A Secure Model to Protect Healthcare IoT System from Version Number and Rank Attack

*Smita Sanjay Ambarkar[1] and Narendra Shekokar[2]

[1]*Department of Computer Engineering, D. J. Sanghvi College of Engineering, University of Mumbai, India*
ambarkarsmita793@gmail.com
[2]Department of Computer Engineering, D. J. Sanghvi College of Engineering, University of Mumbai, India
narendra.shekokar@djsce.ac.in

ABSTRACT

Recently the entire world is witnessing a pandemic outbreak of COVID-19. Resultantly, the healthcare sector battles the challenges like inadequacy of staff members,feeble patient monitoring services, etc. IoT technology provides complete digitization. However, this healthcare IoT falls prey to various attacks and security threats. The main cause of the attacks is the IoT communication and routing protocols.
Routing protocol for low power lossy network (RPL) provides the potent routing mechanism in the 6LoWPAN network. However, RPL is an unsecured protocol; hence providing security to IPV6-RPL connected devices is a challenging task. This paper modelled the rules for RPL protocol signatures like ETX, beacon interval, and energy consumption in a novel attack detection system. The simulation results proved that the proposed system detects the conventional as well as RPL specific attacks precisely version number and rank attacks in healthcare IoT systems with higher accuracy and detection rate.

KEYWORDS

Healthcare IoT, version number attack, rank attack, RPL,6LoWPAN, security.

1. INTRODUCTION

The Internet of things (IoT) provides digitization facilities to many applications like healthcare, home, vehicles, agriculture, etc. [1]. This paper intends to secure a healthcare IoT-based system from RPL attacks in the 6LoWPAN network. Healthcare is one of the paramount services for any country. The ongoing COVID-19 pandemic makes life difficult without proper healthcare services. The incompetent health care service will cause huge devastation of health and wealth in many countries.

IoT helps to revolutionize the healthcare sector by complete digitization techniques. Digitization helps to reduce the burden of healthcare staff and increases the efficacy of healthcare services. IoT networks are supported by many communications protocols, which include 6LoWPAN, LORA, Zigbee, BLE, etc. Among all these communication protocols, the paper uses IPv6-based low-power personal area network (6LoWPAN) communication protocol for implementation because 6LoWPAN provides scalability and auto-configuration. The auto-configuration means the sensor nodes easily join and leaves the network, which makes the network flexible.

IPv6 protocol for low power lossy network (RPL) proposed by the Internet Engineering Taskforce (IETF) [2] RFC 6550 is used as a routing protocol for the 6LoWPAN network. In

RPL, the network layer is responsible for routing decisions hence every node must have a complete view of the current topology.

The RPL protocol built up the network by forming a destination-oriented directed acyclic graph (DODAG), where the parent node is selected on the basis of rank value. Every DODAG has a sink (root) node and a source node (leaf nodes). To identify nodes uniquely in the DODAG, RPL makes the use of trio [DODAG id, RPL instance, and Rank], where each node calculates the value of rank with the help of version number and objective function [3][4].

The rank value depicts the node position in the DODAG graph. In case of any topological inconsistency, the root node performs a global repair mechanism to repair DODAG. Each time this global repair mechanism increments the version number and transfers in the network, the nodes need to preserve this copy of the version number and move to a new DODAG with the different rank positioning. The nodes that are having older version numbers mean their routing table entries are obsolete. Hence, the version number and rank are important parameters for the formation and maintenance of the stable 6LoWPAN-RPL network.

DODAG formed after exchanging the various control messages between the root node and source node. During initialization, the root node sends the first control message as DIO (DODAG information object) which contains rank, version number, and other control information. After receiving the DIO, every source node of DODAG calculates the rank value and sends it as an acknowledgment to the root node in the form of a second control message DAO (DODAG acknowledgment object). DIS (DODAG information solicitation message) is a request message sent by the outsider node for connectingwith the existing DODAG. Moreover, the sensor nodes to verify the version number and other routing parameters will also periodically exchange the DIS message.

All the nodes connected using the initialization process in DODAG experience unsecured behaviour as the routing protocol RPL is an unsecured protocol [2]. Hence RPL network is prone to various attacks like version number modification attack, increased rank attack, decreased rank attacks, DAG inconsistency, flooding attack, etc[3][4]. Among these attacks, version number attack and rank attack agitate the normal routing and devastates the entire network by consuming the maximum energy. The version number attack and rank attack proved as a very dangerous attack as they will destroy the network slowly and they are difficult to detect [5]. Most of the existing research proposed the security methods like machine learning-based intrusion detection systems [6], multi-layered detection systems [7] where, three layers were used for intrusion detection, but these existing IoT security methods failed to consider the compatibility of IoT routing specifications. Hence, the existing attack detection mechanism incurred extra overhead on the low constrained devices. Therefore, this work proposes a novel rule-based detection model that considers routing specific information and energy consumption for activation and detection of attacks. The detection model proposed in this paper is based on the routing parameters such as ETX, beacon interval, and energy consumption of the RPL protocol. This paper is organized as follows; the next section II highlights the literature survey. Section III explains the threat model for the version number and rank attack. Section IV elaborates on the proposed system. Section V demonstrates the implementation details and discusses the results. Finally, the paper is concluded with a precise conclusion.

2. LITERATURE SURVEY

This section discusses the relevant research of intrusion detection techniques used to protect the low constraint IoT devices. The section first discusses the various healthcare IoT systems, which suffer from numerous RPL attacks. The literature survey further discusses the detailed contribution of different authors for the detection of version number attack and rank attack in various applications. IDS provide the defence wall for the protection of the network but implementing the lightweight IDS, which will be best suitable for IoT network, is a challenging task.

