Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

Attacks against Rplin Iot: A Survey

A.Stephen[1], Dr. L. Arockiam[2]
Research Scholar[1], Associate Professor[2]
Department of Computer Science,
St. Joseph's College (Autonomous),
(*Affiliated to Bharathidasan University*),
Tiruchirappalli – 620002, India.

Abstract

Internet of Things is one of the trending technologies in the cotemporary world which allows all the technologies to work together as a single system. The "things" connected in the IoT environment could be anything such as objects, physical/virtual things and human beings. The communication between these connected things should be secured. Otherwise, intruders can misuse the data collected from the IoT environment. So, there is a necessity of providing better routing mechanism for IoT to provide secure communication against various attacks in IoT. Several protocols areused for routing in IoT. IPv6 Routing Protocol for Low Power and Lossy Networks (RPL) is one of the protocols in IoT based system. In this paper, various attacks against RPL protocol are listed out, analyzed and distinguished from each other.

Keywords: IoT, Attacks, Security, RPL

1. Introduction

1.1 Internet of Things

Internet of Things is a technology where the physical things are interconnected through the internet which have unique identities and their own functionalities. The functionalities can be sensing, actuation, sharing information, analyzing and processing the sensed data.Since sensitive data are collected using IoT technology, the communication path should be secured. The attackers can misuse the data in the communication process.

1.2 IoT Architecture

Different types of layered architectures are used by many researchers. There is no standard architecture for IoT. But three layered architecture is most frequently used which was proposed by IETF. The fig 1.1 presents three layered architecture.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

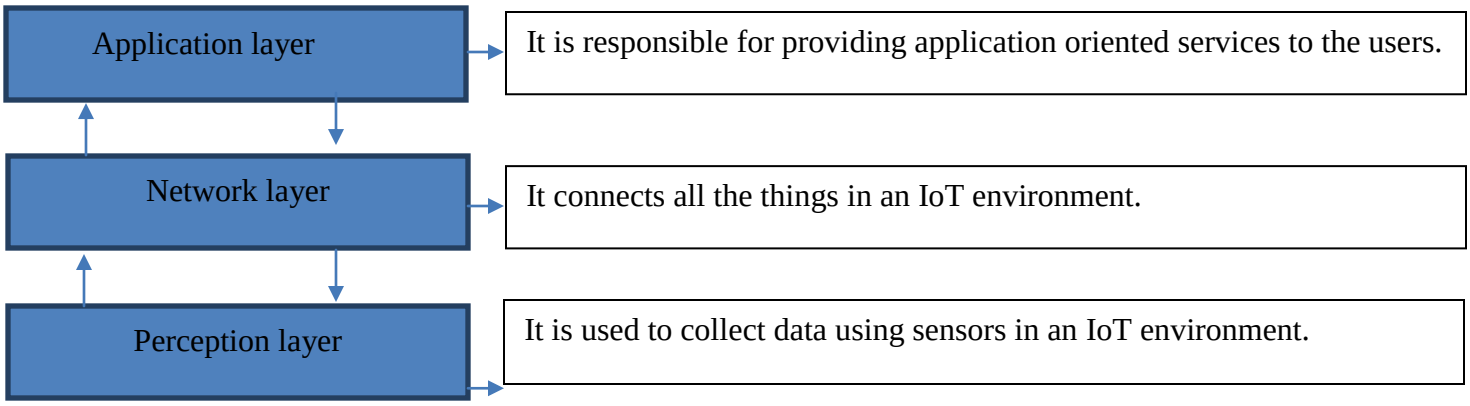


Fig 1.1 Three layered architecture

There are lots of issues in these three layers. This paper focuses various attacks against the routing protocol RPL.

1.3 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).

1.4 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.

