International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT22172120

An overview of DoSL Attacks in IoT Networks

N. Nasreena Hameeda
Department of Computer Science, Rabiammal Ahamed Maideen College for Women,Tiruvarur,Tamil Nadu, India

Article Info
Volume 7, Issue 2
Page Number: 596-601

Publication Issue :
March-April-2021

Article History
Accepted : 20 April 2021
Published : 25 April 2021

ABSTRACT

Many methodologies has been discovered to lower the power consumption in the devices, which is connected to the network in recent years. Many medium access control protocols have been used for low power lossy networks (LLNs).The major goal of introducing this methods is to improve the energy efficiency and to increase the fastness of the communication in the network or the data transmission. The Low power lossy networks is used in many real time scenarios nowadays. These methods use battery-powered devices, which makes transmission easier over lossy links. A particular node generally switches off radio interfaces when no traffic is sent. These devices are made to keep the radio interfaces in ON thus it makes exhausting of batteries causing Denial of sleep attacks. Here, we are going to use time division and channel hoping techniques to get a impact on jamming attacks. We will look on the impacts of such attacks by the ideas got through attacker and to which level the protection allows jamming attacks at upper layers.

Keywords : Internet of things (IoT), channel hoping, communication, radio interfaces, attacks.

I. INTRODUCTION

The Internet of Things has grown in massive and matured. The general and traditional sensor that have built-in networks makes communication that stores and process the data. The systems that requires a very accurate monitoring of data and devices and for long time without the human interaction as well as intervention. The size and cost of the systems makes them limited in the computing and memory factors. These systems or the devices also face the radio environment, which receive links of different qualities. Here we are using low power lossy networks to fill this gap. Transmission of data, MAC and routing allows these devices to connect to a station where the received details are collected, stored and processed.

The devices are actually consuming more energy because of radio communication by working at physical and data link (MAC) layers. Radio interfaces can be switched off or can also be decreased that is can be idle to limit the energy consumption without disturbing the actual process. The sensor nodes undergoes a series of operation that is sleep and activity in an alternate manner.The period of cycle can be identified using MAC layer. The aim is to reduce the cycle and to reduce the energy. The nodes are classified on the basis whether they are time-synchronized or not by the MAC layer.

The industrial internet of things (IIOT) networks need to be provided with proper security at every layer. The denial of service attacks is one of the major problem need to be tackled while setting up IOT services.

The denial of sleep attack drains the battery of the device by making the devices to wake up at unwanted times or to do more duty and this eventually increase the duty cycle.

In this paper, we actually take care of solutions which provides security to the devices while data transmission by nature. We specifically investigate the jamming techniques and scenarios where the communicated is prevented by the attackers this again creates increased duty over the devices. We also look at some existing attacks. The time synchronized and channel hopping (TSCH) networks may minimize the collision risks and provides some cryptography techniques to ensure authentication. We explain how denial of sleep attacks are sometimes successful in these networks.

II. RELATED WORKS

The solutions provided by the MAC layer for low power lossy networks may depend upon whether time synchronization between the nodes is a requirement or not. The non-synchronized nodes have to send a prelude to awake the destination node for new transmission. The attackers prevent long sleep of nodes by waking them up soon. The nodes that are time synchronized should wake up in a synchronized manner to send and receive data. Attack on these nodes would cause receiving of data in wrong time slots and may consume more energy.

Here are some kind of attacks that drain the networks. In [1], the three types of DoS attacks were discovered by authors, they are ding-dong ditching, collision attack and the pulse-delay attacks. Despite of low overhead of the solution, authors consider sometimes this kind of attacks may lead to disability in routing and hence the energy is consumed more. The second one is about the study of replay attacks in asynchronous network. The discussion of some anti-replay mechanism is also done in [2].

One of the not synchronized MAC layer solution is based on the wake up radio nodes are designed with two interfaces; one is responsible to wake up the receiver [3]. In [4], the findings of authors describe the antiDoS protocol that use cryptographic primitives to counteract the Denial of sleep attacks. The cryptographic primitives include hash certificates that provide secured authentication and keys exchange. The attacking layer and the intelligence of attackers categorize the type of attack. The denial of sleep attack either transmit unauthenticated packets or disturb the recorded traffic [5]. The waste of energy is due to decoding of unauthenticated data packets. The jamming attacks are the hardest to be protected against the attackers. In [6], traditional security are not enough to prevent this attack.

Some attackers use their knowledge of the implemented protocols or they transmit only when the channel is in busy traffic. The attacker analyses the sleep-activity cycle of the node and control the transmission of packets according to them using S-MAC protocols [7].

III. JAMMING ATTACKS IN TSCH NETWORK

Here we discuss about how much time synchronized channel hopping networks can be immune against the attacks.

A. TSCH networks

The devices in the TSCH networks are more available to different radio links and conditions. They use time division multiple access and slow channel hopping. The communicating nodes frequently changes the radio channel this makes channel hopping efficient against jamming.

