Assessment of Routing Attacks and Mitigation Techniques with RPL Control Messages: A Survey

ANKUR O. BANG and UDAI PRATAP RAO*, Sardar Vallabhbhai National Institute of Technology (SVNIT), India
PALLAVI KALIYAR, Norwegian University of Science and Technology, Norway
MAURO CONTI, University of Padova, Italy

Routing Protocol for Low-Power and Lossy Networks (RPL) is a standard routing protocol for the Low Power and Lossy Networks (LLNs). It is a part of the IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) protocol stack. Features like energy-efficient mechanisms and availability of the secure modes of operations make RPL suitable for the constrained Internet of Things (IoT) devices. Hence, the majority of IoT applications rely on RPL for data communication. However, routing security in RPL-based IoT networks is a significant concern, motivating us to study and analyze routing attacks and suggested countermeasures against them. To this end, we provide a comprehensive survey on the state-of-the-art security threats and their corresponding countermeasures in RPL-based IoT networks. Based on our study, we propose a novel classification scheme that uses a mapping between RPL attacks and their countermeasure techniques to the RPL control messages used to develop these techniques. Furthermore, we provide an in-depth statistical analysis that includes analysis of routing attacks through the RPL control messages, distribution of various mitigation techniques as per the method used, RPL control messages involved in the mitigation techniques, and details of the tools used by multiple researchers. In the end, we highlight some open challenges and future research opportunities on this topic. We believe this survey will be beneficial to researcher and practitioners working in the area of RPL security.

CCS Concepts: • **Security and privacy** → **Mobile and wireless security**.

Additional Key Words and Phrases: RPL, Internet of Things, Routing Attacks, Routing Protocol, Control Messages, Classification, Mitigation Methods

ACM Reference Format:
Ankur O. Bang, Udai Pratap Rao, Pallavi Kaliyar, and Mauro Conti. 2021. Assessment of Routing Attacks and Mitigation Techniques with RPL Control Messages: A Survey. 1, 1 (October 2021), 35 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

One of the significant challenges for the Internet of Things (IoT) is to allow resource constrained devices to converge with the IP-based environment [1]. The use of Internet Protocol Version 6 (IPv6) over Low-Power Wireless Personal Area Network (6LoWPAN) protocol stack solved this problem.

*Corresponding Author

Authors' addresses: Ankur O. Bang, mr.ankurbang@gmail.com; Udai Pratap Rao, upr@coed.svnit.ac.in, Sardar Vallabhbhai National Institute of Technology (SVNIT), Ichchhanath, Keval Chowk, Surat, Gujarat, India, 395007; Pallavi Kaliyar, pallavi.kaliyar@gmail.com, Norwegian University of Science and Technology, N-2815, Gjøvik, Norway; Mauro Conti, mauro.conti@unipd.it, University of Padova, Via VIII Febbraio, 2, 35122, Padova PD, Italy.

XXXX-XXXX/2021/10-ART $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

The 6LoWPAN group has specified encapsulation and header compression mechanisms [1] for sending and receiving IPv6 packets over IEEE 802.15.4 networks. Routing Protocol for Low Power and Lossy Networks (RPL) is a part of the 6LoWPAN protocol stack and manages the routing task. Although RPL offers optional security mechanisms to protect its network privacy, credibility, and validity of control messages, attackers can still control the legitimate nodes because sensor nodes are not immune to manipulations. This makes it possible for attackers to hamper the routing process and mount different routing attacks. Hence, enhancing routing reliability of the RPL protocol has gained significant attention and has attracted many researchers from the Low Power and Lossy Networks (LLNs) community. However, while providing secure routing solutions to the RPL networks, the resource constraint nature of the IoT devices and working principles of the RPL protocol must be considered.

To the moment, very few studies focus upon the various routing attacks and their countermeasures with regards to the RPL protocol. The majority of these surveys shed little light on the thorough investigation of the RPL routing attacks. Besides this, the bulk of them lacks knowledge from the existing literature and are not fruitful for researchers working in this area. Further, most current work mainly focuses on internal threats to the Wireless Sensor Networks (WSNs) [2]. Hence, there is a significant need to investigate the security dimension of the RPL protocol to get a more profound knowledge about the threats and prevention strategies. The lack of a precise survey covering aspects like (i) The investigation of attacks possible through various RPL control messages, (ii) The involvement of the RPL control message in the proposed mitigation techniques, (iii) In-depth study and classification of the existing security methods constitutes a strong motivation for us to write this survey.

Our survey includes all the unique and relevant attempts to improve the routing security of the RPL protocol. Besides this, this paper's primary goal is to analyze all the routing attacks and respective mitigation methods concerning the RPL control messages. With providing highlights about the advantages and drawbacks of the studied mitigation techniques, our study also presents:

- The distribution of the mitigation techniques as per the method used,
- RPL control messages involved in the mitigation techniques,
- Details of the attack possible through each RPL control message, and
- Details of the tools used to implement (validate) the suggested methods by the various researchers.

Thus, this work will enable the readers to quickly understand the security issues of the RPL protocol with its control messages.

1.1 Related Surveys

Many previous studies have covered various security aspects of the RPL protocol. However, the contributions of these works to the research community are widely scattered and insufficient. This subsection provides a literature review with a short discussion of these works organized in chronological sequence.

L. Wallgren et al. [3] provide details about the RPL's basic functionalities and introduce the attacks related to it along with a discussion on their respective countermeasures. Along with this, they also propose a lightweight Intrusion Detection System (IDS) called *heartbeat* using the Internet Control Message Protocol for IPv6 (ICMPv6) messages. P. Pongle and G. Chavan [4] inspected the history of research efforts that improve the RPL protocol since its standardization (in 2012) until the year 2014. They also mention various threats related to the 6LoWPAN protocol stack. Further, this survey includes a brief overview of the IDSs and their classifications. However, this survey seems to be outdated and does not include the latest attack and mitigation techniques.

In [5], authors summarize the work done till 2015 and contribute mainly by giving the first-ever classification of the routing attacks based on Resource, Topology, and Traffic. They also mention the prerequisites and impact of each attack in their work. However, this study lacks a thorough discussion of the attacks and respective mitigation techniques. Another study [6], published in 2016, explains some aspects regarding the growth of the IoT market projected by the year 2020. The survey examines the efforts made for securing RPL for IoT. Authors in their study classify the routing attacks as attacks on Confidentiality, Integrity, and Availability (CIA). They also state the adverse effect of each attack on the network performance. Besides this, we came across other studies like [7], where the authors present a summary of various attacks and defense mechanisms and [8], which suggest possible solutions for some routing attacks not evaluated until the year 2017. However, all these studies made a minimal discussion about the RPL's security.

Kim et al. [9] review the history of various research efforts related to RPL. This study discusses RPL related papers until 2017, and it is, therefore, outdated. The authors provide a brief statistical overview of hardware platforms, publications, and simulations tools. However, this study does not discuss RPL routing attacks and related mitigation techniques in detail and does not provide research on RPL's security. A. Kamble et al. [10] stated and classified attacks targeting Resource, Topology, and Traffic. However, this work summarizes only a few studies and sheds little light on RPL's research challenges. A. Raoof et al. [11] made a very exhaustive study of various researchers' research efforts. Their work segregates defense methods as per the mitigation techniques used. Besides this, they also bifurcate attacks as WSN's inherited and RPL specific. Further, they discussed the open issues, challenges, and future directions regarding mitigating routing attacks on RPL. However, this study lacks information about various tools and RPL messages involved in the mitigation techniques. Some recent studies [12], [13] did a short survey and focused on privacy and combinations of different routing attacks against the RPL protocol. We, in our survey, mainly focus on the aspect of RPL control messages and discuss attacks and mitigation techniques possible through them. We extend previous studies to notify potential scope of improvement in the existing mitigation techniques, provide an in-depth analysis regarding the relation of RPL control messages and attacks, and discuss challenges and research opportunities to enhance RPL's security.

1.2 Our Survey

As mentioned above, a few surveys have been undertaken to analyze the numerous security concerns of the RPL protocol. To the best of our knowledge, there is no prior survey similar to ours. Interestingly, Table 1 shows how this work separates itself from the previously widely quoted articles. This survey provides a one-stop solution as an opportunity to understand and overcome the difficulties in the existing approaches proposed to enhance RPL's resilience against routing attacks. Thus, this paper encourages researchers to design new and efficient solutions against the RPL routing attacks. Our survey tries to extend previous studies by summarizing all the existing attacks and adding some new recent mitigation techniques suggested by researchers. Besides this, the survey provides a more profound vision of the RPL control messages and their relations with routing attacks and countermeasures. Compared to other existing surveys on the RPL routing attacks, this article is the first to evaluate RPL control messages with routing attacks and countermeasures. Understanding the attacks and countermeasures from the perspective of the control messages is particularly important. It will provide the root cause of the attack and insights into the possible changes that can be made in these control messages to prevent attacks in the future.

1.3 Major Contributions and Scope

Given the shortcomings of the other surveys listed in Table 1, our paper's main contributions can be summarized as follows.

Table 1. Comparison of this survey with other related surveys

Articles	Survey Subject	Year	Research Effort/ Year	Overview of 6LowPAN	RPL Basics	Classification on the basis of					Control Messages in Mitigation Techniques	Effect of Each Attack	Tools Used	Scope of Enhancements	Statistical Analysis	Research Opportunities
						A [1]	B [2]	C [3]	D [4]	E [5]						
Linus Wallgren et.al [3]	Secure routing in wireless sensor networks: Attacks and countermeasures	2013	2010-2013	● [a]	△ [b]	× [c]	×	×	×	×	×	△	×	×	×	×
Pavan Pongle et.al [4]	A survey: Attacks on RPL and 6lowpan in IoT	2015	2011-2014	△	△	×	×	×	×	×	×	△	×	×	×	△
Anthéa Mayzaud et.al [5]	A taxonomy of attacks in RPL-based Internet of Things	2016	2011-2015	×	△	✓ [d]	×	×	×	×	×	△	×	△	×	×
DavidAirehrour et.al [6]	Secure routing for Internet of Things: A survey	2016	2011-2015	✓	●	×	✓	×	×	×	×	●	×	●	×	✓
Divya Sharma et.al [7]	A detailed classification of routing attacks against RPL in Internet of Things	2017	2013-2015	△	△	✓	×	×	×	×	×	△	×	×	×	×
S. Mangelkar et.al [8]	A comparative study on RPL attacks and security solutions	2017	2012-2016	×	△	×	✓	×	×	×	×	△	×	×	×	×
Kim et al. [9]	Challenging the ipv6 routing protocol for low-power and lossy networks (rpl): A survey	2017	2012-2017	×	●	×	×	×	×	×	×	×	●	△	△	△
A. Kamble et.al [10]	Security attacks and secure routing protocols in RPL-based Internet of Things: Survey	2017	2012-2015	×	●	✓	×	×	×	×	×	×	×	×	×	×
A. Raoof et.al [11]	Routing attacks and mitigation methods for RPL-based Internet of Things	2018	2011-2018	×	●	×	×	✓	✓	×	×	×	×	●	×	●
A. Jain and S. Jain [12]	‘A survey on miscellaneous attacks and countermeasures for RPL routing protocol in IoT	2019	2011-2016	×	△	×	×	×	×	×	×	×	×	△	×	×
M. Durairaj et.al [13]	The Internet of Things (IoT) routing security—A study	2020	2011-2019	×	×	✓	×	×	×	×	×	×	×	×	×	×
This Survey	**Assessment of Routing Attacks and Mitigation Techniques with RPL Control Messages: A Survey**	**2021**	**2011-2020**	●	●	**×**	**×**	**×**	**✓**	**✓**	**✓**	**✓**	**✓**	**✓**	**✓**	**✓**

[1] Attacks on Resource, Topology and Traffic. [2] Attack on Confidentiality, Integrity and Availability. [3] RPL Specific and WSNs Inherited. [4] Mitigation Techniques. [5] RPL Control Messages. [a] Aspect is appropriately covered in the survey. [b] Aspect is shallowly covered in the survey. [c] Aspect is not covered in the survey. [d] Aspect is covered to the core in the survey.

- First, we present a comprehensive study of the RPL protocol, its identified attacks, and the suggested mitigation methods against each attack. Next, we provide a novel classification of the attacks and countermeasures possible by exploiting RPL's control messages. We also present a comprehensive overview of the various defense mechanisms along with their limitations.
- We provide first of its kind in-depth statistical analysis that includes analysis of routing attacks through each control messages, distribution of the mitigation techniques, control messages involved in mitigation techniques, and details of the tool used to implement attack/countermeasure by various researchers. We conclude our contributions by highlighting a set of research opportunities relevant to further security enhancement of the RPL protocol.

Our survey is written to target researchers actively involved and working in the security of RPL-based IoT networks. In our view, the contributions mentioned above will provide the targeted readers with an integrated survey to track existing research directions and the latest updates about RPL's security challenges and issues. In particular, we believe that the readers will understand and learn about the following from this article.

- For the novices, it will provide a thorough understanding of the working methodology of the RPL protocol and the role of the control messages while forming the network topology and performing the data communications. They will also gain adequate knowledge about the RPL's strengths and security issues. Our novel classification of the existing mitigation methods will enable researchers to study and move further in a particular method or invent new hybrid methods.
- Our work will provide a precise picture of the vulnerabilities related to the control messages in the RPL and attacks possible through them. Moreover, to help the researchers who are working to enhance RPL's security, our contribution of mapping attacks with the RPL control messages may open new research opportunities towards making architectural changes in the RPL protocol to enhance its security.

The rest of the article is organized as follows. Section 2 describes the overview of the 6LoWPAN protocol stack and the RPL operations. Section 3 presents a classification and description of the attacks possible through each RPL control message. In the same section, we present an in-depth discussion about the mitigation techniques suggested against each identified attack. Key findings from the literature and research opportunities are stated in Section 4. Section 5 elaborates on the identified issues, challenges, and future research opportunities. Finally, Section 6 concludes our work.

2 6LOWPAN PROTOCOL STACK AND RPL

This section contains all the necessary and prerequisite information regarding the 6LoWPAN protocol stack (please refer to section 2.1) and RPL protocol (please refer to section 2.2).

2.1 Overview of 6LoWPAN Protocol Stack

The 6LoWPAN protocol stack arose from the belief that the Internet protocol should be applicable to small devices and low-power machines with minimal computing capacities involved in IoT technology. Thus, the 6LoWPAN networks have characteristics [3], [14] like resource-constrained nodes with restricted energy, memory, and processing power, lossy links, and low data rates (approximately 250 kbps). Moreover, the bulk of the traffic in these networks is either point-to-multipoint (root node to child nodes) or multipoint-to-point (child nodes to root node).

The 6LoWPAN protocol stack [15], [16] is developed by the Internet Engineering Task Force (IETF). This protocol stack is based on IPv6 [17], with the addition of an adaptation layer called

6LoWPAN [17], that handles header compression, fragmentation, and reassembly of IPv6 packets along with other important tasks. Figure 1 shows a comparison between 6LoWPAN and traditional TCP/IP protocol stacks. As our article's scope is restricted to the RPL only, we direct the interested readers to refer [1], [18] to study the other protocols and standards used in the 6LoWPAN protocol stack.

