Critical and Comparative Analysis of DoS and Version Number Attack in Healthcare IoT System

Smita Sanjay Ambarkar and Narendra Shekokar

Abstract Recently the entire world is witnessing the pandemic outbreak of COVID 19, which creates havoc in the healthcare industry. Error tolerance may lead to death threats for the patient in the healthcare system. However, practically the healthcare industry faces many manual error incidences, inadequate staffing, aging population, etc. These challenges will increase the stress level and disturbs the psychological as well as physical health of the healthcare practitioner. Internet of things (IoT) technique is adept to tackle such outbreaks by providing complete digitization of healthcare systems. However, IoT application deployment comes with many security threats and attacks challenges. Here it is worth mentioning that to implement a robust security solution, the comprehensive analysis of attack must carry out. This paper contributes by analyzing two preeminent attacks, the Denial of service (DoS) and version Number attack on the healthcare system. DoS rapidly destroy the network whereas version number haltingly takes control of the network. The paper further critically analyzes the performance and severity of these two attacks based on discrete parameters like routing metric, power consumption, number of packets received, number of expected transmissions, beacon interval, and proposes the robust solution.

Keywords IoT · DoS attack · Version number attack · Cooja · Security · Healthcare system · Sensors · RPL,6LoWPAN

1 Introduction

Internet of Things makes ubiquitous computing more adept and promising for healthcare applications. IoT is an IPv6 network with the support of various wireless
communication protocols like LORA, Wi-fi, Zigbee, 6LoWPAN, Bluetooth, etc. However, the study and implementation of this paper based on 6LoWPAN protocol as it provides certain advantages like the auto-configuration and scalability. 6LoWPAN network allows sensor nodes to move easily. However, any sensor node can easily join or leave the 6LoWPAN networks. This allures the attacker to breach the security of the IoT network and agitate the normal routing. RPL is an IPv6 routing protocol for low-power and lossy IoT networks [1] proposed by IETF (Internet engineering task force). RPL efficiently creates and exchanges the network route but falls prey to numerous routing attacks [2–4]. In comparison with other attacks, the version number and DoS are more threatening and severe.

Version number attack is an internal attack caused by the internal node after joining the IoT network. Each DODAG assigned a version number to every node. Every node in the IoT network must have the same copy of version number. Inconsistent view of version number will disturb the topology and lead to the formation of loops and discontinuity in the network. However, an attacker disrupts the normal routing of the RPL network by advertising the incorrect version number. The DoS attack occurs when a system or machine maliciously gets flooded with traffic or information that makes it crash or be otherwise inaccessible to users. An internal or external intruder node can cause DoS. In contrast to other confidentiality attacks in the RPL protocol, the DoS attack does not abduct any data or information. Nonetheless, the DoS attack will force the system to halt by flooding it with abundant requests. In the healthcare system, this perhaps will cause bereavement of life. The paper will be addressing the practicalities of these two diverse attacks. The next section gives detailed related work. Further in Sect. 3 put forth experimentation details of the version number and DoS attack. Observations about different attack parameters are specified in Sect. 4. The proposed system is explained in Sect. 5. Finally, Sect. 6 presents the conclusion.

2 Related Work

IoT revolutionized the healthcare system and escalated to another level. However, the digitization of healthcare comes with the cost of security [5]. In literature, various authors demonstrated the various aspects of the IoT system [6] presented the energy-efficient IoT system but lack to provide the security aspect whereas the authors also put forth the theoretical aspects of various RPL attacks [7]. The practical way of attacking is still unrevealed. The authors of [8] explain the detailed importance of information security in the healthcare system (HIS). The paper mainly concerns the security of patients’ data. The survey further focuses on version number and DoS attack implementation and prevention techniques.

Version number attack causes severe control message congestion in the network and formation of loops which results in a reduced lifetime of the network and loss of the packet. As per the depth of our knowledge, only a few researchers have addressed the version number attack. The distributed monitoring approach proposed by the authors [13] to detect the version number attack. This distributed monitoring
architecture conserves the resources in a constrained advanced network. Authors of [14], make the use of a hash chain to hinder the modification of version number in the RPL control message. However, the hash chain imposes the extra congestion and overhead on the network. Moreover, hash chains are also prone to several attacks. Hence, this technique will not assure the detection of version number attack.

