Securing RPL Routing Path for IoT against rank attack via utilizing layering technique

Ahmed R. Zarzoor

Directorate of Inspection, Ministry of Health, Baghdad, Iraq
Ahmed.Arjabi@gmail.com

Abstract: RPL is common protocol for the Internet of Things (IoT) network, that used for routing data freely among smart "things" in various environments. Which makes them susceptible to attack, especially of the rank attack (RA) that is common for RPL that based on manipulated the rank value for each node in the network to disrupt the routing path. Also, RA is increasing latency between (source node and destination node) and maximizing nodes' energy usage in the whole network. Therefore, in this study a new technique is proposed to protect RPL against rank attack based on layering mechanism. The proposed technique consists of three steps: Classifying node into layers, calculating path trust value and identifying and alleviating rank attack. The method is implemented via using Cooja simulator software. The network performance is measured according to three metrics: latency, nodes' energy consuming and accuracy of malicious node detection. The simulation results have revealed that the proposed method gives higher accuracy of malicious node detection, low nodes' energy usage, and less latency in comparison with Sec-Trust study.

Keywords: Internet of Things (IoTs), Sink Node (SN), Routing Protocol for Low Power and Lossy Network (RPL), Rank Attack (RA).

1. Introduction

The prevalence of using IoTs networks in many applications of life, such as smart city [1], healthcare [2], agriculture [3], etc. which makes them influence human daily life. Where, in 2031 it can be anticipated that the number of "things" will increase over 51 billion devices [4]. The IoT network consists of mutual smart things (devices or sensors) that are deployed in different areas. Where, they interconnected with each other according to the term of "Device to Device" communication without human intervention. Besides, smart things have limited resources (memory, battery power, calculation) [5]. Also, the smart things are worked in different environment conditions, which makes them an invaluable target for the attackers. The most common attack is by placing malicious node on the route between the source and destination node. So as to disrupt the data collection process, exhausted devices' residual energy and increased latency i.e., attackers target the routing protocol.

RPL has been widely used in IoT network as a routing protocol [6-8]. In this routing protocol, nodes are formed in a tree structure based on the node rank value (distance between the current node and root node). So, the node that has lowest rank value is the one that near to the root (sink) node. Therefore, the most popular attack on that RPL routing protocol is the rank attack [9-11]. In this attack, the malignant node with lowest rank value is used as a parent or root node in the network. In order to cause a several kinds of attacks suck as a sink hole attack, selective forward attack and black hole attack. Also, the rank attack can create many routing routes to the sink node (SN) that affects the entire IoT network performance via increasing dropped data packets, disturbance of the traffic, maximizing latency and increasing nodes' remaining energy consume [12-13].

Therefore, a new method in this study, is proposed to detect rank attack and alleviated its impact on the network performance. The proposed method is based on layering techniques, in which the network is divided into layers (from 0 to n) see Figure 1. Where, in layer 0 the Sink Node SN is placed and its' rank value is equal to zero. While, in layer 1 each node in that layer has the rank (value= 1) and so on. The layering technique is utilized in our previous work [14].

Received: September 9th, 2020. Accepted: December 24th, 2021
DOI: 10.15676/ijeei.2021.13.4.2

But, to select the best route path between the child node and SN based on the total trust value of the path. Thus, the best path is not the one that gives high quality only, but is the one that has high trust value in comparison with other paths. While, in this study the malicious node is identified according to the rank value. For example, the node that has rank value=1 and allocated in layer 4 is considered as malicious node. The rest of this paper is presented as follows: section 2 explores the related works; section 3 presents the study method. While, section 4 discusses the method implementation results. Finally, section 5 includes study's conclusion