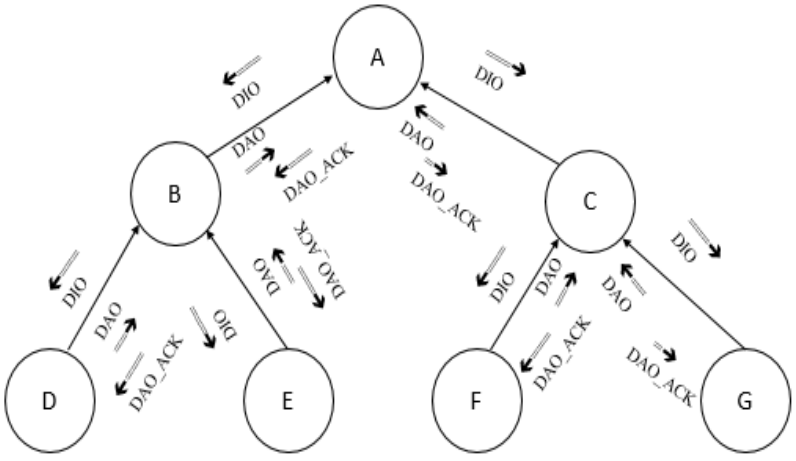


Fig 1.2 DODAG construction process

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

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 1.2 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_Acklogement (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 1.1 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.

This paper is organized into different sections.Section 2 lists out the various attacks against RPL protocol; Section 3 distinguishes the various attacks;Section 4 gives Literature review; Section 5 gives the results and discussions and Section 6 concludes the paper.

1.5 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.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

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.

Blackhole 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

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

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.

2. Literature Review

2.1 Internet of Things overview and security issues & challenges based on RPL

Eleonora Borgia et al.[9] 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.

MdIftekharHussain et al.[26] 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.[16] 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.[46] 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.[3] 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.[22] 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.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

2.2 Sinkhole attack

In [44], 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 [24], 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.

Geroge et al.[14] 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.

In [7], an intrusion detection system (IDS) was proposed to detect sinkhole attack. The proposed IDS detected the sinkhole attack and mitigated the destructive effects which were identified in the networks. They combined watchdog, reputation and trust strategies to detect attacker based on thebehaviourof the devices. The proposed technique was divided into four modules namely cluster configuration routing monitoring, attack detection and attack isolation. The system was implemented in the Cooja simulator. The UDS was compared with SVELTE in terms of detection accuracy in fixed scenario and mobile scenario and false positive rate. The detection accuracy for SVELTE in fixed scenario was 90%, the detection accuracy for INTI in fixed scenario was 92%. The detection accuracy for SVELTE in mobile scenario was 24%, the

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

detection accuracy for INTI in fixed scenario was 70%. The false positive rate for SVELTE was 38%, the false positive rate for INTI was 28%.

In [25],the mechanisms to detect sinkhole attack on ipv6 over low power wireless personal area network were surveyed. The paper analyzed the mechanisms called VERA, TRAIL, Secure Parent, and SVLTE. INTI and Specification based mechanisms were distinguished with each other.

In [32], the intrusion detection system to prevent an active sinkhole attack in Internet of things was presented. In this proposed system, the whole network was divided into clusters of Internet of Things. All the devices were connected with their concerned gateways. The intrusion system was deployed into the gateways. The gateways analyzed the communication over the devices and detected the anomalies using the proposed IDS. The base station had all the records and all the activities over the IOT environment. At the situation of sinkhole attack in the connected network, the base station sent the alert to all the connected devices in the network. The proposed IDS model outperformed in terms of packet delivery ratio (PDR) and energy consumption.

Stephen et al.[42] proposed an active detection technique to detect sinkhole attack. The technique comprised of three phases. The first phase was construction of DODAG, the second phase was detection of sinkhole attack, and the third was sinkhole attack treatment. The technique was simulated using Cooja simulator.

In [23], the light weight technique called Neighbor Passive Monitoring Technique for detecting sinkhole attacks in RPL networks (NPMT) was proposed. The proposed technique comprised of two phases. The first phase was used to identify the suspicious nodes in the network based on inconsistent changes in the nodes rank. The second phase was used to detect the sinkhole attack from the suspicious nodes. The proposed technique was compared with the existing technique SVELTE. The proposed technique NPMT performed better than SVELTE. The technique was implemented using Cooja simulator.