DoS is a flooding attack caused by internal or by external attacker node [10]. The author put forth hello flood and sinkhole as two new classes of attacks. Furthermore, the authors demonstrated that the routing protocols used in IoT networks are not secure. Hence, they have discovered the identity verification protocol as a defense against HELLO flood attacks. Nevertheless, this protocol provides the simple defense mechanism but it will not ensure the security of IoT devices hence authors left the security building mechanism as an open problem. Authors of [11] implemented the heartbeat protocol to counter the DoS, selective forwarding, and other attacks. The authors implemented the attacks by using Contiki cooja. Authors of [12] proposed the anomaly-based IDS approach for the detection of DIS attack and neighbor attack. All the other attacks considered for future implementations. Authors of [9], develops the IoT based system for healthcare for the location of patients in healthcare facilities. Paper demonstrated the DoS attack on the healthcare IoT system using Kali Linux and hydra tool. The authors implemented an external DoS attack by flooding ICMP messages. To prevent this attack, the authors suggested using digital certificates for securing the connection between the edge node and the AWS database. A literature survey reveals that the DoS attack induces lethal damage to the network making it completely inoperable.

3 Attack Experimentation

This paper uses Contiki-Cooja as a simulation tool for the implementation of DoS and version number attack. Contiki OS is an open-source operating system for IoT that runs for low constrained resources. The attacks performed on the reference network, which contains all legitimate nodes. RPL used as a routing protocol. The RPL is an unsecured protocol hence the network provided with minimum security.

The performance of reference nodes measured according to the different parameters concerning energy consumption and routing. At first, the average power consumption of the reference network measured concerning the sum of four parameters, as shown in Fig. 1. (i) The energy spent to process node task (CPU power) (ii) Power consumed by the node in standby mode (LPM power). (iii) Energy spent by the node listening for messages (Rx Listen Power). (iv) energy spent to transmit packets (Tx Transmission Power). The nodes, which are within the transmission range of the sink node, consume more power. The average power consumption is 1.75 mw.

The next parameter considered for performance evaluation is the radio duty cycle. ContikiMAC is the simple, asynchronous radio duty cycle protocol. ContikiMAC estimation of the amount of radio packet transmitted and received by the node is 2.0%. Further, the network convergence used for performance evaluation. According
to the simulation results, the reference network convergence time is 3 min (real). The network convergence calculated as given in Eq. 1,

\[ N_{ct} = (DIO) t_n - (DIO) t_x \]  

(1)

where
Nct—Network convergence time.

(DIO) tn—Time of last DIO joined DODAG.

(DIO) tx—Time of First DIO sent.

3.1 Performance of Reference Network After Version Number Attack

As soon as attack initiated on the reference network, the beacon interval of entire nodes in DODAG instantly falls as the reorganization of the DODAG nodes increases their frequency of broadcasting beacon frames, which assuredly increases the radio duty cycling as given in Fig. 2.

Where, VNA-Version Number Attack.

Reconstruction of DODAG requires the calling of the global repair mechanism. The global repair mechanism consumes time, which is nothing but the network convergence time as given in equation number 1. The network convergence time required after the instigation of version number attack shown in Fig. 3 is 42 min (real), which is large as compared to reference networks convergence time. Further, noticeable parameters are hop counts and routing metric value, which certainly increases. If these parameters are left unnoticed in the healthcare IoT network, the attacker will

Fig. 3 VNA-NC
foment the attack after a regular interval then the sensor reading of the patients will
difficult to recognized and the system will gradually inoperable. Another reason for
system inoperability is a huge increase in power consumption as shown in Fig. 1.
The power consumption increased because repeatedly DODAG is busy reorganizing
itself.

3.2 Performance of Reference Network After DoS Attack

The DoS attack is the most hazardous as in no time it makes the devices completely
inoperable by sending numerous requests in the network.

The implementation of this attack requires the configuration of the attack node
in such a way that it should send the DIS with a very small interval so that the DIS
packet will flood the entire network. All the nodes in DODAG are busy in receiving
the packets they could hardly transmit any, hence the radio listens duty cycling shows
the huge increase as given in Fig. 5. This will show the hasty decrease in the beacon
interval. The routing metric value certainly decreased as compared to the reference
network because with the existing route attacker tried to forward numerous packets.
As all the nodes will show “always-on” behavior the average power consumed will
also be very high given in Fig. 4. The network shown in Fig. 6 shows disconnection as
the convergence time for the network is extremely large as compared to the reference
network, simulation results shown the network convergence time is 57 min (real).

