



A Comparative Study on Attacks against RPL in IoT

Poonam¹, Er. Veena Rani², Dr. Silki³

¹Research scholar, JCDD College of Engineering, Sirsa, Haryana (India),

²Assistant Professor, JCDD College of Engineering, Sirsa, Haryana (India),

³Associate Professor, JCDD College of Engineering, Sirsa, Haryana (India)

¹poonambishnoi181@gmail.com, ²veenuloyal@rediffmail.com, ³DrSilkiBaghla@gmail.com

Abstract

Routing Protocol for Low Power and Lossy Networks (RPL) is the routing protocol for IoT and Wireless Sensor Networks. RPL is a lightweight protocol, having good routing functionality, but has basic security functionality. This may make RPL vulnerable to various attacks. Providing security to IoT networks is challenging, due to their constrained nature and connectivity to the unsecured internet. This survey presents the elaborated review on the security of Routing Protocol for Low Power and Lossy Networks (RPL). This survey is built upon the previous work on RPL security and adapts to the security issues and constraints specific to Internet of Things. An approach to classifying RPL attacks is made based on Confidentiality, Integrity, and Availability. Along with that, we surveyed existing solutions to attacks which are evaluated and given possible solutions (theoretically, from various literature) to the attacks which are not yet evaluated. We further conclude with open research challenges and future work needs to be done in order to secure RPL for Internet of Things (IoT).

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

I INTRODUCTION

The Internet of Things (IoT) is a technology that's presently dynamical and reinventing business and society. This change leads to increase in focus on integrating, the new and massive flow of data from sensors and will be available as the fundamental service. The IHS.com predicts that market for Internet of Things may grow from 15.4 billion devices (in the year 2015) to 75.4 billion devices (in the year 2025), the statistics of the global IoT market. Most of these IoT smart devices cannot be in homes or phones, these are in businesses and industries (e.g. Healthcare). Since these devices are deployed in the field, to track and manage essential data, to increase the efficiency of work [1]. So, security concerns may rise as well. Based on applications of IoT devices, security measures at various levels are taken care of. But, as the network and data flow is concerned, we need a secure routing protocol or add a security feature to routing protocol with minimum overhead. Routing Protocol for Low Power and Lossy Networks (RPL), is standardized for routing in WSNs and IoT device networks. RPL is a distance vector (DV) and a source routing protocol that is intended to work on top of several link layer mechanisms including IEEE 802.15.4 PHY and MAC layers. It targets collection-based networks. RPL is a lightweight protocol and possesses different functionality compared to that of traditional routing protocols. ROLL group of IETF designed this mainly considering the lossy nature of the network.

RPL does not come with any major security features to secure routing completely and hence, it is vulnerable to various attacks on the network [2]. Security in RPL is a major issue that needs to be put in the limelight as routing carries data that should not be leaked or accessed by an intruder or any third party who is not an authorized

member of the network. RPL gets affected majorly due to attacks by an outsider or even sometimes by insider nodes. Measures have been implied to protect RPL from outside attacks, but there still poses threat from insider nodes. In this survey, we explore about Routing Protocol for Low Power and Lossy network, its working and also study its functionality for constrained networks. The security of RPL is studied with respect to attacks that can be made to breach into networks. The attacks are classified into categories and probable countermeasures are suggested. The research aims towards assessing possible attacks and also finding some unaddressed issues with respect to RPL security.

Routing in IoT

Routing protocol is used in the communication process among the nodes in the network. Routing in Internet of Things is classified into two types such as proactive (dynamic path selection process) and reactive (senders nodes trigger the route discovery). [3]

RPL-Routing Protocol for low power and Lossy networks (RPL) is an IPv6 routing protocol used in IoT environment. RPL falls in proactive category which dynamically seeks for the routing path.