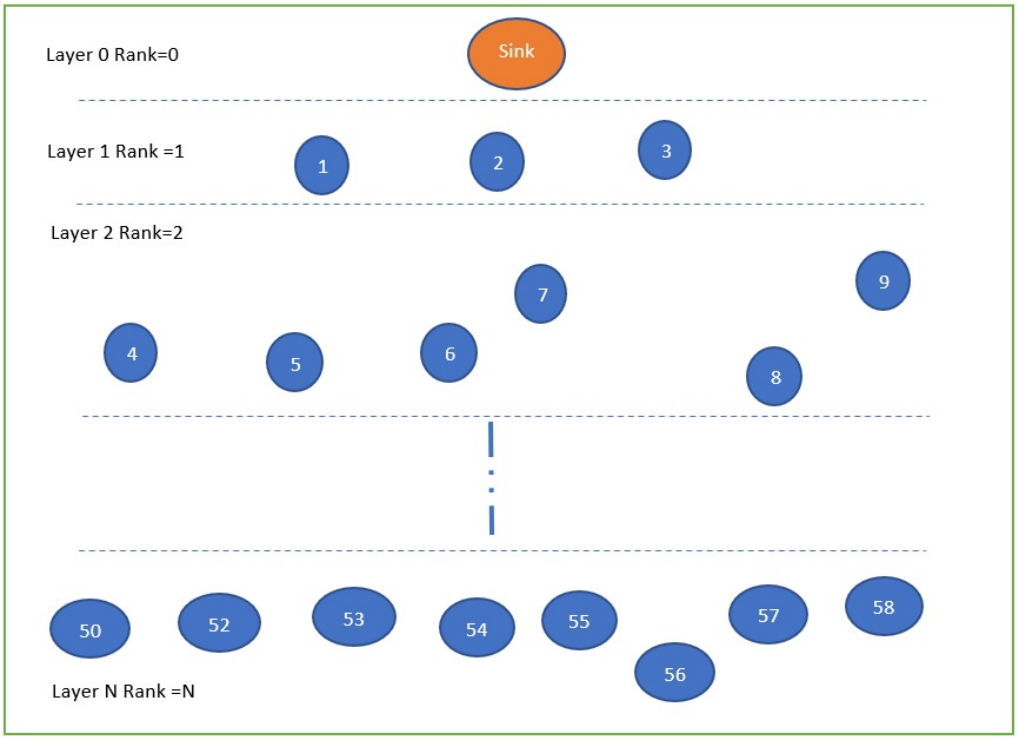

Figure 1. Layering Technique for RPL routing protocol

2. Related Work

Various studies revolving about IoT security have endeavored to specify and relieving the malicious node effects on the routing protocol for RPL protocol. In [15] study, the authors are proposed (Multiparty-RPL) method, in which they used clustering technique to split "destination oriented directed acyclic graph" (DODAG) into groups. Besides, the used device to create a backup of all the paths that creating during clustering process. Where, each DODAG has an ID number, and each node in cluster must has the same DODAG ID, otherwise it belongs to other clusters. Thus, according to that technique the malicious node can detect and be avoided via using an alternative path that store on the device. Kallapur et al [16], presents a technique for computing trust forwards, in order to specify attack based on the change trust forwards between (source and destination node) according to any change on the DODAG.

While, in [17] the researchers proposed "Secure RPL" (SRPL) protocol to protect against misconduct modifying control message (rank value) based on rank threshold and "hash chain authentication" method. The rank threshold is used to identify malignant node that is propagated fake rank value. Whereas, "hash chain authentication" is used to prevent manipulate of node rank value in the DODAG. Djedjig et al study [18], are suggested a new scheme to enhance the security of RPL called "Metric-based RPL Trustworthiness Scheme" (MRTS). In the scheme, they expanded DIO "DODAG information Object "message via adding new two trust metrics: "Extended RPL Node Trustworthiness" ERNT, which is the nodes' trust value and TOF "Trust

Objective Function", that is the cost of the routing path according to the ERNT value". The ERNT value is calculated according to three node metrics (energy usage, honesty and selfishness). In [19] study, researchers proposed a new trust calculation model for running services of IoTs. The calculation is depended on five categories: trust structure (Social trust and Quality of Services trust), trust diffusion (centralized and disseminated), trust formation (multi-trust and single trust), trust aggregation (Fuzzy logic, Belief Theory, Weighted sum, Bayesian systems and Regression Analysis) and update trust (Time-Driven and Event-Driven). Moreover, to test trust calculation model they suggested threat model consisted of five attacks: On-off, Self-promotion, Bad-mouthing, Ballot-stuffing and Opportunistic service. In order, to test trust calculation model.

In [20] study authors suggested E2V tool to detect and relieve "Rank Inconsistency Attack" (RInA), where the tool based on three levels: rank computation, substantiation and malignant node removal. The core idea is about checking each node rank value according to its current energy by the root node. So, if the current energy is greater than or equal to the node initial energy then marks this node as a malicious node. Whilst, Airehrour et al [21], utilized a new system called "SecTrust-RPL" to protect against rank attack and sybil attack. In the SecTrust-RPL, each node calculates trustworthiness of its neighbors by computing two metrics: recommend trust and direct trust. Thus, if the value of direct trust for one neighbor is low, then marks this node as malicious node. Whereas, recommend trust is used when the node not has direct communication with current node in the path between the source and destination node.

While, in [22] study, researchers utilized opining triangle to calculate trust between each node and its neighbors. Also, they used "control node" to make rating for each node trust value and compare it threshold value, in order to specify malignant node. In the [23] study authors utilized ranking and rating technique to detect sink hole attack in RPL protocol. They calculated node ranking and rating based on the distance computation. Also, they detect the misbehave node in IoT network, according to the "Average Packet Transmission" APT-RREQ value. YAVUZ et al [24], are used method based on deep learning to detect three types of attacks: rank, hello flood and version number. They specify the node abnormal behaviour by calculating four features: Received Rating (RR), Received Average Time (RAT), Reception Packets Counts (RCP) and Total Received Time (TRT)

3. Study Method

The main purpose of this study, is to present a new security technique for our previous work [14]. In which, the best routing path between child node and sink or root node is selected based via using "Enhance-Minimum Rank with Hysteresis Objective Function" (E-MHOF). Where, the ideal path is the one that consumes less energy of nodes remaining energy and gives the minimum latency in comparison with other routes in DODAG. However, in the new proposed security technique the optimal route is the one that gives high trust value in comparison with other routes. To achieve that, three steps are used

1. Classifying node into layers.
2. Calculating path trust value.
3. Identifying and alleviating rank attack.

A. Classifying node into layers

In this step, each node in DODAG will be allocated in one layer according to the distance between it and the Sink Node (SN). Whereas, this is done by dividing the network area into equal sub areas called layers, see figure 2. Where, each node is allocated to one layer only via utilizing coordinate points (i.e., reference nodes). Also, in each sub area, every node sends its position information to four reference nodes to form the layer of each sub area. For example, in figure 2, the reference nodes are A, B, C and D of the sub area send their known location information in a message to all nodes (1,2 and 3) that in their coverage range. In turn nodes (1, 2 and 3) send their' location information for the A, B, C and D based on the received strength RSSI signal. In the next step, each reference node sends nodes' position and node ID to the SN. In the SN each

node is assigned a rank value in one layer. For instance, nodes 1,2 and 3 are allocated in layer 1 and assigned to rank value 1, see Figure 2. Finally, the routing table is in the SN consists of the node ID, Rank, Layer, node remaining energy, node initial energy and check validity, which will be described in the next section. See Table 1. Moreover, the routing information such as rank is added to the DIO, "DODAG Adverting Object" message that sent by the SN. Where as, the DIO message will be sent periodically from root node to all nodes in the network, until each node receives DIO message in the network and gets rank value.