Fig. 4 DoS-APC
4 Observations

Attacks in the healthcare IoT system may lead to the death threat of patients hence it is of utmost essential to secure the healthcare IoT systems. This paper addressed two diverse attacks. The following Table 1 provides observations after rigorously comparing various parameters of DoS and version number attacks.
| SN | Observed parameters  | Attacks          | Observations                                      |
|----|---------------------|------------------|--------------------------------------------------|
|    |                     | Version number   | DoS                                              |
| 1  | Routing metric      | Increased        | Decreased                                        |
|    |                     | Version Number attack requires reconstruction of DODAG, which modifies the routing table. Hence, the increase in the routing metric is observed. DoS does not alter any routing table entries and uses the existing route to flood the network. |
| 2  | Beacon interval     | Decreased        | Decreased                                        |
|    |                     | As in both the attacks nodes increases the frequency of broadcasting and receiving of packets. |
| 3  | Average power consumption | Increased | Increased                                        |
|    |                     | Power consumption increased in version number attacks because of the instigation of the global repair mechanism. DoS attack kept nodes “always ON” hence LPM power values decreases and CPU power consumption increases to process incoming DIS messages which result in the rise of total power consumption. |
| 4  | Average received packets | Decreased | Decreased                                        |
|    |                     | Version number attack triggered global repair mechanism that changes complete routing configuration hence the DIS/DIO packet transferred will be lost therefore the intended nodes experience decreased average received packet rate. DoS attack keep node busy in receiving the packets also attack cause congestion in the network results in decreased received packet ratio. |

(continued)
Table 1 (continued)

| SN | Observed parameters | Attacks | Observations |
|----|---------------------|---------|--------------|
| 5  | ETX (Expected transmission count) | Constant | Decreased |

In version number attacks, even though new DOADG is formed the link quality remains the same hence ETX is the same as the reference network. In DoS because of flooding of the DIS message and node continuous processing, the node battery drain off. Further, the processing capacity of the node also deteriorates which adversely affects link quality therefore the ETX value gets decreased.

5 Proposed Security Solution

Cryptography is the top choice for securing IoT networks. However, every time it is not desirable to encrypt each data as it imposes the computational burden on low constraint IoT devices. Instead, Intrusion detection systems provide a promising solution for securing low constraint devices. This paper proposes the Intrusion detection system, which detects the intrusion using energy consumption at the nodes. Authors of [15] SVELTE that detect the intrusion using RPL rank value. However, only the RPL rank value not detects the variety of attacks. Therefore as per the analysis of attacks in the previous section authors of this paper reveals that energy consumption is a vital signature to detect a variety of attacks. Energy consumption of the network increases if it experiences the DOS, version number, sinkhole, wormhole, gray-hole attacks. In the proposed system, the energy consumption of the network calculated using Eq. 2 and stored at the root node.

Energy Consumption = ((1.8 * CPU + 0.0545 * LPM + 21.8 * Rx + 19.5 * Tx)) * 3/RTIMER(SECOND)

The proposed scheme uses a distributed IDS approach to reduce resource consumption. 6LoWPAN network maintains the preferred parent list. RPL protocol used objective function to select the preferred parent. This preferred parent acted as an IDS agent for monitoring. In the proposed algorithm IDS agent will monitor the flow of the other sensors node in the network. The calculated value of energy consumption compared with the threshold. If calculated energy consumption value does not adhere to the threshold then IDS gets activated. Further, to remove the
malicious node, the system calculates and compares the energy consumption values at every node. The node with the highest energy consumption removed from the network. The proposed scheme has a faster detection rate and less overhead as the decision made locally, and no alert messages circulated in networks. Algorithm 1 gives the overall working of the proposed IDS.

---

The algorithms for IDS in 6LoWPAN network

Let, $S$ - the set of sensors node in the network \{$s_1,s_2,s_3$\}, $R$-Root node

$\Delta$ - Threshold for the Energy consumption of the network

$\Delta_i$ - Threshold for Energy consumption at each node $i$.

for Node in $S$ do

Monitor flow from Node to R

Calculate energy_consumption using eq.1

CPU=Current CPU-Last CPU

LPM=Current LPM-Last LPM

Tx=Current Tx-Last Tx

Rx=Current Rx-Last Rx

Total_Energy_Consumption = $\sum_{i=1}^{S} energy_{consumption}$

if (Energy_Consumption > $\Delta$)

IDS activated

end if

end for

for each node in $S$ do

if (Energy Consumption > $\Delta_i$) then

Node removed from network

end if

end for

---

The reference network is formed using Contiki Cooja with 1 sink and 4 source nodes. DoS attack is launched using one attacker node as shown in Fig. 7. The IDS agent started monitoring the network. The IDS activated as the energy consumption of the network is more than the decided threshold and attack detected as shown in Fig. 8. As soon as the attacker node started attacking the network the attack detected, hence the proposed system is very effective as it protects the network from further loss. The future scope of this system is to detect the other RPL attacks and reduced the false-positive ratio.

