Modeling the Greedy Behavior Attack and Analyzing its Impact on IoT Networks

Fatima Salma Sadek, Khaled Belkadi, Abdelhafid Abouaissa, Samir Ouchani, Mohamed-El-Amine Brahmia, Pascal Lorenz

Available online at www.sciencedirect.com

ScienceDirect

00 (2018) 000–000

Procedia Computer Science

www.elsevier.com/locate/procedia

The Smart Cyber-Physical Systems Symposium (SCPS 2021)
November 1-4, 2021, Leuven, Belgium

Modeling the Greedy Behavior Attack and Analyzing its Impact on IoT Networks

Fatima Salma SADEK[a], Khaled BELKADI[a], Abdelhafid ABOUAISSA[b,*], Samir OUCHANI[c], Mohamed-El-Amine BRAHMIA[c], Pascal LORENZ[b]

[a]*SIMPA laboratory, University of Science and Technology of Oran Mohamed Boudiaf, Oran, Algeria*
[b]*IRIMAS Institute , University of Haute Alsace,Colmar, France*
[c]*LINEACT CESI, CESI Engineering School, France*

Abstract

One of the major security issues in the Internet of Things (IoT) is maintaining the network availability against attacks and traffic congestion. In practice, the greedy behavioral attack is considered as an intelligent Denial of Service (DoS), which aims to compromise the availability of the network by consuming as much as possible the bandwidth of the deployed network. This attack is achieved by tuning the CSMA-CA network communication parameters that plays at the physical layer. In this paper, we propose an efficient modeling technique of attacks proper to the behavior of the greedy node in IoT networks while respecting unslotted IEEE 802.15.4. In fact, our developed greedy nodes algorithm relies on CSMA-CA protocol. This fashioned way of attack representation helped us to easily detect greedy nodes on large-scale IoT networks through simulations. Indeed, the obtained numerical results of different scenarios allow us to validate our approach and showed that the greedy nodes can monopolize the transmission channel during a significant period of time. Various relevant parameters (the number of sent/lost packets, the collision rate, and energy consumption) are considered to analyze and evaluate the impact of selfish nodes on the IoT networks.

Keywords: Security IoT, Detection method, CSMA-CA, Greedy nodes, DoS attack, Simulation.

1. Introduction

IoT is a network of connected intelligent physical devices with the internet to collect, extract, analyze, and share data upon an agreed protocol [1, 2] that are applied on a wide range of applications [3]. Due to constrained devices [4], IoT networks are heavily exposed to many attacks like DoS or jamming that target communication channels [5]. Indeed, this resource restriction allows attackers to saturate the network using overpowered servers. However, a

* Corresponding author. Tel.: +3-33-89-202-371
E-mail address: abdelhafid.baouaissa@uha.fr

deep analysis of DoS attacks is essential for a better understanding of the IoT network availability. One of the most dangerous attacks on IoT networks is the greedy behavior attack which is a particular case of DoS attack. It aims to saturate, partially or totally, the network by depriving legitimate nodes from accessing the transmission channel [6]. Therefore, the greedy node is considered malicious since it monopolizes the channel where only its packets are sent. Thus, legitimate nodes will have difficulty accessing to the transmission channel [7]. This attack causes several malfunctions in the network, and reduces the quality of service (QoS) by generating a significant delay in transmission, and causes very long queues and congestion.

To overcome the above discussed issues, we automatically detect and analyze greedy nodes in IoT networks. First, we identify the important characteristics of greedy nodes, then we propose an efficient modeling mechanism that can be applied on large-scale IoT networks. Therefore, we propose a simulation-based analysis approach that automatically detects greedy nodes. The experimental results showed the difference between a greedy node and the legitimate one, as well as its impact on an IoT network with respect to the degradation of QoS parameters. Therefore, our contribution can serve as a basis for future malicious greedy node detection techniques. Furthermore, the simulation results showed the effectiveness and efficiency of detecting greedy nodes and the saturation of the network which degrades its QoS. The next section surveys the related work. In Section 3, we develop our proposed greedy node modeling technique. Then, the performance analysis results are presented in Section 4. Finally, Section 5 concludes the paper.

