International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

A Comparative Analysis of Attacks on RPL in Internet of Things Networks

Dr. Anjali Khokhar
Assistant professor, BITS Engineering college, Bhiwani
Email id -ashu.ishu34@gmail.com

Abstract- The Routing Protocol for Low-Power and Lossy Networks (RPL) is the standard routing protocol widely adopted in Internet of Things (IoT) and Wireless Sensor Network (WSN) environments. While RPL is a lightweight protocol offering efficient routing functionality, it provides only basic security mechanisms, which makes it susceptible to a variety of security attacks. Ensuring security in IoT networks is particularly challenging due to their resource-constrained nature and their direct connectivity to the largely unsecured Internet. This survey presents a comprehensive review of security issues associated with RPL, building upon existing research while addressing security challenges specific to IoT environments. The study proposes a classification of RPL attacks based on the fundamental security principles of Confidentiality, Integrity, and Availability (CIA). Additionally, the survey examines existing countermeasures for identified attacks and provides theoretical solutions, derived from the literature, for attacks that have not yet been thoroughly evaluated. The paper concludes by highlighting open research challenges and outlining future research directions necessary to enhance the security of RPL for Internet of Things applications.

Index Terms-Routing Protocol Security, Internet of Things, IoT, RPL, Low Power and Lossy Networks, LLNs

INTRODUCTION

Internet of Things (IoT) is an emerging technology that is swiftly changing the way businesses are conducted and the way society functions. This has heightened the need to integrate and handle the colossal quantities of information produced by sensors that are emerging as central to service delivery. IHS projects that the global IoT market will expand to almost 75.4 billion connected devices by the year 2025, with an increase of nearly 15.4 billion connected devices in 2015 as compared to 2015. A notable percentage of these intelligent IoT technologies are not confined to the consumer market (homes or smartphone), but are wide spread in the business and industry sectors, including healthcare. They are normally placed in the real-life settings to track, gather, and control critical data with the aim of improving operational efficiency and contributing to informed decision making [1]. Along with the spread of the use of IoT devices, the security issues related to it also expand. Although application specific security measures can be enforced at the different levels, to ensure safe data delivery across the network, a safe routing protocol or the provision of security measures on the current routing protocols at low costs have to be enforced. Routing Protocol for Low-Power and Lossy Networks (RPL) has been standardized to route in the Wireless Sensor Networks (WSNs) and IoT devices networks. RPL is a distance-vector based and source-routing protocol, a protocol that will run over a variety of link-layer technologies, such as the IEEE 802.15.4 physical and MAC layers, and is mostly intended to be used in collection-oriented network architectures. RPL is a lossy and resourceconstrained protocol designed by the IETF ROLL working group to support such networks. Nevertheless, RPL does not have detailed integrated security to ensure complete protection of routing processes, therefore it is vulnerable to numerous network-level attacks [2]. The issue of security in the Routing Protocol of Low-Power and Lossy Networks (RPL) is particularly a matter of concern because the routing processes imply the transmission of sensitive information that should not be disclosed to third parties or even enemies. RPL is especially susceptible to the attacks that are initiated by both external and compromised internal nodes. Even though a number of mechanisms have been suggested to counter the external attacks, insider threats remain a major security issue. This survey will look at the Routing Protocol Low-Power and Lossy Networks, the principles of its operation, and the reason it is applicable in resource-constrained settings. Security of RPL is examined as compared to a number of attack vectors which can be used to impair network integrity and performance. These attacks are categorically grouped and possible countermeasures are addressed. The purpose of the study is to evaluate current attack cases and determine unresolved security problems, thus showing the areas that need exploration to enhance the security of RPL.

Routing in IoT

Routing protocols facilitate communication among nodes within a network. In Internet of Things (IoT) environments, routing approaches are broadly classified into two categories: proactive routing, which dynamically maintains routing paths in advance, and reactive routing, in which sender nodes initiate the route discovery process only when data transmission is required [3].

RPL- The Routing Protocol for Low-Power and Lossy Networks (RPL) is an IPv6-based routing protocol designed for Internet of Things (IoT) environments. RPL belongs to the proactive routing category, as it dynamically establishes and maintains routing paths in advance to support efficient data transmission.