Geroge et al.[13] described the existing techniques to identify sinkhole attack in wireless sensor networks(WSNs). The challenges in WSNs were elucidated in detail. The different approaches used for mitigating sinkhole attacks were explained.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

Leovigible et al.[21] proposed a new methodology for detecting sinkhole attacks in MANETs. The proposal leverages on the existence of "contamination border" formed by the legitimate nodes under the influence of the sinkhole attack. The proposed methodology was implemented using network simulator OMNCT++ (Varga)

Stephen et al.[43] proposed intrusion detection system to detect sinkhole attack on RPL protocol. The IDS used number of packets transmitted and received to detect sinkhole attack based on the intrusion ratio. The alert message was sent to leaf nodes after identifying the intruder node in the network.

2.3 Sybil attack

In [20], 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-2and 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),behaviourclassification based Sybil detection (BCSD), and mobile sybil detection were explained in detail. The research issues based on sybil attack were discussed.

In [33], 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 [38], 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 [27],authors proposed two different techniques to detect sybil attack for a forest wild fire monitoring application. The first technique was a two tire method which usedthe 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.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

In [10], 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.

In [8], the study was done on techniques to detect sybil attack based on network features, cryptography and relationship between neighbors nodes in IoT. Afteranalyzing the several techniques, the authors concluded that there is a need to develop anefficient technique for detecting and mitigating sybil attack in IoT.

In [1], authors presented a comprehensive analytical survey on sybil attack in IoT. The authors classified the sybil attack into three phases namely compromise phase, deployment phase and launching phase. The algorithm using K-means clustering was proposed to visualize the deployment selection procedure of the attacker. The algorithm achieved 48.7% in clustering affected nodes and the legitimate nodes in the IoT.

In [28], a technique to detect sybil attack based on RSSI value in wireless sensor networks (WSN) was introduced. The technique was tested by multiple receivers using their RSSI ratio. The proposed technique achieved 100% to detect sybil attack and produced less false positive.

2.4 Selective forward attack

In [36], authors focused selective forwarding attack in IoT network. A non-cooperative zero-sum gave 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 [18], 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.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

In [45], authors discussed four selective forwarding detection techniques such as Public Key Encryption (PKE), Rivest Shamir Adelemen (RSA), ELGMAL and Chinese Remainder Theorem (CRT). These four techniques were evaluated based on storage space required, energy consumption and time consumption for key management. The authors concluded that minimum storage was required for public key encryption and minimum energy consumption were required for CRT based RSA techniques.

In [11], an Intrusion Detection System (IDS) to prevent nodes from selective forwarding attack based on mobile wireless sensor networks was proposed. The proposed IDS was novel with the combination of sequential probability ratio test with an adaptive threshold of acceptable probability of dropped packets. The IDS used four steps namely data gathering, data analysis, detection, elimination and compromised node setup. It was evaluated using Cooja simulator and performed 100% of detection probability.

In [31], provenance based method to detect selective forwarding attack in RPL based internet of Things was introduced. Each data in the network was consisted of unique sequence number, payload and packet delivery ratio. Packet delivery ratio was used to identify the malicious nodes in the IoT network. The proposed method was simulated using Cooja simulator.Provenance generation time and provenance size were taken as performance metrics.

In [5], authors discussed on trust management scheme to defend against selective forwarding attack in internet of Things. The trust value of each node was stored in a table. It was found that, if the trust value was decreased then there was the possibility of selective forwarding attack in the network. Various existing distributed trust management scheme were tested using Cooja simulator with Tmote Sky environment.

In [35], an algorithm to detect and mitigate selective forwarding attack using efficient fuzzy path selection approach in wireless sensor networkswas proposed. The proposed algorithm was comprised of two phases. The first phase was detecting compromised nodes in the network. The second phase was to mitigate selective forwarding attack by generating new disjoint path using average link residual energy and relative hop count. The proposed algorithm was evaluated in the real environment by deploying various sensors in a rectangular area.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

2.5 Blockhole Attack

In [4], 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.

Himanshu et al.[17] proposed an intrusion detection system to detect and mitigate blackhole attack in internet of things. The proposed IDS was divided into two modules namely local module and global module. The local module was used in the node level. The global module was used in border routed level. The suspicious nodes list was created based on thebehaviourof the nodes. The suspected nodes were only observed in the network. Malicious event was created when there was change in the observed nodes. The malicious nodes were eliminated when the nodes crossed the maliciousevent threshold value. The IDS was simulated using Cooja simulator. It was proved that the proposed IDS worked better than the watchdog approach.