Table 1. Routing Table

Node ID	Rank	Layer	Remaining Energy joules	Initial Energy joules	Check
1	1	1	200	202	Valid
2	1	1	204	205	Valid
3	1	1	206	206	Valid
4	1	2	200	204	Invalid
5	2	2	203	205	Valid
6	2	2	204	207	Valid
7	2	2	210	213	Valid
8	2	2	213	215	Valid
9	2	2	212	217	Valid

B. Calculating path trust value

The routing paths between child node CN and sink node SN is formed according to our previous work "E-MHOF" [14]. Whereas, a parent is selected according to compute of three parameters (ETX, RSSI and nodes' residual energy). Moreover, in this step of proposed study method, the rank value (RV) utilized as fourth parameter in this study. So, the RV that added to the DIO message is checked by each node to detect the malignant node. Thus, the optimal routing path between the CN and SN, is the one that has lowest average value of the nodes' ETX value, the highest average value of nodes' remaining energy and validity check of the RN value. Furthermore, all the paths are created between the CN and SN. In this phase, a one parameter is used to calculate overall trust value of each path that called direct trust (DIR_TR). The value of DIR_TR is calculated by using equation 1 and 2 [21]. The DIR_TR value between 0 and 1, where 1 mean full trust and 0 mean not trust

$$\alpha_i = \alpha_i + 0.005 \tag{1}$$

$$\text{DIR\_TR}(N_i, N_j) = \frac{PF_{ji}(t)}{PF_{ji} + \alpha[PF_{ij}(t) - PF_{ji}(t)]} \tag{2}$$

Where, $PF_{ji}(t)$ is the summation of all forward data packets from node i (N_i) to node j (N_j) during (t) time. While, α is constant value (default value=0.01) that same value used in study [21]. The α value represents 1% of optimal trust of 1.0. While, the punishment increment set half value 0.005. To illustrate, if DIR_TR(N_i, N_j) value is less than threshold value then makes α value increased by (0.01 +0.005=0.015). Thus, the best route is the route that has maximum of total (DIR_TR value) for entire route. For example, in figure 2 there is two routing paths from CH (10) to the sink node: the total direct trust value of the first routing path 10->4->1->sink is (0.1+0.12+0.5=0.72). Whiles, total direct trust value for the second path 10->5->1->sink is (0.22+0.22+0.5=0.94), which makes the second path the optimal path for routing packets between node 10 and SN.

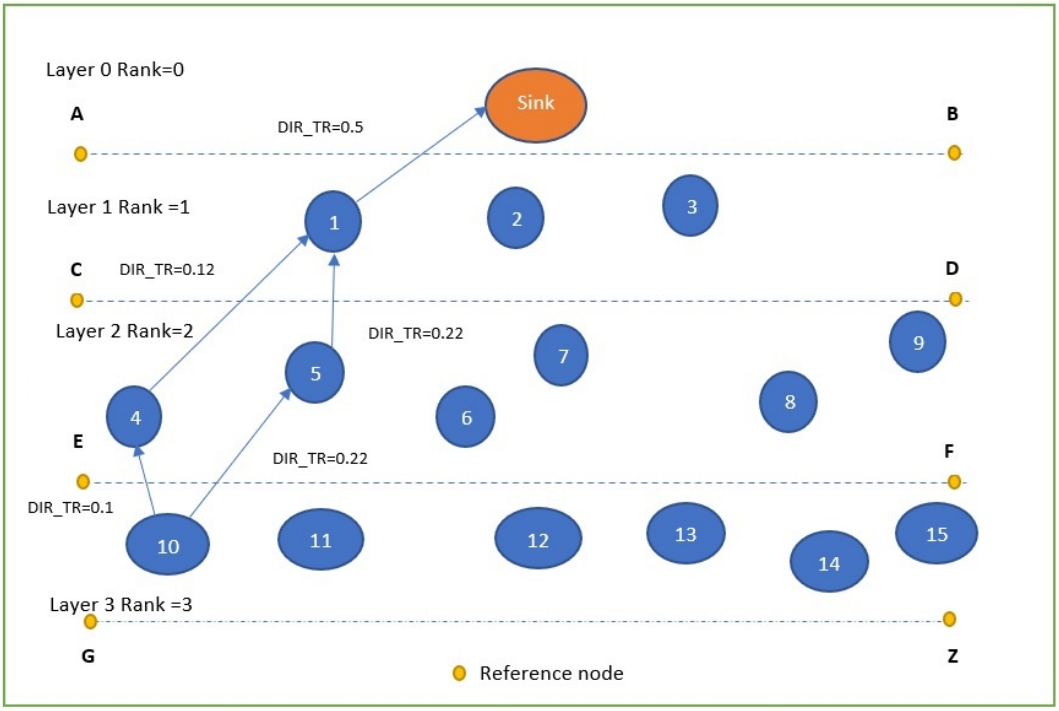

Figure 2. Illustrates the direct trust (DIR_TR) value for two paths between CN (10) and SN

