Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

RSSI Based Rank Attack Detection Technique For RPL

A.Stephen[1] , Dr. L. Arockiam[2]

[1]Research Scholar**,** Department of Computer Science, St. Joseph's College (Autonomous), (Affiliated to Bharathidasan University), Tiruchirappalli – 620 002, India.

[2]Associate Professor Department of Computer Science, St. Joseph's College (Autonomous), (Affiliated to Bharathidasan University), Tiruchirappalli – 620 002, India.

Abstract

"Internet of Things (IoT)" is ahead of the curve in the digital era for the last ten years. IoT is the best thing since sliced bread which makes hard work into smart work in our day- to-day life. IoT connects things over the internet to communicate with each other in a network as an automated system. Routing Protocol for Low-Power and Lossy Networks (RPL) is a routing protocols which is used in IoT network. Several attacks have happened in RPL protocol. Rank attack is the most vulnerable attack among all other attacks. In this paper, rank attack detection technique based on Received Signal Strength Indicator (RSSI) is proposed. The technique is used only when objective function is set as hop count. The work has been mathematically tested by taking random RSSI values of the nodes and found to be more efficient.

Key words: Rank attack, RSSI, IoT, Objective function

Introduction

IoT

"IoT" is a resource constrained technology which has low power, low memory, and low energy. IoT connects many technologies into one technology to make human work much easier. So, it is booming globally day by day in all the fields such as home automation, smart health care, industrial, military and agricultural fields [11]. In IoT, everything is automated and sensitive data are communicated over IoT network. RPL is one of the network protocols which is used for transferring data from one device to another device.

RPL

RPL is created especially for IoT. RPL uses Destination Oriented Directed Acyclic Graph (DODAG) to form a network. Four control messages are used for constructing DODAG in RPL. The control messages are DODAG Information Object (DIO) which is used for broadcasting a

node information, DODAG Advertisement Object (DAO) which is used for broadcasting destination information, DAO_ACK which is used for responding to the DAO message and DODAG Information Solicitation (DIS) which is used for discovering neighbor nodes to join in the network. The DODAG is formed based on the objective function [12].

Objective Function

Objective function selects and optimizes the route in RPL. The widely used objective functions are Hop Count, Energy, Expected Transmission Count (ETX) and Minimum Rank with Hysteresis Objective Function (MRHOF)[13]. The objective function defines rank metric in RPL to select a node's parent.

Rank

Rank is the location of a node in the network [13]. The rank is increased from top to bottom and decreased from bottom to top. A node selects its parent which has lower rank than its rank [12]. In this paper, the hop count is used as the objective function. A node selects its parent based on hop count which has less hops to reach the root node. There is a possibility of changing rank value from low to high and from high to low by the intruder. The illegitimate changes of rank is called rank attack.

Rank Attack

The purpose of increasing and decreasing rank value is to generate traffic and control overhead in the network [9]. Rank attack is classified into two types such as rank increased attack and rank decreased attack [12]. There are many approaches used to detect rank attack such as Energy based technique, PDR based approach and Nodes' behaviour approach. A novel technique is proposed to identify rank attack while objective function is set as hop count. The node having a minimum hop count has good RSSI value for the communication path.

RSSI

Radio Signal Strength Indicator (RSSI) is used to find out the communication range between two nodes. RSSI is measured in decibel (dB). A node which is very near to another node has good RSSI value. A node which is far from another node has a bad RSSI value. The formula for calculating RSSI value is given below [14].

$$RSSI(X) = A – 10n*\log d$$

A – Received Signal Power

n – Path loss Index

d – Distance

The rest of the paper is structured into review of literature which contains related work of the proposed work, methodology that consists of a technique to detect rank attack, result and

discussion which contains mathematical computation to prove the proposed work is better than the other works based on RSSI and finally the conclusion is given.

Review of Literature

In [1], authors presented an overview of RPL topology, structure, security challenges and attacks against RPL in IoT. All the recent techniques which were used to detect and mitigate the RPL based attacks were clearly discussed. These techniques were compared using Frieddman test.

Zahrah et al. [2] reviewed the different techniques and methods to detect RPL attacks. Rank attack and Version number attack were explained in detail. These two attacks were compared by the attack detection accuracy metrics.

Fatima et al. [3] proposed a framework using machine learning for detecting rank attack and wormhole attack in RPL based IoT. The proposed framework consisted of three modules. The first module was choosing attack detection parameters. The second module was used for building and training the model based on machine learning. And the third module was used for activating the model to test the detection of rank and wormhole attacks.

In [4], RSSI based technique to estimate distance using Node MCU ESP 8266 in IoT was proposed. The authors took 300 sample RSSI values for the purpose of testing. The estimated distance based on the RSSI values was compared with the actual distance to find out the error level.