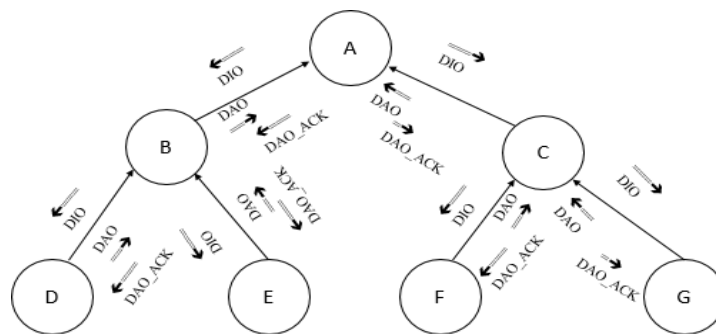


Fig 1 DODAG construction process

The attacks during the communication process can be mitigated by using proactive techniques. It uses Destination Oriented Directed Acyclic Graph (DODAG) for routing. It uses control messages to form DODAG. Fig 1 shows the DODAG construction process. A parent node broadcasts DODAG Information Object (DIO) message to neighboring nodes. The neighboring nodes which receive the DIO message will send DODAG Advertisement Object (DAO) to the parent node. After accepting the DAO messages from the neighboring node, the parent node will send the DAO_Acknowledgement (DAO_ACK) message to its children to join in the network. If a new node comes, it has to broadcast DODAG Information Solicitation (DIS) message to join the network which has the configuration. Table 1 describes the RPL control messages.

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 attacks such as sinkhole attack, Sybil attack, selective forwarding attack, black hole attack, hello flood attack, wormhole attack, rank attack and version number attack were occurred while using RPL routing protocol in IoT.

Sinkhole attack

Sinkhole attack is an attack where compromised node tries to entice network traffic by masquerading as legitimate node in routing process. The sinkhole attack blocks the base station from obtaining legitimate information; it causes threat and makes the way for occurrences of other attacks too.

Sybil attack

Sybil is an attack where a malicious node creates multiple fake identities at the same time in the network. It does not allow the packets of a node to be sent to the destination.

Selective forwarding attack

Selective forwarding is an attack where the malicious nodes neglect to forward the messages to precise destination nodes or simply drop the messages not to propagate anymore.

Black hole attack

A black hole is an attack where the attacker node claims as it has shortest path to the destination. It drops the routing packets and does not propagate the packets to the precise destination.

Hello flood attack

Hello flood attack is an attack where an adversary node sends the hello messages to the neighbor nodes to disturb the network.

Wormhole attack

Wormhole attack is an attack where two or more adversary nodes are connected with the link called wormhole link and the nodes form the tunnels to broadcast the data packets into the network. It makes the network to be confused and disrupt the communication process over the network.

Rank attack

In RPL protocol, the rank value determines the position of each node in the network. The rank value of a node is used to select the parents and routes. The rank of a node increases in a downward direction and decreases in an upward direction. A malicious node is changing the legitimate rank value into falls rank value is called rank attack.



Need of Security for RPL

RPL comes with built-in security modes, which are not enough to mitigate all types of attacks. [3-7], in RFC7416, proposed a security framework which analyzed RPL's security. From this analysis, they came up with a set of security recommendations. For analysis Threat Sources and Classification of Threats and Attacks were considered, both of these are explained in detail as follows:

Threat Sources: Threat source is an adversary which deliberately attacks the network, and based on the attack patterns, capability and position of attacker countermeasures need to be devised. The attackers can be classified into two groups as Outsiders and Insiders.

Outsiders: These attackers are residing outside the network on the internet and may sniff or spoof data into the nodes from the network. These are not authorized nodes from the network.

Insiders: These are the legitimate nodes from the network which are compromised because of some faults, misconfiguration, or some physical tampering of the IoT device.

Classification of Threats and Attacks: [8], discussed attacks and threats related to routing and we relate it to current examples of the routing attacks related to RPL. Here it is classified into three.