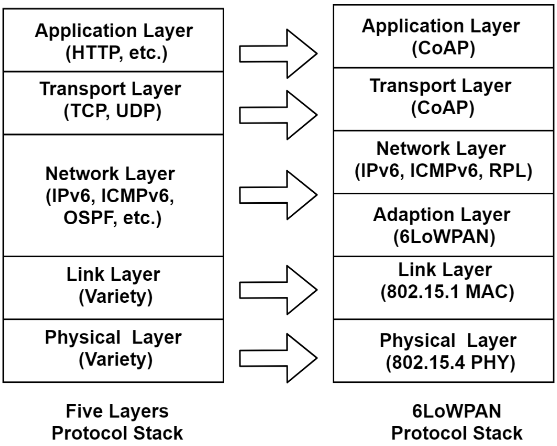
Application Layer (HTTP, etc.)
Transport Layer (TCP, UDP)
Network Layer (IPv6, ICMPv6, OSPF, etc.)
Link Layer (Variety)
Physical Layer (Variety)
Five Layers Protocol Stack
Application Layer (CoAP)
Transport Layer (CoAP)
Network Layer (IPv6, ICMPv6, RPL)
Adaption Layer (6LoWPAN)
Link Layer (802.15.1 MAC)
Physical Layer (802.15.4 PHY)
6LoWPAN Protocol Stack

Fig. 1. Five Layered Protocol and 6LoWPAN Stacks

2.2 Overview of RPL

The routing methods used for the WSNs are found unsuitable for IoT [15]. Besides this, the traditional Internet routing protocols are also of no use for resource-constrained IoT devices [1]. Therefore, from a variety of solutions that existed for routing in the 6LoWPAN networks, the IETF only implemented and standardized the RPL [1] protocol. RPL is designed from scratch to fulfill IoT network routing needs and to reduce resource consumption along the routing paths. Also, it is flexible and can be modified according to the various operating conditions. RPL forms a loop-free tree-like topology, called Destination Oriented Directed Acyclic Graph (DODAG) [19], in which nodes are arranged into a ranked structure, comprising of the root, the children, and the progenies. RPL uses an objective function to ensure the formation of the optimized topology [19]. Topology formation in RPL is based on a set of pre-defined goals, like conservation of energy, lower hop count, and the eminence of connection. A network may have several DODAGs, each having its pre-defined objective function. If required, RPL may run multiple network instances within a single IoT network by creating a separate set of DODAGs for each instance [19]. However, at any given time interval, a node can only be a part of a single DODAG instance [19].

2.2.1 Summary of RPL's Features.

- **RPL Control Messages:** RPL's DODAG is developed and managed using: (a) DODAG Information Solicitation (DIS), (b) DODAG Information Object (DIO), (c) Destination Advertisement Object (DAO), and (d) DAO-Acknowledgment control messages. A new node can enter a prevailing network by transmitting a DIS message to request the DIO messages that carry DODAG information like node ID, version number, and rank. Additionally, a node may wait to collect periodically transmitted DIO messages from its neighbors to maintain and update RPL topology. A timer called *Trickle* maintains the periodic and optimal transmission of the DIO messages [11].
- **Objective Function and Topology Formation:** A node uses its objective function [14] to calculate its rank on receiving a new DIO message. Node's rank value resembles its distance

from the root/sink node in the RPL topology.To guarantee the graph's acyclic nature, the node's rank value must always be higher than its parent node's rank value [1], [14]. When DIO messages from multiple nodes are received, the best-ranking parent (with the lowest rank) among the recipient nodes is selected. Thus, the DIO message plays a vital role in building and maintaining the RPL topology. Once the topology is created, the node sends the DAO message towards the root/sink node of the respective DODAG [14]. Figure 2 depicts the formation of DODAG and the flow of control messages with both existing and newly added nodes.

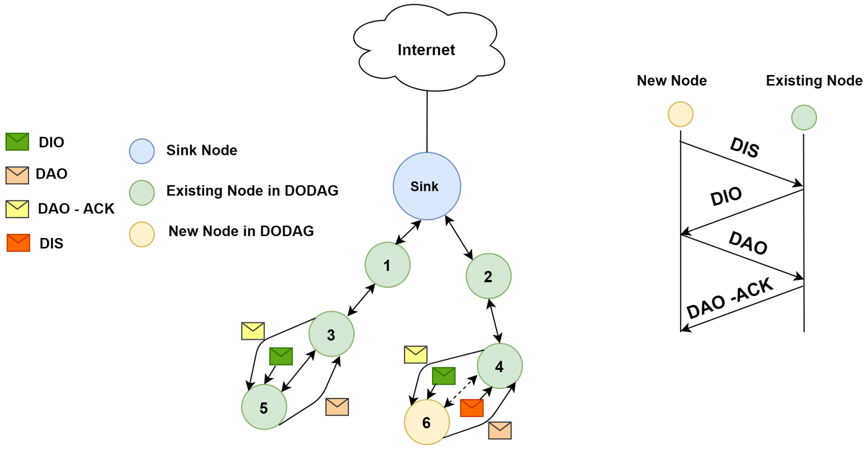

Fig. 2. RPL DODAG Formation

- **Avoidance and Detection of Loop:** Whenever the topology changes, the RPL can detect and repair such changes. RPL relies on two basic rules for preventing loops (i) Any message that travels down the DODAG but originates from an inherited node is ignored, and (ii) Downward movement of these messages is allowed only during the loop avoidance procedure or when the root/sink node initiates a new version of the DODAG [1], [14]. RPL has a mechanism for route validation whenever a loop is detected, and it corrects the inconsistencies associated with the DODAG formation [1], [14].
- **Mode of Operation:** In RPL, there can be multiple DODAGs in a network [14]. Any node can join one or more instances and perform a completely different role in each DODAG [14]. RPL supports Point to Point (P2P), Multipoint to Point (MP2P), Point to Multipoint (P2MP) communications [14]. RPL operates in two modes. Storing, where node keeps downward routing table stored locally and network use this table for traffic management. Non-storing, where node uses source routing to send traffic to the destination nodes [1], [14].
- **Security Features:** RPL provides three types of security modes [14].
  (i) Unsecured Mode: This is RPL's default security mode of operation, which provides no security, here RPL relies on the link layer for security, and RPL control messages are unsecured.
  (ii) Preinstalled Mode: Here symmetric key is preinstalled on the node. RPL control messages are secured with the key. When additional routing security is required, this mode can be used.
  (iii) Authenticated Mode: The authentication authority is responsible for providing a key. To get this key, a newly joined node has to use the preinstalled key to enter DODAG. When authentication of the node is required, this mode is used.

Further, RPL has many other features [14] like *Self-configuration* through which RPL uses IPv6, where IPv6 provides the functionality of neighbor discovery for the construction of routes in the network from source to destination. *Auto healing* feature is useful when nodes are added or removed in RPL topology due to mobility or failure of a node. *Multiple edge routers* that support high availability and load balancing in RPL.

3 CLASSIFICATION OF RPL ROUTING ATTACKS AND RELATED MITIGATION TECHNIQUES

After carefully studying each routing attack, we adopt the following classification.

- **Attack Classification Based on Control Messages:** Some of the previous studies have adopted different classifications. This survey focuses on the routing attacks that originated due to the RPL's structure and working principle. Control messages are the fundamental and core part of the RPL working [14], [1]. Therefore, this survey relates each known attack with the four RPL control messages discussed in the previous section. Figure 3 depicts more about this novel classification. Further, every attack on RPL is clarified, and the known mechanisms are summarized one by one. In addition to it, RPL packets involved in the suggested mitigation techniques are extensively discussed in the later part of the survey.
- **Mitigation Classification Based on Defense Methods:** We classify the studied mitigation mechanisms based on various defense methods used as - specification-based (which use RPL specifications like change in rank, DODAG, and version number to detect the attacker node), trust-based (where the legitimate nodes maintain trust values among themselves and make use of it to detect the attacker node), statistical/mathematical (cryptographic) based, location-based, and acknowledgment-based [11]. This classification has helped us to understand similar problems with each class of the classified methods. We further used this data and tried to extract notably useful information from that and precisely analyze it in Section 4.

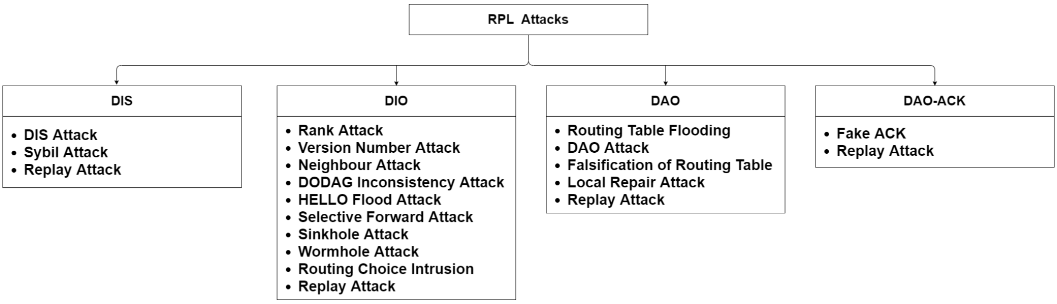

Fig. 3. Classification of RPL Attacks Based on its Control Messages

Each classified attack and the respective mitigating techniques are studied and discussed in the remaining part of this section. In addition, a tabular format describing all the mitigation techniques along with the attack's impact, classification based on mitigation techniques, involved control messages, respective tools used, and scope of development of each technique is provided.

3.1 DIS Specific Attacks and Mitigation Techniques

This subsection provides a brief overview of the respective countermeasures against the potential routing attacks possible through the DIS control message.

Table 2. Summary of Attacks through DIS Control Message and Mitigation Techniques

Mitigation Techniques	Publication Year	Attacks	Attack Impact	Classification Based on Mitigation Technique	Modified / Default Control Messages	Tools Used	Summary of Limitations / Scope of Enhancement
[22]	2013	DIS Attack	Increased Delay	Specification Based	DIO and DAO	Cooja	Accuracy is an Issue
[21]	2016				DIS	Cooja	Method Depends on Cluster Head
[24]	2019				DIS	Cooja	Lossy Nature of RPL is not Taken into Consideration
[23]	2020				DIS	Cooja	Lossy Nature of RPL is Not Taken into Consideration, Depends on Time Stamp
[26]	2017	Sybil Attack	Decreased Packet Delivery Ratio (PDR), Increased Network Overhead and Energy Consumption	Trust Based	DIO *	Cooja	Needs Collaboration with Neighbors to Detect Intrusions
[28]	2019				DIO*	Cooja and Testbed	Trust Calculation Takes Time, Method Depends On Sink Node
[27]	2019				DIO*	Cooja	Trust Calculation is Crucial
[29]	2019				DIO*	Cooja	Trust Calculation is Crucial
[32]	2018			Statistical / Mathematical (Cryptographic) Based	DAO*	Cooja	Taking Hash of Each Node and Checking it at Root Node Creates Overhead
[30]	2019				DIS and DIO	OMNeT++	Includes Heavy Mathematical Calculation, Not Suitable for Larger Networks
[31]	2020				DIS and DIO	OMNeT++	Gini Base Filtering Requires Initial Calculation
[19]	2012	Replay Attack	Increased Delay, Power Consumption and Network Overhead	Acknowledgement Based	DAO	Not Mentioned	Not Suitable for Dynamic Networks

* Denotes Modified Control Message

3.1.1 DIS (DIS Flooding) Attack and Mitigation Techniques. The older design and implementation of the RPL in the Contiki Cooja emulator uses 60 seconds as a predefined transmission time for the DIS message. Thus, a new node continuously transmits a DIS message with a fixed 60 second cycle until it collects a DIO message from any other adjacent node. When a new node wants to join a DODAG, it sends a DIS message to get the information of the surrounding nodes in the network topology. An attacker can misuse this feature, and it can frequently send multiple DIS messages to its neighboring nodes. Figure 4 shows this attack. Here the attacker node with ID 9 mounts a DIS flood attack on the adjacent nodes.

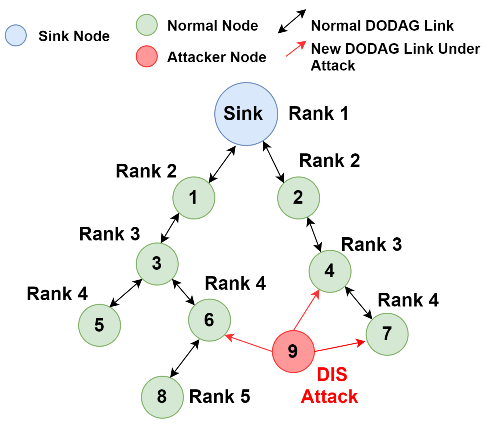

Fig. 4. DIS Flooding Attack

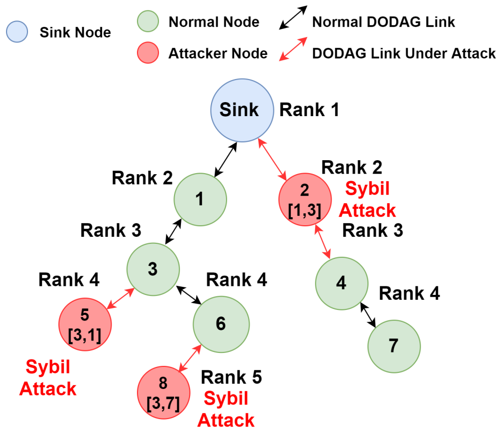

Fig. 5. Sybil Attack

The existing methods against this attack are now discussed one by one. Le et al. [20] examined the DIS attack effects under unicast and multicast mechanisms and have discovered that the DIS attack cannot disturb the delivery rate. However, it can increase end-to-end delay. Till now, there is no particular attack prevention method for this attack. Nevertheless, to minimize the attack's effects, IETF has proposed some changes to the node's reaction upon receiving multiple DIS messages [20], [21]. These changes are still to be tested and examined. Le et al. [21] have demonstrated the successful protection against DIS attack through their specification-based IDS. Their technique is based on semi-auto profiling and construction of an abstract of network operation through network simulation traces for different clusters. Next, it uses these traces as a reference for the node's behavior and verification. However, the security and optimal placement of the cluster head is the primary concern of this method. There are few studies like [23], [24], where the authors have made efforts to investigate the effects of this attack on network performance and have delivered a lightweight mitigation technique against it. They considered two safety threshold values, one for the maximum number of allowed requests and the other for the fixed DIS transmission interval. They have demonstrated the correctness of their work using the Cooja emulator. However, the effect of the lossy nature of the RPL protocol is not taken into consideration while designing these methods. Further, the use of timestamps makes these methods more complicated.

3.1.2 Sybil Attack and Mitigation Techniques. In this attack, the malicious nodes create multiple identities as shown in Figure 5 and mislead the other nodes [25]. In Figure 5, the nodes with IDs 2, 5, and 8 are the sybil attackers with the fake identities shown in the square brackets. By implementing such an attack, the attacker can control various areas of the network without using any physical node. The paper [25] classified sybil attacks into three types, namely SA-1 (restricted to a specific area of the network), SA-2 (distributed over the network), and SA-3 (distributed over the network and the attacker nodes are mobile). Authors in [26] studied and evaluated the performance of the RPL protocol under mobile sybil attack.