2. Related work

In this section, we survey and compare our work with the research initiatives concerning the greedy behavior attack on IoT, and WSN networks based on IEEE 802.15.4(-e).

The author of [8] tackled the greedy behavior attack by using a Markov chain model to demonstrate the degradation of a network throughput performance. They modeled the CSMA-CA protocol as the discrete-time Markov chain. They set the contention window of the greedy node to one and occupy the channel for the first time slots. However, the performance study does not highlight the most relevant simulation parameters such as the energy consumption, the number of sent packets, or the collusion rate.

In [9], the authors proposed a UPPAAL model based on IEEE 802.15.4e standard and star topology. The model is based on two automata, medium and node. They updated the behavior of the greedy node by modifying the length of the initial contention window (CW0) value, the minimum value of BE (minBe), and the maximum value of BE (maxBe). However, the authors did not take into consideration selfish nodes.

In [10], the authors used UPPAAL to model the greedy behavior in WSN based on IEEE 802.15.4 using the unslotted CSMA-CA mode. The greedy node is characterized by the reduction of the backoff performed before accessing the channel, and the increase of the number of attempts to access the channel. In [11], they presented more details and explanations concerning the greedy node algorithm and adding some numerical simulation results. The authors carried out the simulation of both greedy and sane nodes on the TINA platform. Also in [6], the same authors studied the impact of the same greedy node described in [10, 11] on the performance and energy efficiency of the IEEE 802.15.4 network.

3. Greedy node modelling

In this work, we compare the parameters of the legitimate nodes to the greedy one. Also, we propose a greedy node algorithm by modeling the greedy behavior attack in unslotted IEEE 802.15.4 network. To perform analysis, we rely on simulation by attacking a network made up of 10, then 20 legitimate nodes using a single greedy node. First, we analyze eight different parameters of each node in order to highlight the difference between a legitimate and a greedy node, then, we show the impact of this attack on the whole network.

3.1. MAC layer

Besides the management of energy consumption, the MAC layer also manages the following functionalities: acknowledgments, Dedicated Slots, the discovery mechanism neighborhood, beacons, access to the physical channel, GTS (Guaranteed Time Slot), frame validation, node association as well as security which is only available in this

layer in the IEEE 802.15.4 standard and collision detection by using CSMA-CA mechanisms. Our attack aims to saturate the network by modifying the parameters of the CSMA-CA algorithm at the greedy node. The MAC layer can also support two modes: Beacon-enabled and Non Beacon-Enabled. The first uses a superframe in order to synchronize the nodes with the coordinator [12] to access the medium. The second is characterized by the absence of synchronization between the nodes.

3.2. Unslotted CSMA-CA algorithm

Before detailing the unslotted CSMA-CA algorithm, it is essential to describe the parameters used. Backoff Exponent (BE) is a value used in the calculation of the backoff delay. The Clear Channel Assessment (CCA) represents the channel listening period that each node performs before transmission. Then, Number of Backoff (NB) represents a counter of the number of failed channel access attempts. MacMinBE represents the minimum value that BE can take. It varies between 0 and 3 knowing that CSMA-CA uses 3 as default value. MacMaxBE serves as the maximum value that BE can take and it equals to 5 by default. Finally, MacMaxCSMABackoffs is the maximum number of attempts to access the channel. The first step is the initialization of the parameters NB = 0 and BE = MacMinBE = 3. The second step calculates the random backoff to avoid collisions. The algorithm selects a random value between 0 and $2^{BE} - 1$ UnitBackoffPeriod knowing that UnitBackoffPeriod is equal to 20 symbols. While the third step performs a CCA in order to listen to the channel and checks if it is free to transmit or not. The CCA delay = 8 symbols because the time of an RTT (Round-Trip Time or Round-Trip Delay) = 6 symbols. If after a CCA the channel is free, it goes to step five of the algorithm which is transmission, otherwise, it goes to the next step (the fourth). In the fourth step, if the channel is busy, NB and BE are incremented by 1 and step two (2) is repeated (if the channel is busy) until BE= MacMaxBE = 5. If NB = 5 an error message is transmitted to the upper layer and the packet is dropped, otherwise go to step 2, ie recalculate the backoff. At last, in the fifth step, the MAC layer immediately begins the data transfer right after checking the availability of the channel by the CCA procedure, otherwise, collisions may occur if two or more nodes are transmitting at the same time.