IoT used in the healthcare sector enhances the efficacy of the healthcare system. However, the digitization facility of the healthcare IoT system will be at risk if security is not taken care of properly [6]. The authors of [7] explain the importance of IoT in healthcare, attacks on healthcare devices, vulnerabilities in the healthcare IoT system, and security issues in detail. of Authors of [8] emphasize the information security of patient's data in the healthcare system (HIS). The authors of [9] implemented a healthcare system using IoT for tracking healthcare staff and patients within 3 to 5 feet of the coverage range. Paper demonstrated the DoS attack on healthcare IoT systems using Kali Linux and hydra tools. The authors implemented an external DoS attack by flooding ICMP messages. To prevent this attack, for future implementations authors suggested using digital certificates for securing the connection between an edge node and AWS database.

The version number is of vital importance while the formation of DODAG. Adversary changes this version number and disturbs the routing, which ultimately causes the stern control message traffic in the network. As per the comprehensive literature survey, very few researchers have addressed the version number attack. Authors [10] understand the problem of RPL protocol that the protocol is unable to provide protection for DODAG hence they had proposed VeRA the version number and rank authentication scheme, which uses the one-way hash, chain, however, authors failed to provide the details of the energy consumption or CPU consumption values. To prevent the DAG inconsistency caused by version number attack, the authors [11] put forth the rank authentication mechanism. They proposed the Trust Anchor Interconnection Loop (TRAIL), where the root node acted as an anchor node and the root node must validate the rank value. However, this TRAIL mechanism causes extra overhead in the network, which will ultimately increase energy consumption. An author of [12] put forth the distributed monitoring mechanism to detect the malicious nodes, which will illicitly increment, or updates the version number. Authors of [13] proposed the mitigation technique for decreased rank attack and version number attack using an identity-based signature mechanism. In another technique of version number attack mitigation, the authors [14] implements the trust-based mechanism for mitigation of version number attack in which if most nodes are closed to root node and having the better rank then the version number will be changed. Authors [15] illustrate the impact of rank property in the formation of the RPL network. The rank values increase from root to child node hence the root bears the lowest rank value, authors [15] also put forth that the child node contains no mechanism to verify the services provided by the parent node, and hence advisory node changes the rank value and RPL fall prey to increased rank attack.

The above literature implemented the mechanism for version number and rank attack detection either without specifying the energy consumption parameter or with high-energy consumption systems. Therefore, this paper proposes a rule-basedintrusion detection system, which takes care of low energy consumption and hence is adept for low constraint devices. The following section illustrates the threat model for version number and rank attack.

3. THREAT MODEL FOR VERSION NUMBER AND RANK ATTACK IN HEALTHCARE IOT

To implement the robust mechanism against the RPL attack it is necessary to understand the related threat model [18]. Hence, this section illustrates in detail the threat model for healthcare IoT systems.

The nodes in RPL-6LoWPAN networks form DODAG using distance vector routing. Every DODAG has a sink (root) node and a source node. DODAG id, RPL instance, and Rank are used to identify every node uniquely.

The threat model for hospital IoT has shown in figure 1 consists of root (Sink) node and sensor nodes (S1, S2, S3, S4) attached to the patient's body. To understand figure 1 practically, this paper considers sensor S1 as a temperature sensor (DS18B20) that reads the body temperature of a patient. The normal temperature range is 36.5–37.5 °C (97.7–99.5 °F). Sensor S2 is

ECG(AD8232) is a heart rate monitoring sensor. S3 is a blood pressure sensor (Sunrom-1437) that reads the systolic, diastolic, and Pulse. Finally, S4 is an accelerometer sensor (MMA7260QT) that is used for measuring patients' body movements. This sensor will measure the body movement in the X, Y, and Z-axis. This sensor will help to control patient movement within the hospital.

For simplicity, only one sensor per patient is considered. The root node acted as a gateway node. Root node formed a network by sending DIO messages consisting of the version number, rank, and other control information. All the sensor nodes, upon receiving this DIO, calculate the rank value using an objective function. This rank value had sent as an acknowledgment in the form of a DAO message. If any other node wanted (attacker node as shown in figure 1) to join the existing sensor network, then it sent a DIS message in the network and once it got DIO as an acknowledgment it joined the network. Moreover, sensor nodes exchange the DIS message to verify the version number and other routing parameters.

There are two ways for an attacker to perform an attack. One is by using spoofing. The attacker can make use of reconnaissance tools to get the address of the root node in the network and it will send the DIO with the modified version number. After getting a new version number from the attacker node, every other node of the network will update its copy, also update the routing table entry, and hence become a part of the attacker network.

Secondly, in the RPL protocol, the nodes will send DIS to the neighbouring node to ensure the routing entries are not obsolete. The response to this DIS is a DIO message. If it contains a new version number or rank value, then the node will mark their routing table entry obsolete. The attacker will make use of this technique, as shown in figure 1, even though the attacker is not in the coverage range of the root node, it still sends a DIS message to the neighbouring accessible node (S1) as the attacker gets connected with S1. The node S1 will send DIO received from the root node as an acknowledgment of the DIS message towards the attacker node.

