time hybrid IDS framework is proposed in [89] to detect Sinkhole, Selective forwarding, and Wormhole attacks. Specification based IDS modules are deployed on router nodes which perform analysis of their child nodes and forward their local results to the gateway node through data packets. The gateway node is equipped with anomaly based IDS module which employs Unsupervised Optimum-Path Forest Clustering (OPFC) algorithm for projecting clusters by using incoming data packets. The simulation results show that the proposed IDS framework achieves the maximum *TPR* of 96.02% with 2.08% of *FPR*. The main features of the proposed hybrid IDS include high scalability and attacker identification. There are several drawbacks associated with this hybrid IDS. It does not consider the energy constrained nature of nodes, assumes one-way communication (node to gateway), and considers only a static network.

Summary and Insights: Similar to signature and anomaly based IDS, hybrid based IDS solutions also face several challenges that need to be addressed. Delayed attack detection makes IDS solutions inefficient when deployed in real networks. The IDS proposed in [88] is affected by the interpacket delay that causes delayed attack detection. Such issues need to be carefully addressed while designing IDS for IoT applications. Hybrid IDS proposed by Bostani *et al.* [89] utilized MapReduce architecture to manage a large amount of data from motes and perform attack detection efficiently. Other such algorithms available in the literature need to be explored for building scalable and effective IDS solutions corresponding to IoT.

Table VI presents a comparative study of discussed security solutions (Secure Protocol and IDS) based on different evaluation metrics. The performance is compared based on the maximum improvements achieved in percentages (%), and maximum or minimum values (val) achieved.

Table V: Summary of Intrusion Detection System based defense mechanisms

Reference	**Defense Mechanism**	**Type**	**Placement strategy**	**Relevant Attack**	**Limitations**	**Mobility**	**Validation**	**Tools/Motes**	**Performance metrics**
Amin *et al.*[88]	RIDES	Hybrid	Distributed	DoS	Inter packet delay affects the detection time.	No	Simulation	ns-2	*TPR, FPR, ROC*
Le *et al.*[57]	Specification based IDS	Specification	Distributed	Rank, Local repair	No simulation study has been done for the proposed IDS.	No	-	-	-
Raza *et al.*[80]	SVELTE	Anomaly	Hybrid	Sinkhole, Selective forwarding, spoofed or altered information	Synchronization issue, requires strategic placement of IDS modules, high FPR, vulnerable to coordinated attacks.	No	Simulation	Contiki OS /Cooja	Energy consumption, *TPR*
Kasinathan *et al.*[94]	DoS detection IDS Architecture	Signature	Centralized	DoS	The centralized nature of the IDS architecture makes it difficult to detect internal attacks and introduces communication overhead over resource constrained nodes.	No	Testbed	PenTest /Contiki OS	*TP*
Kasinathan *et al.*[77]	Intrusion Detection System for 6LoWPAN networks	Signature	Centralized	DoS	The centralized nature of the IDS architecture makes it difficult to detect internal attacks and introduces communication overhead over resource constrained nodes.	No	Testbed	PenTest /Contiki OS	-
Zhang *et al.*[50]	IDS to defense Routing choice Intrusion	Specification	Distributed	Routing choice intrusion	Assumes secure network initialization and homogeneous devices. Monitoring nodes need to operate in promiscuous mode.	No	Simulation	Contiki OS /Cooja	-
Pongle *et al.*[31]	Real Time Intrusion Detection System	Anomaly	Hybrid	Wormhole	Introduces communication and computational overhead.	No	Simulation	Contiki OS /Cooja	*TPR*, Energy consumption, Control packet overhead
Mayzaud *et al.*[81]	Distributed Monitoring Architecture	Anomaly	Distributed	DODAG inconsistency	It assumes a single attacker case and fails in case of multiple attackers operating in a collaborative manner. Monitoring nodes need to operate in promiscuous modes for anomaly detection. Depends on the coverage of regular nodes by monitoring nodes (strategic placement). Relies on high order devices for monitoring, which adds cost overhead. Architecture relies on local detection.	No	Simulation	Contiki OS /Cooja	-
Mayzaud *et al.*[55]	Distributed Monitoring Architecture	Anomaly	Hybrid	Version number	It considers only a single attacker case, monitoring nodes need to operate in promiscuous modes for anomaly detection, relies on high order devices for monitoring, which adds cost overhead. Do not consider node mobility and depends on the coverage of regular nodes by the monitoring nodes (strategic placement).	No	Simulation	Contiki OS /Cooja	*FPR*