3.3. Greedy node modelling in unslotted IEEE 802.15.4

The greedy node algorithm is realized by modifying the values of severalz parameters of CSMA-CA protocol so that the greedy node can monopolize the transmission channel for a certain period of time. Since the IEEE 802.15.4 standard is a probabilistic network, the goal of the greedy node is to increase its chances of accessing the channel. So, to carry out the attack, it is imperative to reduce the CCA time to increase the opportunity to access the channel. Reducing CCA less than RTT increases the probability of collision if the number of nodes accessing the channel at the same time is important.This situation rarely occurs due to the backoff time which is calculated randomly. Thus, by dividing the CCA by 4, the greedy node increases its probability of accessing the medium and prevents other nodes from transmitting their packets. Also, we update the backoff periods (BackoffPeriod BP) which is equal to 20 symbols for a legitimate node. This one will be divided by 4 and will therefore be equal to 5 symbols for a greedy node. The values of MacMinBE, and MacMaxBE have also been modified to 0, and 1 respectively. In this case, BE will vary between 0 and 1. Thus, the maximum waiting time is achieved by the greedy node will be 80 us.

Regarding the attempt to access the channel before the node drops its packet, the greedy node will double it by increasing the value of MacMaxCSMSBackoff which will be equal to 10 instead of 5. Therefore, the algorithm repeats the process of attempt to access the channel 10 times instead of 5. The greedy node workflow algorithm is presented in Figure 1.