An attacker gets the DIO message which contains the version number and rank, now the attacker sends another DIS to S1 with a modified version number or rank and S1 assumes that the version number or rank value changes hence it updates its routing table and becomes a part of the attacker's network. Similarly, S1 will forward this DIS to other nodes in the network hence all the nodes will update their routing table and fall prey to version number attack or rank attack. Depending on the value of rank forwarded by the advisory node, the network fall prey to increased rank r decreased rank attack.

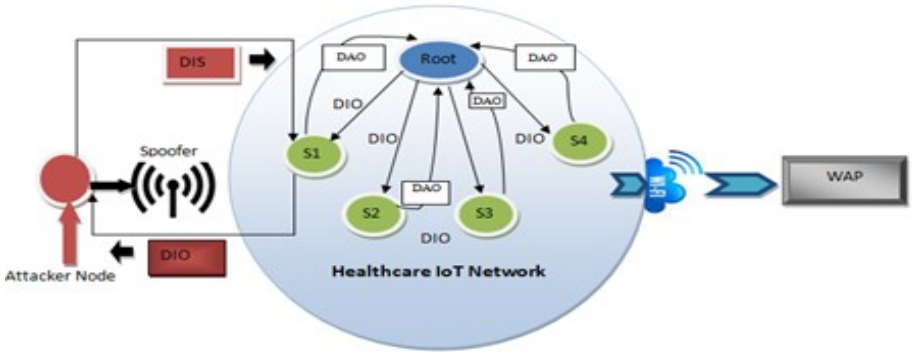


Figure 1. - Threat model for the version number and Rank attack.

4. PROPOSED SYSTEM

Detection of version number attack and rank attack is very challenging. Both the attacks are the strongest threat as they deteriorate the network life slowly and disturb the routing topology [19].

4.1 Proposed Methodology

In the proposed methodology, the preferred parent listis used to select the detection agents. The 6LoWPAN network maintains the preferred parent list and the objective protocol of RPL is used to select the preferred parent. The activation of the proposed rule-based attack detection system depends on the following routing-specific metric. i) Energy consumption ii) Beacon interval iii) Expected transmission of packet (ETX).

At first, the reference network given in figure 2 was analysed thoroughly and the energy consumption parameters at the detection agents were extracted from the network. The energy consumption parameters include consumption of CPU power, low power mode power (LPM), data transmit power (Tx) and data receive power (Rx) of the reference network. The total energy calculated using the following equation number 1, where the extracted energy values (CPU, LPM, Tx, Rx) are multiplied with the current data value given by the sensor datasheet [20].

$$TotalEnergyConsumed = \sum_{s=1}^{n} \frac{(1.8*CPU+0.0545*LPM+21.8*Rx+19.5*Tx)*3}{RTimer}$$ ----------eq.1

S -Set of sensor nodes varies from 1 to n

Energy consumption is a crucial parameter considered for the detection of an attack. An attacker attacks the network and disturbs the entire routing process, increases the control message transmission, which ultimately increases the energy consumption and depletes the battery power.

The second parameter used for the implementation of the detection system is the beacon interval. The beacon interval is inversely proportional to control traffic overhead. The control traffic overhead (CT) is the traffic of control messages (DIO, DAO, DIS) circulated in the 6LoWPAN network. The proposed methodology estimated the value of the beacon interval in the original network. If the beacon interval decreases, then the control traffic overhead increases. Attacker node forwarded the revised version number or revised rank value with the DIS message and eventually, the network changes the entire routing tables, experiences the huge traffic, resultantly network attempts the global repair mechanism.

The third parameter considered in the proposed methodology for attack detection is ETX. The ETX was estimated at the preferred parent node. The ETX is a metric directly affected by a version number and rank attack. The ETX specifies several transmissions for a message to be delivered successfully from source node to destination node. The network is more reliable if the ETX value is lower.

The ETX is calculated using equation number 2.

$$ETX = \frac{1}{df*Dr}$$ ----------eq.2

$df * dr$ is the success probability of data transmission by the node. If the node ‘a’ transfers the message to the neighbouring node 'b' then the forward delivery ratio (df) is the number of messages received successfully by node ‘b’. Whereas, reverse delivery ratio (dr), is the acknowledgment received by node 'a' on the same link. ETX is a very crucial parameter in the RPL network; the attacker node disturbs the routing result in the increase of the ETX value increases and a decrease in network reliability.

The proposed rule-based detection system is activated if the energy consumption, beacon interval, ETX deviates from the estimated threshold values. After activation, the alarm message broadcasted by the sink node in the entire network. The alarm message is in the form of a DIO packet, which contains the authenticated version number and rank values. Upon receiving this DIO message from the sink node, the network repair itself with the help of authenticated version number and rank number. Further, the detection mechanism estimates the energy consumed by every sensor node to detect the intruder node.

The above signatures ETX, beacon interval, and energy consumption, are directly or indirectly proportional to the various other routing parameters of the RPL network. Hence, during the implementation, it was observed that if the above metrics deviated, the other routing parameters also get disturbs and the entire routing process of the RPL protocol gets interrupted. The proposed routing-specific attack detection algorithm is given below.