C. Identifying and alleviating rank attack

In this section, rank attack is detected by utilizing the RV assigned value for each layer from the routing table. For instance, when the attacker manipulates the rank values, see Table 1. where node 4 in layer 2 (gives rank 1). In the sink node according to the routing table information, the node 4 RV must equal to 2, see Table 1. Which, makes the node 4 a malicious node and adds it to the black list. In the next step, node 4 ID is advertised with a message to all nodes in the network to ignore any message from the node 4. Thus, in the routing path between the CN and SN each node checks its RV before forward packet to the parent by using Equation 3.

$$|Rank\ (child) - Rank(Parent)| \quad (3)$$

To demonstrate, in Table 1 the RV of node 4 in layer 1 (RV=1) and CH (10) rank value is 3. Thus, (|3-1|=2) and node 4 is specified as a malignant node. Subsequently, to isolate node 4, an alternative path is elected using the previous study method [14] in which the ideal path is the one that has the minimum (average of ETX value) and maximum (average of remaining energy (RE) value) for every node in the electoral route. Also, the best path is the one that has the maximum total (DIR_TR) value. In another word, in this step, alleviating rank attack process is achieved via isolation any path that contained malicious node in the routing path between the CH and SN.

4. Results

The Cooja simulator software is used to implement the proposed method. So, four scenarios with different malignant nodes rate have been created, in order to conduct a comparison between the proposed method and SecTrust[21] method. In each scenario, the network consists of 200 nodes and one SN, see Table 2. Whilst, the network performance is measured according to the accuracy of malicious node detection (MND), energy usage and latency. For accuracy of MND, four metrics are used: False Native Rate (FNR), True Negative Rate (TNR), False Positive True (FPT) and True Positive Rate (TPR). The four metrics are calculated using equation 4,5,6 and 7 [25-26].

Table 2. Simulator Parameters

Parameter	Value
Operating System (OS)	Contiki OS Version 3.0
Area in Meters (m)	300 X 300
Total number of nodes	200
Malicious nodes rate	15% for Scenario 1 30% for Scenario 2 45% for Scenario 3 50% for Scenario 4
Transmission Packet Ratio (TX)	100%
Received Packet Ratio (RX)	100%
TX and RX Range	100m
Interference Range	
Network protocol	Contiki RPL
Start Delay	5 seconds
Simulation Time	60 minutes
Link failure model	UDGM with distance

$$FPR = \left(\frac{FPR}{FPR+TNR}\right) \times 100 \quad (4)$$

$$TNR = \left(\frac{TNR}{TNR+FPR}\right) \times 100 \quad (5)$$

$$FNR = \left(\frac{TPR+TNR}{FPR+TNR+TPR+FNR}\right) \times 100 \quad (6)$$

$$TPR = \left(\frac{TPR}{TPR+FNR}\right) \times 100 \quad (7)$$

Where, TPR represents the ratio for the entire number of pedantic malicious nodes divided by the entire number of malicious nodes. FPR represents that ratio of the summation of nodes that are incorrectly defined as a malicious nodes divided by the entire number ordinary node. TNR is the ratio of the nodes being correctly marked as malicious node. FNR is the ratio for the rate of a malicious node to the entire ordinary node being wrongly pedantic as normal node. Figure 3, 4, 5 and 6 which demonstrate the calculated values for TNR, FPR, NPR and TPR.

However, the results of the four scenarios implementation have shown: the accuracy of malignant node detection, increased in the proposed method in comparison to the SecTrust see Figure 7. For power usage, the proposed method consumed less power than the SecTrust. Due to in the SecTrust method, each node must compute the direct trust and recommend trust. Whilst, in the propose method only the trust value is calculated by each node. Besides, the malignant node detection is controlled by sink node, see Figure 8. Therefore, the study method consumes less energy in contrast to the SecTrust method. While, for latency, the proposed method gives less delay in comparison with the SecTrust method because of, utilizing a layering technique that, minimized time of check RV. While, in SecTrust, the time is increased because of dual calculation for the (direct trust and recommend trust). Also, the checking of node behavior is managed by SN based on routing table, see Figure 9.