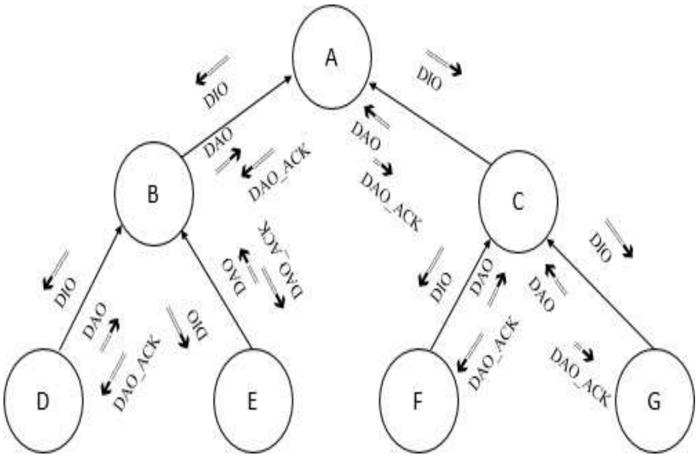


Fig 1 DODAG construction process

The proactive routing techniques can be applied to avoid attacks that happen during the communication process. RPL uses a Destination-Oriented Directed Acyclic Graph (DODAG) framework to route and makes use of control messages to form and maintain the topology. The formation of a DODAG as shown in Figure 1 starts when a parent node sends a DODAG Information Object (DIO) message to its neighbors. On receiving the DIO message, the neighbor nodes respond with a Destination Advertisement Object (DAO) message sent to the parent node. The parent node sends a DAO Acknowledgement (DAO_ACK) message to the child nodes after they have received the DAO messages to ascertain that they are part of the network. A new node that is interested in wanting to join the network will send a DODAG Information Solicitation (DIS) message to seek routing configuration information. Table 1 summarises the different RPL control messages and their functions.

Table 1.1 RPL control messages

RPL Control Message	Description
DODAG Information Object (DIO)	It contains information about a parent node
DODAG Advertisement Object (DAO)	It advertises that a node is within the range with same configuration that wants to join in the concern network
DAO_Acklogement (DAO_ACK)	It acknowledges its children to join in the network
DODAG Information Solicitation (DIS)	It is used to request for DIO message to join in the existing network.

ATTACKS AGAINST RPL

Various security attacks can occur in IoT networks utilizing the RPL routing protocol, including sinkhole attacks, Sybil attacks, selective forwarding attacks, black hole attacks, hello flood attacks, wormhole attacks, rank attacks, and version number attacks**.**

Sinkhole attack

A sinkhole attack occurs when a compromised node attempts to attract network traffic by falsely presenting itself as a legitimate and highly reliable node during the routing process. By drawing traffic toward itself, the malicious node prevents the base station from receiving authentic data, thereby disrupting normal network operation. This attack poses a significant security threat and often serves as a gateway for launching additional attacks within the network.

Sybil attack

A Sybil attack occurs when a malicious node generates and operates multiple fake identities simultaneously within the network. By doing so, the attacker disrupts normal routing operations and can prevent data packets from being correctly forwarded to their intended destination.

Selective forwarding attack

A selective forwarding attack occurs when a malicious node intentionally refuses to forward certain data packets to their intended destination or selectively drops messages, thereby disrupting normal packet propagation within the network.

Black hole attack

A black hole attack occurs when a malicious node falsely advertises itself as having the shortest or most optimal route to the destination. After attracting network traffic, the attacker deliberately drops the routing packets instead of forwarding them to the intended destination.

Hello flood attack

A Hello flood attack occurs when an adversarial node broadcasts an excessive number of Hello messages to neighboring nodes, misleading them and causing disruption in network operations.

Wormhole attack

A wormhole attack occurs when two or more malicious nodes establish a private communication link, known as a *wormhole*, to tunnel data packets across the network. This creates the illusion of a shorter routing path, misleading network nodes, causing routing confusion, and ultimately disrupting normal communication processes.

Rank attack

In the RPL protocol, the rank value determines the hierarchical position of each node within the network topology and plays a crucial role in parent selection and route formation. The rank value increases as nodes move downward away from the root and decreases in the upward direction toward the root. A rank attack occurs when a malicious node deliberately alters its legitimate rank value to a false rank, thereby misleading neighboring nodes and disrupting the routing structure of the network.