Failure to keep routing information confidential (Attacks on Confidentiality): In this, information related to device specific parameters or related to network topology, reachability information or information stored in the node is confidential to the network. The information disclosed may affect the performance of the network, or this information can be used for other purposes. Since nodes can be compromised by physical tampering or attacks carried out because of remote device access are device specific, so these attacks are out of the scope of RPL security. But, Attacks like Sniffing attack and Traffic Analysis Attack can be used for eavesdropping and in doing so it breaches confidentiality.

Failure to keep Integrity (Attacks on Integrity): Failure to keep integrity can cause a lot of damage to the network as inconsistent information can lead to suboptimality or network can be fragmented into parts. Integrity threat space can be any exploitation which manipulates the routing information, such as, falsification or replay routing information, or can carry out Byzantine attacks. Some of the times attackers can assume multiple identities so that it can cause confusion between participant nodes and protocol operation can be compromised.

Lack of availability (Attacks on Availability)

Availability of a node can be threatened in two ways, i.e. either by interference or by the disruption. In here, potential targets can be nodes with high traffic where these can be used to drop the packet flow or use selective forwarding, or just flood with messages so that it is unavailable to service other nodes. Various kinds of DoS attacks can be used to make node or network of nodes unavailable. This can be achieved by overloading the network using Hello Flooding Attack. [9]

II LITERATURE REVIEW

Eleonora Borgia et al. [10] described the key features, driving technologies and issues and challenges in Internet



of Things. The different phases involved in IoT environment were clearly explained. The IoT applications were listed out with brief descriptions.

MdIftekhar Hussain et al.[11] explained the various components used in Internet of Things. The research opportunities in IoT were explained and also the challenges concerned with security and privacy issues in IoT were listed out. The requirements to provide the better quality of service in IoT were explained.

Gordana et al.[12] described the various standard organizations which had given architectural framework for the Internet of Things. The design issues of hardware and software were explained with precise examples. The contribution of Nano technology in IoT was articulated.

VipindevAdat et al.[13] had given the overview with the design of architecture in IoT. The authors analyzed various attacks in the IoT routing protocols such as 6LoWPAN and RPL. The challenges and the security issues were explained.

Anthea et al.[14] articulated a taxonomy of attacks in RPL based Internet of Things. The taxonomy consisted of three main categories such as attacks targeting network resources, attacks modifying the network topology and attacks related to network traffic. These categories of attacks were distinguished from each other. The risk management concern with the attacks was clearly discussed.

Linus wallgren et al.[15] presented an overview of IoT technologies and routing attacks. The network protocols such as 6LoWPAN, CoPA/COAPS and RPL were clearly discussed. The concept behind IDS in IoT was explained. The attacks against RPL namely selective forwarding attack, sink hole attack, hello flood attack, wormhole attack, clone ID and Sybil attack were described, checked and implemented using Contiki and Cooja simulator.

Sinkhole attack

In [16], intrusion detection system was designed to detect sinkhole attack at edge level internet of thing environment. The proposed intrusion detection system was efficient to detect all possible types of sinkhole attack in edge based Internet of Things. The proposed IDS named as SAD- EIOT. NS2 simulator was used to simulate the SAD-IOT system. The SAD-IOT was suitable for surveillance security and monitoring system. A detection accuracy of 95.83% was achieved with the false positive rate of 1.93%. Throughput, packet delivery ratio, packet lose rate and end to end delay were distinguished in the form of normal flow, under attack and proposed schema. In [17], the authors proposed an algorithm to detect sinkhole attack based on energy consumption. In the algorithm, a node will send the control message to the main base station before sending its data to its base station. The control message is compared with its corresponding data hop by hop. The malicious node was detected based on the variation in the control messages. The proposed sinkhole attack detection algorithm was compared with Ngai's algorithm. The algorithm worked better than the Ngai's algorithm. It was also used for detecting wormhole attack.