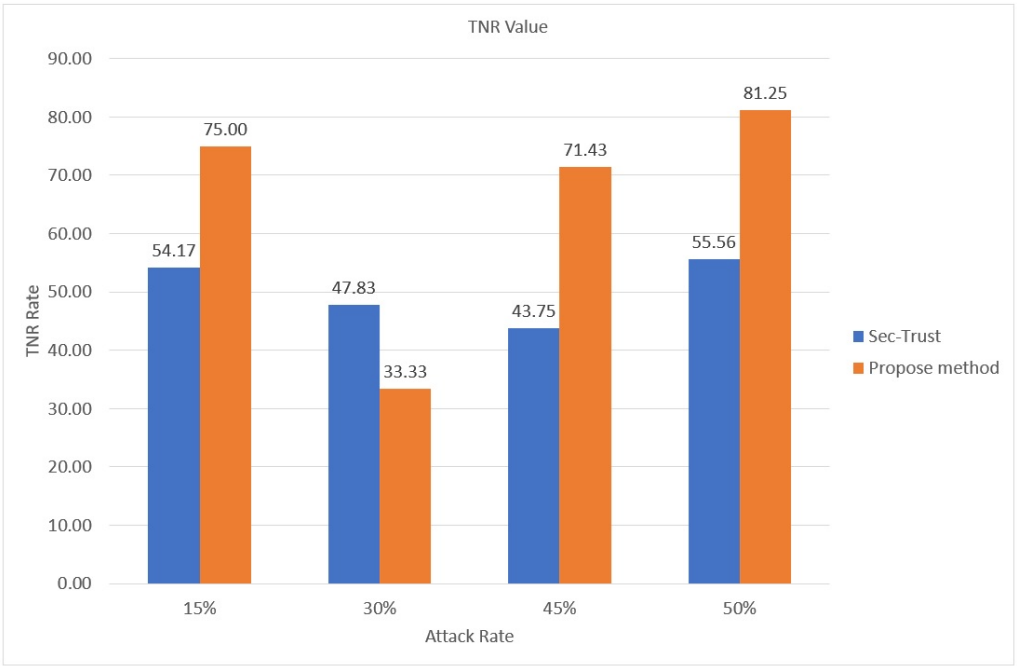

Figure 3. TNR Value for Sec-Trust and proposed method

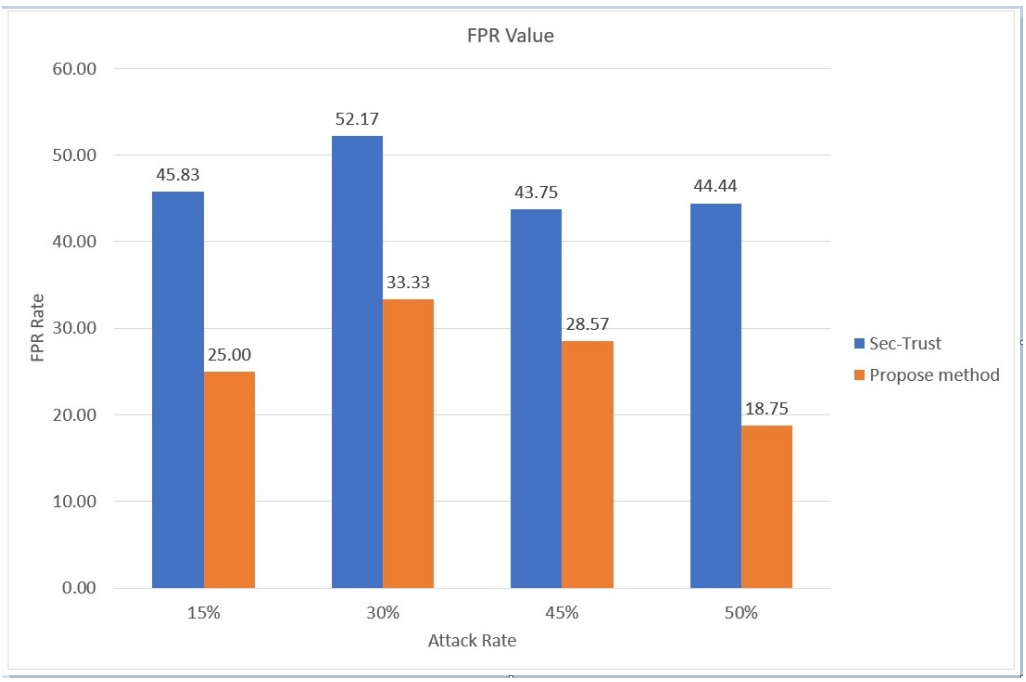

Figure 4. TNR Value for Sec-Trust and proposed method

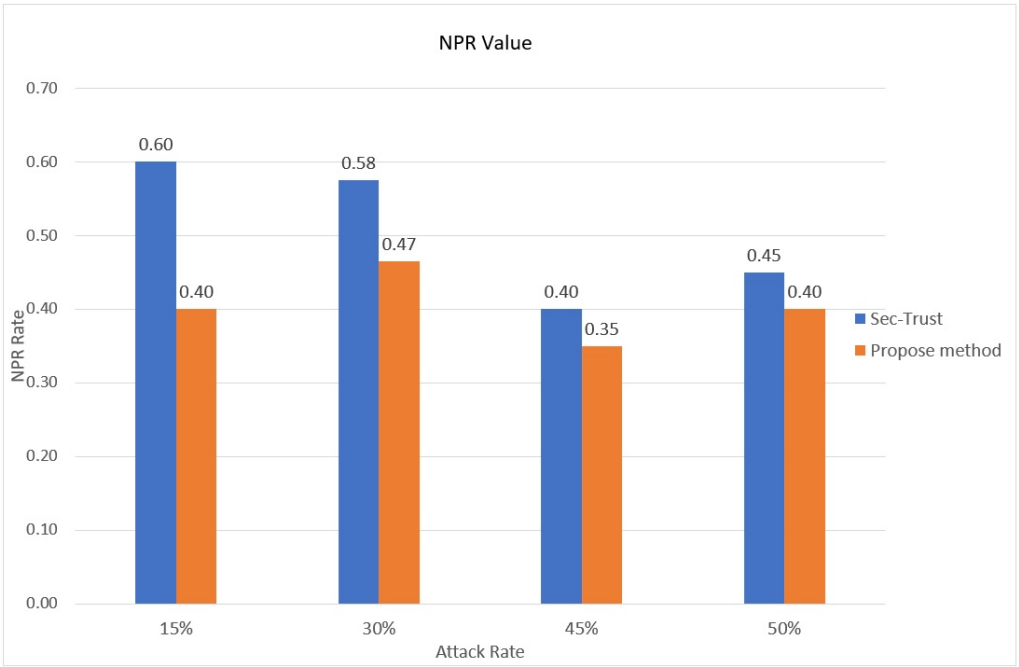

Figure 5. NPR Value for Sec-Trust and proposed method

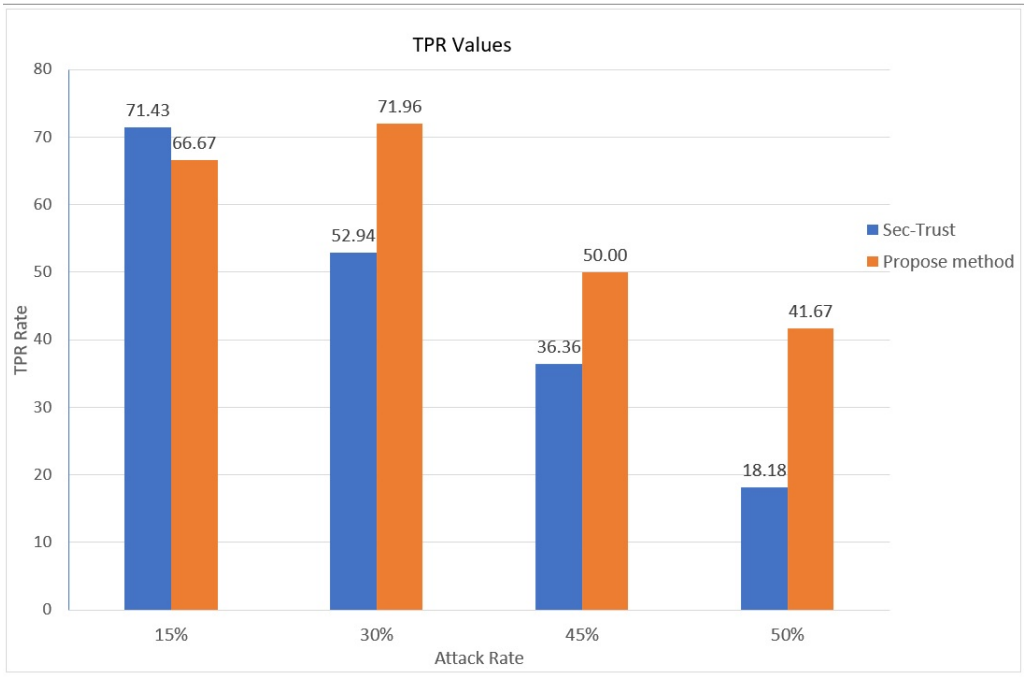

Figure 6. TPR Value for Sec-Trust and proposed method

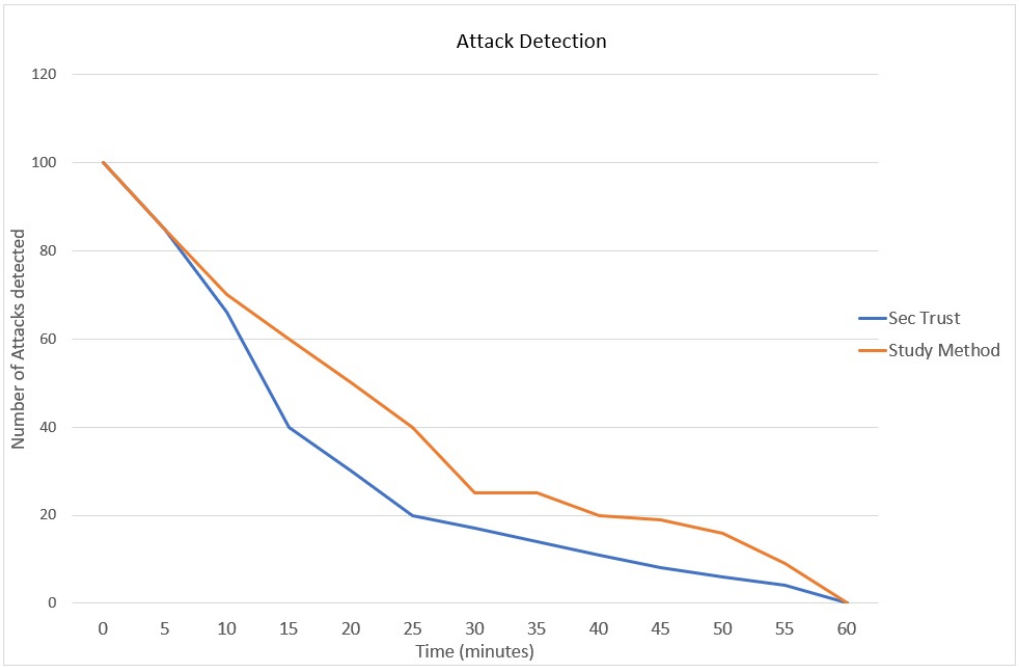

Figure 7. Accuracy of malicious node detection for Sec-Trust and proposed method

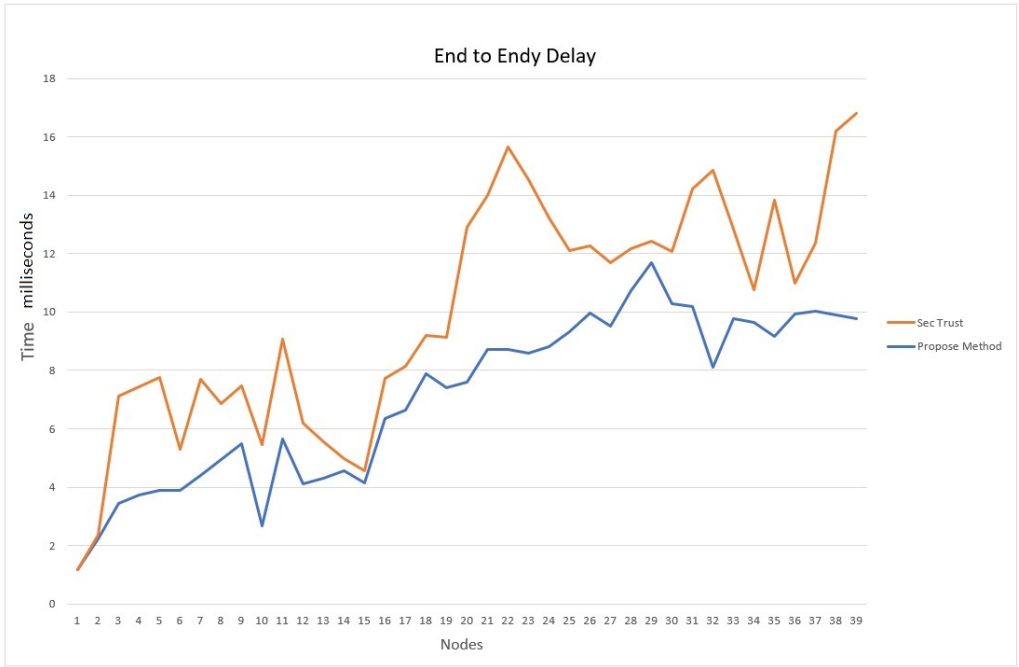

Figure 8. Illustrates, End to End delay for Sec-Trust and proposed method

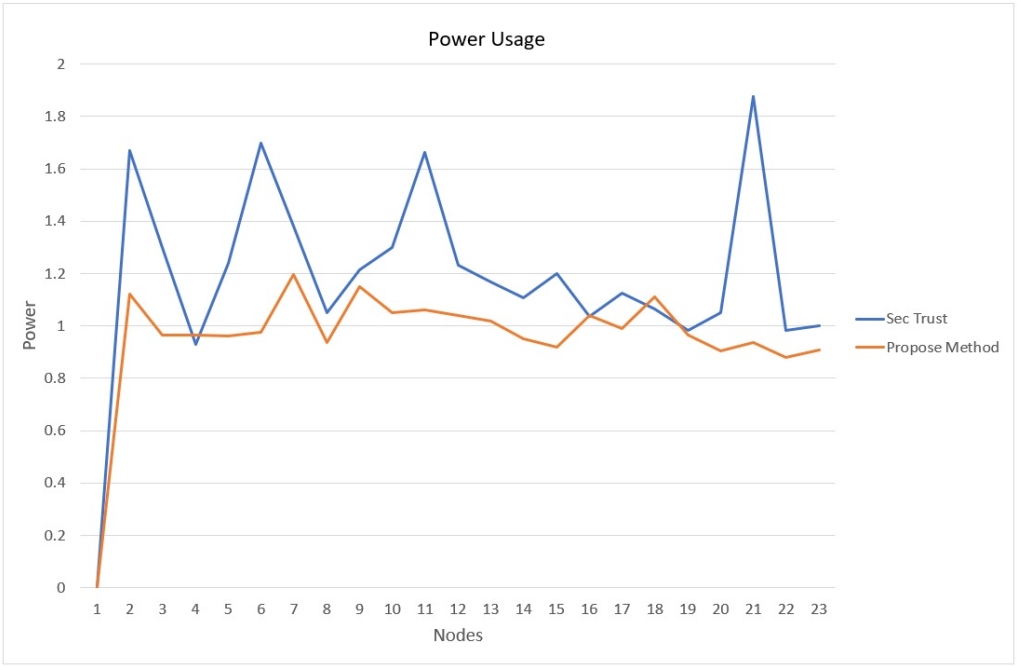

Figure 9. Illustrates, power usage for Sec-Trust and proposed method

5. Conclusion

This study has been used to enhance the security of RPL against ranking attack based on layering technique. The study method consisted of three steps: Classifying node into layers, calculating path trust value and identifying and alleviating rank attack. In