In [38], blackhole attack in Internet of Thigs (IoT) and Wireless Sensor Networks (WSN) were discussed. Authors gave comparative analysis of various existing techniques of blackhole attack. The analysis was done based on energy consumption, network traffic, packet delivery ratio, throughput and end to end delay. The simulation tools used for detecting and mitigating blackhole attack were discussed.

In [30], statistical technique called exponential smoothing approach to detect blackhole attack was explained. This approach was based on time serious analysis of data. The data collection process was done in sink level in the proposed technique. It was used in the dynamic environment. The proposed technique was tested using Cooja simulator.

Firoz et al.[12] proposed an algorithm to mitigateblackhole attack in routing protocol for low power and lossy networks. The proposed technique consisted of local decision and global verification process. Each node in the network monitored the communicationbehaviourof its neighboring nodes by overhearing packets transmitted by neighboring nodes. The second process was to identify the suspicious nodes. The suspicious nodes were verified by changes in their

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

behavior. The confirmed malicious nodes' IDs were broadcasted to the other nodes by the alternative path in the network. The technique was simulated by Cooja simulator.

In [19], case study was done on blockhole attack in 6LoWPAN-RPL. Blackhole attack was tested using Cooja simulator. It was found that blackhole attack increased end to end delay and packet delivery ratio of the nodes in the network. It was also found that the malicious nodes rapidly affected the legitimate nodes.

2.6Rank Attack

Anhtuan et al.[2] explained types of internal threats and their impact on WSN. RPL protocol was clearly explained with its operation in the WSN. RPL attacks were described in detail. The parameters of DODAG and the control messages of DODAG were clearly explained. Contiki OS and Cooja simulator were used for the simulation process.

Stephen et al.[38] proposed the technique called energy based validation and verification (E2V) for detecting and mitigating rank attack (RA) over RPL. The proposed technique used three phases namely rank calculation, substation and malicious node elimination. The technique was used to solve the rank inconsistency attack.

Ghada et al.[15] proposed a secure routing technique based on RPL for Internet of things. The proposed method was used to prevent nodes from the malicious nodes in the network. The author had taken the rank property to provide secure routing. Rank threshold and hash chain authentication were used to deal with the attackers nodes. The proposed method was implemented using Contiki OS and Cooja simulator. It outperformed the existing techniques

Stephen et al.[39] proposed a technique named "Rank Decreased attack IDentification (RDAID)" for identifying the malicious nodes and mitigating the malicious node. Packet delivery ratio (PDR) was used for securing the routing process.

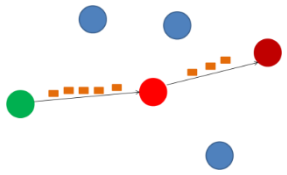
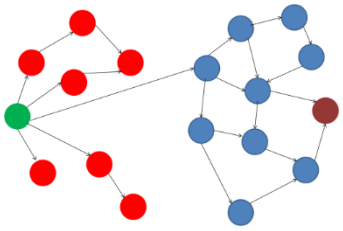
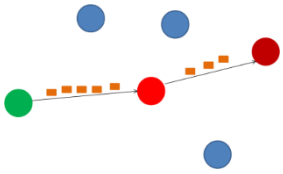
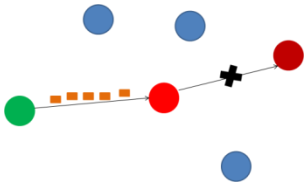
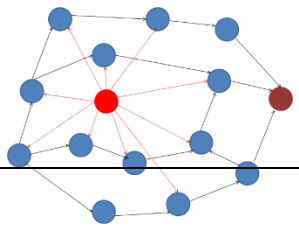
Stephen et al.[40] proposed Rank Increased Attack (RIA) identification algorithm to avoid loop in the RPL DODAG. The proposed technique detects the nodes which were affected by the rank increased attack. It gave the better result than the existing techniques.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