The summary of the studied mitigation techniques is as follows. Some researchers have suggested the use of information about the node's geographical location with the communication messages. This approach is the best one to tackle clone ID/sybil attack because a single node cannot be present at two different locations at the same time instance [3]. Besides this, there are some other methods as proposed by Zhang et al. [25], which makes a social graph of the network and then recognize the attacker nodes on two principles: (i) Sybil nodes have a tight connection between them as compared to with that of the legitimate nodes, and (ii) Sybil node does not have a tight connection with many legitimate nodes. The scheme is best for the SA-1 type of attack. The SA-2 type of attack can be defended by behavioral classification methods, which assumes that the malicious nodes have incomplete, monotonous, and certain specific behaviors compared to the normal nodes. The use of trust-based methods that adopts friend relationship sybil detection schemes and maintains a friend list with each node is suggested for the SA-3 type of attack.

S. Murli et al. in [27], have proposed and evaluated a novel solution against the Artificial Bee Colony (ABC)-inspired mobile sybil attack model in RPL. They have used Cooja emulator on top of Contiki OS to demonstrate their results. Still, the method can be improved concerning the accuracy and time of attack detection. D. Airehrour et al. in [28] proposed a time-based trust-aware approach to tackle sybil attack. They have explained how their trust-based solution can be embedded in the RPL protocol. This method's design has steps like trust calculation, trust monitoring, trust rating, detection, and isolation of attacker node and taking backup of new trust values. The method has too many intermediate stages, and therefore causes latency in the attack detection. One more trust-based method is suggested in [29]. Here the authors determine the node's trust value based on the received signal strength and use the Cooja emulator with Wireshark to evaluate their solution performance. Besides this, some recent studies [30], [31] have proposed a Gini Index-Based countermeasure against the sybil attack in IoT. They have implemented this approach in OMNeT++ and compared its performance with the two existing schemes, called SecRPL and two-step detection. This method has an improved detection rate with optimal energy consumption. However, these methods have a complex mathematical calculations.

M.Conti et al. [32] enhanced the RPL by modifying the DAO packet to add device ID and the hash of software to protect nodes against insider attacks. The authors have proposed two different algorithms, one for the root node and the other for the non-root nodes. The results shown in their work are based on the Cooja emulator. However, calculating, storing, and comparing hash values degrades RPL's performance to some extend.

3.1.3 Replay Attack and Mitigation Techniques. The attacker here records the control messages (DIO, DIS, DAO, and DAO-Ack), then purposely re-transmits them in the network [10]. The attack can be mounted even if the RPL runs in a secure mode. Because to mount the attack, the attacker doesn't need to know about the keys used for cryptography. The attack consequences include obsolete or fake routing entries, poor routing systems, a lower transmission rate of packets, and sometimes detachment of the victim node from the formed DODAG. The attack typically can have more harmful effects on the dynamic networks than the static networks. Note that this attack is common with all control messages. Hence, it is only covered once in this section.

RPL has an optional mechanism for the replay protection [33] within itself, but using it increases the delay, power consumption, and the network overhead. The replay protection mechanism of the RPL protocol is useful in static networks. However, there are no proposals for the mitigation of the attack in dynamic networks. Table 2 summarizes the DIS control message-related attacks and scope of improvement in the studied mitigation techniques. The table also briefs about the classification of methods based on the defense techniques and use of the packets (either modified or as it is) in the respective mitigation technique.

3.2 DIO Specific Attacks and Mitigation Techniques

This subsection provides a brief discussion on the routing attacks possible through the DIO control message and an overview of the respective countermeasures against them.

3.2.1 Rank Attack and Mitigation Techniques. RPL forms a DODAG where the rank value increases from the root node to the child nodes. The task of the child node is to select a parent with a lower rank value. An attacker can change a node's rank value to mount a rank attack or manipulate the parent selection procedure to mount the worst parent selection attack. This affects the routing topology [3], [6]. In Figure 6, nodes with IDs 3 and 2 show decrease and increase rank attacks, respectively. Whereas the node with ID 7 selects the worst parent with node ID 6 instead of the node ID 4 with a lower rank value, thus affects the RPL topology. Note that the worst parent selection is also a part of the rank attack, but selecting the worst parent has a negligible effect on the network. All these manipulations can be done in either of the two ways: (i) Direct manipulation of the rank value in the DIO message, and (ii) Through the objective function used.

A variety of methods for the mitigation of the rank attack(s) are proposed by various authors that include the IDSs and other methods as mentioned hereafter. Perrey et al. [34], [35] proposed a method called 'Trust Anchor Interconnection Loop' (TRAIL). In which, whenever a new DIO message is received, a test message containing a randomly generated nonce and the rank of the sender of the DIO is sent to the root nodes via the receiving nodes. The sender node waits for an acknowledgment duly signed by the root node and includes the sender rank, respective DODAG version, and the original nonce. Every intermediate node ought to review the test message as well as its rank acknowledgment. If authentication fails, the message is discarded, and the local repair

Table 3. Summary of Attacks through DIO Control Message and Mitigation Techniques (Part 1)

Mitigation Techniques	**Publication Year**	**Attacks**	**Attack Impact**	**Classification Based on Mitigation Techniques**	**Modified / Default Control Messages**	**Tools Used**	**Summary of Limitations / Scope of Enhancement**
[34]	2016	Rank Attack	Increased Delay, Control Message Overhead, Power Consumption, Decreased Packet Delivery Ratio (PDR)	Acknowledgement Based	DIO*	RIOT and Testbed	Nodes have to wait for Acknowledgement
[37]	2017			Trust Based	DIO* and DAO	MATLAB	Detection Depends on the Accuracy of Trust Calculations
[46]	2019				DIO*	Cooja	Detection Depends on the Accuracy of Trust Calculation
[41]	2011			Statistical / Mathematical /(Cryptographic) Based	DIO*	MICAz	Use of Hash Function Creates Network Overhead and Delay
[35]	2013				DIO	Not Mentioned	Sender Nodes Have to Wait for Acknowledgment Duly Signed by The Root
[42]	2015				DIO	Cooja	Taking Average of Rank Value is Not Practical with Decreased RankAttack
[39]	2016				DAO and DIS	NS-2	Detection Accuracy and Time is an Issue
[43]	2016				DIO*	Cooja	Hash Chain Authentication Increase Computation Overhead, Not Practical for Large Networks
[55]	2018				Not Mentioned	Cooja	Energy consumptions can be due to other attack also
[44]	2018				DIO*	Cooja	Nodes have to Store Values Like Ego and Sensitive Node List
[45]	2018				DIO	Cooja	IDS Completely Relies on Sink Node and Assumes that the Sink is Secure
[47]	2019				Not Mentioned	Not Mentioned	Implementation of Block-Based Data Structure on Large Networks is Not Practical
[22]	2013			Specification Based	DIO and DAO	Cooja	6LoWPAN Mapper Dependency and Issue With Accuracy
[21]	2016				DIO and DIS	Cooja	Attack Detection Time and Accuracy Can be Improved
[34]	2013	Version Number Attack	Increased Delay, Power Consumption, Decreased Packet Delivery Ratio (PDR)	Acknowledgement Based	DIO	RIOT and Testbed	Nodes have to wait for Acknowledgement
[41]	2011			Statistical /Mathematical /(Cryptographic) Based	DIO*	MICAz	Use of Hash Function Creates Network Overhead and Delay
[35]	2013				DIO	Not Mentioned	Sender Node Waits for Acknowledgment Duly Signed by The Root
[22]	2013			Specification Based	DIO and DAO	Cooja	6LoWPAN Mapper Dependency and Issue with Accuracy
[50]	2019				DIO	Cooja	Rank validation of Node is Not Considered
[22]	2013	Neighbour Attack	Increased Delay	Specification Based	DIO and DAO	Cooja	6LoWPAN Mapper Dependency and Issue with Accuracy
[21]	2016				DIO and DIS	Cooja	Detection Time and Accuracy is an Issue
[51]	2017				DIO	Cooja	Attack Detection Time can be improved
[52]	2018			Location Based	DIO	Cooja	Location Privacy is an Issue

* Denotes Modified Control Message

process is initiated. Once the originating node receives the DIO message, the acknowledgment content is verified and compared with the content of the received DIO message. If all fields are similar, then the usual RPL procedure is carried out. To optimize the control overhead and ensure better scalability for TRAIL, the authors introduce an aggregation mechanism based on the bloom filters. However, this method creates a significant delay because the nodes have to wait for the acknowledgment message.

Other mechanisms, proposed by Airehrour et al. [36] that calculates trust values and Kham and Herrman [37] which have distributed mechanisms to find 'Trust' values exists. In [37], the trust values are passed to the root node, where all these values are added to find the 'Reputational' values. These values are then used to identify the adversaries. The literature [11] says that some IDS which

Table 4. Summary of Attacks through DIO Control Message and Mitigation Techniques (Part 2)

Mitigation Techniques	Publication Year	Attacks	Attack Impact	Classification Based on Mitigation Techniques	Modified / Default Control Messages	Tools Used	Summary of Limitations / Scope of Enhancement
[19]	2012	DODAG Inconsistency Attack	Increased Delay, Power Consumption and Network Overhead	Acknowledgement Based	DAO	Not Mentioned	Not suitable for Large and Dynamic Networks
[53]	2014			Statistical/ Mathematical (Cryptographic) Based	DAO and DIO	Cooja	Do Not Provide Complete Mitigation
[54]	2015				DAO and DIO	Cooja	Do Not Provide Complete Mitigation
[19]	2012	HELLO Flood Attack	Increased Delay, Power Consumption	Acknowledgement Based	DAO	Not Mentioned	Not suitable for Large and Dynamic Network
[3]	2013	Selective Forward Attack	Increased Delay, Disrupt Routing Path	Acknowledgement Based	ICMPv6 echo	Cooja	Not Practical for Larger Network
[57]	2015			Trust Based	DIO*	Not Mentioned	Calculation of Trust is Crucial and Increases Overhead
[58]	2017				DIO*	Not Mentioned	Trust Value Calculation and Accuracy is an Issue
[40]	2014			Statistical / Mathematical (Cryptographic) Based	Not Mentioned	Gambit	Increases Computational Overhead
[60]	2015				DIS	Cooja	Increases Computational Overhead
[39]	2016				DAO and DIS	NS-2	Detection Accuracy and Time is and Issue
[61]	2018				DIO	Cooja	Mobility is Not Taken Under Consideration
[63]	2020				DAO* and DAO-Ack	Cooja	Lossy nature of RPL is not considered, Accuracy can be Improved
[62]	2017			Specification Based	DIO and DAO	Cooja	Network Overhead Increases with Mobile Nodes
[64]	2012	Sinkhole/ Blackhole Attack	Increased Delay, Disrupt Routing Path	Acknowledgement Based	Not Mentioned	Custom-built discrete-time RPL Simulator	Not practical with larger Networks, Node has to Maintain Blacklist
[57]	2015			Trust Based	DIO*	Not Mentioned	Accuracy of Attack Detection can be Improved
[36]	2016				DIS	Cooja	Trust Value Calculation and Accuracy is an Issue
[58]	2017				DIO*	Not Mentioned	Experimental Analysis is Not Done
[66]	2017				DAO and DIO*	Cooja	Trust calculation and Storage is an Issue
[67]	2018				DAO and DIO*	Cooja	Trust calculation and Storage is an Issue
[65]	2019				DAO and DIO*	Cooja	Bulky Trust Calculation Process
[40]	2014			Statistical / Mathematical (Cryptographic) Based	Not Mentioned	Gambit	Computational Hard for Sensor Nodes
[38]	2015				DAO and DIS	Cooja	Increased Computation Overhead
[39]	2016				DAO and DIS	NS-2	Detection Accuracy and Time is an Issue
[71]	2018				DIO	Cooja	Not suitable for Larger Networks
[72]	2020				DIO and DAO	Cooja	Not suitable for Larger Networks
[22]	2013			Specification Based	DIO and DAO	Cooja	6LoWPAN Mapper Dependency and Issue with Accuracy
[21]	2016				DIO and DIS	Cooja	Issue with Accuracy
[69]	2016				DAO and DIO	Cooja	Maintaining Counter and collecting Neighbour Information creates delay in attack detection, Accuracy is an Issue
[68]	2019				DIO	Cooja	All these methods can be more Effective and Lightweight
[70]	2019				DIO	Cooja	Dependent on 6 Mapper This method is not evaluated with larger Sensor Networks

* Denotes Modified Control Message

are statistical/mathematical based can also be useful to tackle rank attack. IDSs like INTI [38], InDReS [39], and Game theory IDS [40] with some extensions can be used for the mitigation of the rank attack. However, mathematical calculations create a significant overhead on the network. Besides this, these methods are not suitable for larger networks.

Dvir et al. [41] introduced the 'Version number and Rank Authentication' (VeRA) mechanism. VeRA creates two related hash chains using a one-way hash function for version numbers and the relevant rank value. VeRA is found prone to rank falsification [35], either by making a fake rank hash chain or simply by re-transmitting the parent's rank. Besides this, the complexity of VeRA

Table 5. Summary of Attacks through DIO Control Message and Mitigation Techniques (Part 3)

Mitigation Techniques	**Publication Year**	**Attacks**	**Attack Impact**	**Classification Based on Mitigation Techniques**	**Modified / Default Control Message**	**Tools Used**	**Summary of Limitations / Scope of Enhancement**
[77]	2013	Wormhole Attack	Disrupt the Network Topology and Traffic Flow	Statistical / Mathematical (Cryptographic) Based	Not Mentioned	NS-2	Not Suitable for Dynamic and Mobile Networks
[40]	2014				Not Mentioned	Gambit	Increase Computation Overhead
[79]	2016				DIO	Java Based Simulator	Increases Power Consumption and has Complex Mathematical Calculation
[80]	2020				DAO* and DIO*	Cooja	Not Practical for Mobile and Large Networks
[22]	2013			Specification Based	DIO and DAO	Cooja	6LoWPAN Mapper Dependency and Issue with Accuracy
[78]	2003			Location Based	Not Mentioned	Not Mentioned	Depends on Acknowledgement Packets and Created Delay
[76]	2015				DIO* and DAO*	Cooja	Location Privacy is an Issue
[74]	2016				Not Mentioned	NS-2	Not Practical for Mobile Nodes
[19]	2012	Replay Attack	Increased Delay, Power Consumption and Network Overhead	Acknowledgement Based	DAO	Not Mentioned	Not Suitable for Large and Dynamic Networks

* Denotes Modified Control Message

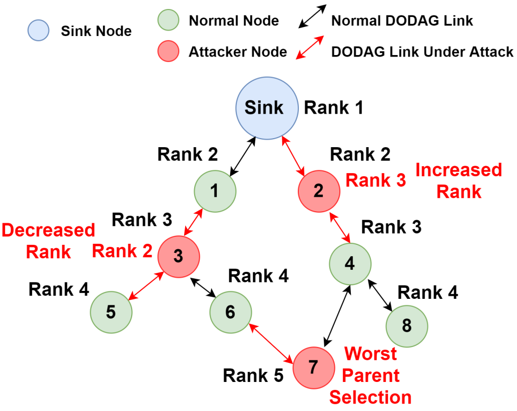

Fig. 6. Rank Attack

increases the consumption of the resources. Iuchi et al. [42] introduced 'Secure Parent Node Selection', in which every node calculates the average of rank value through the received DIO messages and makes use of it to construct a threshold rank value. The threshold value helps to choose a better and valid parent. The method depends on the fact that the attacker always advertises a lower rank than its adjacent nodes.

