Webology (ISSN: 1735-188X)
Volume 18, Number 5, 2021

Location Based Rank Attack Detection Technique (LRADT)

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 – 620 002, India.

Abstract
Internet of Things (IoT) turns up the computerized world with smart automated system through Internet. IoT has lots of issues such as internet outage, light weight, connectivity, big data privacy and security in the connected environment. Network security is the predominant issue in Routing Protocol for Low Power and Lossy Networks (RPL) based IoT. Rank attack is one of the issues in RPL. Rank attack is ruinous to RPL based network in Internet of Things compared with other attacks. In this paper, location based rank attack detection technique is proposed (LRADT). This technique uses distance of each node to find the location of the given nodes to root node in a network. The technique LRADT surpasses the existing technique RDAID by means of packet delivery ratio, attack detection rate and throughput.

Keywords: IoT, Rank Attack, Security, LRADT

1. Introduction

1.1 IoT

In 1999, Kevin Ashton coined the term "Internet of Things (IoT)". According to Kevin Ashton, IoT is a technology which connects physical and virtual things via Internet. Each thing in the connected system has its own identity and attributes. IoT is a resource constrained technology which supports low power, low memory and so on. It only supports light weight process over the connected network. IoT has different layered architecture with regard to the users' requirements or needs. But three layer architecture is the most common and widely used architecture.

1.2 IoT Architecture

The internet |Engineering task force (IETF) explicates three layer architecture in Internet of Things. Taking into account the rapid requirements of the IoT users, the three layer architecture is reformed into four layer architecture, five layer architecture and seven layer architecture. The three layer architecture is the fundamental for all other architectures. It comprises of perception layer, network layer and application layer.

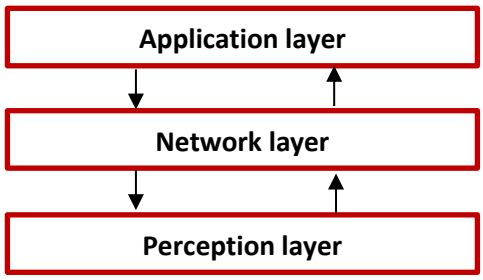

Fig 1.1 IoT Three Layer Architecture

Perception layer monitors the physical properties of the connected things in IoT network. It has the responsibilities of collecting data from the sensors which are embedded in the smart things. Network layer is responsible to connect things, network devices and servers. It is also used to process and transmit the collected data to the application layer. Standard protocols are used to transmit the data. Application layer provides various services to the IoT users according to their needs based on the available data.

1.3 Issues in IoT

Though, IoT is an emerging technology, it is weakened by lots of issues. The various issues in IoT are as follows.

Internet outage:

Internet connection is mandatory for Internet of Things for connecting and communicating smart things. If the Internet connection is unavailable, the entire IoT system is inoperable. And also poor Internet connection leads to worst service.

Light weight:

IoT is a resource constrained technology. It supports only lightweight mechanisms in the IoT system. The heavyweight mechanism cannot be used in IoT. But, for solving critical problems, IoT needs heavy weight mechanisms.

Connectivity:

Due to the rapid growth of IoT technology, numerous devices are connected in a single IoT system. Connecting N number of devices in a single system causes various issues such as device failure, connection problem, poor quality of service, reliability and hard to handle big data.

Big data:

Tremendous devices generate enormous data in IoT. As IoT is resource constrained, the enormous data cannot be stored in the IoT system. So storing and processing big data is not possible in IoT.

Privacy:

IoT accesses anything at any time at anywhere. Everyone or everything which is connected to IoT can easily be tracked. So the privacy of IoT users is a challenging issue.

Security:

Crucial data of the users are collected by the IoT devices which should not be revealed to anyone except the concerned users. Since, IoT is connected through Internet at all the time, an intruder can easily hack the data and system. Collected data is processed by network layer, the network security is more important. Various protocols are used in network layer. RPL is one of the network protocols in IoT. Different attacks occur in RPL protocol. So there is a need to provide a new technique to identify the attacks in RPL.