The TSCH slot frame is denoted as a matrix. Each cell in a timeslot and a channel offset which is transformed into the radio frequency. As long as the network is running the frames are repeated and cells are assigned to devices. Cells are of two types namely, shared or dedicated. The cells which are allotted for the specific transmitters or receivers are called as dedicated cells while the shared ones are based on the mechanism (i.e., slotted ALOHA) which is used to send and receive frames.This frequency f of a device is calculated in a random manner

$$f = F\,[(chOffset + ASN) \bmod N\ bChannels] \quad (1)$$

Where chOffset denotes the channel offset
N bChannels is the number of physical channels.
The F [ ] function maps an integer with a radio frequency.

B. Jamming TSCH networks

TSCH networks are always assumed, as they are naturally resistant to jamming attacks. This is because of the time division and channel hopping mechanisms. Here we investigate about the fastness of this protocol. We look on jamming attacks performed by an attacker who have the knowledge of the attacking timeslots and channels used there. In Table I the discussed scenarios are given.

TABLE I

TARGET OF SELECTIVE JAMMING ATTACKS, REQUIRED KNOWLEDGE AND POTENTIAL IMPACT

Target	Knowledge	Impact
Shared cells	Used channel and slot length	Jeopardized network formation and maintenance
Dedicated cells	Channel and slot length of users	Jeopardized data communicati on

In this paper, we consider three condition related to the intelligence of the attacker. They are random scenario, time aware scenario and fully aware scenario.

a) The random scenario

The random scenario is about the blind attacker who is jamming over random channels at random timeslots. In this condition, the jamming duration should be selected by the attacker;

b) The time-aware scenario

The time-aware scenario is that the attacker is able to predict the users or the target's timeslot in each slot frame. The radio channel is not known to the attacker but leaving the attacker with a 1 N bChannels probability to select the right one;

c) The fully aware scenario

The fully aware scenario is same as time aware attack but the time aware attacker should also calculated the channel hopping for new slot frames. To compute this, an attacker should know N bChannels during multiple slot frames. This makes prediction of new upcoming slots easier for communication.

IV. PERFORMANCE EVALUATION

The main aim of the paper is to examine the effect of random, time aware and fully aware knowledge of attacker against the jamming attacks in both time division and channel hopping mechanisms (TSCH).

The previous studies related to this network gave importance to the synchronized protocols (in [8], [9]). In this paper, we considered channel-hopping feature of the network, which made medium access protocols (MAC) more secure. The slot frame consists 101 slots in 15 ms of each timeslots. The delivery of packet ratio in the network varies with time based on Pister-Hack model [10].

In this paper, we examined the impact of jamming over dedicated cells. The aim is to clearly observe and evaluate the effects of such attacks in the devices. The figure [1] denotes the upstream reliability among the stimulated nodes observed during their communication. Upstream reliability is the calculated ratio of the number of received packets to the number of packets initiated by the sender

$$\text{Upstream reliability} = \frac{\text{Packets received}}{\text{Packets initiated}}$$

The fig 1 is obtained when there is no attack. The loss here is due to the link qualities and variation in the communication links. The Fig 2 denotes us that there is low probability in affecting the communication reliability by a random attacker. The time aware attack is not that much affecting the communication and this is identified from fig 3 This confirms that the jamming attacks is controlled by the efficiency of the channel hopping.