SVELTE IDS [22] uses a specification-based method to mitigate the rank attack. In this IDS, the authors propose a '6LoWPAN Mapper' that runs on the border router. The authors have proposed algorithms that work on input from all the nodes. The proposed method works well. However, it requires additional computations and storage to maintain the whitelisted and blacklisted nodes. Moreover, this method struggles with accuracy. It uses a distributed mini-firewall to protect from global attacks. The authors have used the Cooja emulator to show the results. The technique 'S-RPL' suggested by Glissa et al. [43] can also be used to conquer the rank attack. It uses the decrease rank threshold and hash chain authentication. S-RPL has two algorithms, one for the verification phase and another for the rank updation. However, it increases computational overhead. Recently Shailendra Shukla et al. in [44] proposed a method against the increase rank attack. The proposed solution uses two terms - 'ego' for the node of interest and 'alters' for the node's connection. The method avoids the use of global information and considers local information. However, the nodes have to store values like ego, threshold, and list of the subtle nodes. Hence it is found unsuitable for dynamic and large networks.

In [45], Usman Shafique et al. proposed a Sink Based Intrusion Detection System (SBIDS). The method encrypts the DAO packet having information like IP address, preferred parent, and rank value and sent it to the sink node. The sink node decrypts this DAO message and checks the validity of the rank value. When a malicious node is detected, this method uses the parent switching threshold to change the parent and avoid the path through the attacker node. The IDS entirely relies on the sink node and assumes that the sink is secure. This kind of IDS has an additional overhead on the sink node, and it assumes that the version number is always correctly updated. In [46], the authors use a non-cooperative game model and maintain a direct trust measurement to restrict the malicious node. In [47], authors use the block-based data structure at each node. They proposed using a local node database for the connected nodes in the network and a global node database for the sink nodes. However, they have not implemented and validated their work.

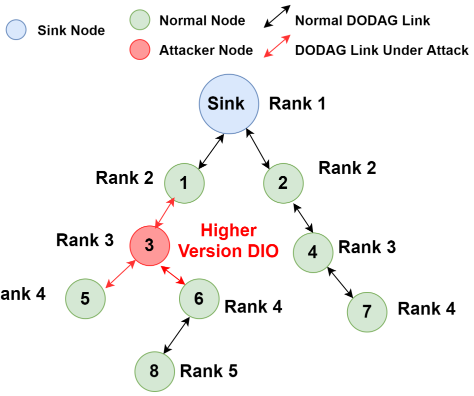

Fig. 7. Version Number Attack

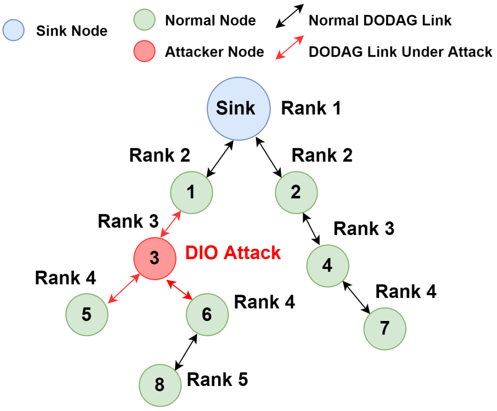

Fig. 8. Neighbour (DIO) Attacks

3.2.2 Version Number Attack and Mitigation Techniques. With the RPL protocol, only the root/sink node can change the DODAG's version number. Besides this, the present RPL model has no mechanisms for maintaining the communicated version number's validity through a DIO message [48]. The attacker exploits this vulnerability to mount the version number attack. When a malicious node sends a higher version DIO message, RPL's global repair procedure starts. This results in topological inconsistencies and the routing loops, particularly if the malicious node is at a distance from the root node [49]. The main objective of the attack is to drain energy of nodes and to delay the delivery of the packets. In Figure 7, the node with ID 3 sends a DIO packet with a higher version number to its child nodes.

Some of the well-known mitigation methods proposed for this attack are as follows. TRAIL (as discussed earlier), a strategy based on acknowledgment packets, is very successful against the version number attack. Many other trust-based methods remarkable for the sinkhole/blackhole attack mitigation are also found fruitful to tackle version number attack. Statistical/Mathematical based IDSs like InDReS [39], Game theory IDS [40], and VeRA [41] are some of the prominent mechanisms used to mitigate this attack. Mitigating the version number attacks is also possible with SVELTE [22] and other specification-based IDSs. Moreover, Mayzaud et al. [48] have designed a distributed IDS for mitigating the attack. In [50], a new lightweight method is suggested to mitigate the attack. Here, the authors have proposed two novel mitigation techniques. Firstly, they suggest considering the version number update coming only from the root/parent node, i.e., from the node with a lower rank value. In the second method, they have suggested using the shield mechanism that updated the version number only when most surrounding nodes have updated their version number. However, they have assumed that the rank of every node is correctly propagated through the RPL network. They have used Cooja emulator to validate the proposed mitigation technique.

3.2.3 Neighbour Attack and Mitigation Techniques. In this attack, an adversary transmits a DIO message to its neighboring nodes without any alteration [4], [20]. Thus, the unmodified DIO messages are forwarded to mount this attack. Figure 8 shows the attack scenario where the node with ID 3 attacks the nodes with ID 5 and 6. The major consequence of the attack is a slight increase in the end-to-end delay. But, it can become more severe when clubbed with other routing attacks. This attack is difficult to detect [4], [20] because the adversaries seem to be opaque in the network. A limited number of solutions and studies are present on the prevention of the attack. Le et al. [21], and Shreenivas et al. [51] studied and stated that some IDSs which are specification based like SVELTE [22] might be extended to detect this attack. Furthermore, location-based mitigation approaches that link the node's position with its communication range can support the logical identification of this attack. The IDS, as in [52], is incorporated by considering location information and received signal strength to identify the malicious nodes. This IDS has also incorporated a secure routing process that can rectify disruption in the routing paths. However, all these methods can only work if the adversary cannot change the signal strength of the compromised node.

3.2.4 DODAG Inconsistency Attack and Mitigation Techniques. The RPL protocol uses its self-repair mechanism to address the inconsistency in the RPL DODAG formation. As per [19], [53], [54], an attacker can misuse this process to launch the DODAG inconsistency attack. The attacker here sends packets with its 'O' and 'R' flags set. Thus, the receiving parent detects an inconsistency with the DODAG because the 'O' flag packets are designed for the ancestor nodes only. It insists the receiver node to drop the packet and reset the trickle timer. Thus, the attack strikes all the crucial network parameters. Different methods suggested against the attack are as follow. Sehgal et al. [53] have suggested using an adaptive solution to reset the trickle timer. The method uses the ratio of inconsistent packets to regular packets. Authors in [54] have attempted to address the DODAG inconsistency attack created by the manipulation of 'R' and 'O' flags in the DIO packets. They have stated the problems with the static value used to reset the tickle timer in a loop formation. Therefore, they proposed a method based on the threshold value to reset the trickle timer. In [55], the authors have proposed a novel approach that uses the energy consumption details of each node stored at the sink node. The proposed method uses this stored list of nodes at the sink node and generates a virtual loop-free tree. Further, the method uses this tree and detects the malicious node based on its energy consumption. However, the method adds an extra burden on the sink node. Besides this, the attacker, when resides deeper in the network topology, can still significantly harm the network.

3.2.5 HELLO Flood Attack and Mitigation Techniques. Whenever a new node joins a network, it uses a HELLO message that an attacker node can use to mount the HELLO flood attack and mislead other nodes. A DIO message or a DIS message can be used to start this attack [3]. As shown in Figure 9 the attack can persist in the RPL networks for some time. The RPL protocol has an inbuilt defense mechanism against the attack. RPL's self-healing mechanism is found beneficial to mitigate this attack. However, it is not suitable for dynamic and large networks.

3.2.6 Selective Forwarding Attack and Mitigation Techniques. In this attack, a malicious node denies to transmits some packets. The attack scenario is shown in Figure 10. It results in the disruption of the routing path [3]. Moreover, the attack can be further extended into the sinkhole/blackhole attack, where the malicious node rejects all the forwarding packets [56]. Various methods for the mitigation of this attack are proposed in the literature, mainly involving the IDSs and other methods. The authors in [3] introduce a technique that creates a disjoint path from the root to the leaf

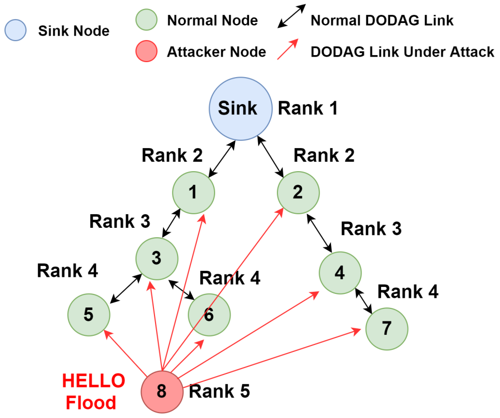

Fig. 9. HELLO Flood Attack

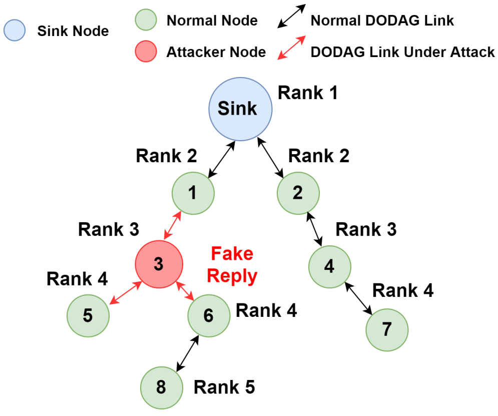

Fig. 10. Selective Forwarding Attack

nodes. However, the problem with it is that it fails with a more extensive network. In [4], the contributors emphasize using encrypted packets. Here the selective forwarding is avoided. However, this method does not avoid the sinkhole/blackhole attack. Besides, it also increases the end-to-end delay.

Heartbeat mechanism, as proposed by Wallgren et al. in [3] is a method that works on periodic Acknowledgment messages. Here, ICMPv6 echo message is broadcasted from the root to the connected nodes to get back an echo message. The node that does not respond within a specified period is declared as a malicious node. The authors advocate the use of IP security (IPSec) to make the technique infallible. Some trust-based techniques are introduced to remove the drawbacks of the acknowledgment-based methods. Airehrour et al. in [36] propose a method that first calculates the trust value of the neighboring nodes and then chooses the preferred parent. However, they have not considered the mobile nature of the nodes. In [57], [58], Djedjig et al. propose a trust-based mechanism for the RPL where each node has a Trusted Platform Module (TPM) as a coprocessor.

Using IDSs based on mathematical methods can be used to detect this attack. However, the use of complex mathematical calculations exhausts the nodes' battery life, especially with the hybrid placement of the IDS [59]. Specification-based IDS like SVELTE [22] is found to be most promising among all. In [60], authors have proposed and evaluated a new variant of the RPL protocol that is immune to insider manipulations and different routing attacks. They have implemented this solution in the Cooja and found that it is better concerning packet delivery ratio and energy efficiency. To detect malicious nodes Sabah Suhail et al. in [61] maintained the count of the received packets from the respective child nodes and kept a record at each parent node. Fatma Gara et al. [62] proposed an IDS which works in the phases like data gathering, analysis, decision, and then finds the compromised nodes. They implement the solution in the Cooja emulator. However, due to the time taken in data gathering, this method's attack detection latency has shown a significant increase. Recently authors in [63] have proposed and evaluated artificial intelligence-based techniques to detect packet drop ratio, which is the first of its kind. Their solution is based on the working of the DAO packet, and after detection, they have used the DIO packet to drop the attacker node as a parent.

3.2.7 Sinkhole/Blackhole Attack and Mitigation Techniques. In the sinkhole/blackhole attack, the malicious node intends to drop the packets going through it [3]. Node with ID 3 in Figure 11 depicts a sinkhole attacker node. Usually, the attacker node advertises a false rank value to form

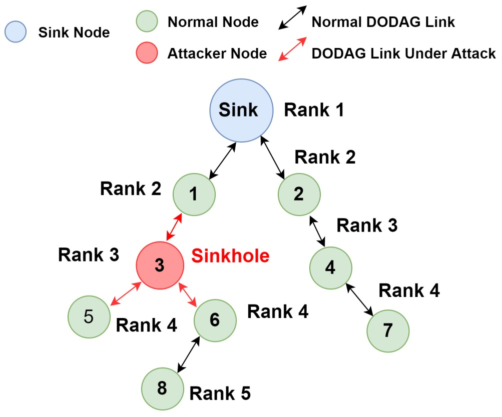

Fig. 11. Sinkhole Attack

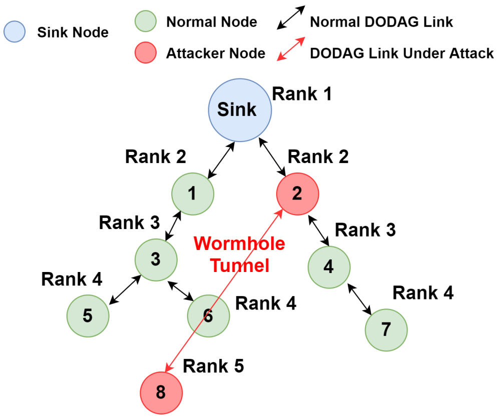

Fig. 12. Wormhole Attack

fake routes. After being a part of such false or non-optimal routes, the attacker node then drops the packets. This attack, when combined with other attacks, can significantly damage the IoT networks.

The discussion about the mitigation techniques is as follows. As blackhole and sinkhole attacks are very similar, the same trust-based methods are fruitful to mitigate both attacks. Weekly and Pister [64] have proposed an acknowledgment-based method, namely "Parent Fail Over" as a solution for this attack. If the root node does not get an acknowledgment message within 10 seconds, it adds this node to the blacklist. However, maintaining the blacklist of an extensive network in a resource-constrained environment is not easy. Further, when this attack is combined with the sybil attack, it is tough to mitigate it with the above method. Weekly and Pister [64] has also proposed a mathematical mechanism 'Rank Verification' as a counter technique against this attack. Their method verifies topological ranking by using a hash-chain. Along with it, other IDS like INTI [38], InDReS [39], and Game theory IDS [40] are also useful against this attack. SVELTE [22] a specification-based IDS (discussed earlier) for the RPL is found quite useful against this attack. However, as per our observation, non of the IDS is suitable for the larger and dynamic networks. Further, the mathematical mechanism-based IDSs create an extra burden on power and memory usages. It can be a potential area where the researcher can focus on. Apart from the above, some trust-based techniques like in [65], [66], [67] are found effective against the sinkhole and the blackhole attacks. All of them are evaluated in the Cooja emulator. As discussed earlier, trust calculation and storage are the main problems with these methods.