the first step, the entire network area is divided into sub-areas via using reference nodes. Also, the RV is assigned to each node based on the layer number. In the next step, the direct trust value is calculated for each node with its direct neighbor. Finally, the RV is used to identify the malicious node and isolated it by selecting an alternative route that has the maximum direct trust value of all the nodes that formed it.

The method has been implemented via using Cooja simulator software. Also, the network performance of the network has been evaluated according to three metrics: latency, power usage and accuracy of malicious node detection. The simulation results have been shown that the Sec-Trust method consumed more energy and given less accuracy of malicious node detection in comparison with the proposed method. Also, latency is higher in the Sec-Trust method, in contrast with the proposed method.

6. Acknowledgment

I would like to appreciate all the excellent suggestions of anonymous reviewers to enhance the quality of this paper.

7. References

[1]. M. A. Naeem, R. Ali, B.-S. Kim, S. A. Nor, S. Hassan, "A periodic caching strategy solution for the smart city in information-centric Internet of Things", Sustainability, vol. 10, no. 7, pp. 2576, 2018.

[2]. A. Albesher, “IoT in Health-care: Recent Advances in the Development of Smart Cyber-Physical Ubiquitous Environments”, *IJCSNS International Journal of Computer Science and Network Security*, VOL.19 No.2, pp 181- 186, 2019.

[3]. M. S. Farooq, S. Riaz, A. Abid, K. Abid and M. A. Naeem, "A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming," in *IEEE Access*, vol. 7, pp. 156237-156271, 2019.

[4]. Zarei, M. Securing Internet of Things against Physical Layer Attacks Using Hybrid Security Algorithm (HSA). *Preprints, pp 1-22,* 2020,

[5]. A. Musaddiq, Y. B. Zikria, O. Hahm, H. Yu, A. K. Bashir, and S. W. Kim, "A survey on resource management in IoT operating systems," *IEEE Access*, vol. 6, pp. 8459–8482, 2018.