Need of Security for RPL

Although RPL includes built-in security modes, these mechanisms are insufficient to mitigate all types of security attacks. In RFC 7416 [3–7], a comprehensive security framework was proposed to analyze the security aspects of RPL. Based on this analysis, a set of security recommendations was formulated. The framework considers threat sources and the classification of threats and attacks, both of which are discussed in detail in the following sections.

Threat Sources: A threat source refers to an adversary that intentionally targets a network to carry out malicious activities. Based on the attacker’s behavior, capabilities, and position within the network, appropriate countermeasures must be designed. Attackers can generally be classified into two categories: outsiders and insiders.

Outsiders: These attackers operate outside the network, typically from the Internet, and may attempt to sniff, intercept, or inject spoofed data into the network nodes. Such entities are unauthorized and do not belong to the legitimate network.

Insiders: These attackers are legitimate nodes within the network that have been compromised due to faults, misconfigurations, or physical tampering of the IoT devices.

Classification of Threats and Attacks: [8], The discussed attacks and threats are related to routing mechanisms and are examined in the context of current RPL-based routing attacks. These threats are categorized into three distinct classes.

Failure to keep routing information confidential (Attacks on Confidentiality): In this context, information related to device-specific parameters, network topology, reachability, or data stored within network nodes is considered confidential. Unauthorized disclosure of such information can negatively impact network performance or be misused for malicious purposes. While nodes may be compromised through physical tampering or remote device access, such device-specific attacks fall outside the direct scope of RPL security mechanisms. However, attacks such as **sniffing** and **traffic analysis** can be exploited to eavesdrop on network communications, thereby breaching confidentiality and exposing sensitive routing and data information.

Failure to keep Integrity (Attacks on Integrity): A failure to preserve data integrity can severely damage network operations, as inconsistent or altered routing information may result in suboptimal routing decisions or cause the network to become fragmented. Integrity threats encompass any form of exploitation that manipulates routing information, including the falsification or replay of routing messages, as well as Byzantine attacks. In some cases, attackers may assume multiple identities, creating confusion among participating nodes and ultimately compromising the normal operation of the routing protocol.

Lack of availability (Attacks on Availability)

The availability of a node can be compromised in two primary ways: through interference or service disruption. Nodes that handle high traffic volumes are often targeted, as attackers can exploit them to drop packet flows, perform selective forwarding, or overwhelm them with excessive messages, rendering the nodes unable to serve legitimate requests. Various types of Denial-of-Service (DoS) attacks can be employed to make individual nodes or entire network segments unavailable. One common method to achieve this is by overloading the network through attacks such as the Hello Flooding attack, which exhausts node resources and disrupts normal network operations. [9]

LITERATURE REVIEW

Eleonora Borgia et al. [10] the key features, enabling technologies, and major issues and challenges of the Internet of Things (IoT) were discussed in detail. The various phases involved in an IoT environment were clearly explained, and a range of IoT applications were identified and briefly described.

MdIftekhar Hussain et al. [11] the various components of the Internet of Things (IoT) were explained, along with the associated research opportunities. Key challenges related to security and privacy in IoT environments were identified, and the requirements for achieving improved Quality of Service (QoS) in IoT systems were discussed.

Gordana et al. [12] the roles of various standardization organizations that have proposed architectural frameworks for the Internet of Things (IoT) were discussed. Key hardware and software design issues were explained with relevant examples, and the contribution of nanotechnology to the advancement of IoT systems was also highlighted.

VipindevAdat et al. [13] an overview of IoT architecture design was presented, followed by an analysis of various attacks targeting IoT routing protocols such as 6LoWPAN and RPL. Additionally, the associated challenges and security issues were examined in detail.

Anthea et al. [14] A taxonomy of attacks in RPL-based Internet of Things (IoT) networks was presented, comprising three primary categories: attacks targeting network resources, attacks that modify network topology, and attacks related to network traffic. These attack categories were clearly differentiated, and the associated risk management concerns were thoroughly discussed.

Linus wallgren et al. [15] An overview of Internet of Things (IoT) technologies and routing attacks was presented, with a detailed discussion of network protocols such as 6LoWPAN**,** CoAP/CoAPS, and RPL. The concept of Intrusion Detection Systems (IDS) in IoT environments was explained, and several RPL-specific attacks—including selective forwarding, sinkhole, hello flood, wormhole, clone ID, and Sybil attacks—were described, analyzed, and implemented using the Contiki operating system and the Cooja simulator.

