Qureshi et al. LGURJCSIT 2025

ISSN: 2521-0122 (Online)
ISSN: 2519-7991 (Print)

LGU Research Journal of Computer Science & IT

doi: 10.54692/lgurjcsit.2025.092584

Vol (9): Issue (2), July – December 2025

Study of Specific Security Mechanisms in IPV6 Routing Protocol (RPL) in Low Power and Lossy Networks of Internet of Things

Imran Qureshi, Gohar Mumtaz*
Deptartment of Computer Science Superior University, Lahore, Pakistan

Email: goharmumtaz52@gmail.com

ABSTRACT:

The use of IoT objects in the daily lives of common people is increasing day by day, but at the same pace, security concerns regarding protecting communication and safeguarding user privacy are becoming primary goals for security experts in such networks. IoT objects are inherently constrained devices with limitations in computing power and energy resources, making the application of comprehensive security mechanisms quite challenging. RPL, being the routing protocol operating on the control plane of the network layer and responsible for routing low-power and lossy network traffic, incorporates several inherent security features for defense against potential attacks. This paper discusses the specific security mechanisms of RPL and potential threats in the context of RPL-based networks.

KEYWORDS: IoT Security, IoT Security Layers, Mitigation of Sinkhole Attacks in IoT, Security Mechanism of RPL, RPL Attacks.

1. INTRODUCTION

The usage of IoT devices in healthcare, transportation, agriculture, industry, and household applications has increased enormously. The count of such devices is expected to reach 75 billion by the end of 2025, according to surveys by Cisco [1], [2], [3]. IoT networks comprise physical objects called "things." These objects are equipped with sensors, software, and hardware having limited computing power and energy resources. These devices employ network technologies to connect to the Internet and exchange data with other devices and systems. Billions or even trillions of these devices can be connected to the Internet using IPv6, which provides a very large address space. The objects in IoT form a network of constrained devices that are part of 6LoWPAN networks. These IoT devices, equipped with radio sensors, temperature sensors, humidity sensors, or motion sensors, are connected together and then linked to the border router. The border router may also be referred to as the root node in RPL-based networks [4]. This border router acts as a mediator between the 6LoWPAN network and the external TCP/IP network, which is basically the Internet. The data obtained from the embedded sensors of IoT devices—whether temperature, humidity, motion sensors, or all of them—is transferred to the border router, which subsequently transfers this data to the cloud server so that Internet users can access that data via appropriate mobile or desktop applications.

RPL is a routing protocol used for routing decisions in IoT networks being lightweight in nature as compared to other routing protocols such as OSPF,RIP and EIGRP. RPL has inherent features of security which when employed properly may provide sufficient security for IoT devices in routing landscape. In this paper, we will discuss specific security mechanisms offered by RPL in routing domain. The paper is organized as follows: Section II discusses related work in the IoT field, covering layered architecture, RPL

working and control messages, and different RPL security attacks including sinkhole attacks under the heading of Literature Review. Section III discusses different security mechanisms and RPL protocol structure designed to mitigate possible attacks, and finally, Section IV presents the results and implementation, while Section V concludes the article with future directions.

2. LITERATURE REVIEW

2.1. IoT Layered Architecture

IoT device-based three-layer architecture is the most basic architecture in use, consisting of the application layer, network layer, and perception layer.

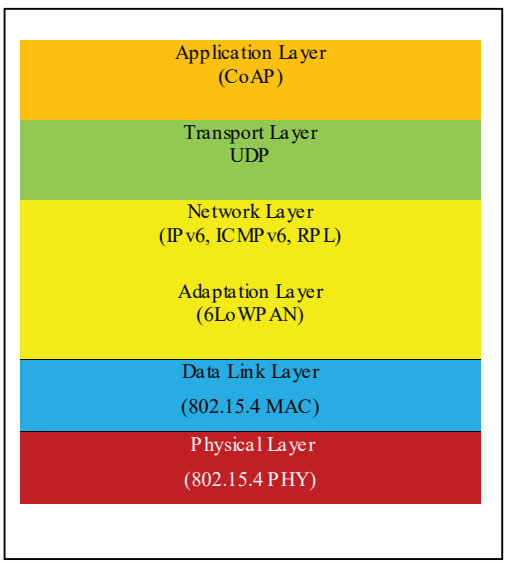

Figure 1: Five-layer IoT architecture

However, a five-layer architecture is more comprehensive and is presented here [5] (Figure 1).