The rule-based routing specific attack detection algorithm in the 6LoWPAN network

1. Let, S_{ni} - the set of sensors node in the network {where n =1, 2, 3…}
2. R-Root node of DODAG
3. ΔTE- Reference threshold estimated for Energy consumption of the network.
4. T_e–Reference threshold estimated for Energy consumption at each node i.
5. ABI-Average value of beacon interval at the root node
6. Δ B-Threshold of the average beacon interval
7. Δ ETX-Threshold value of ETX
8. For root node in S_{ni} do
    a. Monitor the root node R at regular intervals.
        Calculate the value of energy consumed using eq.1
        Total_Energy_Consumption =$\sum_{i=1}^{n} energy_{consumption}$
        Calculate the value of ETX using eq.2

$$ETX = \frac{1}{Df * Dr}$$

    b. if (Energy_Consumption> ΔTE)
        if (ABI<Δ B)
            if (ETX>Δ ETX)
                Detection mechanism activated and intrusion detected, alarm message broadcasted.
            End if

End for

9. for each node(ie for i=1-n) inS_{ni}do
    c. if (Energy Consumption>Te) then
        remove the node from the network.
        End if

End for.

5. Results and Discussion

The proposed system implemented using a Contiki-Cooja simulator. The experimentation starts with reference network implementation as shown in figure 2 consisting of a root sensor node (node number 1), which acts as a detection agent and the randomly deployed 20 source nodes (node number2 to 21). Nodes in the reference network setup using the transmission range of 50m and interference range of 100m.

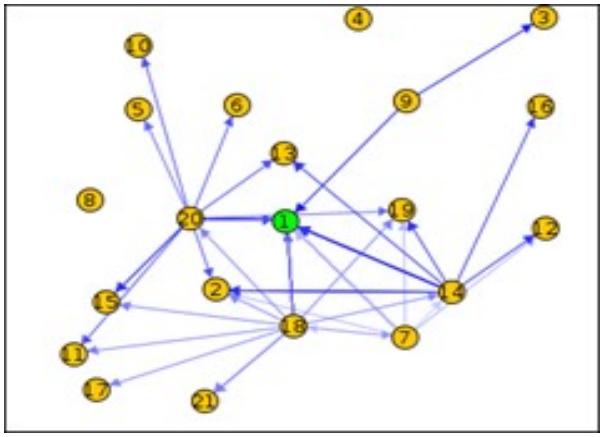


Figure 2. -Reference Network

The proposed rule-based activation and detection algorithm given the preceding section 4.1 required the threshold values of energy consumption, beacon interval, and ETX of the reference network. The threshold values were estimated using the averaging method. The implementation started with analysing the reference network thoroughly. At first, the CPU power, LPM power, transmit power(Tx), and receive power(Rx) of the reference network are extracted as given in figure 3 below, and the total energy consumption calculated using equation number 1.

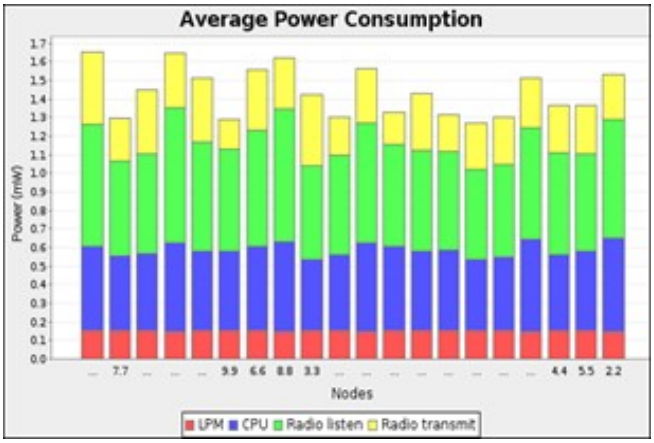


Figure 3. -Average Power Consumption of reference network

Further, the beacon interval and ETX parameters are extracted from the reference network. The reference network is a stable network with all genuine nodes hence precise control messages were circulated in the network. The following figure 4 shows the comparative values of beacon interval and ETX.

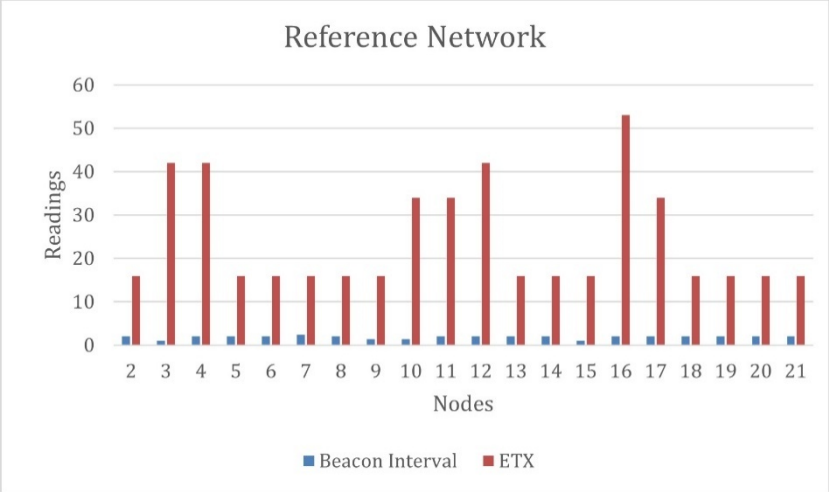


Figure 4. - Beacon interval and ETX of the reference network

Subsequently, the attacks were launched using an attacker node varies from 10% to 30%. The detailed implementation of attacks is given in the following section 5.1.

5.1 Attack Implementation

To prove the precise results, this paper launched the attacks on the reference network and the attacked reference network was analysed thoroughly. Further, the results proved that the attack was detected using the proposed detection system in less time and with more accuracy.