Sinkhole attack

A sinkhole attack detector named an Intrusion Detection System (IDS) was created in [16] to identify sinkhole attacks in an edge-level Internet of Things (IoT) setup. The suggested IDS, which is called SADEIOT, proved to be very efficient when detecting all the major types of sinkhole attacks on edge-based IoT networks. NS2 simulator was applied to model and analyse the performance of the SAD-EIOT system. The suggested methodology was discovered to be suitable in surveillance, security, and monitoring solutions. The detection accuracy of 95.83% and false positive of 1.93% were obtained in the experiment. Such performance indicators like throughput, fraction of packet delivery, fraction of packet loss, and end-to-end delay were examined and compared in standard conditions, during an attack, and within the scheme of detection suggested.

The authors in [17] suggested an energy-based algorithm in order to identify sinkhole attacks. Under this system, every node sends a control message to the central base station before sending its information. Comparison of the control message with the respective data packets is then done on the hop-by-hop basis. Malicious nodes are determined by an anomaly or difference in the control messages. The sinkhole attack detecting algorithm proposed was tested against Ngai detector algorithm and proved to be better. The algorithm was also generalized to detect wormhole attacks which also demonstrate the adaptability of the algorithm in detecting various routing threats. [18]. The paper has examined the current methods of sinkhole attacks detection in Wireless Sensor Networks

(WSNs) such as rule-based detection, anomaly-based detection, statistical detection, hybrid intrusion detection systems, and key management systems. The sinkhole attack was well-defined and presented in the form of graphic representation. Moreover, the difficulties which relate to sinkhole attacks detection, including the connection between dynamic communication patterns of WSNs, the unpredictability of sinkhole action, insider threats, resource limitation, and physical attacks were discussed at length.

Rintaro Harada et.al.[(2022) [19] In this research, a new Distributed Denial-ofservice (DDoS) attack suppression framework is suggested that will have a significant impact on minimizing the unintended dropping of legitimate traffic by the non-compromised Internet of Things (IoT) devices. The proposed system can meet this goal by having minimal network equipment by dynamically adjusting frame priorities in IoT-enabled networks. The experimental findings prove that the system is effective in averting the loss of normal traffic within some few seconds by generating attack traffic by a traffic generator. More so, the system was able to block the dumping of legitimate traffic in 30 milliseconds using Mirai-based DDoS attack traffic. The findings also verify that the attack traffic detected by a DDoS protection system in front of an IoT server was automatically blocked at the network switches that were in the path of the traffic caused by the IoT devices, namely, at the ports to the backbone network, via the combination of the products of several vendors.

Md. Ashraful Islam et.al.[(2021) [20] the sensitive information in a cryptographic module may be transmitted by the common-mode current through a power cable, which allows attackers to execute remote eavesdropping by means of side-channel attacks. This leakage is caused by mode conversion, in which secret information passes on the normal-mode noise to the common-mode current at connector areas where discontinuities occur in the imbalance factor between the power cable and power delivery network (PDN) trace. Consequently, the common-mode current that is generated spreads through the power cable as side-channel information. The mitigation to this weakness is to use mode-conversion suppression method at the discontinuity point of the PDN to suppress common-mode current and increase resistance to side-channel attacks (SCAs). In particular, a capacitor is installed at the point of discontinuity to prevent mode conversion by lowering the normal-mode voltage. This method is very effective in reducing the current in the common-mode of the power cable, and thus enhances the SCAs resistance of the cryptographic module. As confirmed by experimental evidence, mode conversion is strongly suppressed and common-mode current is attenuated by installing a capacitor across the imbalance discontinuity point of the PDN which offers an efficient protection against external side-channel attacks.

Yutaka Abe et.al.[(2022) [21] the Cell Suppression Problem (CSP) aims at safeguarding sensitive cell values in tabular data when there are linear constraints, e.g. marginal sum constraints. The currently existing algorithms of solving CSPs are designed to make sure that there is enough uncertainty in each sensitive cell by keeping a large range of potential values. Deterministic CSP algorithms are however susceptible to matching attacks, whereby an adversary can minimize uncertainty by comparing the suppression pattern of an original table with the candidate tables produced by the same algorithm. Although it has been suggested that one possible defense to such attacks is the introduction of nondeterminism to CSP algorithms, this paper has shown that an even greater matching attack can undermine nondeterministic methods.