Table V: Summary of Intrusion Detection System based defense mechanisms

Reference	**Defense Mechanism**	**Type**	**Placement strategy**	**Relevant Attack**	**Limitations**	**Mobility**	**Validation**	**Tools/Motes**	**Performance metrics**
Mayzaud *et al.*[82]	Distributed Monitoring Architecture	Anomaly	Hybrid	Version number	It considers only a single attacker case, monitoring nodes need to operate in promiscuous modes for anomaly detection, relies on high order devices for monitoring, which adds cost overhead. Do not consider node mobility and depends on the coverage of regular nodes by the monitoring nodes (strategic placement).	No	Simulation	Contiki OS /Cooja	*FPR*
Surender *et al.*[85]	InDReS	Specification	Distributed	Sinkhole	It considers only homogeneous nodes and do not consider network dynamicity. This approach may fail if leader node itself gets compromised.	No	Simulation	ns-2	Packet drop ratio, *PDR*, Throughput, Energy consumption, Control packet overhead
Le *et al.*[58]	Specification based IDS	Specification	Hybrid	Rank, Sinkhole, Local repair, Neighbor, DIS	Introduces communication overhead, requires a good network trace for the creation of effective specification, and shows less accuracy when it works for a long time.	No	Simulation	Contiki OS /Cooja	*TPR*, *FPR*, Energy consumption
Lai *et al.*[87]	RPL-Based Wormhole Detection	Specification	Distributed	Wormhole	Node mobility is not considered which can severely affect detection results. Critical parameters like *PDR*, end-to-end delay and energy consumption are not analyzed.	No	Simulation	-	Precision, Recall and Accuracy
Shreenivas *et al.*[63]	Extended SVELTE based on ETX metric	Anomaly	Hybrid	ETX manipulation, Rank	Do not consider mobility. Parameters like end-to-end delay, *PDR* are not not analyzed.	No	Simulation	Contiki OS /Cooja	Average power consumption, *TPR*
Chen *et al.*[99]	Intrusion Detection System for Detecting Wormhole and Flooding Attacks	Anomaly	-	Wormhole, Flooding	Overhead of maintaining blacklist in large-scale networks affects overall network performance. Placement strategy for IDS modules is not discussed.	No	Simulation	-	Precision, Recall, Accuracy and Miss rate
Ahsan *et al.*[100]	ABR-SAR based IDS for Wormhole detection	Anomaly	Hybrid	Wormhole	Increases implementation complexity. Strategic placement of SAN is needed so that every node must be in range of at least one another SAN.	No	Simulation	Contiki OS /Cooja	Detection rate, Average power consumption
Gara *et al.*[83]	Hybrid Intrusion Detection System based on Sequential Probability Ratio Test with an Adaptive Threshold	Anomaly	Hybrid	Selective forwarding	Exchange of HELLO messages increases network overhead.	Yes	Simulation	Contiki OS /Cooja	Detection rate, Control packet overhead

Table V: Summary of Intrusion Detection System based defense mechanisms

Reference	Defense Mechanism	Type	Placement strategy	Relevant Attack	Limitations	Mobility	Validation	Tools/Motes	Performance metrics
Gara *et al.*[84]	Hybrid Intrusion Detection System based on Sequential Probability Ratio Test with an Adaptive Threshold	Anomaly	Hybrid	Selective forwarding and Clone ID	Exchange of HELLO messages increases network overhead.	Yes	Simulation	Contiki OS /Cooja	Detection rate, Control packet overhead
Napiah *et al.*[76]	Compression Header Analyzer Intrusion Detection System (CHA-IDS)	Signature	Centralized	HELLO flooding, Sinkhole and Wormhole	Introduces memory and energy consumption. It cannot identify the attacker.	No	Simulation	Contiki OS/ Cooja/ Weka	*TPR, FPR*, Accuracy, Energy Consumption
Bostani *et al.*[89]	Hybrid of Anomaly and Specification based IDS	Hybrid	Distributed	Sinkhole and Selective forwarding	Assumes one way communication. Energy overhead analysis is not done.	No	Simulation	MATLAB	*TPR, FPR*, Accuracy
Shafique *et al.*[86]	SBIDS	Specification	Centralized	Rank	Introduces communication overhead and increases Average power consumption.	Yes	Simulation	Contiki OS /Cooja	*TP, FP, FN, FP*, Accuracy, Average power consumption
Ioulianou *et al.*[78]	Framework of Signature-based IDS	Signature	Hybrid	HELLO flooding and Version number	No validation is performed in support of the framework.	No	-	-	-
Kfoury *et al.*[79]	SOMIDS	Signature	Centralized	HELLO flooding, Sinkhole, and Version number	No evaluation in terms of prominent performance metrics is done. Energy consumption of 6BR is not studied.	No	Simulation	Contiki OS /Cooja /Python	-
Shukla *et al.*[95]	ML-IDS (KM-IDS, DT-IDS and Hybrid-IDS)	Signature	Centralized	Wormhole	*FP* value is not reported. Energy consumption and deployment strategy are not discussed.	No	Simulation	C++	Detection rate

Table VI: Performance comparison of security solutions in terms of different evaluation metrics

Reference	**Throughput (%)**	**Routing convergence time (%)**	**Extra messages per node (val)**	**Packet delivery ratio (%)**	**Energy consumption (%)**	**Control packet overhead (%)**	**DAO forwarding overhead (%)**	**Upward latency (%)**	**Downward latency (%)**	**Average power consumption (%)**	**Packet reception ratio (%)**	**Packet loss (%)**	**Node rank changes (%)**	**True negatives (%)**	**False negatives (%)**	**False positives (%)**	**False positive rate (val)**	**Receiver operating characteristic (val)**	**Packet drop ratio (%)**	**Precision (val)**	**Recall (val)**	**Accuracy (val)**	**Miss rate (val)**	**Detection rate or *TPR* (val)**	**Affected child nodes (%)**	**True positives (%)**
Dvir *et al.*[53]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Landsmann *et al.*[54]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Perrey *et al.*[91]		20	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Seeber *et al.*[68]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Sehgal *et al.* [60]	-	-	-	99	40	55	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Mayzaud *et al.*[61]	-	-	-	99	50	50	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Ghaleb *et al.*[75]	-	-	-	99	-	-	90	70	55	30	-	-	-	-	-	-	-	-		-	-	-	-	-	-	-
Iuchi *et al.*[69]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	99	-
Glissa *et al.*[67]	-	-	-	93	-	35	-	-	-	35	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Djedjig *et al.*[72]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Ariehrour *et al.*[70]	63	-	-	-	-	-	-	-	-	-	30	80	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Ariehrour *et al.* [71]	66	-	-	-	-	-	-	-	-	-	-	28	66	-	-	-	-	-	-	-	-	-	-	-	-	-
Ariehrour *et al.*[73]	-	-	-	-	-	-	-	-	-	-	-	15	62	-	-	-	-	-	-	-	-	-	-	-	-	-
Nygaard *et al.*[74]	-	-	-	-	99	-	-	-	-	-	-	-	-	-	0	-	-	-	-	-	-	100	-	100	-	-
Amin *et al.*[88]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	5	98	-	-	-	-	-	90	-	-
Le *et al.*[57]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Raza *et al.*[80]	-	-	-	-	99	-	-	-	-	99	-	-	-	-	-	-	-	-	-	-	-	-	-	100	-	-
Kasinathan *et al.*[94]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	100
Kasinathan *et al.*[77]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Zhang *et al.*[50]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Pongle *et al.*[31]	-	-	-	-	0	86	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	94	-	-
Mayzaud *et al.*[55]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	-	-	-	-	-	-	-	-	-
Mayzaud *et al.*[82]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	-	-	-	-	-	-	-	-	-
Surender *et al.*[85]	8	-	-	8	11	17	-	-	-	-	-	-	-	-	-	-	-	-	38	-	-	-	-	-	-	-
Le *et al.*[58]	-	-	-	-	0	-	-	-	-	-	-	-	-	-	-	-	0	-	-	-	-	-	-	100	-	-
Lai *et al.*[87]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	100	100	100	-	-	-	-
Shreenivas *et al.*[63]	-	-	-	-	-	-	-	-	-	0	-	-	-	-	-	-	-	-	-	-	-	-	-	100	-	-
Chen *et al.*[99]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	100	100	100	0	-	-	-
Ahsan *et al.*[100]	-	-	-	-	-	-	-	-	-	0	-	-	-	-	-	-	-	-	-	-	-	-	-	95	-	-
Gara *et al.*[83]	-	-	-	-	-	0	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	100	-	-
Gara *et al.*[84]	-	-	-	-	-	0	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	100	-	-
Napiah *et al.*[76]	-	-	-	-	0	-	-	-	-	-	-	-	-	-	-	-	0	-	-	-	-	99	-	99	-	-
Bostani *et al.*[89]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	97	-	96	-	-
Shafique *et al.*[86]	-	-	-	-	-	-	-	-	-	0	-	-	-	3	0	0	-	-	-	-	-	100	-	-	-	99
Ioulianou *et al.*[78]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Kfoury *et al.*[79]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Shukla *et al.*[95]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	93	-	-