1.4 RPL

Routing Protocol for Low-Power and Lossy Networks is explicitly designed for Low power Lossy Network. It is used in IoT for routing. RPL uses Destination Oriented Directed Acyclic Graph (DODAG) to form the network. It utilizes four types of control messages to construct DODAG. The control messages are as follows (i) DODAG information Object (DIO) which is used for providing node basic information. (ii) DODAG Information Solicitation (DIS) is used for probing neighbour nodes in the network. (iii) DODAG Advertisement Object (DAO) is used to propagate reverse route information. (iv) DODAG Information Advertisement Acknowledgement (DAO_ACK) provides acknowledgement for DAO message. For constructing DODAG, the objective function such as Expected Transmission Count (ETX), Hop count and Energy are used.

1.5 Rank Attack

Position of a node towards the root node is specified by the Rank. A node in the network selects its parent which is less than its Rank. The rank of a parent node must be less than its child node. Inconsistent change of rank in the network may form loop. Illegitimate change in the rank of a node over RPL protocol is called as rank attack in the IoT network. The rank attack is classified into two types namely rank increased attack and rank decreased attack. Impacts of rank attacks are less packet delivery ratio, worst parent selection and high packet loss.

The proposed LRADT technique is used to detect both rank increased attack and rank decreased attack. The technique uses location of the nodes to identify attack in the network. It is simulated using Contiki OS and Cooja simulator with fifty nodes in random position environment.

Rest of the paper is formulated into different sections such as review of literature which speaks about the related works of rank attack, methodology which explicates the proposed technique, result and discussion which justifies the proposed technique, experimental result which brings out the fact of the proposed work in virtual IoT environment and finally conclusion.

II Review of literature

Shadab Alam et al..[1] discussed the enabling technologies in Internet of Things. The authors explained requirements of IoT system with concerned application.

Mark Mbock et al.[2] detailed the privacy and security issues in IoT in terms of security requirements, techniques to face IoT threats and counter measuring the privacy issues. The threat taxonomy was figured out relatively to the current IoT applications scenario.

Akanksha Jain et al.[3] surveyed attacks and countermeasures for RPL protocol. The paper was one of the bedrocks to learn and analyze distinct attacks in RPL routing protocol. The authors unfolded the impacts of various attacks such as sinkhole attack, wormhole attack, selective forward attack and rank attack in IoT network. The paper was a panacea to fathom out the countermeasure of the RPL attacks.

Somnath Karmakar et al.[4] analyzed the attacks in RPL based Internet of Things and found that rank attack was the predominant attack among other attacks which caused detrimental impacts on the IoT system. Authors proposed a technique to detect rank attack with low overhead. The technique was used to detect both rank increased attack and rank decreased attack in non-storing mode. The proposed technique made use of DAO control message by incorporating message authentication code in the control message to detect the attack. The technique was energy efficient and provided better detection accuracy. It was implemented by Cooja simulator.

Nabil Djedjig et al.[5] recommended a new RPL version using trust based mechanism. Trusted platform module was used to check the trustworthiness of the proposed RPL. The new RPL version was evaluated by the authentication method in the trusted platform module. The behavior of the available nodes in the network analyzed to confirm trustworthiness of the IoT system.

Eli Kfoury et al.[6] suggested intrusion detection system to detect attacks in the RPL protocol. The self-organization map was trained by the supervised learning method to detect the attacks. The abnormal behavior in the protocol was found using the self-organization map. The required data for the model was generated using Cooja simulator by running the RPL based IoT network system. It performed better in terms of energy consumption and attack detection accuracy

Mina Zaminkar et al.[7] proposed SoS-RPL to secure against sinkhole attack in Internet of Things. It consisted of two sections. The first section was used to rate and rank the nodes using distance. The second section was used to discover the malicious sources in the IoT network by calculating average packet transmission of route request (RREQ). The SoS-RPL was tested using NS-3 simulation. It provided good packet delivery rate and better detection rate.

Mina Zaminkar et al.[8] suggested DSH-RPL for secured IoT ecosystem. It comprised of four phases. Reliable RPL was created in the first phase. In the second phase the sinkhole attack

was detected. The detected malicious nodes were quarantined in the third phase. In the fourth phase, data was transmitted after homomorphic encryption process. It reduced false positive rate and false negative rate. It increased packet delivery rate compared with Sec Trust-RPL and IBOOS-RPL.

Zahrah et al.[9] proposed SRPL-RPL protocol to detect and mitigate rank and version number attacks. The attacks were detected using rank strategy. The mitigation was done using threshold and attack status table. The proposed SRL-RPL was compared with existing system such as sink based intrusion detection systems and RPL+Shield technique. The proposed SRPL-RPL outperformed better than these existing protocols with regard to packet delivery ratio, energy consumption and attack detection accuracy rate.