Sybil attack

In [22], the authors conducted a comprehensive survey of Sybil attacks and corresponding defense mechanisms in Internet of Things (IoT) environments. Sybil attacks were classified into three categories—SA-1, SA-2, and SA-3—based on the attacker's capabilities. A comparative analysis of these three attack types was presented in tabular form. Various Sybil attack detection and mitigation schemes, including Social Graph–Based Sybil Detection (SGSD)**,** Behavior Classification–Based Sybil Detection (BCSD), and mobile Sybil detection techniques, were discussed in detail. Additionally, the study examined open research challenges and issues associated with Sybil attacks in IoT networks.

In [23], A mechanism for mitigating sinkhole attacks was introduced, emphasizing robustness and low computational overhead. The proposed approach detects sinkhole attacks based on the Received Signal Strength Indicator (RSSI) and was shown to be stable and effective in static network environments.

In [24], A system for detecting both direct and indirect Sybil attacks in Internet of Things (IoT) environments was proposed. The system leveraged localization information, such as the Received Signal Strength Indicator (RSSI) and RSSI ratio among neighboring nodes, to identify malicious behavior. The proposed detection approach introduced minimal network overhead, making it suitable for resource-constrained IoT networks.

In [25], The authors proposed two distinct techniques for detecting Sybil attacks in a forest wildfire monitoring application. The first approach employed a two-tier detection method, in which high-energy nodes operating at a lower level were utilized for attack detection. The second approach was based on residual energy–based detection. Following the identification of a Sybil attack, a cluster head was elected using nominee packets. Legitimate data packets were verified by examining the cluster head information embedded within the packets. The proposed techniques achieved high detection accuracy while maintaining a low false-negative rate, demonstrating their effectiveness in Sybil attack detection.

In [26], Various security attacks targeting the RPL protocol were analyzed, with particular emphasis on the Sybil attack. The study revealed that RPL is more severely affected by Sybil attacks in mobile environments compared to static scenarios. Additionally, the Sybil attack was found to significantly reduce the packet delivery ratio while increasing control message overhead, thereby degrading the overall performance of the RPL protocol.

Selective forward attack

In [27], The authors focused on selective forwarding attacks in Internet of Things (IoT) networks and proposed a non-cooperative zero-sum game-theoretic model for intruder detection. Malicious nodes were identified through hop-by-hop inspection based on a predefined packet loss rate threshold. The proposed model was evaluated using the Cooja simulator and demonstrated efficient performance in heterogeneous network environments.

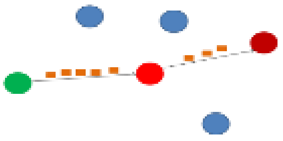
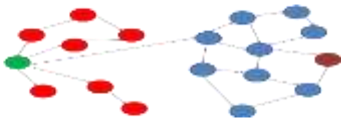
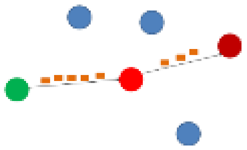
In [28], A method for detecting and mitigating selective forwarding attacks using adaptive learning automata and communication quality metrics was proposed. The approach addressed both ordinary selective forwarding attacks and their special-case variants, with packet loss used as the primary detection metric. The proposed method was evaluated through simulations conducted in OMNeT++ and was compared with the existing CLAIDS approach proposed by Fathinavid and Ansari.

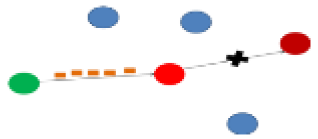
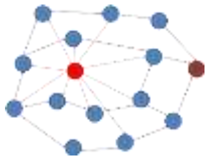
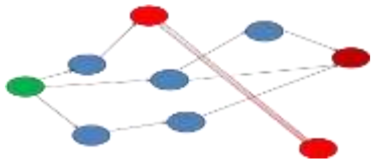
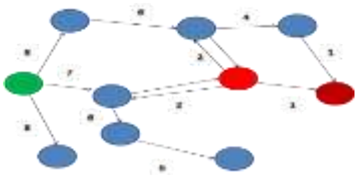
Blockhole Attack

In [29], the authors proposed a trust-based mechanism to mitigate black hole attacks in the RPL protocol. In this approach, the packet delivery ratio of each node was used as the trust metric. The mechanism was applied at two levels—inter-DODAG and intra-DODAG—to enhance attack detection and mitigation. The proposed solution was implemented and evaluated using the Cooja simulator.

