Annals of Telecommunications (2018) 73:429–438
https://doi.org/10.1007/s12243-018-0645-4

Detection of rank attack in routing protocol for Low Power and Lossy Networks

Usman Shafique[1] · Abid Khan[2] · Abdur Rehman[1] · Faisal Bashir[1] · Masoom Alam[2]

Received: 9 May 2017 / Accepted: 29 April 2018 / Published online: 16 May 2018

Abstract
Internet Engineering Task Force (IETF) has recommended the use of routing protocol for Low Power and Lossy Network (RPL) for Internet Protocol version 6 (IPv6) enabled Internet of Things. However, RPL is vulnerable to internal and external attacks in a network. A malicious node in a rank attack, which is consumed by its child nodes, advertises false rank information. This consequently causes the selection of a malicious node as preferred parent for routing information to the sink node. Given the widespread application of RPL protocol in smart homes, smart cities, and the smart world, it is imperative to address this problem. In this paper, a novel Sink-based intrusion detection system (SBIDS) for the detection of rank attack in RPL is presented. SBIDS has less computational overhead as all detection processes take place at the sink node, which saves network resources. Through a comprehensive simulation analysis, it is shown that the proposed SBIDS provides high detection rate.

Keywords Internet of things · IPV6 · RPL · Sink based intrusion detection

1 Introduction

Internet of Things (IoT) has recently gained focus of researchers, due to its vast applications including transportation, logistics, healthcare, education, communication, and smart environment [1–5]. Thus, IoT is the future of the Internet, as the smart objects have revolutionized communication. To this effect, various underlying technologies have been proposed for the realization of IoT. A notable development in this regard is the specification of a novel protocol by IETF [6]. Routing protocol for Low Power and Lossy Networks is IPv6-based routing protocol for Low power Lossy Networks (LLN).

RPL is the proposed basic routing protocol for IPv6 over Low-power Wireless Personal Area Network (6LoWPAN). Proactive routing protocol named RPL is the proposed standard protocol for LLNs by IETF and is newly updated in March 2012 as [7]. RPL provides IPv6 Internet connectivity and furthermore, using RPL the cost of reaching the root (base station) from any node within the LLN is also reduced. RPL forms a directed acyclic graph (DAG)-based topology, which is a mathematical graph model with no directed cycles. This graph is constructed by following distance vector rules defined in [6]. DAG nodes and the data are converged at a single sink node. RPL is multi-hop routing protocol where each node can have many adjacent nodes. A node a is denoted as a neighbor of node b if and only if it is in the radio range of node b. RPL constructs network topology on-the-fly as nodes are organized in the fields. All RPL devices have the best path to the root through next hop nodes since RPL is categorized as proactive. The DAG-based topology formed by RPL is divided into one or more Destinations Oriented DAGs (DODAGs). Each DODAG holds the DODAG root, which is configured by an administrator. DODAG root is responsible for the creation and maintenance of the DODAG. Three types of traffic

✉ Abid Khan
abidkhan@comsats.edu.pk

Usman Shafique
usman.buic@bahria.edu.pk

Abdur Rehman
abdul.mul103@gmail.com

Faisal Bashir
faisalawn@yahoo.com

Masoom Alam
masoom.alam@comsats.edu.pk

[1] Bahria University, Islamabad, Pakistan

[2] Computer Science Department, COMSATS Institute of Information Technology, Islamabad, Pakistan

are supported by RPL: (i) Multipoint-to-Point (MP2P), (ii) Point-to-Multipoint (P2MP), and (iii) Point-to-Point (P2P). MP2P traffic pattern is embraced by most LLN applications in RPL [7]. RPL protocol supports both private and public key cryptographic solutions for information security even though LLNs are constrained in terms of computing resources. Depending on the computing resources available on the network devices, RPL can be operated using both insecure and secure mode. RPL [7] does not apply security protection for control messages (such as DIO, DIS, DAO and DAO_ACK control messages) or data packets in the insecure mode. During nodes joining and transmissions, security fields are not triggered. Using preinstalled keys or combination of both public and private key cryptography, the secure mode provides two mechanisms for protection. In the preinstalled key mode, nodes have preinstalled keys (before deployment) and they use symmetric key cryptography for providing authentication and confidentially. Lightweight public-key cryptographic techniques are recommended for key exchange among the network nodes and message security is provided with symmetric key cryptography in the other mode.

Rank is an attribute of a node in RPL network that represents its position with respect to rich energy device called sink. In rank attack, a malicious node introduces the false rank through DIO on the resultant neighboring node converged towards it, and gets selected as a preferred parent through DAO. Once a malicious node becomes the preferred parent node (PPN) in the attacking region, a number of QOS parameters can be compromised [7]. Although, some solutions are available for prevention and detection of rank attacks in RPL network [8, 9]. However, these solutions consume high resources and thus decrease network lifetime.

Our contributions in this paper are as follows:

1. A sink/root-based statistical intrusion detection system (IDS) to detect the rank attack is proposed.
2. The proposed scheme does not affect the network lifetime as all the computation in detection process takes place at the sink.
3. Extensive simulations are performed in Contiki OS based Cooja simulator [10] to demonstrate that the proposed scheme can detect malicious nodes.

The remaining contents of the paper are organized as follows: RPL operations, which are required to establish the network are presented in Section 2. Rank attacks and their impact in RPL are discussed in Section 3. A detailed overview of the existing work on RPL attacks is provided in Section 4. The network model and attacker model assumed for this work are presented in Section 5. Section 6 describes our novel sink based intrusion detection scheme for the detection of the rank attack. Section 7 provides the detailed experimental evaluation and Section 8 concludes the paper.