Mirko Ivanic et al. [5] presented RSSI based distance estimation technique for indoor and outdoor IoT environment. Curve fitting model was applied in this technique for finding the distance.

Mohamad Nikravan et al. [6] proposed a lightweight offline/online signature based scheme for mitigating rank and version number attack in IoT. The proposed scheme contained two phases such as offline phase and online phase. The proposed technique was compared with VeRA and TRAIL. And the proposed scheme secured more than the two existing algorithms.

Ahmed Raoof et al. [7] analyzed RPL protocol and attacks against the RPL protocol. Various techniques and methods used for identifying and mitigating RPL attacks were surveyed. The mitigation techniques were classified based on the attacks. The paper provided brief knowledge about mitigation techniques of RPL attacks.

Rashmi Sahay et al. [8] explored the vulnerabilities of rank property in RPL. The attack graph was presented to analyze various possible threads against rank property in RPL. The impact of the attacks which affected rank property were tested in Cooja simulator in Sky mote.

Felisberto Semedo et al. assessed the vulnerabilities in RPL objective functions for IoT. OF0 and Minimum Rank with Hysteresis Objective Function (MRHOF) were examined in the rank attack environment using Contiki Cooja simulator [9].

Usman Shafique et al. [10] proposed intrusion detection system to detect malicious nodes in RPL based IoT. The proposed work had high computation overhead because the detection process was done in sink node. The IDS was simulated with Cooja simulator.

Methodology

RSSI based rank attack detection technique is proposed specifically for hop count based DODAG construction. The nodes which have minimum hops to reach the root have low rank and nodes which have maximum hops to reach the root have high rank in the network. For each node, the RSSI value is calculated from the node to its parent. The total RSSI value from a node to root is computed by adding RSSI values of current node and RSSI values of its intermediate node. The computed values are stored in the root node .If any inconsistent change in the rank is found, the node is compared with its total RSSI value from root (TRRX) with its parent's total RSSI value from the root (TRRP(X)). If the current node has less RSSI value than its parent and higher rank than its parent then the current node is considered as malicious node. And the malicious node is removed from the network and new network will be formed. This technique contains three phases such as **Construction phase** where DODAG is formed, **TRRX computation phase** where the RSSI computation process is held and **Rank attack detection phase** where rank attack is identified using RSSI value.

Terms used in the Technique

TRRX - Total RSSI value from root node to current node.

Rnode - Root node.

IMn - Inter Mediator node.

X - Current node.

Pnode - Parent node

NBnodes – Neighbor nodes

OF – Objective Function

HC – Hop Count

TRRP(X) - RSSI value from root node to parent node of current node

Technique

Phase I – DODAG Construction

Input: RPL Control messages

Output: DODAG

Step 1: Rnode broadcasts the DIO message to start DODAG construction

Step 2: NBnodes receive and accept DIO message ⇔ OF(Rnode) & OF(NBnodes) =HC

Step 3: Compute Rank based on OF (HC) to select Parent Node

Rank (Pnode) < Rank (Child node)

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

Step 5: Parent node sends DAO_ACK message to its children then the DODAG is constructed.

Phase II – TRRX computation

Input: RSSI (X)

Output: TRRX

Step 1: If Pnode(X) = Rnode Then

TRRX = RSSI(X)

Step 2: If Pnode(X) ≠ Rnode Then

TRRX = RSSI(X+IMn1+IMn2+……IMnn)

Step 3: TRRX is stored in Rnode

Phase III – Rank Attack Detection

Input: TRRX, TRRP(X)

Output: Rank Attack Detection

Step 1: If Rank(X) > Rank(Pnode(X)) && TRRX < TRRP(X) then

X is legitimate node

Step 2: If Rank(X) < Rank(Pnode(X)) && TRRX < TRRP(X) then

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

Step 3: If Rank(X) > Rank(Pnode(X)) && TRRX > TRRP(X) then

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

Step 4: Form the new network after eliminating malicious nodes

Result and Discussion

Fourteen nodes have been taken for testing the proposed technique. The RSSI values of the nodes are taken randomly.