H.Patel et al. in [68] proposed and evaluated a strainer-based detection technique for the blackhole detection through monitoring the traffic on each node. Their architecture is based on the local and global modules for the detection of the attack. The local module has a strainer, observer, detector, and alternator. In contrast, the global module has to collect and make decisions through a decision-maker based on four neighboring nodes' behavior. The method is evaluated in the Cooja emulator. A similar kind of work is presented in [69], which emphasizes the observation of the communication of adjacent nodes and has local and global modules. A defense mechanism against the sinkhole and the clone ID attack [70] illustrates and examines the result of this hybrid assault on the efficiency of the RPL protocol. This method is inspired by earlier detection methods on the sinkhole and the clone ID attacks. Other mathematical-based methods based on some mathematical calculations as in [71] are found effective against this attack. Sonxay Luangoudom et al. proposed and evaluate their method [72] in Cooja, which is similar to SVELTE [22] IDS discussed earlier.

3.2.8 Wormhole Attack and Mitigation Techniques. This attack uses two malicious/compromised nodes as shown in Figure 12 and creates a direct communication link to forward network traffic and thus ignores the intermediate nodes [73]. Usually, such a connection is utilized for communication without malicious purposes [3]. The attack, when combined with the sinkhole attack or the sybil attack, becomes more troublesome. Intrusion Detection and Prevention Systems (IDPSs) and visualization mechanisms can detect it. Wormhole attack is also prominent in the WSNs. To avoid this, the 'Round-Trip Time' oriented method is proposed in [74], [75]. The method estimates the distance between the nodes and creates a virtual map of the nodes present in the vicinity. However, if an attacker is using a high-speed connection, then the method has some limitations. Some IDSs which have location information like Pongle and Chavan [76] are found effective against wormhole attack. Some game theory-based mathematical models are also used to mitigate the wormhole attack. The authors proposed Merkle tree-based authentication to counter the wormhole attack in [77]. However, all these methods have a huge scope of further enhancements.

Adding geographical location information to communication messages [3] is found to be the most promising method to avoid the wormhole attack. As in [76], the node uses GPS or indoor location beacons to involve the nodes' geographical locations for the path authentication process. However, it may cause a problem with location privacy. Besides this, an attacker may also manipulate or send false location information. Moreover, such methods face difficulties to detect the attackers which are mobile. Another approach [78] called 'Packet Leashes' adds a trip to packets to limit packets' flow within a geographical region. The authors have used GPS-enabled hardware in this method. Moreover, the method needs an accurate clock synchronization to work correctly. SVELTE-IDS [22] with some extensions is capable of mitigating the wormhole attack. Work was done in [79] uses rank values extracted from the DIO messages and uses them to detect the adversaries. A recent paper by P. Kaliyar et al. [80] stated the concept of the Highest Rank Common Ancestor (HRCA) method to tackle the combination of the sybil and the wormhole attacks together. They evaluated their method in the Cooja emulator. The detection algorithm for the wormhole attack runs periodically, and the sybil nodes can be detected through the list of familiar parents. Some recent studies like [79] detect the wormhole attack based on the rank of the node obtained through the DIO message. This method has a scope of improvement regarding the attacker isolation time and the accuracy of the attack detection.

3.2.9 Routing Choice Intrusion Attack and Mitigation Techniques. It is an attack where first the attacker observes and learns about the routing choice mechanisms and then uses this knowledge to interfere with the routing paths and thus can alter them. However, we do not come across any apparent effort to mitigate such an attack in the literature. Exploring this attack has a good scope in the future. The attack is related to the DIS message. The DIS message contains a DAG routing metric container that enables the attacker to learn about the routing process. Another possible way of gaining information about the routing process is to understand the objective function's working. Tables 3, 4, and 5 summarize the DIO control message-related attacks and respective mitigation techniques. The table also briefs about the classification of methods based on the defense techniques and use of the packets (either modified or as it is) in the respective mitigation technique. The table also highlights the summary of limitations and scope of improvement in the existing methods.

3.3 DAO Specific Attacks and Mitigation Techniques

This subsection examines and discusses possible attacks through the DAO packet. Furthermore, it presents a summary of the studied methods against each possible attack.

3.3.1 Storing Mode Attacks and Mitigation Techniques. When the RPL protocol is operating in the storing mode, every node is supposed to store the downward routes in its routing table [19]. An attacker can exploit this mechanism. There are three types of storing mode attacks, as listed below.

- **Routing Table Flooding:** The nodes operating in the RPL's storing mode have to maintain a routing table. An attacker may send several bogus routes (through a DAO message) to saturate the victim's routing table. This makes the victim node avoid genuine DAO messages. Therefore, it cannot build accurate routes [10].
- **DAO Inconsistency Attack:** In this attack, an adversary misuses the DAO inconsistency repair mechanism of the RPL protocol. The malicious node returns every packet which it receives by making its 'F' flag set. This leads to the complete isolation of the attacker's sub-DODAG or generates longer routes to reach the destination node. The attack mainly increases the end-to-end delay.
- **Falsification of the Routing Table:** In this attack, a malicious node announces false routes to other nodes. The nodes advertised in the false route may be a part of the network but may not be present in the adversary's sub-DODAG or maybe totally fake [10]. The attack causes packet loss and increases the end-to-end delays.

To the best of our knowledge, to date, no proposed methods for detecting or mitigating storing mode attacks and no comprehensive analysis of how these attacks affect on RPL network is available. However, as mentioned in the RFC-6653, the frequency at which the trickle time reset is 20 per hour. This mechanism can address and minimize the effect of the DAO inconsistency attack. Pu. challenged this method in [81], stating that the attacker could still start the attack without affecting the pre-defined fixed limit. Hence, he introduced a Dynamic Threshold Mechanism (DTM) to change the trickle timer reset rate limit.

3.3.2 Local Repair Attack and Mitigation Techniques. In this attack, as shown in Figure 13, a malicious or compromised node forcefully uses the local repair messages and forces nearby nodes to regenerate their routes through the attacker node. This leads to the creation of a similar topology as existed before. The attack leads to an increase in the control message overhead and drains the resources [4] of the nodes. As per our knowledge, there is no specific method for mitigating the local repair attack until the present. However, authors who proposed other techniques and IDSs advocated extensions to their solution to alleviate this attack.

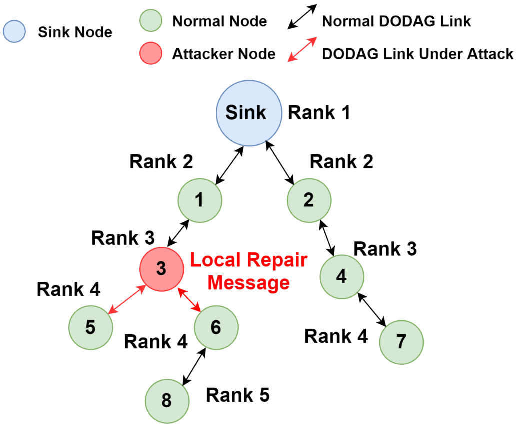

Fig. 13. Local Repair Attack

Table 6. Summary of Attacks through DAO Control Message and Mitigation Techniques

Mitigation Techniques	Publication Year	Attacks	Attack Impact	Classification Based on MitigationTechniques	Modified / Default Control Messages	Tools Used	Summary of Limitations / Scope of Enhancement
[19]	2012	Routing Table Flood (Storing Mode)	Increased Resource Consumption (Energy and Memory)	Acknowledgement Based	DAO	Not Mentioned	Not Suitable for Dynamic Networks
[19]	2012	DAO Attack (Storing Mode)	Fake Routes, Sub Optimal DODAG	Acknowledgement Based	DAO	Not Mentioned	Not Suitable for Dynamic Networks
[19]	2012	Falsification of Root Table (Storing Mode)	Falsification of Routes	Acknowledgement Based	DAO	Not Mentioned	Not Suitable for Dynamic Networks
[58]	2017	Local Repair Attack	Increased Delay, Network Overhead and Resource Consumption	Trust Based	DIO*	Not Mentioned	Not suitable for Large and Dynamic Networks
[35]	2013			Statistical / Mathematical (Cryptographic) Based	DIO	Not Mentioned	Sender Node have to Waits for Rank Value Acknowledgement Duly Signed by the Root
[19]	2012	Replay Attack	Increased Delay, Power Consumption and Network Overhead	Acknowledgement Based	DAO	Not Mentioned	Not Suitable for Dynamic Networks

* Denotes Modified Control Message

Authors proposed an extension of TRAIL [34] that is capable of mitigating local repair attack. Djedjig et al. [58] and Airehrour et al. [36] suggested strategies for expanding their systems for the identification and mitigation of this attack. However, no experimental assessment is done by them. SVELTE [22] authors also have introduced an extension for their IDS to work against local repair attack. Furthermore, specification-based IDSs can be used to mitigate this attack. But, specification-based methods generate high false-negative detection [21] regarding this attack.

Table 6 summarizes the DAO control message related attacks and respective mitigation techniques. It also briefs about the classification of methods based on the defence techniques and use of the packets (either modified or as it is) in the respective mitigation technique. The table also highlights the summary of limitations and scope of improvement in each of the existing methods.

3.4 DAO-Acknowledgment Specific Attacks and Mitigation Techniques

The attacks possible through the DAO-Acknowledgment packet are discussed in this subsection. Further, we have studied and summarized all the existing methods against each identified attack possible through the DAO-Acknowledgement packet.

3.4.1 Fake DAO-Acknowledgment Attack and Mitigation Techniques. When the DAO-Acknowledgment message is enabled in RPL, every node sends an acknowledgment message against the received DAO message. An attacker can exploit this feature and may send a fake DAO-Acknowledgment message. The fake acknowledgment depicts like the packet is received, but an attacker can drop the packet(s). Thus, this attack can cause an increase in the end-to-end delay and network overhead. On the other hand, an attacker can also trigger a replay attack through the DAO-Acknowledgement message. To date, RPL depends on its self-healing mechanism to tackle this attack. Nevertheless, RPL's self-healing mechanism is not suitable for dynamic networks.

Table 7 summarizes the DAO-Acknowledgement control message related attacks, defense techniques, and RPL packets used in each suggested mitigation technique.

Table 7. Summary of Attacks through DAO-ACK Control Message and and Mitigation Techniques

Mitigation Techniques	Publication Year	Attacks	Attack Impact	Classification Based on Mitigation Techniques	Modified / Default Control Message	Tools Used	Summary of Limitations / Scope of Enhancement
[19]	2012	Fake-Ack Attack	Increased Delay, Power Consumption and Network Overhead	Acknowledgement Based	DAO	Not Mentioned	Not Suitable for Dynamic Network
[19]	2012	Replay Attack	Increased Delay, Power Consumption and Network Overhead	Acknowledgement Based	DAO	Not Mentioned	Not Suitable for Dynamic Network

4 DETAILED FINDINGS AND INFERENCES

This section presents useful information derived from our study. All the information will add up to crucial and in-depth knowledge about the RPL's security issues. Along with that, this section elaborates on future enhancements as per the stated findings. Firstly, the identified percentage of the attacks possible through each RPL control message is stated. Secondly, a discussion is made about the distribution of different mitigation techniques suggested by the various researchers against all the identified attacks of the RPL protocol. Further, a brief discussion is made about the identified common problems that prevail with five types of classified and covered methods in this and previous surveys. After that, a crucial statistical analysis and discussion about the attacks possible through each control message, and contorl messages (either modified or unmodified) used in the respective mitigation technique is provided. This discussion will add up valuable conclusions for the readers and help them to understand the existing attacks possible due to the RPL's working principles. We have also put forward some essential data about different simulators/testbeds used to validate various mitigation techniques. To find out all the corresponding percentages/values, we have summarized all the data (extracted from the studied papers) and then have worked on it. Finally, this section also covers the year-wise distribution of the published papers regarding routing attacks on RPL from the year 2010 and before to mid-2020.

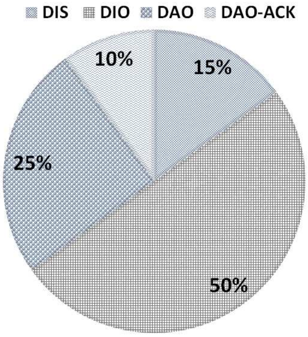

Fig. 14. Percentage of Attacks Through Each Control Message

4.1 Relation of RPL Control Messages and Attacks

Our study based on the existing literature in section 3 noted that a large percentage of routing attacks in RPL is made possible through its control messages. Figure 14 shows the relation between the RPL control messages and the identified attacks. Further, through our study to investigate the possible number of attacks through each RPL control message, we realized that 50% of the total attacks are possible alone through the DIO control message. This data is followed by the DAO, DIS, and DAO-Acknowledgement control messages, contributing 25%, 15%, and 10% of the attacks, respectively.

The RPL protocol relies mainly on the DIO message for the topology creation and maintenance [1], [9], [11], [14]. Hence it is a high-profit area for the attackers. Interestingly, our analysis also reveals that the DIO message is most frequently used to mount the internal routing attacks. Readers must note that in the RPL protocol, whenever a parent node mounts an attack, it can affect many child nodes. Hence, more attention is to be paid to the security of the DIO control message. The DIO packet carries all the crucial information that is necessary for topology formation [9], [11],[14]. Therefore, when it carries falsified information, this packet has the highest potential to mount a large variety of attacks, as shown in Figure 14. When enabled, the DAO-Acknowledgment packet can also be used by an attacker to send fake replies to the connected child nodes. Besides this, the DAO packets travel from the child node to a single selected parent node [1], [14]. Thus, DAO packets have less potential to disturb the complete network. However, still, many attacks are possible through the DAO packet. When studied about the RPL functioning, the DIS packet is also crucial as it is the first packet that allows any node to join the DODAG [1], [14]. The surveyed literature is evident that many dangerous attacks are possible through the DIS packet.