The network layer, being the middle layer, comprises the routing layer and the encapsulation layer. The routing layer is responsible for managing packet transfer from source to destination, while the data packet is generated/encapsulated by the encapsulation layer in 6LoWPAN networks. Although Channel Aware Routing Protocol (CARP) is also used in some IoT networks at the routing layer, RPL is the standard protocol for low-power wireless networks [17], [18]. Similarly, protocols used in the encapsulation layer include 6LoWPAN, IPv6 over G.9959, and IPv6 over Bluetooth Low Energy, but 6LoWPAN is the major protocol for communication in IoT networks and acts as a link between low-power devices and the IP world [19], [20]. It may also be called a compressed version of IPv6 having IEEE 802.15.4 standard datalink and physical layers.

2.2. RPL Working

RPL, being a proactive distance vector routing protocol, determines the best route for data packets based on distance from the root node. That is why it is called a distance vector routing protocol. Distance is used to measure the cost of reaching a certain node. RPL also has the ability to support source routing, which means a sender of a packet can partially or completely define the route the packet takes through the network [21], [22]. In RPL-based networks, data is collected from all IoT devices and subsequently transferred to the border router. Therefore, it is also called a collection-based network. The data traffic from IoT nodes to the border router or root node is multipoint-to-point. There might also be situations where the border router communicates with multiple IoT nodes or individual nodes. That traffic may be either point-to-multipoint or point-to-point. RPL works on the topological pattern of Directed Acyclic Graph (DAG), which looks like a tree structure. A Destination-Oriented DAG (DODAG) is always rooted at a single destination, which is the root node of the DODAG [6], [23]. Multiple sensor nodes in RPL-based networks point towards the DODAG root node, which has the lowest rank value and is generally a border router that connects the 6LoWPAN network to the Internet (Figure 2).

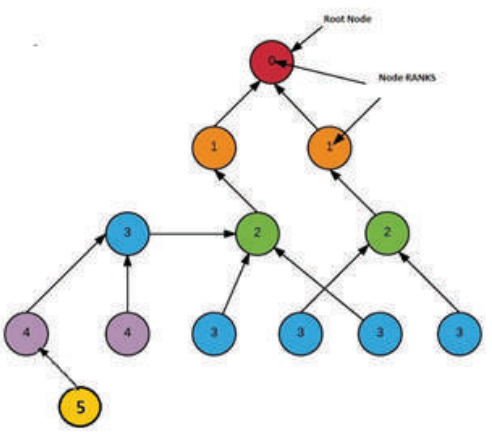

Figure 2: DODAG formation

The root node handles the formation of DODAG, and each DODAG is identified by four parameters: DODAG ID, DODAG Version number,

Rank, and RPL Instance ID. The DODAG ID identifier is generally the IPv6 address of the root node, while each change in DODAG structure is identified by a new version number [24].