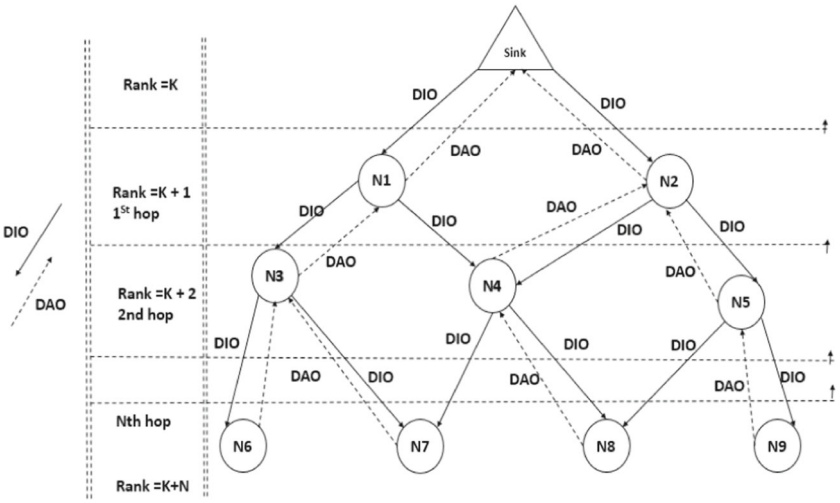
2 RPL operations

In order to construct and maintain the topology or a DODAG [7], four control messages are used by RPL. These include (i) DODAG information solicitation (DIS), (ii) DODAG information object (DIO), (iii) DODAG destination advertisement object (DAO), and (iv) DODAG destination advertisement object acknowledgment (ACK). Neighboring devices are discovered and to request for a DIO message from neighbors for joining the DODAG are done using this message. DODAG information object (DIO) has a major role and this control message is intermittently multicast by all RPL nodes in the network. For topology construction and maintenance, essential network information is contained by it. Every DIO control message contains the RPL Instance ID, DODAGID, instance version number, rank, and other requisite information required for topology creation and maintenance. Although RPL also constructs and maintains network topology through DIO control messages, but it uses trickle timer [11], which maintains a low frequency of DIO control message. Nodes in a Lossy and shared medium can use the Trickle algorithm. The Trickle algorithm allows nodes to exchange information in a highly robust, and energy efficient manner. Furthermore, this algorithm is simple, and scalable as pointed by [11]. Destination advertisement object (DAO) control message is sent to the preferred parent when a node joins the DODAG effectively and selects its preferred parent. This packet is forwarded to the DODAG root by the parent node. The movement of DAO messages to DIO message is opposite as shown in Fig. 1a and it is unicasted upwards to the root node. The root uses DAO messages to obtain information about the connecting nodes in “DODAG.Storing” and non-storing modes of operations are used for DAO transmission. The DAO message received from its child nodes is momentarily stored by parent node in storing mode. It joins its own DAO information in the packet and sends it to the DODAG root. On the other hand, when any node receives a DAO message, it instantaneously sends it to the DODAG root in non-storing mode. Destination advertisement object-ACK (DAO-ACK) is transferred optionally from sink to leaf nodes in downwards direction for reliable topology formation.

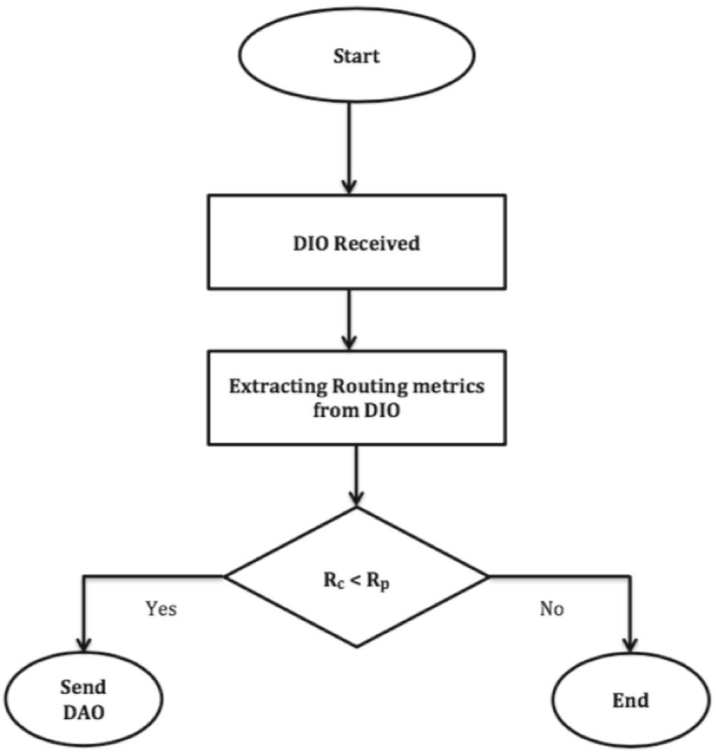
Figure 1b illustrates the parent node selection process, which is invoked every time a node receives a DIO message.

2.1 Topology construction in RPL

The administrator configures the DODAG root node, which is responsible for constructing the complete DODAG topology, initially; the root node [7] calculates RPL instance ID, DODAGID, DODAG version number, base rank, objective function (OF), routing cost, and related information. Sink node multicasts this information in DIO control message to the neighboring nodes. Neighboring nodes extract and use the



(a) Flow of RPL control messages



(b) Selection of Parent node by child node

Fig. 1 **a** Flow of RPL control messages. **b** Selection of parent node by child node

received information on receiving DIO messages to update their rank, to join DODAG and based on best rank chooses preferred parent. Instantly, they send a DAO message to their preferred parent representing that they have joined the network.