3. Methodology

Location based rank attack detection technique (LRADT) is proposed to detect rank attack in hop count based RPL construction. The proposed technique calculates distance of each node to its parent node and to its root node, to identify the node location. The location of each node is identified by calculating the distance of each node and stored in the root node. The distance of a node is compared with its parent's distance to root node, when there is an inconsistent change in the rank of the parent and child. If the distance and rank of the current node are less than its parent then it is affected by rank decreased attack. If the distance is less than its parent and rank is higher than the parent then the node is affected by rank increased attack. The affected node is cleared away from the network. The logic behind the rank and distance is, while constructing RPL network by hop count as the objective function parent node must have less distance than the child node. LRADT is compared with the RDAID technique. The RDAID technique uses packet delivery ratio of each transaction of the nodes in the network. The LRADT performs better than the RDAID technique in terms of packet delivery ratio, throughput and attack detection rate.

3.1 Theoretical Analysis

The location based rank attack detection technique is used to detect rank attack specifically while setting hop count as an objective function in RPL network. For examining the proposed technique, the RPL based IoT network with ten nodes (A,B,C,D,E,F,G,H,I,J) has been taken. Node "A" is the root node. The rank of a node is shared by the DIO message in the RPL network. Fig. 3.1 represents the RPL network with rank of each node towards root node before attack.

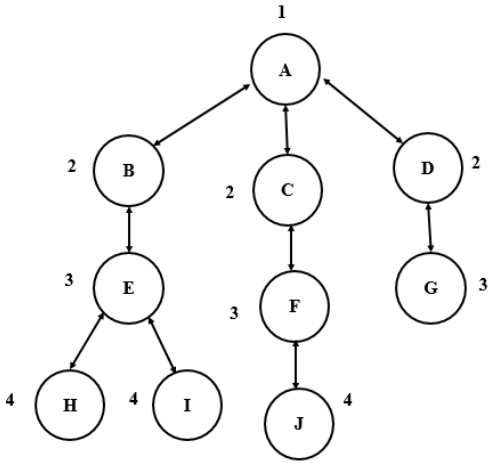

Fig. 3.1 RPL network before attack

Table 3.1 shows the distance of each node from the root node as well as to its parent node. This table is stored in the root node. The distance of the nodes in the given network is calculated periodically. The X and Y values for finding location of the nodes given in the table are taken from Cooja simulator. For identifying the location, first the distance from node to its parent is calculated and then the distance from node to root is calculated.

Table 3.1 Location of the Nodes

Node	Rank	X	Y	Distance to its parent	Distance to the root
A	1	76.42	23.14	--------	---
B	2	46.95	45.17	51.5	51.5
C	2	78.29	47.96	26.69	26.69
D	2	112.7	44.24	57.38	57.38
E	2	45.71	67.19	23.26	74.76
F	3	81.70	72.78	28.23	54.92
G	3	111.4	70.91	25.37	82.75
H	4	126.17	96.66	48.51	123.27
I	4	56.88	94.28	15.92	90.68
J	4	82.94	99.76	28.22	83.14

Before the occurrence of rank attack, the parent nodes have lower rank than their children nodes. Fig 3.2 depicts the rank attack scenario. In Fig 3.2, node E is considered as a malicious node which is affected by rank attack. For identifying whether the node is affected by rank attack, rank of the node E and its parent's rank are compared. The parent node must have low rank than its child / children.