VI. Cross-layered security solutions for RPL

RPL security is not restricted to network layer specific defense solutions. IEEE 802.15.4 MAC layer implements several features to provide security services such as confidentiality, integrity, and replay protection. Data confidentiality is achieved through symmetric key cryptography techniques based on Advanced Encryption Standard in Counter with CBC-MAC (AES-CCM) algorithm, message integrity through Message Authentication Code (MAC), and replay protection through monotonically increasing sequence numbers [62], [101], [102]. IEEE 802.15.4 MAC layer defines eight different security levels, which can be chosen as per the security requirements of the application. Oliveira *et al.* [103] proposed a network access control (NAC) security framework for 6LoWPAN networks. The proposed framework aims to control the access of nodes to the existing network using prior administrative authorization, and later applies security compliance on the authorized nodes for security management. The security mechanism of the framework is capable of defending the network from unknown attacks. The major limitations of the NAC security framework include the requirement of Lightweight Secure Neighbor Discovery for LLNs, secure reprogramming mechanism, and message authentication mechanism for implementing the proposed framework in a real network. The resource constrained nature of LLN nodes may limit some of these requirements. Moreover, the proposed framework is not implemented and analyzed for validation. Further, the authors extended their previous work [103] and proposed a network admission control solution in [104], [105]. The proposed solution has three main tasks, i.e., node detection and authentication, node authorization, and data filtering. The main limitations of the proposed solution include: (1) inherits attacks from neighbor discovery and RPL protocols; (2) it uses symmetric encryption, which increases resource consumption of nodes. The authors suggested using data filtering on RPL control messages, and elliptic curve mechanisms for minimizing resource consumption of nodes.

VII. Open issues, research challenges and future directions

In this section, we have discussed some open issues and research challenges that need to be studied and addressed.

Security Against Newly Developed Routing Attacks: One of the most concerning issues in IoT security is defense against newly developed attacks. DIO suppression [62], Routing choice intrusion [50], and ETX manipulation [63] are three such attacks which target the RPL network by degrading networks performance silently. Many other attacks specific to RPL are yet to be found and will require robust defense mechanisms. Very few efforts towards the development of defense mechanisms against such attacks have been carried out. Hence, several defense techniques for defending against newly discovered attacks need to be proposed.

Scalability: Most of the existing defense solutions have been tested on small network scenarios, but in the practical world, IoT is enabled by a large network of heterogeneous resource constrained nodes [50], [53], [87], [93]. The performance of existing solutions may degrade in the case of large network which puts IoT applications open to attackers. In addition to it, most of the critical IoT applications require a minimum delay in information forwarding, hence the demand of fast-reacting and lightweight defense solutions is increasing in order to carry out seamless network operations. These solutions must not degrade the QoS of the network while supporting high scalability. Hence, research can be carried out towards the development of highly scalable lightweight defense solutions.

Mobility: Lamaazi *et al.* [106] showed that the performance of RPL is severely influenced by mobile nodes. The standard specification of RPL [3] does not define any mechanism to support mobility. Thus, the overall network performance is degraded in the presence of mobile nodes. Some types of IoT nodes have dynamic characteristics (mobility), which lead to an increase in the number of link disconnections, collisions, and packet loss. When these mobile nodes perform malicious activities, the network performance drastically degrades. This leads to a rise in the number of problems that need to be addressed for securing RPL networks. In [107]–[109] impact of the Version number and Sybil attack, respectively under mobility is analyzed. However, the impact of other attacks on RPL under mobility needs to be studied. Most of the existing secure protocol and IDS based defense solutions for RPL consider the only static environment and may not be applicable for the mobile environment.

Cryptography Challenges: The key management is one of the significant challenges for resource constrained networks, which requires attention. Several defense solutions [53], [54], [67], [92], [93] use cryptography techniques like Hash Chain Authentication, Merkle Tree Authentication, and Dynamic Keying impose computational, memory, and energy overhead on resource constrained devices. These overheads affect node lifetime, which is an essential criterion for critical IoT applications, e.g., industrial, forest, and landslide monitoring. The development of lightweight cryptography based security solutions for RPL that are suitable for resource constrained devices is still a big challenge and needs to be addressed.