Each preferred parent is an intermediate node, which operates as a router between the child node and the root node. The root node is the preferred parent of all initial hop nodes in the network. The initial hop nodes further transmit DIO messages in the downward direction, whereas, the receiving nodes send DAO message upwards to their preferred parent. In Fig. 2, DODAG root (node 1) sets its rank to ($R = 1$) and fills all other essential information in the DIO control message and multicasts it to the neighbors. Neighbor nodes (5, 12, and 19) calculate their own ranks bearing in mind the objective function and they decide to add DODAG root as their preferred parent. After being a part of DOADG nodes 5, 12, and 19 multicasts their DIO messages with rank 2 for neighbors.

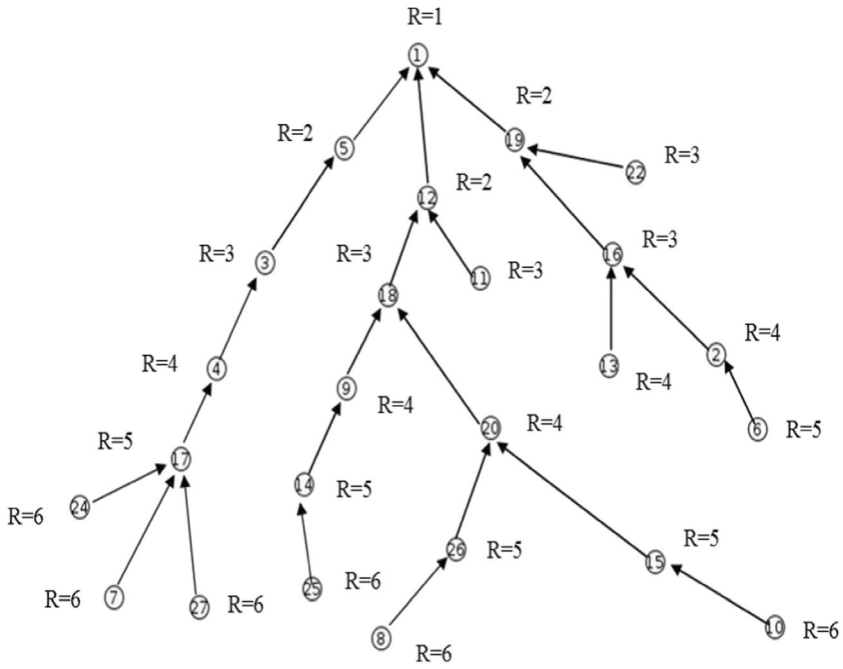


Fig. 2 RPL topology based on ranks

The rank increases downwards in the DODAG. DODAG root ignores DIO from these nodes because of higher rank value depicting that it is coming from downward. Node 12 can add nodes 5 and 19 as a candidate parent if it is in the radio range of node 12. Nodes 12 and 16 join DODAG and choose node 12 as a preferred parent. Noticeably, all further downward nodes receive DIO messages from multiple neighboring nodes but they choose a preferred parent, which has the best rank. Until all the nodes join the DODAG, topology formation continues.

3 Rank attack

In rank attack, malicious node introduces the false rank through DIO on the resultant neighboring node converged towards it, and selected as a preferred parent through DAO. Network performance can be affected once the malicious node becomes the preferred parent node (PPN) in the attacking region [7]. In order to launch a rank attack in RPL network, one malicious node is introduced by the attacker, after the topology set up. All nodes, according to defined OF obey rank rules defining all RPL child nodes select PPN with the lowest rank in RPL. As per standard RPL rules, various paths are established in the network. Under the normal network conditions, we ran a 15-min simulation and collected the network performance results.

Performance assessment is done on the basis of these results which are used as a benchmark. In order to maintain and update RPL network topology, all RPL nodes multicast DIO control message after specific interval to surroundings nodes.

According to standard rules, as shown in Fig. 3, malicious node (MN) 53 selects node 24 as PPN, it announced lowest rank based on objective function (OF) method to attract the child neighboring RPL nodes. Lowest RPL nodes 50, 43 select intruder node 53 as its PPN. MN updates false information in each DIO control message and drops partially data packets received from its child nodes. The paths which are most important to discuss which exists before the presence (MN) surrounding attacking area are as follows.

1) *Path 1:* Node (28) → Node (45) → Node (3) → Node (29) → Node (14) → Node (2) → Node (50) → Node (37) → Node (11) → Node (21) → Node (6) → Node (23) → *Sink*

Fig. 3 RA is launched by node 53

2) *Path2:* Node (44) → Node (29) → Node (14) → Node (2) → Node (50) → Node (37) → Node (11) → Node (21) → Node (6) → Node (23) → *Sink*
3) *Path 3:* Node (49) → Node (50) → Node (37) → Node (11) → Node (21) → Node (6) → Node (23) → *Sink*

We have the subsequent new routes of victim nodes to the sink node after the introduction of MN.

1) *Path 1:*
Node (28) → Node (45) → Node (3) → Node (29) → Node (14) → Node (2) → Node (50) → **Node (53)** → Node (24) → Node (6) → Node (23) → *Sink*
2) *Path2:*
Node (44) → Node (29) → Node (14) → Node (2) → Node (50) → **Node (53)** → Node (24) → Node (6) → Node (23) → *Sink*
3) *Path 3:*
Node (49) → Node (50) → **Node(53)** → Node (24) → Node(6) → Node(23) → *Sink*
4) Path 4: Node (43) → **Node (53)** → Node (24) → Node (6) → Node (23) → *Sink*