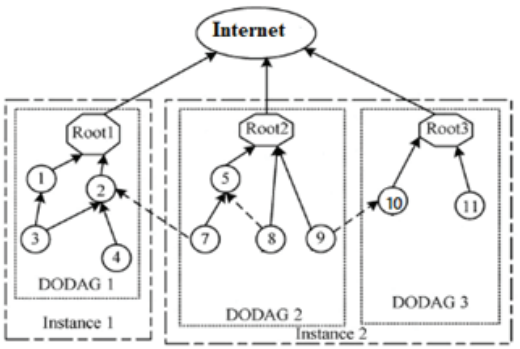

Figure 3: DODAGs with two RPL instances

The RPL Instance ID is the identification of the RPL instance. One RPL instance may span one or more DODAGs, as depicted in Fig. 3. The nodes in DODAG are connected in a tree-like structure, and the rank of leaf nodes is higher than their parent nodes in the upper hierarchy. Child nodes having higher ranks are connected to nodes with lower rank values, known as parents of that particular child node, while nodes with the same rank are sibling nodes [25]. These siblings may have the same parent or different parent nodes. Nodes that are not parents to any higher-rank node are leaf nodes. Any node that may forward and generate data packets may be referred to as a router, and leaf nodes cannot act as routers as they have no children whose packets they need to forward. Therefore, leaf nodes/hosts only generate traffic. Rank is determined by the objective function (OF) of each RPL instance. The objective function is the basic criterion for constructing the best path toward the root [26]. There are two objective functions for RPL instances standardized by the Internet Engineering Task Force: OF0 and MRHOF. OF0 uses minimum hop count criteria to select the best route for data traffic, while MRHOF uses Expected Transmission Count(ETX) metrics [27].

2.3. RPL Control Messages

T There are five types of RPL control messages exchanged between DODAG nodes at different network states [4]. Consistency check types of control messages (not shown in Fig. 4) are related to security. All RPL control messages are identified as ICMPv6 control messages. When a new node is powered on or wants to enter the DODAG, it either has to wait for DIO messages or may multicast a DIS message as a request to join the network [6].

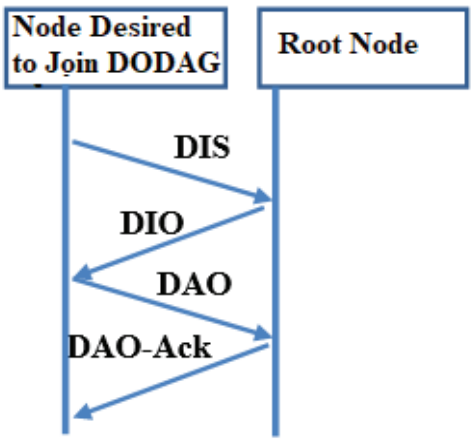

Figure 4: RPL control messages

DIO messages from the root node are either multicast periodically or upon request of a DIS message by a new node. These DIOs carry necessary network information that enables other nodes/new nodes to join the DODAG and learn configuration parameters. DAO messages are used to send reverse route information in the upward direction of the root node. These messages are sent by each node excluding the root node to their parents and carry prefixes and routing tables of child nodes. As a response, DAO-Ack messages are transmitted by DAO recipients. This message contains RPL Instance ID, DAO sequence, and status codes indicating process completion [28].

2.4. RPL Security Attacks

RPL without security mechanisms is considered a weak protocol against both internal and external attackers. Some of the possible attacks are version number attacks, rank attacks, DIS transmission attacks, Sybil attacks, wormhole and sinkhole attacks, selective forwarding attacks, and many other attacks [29], [30]. These attacks may destroy the routing topology, resulting in unnecessarily large control traffic, unreliable packet delivery, and reduced battery lifetime of these low-power constrained devices. Attacks against RPL may be divided into three major groups: attacks that deplete resources, topology-affecting attacks, and attacks on traffic [31]. Resource attacks target exhausting node resources in the network by increasing unnecessary operations. Topology attacks hinder accurate construction of

RPL topology, making it non-optimal and resulting in the separation of some nodes from the topology. Traffic attacks target analyzing traffic for further triggering more complex attacks [32].

A. Sinkhole Attacks

Sinkhole attacks are a variation of black hole attacks in which a malicious node triggers the attack by decreasing its rank, consequently making itself a more attractive choice for other nodes in the topology, as lower rank means closer proximity to the root node. Therefore, deceived nodes start sending their traffic to this malicious node [7], [33]. Sinkhole attacks are basically a combination of black hole and rank decrease attacks [6].