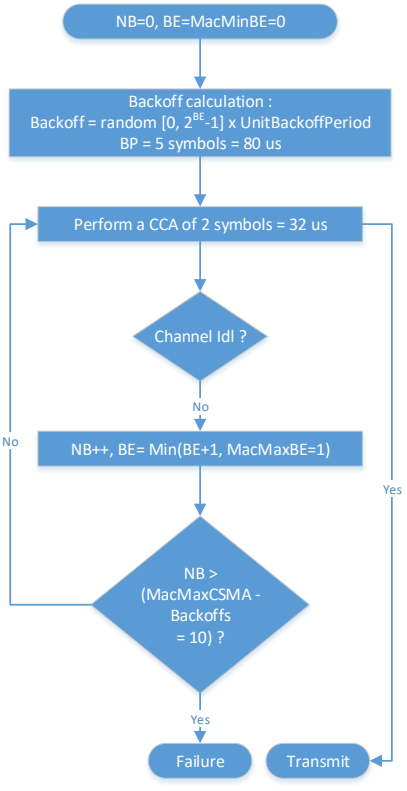


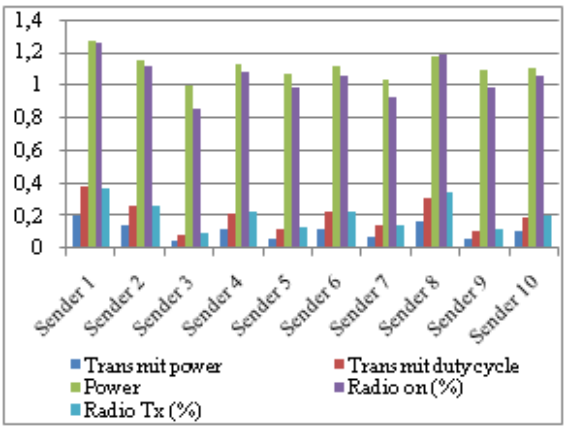
Fig. 1: Greedy node algorithm flowchart

4. Performance analysis

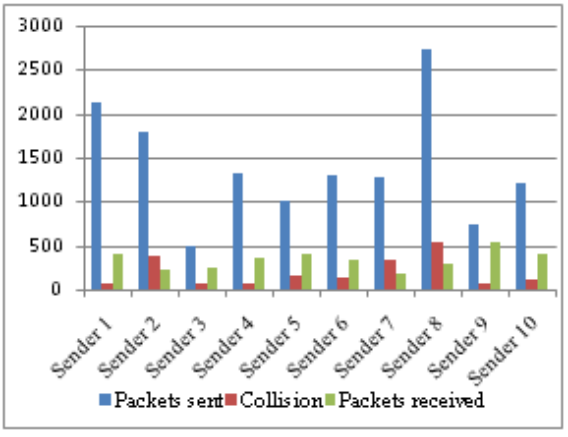
The simulation was done on Contiki OS since it requires fewer resources compared to the existing ones [13, 14]. Concerning the lower layers of Contiki OS, MAC layer in the IoT communication protocol stack, is replaced by the three layers: Framer, RDC (Radio Duty Cycle), and MAC [15]. Particularly, we will be interested to the RDC and MAC layers since the attack's objective is to modify the above-mentioned parameters in these two layers. We used the Cooja simulator into Contiki OS which is flexible and extensible, and all modules can be modified or replaced at any level. According to our observation, the simulated networks reach a certain stability after seven minutes of simulation. It is important to note that all simulated networks have a Peer-to-Peer topology, and that the node position is random. The used wake-up frequency in the ContikiMAC primitive is 8 Hz.

Regarding the used parameters to compare the behavior of greedy nodes with the legitimate ones, we look forward the numbers of sent/received packets, the number of collisions, the transmission power, the transmission duty cycle, the power consumption as well as the radio on rate and radio transmission rate. We have not chose to represent the parameters of the sink node because it does not have the same characteristics as the sender nodes since it is responsible for collecting information.

Our first simulation runs first a legitimate network of 10 sender nodes and one sink node, called network 1. The simulation results are presented below. Figure 2(a) represents the energy consumption of network 1. We notice that the transmission power as well as the power values are almost the same for all nodes. The same observation is for the transmit duty cycle. The radio on parameters is expressed as a percentage. It represents the period when the sensor is on. Radio Tx represents the radio transmission period. This value is also expressed as a percentage. We observe that the energy consumption is uniform between nodes in network 1. Also, we did not noticed any significant difference in the energy consumption parameters between the nodes.



(a) Energy consumption in network 1.



(b) Packets sent/received, and collision in network 1.

Fig. 2: Comparison of energy consumption, sent/received packets and collision in Network 1.

We see in Figure 2(b) that the nodes of network 1 compete to access the channel in particular the sender nodes 1, 2, and 8. Although these nodes transmit a little more than the others, they do not deviate too much from the average of transmitted packets than the other sender nodes. We can therefore say that it is a more or less fair transmission and none of nodes monopolizes the transmission channel in a significant manner. In this scenario called "Network 2", we increase the number of nodes to be 20, then we we compare the efficiency of our greedy node to that of [6].

Figure 3 shows the monopolization of the transmission channel by the greedy node, while the other legitimate nodes in the network send very few packets. The results show a clear monopolization of the transmission channel by the malicious node and that it manages to disrupt the network by denying the medium service. Despite the large number of deployed legitimate nodes in the network, a single greedy node manages to send the most packets preventing others

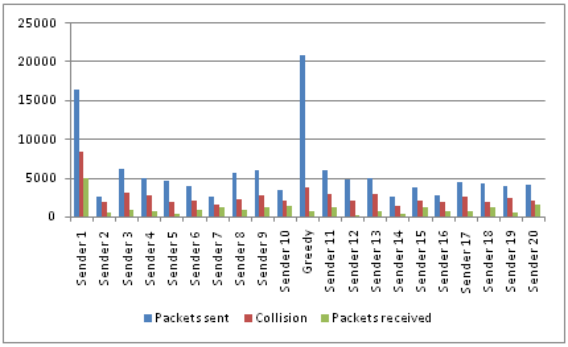


Fig. 3: The sent, received, and collision Packets of network 2 compromised by our efficient greedy node.

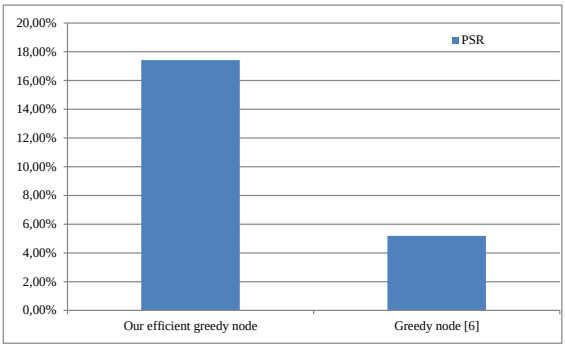


Fig. 4: Packets sent rate.

from correctly sending their packets. To highlight our greedy node modeling, we compare our model with the one presented in [6]. Figure 4 represents the rate of the sent packets by our greedy node and that of [6], in network 2.

