Attack Probability Analysis on the MTD System

Jang-Geun Ki(✉) and Kee-Young Kwon

Division of Electrical and Electronic and Control Engineering,
Kongju National University, Cheonan 31080, South Korea
{kjg, kky}@kongju.ac.kr

Abstract. Interests in wireless communication technologies have increased in these days, along with rapid prevalence of wireless terminals. Wireless communications have the disadvantage of being vulnerable to security by allowing anyone to receive radio signals by broadcasting wireless signals. There have been lots of researches on MTD (Moving Target Defense) techniques that constantly change the system's vulnerable surfaces over time to protect the wireless communications system from malicious attackers. In this paper, attack analyses have been conducted to improve the security of the wireless communication systems in which the MTD technologies are applied.

Keywords: Moving Target Defense · Attack vulnerability

1 Introduction

Wireless networks have been widely deployed recently because of ease installation, low cost and high bandwidth. However, due to the nature of the wireless signal transmission, wireless communication systems are inherently vulnerable to security breaches, primarily because of easy access to data signal by the unauthorized attackers.

Many studies have been co ducted to improve the wireless security technologies considerably, but attacks such as sniffing, DOS(Denial Of Service), session hijacking, and jamming, etc., also have increased. Therefore, efficient security measures are needed.

In order to prevent the malicious attacks, much attention has been focused on the MTD (Moving Target Defense) [1–4] technology, which is constantly changing the system's vulnerable surfaces that can be attacked in a variety of ways. Communication systems with the MTD mechanism will reduce system vulnerability due to continual changes in the function of the weak points in the system, thereby increasing the cost of attack and decreasing the aggressiveness of attackers, thereby ultimately increasing the self-defense and resilience of the system. These MTD techniques can be applied to all layers ranging from the physical layer of the communication system to the application layer, and the security can be stronger when the MTD technology applies to multiple layers at the same time.

In this paper, attack success probabilities in case of scanning attack and jamming attack have been mathematically analyzed in the MTD-based wireless communication system.

S. O. Hwang et al. (Eds.): ICGHIT 2018, LNEE 502, pp. 10–13, 2019.
https://doi.org/10.1007/978-981-13-0311-1_2

2 MTD System and Attack Modeling

In order to evaluate the attack success probability on the MTD-based communication system [3], assumptions are as follows:

- There are total N channels in the communication system.
- The sender changes the transmission channel at every T time or at the next time slot right after detecting the attack success.
- Attack occurs at every unit time slot and attacker chooses an attacked channel randomly.
- Once the attack succeeds, the success will continue until the transmission channel of the sender changes.

Figure 1 shows an example of the operation of data transmission channel and attack channel when the sender changes the transmission channel at every T time period during scan attack or at the next time slot right after detecting the attack success during jamming attack.

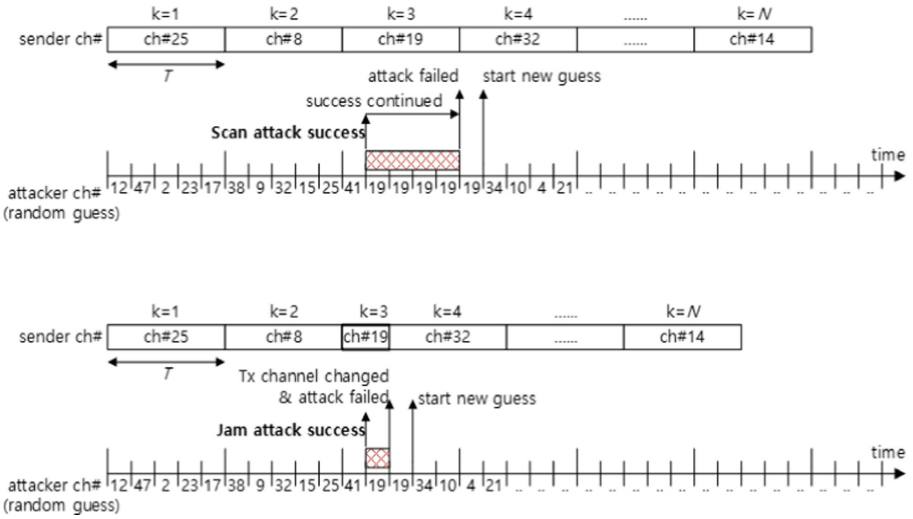

Fig. 1. Example of data channel and attack channel.