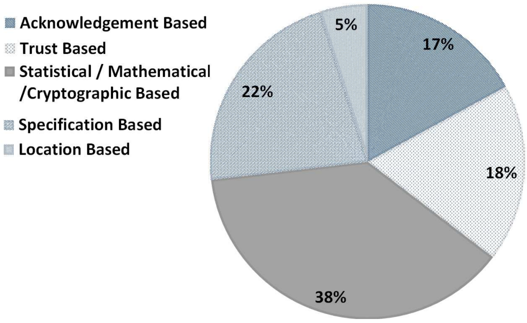

Fig. 15. Classification of Mitigation Techniques

4.2 Relationship of Mitigation Techniques and Attacks

During our study, we adhered to the classification made by [11]. It has helped us find the relation of the RPL routing attacks and their control messages used in each class of the mitigation methods. Further, we expanded our research to examine the distribution of different methods against each routing attack covered in our study. Figure 15 shows the distribution of the used mitigation methods. The statistical/mathematical-based methods are the first choice against the RPL routing attacks as they cover nearly 38% among all the studied methods. In contrast, the specification-based methods cover 22%. The acknowledgment-based methods and the trust-based methods cover 17% and 16%, respectively. However, the location-based methods cover only 5% of the total methods involved to mitigate various attacks. In addition to it, our study further describes each attack with the relevant mitigation techniques. Figure 16 shows the details about attack-wise distribution of mitigation techniques. Our investigation reveals that the studies mainly focus on sinkhole/blackhole, selective forward, and rank attack. Fewer contributions are made against the attacks like local repair, falsification of the routing table, DAO attack, route cloning attack, and reply attacks. Further,

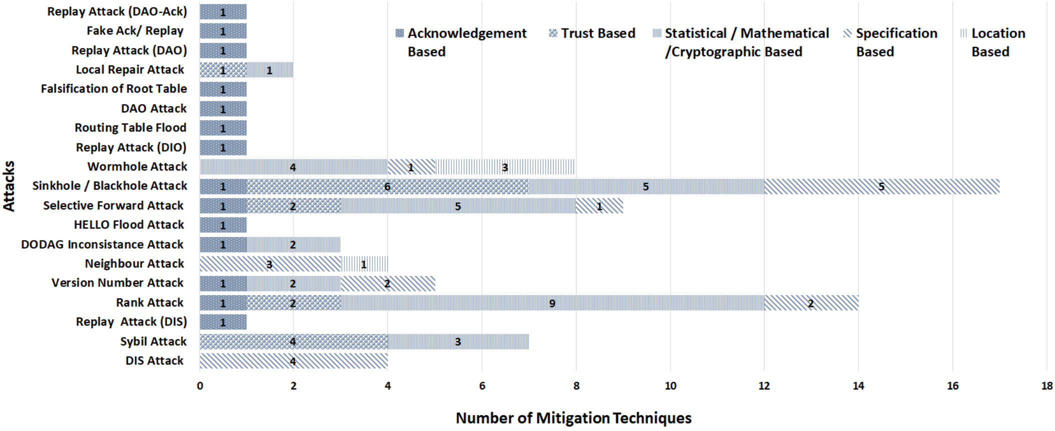

Fig. 16. Attack Wise Distribution of Mitigation Techniques

we foresee an excellent opportunity for the researchers to work against DODAG inconsistency attack, neighbor attack, sybil attack, and DIS attack.

4.3 Identified Problems with the Studied Mitigation Techniques

Major drawbacks of each type of method that we observed and not stated in other prominent surveys [3], [4], [6], [11] are as follows.

- ***Acknowledgment Based Methods:*** These methods use acknowledgment packets either on a periodic time interval or on receiving the desired packet. Thus, unnecessarily increase packet overhead even when the network operates normally.
- ***Trust Based Methods:*** Trust-based methods need additional computing and storage overhead to calculate and store the trust values whenever a message is transmitted.
- ***Location Based Methods:*** Location-based methods are found amply appropriate against the sybil/clone ID attacks. However, these methods endanger the node's location-privacy.
- ***Statistical/Mathematical (Cryptographic) Methods:*** Cryptographic methods are considered unbreakable but need mathematical calculation. Considering the resource-constrained environment, they create a significant delay in the network and require additional computational power. Besides this, the security of the keys stored on the remote devices is also an issue.
- ***Specification Based Methods:*** These methods raise the alarm whenever an anomaly is detected. However, accuracy is an issue with these methods. Moreover, the alarm is raised when an attacker has done significant harm to the network.

4.4 Analysis and Discussion about the RPL Control Messages used in Mitigation Techniques

Along with the default RPL control messages, many researchers have proposed modified structure of the RPL messages or have used a combination of the RPL messages to defend against the various RPL routing attacks. Firstly, we find out the number of default, modified, or combination of control messages involved in mitigating the respective attacks classified as per each RPL control message. Next, we present the percentage of modified and unmodified packets used in the studied mitigation techniques.

4.4.1 Attack Details and the Control Messages used in the Mitigation Methods. To analyze and assess the RPL control messages used in the mitigation techniques, we use the four attack categories (i.e., attack through each RPL control message). Further, we studied and presented a thorough study about the control messages associated with each mitigation technique suggested against the respective attacks. This information will enable the readers to quickly learn about the control messages that various researchers use to mitigate various attacks.

(1) *Attacks Through DIS Control Message and Messages Involved in the Mitigation Techniques*
As per the classifications made by us, the DIS flooding attack, sybil, and replay attack are possible through the DIS control message. Our study reveals that out of the studied methods, DIS attack is mitigated by using the DIS and the combination of DIO and DAO messages. Whereas, mitigation of the sybil attack mainly involves trust-based methods. These methods involve the modified DIO packets and the combination of DIS and DIO messages. Besides this, the methods using DAO messages are found useful against the replay attack. Figure 17 shows the details about them.

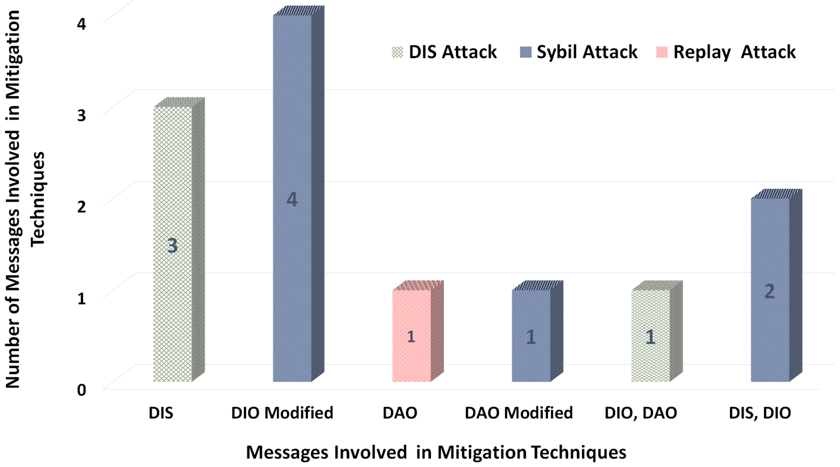

Fig. 17. Attacks Through DIS Control Message and Messages Involved in Mitigation Techniques

(2) *Attacks Through DIO Control Message and Messages Involved in Mitigation Techniques* A significant number of attacks like rank, version number, selective forward, and sinkhole/blackhole are possible on the RPL network through the DIO message. Figure 18 explains more about it.

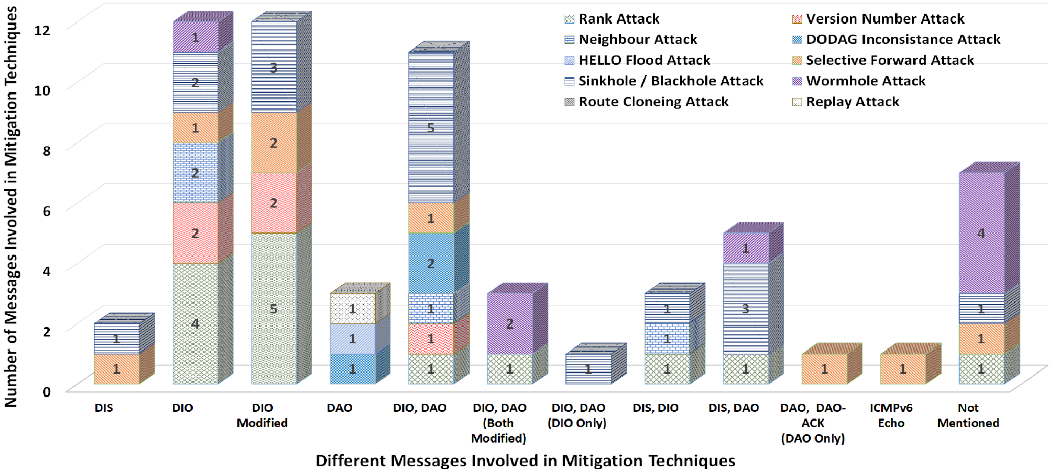

Fig. 18. Attacks Through DIO Control Message and Messages Involved in Mitigation Techniques

Our study shows that most reviewed mitigation techniques rely on the normal DIO packet or the modified structure of the DIO packet and the combination of the DIO or the DAO packets to address these attacks. Further, a counter method against selective forward attack has also used the ICMPv6 *Eco* message. The majority of methods have used the modified DAO and DAO-Acknowledgement messages against the selective forward attack. Mitigation techniques used to counter sinkhole/blackhole attacks also involve the combination of DIS-DIO, DIS-DAO, and unmodified DIO- DAO pairs. Whereas, the combination of DIO and DAO and modified DIO and modified DAO is the most popular one, which is used against eleven and six kinds of attack, respectively. Nearly twelve mitigation methods use the DIO and the modified DIO messages to mitigate various RPL routing attacks. However, we came across nine methods where the authors do not mention the RPL control message's involvement in the suggested mitigation techniques against the attack possible through the DIO message. The above discussion clarifies that various messages or combinations of the various messages are used to date to mitigate a large variety of attacks possible through the DIO message. Moreover, the mitigation techniques using the combination of messages have extensively used the DIO message. The main reason behind it is the working principle of the RPL protocol, which is highly dependent on the DIO message. So, to design an efficient mitigation technique, a proper control message or combination of them must be chosen.

(3) *Attacks Through DAO Control Message and Messages Involved in Mitigation Techniques*
The DAO message travels from the child node to the parent node. Routing table flood, DAO attack, falsification of the routing table, and replay attack are the prominent attacks through this control message. The majority of the suggested methods used the DAO message packet to mitigate these attacks. Whereas, local repair attacks are addressed through the methods making use of DIO and modified DIO control packets. The graph in Figure 19 illustrates more about it.

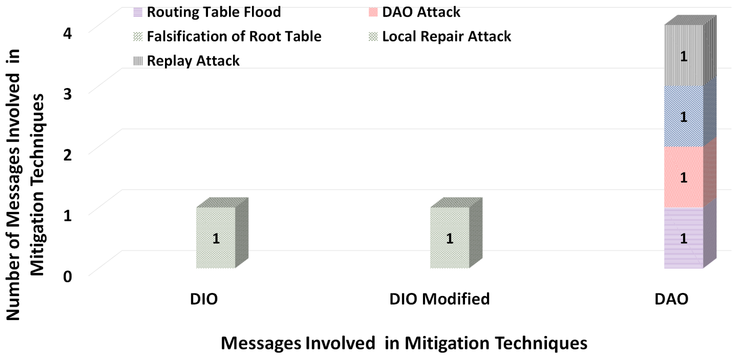

Fig. 19. Attacks Through DAO Control Message and Messages Involved in Mitigation Techniques

From the studied methods, it is clear that four mitigation techniques out of six have used DAO message. This message is extensively used against the attack, which is caused due to the malfunctioning of the DAO message. As the DAO message purely affects the selected parent in the formed topology, it can only help mitigate the attacks originated through the DAO message. However, as per our observations, the local repair attack originated from the DAO attack can be tackled by DIO message. The reason behind using the DIO message is its timely propagation in the formed topology through the tickle algorithm. Thus, a DIO message is mainly selected to mitigate the local repair attack. All the DAO message originated attacks target the formed topology. Therefore, it is necessary to handle the weakness that arises due to the negligence of the security of the DAO message. Besides this, the mitigation techniques or IDSs that need to send data toward the sink node have to pay more attention for securing the DAO message.

(4) *Attacks Through DAO-Ack Control Message and the Messages Involved in Mitigation Techniques*
Attacks through the DAO-Acknowledgment message are possible only if it is enabled in the RPL's operations. The possible attacks through this control message are fake acknowledgment and replay attacks. Our study shows that the researchers have used the DAO message alone to aid the mitigation techniques against these attacks. Figure 20 shows the details

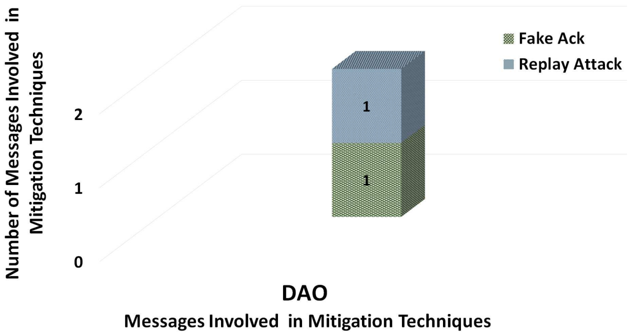

Fig. 20. Attack Through DAO-Ack Control Message and Message Involved in the Mitigation Techniques

about it. As DAO and DAO-Ack messages are co-related with each other, the majority of the researchers have used DAO messages in the suggested mitigation techniques.

4.4.2 Unmodified vs Modified Control Messages. Modifying the RPL control messages to implant the suggested methods is a practice adopted by many researchers. The reason behind it is that many of the defense methods use some additional information like location, hash values, and trust values, along with the RPL control messages. As per our study, out of the suggested mitigation techniques, 72% methods used unmodified packets, whereas 28% methods used modified packets. Figure 21 shows a pie graph about the same. Note that '*' in the table number 2, 3, 4, 5, 6, and 7 denotes the use of modified packet formats. Moreover, modifying the RPL control message can effectively deal with many of the routing attacks. However, the researcher must be careful while modifying the existing packets. Because modifying a control message to carry bulky information may hamper the network performance and create extra power overhead.

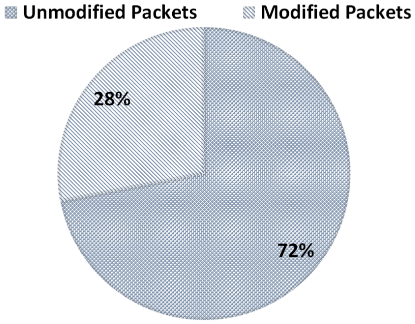

Fig. 21. Unmodified vs Modified Control Packets

4.5 Analysis of Tools Used to Validate Various Mitigation Techniques

This study was extended to find out various tools used to implement and validate the suggested solutions. Figure 22, shows a variety of tools used to validate the mitigation techniques. This study shows that out of all the studied research papers, nearly forty-four techniques are implemented in the Cooja simulator, and five techniques have used the NS-2 simulator. Whereas, only two studies have done actual hardware implementation using TestBeds. Besides this, nearly twenty methods have not implemented their suggested solutions. Other tools like Omnet++, Gambit, and MATLAB are also used to implement few given solutions. Through our study, we infer that most of the exisitng papers focus mainly on simulations rather than performing actual hardware implementations. More than 85% of the total reviewed articles have used simulation tools.

The Cooja simulator's dominance is because it is an open-source simulator/emulator tool and runs on the widely adopted Contiki OS for WSNs [82], [83]. Also, the default implementation of the RPL protocol is readily available in Cooja. Moreover, with Cooja, one can easily create different network layouts, topologies and can compile various motes [82]. Besides this, it also supports many plugins for mobility and data collection and support script utilities to produce more accurate results [83]. Additionally, the simulation results of Cooja are very close to actual hardware implementations [50].

However, the simulation-based assessment does not represent fact as it does not take into account a set of limitations such as climate change, natural processes, and human experiences [11]. While going through vast RPL related papers we come across some prominent studies [84], [85], [86], [87] that focus on practical hardware implementation using large-scale IoT testbeds. Accordingly, we also want to highlight that most security papers are not evaluated on actual sensor nodes (hardware) and hence might not be considered practical. This significant disparity in actual hardware implementations can be attributed to the lower amount of testing laboratories and the high hardware cost. This point also makes it hard for researchers, especially research scholars and academicians, to validate their proposed solutions on actual sensor nodes.