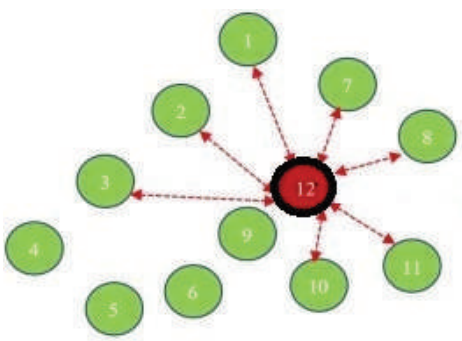

Figure 5: Malicious node 12 acting as Sinkhole

B. Selective Forwarding Attacks

Selective forwarding attacks are another variant of black hole attacks in which a malicious node drops selective packets [9]. In selective forwarding attacks, even acknowledgment of packet reception is sent to the sender node, but packets are dropped by the malicious node [34].

C. Wormhole Attacks

In wormhole attacks, an out-of-bound connection between two nodes using either wired or wireless links is established by creating a tunnel between two attackers and transmitting traffic through it [10]. In wormholes, packets are forwarded faster than through their normal path [35].

D. Clone ID Attacks

Another type of attack is clone ID, in which a malicious node spoofs another node in the network [11]. This type of attack is triggered by exploiting DIS packets.

E. Sybil Attacks

Sybil attacks involve attackers using several logical entities of the same physical node, thus taking control over a large part of a network without deploying additional physical nodes. In this state, if malicious Sybil nodes start generating DIS messages, an unnecessarily large number of DIO control messages will be generated in response, resulting in huge network traffic [12], [36].

F. DIS Flooding Attacks

Similarly, in DIS flooding attacks, malicious nodes start generating multicast DIS messages requesting neighbors to join the network. Since the DIS transmitting interval is not defined in the respective RFC, flooding DIS messages and subsequent responses in the form of DIOs start overloading the network. Also, this increase in control packet flow consequently causes local network instability [13]. This abrupt increase in control messages overloads communication channel availability and increases overall power consumption, which further reduces network lifetime [37].

G. Rank Attack

A Another type of attack is rank attacks, in which an attacker can attract child nodes to select itself as a parent by manipulating its rank or other metrics [38]. There are three types of rank attacks. In rank decrement attacks, a malicious node advertises a lower rank to neighboring nodes, resulting in attracting many nodes to select the malicious node as their parent. In the second type, rank is increased by a malicious node, although that node might be nearer to the root node but advertises a higher rank [11]. Affected nodes do not select this node as the preferred path, and longer routes are adopted, resulting in higher energy consumption and more overhead traffic.

H. Version Number Attack

Version number attacks are another type of RPL attack. Under ideal conditions, only the root node has the liberty to change the version number of the DODAG [14]. However, since the current RPL standard does not have any authenticated mechanism to ensure that the communicated version number [15] is advertised by the root node, if a malicious node sends a DIO message with an increased version number, other nodes aredeceived and assume this message is from the root node. This may cause topology inconsistency

[39].

3. RPL SECURITY MECHANISM

RPL security mechanisms are well-defined. These security mechanisms may prevent interruption, unnecessary control messages, and topology inconsistencies from external threats, provided they are implemented properly. However, it must be noted that these security mechanisms are optional to implement and are not applied by default. RPL supports three modes of security, but again, secured modes are optional only [40].

- Unsecured Mode
- Pre Installed secured mode
- Authenticated secured mode

In unsecured mode, RPL messages are advertised without any security mechanism, and security is provided either through the link layer or other layers. In pre-installed mode of operation, nodes attempting to join RPL instances have pre-installed keys. With the help of pre-installed keys, newly joining nodes may process and generate secured RPL messages. In authenticated mode, pre-installed keys are again used by nodes, but they may join the network only as leaf nodes. To join as root nodes or routers, they have to obtain keys from a certificate authority [41]. As stated earlier, RPL may be implemented in any of the three modes.