Resource Limitations for Machine Learning: Utilization of ML for the development of RPL specific security solutions is still a big task because of resource constraints. ML is proven to be effective in securing various wireless and wired networks with abundant resources. Thus, the customization of ML algorithms needs to be done in order to be used in resource constrained IoT. The efforts to address this challenge will lead to the development of lightweight signature and anomaly based IDS solutions which may be very useful in providing quick detection and facilitation of fast mitigation procedures.

Issues with Trust Based Secure RPL Protocols: Defense solutions proposed in [70], [73] require every node in the network to operate in a promiscuous mode, in order to overhear neighbor packet transmissions. Such requirements make these solutions unsuitable for resource constrained IoT nodes. Thus, improvements in existing trust based solutions without relying on such strict requirements must be carried out.

Hardware Security: Node tampering is one of the widely used methods for compromising a node and reprogramming it to perform malicious activities [49] in the network. All the insider attacks are performed by compromising a legitimate node, which is already a part of the IoT network. An attacker can reprogram a node with malicious functions like decreasing rank and increasing rank. In addition, a node can be reprogrammed in such a way that it skips checking rank function. Moreover, node tampering may lead to shared secret keys getting exposed. Thus, the development of tamper-proof node design is an open research area. It may also affect many factors involved in IoT security, and most importantly in the prevention from insider attacks. Some authors have suggested using TPM [68], [72] for securing IoT devices against insider attacks. However, TPM adds an extra cost to IoT networks and maybe infeasible for some IoT applications.

Network Security Monitoring over Encrypted Traffic: The rapid growth in encrypted traffic is creating challenges for security monitoring and intrusion detection. Encryption is being used by digital business organizations as a primary tool for securing information. Encryption not only brings security to businesses, but it also benefits the attacker to evade detection [110]. IoT specific IDS solutions present in the literature are developed based on the assumption of non-encrypted traffic. However, in the present scenario, IoT applications are using encryption due to the availability of resource-rich hardware. Hence this issue needs to be considered while developing IDS for current IoT applications. Encrypted Traffic Analytics (ETA) is one of the possible solutions that can be studied to address this issue.

A. Potential Areas for Future Research

In addition to previously discussed issues and challenges, we list potential research areas for upcoming researchers in this field.

Moving target IPv6 defense: By continually changing the IPv6 address of a device, the attacks including eavesdropping, denial-of-service, or man-in-the-middle attack can be defended. Moving target IPv6 defense mechanisms provide such capability to devices. Lightweight moving target based defense mechanisms for securing resource constrained devices against targeted attacks can be explored in-depth. Also, research on achieving resilience using temporary-private IPv6 addresses [111] can be carried out.

Collaborative IDS: These types of IDS leverage collaboration among sensor nodes and 6BR for efficient and quick detection of attackers. Very few research works present in the literature that focuses on the development of collaborative IDS and can be explored further.

Defense against coordinated attacks: In the present scenario, the attackers are now targeting IoT networks using coordinated attack strategy. These attacks severely degrade the network's performance without being detected. Popular IDS like SVELTE [80] are vulnerable to coordinated attacks. Thus, an efficient attack detection and mitigation solution to defend RPL against coordinated routing attacks needs to be developed.

Active Learning: Data insufficiency is of the significant problems for ML-based IDS. This problem can be solved by active learning, which optimizes the model learning during the training phase. This research area has recently gained the attention of security researchers. This needs a more in-depth study for leveraging its use in the development of IoT based IDSs.

Encrypted Traffic Analytics: ETA utilizes network traffic information that is independent of protocol details, e.g., lengths and arrival times of flows. These details can be used irrespective of encrypted and encrypted traffic for security monitoring of networks. ETA is an emerging topic in the field of network security and can be applied to IoT security as well.

Key management: Most of the IoT applications involve unattended device operation in an untrusted environment, where nodes may quickly become the target of attackers. In the secure mode of RPL, the nodes are pre-loaded with security keys, which can be considered as a significant security vulnerability due to a single point of failure. The development of scalable and efficient key management mechanisms like generation, management, and storage are the growing research areas in RPL security. The exiting WSN based key management solutions present in the literature can be improved and applied in RPL.

Energy efficient cryptography: Traditional cryptography algorithms are capable of achieving a higher level of security. However, these algorithms are computation-intensive. Hence, they consume many resources. Such algorithms cannot be directly used in IoT applications because energy resources are limited. Thus, the development of energy-efficient cryptography algorithms to achieve the required level of security with minimum energy consumption is an essential concern for IoT security in the present scenario.

Security of IPv6 over the TSCH mode of IEEE 802.15.4e (6TiSCH) networks: Recently, 6TiSCH protocol [112] has been standardized to attain low-power, scalable, and highly reliable operations in industrial applications. 6TiSCH uses time-slotted channel hopping (TSCH) MAC with IPv6 addressing to achieve industrial-grade performance. It is integrated with 6LoWPAN, RPL, and CoAP protocols. One of the important considerations of 6TiSCH is the requirement of node-to-node synchronization to prevent synchronization loops in the network. The attacks particular to RPL may disrupt node-to-node synchronization, which decreases throughput and increases communication latency. The research on the security of RPL and 6TiSCH combination is still in its early stage and is a potential research area for security researchers.

Addressing RPL specific flooding attacks: There is no efficient and suitable solution specially designed for defending flooding attack against RPL protocol [30]. To defend the DIS attack, RPL parameters can be used for setting safety thresholds in the RPL protocol. For example, DIS interval can be used to block the neighbors who are sending DIS messages very frequently, i.e., DIS messages are received before the expiry of DIS interval. Outlier Detection (OD) methods can be used to detect the neighbors (attacker) with abnormal behavior. DIS and DIO flooding attacks can be detected using OD based IDS. The main advantage of using OD is that these methods impose significantly less overhead on resource constrained nodes.