4 Related work

In this section, the behavior of RPL protocol is discussed in the presence of various security attacks. LLNs support multi-hop communication in which network devices forward packets to the destination which are generated by other nodes. Security of any protocol is an important aspect for real-time network deployment. RPL is vulnerable to internal and external attacks [12–14]. Rank of nodes is an important parameter in RPL network, which corresponds to the distance to a node from the root (central controller device); it increases downward (sink to nodes) and decreases upward. Rank of a node can be used for route optimization, loop prevention, and topology maintenance. A rank attack can decrease network performance in terms of packet delivery ratio to almost 60% if an attack is launched by the number of malicious nodes as described in [15]. Dvir et al. [8] discussed rank authentication mechanism to avoid false announced rank by using cryptographic techniques; however, these techniques have high computational cost as the nature of devices in IoT are low power. This technique is still vulnerable to other attacks as discussed in [16, 17]. Moreover, if a node is compromised, cryptographic information (keys) are also compromised. Lee et al. [18] proposed monitoring node (MN)-based scheme which acts as watchdogs; each MN has finite state machine (FSM), which makes the decision to detect rank and local repair attack in RPL network. This scheme is not valid for large networks because a large network of MNs is required which will increase communication overhead. Raza et al. [9] purposed an IDS "SVELTE" to detect sinkhole, selective forwarding, and malicious traffic using a utility called 6mapper this hosted at the sink node. However, this work can only be used for the detection of simple rank attack with no objective function [19] and also it has high false alarm rate. K. weekly et al. [20] proposed two techniques, which are applied together to provide defense against an RPL network under sinkhole attack, but still it has control overhead. The solution for the detection of false rank value is proposed in [21] using host-based IDS; it has used a probabilistic scheme in which each node using its neighborhood information attempts to detect false rank value. However, due to resource-constrained nature of RPL, devices in network storage and processing is discouraged by RFC 6550. Zhang et al. [22] proposed a new type of intrusion named as "Routing Choice" (RC). RC is not directly related to the rank attack and is based on false preferred parent selection. The monitoring nodes used for the detection of RC can have high communication overhead in RPL network. Seeber et al. [23] proposed an alternative approach for the detection of various routing attacks in RPL using a trusted platform module (TPM). It recommended offloading all security features from RPL node and introduced an overlay network of TPM node for detection of network attack.

Mayzaud et al. [24] discussed internal attacks in RPL that caused decrease in lifetime of the network. Similarly, Karthik et al. [25] investigated the rank attacks and their impact on RPL network. Airehrour et al. [26] proposed a non-cryptographic trust-based mechanism to identify black hole attack. The attack increases packet drops and control overhead in the network. Secure-RPL (SRPL) [27] techniques prevent RPL network from Rank attack. It uses hash-based authentication mechanism which is based on a threshold value to detect the attack. The computation overhead of the proposed authentication mechanism is relatively high for resource-constrained devices. Kamble et al. [28] described taxonomy of attacks in RPL network and their countermeasures against each attack.

For any protocol to gain wider acceptance and commercial viability in addition to its performance efficiency, its security features. Thus, the focus of this research is aimed at reviewing the security features of RPL protocol primarily in context of tackling the rank attack to mitigate its effects on RPL. The proposed scheme does not impact the longevity of network life as all detection process takes place on the sink node which is rich in terms of memory and processing.

5 System models

In this section, we present the network model and attacker model considered for our proposed scheme.

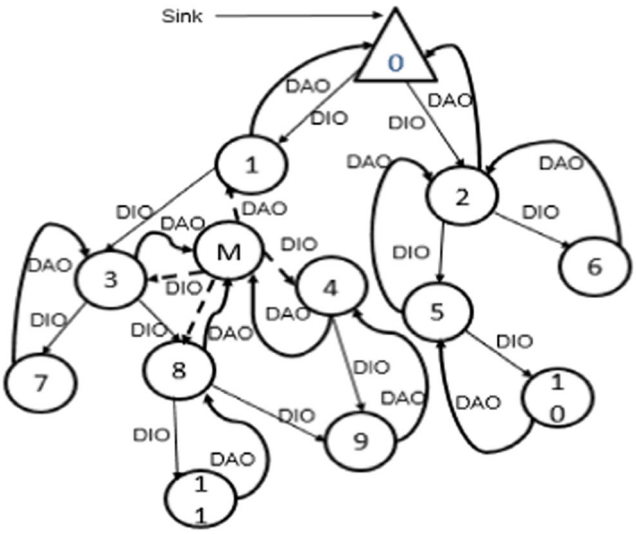


Fig. 4 Attacker model

5.1 Network model

The network model considered consists of the following entities:

Sensor node:

Sensor node is a small device which can be used to capture sensory information, processing and communicating this information to the sink node. It supports [7] both multicast and unicast RPL control messages.

Sink node:

Sink node is an energy-rich device [7] having high processing power as compared to other nodes. It has a collection of secret keys (key ring) containing the symmetric key of each network device. DIO control messages are multicast by the sink node which is further communicated to leaf nodes via intermediate devices. All intermediate nodes issue DAO messages upwards. The DAO messages are sent via preferred parent and integrity of DAO messages is protected using any keyed hash algorithm.

Storing and non-storing mode of DAO:

In storing mode, every node has routing table for its sub DODAG nodes whereas in non-storing mode DODAG root (sink) has a downward route for all DODAG nodes. The non-storing mode provides source routing within the network from sink to leaf nodes. Hence, non-storing mode is more suitable for resource-constrained RPL devices [7].

Malicious node (MN):

Once a network gets stabled, MN advertises lower rank. Consequently, neighboring nodes are converged towards it and select it as PPN through DAO.

5.2 Attacker model

We make the following assumptions about the adversary.