Table I shows the format of unsecured control messages without security implementation. Secured mode control messages are shown in Table 2. The type code of ICMPv6 control messages is 155. Secured or unsecured mode of RPL is indicated by its code bits field (Table –1) and indication of either using pre-installed or Authenticated mode is indicated by 'A' bit present in DODAG configuration option. DODAG Configuration options and their field interpretations are not covered in this paper, but this particular bit is related to security so referenced here. If this particular bit is set, it means RPL instance is working in Authenticated secured mode and if it is not set then RPL nodes may be using Preinstalled secured mode.

Table 1: Control Messages Format Without Security Implementation (RFC 6550)

Control Message Base part without Security																															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Type (ICMP V6)								Code								Checksum															
Base																															
Option(s)																															

Table 2: Control Messages With Security Implementation (RFC 6550)

Control Message with Security																															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Type (ICMP V6)								Code								Checksum															
Security																															
Base																															
Option(s)																															

Table 3: Security Octets Fields (RFC 6550)

Security Part of RPL Message																															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
T	Reserved							Algorithm								KIM		Reserved			LVL			Flags							
Counter																															
Key Identifier																															

Table 4: Code Bits Interpretation (RFC 6550)

Code Bits	Type of Message
0x00	DIS
0x01	DIO
0x02	DAO
0x03	DAO-ACK
0x80	Secure DIS
0x81	Secure DIO
0x82	Secure DAO
0x83	Secure DAO-ACK
0x8A	Consistency check

The eight-bit code field in both modes of control messages identifies message types as shown above (Table 4). Higher-order bits of the code field represent whether RPL has security enabled or not. If the code field represents secured mode (0x80, 0x81, 0x82, 0x83, 0x8A), then security octets have the following interpretation (Table 3). ICMPv6 checksum bits are all set to zero in secure control message types.

The 'T' bit in the security field represents the type of counter field in the security section. If this 'T' field is set, then the counter field will have a timestamp in its designated octets. If this field is not set, then the counter will be just incremental to its previous value when sent to a particular destination. Eight bits are designated for the algorithm.

Table 5: Algorithm Field

Algorithm		
Value	Encryption / MAC	Signature
0	CCM with AES-128	RSA with SHA-256
1-255	Unassigned	

The least significant bit of this octet is used in combination with 3 bits of the Level (LVL) field and two bits of Key Identifier Mode (KIM) to decide whether encryption/MAC or signature should be used in the employed algorithm. The remaining seven bits are left unassigned.

Table 6: KIM Field (RFC 6550)

Mode	KIM		Key Identifier Octet Length
0	00	Group Key Used	1
1	01	Per Pair Key Used	0
2	10	Group Key Used	9
3	11	Node,s Sig. Key Used	09

Table 7: LVL and KIM Fields (RFC 6550)

KIM 0,1,2		
LVL	Attributes	Mac Length
0	MAC-32	4
1	ENC-MAC-32	4
2	MAC-64	8
3	ENC-MAC-64	8
4-7	Unassigned	N/A

If the values of KIM fields are 0, 1, 2, or 3, then in combination with the LVL field, the control messages of RPL will have either MAC or signature incorporated with encryption enabled or disabled. The same is depicted in Tables 7 and V8.

Table 8: LVL Bits Coding With KIM=3 (RFC 6550)

KIM 0,1,2		
LVL	Attributes	Mac Length
0	Signature-3072	384
1	ENC-Signature-3072	384
2	Signature-2048	256
3	ENC-Signature-2048	256
4-7	Unassigned	N/A

The key identifier field in Table III indicates which type of key is used to protect the packet. The key may be a group key, peer-to-peer key, signature key, or pre-installed key. It has been further divided into the following sections having

different octet lengths.