Different attack scenario in RPL

Section Three explains various attack scenarios with corresponding diagrams. In these illustrations, the green node represents the source node, the red node denotes the malicious node, the brown node indicates the destination node, and the blue nodes represent neighboring nodes. **Table 3.1 RPL attacks scenario**

S. No	Name of the attack	Description	Diagram
1	Sinkhole Attack	Compromised node tries to drop the packets	
2	Sybil Attack	Malicious node creates multiple fake identities	
3	Selective Forwarding Attack	The malicious nodes selectively drops or forward the packets	

4	Black Hole Attack	The attacker node claims as it has shortest path and drops all the packets.	
5	Hello Flood Attack	Adversary node sends the hello messages to the neighbors‟ node to disturb the network.	
6	Wormhole Attack	Two or more adversary nodes are connected with the link called wormhole link and the nodes form the „tunnel‟ to broadcast the data packets into the network.	
7	Rank Attack	The rank value determines that the position of each node in the network. The rank value of a node is used to select the parents and routes	

CONCLUSION

Internet of things (IoT) is a fast-evolving technology that needs international connectivity and ubiquitous connectivity, allowing the users to have the access to IoT devices at any time and place. Consequently, security is an important factor that can guarantee access control and secure communication in IoT systems. The following paper entails an in-depth discussion of the IoT security concerns and specifically the attacks that target the Routing Protocol for Low-Power and Lossy Networks (RPL). Resting on a comprehensive investigation of the occurrence of RPL-associated attacks, the article sparks the need to devise new and efficient mitigating measures to improve the security and reliability of the IoT networks.

REFERENCES

1. Bhalaji, N., K. S. Hariharasudan, and K. Aashika, "A trust based mechanism to combat blackhole attack in RPL protocol", In International Conference on Intelligent Computing and Communication Technologies, pp. 457-464, 2019.
2. Carolina V. L. Mendoza and Joao H. Kleinschmidt, "Defense for selective attacks in the IoT with a distributed trust management scheme", In 2016 IEEE International Symposium on Consumer Electronics (ISCE), pp. 53-54. IEEE, 2016.

3. Cervantes, Christian, Diego Poplade, Michele Nogueira, and Aldri Santos. "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things", IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 606- 611. 2015.
4. Christian Cervantes, Diego Poplade, Michele Nogueira and Aldri 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), pp. 606-611, 2015.
5. Danilo Evangelista, Farouk Mezghani, Michele Nogueira, Aldri Santos,"Evaluation of Sybil attack detection approaches in the Internet of Things content dissemination", In 2016 Wireless Days (WD), pp. 1-6, 2016.
6. Firoz Ahmed and Young-Bae Ko, "Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks", Security and Communication Networks, Vol. 9, Issue 18, pp 5143-5154, 2016.
7. George W. Kibirige and Camilius Sanga, "A survey on detection of sinkhole attack in wireless sensor network", arXiv preprint arXiv:1505.01941, 2015.
8. Himanshu B. Patel and Devesh C. Jinwala, "Blackhole detection in 6LoWPAN based internet of things: an anomaly based approach",In TENCON 2019-2019 IEEE Region 10 Conference (TENCON), pp. 947-954, 2019
9. Hongliang Zhu1, Zhihua Zhang, Juan Du1, Shoushan Luo1 and Yang Xin, "Detection of selective forwarding attacks based on adaptive learning automata and communication quality in wireless sensor networks", International Journal of Distributed Sensor Networks, Vol. 14, Issue 11, pp. 1-15, 2018
10. Kuan Zhang, Xiaohui Liang, Rongxing Lu and Xuemin Shen, "Sybil attacks and their defenses in the internet of things", IEEE Internet of Things Journal, Vol.1, Issue 5, pp. 372-383, 2014.
11. Leovigildo Sanchez-Casado, Gabriel Macia-Fernandez, Pedro Garcia-Teodoro, and Nils Aschenbruck, "Identification of contamination zones for sinkhole detection in MANETs", Journal of Network and Computer Applications, pp. 62-77, 2015.
12. Linus Wallgren, Shahid Raza and Thiemo Voigt, “Routing Attacks and Countermeasures in the RPL-Based Internet of things”, International journal of Distributed Sensor Networks, pp. 1-11, 2013.
13. Mahmood Alzubaidi, Mohammed Anbar and Sabri M. Hanshi, "Neighbor-passive monitoring technique for detecting sinkhole attacks in RPL networks", In Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence, pp. 173-182, 2017.
14. Maliheh Bahekmat, Mohammad Hossein Yaghmaee, Ashraf Sadat HeydariYazdi, and Sanaz Sadeghi, "A novel algorithm for detecting sinkhole attacks in WSNs", International Journal of Computer Theory and Engineering Vol. 4, Issue 3, pp. 418 422, 2012.