5.1.1. Version Number Attack

The one attacker node (node number 22) as shown in figure 5 below, launches the version number attack in the reference network. At first, the attacker node transfers the DIS message to the neighbouring connected node. The neighbouring node sends the DIO towards an attacker node, which contains the version number field. The attacker node alters the version number field in its DIO message, updates the version in its record, reset its tickle timer, and transfers this version number value to the connected node. The difficulty with the RPL protocol is that there is no mechanism exists to check the integrity of the version number in the received DIO message. As soon as the neighbouring node receives this DIO packet, it considers that its routing table values are obsolete. At the same time, it forwards the altered version number to the other connected nodes by using a DIS message. The illegitimate version number value propagated in the network, resultantly the entire network experiences loop, the value of ETX certainly raised as shown in figure 7 and the network performs the global repair mechanism. The global repair mechanism includes the reestablishment of all routing tables. Routing table reestablishment increases the control message traffic, which involves a decrease in beacon interval as given in figure 7. The global repair, the mechanism that consumes the power of the networks shown in figure 6 attenuates the network life and the network certainly experiences an attack. Moreover, the newly created network was not created from root hence it is acyclic, allowing loops in the networks.

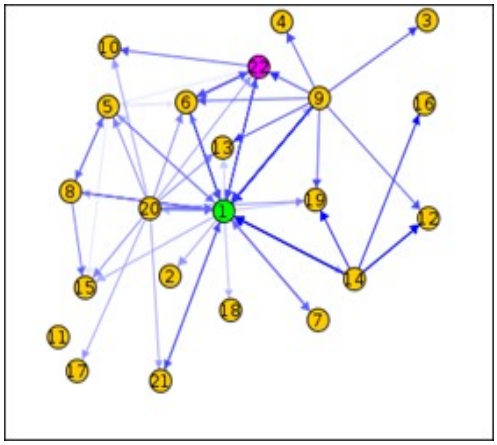


Figure 5. - Snapshot of VNA

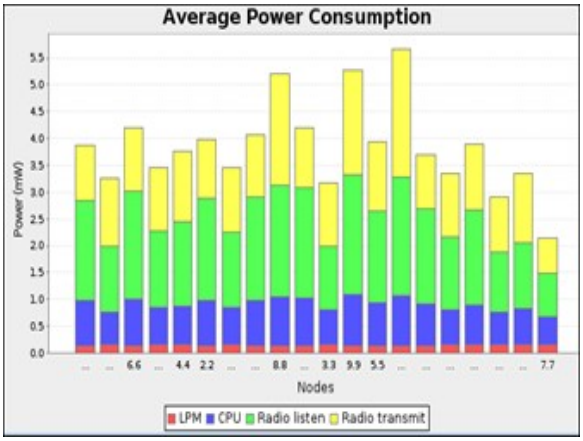


Figure 6. -Average Power consumption of VNA

VNA-Version number attack

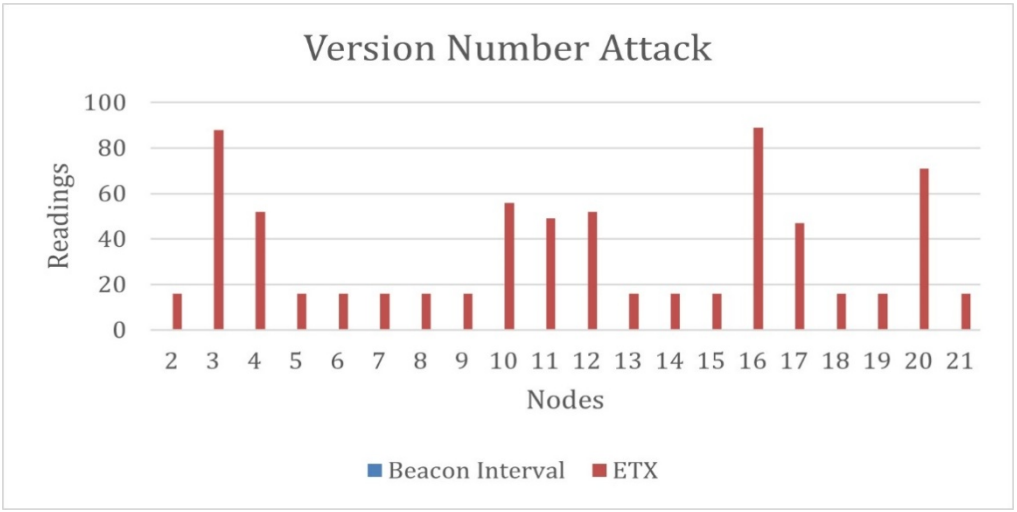


Figure 7. - Beacon interval and ETX of version number attack

5.1.2. Rank Attack

Routing metric and rank property are the two vital measures that prevent the formation of loops in the RPL network. However, the attacker node wields the rank and forwards the higher value or lower value of the rank in the network. Hence, the network experiences the increased rank or decreased rank attacks. The increased rank attack launched in the reference network, as shown in figure 8 using the sensor node with ID -22. The sensor nodes with the lower rank values acted as preferred parents for the descendent nodes. The root node has the lowest rank value. The advisory node advertises the higher rank value, hence the entire parent-child relationship of the network disturbed, and loops were formed in the network. The formation of these loops increases the number of transmissions from one node to another hence the ETX raises, and the beacon interval decreases than its threshold as shown in figure 10, respectively. Moreover, attacked network consumes the access power than the reference network as shown in figure 9.