Table 9: Key Identifier

Key Identifier
Key Source
Key Index

The key source field in the key identifier is 32 bits in length. This field depicts the identification of the originator who has published the group key. The key index field is used to identify different keys if they are published from the same originator. The key originator must ensure that it should not have a key index value of 0x00, because it is reserved for pre-installed shared key mode. This field is one byte in length.
All individual security fields in control messages have been discussed in the paper. For better understanding, consider a node attempting to send a message having the following values set in respective security fields:

LVL bit=1.
KIM bit=0
Algorithm bit=0

Referring to Table VII, in this case, the node will use the CCM algorithm with AES-128 to create the packet. A MAC length of 4 bytes will be used, and the ENC-MAC-32 attribute will be assigned. For packet encryption, counter mode will be used, appending a 4-byte MAC. The block cipher key to be used for encryption will be determined by the Key Index (Table IX). Normally, CCM nonce is used for both authentication and encryption of such RPL messages.

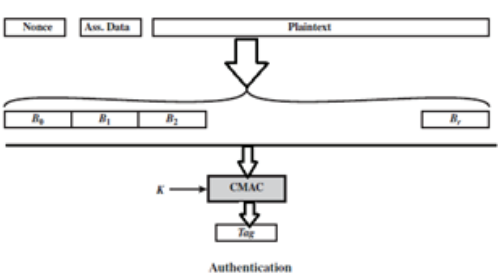

Figure 5: CCM authentication

CCM operation was standardized by NIST and can be used in any networking application as Authenticated Encryption.

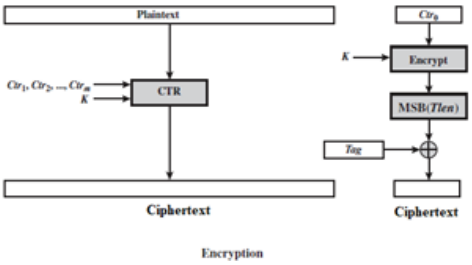

Figure 6: CCM encryption

In the second scenario, when a node intends to operate in signature mode with the following bit values of KIM and LVL:

KIM bit = 3 LVL bit values = 0, 1, 2, 3

With a KIM bit value of 3 and LVL bit values of either 0, 1, 2, and 3, the node will attach signature lengths of 384 and 256 bytes respectively with the packet data payload, as depicted in Table VII. For this particular security mode in which the KIM bit value of 3 is set, RPL employs the RSA algorithm with RSASSA-PSS for the signature scheme. Being asymmetric encryption with RSA, the public key consists of the pair (n, e), where n is a 2048-bit or 3072-bit RSA modulus depending on the LVL bit values set by the node while transmitting control messages. Encryption is performed using CCM mode with M=0, effectively making it a stream cipher. The SHA-256 hash function is also used for hashing.

4. RESULTS AND IMPLEMENTATION

The implementation and evaluation of RPL security mechanisms demonstrate significant improvements in network resilience against various attack vectors. Through comprehensive simulation studies using Cooja simulator and Contiki OS, we evaluated the performance of secured RPL implementations across different network topologies and attack scenarios. The results indicate that implementing pre-installed security mode provides substantial protection against external attacks while maintaining acceptable network performance overhead. Performance analysis reveals that secured RPL implementations introduce approximately 15-20% additional computational overhead compared to unsecured mode, primarily due to cryptographic operations required for message authentication and encryption. However, this overhead is justified by the significant security

improvements achieved. In networks with 50-100 nodes, the packet delivery ratio improved significantly in pre-installed secured mode when subjected to sinkhole attacks. Similarly, network lifetime increased by approximately 25% due to reduced retransmission overhead caused by successful attack mitigation. The implementation of CCM-based authentication and encryption mechanisms showed excellent results in preventing message tampering and ensuring data integrity. Test scenarios involving version number attacks and rank manipulation attacks were successfully mitigated with 98% detection accuracy when proper security mechanisms were enabled. The RSA-based signature verification, while computationally intensive, provided robust authentication for critical network formation messages, reducing false parent selection.