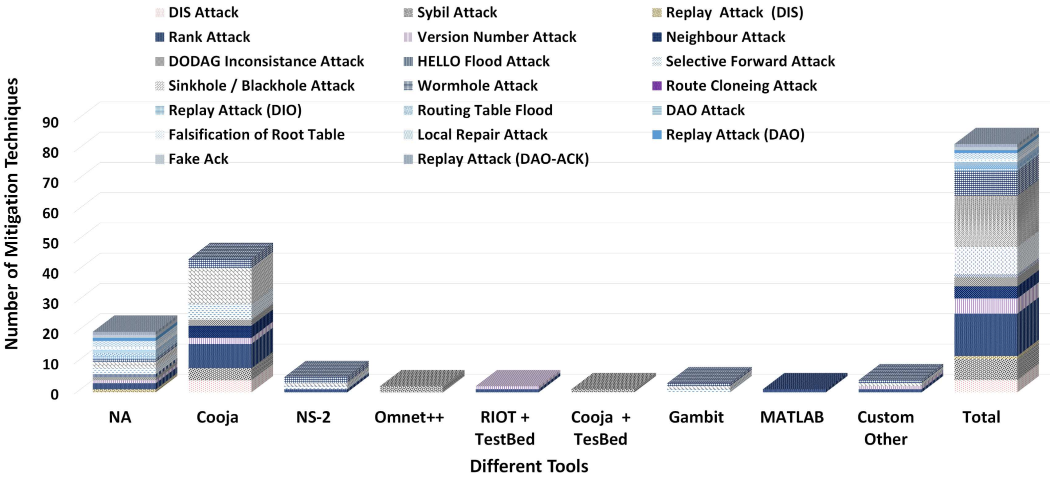

Fig. 22. Analysis of Tools Used to Validate Various Mitigation Techniques Against All Attacks

4.6 Year-wise Publication Statistics

The year-wise distribution and publication statistics of the various papers published and reviewed in this article are shown in Figure 23. From this Figure, it is quite clear that very few papers were published until 2011 concerning RPL and LLN's. However, after the standardization of this protocol by IETF, publications gradually increase till 2014. After 2014, the publication percentage raised by nearly 60% and was highest in the year 2016. During this period, a variety of mitigation techniques and various IDS were published. More focus was given on the traditional routing attacks like sinkhole/blackhole, selective forward, and reply attacks. Moreover, few RPL specific attacks like rank attack, version number attacks, and DODAG inconsistency were concentrated from 2014 to mid-2018. However, the publication count dropped by roughly half, particularly in the year 2018. After 2018 extensive work concentrating on known attacks like sybil, wormhole, local repair, neighbor, DIS, and DAO attack were published. Moreover, the researchers during this time have not focused on the hybrid attacks that combined two or more known routing attacks. Recently,

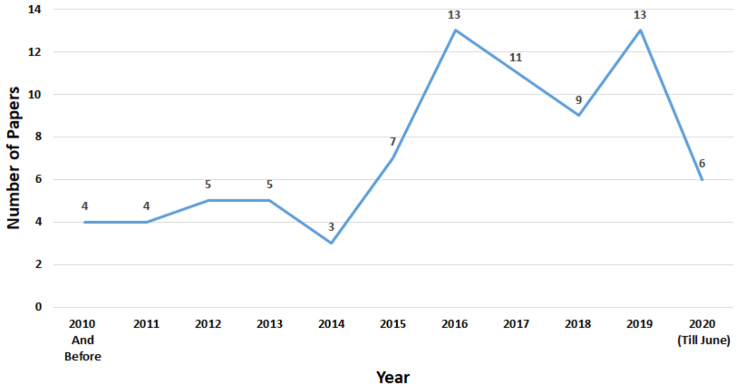

Fig. 23. Year Wise Publication Details

investigations focusing on novel methods and hybrid routing attacks are increasing the publication count rapidly in this field. This discussion makes an obvious picture of how the research flow has progressed in securing the RPL protocol. More research publications concentrating on RPL's security will emerge; this statement can be justified by the fact that RPL protocol is still prone to many security issues.

5 CHALLENGES AND RESEARCH OPPORTUNITIES

There is a significant research volume on various mitigation techniques against routing attacks in the RPL-based IoT networks. However, many issues are yet to be addressed. Moreover, the approach of providing security to RPL must be chosen so that it must not hamper the performance of the protocol and the resource constraint devices on which it runs. Below are the key issues and challenges that the current research community on the topic is facing. We have suggested a few future directions that can be useful to carry the future work on mitigating the identified or new routing attacks.

(1) **Implementing RPL's Default Security Features:** Although RPL comes with many security features, these are treated as optional. However, Perazzo et al. [33] have made an effort to implement RPL's security feature partially. Therefore, exploring and improving the security capabilities of RPL is one of the first activities for future research. Such deployment could be difficult for existing systems in terms of resource consumption. With rapid hardware developments, we assume that incorporating the full list of RPL security features will soon be feasible. Moreover, we foresee a great opportunity to develop new lightweight solutions in this regard.

(2) **Large Network and RPL's Routing Attacks:** From the studied literature, we came to know that less amount of work has targeted the effects of routing attack on large-scale IoT networks. The architectural flows in RPL make it unsuitable for the larger networks (e.g., more than 250 sensor nodes) [88]. The main issues along with the above-mentioned security challenges, are delay in topology formation, bottleneck, and high power consumption of the nodes present near the root node. These larger networks make the IDS implementation very hard. Besides this, attacks like sybil, replay, and wormhole are among the most hazardous attacks [89] on the larger RPL-based IoT networks. Besides, when a larger number of the RPL control messages are used, the network is likely to suffer from jams [33]. This can be used to mount Denial of Service (DoS) attacks. Some recent approaches [90], [91], [92], [93], [94] have targeted this problem. However, all these works are at the very infant stages.

(3) **IDS and Scalability Issues:** Most of the papers have mentioned extension to their IDS. However, as per our observations, these IDSs have marginal extensibility to detect the additional routing attacks. Moreover, most of the suggested extensions have not been practically evaluated. We concluded that IDS defending all the routing attacks will face scalability issues through our study. Therefore, researchers must investigate this issue.

(4) **Exploring Multisink Property of RPL to Develop Collaborative IDSs:** For efficient and speedy detection of intruders, these types of IDS rely on collaboration between sensor nodes and the sink node. There are just a few research articles in the literature that focus on the development of collaborative IDS. To enhance the scalability and security of RPL, we suggest that researchers must explore the multilink property of RPL that involves multiple sink nodes for large-scale RPL deployment.

(5) **Cross-layer Attack and Defense Mechanisms:** Cross-layers attacks on the 6LoWPAN protocol stack are hugely neglected till now. As per our investigation, V.K.Asati et al. [95] are the first to move in this direction. The researchers should explore this research area as cross-layer attacks are hard to detect. Moreover, developing a cross-layer IDS against such attacks can be an important area to work.

(6) **Implementing Outlier Detection Techniques:** An outlier is an observation that differs very significantly from the rest of the data. We advise the researchers to work in this direction to detect anomalies in the RPL networks. Many novel methods, including techniques based on machine learning models, Z-score value analysis, probabilistic or statistical modeling, linear regression models, information theory, and proximity models, would be developed to defend against multiple RPL routing attacks.

(7) **Developing Secure RPL Based Multicast Routing Protocols:** By default RPL supports optional support for multicast routing [14], [96]. In recent times many studies have proposed such multicast variants of the RPL protocol [97], [98], [99]. However, security remains a major concern while deploying these varients. Researchers must focus on developing secure variants of such protocols.

(8) **Developing Security Solutions for Dynamic RPL Networks:** There is no method to facilitate mobility in the standard specification of RPL [14]. As a result, in the presence of mobile nodes, total network performance suffers. Link disconnections, collisions, and packet loss increase with the mobile nodes. Identifying an attacker node in such situations is indeed a challenging task.

(9) **Security of RPL and IPv6 over the TSCH mode of IEEE 802.15.4e (6TiSCH) Combinations:** 6TiSCH achieves industrial-grade performance by combining a time-slotted channel hopping (TSCH) MAC with IPv6 addressing [100]. Also, it is integrated with 6LoWPAN, RPL, and CoAP protocols [100]. However, it requires node-to-node synchronization to prevent looping in the network and attacks on RPL may disturb this process. The study of the security of the RPL and 6TiSCH combination is still in its initial stage, but it is a potential subject for security researchers to investigate.

(10) **Exploring Large Number of RPL's Optional Features:** Availability of optional features is one of the most vital points of the RPL protocol while enhancing its security. All these features provide RPL with immense flexibility to use it with various applications. On the security front, research may explore all these features to provide security to this protocol. To hint the researchers, we highlight some features like multi-instance RPL property, modifying the RPL's objective function, exploring storing and non storing modes of the RPL protocol, and changing the existing format or proposing entirely new control messages.

(11) **Architectural Level Changes:** With the expansion of the IoT ecosystem, new applications are emerging. As RPL is the only standard routing protocol, researchers have to make efforts

to make this protocol suitable for various emerging applications [9], [101], [102], [103], [104]. Architectural level changes done in RPL may resolve the attacks carried through various control messages.

(12) **Investigating New and Hybrid Attacks:** Even though a large number of mitigation techniques are present for each distinguished attack, still work can be done by combining the merits of two or more methods that are efficient to address a large set of attacks. Moreover, the combination of two or more routing attacks are needed to be investigated, and new methods to mitigate such blended attacks ought to be developed.

(13) **Using Hardware Platforms:** Less attention is given on the actual implementation of the suggested methods. As mentioned in [9], a majority of work is evaluated using simulation on Contiki/Tiny OS and by using Telos B [105] or Zolerita Z1 [106] platforms. However, both of these platforms are now outdated. Telos B has many old components, whereas the manufacturing of Zolerita Z1 is suspended [106]. Thus, using these platforms will not provide a fully functional security solution due to resource restrictions. We suggest switching towards more recent hardware platforms like Cortex-M3 [107]. The advancement in electronics has made it much more feasible to work on new platforms with a multi-core processor, adequate memory, and larger batteries.

6 CONCLUSION

We have extensively reviewed the RPL standard and have studied recent IETF's suggestions to modify it. Based on that, we have provided a background of the 6LoWPAN protocol stack and working principles of the RPL protocol. Recent articles concentrating on the RPL routing attacks were thoroughly investigated to present a brief overview of the attacks and the respective countermeasures. Further, all the studied methods were carefully examined in a systematic way to classify and relate the attacks with the RPL control messages. Also, all the studied methods were classified as per the used mitigation techniques. Besides this, all the existing classes of mitigation methods were carefully investigated to find the potential drawbacks. To aid the readers to gain quick and in-depth knowledge about the current research status, we present statistical analysis and point out all the critical findings related to the relation of RPL control messages and attacks, the relation of mitigation techniques and attacks, attack details and control messages used in the studied mitigation techniques, and analysis of tools used to validate the proposed solutions. To summarize, nearly 50% of the attacks are possible through the DIO control message alone. Therefore, securing the information carried by this control message is crucial. As far as the distribution of mitigation methods is concerned, mathematical/statistical methods cover 38%, followed by specification-based (22%), trust-based (18%), acknowledgment-based (17%), and location-based (5%) methods. Among the classified methods, 28% suggested modifying the format of the RPL control messages. Besides this, Cooja is the most popular tool among all and is used to validate nearly 45% of the total proposed methods. In addition to it, a thorough discussion is made regarding future research opportunities related to the RPL protocol. We think our survey will provide a strong base to study and lead to the rapid development of new and more appropriate mitigation methods against routing attacks on RPL-based IoT networks.

REFERENCES

[1] 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, 2012.

[2] 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.

[3] 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

[4] P. Pongle and G. Chavan, "A survey: Attacks on rpl and 6LoWPAN in iot," in *2015 International conference on pervasive computing (ICPC).* IEEE, 2015, pp. 1–6.

[5] A. Mayzaud, R. Badonnel, and I. Chrisment, "A taxonomy of attacks in rpl-based internet of things," 2016.

[6] 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

[7] D. Sharma, I. Mishra, and S. Jain, "A detailed classification of routing attacks against rpl in internet of things," *International Journal of Advance Research, Ideas and Innovations in Technology*, vol. 3, no. 1, pp. 692–703, 2017.

[8] S. Mangelkar, S. N. Dhage, and A. V. Nimkar, "A comparative study on rpl attacks and security solutions," in *2017 International Conference on Intelligent Computing and Control (I2C2).* IEEE, 2017, pp. 1–6.

[9] H.-S. Kim, J. Ko, D. E. Culler, and J. Paek, "Challenging the ipv6 routing protocol for low-power and lossy networks (rpl): A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2502–2525, 2017.

[10] A. Kamble, V. S. Malemath, and D. Patil, "Security attacks and secure routing protocols in rpl-based internet of things: Survey," in *2017 International Conference on Emerging Trends & Innovation in ICT (ICEI).* IEEE, 2017, pp. 33–39.

[11] A. Raoof, A. Matrawy, and C.-H. Lung, "Routing attacks and mitigation methods for rpl-based internet of things," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1582–1606, 2018.

[12] A. Jain and S. Jain, "A survey on miscellaneous attacks and countermeasures for rpl routing protocol in iot," in *Emerging Technologies in Data Mining and Information Security.* Springer, 2019, pp. 611–620.

[13] M. Durairaj and J. H. M. Asha, "The internet of things (iot) routing security—a study," in *International Conference on Communication, Computing and Electronics Systems.* Springer, 2020, pp. 603–612.

[14] T. Winter, P. Thubert, A. Brandt, J. W. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J.-P. Vasseur, and R. K. Alexander, "Rpl: Ipv6 routing protocol for low-power and lossy networks." *rfc*, vol. 6550, pp. 1–157, 2012.

[15] S. Deering, R. Hinden *et al.*, "Internet protocol, version 6 (ipv6) specification," 1998.

[16] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler *et al.*, "Transmission of ipv6 packets over ieee 802.15. 4 networks," *Internet proposed standard RFC*, vol. 4944, p. 130, 2007.

[17] J. Hui, P. Thubert *et al.*, "Compression format for ipv6 datagrams over ieee 802.15. 4-based networks," 2011.

[18] I. S. Association *et al.*, "Ieee standard for low-rate wireless networks," *IEEE Std*, vol. 802, pp. 4–2015, 2016.

[19] J. W. Hui, "The routing protocol for low-power and lossy networks (rpl) option for carrying rpl information in dataplane datagrams," 2012.

[20] 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 *2013 IEEE Symposium on Computers and Communications (ISCC).* IEEE, 2013, pp. 000 789–000 794.

[21] 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.

[22] 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.

[23] A. Verma and V. Ranga, "Mitigation of dis flooding attacks in rpl-based 6LoWPAN networks," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 2, p. e3802, 2020.

[24] 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).* IEEE, 2019, pp. 552–557.

[25] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 372–383, 2014.