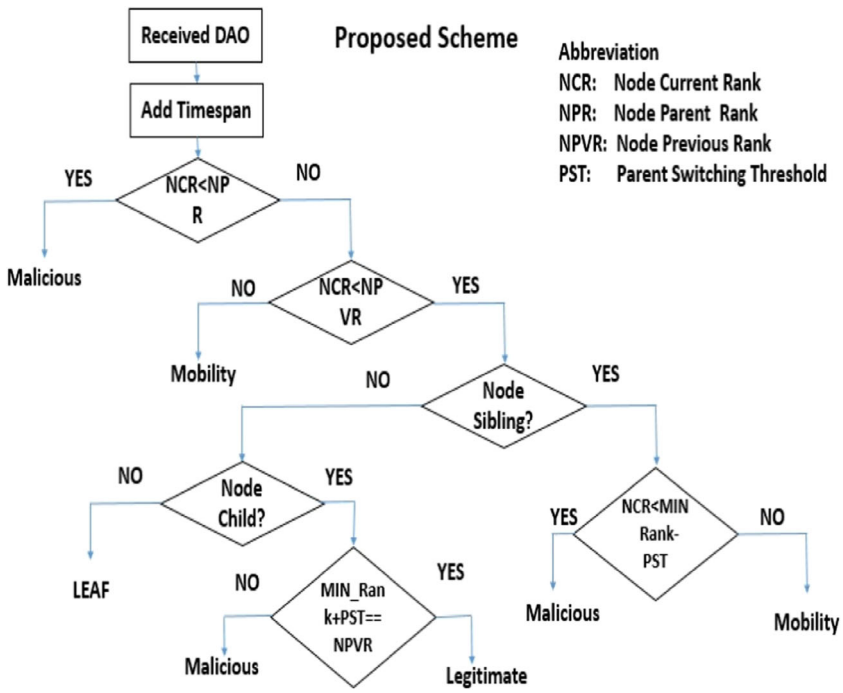


Fig. 5 Rank attack detection at sink

Table 1 List of abbreviations

Abbreviation	Detail
NCR	Node current rank
NPR	Node parent rank
NPVR	Node previous rank
PST	Parent switching threshold

- The sink is trusted and cannot be compromised by an attacker.
- An adversary can deploy malicious nodes in RPL network when the network gets stable.

An adversary can also compromise sensor node by capturing keys, afterwards, node behaves legitimately and introduce minimum rank and routing metric through DIO message. Neighboring corresponding nodes select it as preferred parent through DAO; Fig. 4 shows the attacker model in which malicious node advertise their fake rank neighboring node selects it as PPN through DAO.

6 Sink-based intrusion detection system

Rank is only an attribute used for parent selection within the RPL [7]. Invalid rank is considered if a node decreases its rank below its certain threshold called parent switching threshold (PST) less than the advertised rank. For the detection of the rank attack using a sink-based intrusion detection system (SBIDS), Fig. 5 shows the proposed approach used. In non-storing mode, each node sends their IP address, preferred parent IP address, and rank in DAO message after encrypting with key which is shared between node and sink to avoid integrity violation following steps that take place when node sends their DAO message.

Step 1: DAO. *Add* (node IP address, PPN IP address, rank)
Step 2: *Encrypt* (K, DAO)
Step 3: DAO. *Send* ()

After passing DAO message from intermediate nodes upon receiving DAO message at the sink, it will be decrypted. Figure 5 shows flow chart where different detection steps occur to ensure the legitimacy of the node. Timespan will be added to each DAO message which shows freshness of control message. NCR is compared to NPR violating rank rule as mentioned in [7]; it is considered as malicious node otherwise;