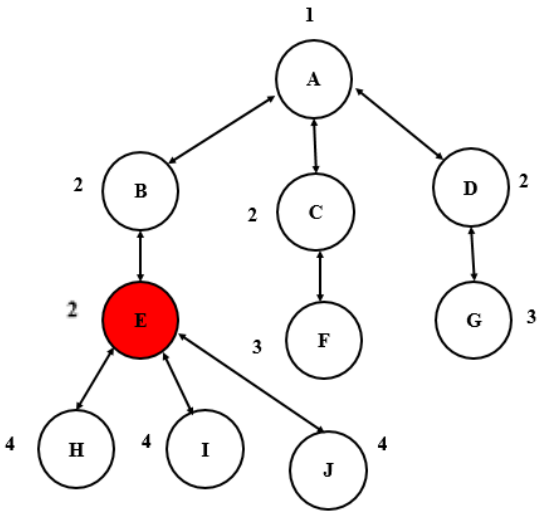

Fig. 3.2 RPL network after attack

Rank of node E is 2 as well as the rank of its parent also 2. Ranks of both nodes are same. So, there is an illegitimate change in the rank. Now, for identifying which node is affected by the rank attack, the location of both nodes are found by calculating distance of both nodes. In the table 3.1 node E is located 74.76 meters from the root node and node B is located 26.69 meters from the root node. So, node E is far away from the root node compared with node B. Now it is found that node E is affected by rank attack. Fig 3.3 depicts re-construction of the network.

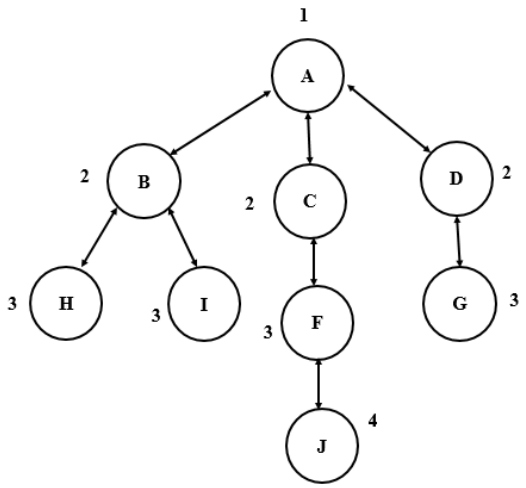

Fig. 3.3 RPL network after reconstruction

The affected node E should be removed from the network. The root node sends the message to all the nodes in the network that node E is affected by rank attack. The nodes connected with node E receive the message from root node and remove node E from the network. After removing the affected node, the nodes will form new network with a new version.

3.2 Labels used in the Technique

X – Root node,
P – Parent node
N – Nodes in the network
Y – Neighbor nodes
K –Current node
R – Rank of a Node
C – Child node

Input : RPL Control messages, LRADT
Output : Rank Attack Detection

1: X multicasts the DIO message and followed by N to start DODAG construction

$$X, N \xrightarrow{DIO} Y$$

2: Yi receive and accept DIO message

3: Compute R

$$R(K) = R(P) + HC(K, P)$$

$$R(P) < R(K)$$

4: Child Node unicasts DAO message to its selected preferred parent node

$$C \xrightarrow{DAO} P$$

5: P sends DAO_ACK message to C then the DODAG is constructed.

6: Identify the node location by Calculating D for all nodes from K to P and K to X

$$D = | x2-x1| + |y2-y1|$$

7: If $R(K) > R(P(K)) \&\& D(P(K)) < D(K)$ then

K is legitimate node

8: If $R(K) < R(P(K)) \&\& D(P(K)) > D(K)$ then

K is affected by Rank Decreased Attack then remove K from the network

9: If R(K) < R(P(K)) && D(P(K)) D(K)then

K is affected by Rank increased Attack then remove K from the network

10: Form the new network after eliminating malicious nodes

The above proposed technique uses traditional process for constructing DODAG in RPL which is given in the technique from step 1 to step 5. The novelty of the proposed work is to identify the rank attack using location of the nodes in the network which is given in the technique from step 6 to step 10.

4. Experimental Evaluation

Contiki operating system and Cooja simulator are used for deploying the proposed technique. It is one of the best network simulation tools for IoT. Simulation is done with the proposed technique for fifty nodes. In Fig 4.1, the green colour node is root node. The yellow colour nodes are legitimate nodes and pink colour nodes are malicious nodes affected by rank attack.

Fig 4.1 Attack simulation

In output window, the affected nodes are listed. The packets are analyzed in 6LOWPAN analyzer mode in Cooja simulator. Fig 4.2 shows the comparison of RDAID and LRADT techniques. It shows the performance metrics evaluation in percentage.