[26] F. Medjek, D. Tandjaoui, I. Romdhani, and N. Djedjig, "Performance evaluation of rpl protocol under mobile sybil attacks," in *2017 IEEE Trustcom/BigDataSE/ICESS.* IEEE, 2017, pp. 1049–1055.

[27] S. Murali and A. Jamalipour, "A lightweight intrusion detection for sybil attack under mobile rpl in the internet of things," *IEEE Internet of Things Journal*, 2019.

[28] 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.

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

[30] B. Groves and C. Pu, "A gini index-based countermeasure against sybil attack in the internet of things," in *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM).* IEEE, 2019, pp. 1–6.

[31] C. Pu, "Sybil attack in rpl-based internet of things: Analysis and defenses," *IEEE Internet of Things Journal*, 2020.

[32] C. Mauro, K. Pallavi, M. M. Rabbani, and S. Ranise, "Split: A secure and scalable rpl routing protocol for internet of things," 2018.

[33] 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.

[34] H. Perrey, M. Landsmann, O. Ugus, M. Wählisch, and T. C. Schmidt, "Trail: Topology authentication in rpl," in *Proceedings of the 2016 International Conference on Embedded Wireless Systems and Networks.* Junction Publishing, 2016, pp. 59–64.

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

[36] D. Airehrour, J. Gutierrez, and S. K. Ray, "Securing rpl routing protocol from blackhole attacks using a trust-based mechanism," in *2016 26th International Telecommunication Networks and Applications Conference (ITNAC).* IEEE, 2016, pp. 115–120.

[37] Z. A. Khan and P. Herrmann, "A trust based distributed intrusion detection mechanism for internet of things," in *2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA).* IEEE, 2017, pp. 1169–1176.

[38] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for internet of things," in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM).* IEEE, 2015, pp. 606–611.

[39] M. Surendar and A. Umamakeswari, "Indres: An intrusion detection and response system for internet of things with 6LoWPAN," in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET).* IEEE, 2016, pp. 1903–1908.

[40] T. T. Miao, R. T. Chekka, and K.-H. Kim, "Gidps: A game theory-based idps for rpl-networked low power lossy networks with energy limitation," *2014 Sixth International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 278–283, 2014.

[41] A. Dvir, L. Buttyan *et al.*, "Vera-version number and rank authentication in rpl," in *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems.* IEEE, 2011, pp. 709–714.

[42] 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 *2015 21st Asia-Pacific Conference on Communications (APCC).* IEEE, 2015, pp. 299–303.

[43] 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).* IEEE, 2016, pp. 1–7.

[44] S. Shukla, S. Singh, A. Kumar, and R. Matam, "Defending against increased rank attack on rpl in low-power wireless networks," in *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC).* IEEE, 2018, pp. 246–251.

[45] 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.

[46] V. Kiran, S. Rani, and P. Singh, "Towards a light weight routing security in iot using non-cooperative game models and dempster–shaffer theory," *Wireless Personal Communications*, pp. 1–21, 2019.

[47] J. Kaur, "A ultimate approach of mitigating attacks in rpl based low power lossy networks," *arXiv preprint arXiv:1910.13435*, 2019.

[48] 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, 2017.

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

[50] A. Arış, S. B. Ö. Yalçın, and S. F. Oktuğ, "New lightweight mitigation techniques for rpl version number attacks," *Ad Hoc Networks*, vol. 85, pp. 81–91, 2019.

[51] D. Shreenivas, S. Raza, and T. Voigt, "Intrusion detection in the rpl-connected 6LoWPAN networks," in *Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security.* ACM, 2017, pp. 31–38.

[52] A. Thomas, T. G. Kumar, and A. K. Mohan, "Neighbor attack detection in internet of things," in *Advanced Computational and Communication Paradigms.* Springer, 2018, pp. 187–196.

[53] A. Sehgal, A. Mayzaud, R. Badonnel, I. Chrisment, and J. Schönwälder, "Addressing dodag inconsistency attacks in rpl networks," in *2014 Global Information Infrastructure and Networking Symposium (GIIS).* IEEE, 2014, pp. 1–8.

[54] 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, 2015.

[55] R. Stephen and L. Arockiam, "E2v: Techniques for detecting and mitigating rank inconsistency attack (rina) in rpl based internet of things," in *Journal of Physics: Conference Series*, vol. 1142, no. 1. IOP Publishing, 2018, p. 012009.

[56] L. K. Bysani and A. K. Turuk, "A survey on selective forwarding attack in wireless sensor networks," in *2011 International Conference on Devices and Communications (ICDeCom).* IEEE, 2011, pp. 1–5.

[57] N. Djedjig, D. Tandjaoui, and F. Medjek, “Trust-based rpl for the internet of things,” in *2015 IEEE Symposium on Computers and Communication (ISCC).* IEEE, 2015, pp. 962–967.

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

[59] L. Patra and U. P. Rao, “Internet of things—architecture, applications, security and other major challenges,” in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom).* IEEE, 2016, pp. 1201–1206.

[60] K. Heurtefeux, O. Erdene-Ochir, N. Mohsin, and H. Menouar, “Enhancing rpl resilience against routing layer insider attacks,” in *2015 IEEE 29th International Conference on Advanced Information Networking and Applications.* IEEE, 2015, pp. 802–807.

[61] S. Suhail, S. R. Pandey, and C. S. Hong, “Detection of selective forwarding attack in rpl-based internet of things through provenance,” *Journal of Korean Information Science Society*, pp. 965–967, 2018.

[62] F. Gara, L. B. Saad, and R. B. Ayed, “An intrusion detection system for selective forwarding attack in ipv6-based mobile wsns,” in *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC).* IEEE, 2017, pp. 276–281.

[63] V. Neerugatti and A. R. M. Reddy, “Artificial intelligence-based technique for detection of selective forwarding attack in rpl-based internet of things networks,” in *Emerging Research in Data Engineering Systems and Computer Communications.* Springer, 2020, pp. 67–77.

[64] K. Weekly and K. Pister, “Evaluating sinkhole defense techniques in rpl networks,” in *2012 20th IEEE International Conference on Network Protocols (ICNP).* IEEE, 2012, pp. 1–6.

[65] N. Bhalaji, K. Hariharasudan, and K. Aashika, “A trust based mechanism to combat blackhole attack in rpl protocol,” in *International Conference on Intelligent Computing and Communication Technologies.* Springer, 2019, pp. 457–464.

[66] D. Airehrour, J. Ray, and S. K. Ray, “A trust-aware rpl routing protocol to detect blackhole and selective forwarding attacks,” 2017.

[67] D. Airehrour, J. Gutierrez, S. K. Ray *et al.*, “A trust-based defence scheme for mitigating blackhole and selective forwarding attacks in the rpl routing protocol,” *Australian Journal of Telecommunications and the Digital Economy*, vol. 6, no. 1, p. 41, 2018.

[68] H. B. Patel and D. C. Jinwala, “Blackhole detection in 6LoWPAN based internet of things: an anomaly based approach,” in *TENCON 2019-2019 IEEE Region 10 Conference (TENCON).* IEEE, 2019, pp. 947–954.

[69] F. Ahmed and Y.-B. Ko, “Mitigation of black hole attacks in routing protocol for low power and lossy networks,” *Security and Communication Networks*, vol. 9, no. 18, pp. 5143–5154, 2016.

[70] S. M. H. Mirshahjafari and B. S. Ghahfarokhi, “Sinkhole+ cloneid: A hybrid attack on rpl performance and detection method,” *Information Security Journal: A Global Perspective*, vol. 28, no. 4-5, pp. 107–119, 2019.

[71] V. Neerugatti, A. R. M. Reddy, and A. Rama, “Detection and prevention of black hole attack in rpl protocol based on the threshold value of nodes in the internet of things networks,” *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 8.,2019

[72] S. Luangoudom, D. Tran, T. Nguyen, H. A. Tran, G. Nguyen, and Q. T. Ha, “svblock: mitigating black hole attack in low-power and lossy networks,” *International Journal of Sensor Networks*, vol. 32, no. 2, pp. 77–86, 2020.

[73] P. Nagrath and B. Gupta, “Wormhole attacks in wireless adhoc networks and their counter measurements: A survey,” in *2011 3rd International Conference on Electronics Computer Technology*, vol. 6. IEEE, 2011, pp. 245–250.

[74] S. Mukherjee, M. Chattopadhyay, S. Chattopadhyay, and P. Kar, “Wormhole detection based on ordinal mds using rtt in wireless sensor network,” *Journal of Computer Networks and Communications*, vol. 2016, 2016.

[75] V. K. Raju and K. V. Kumar, “A simple and efficient mechanism to detect and avoid wormhole attacks in mobile ad hoc networks,” in *2012 International Conference on Computing Sciences.* IEEE, 2012, pp. 271–275.

[76] 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, 2015.

[77] F. I. Khan, T. Shon, T. Lee, and K. Kim, “Wormhole attack prevention mechanism for rpl based lln network,” in *2013 Fifth International Conference on Ubiquitous and Future Networks (ICUFN).* IEEE, 2013, pp. 149–154.

[78] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Packet leashes: A defense against wormhole attacks in wireless ad hoc networks,” in *Proceedings of INFOCOM*, vol. 2003, 2003.

[79] 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.

[80] P. Kaliyar, W. B. Jaballah, M. Conti, and C. Lal, “Lidl: Localization with early detection of sybil and wormhole attacks in iot networks,” *Computers & Security*, p. 101849, 2020.

[81] C. Pu, “Mitigating dao inconsistency attack in rpl-based low power and lossy networks,” in *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC).* IEEE, 2018, pp. 570–574.

[82] K. Gaurav, ““Programming Internet of Things using Contiki and Cooja,” June 2017. [Online]. Available: https://www.opensourceforu.com/2017/06/programming-internet-things-using-contiki-cooja/ [Accessed on 25.07.2021]

[83] Fredrik Österlind, ""A Sensor Network Simulator for the Contiki OS," Feb 2006. [Online]. Available: https://core.ac.uk/download/pdf/300993645.pdf [Accessed on 25.07.2021]

[84] S. Kim, H.-S. Kim, and C. Kim, "Alice: Autonomous link-based cell scheduling for tsch," in *Proceedings of the 18th International Conference on Information Processing in Sensor Networks*, 2019, pp. 121–132.

[85] S. Kim, H.-S. Kim, and C.-k. Kim, "A3: Adaptive autonomous allocation of tsch slots," in *Proceedings of the 20th International Conference on Information Processing in Sensor Networks (co-located with CPS-IoT Week 2021)*, 2021, pp. 299–314.

[86] H.-S. Kim, J. Paek, D. E. Culler, and S. Bahk, "Pc-rpl: Joint control of routing topology and transmission power in real low-power and lossy networks," *ACM Trans. Sen. Netw.*, vol. 16, no. 2, Mar. 2020. [Online]. Available: https://doi.org/10.1145/3372026

[87] H.-S. Kim, J. Paek, and S. Bahk, "Transmission power control in ipv6 routing protocol for low-power wireless network: Poster abstract," in *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*, ser. SenSys '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 334–335. [Online]. Available: https://doi.org/10.1145/2994551.2996693

[88] X. Liu, Z. Sheng, C. Yin, F. Ali, and D. Roggen, "Performance analysis of routing protocol for low power and lossy networks (rpl) in large scale networks," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2172–2185, 2017.

[89] A. Abdou, A. Matrawy, and P. C. Van Oorschot, "Accurate manipulation of delay-based internet geolocation," in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 2017, pp. 887–898.

[90] A. Abdou, A. Matrawy, and P. C. Van Oorschot, "Cpv: Delay-based location verification for the internet," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 2, pp. 130–144, 2015.

[91] M. Conti, P. Kaliyar, and C. Lal, "Remi: a reliable and secure multicast routing protocol for iot networks," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 2017, pp. 1–8.

[92] P. Thubert, ""rpl-bier," internet engineering task force, internet-draft draft-thubert-roll-bier-01," Jan 2018. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-thubert-roll-bier-00 [Accessed on 05.09.2020]

[93] O. Bergmann, C. Bormann, S. Gerdes, and H. Chen, "Constrained- cast: Source-routed multicast for rpl," internet engineering task force, internet draft draft-ietf-roll-ccast-01," Oct 2017. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-roll-ccast-01 [Accessed on 05.09.2020]

[94] J. Hui and R. Kelsey, "Multicast protocol for low-power and lossy networks (mpl)," rfc 7731," Feb 2016. [Online]. Available: https://rfc-editor.org/rfc/rfc7731.txt [Accessed on 07.09.2020]

[95] V. K. Asati, E. S. Pilli, S. K. Vipparthi, S. Garg, S. Singhal, and S. Pancholi, "Rmdd: Cross layer attack in internet of things," in *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. IEEE, 2018, pp. 172–178.

[96] M. Conti, P. Kaliyar, and C. Lal, "A robust multicast communication protocol for low power and lossy networks," *Journal of Network and Computer Applications*, vol. 164, p. 102675, 2020.

[97] M. Shafiq, H. Ashraf, A. Ullah, M. Masud, M. Azeem, N. Jhanjhi, and M. Humayun, "Robust cluster-based routing protocol for iot-assisted smart devices in wsn," *CMC-COMPUTERS MATERIALS & CONTINUA*, vol. 67, no. 3, pp. 3505–3521, 2021.

[98] M. Zhao, H. Y. Shwe, and P. H. J. Chong, "Cluster-parent based rpl for low-power and lossy networks in building environment," in *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*. IEEE, 2015, pp. 779–784.

[99] S. Sankar, S. Ramasubbareddy, A. K. Luhach, A. Nayyar, and B. Qureshi, "Ct-rpl: Cluster tree based routing protocol to maximize the lifetime of internet of things," *Sensors*, vol. 20, no. 20, p. 5858, 2020.

[100] X. Vilajosana, T. Watteyne, T. Chang, M. Vučinić, S. Duquennoy, and P. Thubert, "Ietf 6tisch: A tutorial," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 595–615, 2019.

[101] A. I. Sabbah, A. El-Mougy, and M. Ibnkahla, "A survey of networking challenges and routing protocols in smart grids," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 210–221, 2013.

[102] A. A. Khan, M. H. Rehmani, and M. Reisslein, "Requirements, design challenges, and review of routing and mac protocols for cr-based smart grid systems," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 206–215, 2017.

[103] J. R. Renofio, M. E. Pellenz, E. Jamhour, A. Santin, M. C. Penna, and R. D. Souza, "On the dynamics of the rpl protocol in ami networks under jamming attacks," in *2016 IEEE International Conference on Communications (ICC)*. IEEE, 2016, pp. 1–6.

[104] R. Bruzgiene, L. Narbutaite, and T. Adomkus, "Manet network in internet of things system," *Ad Hoc Networks*, pp. 89–114, 2017.

[105] "Telosb cm5000 mote module1." [Online]. Available: https://www. advanticsys.com/shop/mtmcm5000msp-p-14.html [Accessed on 10.09.2020]

[106] "Zolertia z1 mote module." [Online]. Available: https://zolertia.iol [Accessed on 10.09.2020]

[107] "Cortex-m3 processor." [Online]. Available: https://developer.arm.com/ products/processors/cortex-m/cortex-m3 [Accessed on 10.09.2020]