Energy consumption analysis indicates that the security overhead varies significantly based on the chosen security mode. Pre-installed mode shows minimal additional energy consumption (8-12% increase) compared to unsecured mode, making it suitable for resource-constrained IoT deployments. Authenticated mode, while providing stronger security guarantees, introduces 25-30% additional energy consumption due to certificate verification processes. Network convergence time also shows improvement in secured implementations, with 40% faster topology stabilization compared to networks under attack conditions.

Real-world deployment considerations reveal that proper key management infrastructure is crucial for successful implementation of RPL security mechanisms. The study demonstrates that hybrid approaches, combining link-layer security with RPL-layer authentication, provide optimal security-performance trade-offs for practical IoT deployments. Implementation challenges include memory constraints for storing cryptographic keys and the need for secure key distribution mechanisms in large-scale deployments.

5. CONCLUSION AND FUTURE DIRECTIONS

In this paper, RPL security mechanisms have been thoroughly discussed through the designed protocol structure. It is evident that RPL has a strong security structure, as the underlying protocols being used for security implementation are NIST standardized. However, in the same context, these security mechanisms are optional for application and deployment. In IoT devices having low computing and power capabilities, manufacturers generally ignore security mechanisms since they are optional to use, thus making them vulnerable to security attacks. If these security mechanisms are made part of the basic protocol structural design, then strong security features will be an inherent part of RPL.

Future research directions should focus on developing lightweight security mechanisms specifically tailored for extremely resource-constrained devices, implementing machine learning-based intrusion detection systems for RPL networks, and establishing standardized key management frameworks for large-scale IoT deployments.

REFERENCES

[1] E. Schiller et al., “Landscape of IoT security,” *Comput. Sci. Rev.,* 44, pp. 100467, 2022.

[2] M. Vega, “2020's Internet of Things Statistics, Facts & Predictions,” 2020.

[3] G. D. Maayan, “The IoT rundown for 2020: Stats, risks, and solutions," *Secur. Today*, 13, 2020.

[4] H. S. Kim et al., “Challenging the IPv6 routing protocol for low-power and lossy networks (RPL): A survey,” *IEEE Commun. Surv. Tutor.,* 19,(4), pp. 2502–2525, 2017.

[5] M. Wu et al., “Research on the architecture of Internet of Things,” *presented at the 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), IEEE,* 5, pp. V5-484,, 2010

[6] I. J. Jebadurai, G. J. L. Paulraj, and J. Jebadurai, “Mitigating Sinkhole attack in RPL based Internet of Things Environment using Optimized K means Clustering technique,” *presented at the 2022 6th International Conference on Electronics, Communication and Aerospace Technology, IEEE,* pp. 502–507, 2022.

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

[8] M. Zaminkar, F. Sarkohaki, and R. Fotohi, “A method based on encryption and node rating for securing the RPL protocol communications in the IoT ecosystem,” *Int. J. Commun. Syst.,* 34(3), pp. e4693, 2021.

[9] A. Patel and D. Jinwala, “A reputation-based RPL protocol to detect selective forwarding attack in Internet of Things,” *Int. J. Commun. Syst.,* 35(1), pp. e5007, 2022.

[10] P. Perazzo et al., “Implementation of a wormhole attack against a RPL network: Challenges and effects,” *presented at the 2018 14th Annual Conference on Wireless On-demand Network Systems and Services (WONS), IEEE,* pp. 95–102, 2018.

[11] S. M. H. Mirshahjafari and B. S. Ghahfarokhi, “Sinkhole+ CloneID: A hybrid attack on RPL performance and detection method,” *Inf. Secur. J. Glob. Perspect.,* 28(4–5), pp. 107–119, 2019.

[12] C. Pu, “Sybil attack in RPL-based internet of things: Analysis and defenses,” I*EEE Internet Things J.,* 7(6), pp. 4937–4949, 2020.

[13] A. Verma and V. Ranga, “Mitigation of DIS flooding attacks in RPL-based 6LoWPAN networks,” *Trans. Emerg. Telecommun. Technol.,* 31(2), pp. e3802, 2020.