Let S be the set of all nodes in the network then

S = {A,B,C,D,E,F,G,H,I,J,K,N,M,N}

The communication path from Rnode to Nnode be

Path(Rnode, Nnode) = (Rnode, IMn1, IMn2, IMn3,…..IMnn, Nnode)

Path(X,Rnode) = (X, IMn1, IMn2, IMn3,…….IMnn, Rnode)

The communication path from Rnode to X be

If Parent(X) ≠ Rnode then, ∃ IMnode ∈ P(Rnode, Nnode) ------A

If Parent(X) = Rnode then ∄ IMnode -------B

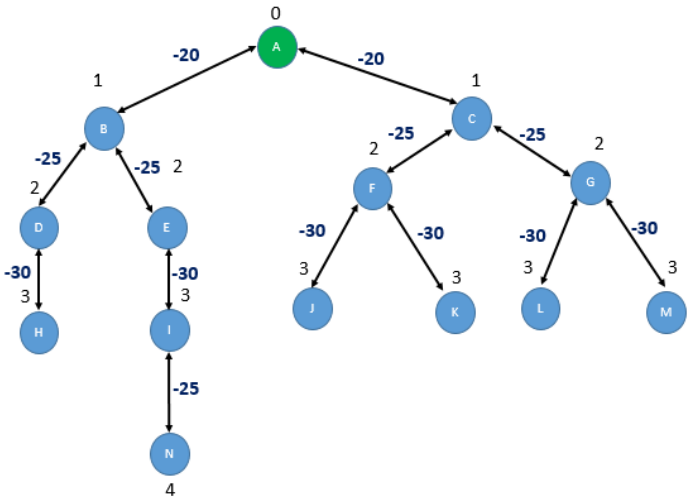

Fig 3.1 Rank and RSSI value of each Node

Fig 3.1 shows the hop count based DODAG construction. The RSSI value of each node concern with their path is given in the fig 3.1. A is the root node of all the nodes in the network. The rank attack detection process is done in the root node by analyzing the total RSSI value of each node (TRRX) in the network.

Table 3.1 Node properties

Node	Parent	Rank	IMN	RSSI(dB)	TRRX(dB)
A	-----	0	-----	---------	--------
B	A	1	-----	-20	-20
C	A	1	------	-20	-20
D	B	2	B	-25	-45
E	B	2	B	-25	-45
F	C	2	C	-25	-45
G	C	2	C	-25	-45
H	D	3	D-B	-30	-75
I	E	3	E-B	-30	-75
J	F	3	F-C	-30	-75
K	F	3	F-C	-30	-75
L	G	3	G-C	-30	-75
M	G	3	G-C	-30	-75
N	k	4	K-F	-25	-100

Table 3.1 shows rank of each node, RSSI values, intermediator nodes for each node and TRRX value from a node to root node. The RSSI value of the each node is taken randomly. Based on the RSSI value, the TRRX is computed.

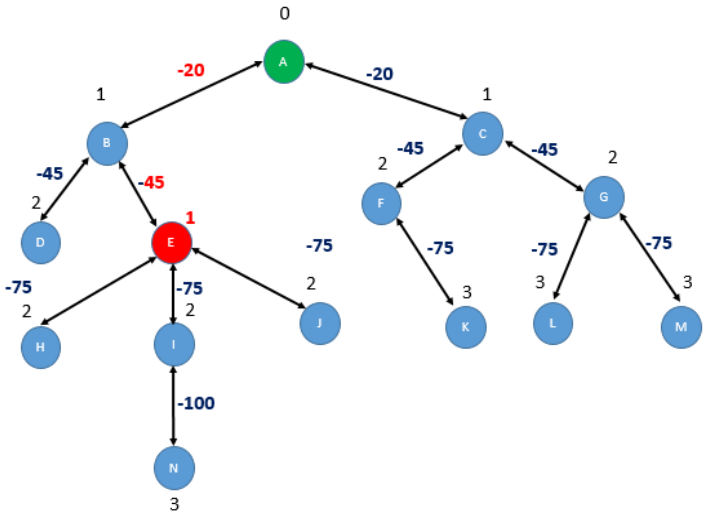

Fig 3.2 Malicious Node Identification

Fig 3.2 depicts the rank attack scenario by considering node E as the malicious node. In this scenario, the malicious node changes its actual value to lower rank in order to attract its nearby nodes in the network. The malicious node E is identified by comparing its TRRX with TRRP(X). From the table 3.1, TRRX(E) < TRRP(E) and Rank(X) < Rank (Parent(X)). So, node E is declared as malicious node.

Here, node H and J select E as their parents without knowing that the node E is affected by rank attack. The decreased rank attack causes several problems in the network such as packet loss, packet dropping and high traffic.