15. MelancyMascarenhas and Vineet Jain, "A survey on mechanisms for detecting sinkhole attack on 6LoWPAN in IoT", International Journal of Latest Trends in Engineering and Technology, Vol. 10, Issue 1, pp.134-137, 2018.
16. Md. IftekharHussain, “Internet of Things: challenges and research opportunities”, DOI
10.1007/s40012-016-0136-6, pp. 1-9, 2016.
17. Mian Ahmad Jan,Priyadarsi Nanda, Xiangjian He and Ren Ping Liu, "A Sybil attack detection scheme for a forest wildfire monitoring application", Future Generation Computer Systems, Vol. 80, pp. 613-626, 2018.
18. Sabah Suhail, Shashi Raj Pandey and ChoongSeon Hong, "Detection of Selective Forwarding Attack in RPL-Based Internet of Things through Provenance", pp 965967, 2018.
19. Rintaro Harada;Naotaka Shibata;Shin Kaneko;Kazuaki Honda;Jun Terada;Yota Ishida;Kunio Akashi;Toshiyuki Miyachi Quick Suppression of DDoS Attacks by Frame Priority Control in IoT Backhaul With Construction of Mirai-Based Attacks IEEE Access Year: 2022 | Volume: 10 | Journal Article | Publisher: IEEE
20. Md. Ashraful Islam;Masaki Himuro;Kengo Iokibe;Yoshitaka Toyota Common-mode Current Reduction by Applying Mode-conversion Suppression Technique to Power Delivery Network as Side-channel Attack Countermeasure 2021 International
Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2)
21. Yutaka Abe;Kazuhiro Minami Matching Attacks on Non-deterministic Algorithms for Cell Suppression Problem for Tabular Data 2022 IEEE International Conference on Big Data (Big Data) 2022 IEEE International Conference on Big Data (Big Data) Year: 2022 | Conference IEEE
22. Rashmi Sahay, G. Geethakumari, BarshaMitra and V. Thejas, "Exponential smoothing based approach for detection of blackhole attacks in IoT", In 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1-6, 2018.
23. Sabeen Tahir, Sheikh Tahir Bakhsh and Rayan A Alsemmeari, "An intrusion detection system for the prevention of an active sinkhole routing attack in Internet of things", International Journal of Distributed Sensor Networks Vol 15, Issue 11, pp. 1-10, 2019.
24. Shoukat Ali, Dr. Muazzam A Khan, Jawad Ahmad, Asad W. Malik, and Anisur Rehman, "Detection and prevention of Black Hole Attacks in IOT & WSN", In 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC), pp. 217-226, 2018.
25. Sohail Abbas, "An Efficient Sybil Attack Detection for Internet of Things", In World Conference on Information Systems and Technologies, pp. 339-349, 2019.

26. Stephen. R and Arockiam. L, "RDAID: Rank Increased Attack IDentification Algorithm for Internet of Things", International Journal of Scientific Research in Computer Science Applications and Management Studies, Volume. 7, Issue 3, pp 1-5, 2018.
27. Stephen. R and Arockiam. L, "RDAIDRPL: Rank Increased Attack IDentification Algorithm for Avoiding Loop in the RPL DODAG", International Journal of Pure and Applied Mathematics, Vol. 119, Issue 16, pp.1-8, 2018.
28. Surinder Singh, Hardeep Singh Saini, "Detection Techniques for Selective Forwarding Attack in Wireless Sensor Networks", International Journal of Recent Technology and Engineering (IJRTE), Vol. 7, Issue 6S, pp. 380-383, 2019.
29. Vipindev Adat and B. B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture", DOI 10.1007/s11235-017-0345-9, pp. 1-99, 2017.