Security solutions for dynamic networks: To provide RPL with the ability to work efficiently in a dynamic network (i.e., mobility scenario), many enhancements have been proposed in the literature. Several RPL mobility enhancements are EMA-RPL, MoMoRo , mRPL, Co-RPL, and ME-RPL. Most of the existing RPL security solutions like SVELTE, SecRPL, SecTrust-RPL, and SRPL assume static network topology and may not be suitable for dynamic scenarios. However, at present, there are many use-cases in which RPL is deployed in dynamic networks. Thus, the existing solutions must be improved to make them suitable for dynamic networks. Also, this requirement must be fulfilled by the defense solutions which may be developed in the future.

Fog computing for RPL security: Resource constrained nature of LLNs limits the usage of existing state-of-the-art security mechanisms. However, in the present scenario, this limitation may be handled by currently emerging computing paradigms. One such emerging computing paradigm is Fog computing, which can be leveraged for securing IoT applications. To develop security solutions based on the combination of Edge, Fog Computing, RPL, and 6LoWPAN is a potential research area. The resource constrained nature of LLN nodes must also be taken care of beforehand as they demand low complexity authentication, and low message overhead based security solutions.

VIII. Conclusion

Self-organization, self-healing, global connectivity, resource constrained, and open nature characteristics of IoT make it the best choice for the development of applications that make human life easier. However, these characteristics also expose IoT to attackers targeting users' security and privacy. The network layer is one of the most favorite targets of attackers in the case of wireless networks, and because most of the IoT devices communicate using wireless medium IoT is more prone to attackers. To support efficient routing in LLNs, the RPL protocol has been standardized. RPL protocol is vulnerable to different attacks, which include attacks inherited from WSN and attacks specific to RPL. In this paper, we presented an exhaustive study on various attacks and defense solutions, in particular to the RPL protocol. First, we discussed a taxonomy of attacks on RPL in which attacks are classified based on their primary targets, including resources, topology, and traffic. Then, a taxonomy of different RPL specific defense solutions present in the literature is proposed. Various research challenges, open issues, and future research directions observed from the literature survey are also discussed. We observed that the research related to defense solutions specific to secure RPL protocol and RPL specific IDS methods is still in the early phase and requires more attention for providing full-fledged security to IoT applications.

Acknowledgment

This research was supported by the Ministry of Human Resource Development, Government of India.

References

[1] K. Ashton, "That 'Internet of things' Thing," *RFID journal*, vol. 22, no. 7, pp. 97–114, 2009.

[2] A. Čolaković and M. Hadžialić, "Internet of things (iot): A review of enabling technologies, challenges, and open research issues," *Computer Networks*, vol. 144, pp. 17 – 39, 2018.

[3] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J.-P. Vasseur, and R. Alexander, "RPL: IPv6 routing protocol for low-power and lossy networks," Tech. Rep., 2012.

[4] A. Musaddiq, Y. B. Zikria, O. Hahm, H. Yu, A. K. Bashir, and S. W. Kim, "A Survey on Resource Management in IoT Operating Systems," *IEEE Access*, vol. 6, pp. 8459–8482, 2018.

[5] J. Tripathi, *On Design, Evaluation and Enhancement of IP-Based Routing Solutions for Low Power and Lossy Networks*. Drexel University, 2014, PhD dissertation.

[6] I. E. Radoi, "Performance Evaluation of Routing Protocols in Lossy Links for Smart Building Networks," Master's thesis, School of Informatics University of Edinburgh, Edinburgh, 2011.

[7] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2347–2376, Fourthquarter 2015.

[8] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia, and M. Dohler, "Standardized Protocol Stack for the Internet of (Important) Things," *IEEE Communications Surveys Tutorials*, vol. 15, no. 3, pp. 1389–1406, 2013.

[9] J. Postel, "User datagram protocol," Tech. Rep., 1980.

[10] O. Iova, P. Picco, T. Istomin, and C. Kiraly, "RPL: The Routing Standard for the Internet of Things... Or Is It?" *IEEE Communications Magazine*, vol. 54, no. 12, pp. 16–22, December 2016.

[11] O. Gaddour and A. Koubaa, "RPL in a nutshell: A survey," *Computer Networks*, vol. 56, no. 14, pp. 3163 – 3178, 2012.

[12] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," *IEEE Communications Surveys Tutorials*, vol. 17, no. 3, pp. 1294–1312, thirdquarter 2015.

[13] I. Tomić and J. A. McCann, "A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1910–1923, Dec 2017.

[14] A. Oliveira and T. Vazão, "Low-power and lossy networks under mobility: A survey," *Computer Networks*, vol. 107, pp. 339 – 352, 2016.

[15] B. Ghaleb, A. Y. Al-Dubai, E. Ekonomou, A. Alsarhan, Y. Nasser, L. M. Mackenzie, and A. Boukerche, "A Survey of Limitations and Enhancements of the IPv6 Routing Protocol for Low-power and Lossy Networks: A Focus on Core Operations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1607–1635, 2018.

[16] H. Kharrufa, H. A. Al-Kashoash, and A. H. Kemp, "RPL-based routing protocols in IoT applications: A Review," *IEEE Sensors Journal*, vol. 19, no. 15, pp. 5952–5967, 2019.

[17] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the internet of things," *Digital Communications and Networks*, vol. 4, no. 2, pp. 118 – 137, 2018.

[18] D. M. Mendez, I. Papapanagiotou, and B. Yang, "Internet of things: Survey on security and privacy," *arXiv preprint arXiv:1707.01879*, 2017.

[19] K. Grgić, V. Križanović Čik, and V. Mandrić Radivojević, "Security Aspects of IPv6-based Wireless Sensor Networks," *International journal of electrical and computer engineering systems*, vol. 7, no. 1., pp. 29–37, 2016.

[20] A. El Hajjar, G. Roussos, and M. Paterson, "On the performance of key pre-distribution for RPL-based IoT Networks," in *Interoperability, Safety and Security in IoT*. Springer, 2016, pp. 67–78.