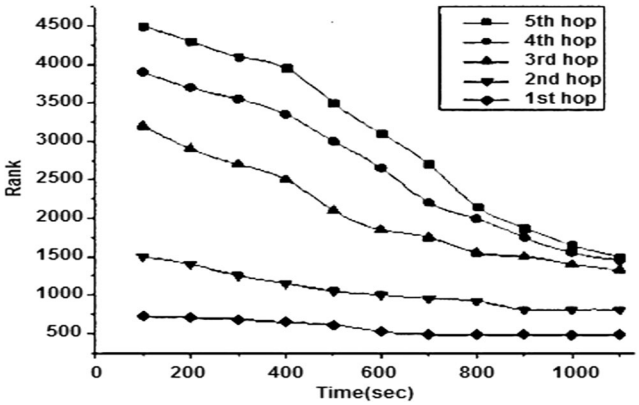


Fig. 7 Rank changes in RPL

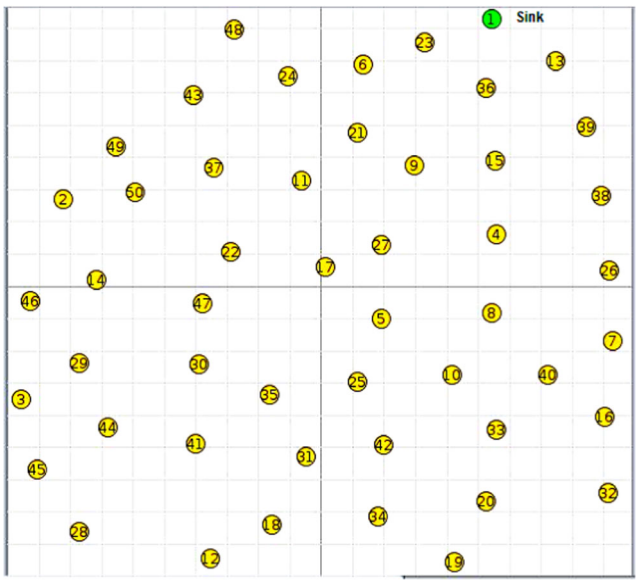


Fig. 6 Random topology comprising sky motes

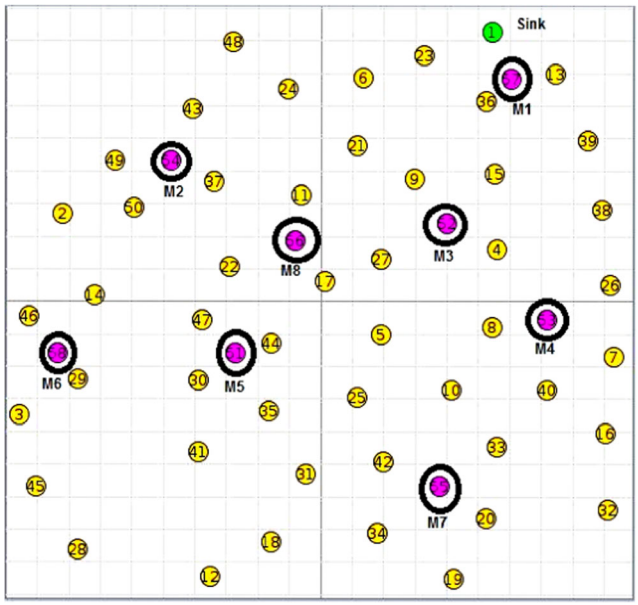


Fig. 8 RPL network under eight malicious nodes

Table 2 Network parameter used for experiment

Network parameters	Values
Network layer	RPL
Mac layer	IEEE 802.15.4
Topology	Random
Simulation area	200 × 200
Simulation time	600 s
Data reporting duration	500 s
Objective function (OF)	MRHF
DIO minimum interval	4 s
DIO maximum interval	17.5 min
Data reporting intervals	1 packet /10 s
Number of malicious nodes	2–8
TX range	20 m
Interference range	30 m
Packet size	50 bytes
Sensor nodes	50
TX power	17.4 mA (0.0174 W)
RX power	18.8 mA (0.0188 W)

it checks if node at t_i rank is less than its t_{i-1} rank than we can say that either it is malicious or it is due to mobility. Under mobility, node does not change their rank when a node reaches its destination position, it becomes stabilized with respect to their neighboring nodes [29]. SBIDS checks a minimum of rank among their siblings and deduct parent switching threshold (if this value exceeds node change their PPN) and then it will compare rank of this node at t_i. If it is less, then it has more probability of malicious node. Figure 5 shows a detailed flowchart of detection steps and Table 1 describes abbreviation detail used in detection process.

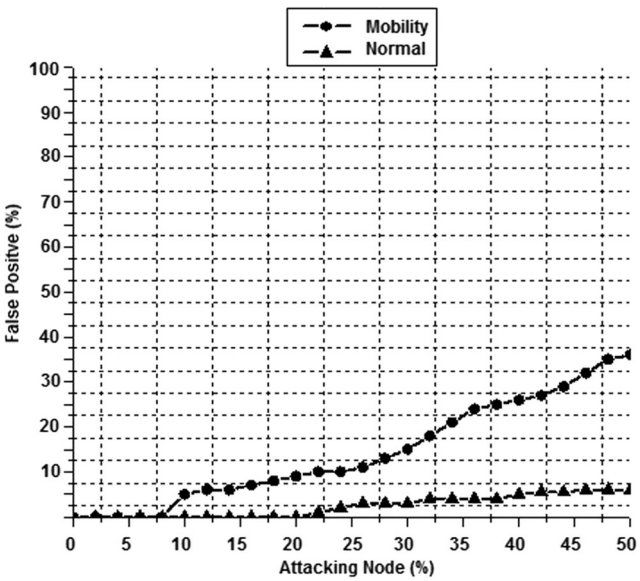


Fig. 9 False positive rate in intrusion identification

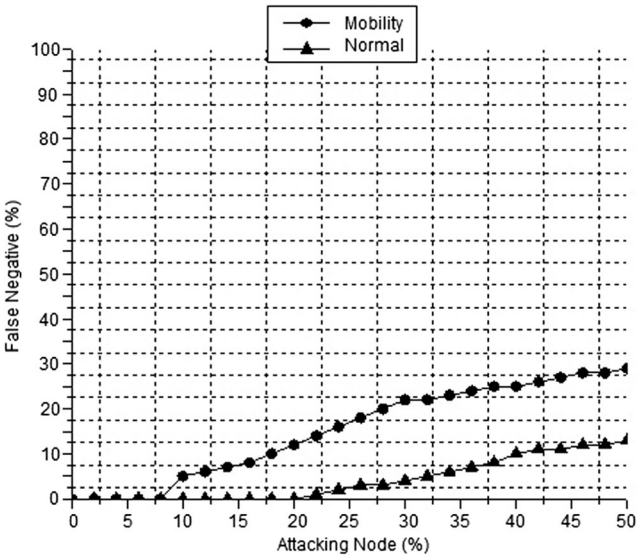


Fig. 10 False negative rate in intruder identification

7 Experimental results

We have used Contiki [10] which is an open-source operating system having high portability and flexibility. It is networked and a multi-tasking system for wireless LLNs of the IoT devices. Hence, it is used for generating simulations in this research. For simulating the performance of various networks, Cooja simulator [10] runs over Contiki OS. Evaluation of protocols is also done by Cooja, which is a Java-based simulator. Cooja also operates as an emulator, where the written code can directly be installed on sensor nodes (for example Sky mote) supporting both Windows and Linux platform. Random topology node arrangements are taken into consideration for testing the detection capability of our proposed scheme. Figure 6 shows our random topology before the rank attack.

Nodes in RPL become stable very quickly after the network deployment. Rank of nodes per hop and how they get

Table 3 Percentage of ACC, TP, TN, FP, FN, and CI under normal condition

AN (%)	TP (%)	TN (%)	FP (%)	FN (%)	ACC (%)	CI (%)
	99	3	0	0	100	95.48–100
10	99	5	0	0	100	95.34–100
15	98.5	3	0	0	100	95.38–100
20	98	4	1	1	98.07	93.69–99.94
25	95.5	5	3	2	95.26	90.71–99.21
30	94.4	5.5	4	4	92.58	91.87–97.99
35	94	5.8	4	8	89.26	88.80–96.52
40	93.5	6	6	10	86.14	85.23–94.98
45	93	8	7	11	84.87	83.10–92.18
50	92.5	9	8	12.5	83.19	81.18–91.10

Table 4 Percentage of ACC, TP, TN, FP, FN, and CI under mobility condition

AN (%)	TP (%)	TN (%)	FP (%)	FN (%)	ACC (%)	CI (%)
5	97	0	0	0	100	95.58–100
10	92.5	0	5	5	90.24	87.88–98.19
15	90.5	1	8	10	83.56	81.24–92.75
20	89	6	14	13.75	77.39	77–92.75
25	88	12	20	15	74.07	72.26–88.05
30	83	16	22	17	71.73	69.78–86.13
35	75	23	25	20	68.53	65.16–82.88
40	70	26	26	24	65.75	62.72–81.24
45	66	32	28	25.5	64.68	59.76–78.98
50	60	36	29	29	62.33	56.55–76.75

stable with the passage of time are shown in Fig. 7. It also reflects the nodes getting more time to stable which are far away from sink in comparison to those nodes which are near.