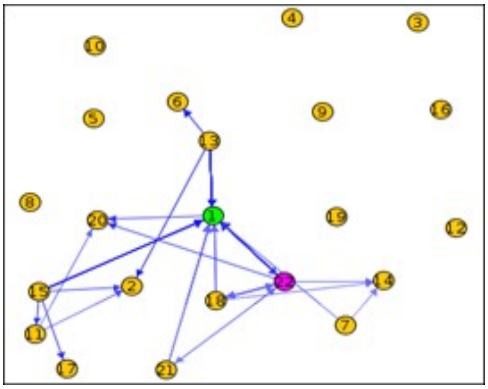


Figure 8. - Snapshot of IRA

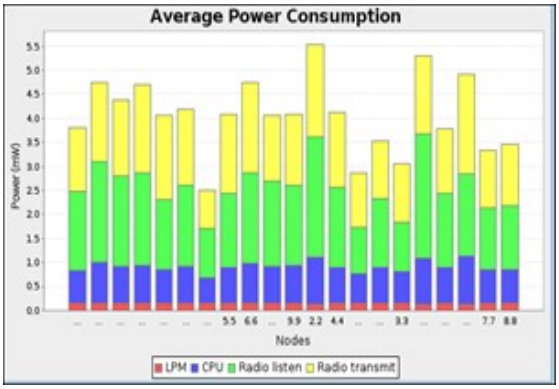


Figure 9. -Average Power Consumption IRA

IRA-Increased rank attack

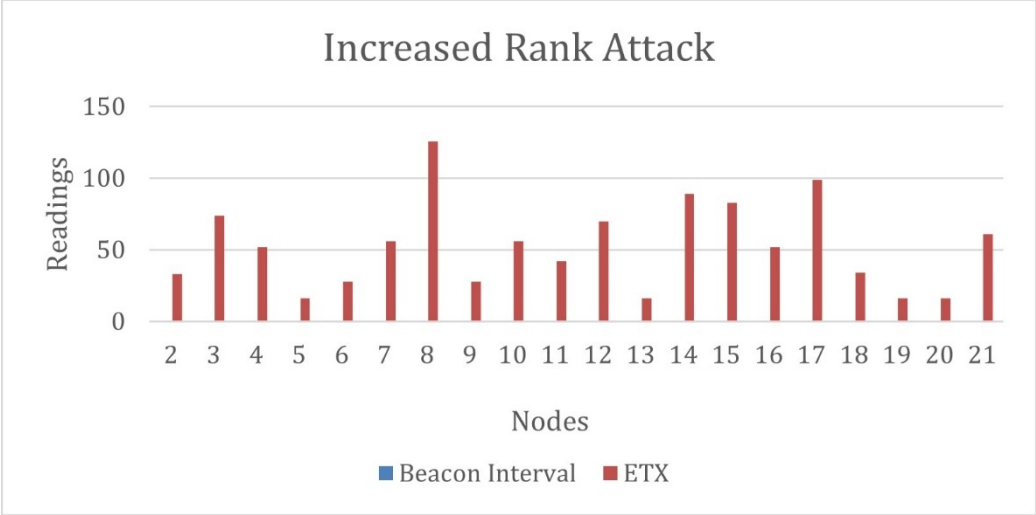
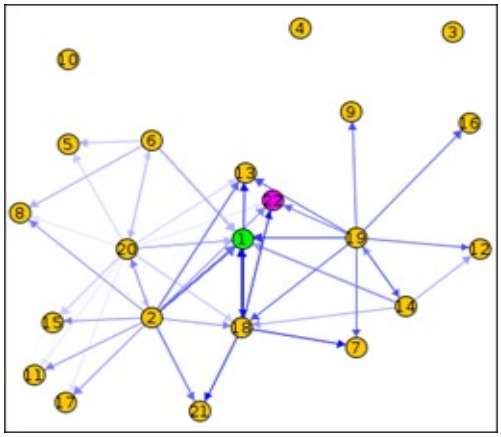


Figure 10- Beacon interval and ETX of increased rank attack

The decreased rank attack opts for the exact reverse technique for launching an attack. The advisory node with ID -22 as shown in figure 11 below, advertises the lower rank value and the network experiences a decreased rank attack. The lower rank value compels the other genuine nodes with lower rank to choose an advisory node as a preferred parent. This is an alarming situation as most of the nodes forward the data to the root advisory node and the attacker takes control of the maximum part of the network. The rerouting mechanism of the network forced to reduce the beacon interval and increase in ETX value given in figure 13. The power consumption also raised as compared to the reference network as shown in figure 12, however, once the advisory succeeds in controlling most of the networks as the preferred parent the entire network is controlled by the advisory. This is more dangerous than an increased rank attack and its detection is also tedious.