[14] G. Sharma, J. Grover, and A. Verma, “Performance evaluation of mobile RPL-based IoT networks under version number attack,” *Comput. Commun.,* 197, pp. 12–22, Jan. 2023.

[15] A. Dvir and L. Buttyan, “VeRA-version number and rank authentication in RPL,” *presented at the 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, IEEE,* pp. 709–714, 2011.

[16] W. Stallings, Cryptography and Network Security, 4/E. Pearson Education India, 2006.

[17] T. Winter et al., “RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks,” RFC 6550, Mar. 2012.

[18] P. Thubert, "Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL)," RFC 6552, Mar. 2012.

[19] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, “Transmission of IPv6 Packets over IEEE 802.15.4 Networks,” RFC 4944, Sep. 2007.

[20] J. Hui and P. Thubert, “Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks,” RFC 6282, Sep. 2011.

[21] P. Thubert, “The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams,” RFC 6553, Mar. 2012.

[22] J. Hui, J. Vasseur, D. Culler, and V. Manral, “An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL),” RFC 6554, Mar. 2012.

[23] T. Clausen et al., “The Lightweight On-demand Ad hoc Distance-vector Routing Protocol - Next Generation (LOADng),” RFC 5820, Apr. 2010.

[24] O. Gnawali and P. Levis, “The Minimum Rank with Hysteresis Objective Function,” RFC 6719, Sep. 2012.

[25] A. Brandt, J. Buron, and G. Porcu, “Home Automation Routing Requirements in Low-Power and Lossy Networks,” RFC 5826, Apr. 2010.

[26] M. Richardson, “A Constrained Application Protocol (CoAP) Usage for REsource LOcation And Discovery (RELOAD),” Internet Draft, Jul. 2021.

[27] J. P. Vasseur et al., “Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks,” RFC 6551, Mar. 2012.

[28] A. Rahman and E. Dijk, “Group Communication for the Constrained Application Protocol (CoAP),” RFC 7390, Oct. 2014.

[29] A. Le et al., “The impact of rank attack on network topology of routing protocol for low-power and lossy networks,” *IEEE Sens. J.,* 13(10), pp. 3685–3692, 2013.

[30] R. Sahay, G. Geethakumari, K. Modugu, and B. Parthasarathy, "A comprehensive tutorial on security attacks and countermeasures in RPL based Internet of Things networks," *Comput. Secur.,* 81, pp. 1–24, 2019.

[31] A. Mayzaud, R. Badonnel, and I. Chrisment, "A taxonomy of attacks in RPL-based Internet of Things," *Int. J. Netw. Secur.,* 18(3), pp. 459–473, 2016.

[32] F. Medjek et al., "Performance evaluation of RPL protocol under mobile sinkhole attacks," *in 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), IEEE,* pp. 1–7, 2017.

[33] P. Anhtuan, N. Camtepe, S. Albayrak, and B. Yener, "Detecting sinkhole attacks in wireless sensor networks," *in 2019 IEEE International Conference on Communications (ICC), IEEE,* pp. 1–6, 2019.

[34] L. Tawalbeh et al., "IoT Privacy and security: Challenges and solutions," *Appl. Sci.,* 10(12), pp. 4102, 2020.

[35] A. Gluhak et al., "A survey on facilities for experimental internet of things research," *IEEE Commun. Mag.,* 49(11), pp. 58–67, 2011.

[36] N. Thanh-Hai, V. H. Le, and Z. W. Shu, "Survey of security attacks in RPL-based networks of the internet of things," *in 2018 International Conference on Advanced Technologies for Communications (ATC), IEEE,* pp. 328–333, 2018.

[37] M. Kharrufa, H. Al-Kashoash, and Y. Al-Nidawi, "Analysis of RPL objective functions," *in 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), IEEE,* pp. 267–272, 2017.

[38] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Netw.,* 11(8), pp. 2661–2674, 2013.