[18] analyzed the existing techniques to detect sinkhole attack in wireless sensor network such as rule based, anomaly based detection, statistical method, hybrid based intrusion detection and key management. The sinkhole attack was defined and explained with graphical representation. The challenges in detection of sinkhole attack like communication pattern in wireless sensor networks, unpredictable sinkhole attack, insider attack and resource constraints and physical attack were discussed.



Rintaro Harada et.al.[(2022) [19] We propose a novel distributed denial of service (DDoS) attack suppression system that significantly reduces discarding of normal traffic (i.e., the traffic from Internet of Things (IoT) devices that are not infected with a malware) with a small number of equipment by controlling the priority of frames in a network accommodating IoT devices. Experimental results showed that our proposed system prevented the discarding of the normal traffic in a few seconds when attack traffic was generated by a traffic generator. Moreover, we constructed Mirai-based DDoS attack traffic and experimentally demonstrated that the discarding of the normal traffic was prevented in 30 milliseconds in our proposed system. We also confirmed that the attack traffic detected by a DDoS protector that was installed in front of an IoT server was autonomously blocked at the switches that the traffic came through from the IoT devices (i.e., the entrances to a backbone network) by integrating various vendors' products.

Md. Ashraful Islam et.al.[(2021)[20] The common-mode current flowing through a power cable contains the secret information of a cryptographic module that allows an attacker to eavesdrop from a remote location. Mode conversion conveys secret information as side-channel information from the normal-mode noise to the common-mode current at the connector section where the imbalance factor between the power cable and the trace on a power delivery network (PDN) is discontinuous. This common-mode current is generated due to mode conversion and flows through a power cable as side-channel information. We apply the mode-conversion suppression technique at the discontinuity point on a PDN to reduce the common-mode current as a side-channel attack (SCA) countermeasure. We place a capacitor at the discontinuity point to suppress mode conversion by reducing normal-mode voltage. Therefore, the common-mode current in a power cable should enhance the SCA resistance of the cryptographic module. We experimentally confirmed that installing a capacitor at the discontinuity point of the imbalance factor on a PDN efficiently suppresses mode conversion and reduces the common-mode current to counter SCAs from outside the cryptographic module.

Yutaka Abe et.al.[(2022) [21] The objective of the cell suppression problem (CSP) is to protect sensitive cell values in tabular data under the presence of linear relations concerning marginal sums. Previous algorithms for solving CSPs ensure that every sensitive cell has enough uncertainty on its values based on the interval width of all possible values. However, every deterministic CSP algorithm is vulnerable to an attack scheme that narrows down the width of sensitive cell values by matching the suppression pattern of an original table with that of each candidate table with the same CSP algorithm. Although to make a CSP algorithm non-deterministic is a promising approach against the matching attack, we find that there still exists an expanded matching attack to the algorithm.

Sybil attack

In [22], the authors took the survey on Sybil attacks and their defense scheme in internet of things. The authors classified the Sybil attack into three types such as SA-1, SA-2 and SA-3, based on the capabilities of the Sybil attack. The comparisons of three types of attack were given in a table. The Sybil attack defense scheme like social graph based Sybil detection (SGSD), behavior classification based Sybil detection (BCSD), and mobile sybil detection were explained in detail. The research issues based on sybil attack were discussed.

In [23], the mechanism to solve sinkhole attack was introduced. The mechanism was robust and lightweight. The sinkhole attack was identified based on received signal strength indicator (RSSI). The proposed mechanism was

stable enough in the static environment.

In [24], the system for detecting both direct and indirect Sybil attack in Internet of Things was recommended. The system utilized localization information dissemination such as received signal strength indicator and the ratio of RSSI for each neighbor nodes. The proposed detection system produced low overhead in network.

In [25], authors proposed two different techniques to detect sybil attack for a forest wild fire monitoring application. The first technique was a two tier method which used the high energy nodes operating at lower level. The second technique was residual energy based detection. After detecting the sybil attack, the cluster head was elected by the nominee packets. The legitimate packets were identified by looking at the cluster head in the packet. The proposed technique resulted high detection accuracy and low false-negative rate.