Figure 4 shows a significant difference in the rate of the sent packets between two nodes, where our efficient node sends almost four times more packets than the greedy node in [6]. We observe that the rate of packets sent by the greedy node is significant, as the greedy node occupies the channel, the less the legitimate nodes are able to send their packets, resulting in packet loss in the network. This happens because legitimate nodes have only 5 attempts to access the channel before dropping their packets. Thus, if the channel is found busy at every CCA run, the legitimate node ends up dropping its packets. From the results of our study, we conclude that a node is suspected of being greedy if it transmits a very large number of packets compared to the other nodes of the network, consumes more energy. And, also if its transmission and "radio on" rates are high, as well as the transmission duty cycle and transmission power, and if its receive fewer packets.

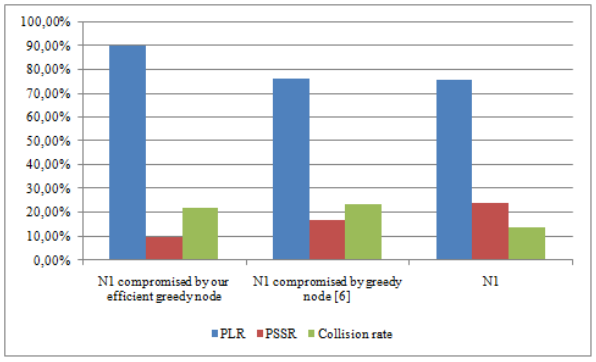
We analyze in the following the impact of our attack on the entire network using three metrics namely: Packets Lost Rate (PLR), Packets Sent Successfully Rate (PSSR), and collision rate. We evaluate and compare the quality of service in the three network scenarios: the first is a safe network named N1, then the second and the third compromise N1 by our greedy node and the presented one in [6], respectively. The results are summarized in Figure 5.

We see in Figure 5(a) that the presence of a greedy node causes an increase in the number of collisions and lost of packets. In addition, it reduces the number of successfully sent packets in the whole network. Further, we have demonstrated that our greedy node algorithm is more efficient than that one proposed in [6] in terms of degradation of the quality of service of the network, since the collision rate and lost packets rate are higher, and the rate of successfully sent packets rate is lower. Furthermore, we observe almost the same rate of packets lost in the normal state network N1 and the network containing the greedy node [6].

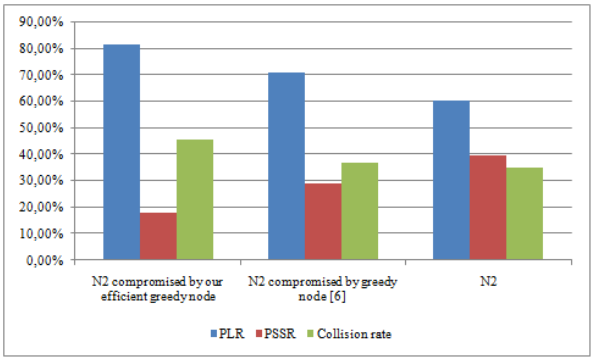
We see in Figure 5(b) that the collision rate in the network N2 that is compromised by the greedy node of [6] is almost the same as that of the network N2 in the normal state. Despite the increasing number of legitimate nodes from 10 to 20, our greedy node retains its efficiency by significantly degrading QoS, causing a significant number of collisions and of packets lost. According to the comparative study carried out in this section, we have demonstrated the efficiency of our attack algorithm despite the increase in the number of legitimate nodes, and that our algorithm is more efficient than the proposed one in [6].

5. Conclusion

The nature of connected objects with respect to their different resource constraints make them vulnerable to cyber attacks. The greedy behavioral attack is considered as a smart DoS attack that aims to monopolize the transmission medium by a malicious node. We presented an efficient greedy node algorithm and demonstrated that a single greedy node can disrupt a whole IoT network. We also highlighted the difference between a greedy node and a legitimate node using different parameters. In addition, we conducted a comparative study between simulated IoT networks in three different scenarios: normal, compromised by an existing greedy node and when deploying our greedy node. We



(a) Network N1.