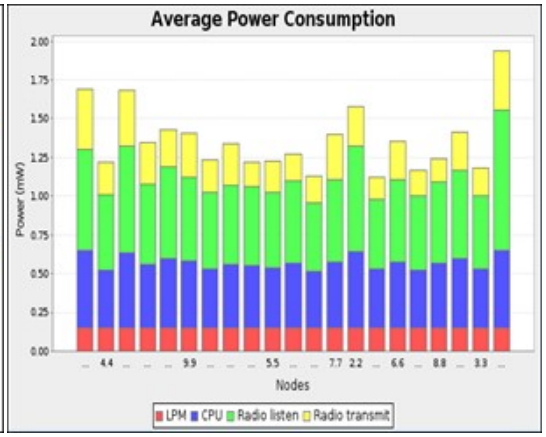


Figure 11. - Snapshot of DRA Figure 12. -Average Power Consumption DRA

DRA-Decreased Rank attack

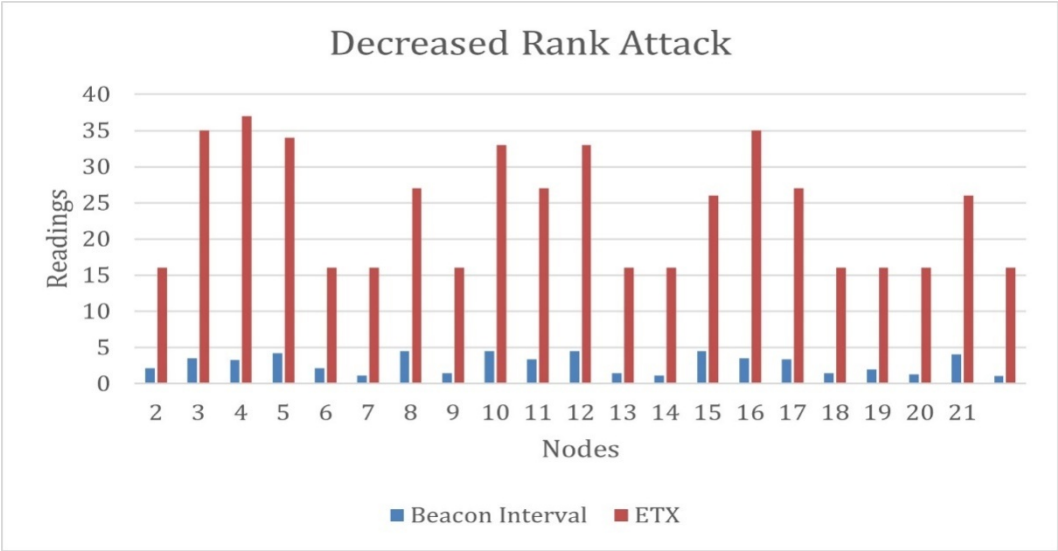


Figure 13- Beacon interval and ETX of decreased rank attack

5.2. Attack detection

The above section 5.1 implements the crucial attack, which proved to be dangerous for healthcare IoT systems. For testing the inbuilt security mechanism of RPL, this research executed the attack multiple times by gradually increasing the number of attacker nodes. The attacked network was observed for 10-12 hours. It was observed that the inherent healing mechanism of RPL will not work and the network continues to deteriorate its performance and certainly the entire network collapse. Hence, it is of utmost importance to implement a protection mechanism for the RPL-IoT network.

The proposed methodology put forth the rule-based detection system, which considers all the essential routing parameters as discussed in the above section 4.1 of the proposed methodology for the detection of the attack. Attack's implementation results proved that the routing parameters deviate from the threshold values and the attack was detected with a detection rate of 90% and a false-positive rate of 11%. After detecting the attack, the alert message broadcasted in the network by the sink node. The proposed method proved that it consumed less power hence it is a lightweight rule-based attack detection mechanism, best suitable for constrained

IoT devices. Further, the attacker node is removed from the network, and the network repair itself.

The CPU power consumption of the proposed attack detection system is shown in figure14, was calculated as 77% which is less as compared to the centralized IDS proposed by [21]. The proposed detection system is further compared with the IDS proposed by the authors [22]. The system proposed by authors [22] detects the version number attack however the real-time data not used hence the accuracy of detection is less as compared to the proposed method. In addition, the time required to detect an attack is another important factor in the implementation of the attack detection system, as more the time required for detection more damage will cause to the network. The proposed detection system detects the attacks on 60 clock ticks (simulator time) hence the damage caused to the network is negligible.

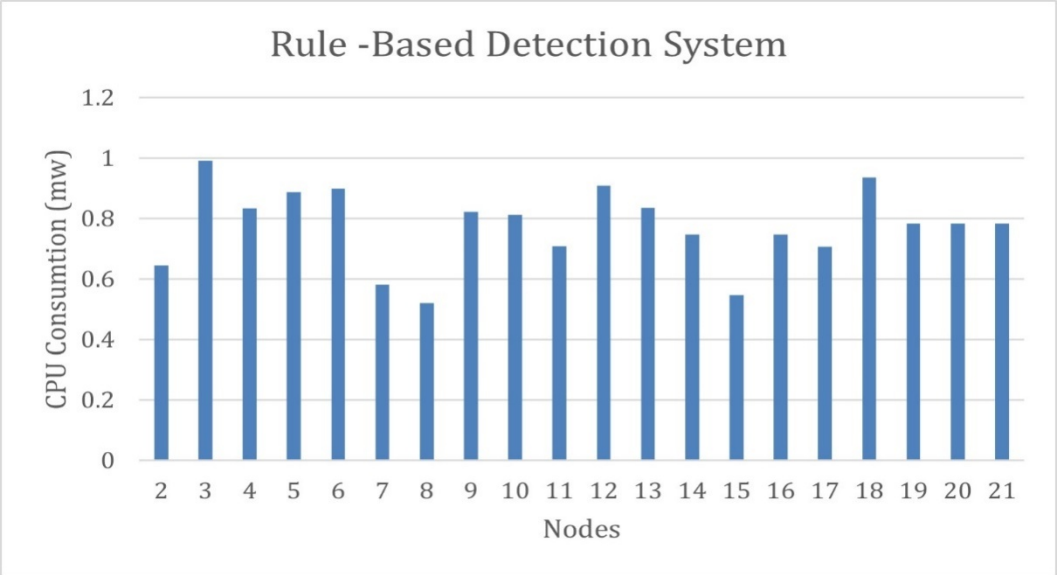


Figure 14. - CPU power consumption after attack detection and removal of the node