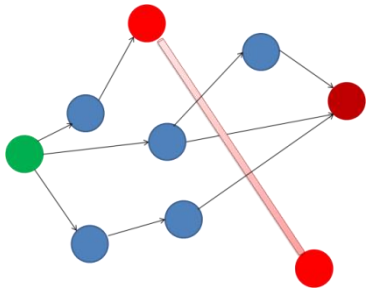
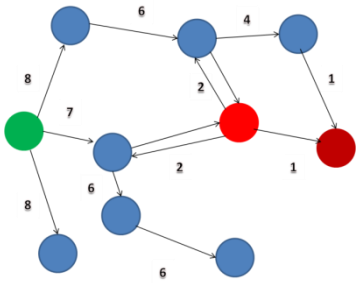
3. Different attack scenario in RPL

Section three explains various attack scenario 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
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.	

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

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	

4. Detection and Mitigation Mechanism of RPL based Attacks.

The different types of mechanisms which are used for detecting and mitigating RPL attacks are listed out in the table 4.1 based on the attack type.

Table 4.1 List of RPL attack detection and mitigation mechanisms

S.No	Attack type	Mechanism
1	Sinkhole attack	Energy based detection[24],[27], K-means clustering [1], Watchdog Mechanism[7], Cluster based Detection[32], Neighbor Passive Monitoring Technique[23].

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

2	Sybil attack	Social graph based Sybil detection [20], Technique based on received signal strength indicator (RSSI) [33], [38], [28].
3	Selective forwarding attack	Hop by Hop inspection[36], Adaptive learning mechanism[18], Public key encryption technique[45], Provenance based method[31], Trust management scheme[5] and fuzzy path selection approach [35].
4	Blockhole attack	Trust based mechanism[4], Strained based intrusion detection system[17], Exponential smoothing approach[30], Nodes'behaviour approach[12].
5	Rank attack	Energy basedtechnique[38], PDR based approach[39], Nodes'behaviourapproach[15].

5. 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.

REFERENCES

[1] Alekha Kumar Mishra, Asis Kumar Tripathy, Deepak Puthal, and Laurence T. Yang, "Analytical model for sybil attack phases in internet of things", IEEE Internet of Things Journal, Vol. 6, Issue 1, pp. 379-387, 2018.

[2] Anhtuan Le, Jonathan Loo, AboubakerLasebae, Alexey Vinel, Yue Chen and Michael Chai, "The impact of rank attack on network topology of routing protocol for low-power and lossy networks, IEEE Sensors Journal, Vol. 13, Issue 10, pp.3685-3692, 2013.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

[3] AntheaMayzaud, Remi Badonnel and Isabella Christment, “A Taxonomy of Attacks in RPL-based Internet of Things”, International Journal of Network Security, Volume 18, Issue 3, pp. 459-473, 2016.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] Eleonora Borgia, “The Internet of Things vision: Key Features, Applications and Open Issues”,DOI : http://dx.doi.org/10.1016/j.comcom.2014.09, pp.1-55, 2014.

[10] FaizaMedjek, DjamelTandjaoui, Mohammed Riyadh Abdmeziem, Nabil Djedjig "Analytical evaluation of the impacts of Sybil attacks against RPL under mobility", In 2015 12th International Symposium on Programming and Systems (ISPS), pp. 1- 9, 2015.

[11] FatmaGara, Leila Ben Saad and Rahma Ben Ayed, "An intrusion detection system for selective forwarding attack in IPv6-based mobile WSNs",In 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 276-281, 2017.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

[12] 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.

[13] George W. Kibirige and Camilius Sanga, "A survey on detection of sinkhole attack in wireless sensor network", arXiv preprint arXiv:1505.01941, 2015.

[14] Geroge W Kibirige and Camilius Sanga, “A survey on Detection of Sinkhole Attack in Wireless Sensor Network”, International Journal of Computer Science and Information Security, pp. 1-9, 2015.

[15] GhadaGlissa, AbderrezakRachedi and ArefMeddeb, "A secure routing protocol based on RPL for Internet of Things", In 2016 IEEE Global Communications Conference (GLOBECOM), pp. 1-7, 2016.