[21] P. Ilia, G. Oikonomou, and T. Tryfonas, "Cryptographic key exchange in IPv6-based low power, lossy networks," in *IFIP International Workshop on Information Security Theory and Practices*. Springer, 2013, pp. 34–49.

[22] W. Bechkit, Y. Challal, A. Bouabdallah, and V. Tarokh, "A highly scalable key pre-distribution scheme for wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 2, pp. 948–959, 2013.

[23] T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano, and M. Richardson, "A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)," Tech. Rep., 2015.

[24] M. Abomhara and G. M. Køien, "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks," *Journal of Cyber Security*, vol. 4, no. 1, pp. 65–88.

[25] N. Kulkarni, S. S. Chikkaraddi, and N. Sushmitha, "Survey on the Various Security Issues Associated with the Internet of Things," *Wireless Communication*, vol. 10, no. 5, pp. 99–103, 2018.

[26] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici, and M. Ochoa, "Insight into Insiders: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures," *CoRR*, vol. abs/1805.01612, 2018.

[27] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," *Journal of Network and Computer Applications*, vol. 66, pp. 198–213, 2016.

[28] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.

[29] L. Wallgren, S. Raza, and T. Voigt, "Routing Attacks and Countermeasures in the RPL-based Internet of Things," *International Journal of Distributed Sensor Networks*, vol. 9, no. 8, p. 794326, 2013.

[30] A. Mayzaud, R. Badonnel, I. Chrisment, and I. Grand Est -Nancy, "A Taxonomy of Attacks in RPL-based Internet of Things," *International Journal of Network Security*, vol. 18, no. 3, pp. 459–473, 2016.

[31] P. Pongle and G. Chavan, "Real Time Intrusion and Wormhole Attack Detection in Internet of Things," *International Journal of Computer Applications*, vol. 121, no. 9, pp. 1–9, 2015.

[32] P. Sethi and S. R. Sarangi, "Internet of things: architectures, protocols, and applications," *Journal of Electrical and Computer Engineering*, vol. 2017, pp. 1–27, January 2017.

[33] M. R. Abdmeziem, D. Tandjaoui, and I. Romdhani, *Architecting the Internet of Things: State of the Art*. Cham: Springer International Publishing, 2016, pp. 55–75.

[34] L. D. Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, Nov 2014.

[35] D. Miorandi, S. Sicari, F. D. Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497 – 1516, 2012.

[36] A. V. Dastjerdi and R. Buyya, "Fog computing: Helping the internet of things realize its potential," *Computer*, vol. 49, no. 8, pp. 112–116, 2016.

[37] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar, "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19 293–19 304, 2017.

[38] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in *International conference on wireless algorithms, systems, and applications*. Springer, 2015, pp. 685–695.

[39] S. Prabavathy, K. Sundarakantham, and S. M. Shalinie, "Design of cognitive fog computing for intrusion detection in Internet of Things," *Journal of Communications and Networks*, vol. 20, no. 3, pp. 291–298, 2018.

[40] H. Lamaazi and N. Benamar, "A comprehensive survey on enhancements and limitations of the RPL protocol: A focus on the objective function," *Ad Hoc Networks*, vol. 96, p. 102001, 2020.

[41] O. Gnawali and P. Levis, "The etx objective function for rpl," draft-gnawali-roll-etxof-01," 2010.

[42] ——, "The minimum rank with hysteresis objective function," Tech. Rep., 2012.

[43] P. Thubert, "Objective function zero for the routing protocol for low-power and lossy networks (RPL)," Tech. Rep., 2012.

[44] H. Lamaazi and N. Benamar, "OF-EC: A novel energy consumption aware objective function for RPL based on fuzzy logic." *Journal of Network and Computer Applications*, vol. 117, pp. 42–58, 2018.

[45] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko, "The trickle algorithm," Tech. Rep., 2011.

[46] P. Perazzo, C. Vallati, A. Arena, G. Anastasi, and G. Dini, "An implementation and evaluation of the security features of rpl," in *International Conference on Ad-Hoc Networks and Wireless*. Springer, 2017, pp. 63–76.

[47] 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.

[48] W. Xie, M. Goyal, H. Hosseini, J. Martocci, Y. Bashir, E. Baccelli, and A. Durresi, "Routing loops in dag-based low power and lossy networks," in *24th IEEE International Conference on Advanced Information Networking and Applications (AINA)*. IEEE, 2010, pp. 888–895.

[49] A. Le, J. Loo, Y. Luo, and A. Lasebae, "The impacts of internal threats towards Routing Protocol for Low power and lossy network performance," in *IEEE Symposium on Computers and Communications (ISCC)*, July 2013, pp. 789–794.

[50] L. Zhang, G. Feng, and S. Qin, "Intrusion detection system for RPL from routing choice intrusion," in *2015 IEEE International Conference on Communication Workshop (ICCW)*. IEEE, June 2015, pp. 2652–2658.

[51] A. Verma and V. Ranga, "Mitigation of DIS flooding attacks in RPL-based 6LoWPAN networks," *Transactions on Emerging Telecommunications Technologies*, p. e3802, Early Access.

[52] A. Verma and V. Ranga, "Addressing Flooding Attacks in IPv6-based Low Power and Lossy Networks," in *TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON)*, Oct 2019, pp. 552–557.

[53] A. Dvir, T. Holczer, and L. Buttyan, "VeRA - Version number and rank authentication in RPL," in *Proceedings of 8th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS)*. IEEE, oct 2011, pp. 709–714.

[54] M. Landsmann, M. Wahlisch, and T. C. Schmidt, "Topology authentication in RPL," in *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2013, pp. 73–74.

[55] A. Mayzaud, R. Badonnel, and I. Chrisment, "Detecting version number attacks in RPL-based networks using a distributed monitoring architecture," in *Proceedings of 12th IEEE/IFIP/In Assoc. with ACM SIGCOMM International Conference on Network and Service Management (CNSM 2016)*. IEEE, 2016, pp. 127–135.