Conclusion

IoT achieves technological excellence; however, before implementing the applications using IoT, security must be the utmost concern. The use of IoT provides potency to the healthcare sector. Nonetheless, the healthcare IoT system will collapse without incorporating the security of healthcare IoT devices. Very few researchers addressed the defence mechanism of version number and rank attacks. Hence, this paper provided the robust rule-based detection algorithm based on RPL vital routing parameters. The simulation results prove that the proposed detection system detects the version number and rank attack with more accuracy and in less time. The results demonstrated that the proposed system consumes less energy hence it will be a pertinent solution for providing security to the IoT network. The future research of this proposed system is to test the prevention against the other RPL attacks with increased accuracy and less false positive ratio.

REFERENCES

[1] Dudhe, P. V., Kadam, N. V., Hushangabade, R. M., & Deshmukh, M. S. (2017, August). Internet of Things (IoT): An overview and its applications. In 2017 International *Conference* on Energy, Communication, Data Analytics and Soft Computing (ICECDS) (pp. 2650-2653). IEEE.

[2] Vasseur, J. P., Kim, M., Pister, K., Dejean, N., & Barthel, D. (2012). Routing metrics used for path calculation in low-power and lossy networks. In RFC 6551 (pp. 1-30). IETF.

[3] Barbir, A., Murphy, S., & Yang, Y. (2004). Generic threats to routing protocols. IETF Draft: draft-ietf-rpsec-routing-threats-07.

[4] Mayzaud, A., Badonnel, R., &Chrisment, I. (2016). A Taxonomy of Attacks in RPL-based Internet of Things. International Journal of Network Security, 18(3), 459-473.

[5] Ambarkar, S. S., &Shekokar, N. (2021). Critical and Comparative Analysis of DoS and Version Number Attack in Healthcare IoT System. In Proceeding of First Doctoral Symposium on Natural Computing Research (Vol. 169, p. 301). Nature Publishing Group.

[6] Qu, H., Lei, L., Tang, X., & Wang, P. (2018). A lightweight intrusion detection method based on fuzzy clustering algorithm for wireless sensor networks. Advances in Fuzzy Systems, 2018.

[7] Subba, B., Biswas, S., &Karmakar, S. (2018). A game theory based multi layered intrusion detection framework for VANET. Future Generation Computer Systems, 82, 12-28.

[8] Kamble, A., Malemath, V. S., & Patil, D. (2017, February). Security attacks and secure routing protocols in RPL-based Internet of Things: Survey. In 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI) (pp. 33-39). IEEE.

[9] Chacko, A., &Hayajneh, T. (2018). Security and privacy issues with IoT in healthcare. EAI Endorsed Transactions on Pervasive Health and Technology, 4(14).

[10] Fatima, A., &Colomo-Palacios, R. (2018). Security aspects in healthcare information systems: A systematic mapping. Procedia computer science, 138, 12-19.

[11] Bradley, C., El-Tawab, S., &Heydari, M. H. (2018, April). Security analysis of an IoT system used for indoor localization in healthcare facilities. In 2018 Systems and Information Engineering Design Symposium (SIEDS) (pp. 147-152). IEEE.

[12] Dvir, A., &Buttyan, L. (2011, October). VeRA-version number and rank authentication in RPL. In 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems (pp. 709-714). IEEE.

[13] Perrey, H., Landsmann, M., Ugus, O., Schmidt, T. C., &Wählisch, M. (2013). TRAIL: Topology authentication in RPL. arXiv preprint arXiv:1312.0984.

[14] Mayzaud, A., Badonnel, R., &Chrisment, I. (2017). A distributed monitoring strategy for detecting version number attacks in RPL-based networks. IEEE Transactions on Network and Service Management, 14(2), 472-486.

[15] Nikravan, M., Movaghar, A., &Hosseinzadeh, M. (2018). A lightweight defense approach to mitigate version number and rank attacks in low-power and lossy networks. Wireless Personal Communications, 99(2), 1035-1059.

[16] Arış, A., Yalçın, S. B. Ö., &Oktuğ, S. F. (2019). New lightweight mitigation techniques for RPL version number attacks. Ad Hoc Networks, 85, 81-91.

[17] Le, A., Loo, J., Lasebae, A., Vinel, A., Chen, Y., & Chai, M. (2013). The impact of rank attack on network topology of routing protocol for low-power and lossy networks. IEEE Sensors Journal, 13(10), 3685-3692.

[18] Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the internet of things: a survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials, 17(3), 1294-1312.

[19] Boudouaia, M. A., Ali-Pacha, A., Abouaissa, A., & Lorenz, P. (2020). Security Against Rank Attack in RPL Protocol. IEEE Network, 34(4), 133-139.

[20] Moteiv Corporation, "Tmote Sky Datasheet," 2006. [Online]. Available: http://www.moteiv.com/products/docs/tmote-sky-datasheet.pdf.

[21] Sforzin, A., Mármol, F. G., Conti, M., &Bohli, J. M. (2016, July). Rpids: Raspberry pi ids—a fruitful intrusion detection system for iot. In 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and

Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld) (pp. 440-448). IEEE.

[22] Sahay, R., Geethakumari, G., Mitra, B., & Sahoo, I. (2018, December). Efficient framework for detection of version number attack in internet of things. In International Conference on Intelligent Systems Design and Applications (pp. 480-492). Springer, Cham.