(b) Network N2.

Fig. 5: Comparison of QoS parameters of sane and compromised network by our efficient greedy node and the greedy node of [6].

have shown that the greedy behavior attack aims to disrupt the entire IoT network by causing a high collision rate that generates a large number of lost packets, and consequently a denial of service by depriving legitimate nodes from accessing the IoT network. The perspective of this work is to exploit the numerical results presented in this paper to perform anomaly detection of greedy behavioral attacks. Also, it is interesting to identify greedy nodes in order to neutralize and isolate them.

References

[1] Ammar Rayes and Samer Salam. Internet of things from hype to reality. *Springer*, 2017.

[2] Shanzhi Chen, Hui Xu, Dake Liu, Bo Hu, and Hucheng Wang. A vision of iot: Applications, challenges, and opportunities with china perspective. *IEEE Internet of Things Journal*, 1(4):349–359, 2014.

[3] Khaoula Zaimen, Mohamed El Amine Brahmia, Jean-François Dollinger, Laurent Moalic, Abdelhafid Abouaissa, and Lhassane Idoumghar. A Overview on WSN Deployment and a Novel Conceptual BIM-based Approach in Smart Buildings. In *2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, pages 1–6. IEEE, 2020.

[4] Walid Miloud Dahmane, Mohamed El Amine Brahmia, Jean-François Dollinger, Samir Ouchani, et al. A bim-based framework for an optimal wsn deployment in smart building. In *2020 11th International Conference on Network of the Future (NoF)*, pages 110–114. IEEE, 2020.

[5] Rodrigo Roman, Jianying Zhou, and Javier Lopez. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10):2266–2279, 2013.

[6] Abdelkrim Abdelli, Lynda Mokdad, Jalel Ben Othman, and Youcef Hammal. Dealing with a non green behaviour in wsn. *Simulation Modelling Practice and Theory*, 84:124–142, 2018.

[7] Soufiene Djahel, Farid Naït-abdesselam, and Damla Turgut. Characterizing the greedy behavior in wireless ad hoc networks. *Security and Communication Networks*, 4(3):284–298, 2011.

[8] Joongheon Kim and Kyeong Seon Kim. Detecting selfish backoff attack in ieee 802.15. 4 csma/ca using logistic classification. In *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, pages 26–27. IEEE, 2018.

[9] Yassine Boufenneche, Nawel Gharbi, Rafik Zitouni, and Laurent George. Formal modeling of greedy behavior in secure internet of things networks. In *2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN)*, pages 188–193. IEEE, 2019.

[10] Youcef Hammal, Jalel Ben-Othman, Lynda Mokdad, and Abdelkrim Abdelli. Formal modeling of greedy nodes in 802.15. 4 wsn. *ICT Express*, 1(1):10–13, 2015.

[11] Lynda Mokdad, Abdelkrim Abdelli, and Jalel Ben-Othman. Detection of greedy behavior in wsn using ieee 802.15 protocol. In *2014 IEEE 22nd International Symposium on Modelling, Analysis & Simulation of Computer and Telecommunication Systems*, pages 106–111. IEEE, 2014.

[12] Michele Zorzi, Alexander Gluhak, Sebastian Lange, and Alessandro Bassi. From today's intranet of things to a future internet of things: a wireless-and mobility-related view. *IEEE Wireless communications*, 17(6):44–51, 2010.

[13] Christopher Pinola. Evaluating the Performance of Synchronous and Asynchronous Media Access Control Protocols in the Contiki Operating System. Technical report, Worcester Polytechnic Institute, 2013.

[14] JF. Dollinger A. Abouaissa L. Idoumghar A. Syarif, M.A. Brahmia. RPL-OC: Extension of RPL Protocol for LLN Networks based on the Operator Calculus Approach. *Sixth International Congress on Information and Communication Technology, ICICT, 25-26 Feb, London, UK*, 4, 2021.

[15] Adam Dunkels. The contikimac radio duty cycling protocol. Technical report, Swedish Institute of Computer Science Publications Database, SICS, ISSN 1100-3154, 2011.