Detecting Selfish Backoff Attack in IEEE 802.15.4 CSMA/CA using Logistic Classification

Joongheon Kim and Kyeong Seon Kim
Chung-Ang University, Seoul, Korea
joongheon@cau.ac.kr

***Abstract*—This paper discussed about the detection of random access attack in IEEE 802.15.4 wireless networks. In IEEE 802.15.4, the medium access control mechanism is designed based on carrier sensing multiple access with collision avoidance (CSMA/CA) with exponential backoff. When an IEEE 802.15.4 device has very small backoff, it takes higher priority to get the channel compared to the other conventional IEEE 802.15.4 devices. This obviously degrades the network throughput performance of normal IEEE 802.15.4 devices. This paper presents the analysis of the impacts and proposes the method for detecting the malicious selfish backoff attacker via logistic classification.**

I. Introduction

In carrier sensing multiple access with collision avoidance (CSMA/CS)-based wireless networks, security over wireless medium access is one of the active research topics nowadays. Furthermore, this paper is focusing on IEEE 802.15.4 low-power wireless personal area networks (LR-WPAN) which is definitely beneficial in terms of power/energy management and thus it is good to be used for Internet of Things (IoT) applications and wearable computing systems. In CSMA/CA, when multiple devices content the channel at the same time, they will move to backoff stage where the backoff timer will be randomly selected within the given backoff interval based on exponential backoff mechanisms.

Suppose that a malicious/selfish device sets its own backoff timer to be very small (named to *selfish backoff*). This means the selfish device can access the channel faster than the others since the selfish device can take the channel with higher priority. This will eventually lead to the performance degradation in the entire network. This is called *selfish backoff attack* in this paper.

This paper presents the results of mathematical throughput analysis in CSMA/CA with exponential random backoff (details are in [1]); and also proposes a method to detect malicious/selfish attackers via logistic classification. In addition, this paper is doing mathematical analysis for the selfish backoff attack; and simulates the impacts on the performance in the wireless networks.

As one promising application, micro-grid user communications with IEEE 802.15.4-based low-power IoT networking capabilities are of our interests. In micro-grid systems, users are exchanging their information via wireline or wireless technologies. For this purpose, secure communications and networking are definitely required.

II. Bianchi's IEEE 802.15.4 CSMA/CA [1]

The details of CSMA/CA mathematical analysis are briefly introduced in [1]. This paper introduces the basic concept of the analysis and presents the analysis result. As presented in [1], CSMA/CA can be represented as the discrete-time Markov chain.

Then, the probability that a node transmits in a randomly chosen time (τ) can be eventually calculated. Notice that τ_{erb} is the probability that a node transmits in a randomly chosen time with exponential random backoff. Regardless of the backoff stage, any transmission occurs when the backoff counter is 0. Then, τ_{erb} can be computed as follows:

$$\tau_{\text{erb}}(p) = \frac{2}{(W+1) + pW\left(\sum_{i=0}^{m-1}(2p)^i\right)}. \quad (1)$$

where p and W stand for packet collision probability ($p \in (0,1)$ [1]) and $CW_{\min}$ (i.e., minimum contention window size), respectively.

Notice that more details about this result are well-discussed in [1]; and the analysis in this paper is based on the theory.

III. Selfish Backoff Attack

A. An Overview of Selfish Backoff Attack

Among all devices with IEEE 802.15.4 CSMA/CA, when one is using selfish backoff strategies, it can be harmful for the other networked devices. Suppose that a selfish device (i.e., attacker) is setting its $CW_{\min}$ and $CW_{\max}$ to 1. Then, when the attacker contents the channel with the other devices, it always wins the game because it can occupy the channel at the first time slot while the other devices are waiting to carrier-sense the channel. Then, the attack will always grab the channel that can lead to throughput degradation of all the other networked devices.