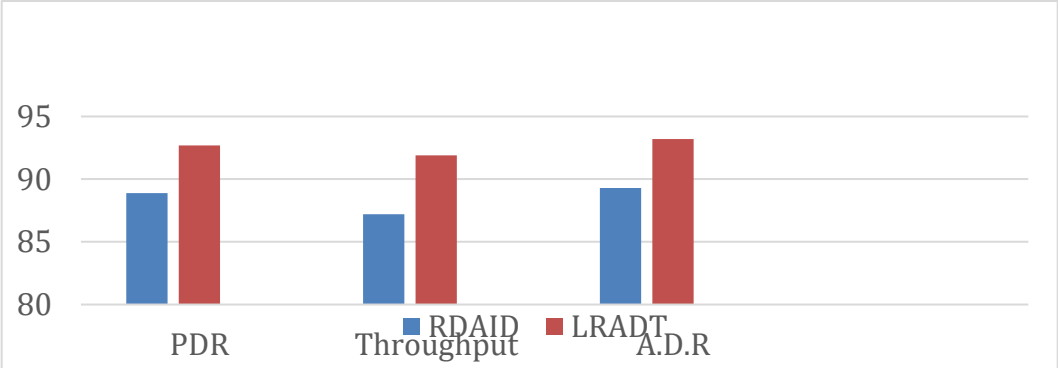

Fig 4.2 Attack simulation comparison

The attack detection rate (A.D.R) is measured using confusion matrix. Proposed technique outperforms the existing technique RDAID in terms of packet delivery ratio, throughput and attack detection rate. The better attack detection rate leads to better packet delivery ratio and the better packet delivery ratio leads to better throughput in the network. These are achieved by the proposed "LRADT" technique.

Conclusion

The technique "LRADT" is the proficient technique to detect and mitigate rank attack in hop count based RPL network in IoT. It uses location of a node to find out the rank attack. It outperforms the RDAID technique in terms of packet delivery ratio, throughput and attack detection rate. The technique is implemented using Cooja simulator in sky Mote with fifty nodes. In future, the work will be enhanced to detect rank attack in ETX and Energy based RPL network in IoT.

References

[1] Shadab Alam, Shams Tabrez Siddiqui, Ausaf Ahmad, Riaz Ahmad and Mohammed Shuaib, "Internet of Things (IoT) Enabling Technologies, Requirements, and Security Challenges", Advances in Data and Information Sciences, https://doi.org/10.1007/978-981-15-0694-9_12, pp. 119-126, 2020.

[2] Mark Mbock Ogonji, George Okeyo and Joseph Muliaro Wafula, "A survey on privacy and security of Internet of Things", Computer Science Review, pp. 1-19, 2020.

[3] Akanksha Jain and Sweta Jain, "A Survey on Miscellaneous Attacks and Countermeasures for RPL Routing Protocol in IoT", Emerging Technologies in Data Mining and Information Security, Advances in Intelligent Systems and Computing, https://doi.org/10.1007/978-981-13-1501-5_54, pp. 611 - 620, 2019.

[4] Somnath Karmakar, Jayasree Sengupta and Sipra Das Bit, "LEADER: Low Overhead Rank Attack Detection for Securing RPL based IoT", IEEE, International Conference on COMmunication Systems & NETworkS (COMSNETS), pp. 429-437, 2021.

[5] Djedjig Nabil, Djamel Tandjaoui and Faiza Medjek, "Trust-based RPL for the Internet of Things", IEEE Symposium on Computers and Communication (ISCC), pp. 962-967, 2015.

[6] Elie Kfoury, Julien Saab, Paul Younes and Roger Achkar, "A self organizing map intrusion detection system for rpl protocol attacks." International Journal of Interdisciplinary Telecommunications and Networking (IJITN) Volume 11, Issue no. 1, pp. 30-43, 2019

[7] Mina Zaminkar and Reza Fotohi, "SoS-RPL: securing internet of things against sinkhole attack using RPL protocol-based node rating and ranking mechanism." Wireless Personal Communications, pp. 1287-1312, 2020.

[8] Mina Zaminkar, Fateme Sarkohaki and Reza Fotohi, "A method based on encryption and node rating for securing the RPL protocol communications in the IoT ecosystem." International Journal of Communication Systems, Volume 34, Issue 3, pp. 1-24, 2021.

[9] Erol Gelenbe, Piotr Frohlich, Mateusz Nowak and Dimitrios Tzovaras "IoT Network Attack Detection and Mitigation", IEEE, Mediterranean Conference on Embedded Computing (MECO), pp. 1-6 , 2020.

[10] Zahrah A. Almusaylim , NZ Jhanjhi and Abdulaziz Alhumam, "Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP." Sensors, Volume 20, Issue 21, pp. 1-25, 2020.