Malicious nodes are placed at different locations to measure the accuracy of detection by SBIDS. Figure 8 shows setup 8 malicious nodes distributed at different hops. Table 2 shows the network parameters used in the simulation analysis. It also shows node characteristics mirrored according to mote sky sensor nodes [9].

Under normal conditions, SBIDS can detect all malicious nodes, but with the increasing percentage of malicious nodes, the detection rate is decreased. We have measured accuracy of detection by introducing mobility in a network. SBIDS produced four types of errors which are false positive (FP), false negative (FN), true positive (TP), and true negative (TN). FP is produced, when a node moves from higher hop to lower hop and as a result, it gives the shortest path to their neighbors towards the sink. On the other hand, if MN joins the network as a leaf node SBIDS detects as FN. The accuracy of SBIDS to correctly identify attacking node as TP or TN depends on detecting non-attacking node.

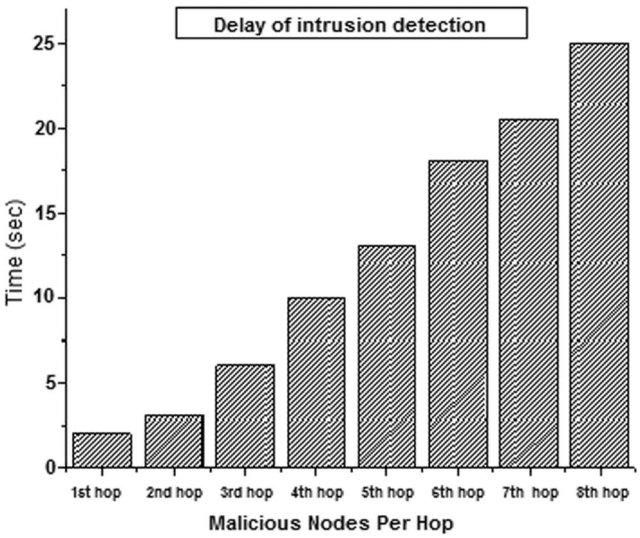


Fig. 11 Latency of malicious node detection

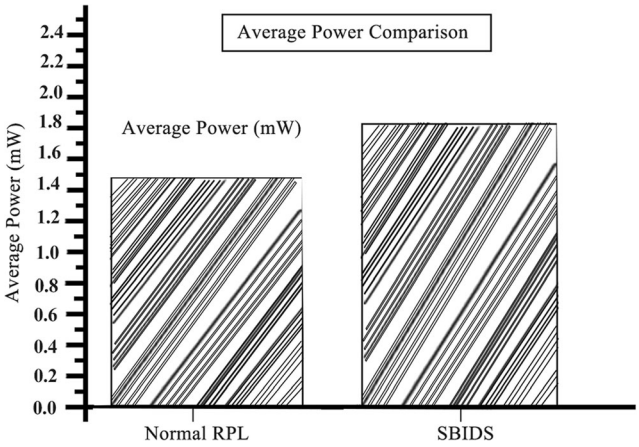


Fig. 12 Average power consumption

The detection capability of SBIDS is tested by increasing the percentage of malicious nodes and introduced mobility in the network. Each simulation is executed 20 times and average results are presented. Figures 9 and 10 show false positive and false negative rate. Table 3 shows accuracy of SBIDS under normal condition and similarly. Table 4 shows SIBDS accuracy under mobility on the basis of 95% confidence interval (CI).

We have measured detection time takes SBIDS at various hops as mentioned in Fig. 11; malicious nodes are placed at different hops.

It is concluded that distance of malicious node is directly proportional to the time taken for the detection. Figure 11 shows the latency of malicious node detection.

SBIDS provides 100% accuracy under normal conditions, but the accuracy is decreased by increasing number of nodes with mobility. Hence, extra 48 bit (16-bit IP address, 16-bit rank, 16-bit parent ID) is used in DAO packet which is communication overhead of SBIDS.

In IoT, nodes are battery powered and have limited resources in terms of memory power and energy. The average power consumption of 50 nodes is measured using Contiki power trace [30]; simulation setup is same as mentioned in Fig. 5. We ran simulation for 15 min under normal condition (when DAO control messages are not modified) and after SBIDS (adding extra 48 bits in DAO control message). Figure 12 shows that DAO control message consumes more power.

8 Conclusion

In the current decade, efforts are underway to connect networks of miniature-sized and resource-constrained devices with the Internet using IPv6 protocol to form IoT. RPL is

proposed by working group of IETF to be used in IoT. Several internal attacks are identified in RPL including rank attacks. Malicious node advertises false rank in rank attack to its neighboring nodes to disrupt the directed graph-based network topology. The attack on rank creates unoptimized paths, loop formation, overhead, and more packet collisions causing downgrading of the network performance in terms of increasing end-to-end delay, decreasing the packet delivery ratio, and increasing the energy consumption of the network devices.

In this work, the detailed behavior of RPL protocol is analyzed. A novel sink-based intrusion detection system is proposed which detects malicious nodes with high accuracy. This scheme has less computational overhead as all detection processes take place at the sink. Detailed simulation analysis of SBIDS shows that it is an effective method for identifying rank attack in RPL networks. In future, the proposed SBIDS algorithm can be enhanced to accommodate more routing metrics along with rank including energy, throughput, hop count, trace load, bandwidth, and delay. Furthermore, rank attack detection can be accomplished via lightweight cryptographic solutions.