B. Mathematical Analysis

In the backoff mechanism with a deterministic contention window size (a.k.a., selfish backoff), it is true that

$$W_i = C_w \quad (2)$$

where $CW_{\min} = CW_{\max} = C_w$. Then, $\tau_{\text{sb}}(p)$ can be defined as the probability that a node transmits in a randomly chosen slot time with selfish backoff depending on collision probability p. Regardless of the backoff stage, any transmission occurs

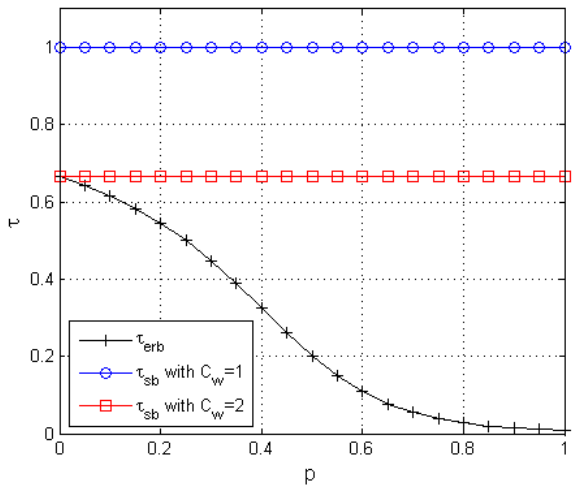

Fig. 1. Simulation results

when the backoff time counter is equal to 0, i.e.,

$$\tau_{\text{sb}}(p) = \frac{2}{C_w + 1}. \tag{3}$$

which can be derived by [1].

C. Logistic Classification

As presented in Fig. 1, we can observe explicit classification between normal CSMA/CA behavior and selfish access control. Therefore, we can design classification based on this result.

IV. Simulation Results

The corresponding simulations are for observing the impacts of selfish backoff attack with various C_w settings. According to the IEEE 802.15.4 [2], BE is 3, i.e., maximum backoff stage is 7 due to $m = 2^{\text{BE}} - 1 = 7$. In addition, C_w in (2) is 2 [2]. For the selfish backoff attack parameter setting, two possible scenarios are considered where $C_w = 1$ and $C_w = 2$.

When $C_w = 1$, the attacker will access the channel immediately without any backoff waiting, in turn, nearby IEEE 802.15.4 devices cannot have chances to access the channel. In Fig. 1, these three backoff strategies are considered. AS shown Fig. 1, the selfish backoff attacks with various C_w are all independent to the packet collision probability p. In addition, the selfish backoff attack with $C_w = 1$ can throughput with 1 because it can access the channel immediately.

When $C_w = 2$, the other nearby neighbor networked devices can access the channel at the first slot time (i.e., the case that the device selects the first slot with uniform random selection within the given time interval), i.e., then the throughput is less than 1 as also presented in Fig. 1.

V. Concluding Remarks and Future Work

This paper briefly introduces the analysis of IEEE 802.15.4 CSMA/CA channel access with exponential random backoff (initially well-discussed in [1]). In IEEE 802.15.4 channel access, when a selfish device accesses the wireless channel faster than the other devices, its throughput increases whereas the performance of the other devices degrades. Therefore, we mathematically analyzes the performance of the selfish backoff mechanism and the throughput degradation of the other devices. As shown in simulation results, the impacts of selfish backoff are observed. In addition, detection algorithms for classifying malicious attackers via logistic classification is proposed.

As a future research direction, we have a plan to numerically estimate the impacts of selfish backoff attacks in micro-grid networks.

Acknowledgement

This research was supported by Korea Electric Power Corporation (KEPCO) Research Institute (R17XA05-41), 2018; and also supported by National Research Foundation of Korea (NRF Korea) under Grant 2016R1C1B1015406. Joongheon Kim is a corresponding author of this paper (email: joongheon@cau.ac.kr).

References

[1] G. Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 3, pp. 535 547, March 2000.

[2] J.A. Gutierrez, M. Naeve, E. Callaway, M. Bourgeois, V. Mitter, and B. Heile, "IEEE 802.15.4: A Developing Standard for Low-Power Low-Cost Wireless Personal Area Networks," *IEEE Network*, vol. 15, no. 5, pp. 12 - 19, May 2001.