In [26], various attacks were analyzed against RPL. Sybil attack was analyzed in detail. The RPL protocol was affected more by the sybil attack in mobile environment compared with static environment. It was found that the sybil attack decreased the packet delivery ratio and increased the control messages overhead in RPL protocol.

Selective forward attack

In [27], authors focused selective forwarding attack in IoT network. A non-cooperative zero-sum game theoretic model for detecting intruders in the network. The malicious nodes were detected based on hop by hop inspection using packet loss rate threshold value. The proposed model was simulated using Cooja simulator. The model efficiently worked in the heterogeneous environment.

In [28], a method to detect and eliminate selective forwarding attack using adaptive learning automata and communication quality was proposed. This method was used for ordinary selective forwarding attack and special case of selective forwarding attack. Packet loss was considered as metric to detect selective forwarding attack. The proposed method was simulated using OMNeT++. The method was compared with the existing method CLAIDS which was proposed by Fathinavid and Ansari.

Blockhole Attack

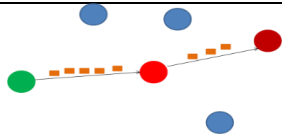
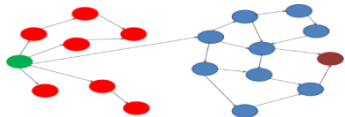
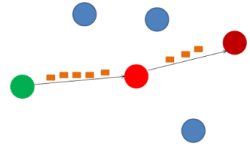
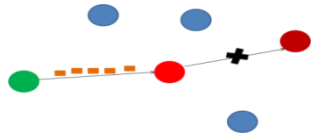
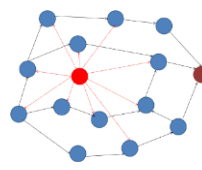
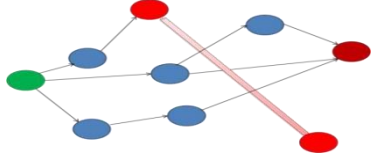
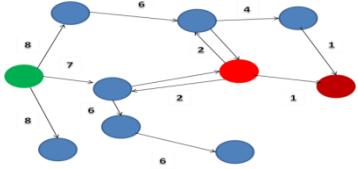
In [29], authors proposed a trust based mechanism to tackle blackhole attack in RPL protocol. Packet delivery ratio of the node was taken as the trust value. The proposed mechanism was used in two levels namely inter-DODAG level and intra-DODAG level. It was implemented using Cooja simulator.

Different attack scenario in RPL

Section three explains various attack scenarios with concerned diagram. Green color node indicates source node. Red colour node indicates malicious node. Brown colour indicates destination node. Blue colour nodes indicate neighbor nodes

Table 3.1 RPL attacks scenario

S. No	Name of the attack	Description	Diagram
	Sinkhole	Compromised node tries to drop the	

1	Attack	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

IoT is the current trending technology. It requires global connectivity and accessibility so that anyone can access IoT devices anywhere at any time. So security plays a vital role in the IoT technology to provide the access control



and the secure communication. In this paper, IoT security issues and attacks related to RPL are clearly explained. Based on the survey on RPL attacks, it is a necessary to provide a novel technique to mitigate these attacks. IoT is the current trending technology. It requires global connectivity and accessibility so that anyone can access IoT devices anywhere at any time. So security plays a vital role in the IoT technology to provide the access control and the secure communication. In this paper, IoT security issues and attacks related to RPL are clearly explained. Based on the survey on RPL attacks, it is a necessary to provide a novel technique to mitigate these attacks.

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 Bahekmatt, Mohammad Hossein Yaghmaee, Ashraf Sadat Heydari Yazdi, 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. Melancy Mascarenhas 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. Iftexhar Hussain, "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 965-967, 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, Barsha Mitra 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. VipindevAdat and B. B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture", DOI 10.1007/s11235-017-0345-9, pp. 1-99,