Acknowledgments The authors would like to thank Higher Education Commission of Pakistan, COMSATS Institute of Information Technology, and Bahria University Islamabad, for their continuous support for our research.

References

1. Atzori L, Iera A, Morabito G (2010) The Internet of Things: a survey. Comput Netw 54(15):2787–2805
2. Whitmore A, Agarwal A, Da Xu L (2015) The Internet of Things: a survey of topics and trends. Inf Syst Front 17(2):261–274
3. Da Xu L, He W, Li S (2014) Internet of things in industries: a survey. IEEE Trans Ind Inform 104:2233–2243
4. Chen, T-Yi, et al (2013) A IoT application of safe building in IPv6 network environment. computer software and applications conference (COMPSAC), 2013 I.E. 37th Annual. IEEE, pp 748–753
5. Ruan DX, Wu D, Wu XB (2012) The Internet of things technology in logistics application: stages, trend and drive modes. Management of Technology (ISMOT), 2012 International Symposium on IEEE, pp 452–455
6. Clausen T, Herberg U, Philipp M (2011) A critical evaluation of the IPv6 routing protocol for low power and lossy networks (RPL). wireless and mobile computing, networking and communications (WiMob), 2011 I.E. 7th international conference on. IEEE
7. Winter T, Thubert P (2010) RFC 6550: RPL: IPv6 routing protocol for Low-Power and Lossy Networks, Internet Engineering Task Force (IETF) Request For Comments, March
8. Dvir A, Holczer T, Buttyan L (2011) VeRA-version number and rank authentication in rpl. Mobile Adhoc and sensor systems (MASS), 2011 I.E. 8th International Conference on. IEEE
9. Raza S, Shahid LW, Voigt T (2013) SVELTE: real-time intrusion detection in the Internet of Things. Ad Hoc Netw 11(8):2661–2674
10. Ali H (2012) A performance evaluation of RPL in Contiki: a Cooja simulation based study, Master Thesis Blekinge Institute of Technology, School of Computing
11. Levis P, Clausen T, Hui J, Gnawali O, Ko J (2011) RFC 6206: the trickle algorithm draft-ietf-roll- trickle-08, Internet Engineering Task Force (IETF) Request For Comments, Jan
12. Mayzaud A, Badonnel R, Chrisment I (2016) A taxonomy of attacks in RPL-based Internet of Things. Int J Netw Secur 18(3):459–473
13. Pongle P, Chavan G (2015) A survey: attacks on RPL and 6LoWPAN in IoT. Pervasive computing (ICPC), 2015 International Conference on. IEEE,. pp 0–5
14. Wallgren L, Raza S, Voigt T (2013) Routing attacks and countermeasures in the RPL-based internet of things. Int J Distrib Sens Netw 9(8):794326
15. Le A, Loo J, Luo Y, Lasebae A (2013) The impacts of internal threats towards routing protocol for low power and lossy network performance, IEEE Symposium Computer and Communications (ISCC), pp 789–794
16. Landsmann M, Wahlisch M, Schmidt T (2013) Topology authentication in RPL. computer communications workshops (INFOCOM WKSHPS), 2013 I.E. conference on. IEEE, pp 73–74
17. Heiner P, et al (2013) TRAIL: topology authentication in RPL. arXiv preprint arXiv:1312.0984
18. Anhtuan L, et al (2011) Specification-based IDS for securing RPL from topology attacks. Wireless Days (WD), 2011 IFIP. IEEE, pp 4–6
19. Takumi M, Toyoda K, Sasase I (2015) Low false alarm attacker's detection in RPL by considering timing inconstancy between the rank measurements. IEICE Commun Express 4(2):44–49
20. Weekly K, Pister K (2012) Evaluating sinkhole defense techniques in RPL networks. Network protocols (ICNP), 2012 20th IEEE International Conference on. IEEE
21. Iuchi K et al (2015) Secure parent node selection scheme in route construction to exclude attacking nodes from RPL network. IEICE Commun Express 4(11):340–345
22. Zhang L, Feng G, Qin S (2015) Intrusion detection system for RPL from routing choice intrusion. Communication Workshop (ICCW), 2015 I.E. International Conference on. IEEE, pp 2652–2658
23. Sebastian S, et al (2013) Towards a trust computing architecture for RPL in cyber physical systems. Network and service management (CNSM), 2013 9th International Conference on. IEEE, pp 134–137
24. Anthea M, Badonnel R, Chrisment I (2017) A distributed monitoring strategy for detecting version number attacks in RPL-based networks. IEEE Trans Netw Serv Manag
25. Karthik VK, Pushpalatha M (2017) Addressing attacks and security mechanism in the RPL based IOT. Int J Comput Sci Eng 5(5):1715–1721
26. Airehrour D, Gutierrez J, Ray SK (2016) Securing RPL routing protocol from blackhole attacks using a trust-based mechanism. Telecommunication Networks and Applications Conference (ITNAC), 2016 26th International. IEEE
27. Glissa G, Rachedi A, Meddeb A (2016) A secure routing protocol based on RPL for Internet of Things. Global Communications Conference (GLOBECOM), 2016 IEEE. IEEE
28. Kamble A, Malemath VS, Patil D (2017) Security attacks and secure routing protocols in RPL-based Internet of Things: survey. Emerging Trends & Innovation in ICT (ICEI), 2017 International Conference on IEEE
29. Lee KC, et al (2012) RPL under mobility. Consumer Communications and Networking Conference (CCNC), 2012 IEEE. IEEE
30. Adam D et al (2011) Powertrace: network-level power profiling for low-power. Wirel Netw