[6]. S. Taghizadeh, H. Bobarshad and H. Elbiaze, "CLRPL: Context-Aware and Load Balancing RPL for Iot Networks Under Heavy and Highly Dynamic Load," in IEEE Access, vol. 6, pp. 23277-23291, 2018

[7]. Lim, Chansook. "A Survey on Congestion Control for RPL-Based Wireless Sensor Networks." Sensors (Basel, Switzerland) vol. 19, No. 11, 2019

[8]. J. Eriksson, N. Finne, N. Tsiftes, S. Duquennoy and T. Voigt, "Scaling RPL to Dense and Large Networks with Constrained Memory", EWSN '18: Proceedings of the 2018 *International Conference on Embedded Wireless Systems and Networks*, pp 126–134, 2018

[9]. S. Shukla, S. Singh, A. Kumar and R. Matam, "Defending Against Increased Rank Attack on RPL in Low-Power Wireless Networks," *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, Solan Himachal Pradesh, pp. 246-251, 2018

[10]. R Stephen and L Arockiam, "E2V: Techniques for Detecting and Mitigating Rank Inconsistency Attack (RInA) in RPL based Internet of Things", *IOP Conf. Series: Journal of Physics: Conf. Series*, pp. 1-12, 2018.

[11]. Shafique, U., Khan, A., Rehman, A. et al. Detection of rank attack in routing protocol for Low Power and Lossy Networks. Ann. Telecommun. Vol 73, pp. 429–438, 2018.

[12]. K. K. Rai and K. Asawa, "Impact analysis of rank attack with spoofed IP on routing in 6LoWPAN network," *2017 Tenth International Conference on Contemporary Computing (IC3)*, Noida, pp. 1-5, 2017.

[13]. R. Sahay, G. Geethakumari, and K. Modugu, "Attack graph — Based vulnerability assessment of rank property in RPL-6LOWPAN in IoT," presented at the 2018 IEEE 4th *World Forum on Internet of Things (WF-IoT)*, Singapore, 2018.

[14]. Ahmed R. Zarzoor, "Optimizing RPL Performance Based on The Selection of Best Route Between Child And Root Node using E-MHOF method", *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 11, No. 1, pp. 25- 32, 2020

[15]. G. Ma, X. Li, Q. Pei and Z. Li, "A Security Routing Protocol for Internet of Things Based on RPL," 2017 *International Conference on Networking and Network Applications (NaNA)*, Kathmandu, pp. 209-213, 2017

[16]. P. V. Kallapur, N. Ranjan, R. Vidyarthi, Anshuman and V. Singh, "Enhanced variant of RPL for improved security," 2017 *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Udupi, pp. 2302-2306, 2017

[17]. G. Glissa, A. Rachedi and A. Meddeb, "A Secure Routing Protocol Based on RPL for Internet of Things," *2016 IEEE Global Communications Conference (GLOBECOM)*, Washington, DC, pp. 1-7, 2016

[18]. N. Djedjig, D. Tandjaoui, F. Medjek and I. Romdhani, "New trust metric for the RPL routing protocol," *2017 8th International Conference on Information and Communication Systems (ICICS)*, Irbid, pp. 328-335, 2017.

[19]. J. Guo, R. Chen, and J. J. Tsai, "A survey of trust computation models for service management in the internet of things systems," Computer Communications, vol. 97, pp. 1–14, 2017.

[20]. R Stephen and L Arockiam, "E2V: Techniques for Detecting and Mitigating Rank Inconsistency Attack (RInA) in RPL based Internet of Things", Journal of Physics: Conference Series, vol. 1142, pp 1-13, 2018.

[21]. D. Airehrour, J. A. Gutierrez, and S. K. Ray, "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things," Future Generation Computer Systems, vol. 93, pp. 860-876, 2019.

[22]. Z. Khan, J. Ullrich, A. Voyiatzis, P. Herrmann, "Trust-Based Resilient Routing Mechanism for The Internet of Things". In Proceedings of the 12th International Conference on Availability, Reliability and Security—ARES '17, No.27, pp 1-6, 2017.

[23]. M. Zaminkar, R. Fotohi, "SoS-RPL: Securing Internet of Things Against Sinkhole Attack Using RPL Protocol-Based Node Rating and Ranking Mechanism". Wireless Pers Commun, pp. 1-26, 2020.

[24]. F. YAVUZ, D. ÜNAL and E. GÜL, "Deep Learning for Detection of Routing Attacks in the Internet of Things", *International Journal of Computational Intelligence Systems*, Vol. 12, pp. 39-58, 2018.

[25]. K. Mabodi, M. Yusefi, M and S. Zandiyan, L. Irankhah and R. Fotohi , "Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication", *The Journal of Supercomputing* pp 1-25, 2020.

[26]. M. Zaminkar and R. Fotohi, "SoS-RPL: Securing Internet of Things Against Sinkhole Attack Using RPL Protocol-Based Node Rating and Ranking Mechanism". Wireless Pers Commun, pp. 1-26, 2020.

Ahmed R. Zarzoor received his MSc. degree in software engineering from University of Bradford, UK, Bradford in 2006, and received a PhD degree in computer since from Post-graduation Studies Iraqi Commission for Computer & informatics, Baghdad – Iraq. He is currently a Director of Information Technology at the Ministry of Health, Baghdad, Iraq. His main interest includes WSN, IoTs, MANET, Computer Networks & Security, Soft Computing and Machine Learning