[56] A. Le, J. Loo, A. Lasebae, M. Aiash, and Y. Luo, "6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach," *International Journal of Communication Systems*, vol. 25, no. 9, pp. 1189–1212, 2012.

[57] A. Le, J. Loo, Y. Luo, and A. Lasebae, "Specification-based IDS for securing RPL from topology attacks," *IFIP Wireless Days*, vol. 1, no. 1, pp. 4–6, 2011.

[58] A. Le, J. Loo, K. Chai, and M. Aiash, "A specification-based IDS for detecting attacks on RPL-based network topology," *Information*, vol. 7, no. 2, p. 25, 2016.

[59] J. Hui and J. Vasseur, "The routing protocol for low-power and lossy networks (rpl) option for carrying rpl information in data-plane datagrams," Tech. Rep., 2012.

[60] A. Sehgal, A. Mayzaud, R. Badonnel, I. Chrisment, and J. Schönwälder, "Addressing DODAG inconsistency attacks in RPL networks," in *Global Information Infrastructure and Networking Symposium, GIIS*. IEEE, sep 2014, pp. 1–8.

[61] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, "Mitigation of topological inconsistency attacks in RPL-based low-power lossy networks," *International Journal of Network Management*, vol. 25, no. 5, pp. 320–339, sep 2015.

[62] P. Perazzo, C. Vallati, G. Anastasi, and G. Dini, "DIO Suppression Attack Against Routing in the Internet of Things," *IEEE Communications Letters*, vol. 21, no. 11, pp. 2524–2527, Nov 2017.

[63] D. Shreenivas, S. Raza, and T. Voigt, "Intrusion Detection in the RPL-connected 6LoWPAN Networks," in *Proceedings of the 3rd International Workshop on IoT Privacy, Trust, and Security - IoTPTS '17*. ACM, 2017, pp. 31–38.

[64] S. Deshmukh-Bhosale and S. S. Sonavane, "A Real-Time Intrusion Detection System for Wormhole Attack in the RPL based Internet of Things," *Procedia Manufacturing*, vol. 32, pp. 840–847, 2019.

[65] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, 2003*. IEEE, 2003, pp. 113–127.

[66] B. Bhushan and G. Sahoo, "Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks," *Wireless Personal Communications*, vol. 98, no. 2, pp. 2037–2077, 2018.

[67] G. Glissa, A. Rachedi, and A. Meddeb, "A Secure Routing Protocol Based on RPL for Internet of Things," in *2016 IEEE Global Communications Conference (GLOBECOM)*, Dec 2016, pp. 1–7.

[68] S. Seeber, A. Sehgal, B. Stelte, G. D. Rodosek, and J. Schonwalder, "Towards a trust computing architecture for RPL in Cyber Physical Systems," in *Proceedings of 9th International Conference on Network and Service Management (CNSM)*. IEEE, 2013, pp. 134–137.

[69] K. Iuchi, T. Matsunaga, K. Toyoda, and I. Sasase, "Secure parent node selection scheme in route construction to exclude attacking nodes from RPL network," in *Proceedings of 21st Asia-Pacific Conference on Communications (APCC)*. IEEE, 2015, pp. 299–303.

[70] D. Airehrour, J. A. Gutierrez, and S. K. Ray, "A Trust-Aware RPL Routing Protocol to Detect Blackhole and Selective Forwarding Attacks," *Australian Journal of Telecommunications and the Digital Economy*, vol. 5, no. 1, pp. 50–69, 2017.

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

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

[73] 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.

[74] F. Nygaard, "Intrusion Detection System In IoT," Master's thesis, NTNU, 2017.

[75] B. Ghaleb, A. Al-Dubai, E. Ekonomou, M. Qasem, I. Romdhani, and L. Mackenzie, "Addressing the DAO Insider Attack in RPL's Internet of Things Networks," *IEEE Communications Letters*, vol. 23, no. 1, pp. 68–71, Jan 2019.

[76] M. N. Napiah, M. Y. I. B. Idris, R. Ramli, and I. Ahmedy, "Compression header analyzer intrusion detection system (CHA-IDS) for 6LoWPAN communication protocol," *IEEE Access*, vol. 6, pp. 16 623–16 638, 2018.

[77] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, and M. A. Spirito, "DEMO: An IDS framework for internet of things empowered by 6LoWPAN," in *Proceedings of the ACM SIGSAC conference on Computer & communications security*, ser. CCS '13. New York, NY, USA: ACM, 2013, pp. 1337–1340.

[78] P. Ioulianou, V. Vasilakis, I. Moscholios, and M. Logothetis, "A Signature-based Intrusion Detection System for the Internet of Things," in *Information and Communication Technology Form*, June 2018, In press.

[79] E. Kfoury, J. Saab, P. Younes, and R. Achkar, "A Self Organizing Map Intrusion Detection System for RPL Protocol Attacks," *International Journal of Interdisciplinary Telecommunications and Networking (IJITN)*, vol. 11, no. 1, pp. 30–43, 2019.

[80] S. Raza, L. Wallgren, and T. Voigt, "Svelte: Real-time intrusion detection in the internet of things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661 – 2674, 2013.

[81] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, "Using the RPL protocol for supporting passive monitoring in the Internet of Things," *Proceedings of the NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, pp. 366–374, 2016.

[82] A. Mayzaud, R. Badonnel, and I. Chrisment, "A distributed monitoring strategy for detecting version number attacks in RPL-based networks," *IEEE Transactions on Network and Service Management*, vol. 14, no. 2, pp. 472–486, June 2017.

[83] F. Gara, L. B. Saad, and R. B. Ayed, "An intrusion detection system for selective forwarding attack in IPv6-based mobile WSNs," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2017 13th International*. IEEE, 2017, pp. 276–281.

[84] ——, "An Efficient Intrusion Detection System for Selective Forwarding and Clone Attackers in IPv6-based Wireless Sensor Networks under Mobility," *International Journal on Semantic Web and Information Systems (IJSWIS)*, vol. 13, no. 3, pp. 22–47, 2017.