3 Attack Success Probability

Depending on the attackers' attack methods, the data sender and receiver may be able to detect whether the attack is successful or not. As an example, scanning or monitoring attack is very difficult to detect while jamming attack can be detected easily. Detecting the attack can affect the sender's decision to change the transmission channel and result in the different attack success probability. Therefore, we consider two kinds of attacks, scanning and jamming attacks. At each time slot, the attack is considered as a success if

the data transmission channel of the sender and the selected attack channel of the attacker are the same. The attack success probability is defined as the portion of the attack success slots compared to the total communication slots.

3.1 Scanning Attack Success Probability

Success probability of scanning attack is defined as the ratio of the coincidence between the sender's channel and the attacker's channel when the sender transmits data using the randomly selected channel at every determined interval. Scanning attack success probability is calculated in the following expression.

$$P_{scan} = \frac{\sum_{i=1}^{T} \left(\frac{N-1}{N}\right)^{i-1} \left(\frac{1}{N}\right)(T-i+1)}{T} \tag{1}$$

3.2 Jamming Attack Success Probability

Success probability of jamming attack is defined as the same way as the scanning attack success probability except that the sender can change its channel right after the attack success as well as at every determined interval. In this case, attacker should newly guess the sender's channel at every time slot because the sender will change its channel right after the attack success.

Jamming attack success probability can be easily obtained as shown below.

$$P_{jam} = \frac{1}{T} \tag{2}$$

3.3 Results

Figure 2 shows the attack success probability of the random scanning attack and the random jamming attack according to the change of the T time.

As shown in the figure, in the case of random scanning attack, the bigger T values result in the increase of attack success probability. On the other hand, in the random jamming attack case, the change of the T value does not affect the attack success probability.

In both attack cases, the higher the N value, the smaller the attack success probability.

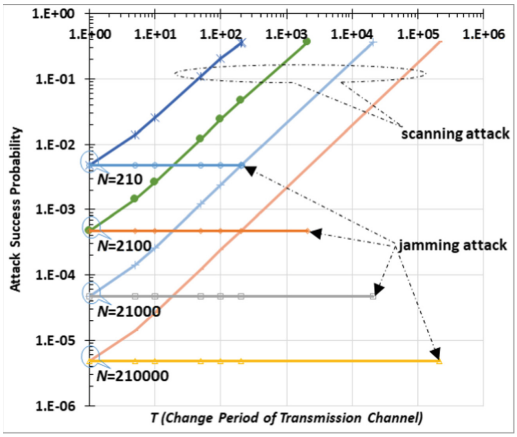

Fig. 2. Random scanning/jamming attack success probability.

4 Conclusion

With the increase of mobile terminals, wireless technologies have been developed rapidly. In order to develop a resilient wireless communication system, a MTD-based approach changes the radio parameters dynamically so that the vulnerability of the system can be protected from the malicious attack.

In this paper, random scanning and jamming attack success probabilities have been analyzed to improve the security of the wireless communication systems in which the MTD technologies are applied.

In the scanning attack, the bigger the T value (period of changing the sender's channel), the higher the attack success probability. On the other hand, in the jamming attack, the change of the T value does not affect the attack success probability. In both attack cases, the higher the N value (total number of channels to be used by the sender), the smaller the attack success probability.

References

1. Casola, V., Benedictis, A.D., Albanese, M.: A moving target defense approach for protecting resource-constrained distributed devices. In: IEEE 14th International Conference on Information Reuse and Integration (IRI), pp. 22–29. IEEE, San Francisco (2013)
2. Kampanakis, P., Perros, H., Beyene, T.: SDN-based solutions for moving target defense network protection. In: IEEE 15th International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM). IEEE, Sydney (2014)
3. Ki, J.G.: Performance analysis of SDR communication system based on MTD technology. J. Inst. Internet Broadcast. Commun. (JIIBC) **17**(2), 51–56 (2017)
4. Jajodia, S., Ghosh, A.K., Subrahmanian, V.S., Swarup, V., Wang, C., Wang, X.S.: Moving Target Defense II: Application of Game Theory and Adversarial Modeling. Springer, New York (2013). ISBN 978-1-4614-5416-8