---

6 Conclusion

Undoubtedly, the healthcare sector needs automation and IoT is an elite technology for that. Nonetheless, IoT provides efficiency and accuracy to healthcare sectors; it comes with the cost of privacy and security depletion, which is not tolerable for the
healthcare sector. Hence, there is a need to understand the impact of various attacks and threats on the IoT network. In this work, we have presented a detailed comparative analysis of version number and DoS attack. DoS and version number attack expend the IoT network resources and slackens the performance of the network. Hence, the detection of these attacks is very essential. This paper intensively reviewed the RPL protocol standard the put forth various peculiar parameters to show the impact of rarely addressed version number attack and popular DoS attack. Further, the paper proposes IDS as a solution for security. The proposed algorithm is effective as it detects the attack at a faster rate. Thereby, preventing the system from further damage.
References

1. Kushalnagar N, Montenegro G, Schumacher C (2016) IPv6 over low-power wireless personal area networks (6LoWPANs (Online). Available https://tools.ietf.org/html/rfc4919
2. Mayzaud A, Badonnel R, Chrisment I (2016) A taxonomy of attacks in RPL-based Internet of Things. Int J Netw Secur 18(3):459–473
3. Wallgren L, Raza S, Voigt T (2013) Routing attacks and countermeasures in the RPL-based Internet of Things. Int J Distrib Sens Netw, Sage, pp 1–11
4. Dhumane A, Prasad R, Prasad J (2016) Routing issues in Internet of Things: a surve. In: Proceedings of the international multi conference of engineers and computer scientists, pp 16–18, Mar 2016
5. Ambarkar SS, Shekokar N (2020) Toward smart and secure IoT based healthcare system. In: Dey N, Mahalle P, Shafi P, Kimabahune V, Hassanien A (eds) Studies in systems, decision and control Internet of Things, smart computing and technology: a roadmap ahead, vol 266, Springer, Cham
6. Mangla M, Akhare R, Ambarkar S (2019) Context-aware automation based energy conservation techniques for IoT ecosystem. In: Mittal M, Tanwar S, Agarwal B, Goyal L (eds) Studies in systems, decision and control energy conservation for IoT devices, vol 206, Springer, Singapore
7. Kamble A, Malemath VS, Patil D (2017) Security attacks and secure routing protocols in RPL-based Internet of Things: survey. In: International conference on emerging trends and innovation in ICT (ICEI), Pune, pp 33–39
8. Fatima A, Colomo-Palacios R (2018) Security aspects in healthcare information systems: A systematic mapping. Procedia Comput Sci 138:12–19. ISSN 1877-0509
9. Bradley C, El-Tawab S, Heydari MH (2018) Security analysis of an IoT system used for indoor localization in healthcare facilities. Syst Inf Eng Des Symp (SIEDS), Charlottesville, VA, pp 147–152. https://doi.org/10.1109/SIEDS.2018.8374726
10. Karlof C, Wagner D (2003) Secure routing in wireless sensor networks: attacks and countermeasures. Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, Anchorage, AK, USA 2003:113–127. https://doi.org/10.1109/SNPA.2003.1203362
11. Wallgren L, Raza S, Voigt T (2013) Routing attacks and countermeasures in the RPL-based Internet of Things. Int J Distrib Sens Netw. https://doi.org/10.1155/2013/794326
12. Farzaneh B, Montazeri MA, Jamali S (2019) An anomaly-based IDS for detecting attacks in RPL-based Internet of Things. In: 5th international conference on web research (ICWR), Tehran, Iran, pp 61–66
13. Mayzaud A, Badonnel R, Chrisment I (2017) A distributed monitoring strategy for detecting version number attacks in rpl-based networks. In: IEEE transactions on network and service management, vol 14, no 2, pp 472–486. https://doi.org/10.1109/TNSM.2017.2705290
14. Dvir A, Buttyan L (2011) VeRA-version number and rank authentication in RPL. In: IEEE 8th international conference on mobile adhoc and sensor systems (MASS), pp 709–714, 17 Oct 2011
15. Raza S, Wallgren L, Voigt T (2013) SVELTE: Real-time intrusiondetection in the Internet of Things. Ad Hoc Netw 11(8):2661–2674