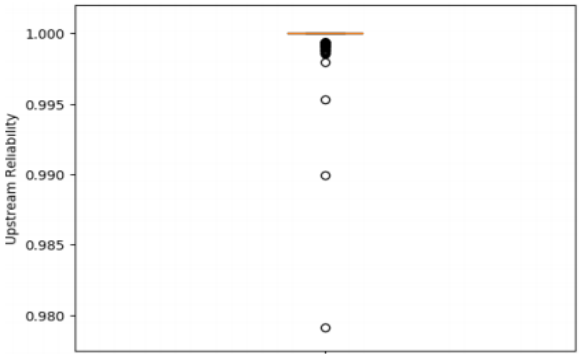

Fig 1. No attacker

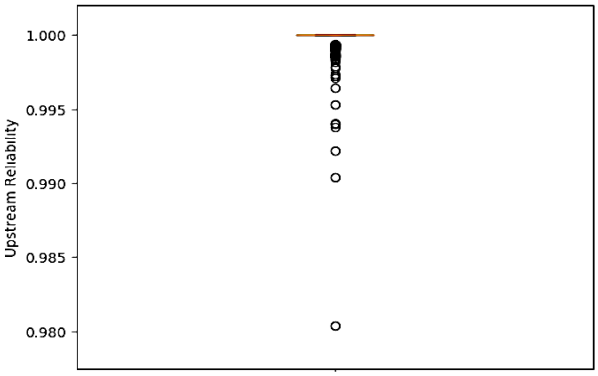

Fig 2. Random attacker

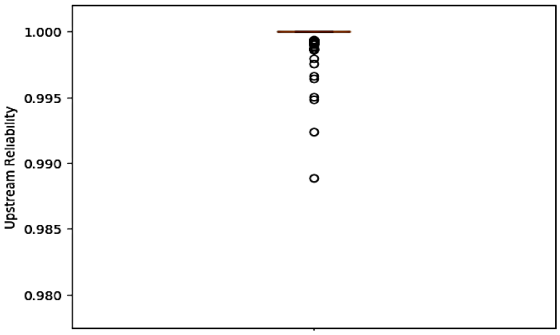

Fig 3. Time aware attacker

Once the attacker gets the full knowledge, the attack will be efficient and significantly affects the reliability communication links. This will make retransmissions from the sender, which is actually costly, and consume more energy. As a result, the communication latency over the link will increase.

V. CONCLUSION

In this paper, we made an overview of types of denial of sleep (DoSL) attacks in both time-synchronized networks and non-synchronized networks in the Internet of things network. We look on previous studies and thus we gave importance to the jammers who attack the synchronized networks either randomly or selectively and their vulnerabilities. They do this so by using their intelligence in others activity that is having a knowledge about the channel and the time slots used by the user. The preceding studies cared about the synchronized links and protocols but in this paper, we focused on the channel-hopping feature of the IoT network. This probably will create a secured network in the medium access layer (MAC). We also predicted the outcome of the attacks in three different condition on a basic example. We also came to conclude that the reliability and latency might reduce the risk of knowing the activity of the user by the attacker.

VI. FUTURE ENHANCEMENT

There is a plan over there to enhance the study by extending it over larger and heavy communication network. In denser topology, the jamming attack by the random attacker will be more efficient. We are also planning to study the detect and mitigate the denial of sleep attacks. Many approaches are available in avoiding the low quality channels and for the detection of the jamming attacks. When it comes to mitigation, some 6tisch standardization activities are proposed [11]. We also having a plan to study the denial of sleep attacks i.e., replay over networks.

VII. REFERENCES

[1]. K. F. Krentz, C. Meinel, and H. Graupner, "Countering Three Denial-of-Sleep Attacks on ContikiMAC," in international Conference on Embedded Wireless Systems and Networks (EWSN), pp. 108–119, 2017.

[2]. V. Manju and M. Sasikumar, "Mitigation of Replay Attack In Wireless Sensor Network," International Journal on Information Technology, vol. 5, 2014

[3]. L. Gu and J. A. Stankovic, "Radio-triggered wake-up for wireless sensor networks," International Journal of Time-Critical Computing Systems (Real-Time Systems), vol. 29, no. 2, pp. 157–182, 2005

[4]. A. T. Capossele, V. Cervo, C. Petrioli, and D. Spenza, "Counteracting DoSL Attacks in Wake-Up-Radio-Based Sensing Systems," in 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), pp. 1–9, June 2016.

[5]. D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midriff, "Effects of DoSL Attacks on Wireless Sensor Network MAC Protocols," IEEE Transactions on Vehicular Technology, vol. 58, pp. 367– 380, Jan 2009

[6]. W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks", 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), (Urbana-Champaign, IL, USA), pp. 46–57, 2005

[7]. P. Thubert and T. Watteyne, "6TiSCH: IPv6 over the TSCH mode of IEEE 802.15.4e." IETF working group.

[8]. O. Dagdeviren, R. Sokullu, and I. Korkmaz, "GTS Attack: An IEEE 802.15.4 MAC Layer Attack in Wireless Sensor Networks," International Journal on Advances in Internet Technology, vol. 2, no. 1, 2009.

[9]. K. F. Krentz and C. Meinel, "Denial-of-sleep defenses for IEEE 802.15.4 coordinated sampled listening (CSL)," Computer Networks, vol. 148, pp. 60 – 71, January 2019

[10]. E. Municio, G. Daneels, M. Vucinic, S. Latre, J. Famaey, Y. Tanaka, K. Brun, K. Muraoka, X. Vilajosana, and T. Watteyne, "Simulating 6TiSCH Networks," Wiley Transactions on Emerging Telecommunications (ETT), 2018.

[11]. M. Tiloca, S. Duquennoy, and G. Dini, "Robust Scheduling against Selective Jamming in 6TiSCH Networks," draft, IETF, December 2018.

[12]. Antoine Gallais, Thin-Hinen Hedli, Valeria Loscrì, Nathalie Mitton. Denial-of-Sleep Attacks against IoT Networks. CoDIT 2019 - 6th International Conference on Control, Decision and Information Technologies, Apr 2019, Paris, France. ffhal-0206060

Cite this article as :

N. Nasreena Hameeda, "An overview of DoSL Attacks in IoT Networks ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 2, pp. 596-601, March-April 2021. Available at
doi : https://doi.org/10.32628/CSEIT22172120
Journal URL : https://ijsrcseit.com/CSEIT22172120