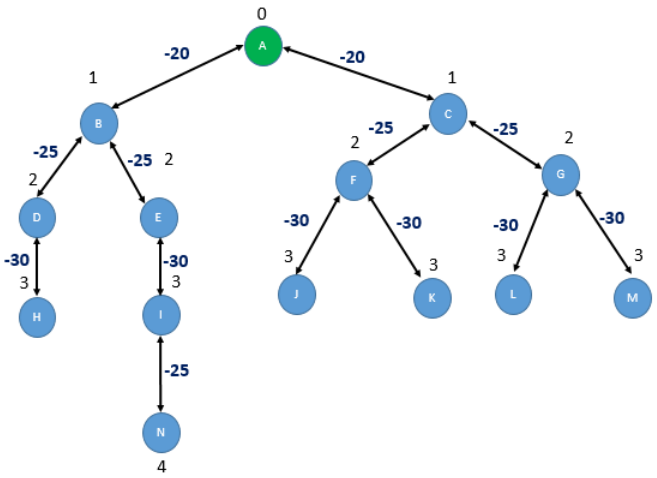

Fig 3.3 Re-construction of DODAG

So, E is declared as malicious node. And the root node informs to all nodes in the network that E is a malicious node and eliminates the node E from the network. After eliminating node E, the network is re-constructed with new DODAG version. The detection process is performed when there is inconsistent changes in the rank in the network.

Conclusion

There is no specific technique proposed to identify rank attack concerned with the selection of specific objective function. This research article focuses specifically on the hop count based DODAG construction rank issues. The article provides the novel technique to detect rank attack based on RSSI value while setting Hop count as an objective function. The proposed technique has been mathematically proved. In future, the proposed work could be implemented in Cooja simulator.

References

[1] Mohammed Amine Boudouaia, Adda Ali-Pacha, Abdelhafid Abouaissa, and Pascal Lorenz, "Security Against Rank Attack in RPL Protocol", IEEE Network, Volume 34, Issue 4, pp. 133-139, 2020.

[2] Zahrah A. Almusaylim, Abdulaziz Alhumam and N.Z. Jhanjhi,. "Proposing a Secure RPL based Internet of Things Routing Protocol: A Review", Ad Hoc Networks, volume 101, Article 102093, pp. 1-7, 2020.

[3] Jhanjhi, N. Z., Sarfraz Nawaz Brohi, and Nazir A. Malik, "Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning", DOI: 10.1109/MACS48846.2019.9024821, pp. 1-9, 2019.

[4] Suvankar Barai, Debajyoti Biswas and Buddhadeb Sau, "Estimate distance measurement using NodeMCU ESP8266 based on RSSI technique", IEEE, DOI: 10.1109/CAMA.2017.8273392, pp. 170-173, 2017.

[5] Mirko Ivanic and Ivan Mezei, "Distance estimation based on RSSI improvements of orientation aware nodes", IEEE, DOI: 10.1109/ZINC.2018.8448660, pp. 140-143, 2018.

[6] Mohammad Nikravan1, Ali Movaghar and Mehdi Hosseinzadeh, "A lightweight defense approach to mitigate version number and rank attacks in low-power and lossy networks", Wireless Personal Communications, Issue 99, Volume, pp. 1035-1059, 2018.

[7] Ahmed Raoof, Ashraf Matrawy, and Chung-Horng Lung, "Routing attacks and mitigation methods for RPL-based Internet of Things", IEEE, Volume 21, Issue 2, pp. 1582-1606, 2018.

[8] Rashmi Sahay, G. Geethakumari and Koushik Modugu, "Attack graph—Based vulnerability assessment of rank property in RPL-6LOWPAN in IoT", IEEE, DOI: 10.1109/WF-IoT.2018.8355171, pp. 308-313, 2018.

[9] Felisberto Semedo, Naghmeh Moradpoor and Majid Rafiq, "Vulnerability assessment of objective function of RPL protocol for Internet of Things", https://doi.org/10.1145/3264437.3264438, pp. 1-6. 2018.

[10] Usman Shafique, Abid Khan, Abdur Rehman, Faisal Bashir and Masoom Alam "Detection of rank attack in routing protocol for Low Power and Lossy Networks", Annals of Telecommunications, Volume 73, Issue 7-8, pp. 429-438, 2018.

[11] C. C. Sobin, "A Survey on Architecture, Protocols and Challenges in IoT", https://doi.org/10.1007/s11277-020-07108-5, pp 1-47, 2020.

[12] Zahrah A. Almusaylim, Abdulaziz Alhumam, N.Z.Jhanjhi, "Proposing a Secure RPL based Internet of Things Routing Protocol: A Review", Ad Hoc Networks, https://doi.org/10.1016/j.adhoc.2020.102096, Volume 101, pp 1-17, 2020.

[13] Boualam S.R., Ezzouhairi A, "New Objective Function for RPL Protocol", Embedded Systems and Artificial Intelligence, Springer, vol 1076, https://doi.org/10.1007/978-981-15-0947-6_64, pp. 681-690, 2020.

[14] Jungang Zheng , Chengdong Wu, Hao Chu and Yang Xu, "An improved RSSI measurement in wireless sensor networks", Procedia engineering, pp. 876-880, 2011.