[85] M. Surendar and A. Umamakeswari, "InDReS: An Intrusion Detection and response system for Internet of Things with 6LoWPAN," in *Proceedings of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. IEEE, 2016, pp. 1903–1908.

[86] U. Shafique, A. Khan, A. Rehman, F. Bashir, and M. Alam, "Detection of rank attack in routing protocol for Low Power and Lossy Networks," *Annals of Telecommunications*, vol. 73, no. 7-8, pp. 429–438, 2018.

[87] G.-H. Lai, "Detection of wormhole attacks on IPv6 mobility-based wireless sensor network," *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, no. 1, p. 274, 2016.

[88] S. O. Amin, M. S. Siddiqui, C. S. Hong, and S. Lee, "RIDES: Robust intrusion detection system for IP-based ubiquitous sensor networks," *Sensors*, vol. 9, no. 5, pp. 3447–3468, 2009.

[89] H. Bostani and M. Sheikhan, "Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach," *Computer Communications*, vol. 98, pp. 52–71, 2017.

[90] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *Journal of Network and Computer Applications*, vol. 84, pp. 25–37, apr 2017.

[91] H. Perrey, M. Landsmann, O. Ugus, T. C. Schmidt, and M. Wählisch, "TRAIL: Topology Authentication in RPL," *CoRR*, vol. abs/1312.0984, 2013.

[92] C. Taylor and T. Johnson, "Strong authentication countermeasures using dynamic keying for sinkhole and distance spoofing attacks in smart grid networks," in *2015 IEEE Wireless Communications and Networking Conference (WCNC)*, March 2015, pp. 1835–1840.

[93] F. Idris Khan, T. Shon, T. Lee, and K.-H. Kim, "Merkle tree-based wormhole attack avoidance mechanism in low power and lossy network based networks," *Security and Communication Networks*, vol. 7, no. 8, pp. 1292–1309, 2014.

[94] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-Service detection in 6LoWPAN based Internet of Things," in *Proceedings of 2013 IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob)*. IEEE, 2013, pp. 600–607.

[95] P. Shukla, "ML-IDS: A machine learning approach to detect wormhole attacks in Internet of Things," in *Intelligent Systems Conference (IntelliSys)*. IEEE, 2017, pp. 234–240.

[96] A. Verma and V. Ranga, "Evaluation of Network Intrusion Detection Systems for RPL Based 6LoWPAN Networks in IoT," *Wireless Personal Communications*, vol. 108, no. 3, pp. 1571–1594, 2019.

[97] ——, "ELNIDS: Ensemble Learning based Network Intrusion Detection System for RPL based Internet of Things," in *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*. IEEE, 2019, pp. 1–6.

[98] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things," *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015*, pp. 606–611, 2015.

[99] C.-M. Chen, S.-C. Hsu, and G.-H. Lai, "Defense denial-of service attacks on IPv6 wireless sensor networks," in *Genetic and Evolutionary Computing*. Springer, 2016, pp. 319–326.

[100] M. S. Ahsan, M. N. M. Bhutta, and M. Maqsood, "Wormhole attack detection in routing protocol for low power lossy networks," in *International Conference on Information and Communication Technologies (ICICT)*. IEEE, 2017, pp. 58–67.

[101] N. Sastry and D. Wagner, "Security considerations for IEEE 802.15. 4 networks," in *Proceedings of the 3rd ACM workshop on Wireless security*. ACM, 2004, pp. 32–42.

[102] Y. M. Amin and A. T. Abdel-Hamid, "A comprehensive taxonomy and analysis of IEEE 802.15. 4 attacks," *Journal of Electrical and Computer Engineering*, vol. 2016, p. 4, 2016.

[103] L. Oliveira, J. Rodrigues, A. de Sousa, and J. Lloret, "A network access control framework for 6LoWPAN networks," *Sensors*, vol. 13, no. 1, pp. 1210–1230, 2013.

[104] L. M. Oliveira, J. J. Rodrigues, C. Neto, and A. F. de Sousa, "Network admission control solution for 6LoWPAN networks," in *2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*. IEEE, 2013, pp. 472–477.

[105] L. M. L. Oliveira, J. J. Rodrigues, A. F. de Sousa, and V. M. Denisov, "Network admission control solution for 6LoWPAN networks based on symmetric key mechanisms," *IEEE transactions on industrial informatics*, vol. 12, no. 6, pp. 2186–2195, 2016.

[106] H. Lamaazi, N. Benamar, and A. J. Jara, "RPL-based networks in static and mobile environment: A performance assessment analysis," *Journal of King Saud University - Computer and Information Sciences*, pp. 1–14, 2016.

[107] A. Aris, S. F. Oktug, and S. B. O. Yalcin, "RPL version number attacks: In-depth study," in *Proceedings of the 2016 IEEE/IFIP Network Operations and Management Symposium (NOMS 2016)*. IEEE, 2016, pp. 776–779.

[108] F. Medjek, D. Tandjaoui, M. R. Abdmeziem, and N. Djedjig, "Analytical evaluation of the impacts of Sybil attacks against RPL under mobility," in *12th International Symposium on Programming and Systems (ISPS)*. IEEE, 2015, pp. 1–9.

[109] F. Medjek, D. Tandjaoui, I. Romdhani, and N. Djedjig, "Performance evaluation of RPL protocol under mobile sybil attacks," *IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 1049–1055, 2017.

[110] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, and N. Feamster, "Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic," *arXiv preprint arXiv:1708.05044*, 2017.

[111] M. Mavani and K. Asawa, "Resilient against spoofing in 6LoWPAN networks by temporary-private IPv6 addresses," *Peer-to-Peer Networking and Applications*, pp. 1–15, 2019.

[112] X. Vilajosana, T. Watteyne, T. Chang, M. Vučinić, S. Duquennoy, and P. Thubert, "IETF 6TiSCH: A Tutorial," *IEEE Communications Surveys & Tutorials*, 2019, In Early access.