[16] GordanaGardasevic, MladenVeletic, NebojsaMaletic, DraganVasiljevic, Igor Radusinovic, SlavicaTomovic and MilutinRadonjic, “The IoT Architectural Framework, Design Issues and Application Domains”, DOI 10.1007/s11277-016-3842-3, pp. 1-22, 2016.

[17] 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.

[18] 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.

[19] KarishmaChugh, AboubakerLasebae and Jonathan Loo, "Case study of a black hole attack on LoWPAN-RPL", In Proc. of the Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), Rome, Italy (August 2012), pp. 157-162, 2012.

[20] 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.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

[21] 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.

[22] 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.

[23] 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.

[24] MalihehBahekmat, Mohammad Hossein Yaghmaee, Ashraf Sadat HeydariYazdi, and SanazSadeghi, "A novel algorithm for detecting sinkhole attacks in WSNs", International Journal of Computer Theory and Engineering Vol. 4, Issue 3, pp. 418 -422, 2012.

[25] 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.

[26] Md. IftekharHussain, “Internet of Things: challenges and research opportunities”, DOI 10.1007/s40012-016-0136-6, pp. 1-9, 2016.

[27] 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.

[28] Murat Demirbas and Youngwhan Song, "An RSSI-based scheme for sybil attack detection in wireless sensor networks", In 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'06), pp. 1-7, 2006.

[29] OlfGaddour and AnisKoubba, “RPL in nutshell: A survey”, computer networks, Vol. 56, Issue 14, pp.3163-3178, 2012.

[30] 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.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

[31] 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.

[32] 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.

[33] Salavat Marian, PopaMircea, "Sybil attack type detection in wireless sensor networks based on received signal strength indicator detection scheme", In 2015 IEEE 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics, pp. 121-124, 2015.

[34] Salehi, S. Ahmad, M. A. Razzaque, ParisaNaraei, and Ali Farrokhtala, "Detection of sinkhole attack in wireless sensor networks", In 2013 IEEE International Conference on Space Science and Communication (IconSpace), pp. 361-365, 2013.

[35] SeyyitAlperSert, Carol Fung, Roy George and Adnan Yazıcı, "An efficient fuzzy path selection approach to mitigate selective forwarding attacks in wireless sensor networks", In 2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), pp. 1-6, 2017.

[36] ShaplaKhanam, Ismail Ahmedyand Mohd Yamani Idna Idris, "An efficient detection of selective forwarding attacks in heterogeneous IoT Networks", pp 1-8, 2017.

[37] Shoukat Ali, Dr. Muazzam A Khan, Jawad Ahmad, Asad W. Malik, and AnisurRehman, "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.

[38] Sohail Abbas, "An Efficient Sybil Attack Detection for Internet of Things", In World Conference on Information Systems and Technologies, pp. 339-349, 2019.

[39] 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.

[40] 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.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 9767 - 9786
Received 05 March 2021; Accepted 01 April 2021.

[41] Stephen. R and Arockiam. L, “E2V: Techniques for Detecting and Mitigating Rank \Inconsistency Attack (RInA) in RPL based Internet of Things”, Journal of Physics, doi:10.1088/1742-6596/1142/1/012009, pp. 1-13, 2018.

[42] Stephen, A. Dalvin Vinoth Kumar and L. Arockiam, "Deist: dynamic detection of Sinkhole attack for Internet of Things", International Journal of Engineering and Computer Science, Vol. 5, Issue 12, pp. 19358-19362,2016.

[43] Stephen, R., and L. Arockiam, "Intrusion detection system to detect sinkhole attack on RPL protocol in Internet of Things", International Journal of Electrical Electronics and Computer Science, Vol 4, Issue 4, pp. 16-20, 2017.

[44] SumitPundir, Mohammad Wazid, DeveshPratap Singh, Ashok Kumar Das, Joel J. P. C. Rodrigues and Youngho Park, "Designing Efficient Sinkhole Attack Detection Mechanism in Edge-Based IoT Deployment", Sensors Vol. 20, Issue 5, 1-27, 2020.

[45] 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.

[46] 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, 2017.