ISSN 2959-6157

Security Evaluation of I/Q Offset and CFO Physical Layer Fingerprint identification model in Bluetooth Communication under Attacker Simulation

Fengting Fei[1+], Zhuohang Lai[2+], Changhe Li[3+], Jiayue He[4*+]

[1]Ulink College of Shanghai, Shanghai, China, fengting_fei@outlook.com
[2]Quanzhou NO.5 middle school, Quanzhou,China, laizhuohang123@iCloud.com
[3]School of Computer Science and Engineering, Xi'an University of Technology, Xi'an, China, 2158387087@qq .com
[4]Suzhou Foreign Language School, Suzhou, China, linda_jiayue_he@ 163.com
+*These authors contributed equally to this work and should be considered co-first authors.*

Abstract:

In this paper, by considering the presence of attackers, a model is established to demonstrate the process of identifying the target device by the receiver through physical fingerprinting in Bluetooth communication. Based on this model, the security and robustness of the physical layer device identification techniques using I/Q offset, as well as the combination of I/Q offset and CFO, will be evaluated. This paper will help users recognize the potential impact of attackers on the security of Bluetooth communication and understand how to enhance the security and accuracy of device identification.

Keywords: Bluetooth Communication, Physical Layer Fingerprint, Identification, Attack.

1. INTRODUCTION

Bluetooth is a low cost, low power, radio frequency technology for short-range communications. This technology allows mobile phones, computers and other devices to make wireless connections with other Bluetooth accessories. Because of the increasing number of the Bluetooth users, the security issues associated with Bluetooth are gradually exposed and aroused people's attention. For example, in [1], the author discussed the security mechanism of Bluetooth, such as encryption and key management, and discusses the vulnerabilities of these encryption schemes, indicating that more advanced security protocols are needed in the future to make Bluetooth technology secure even when applied in large-scale scenarios. It is too broad to discuss the security of Bluetooth communication, but it is a good point to analyze whether the device can be accurately identified. Because in Bluetooth communication, the target device must be accurately identified and connected and the access request from the unauthorized devices should be blocked. In addition, it may be too abstract to evaluate the security of the identification process, so the model is built and the data obtained from the model can help us quantify the impact of attacker in the identification process, so the security and robustness of the entire process can be evaluated. Later, since the original model, CFO is also used as a physical fingerprint for device identification. The mean and standard deviation of the success rate difference between the target transmitter and the attacker is calculated to quantify the impact of this operation on the overall security.

2. BACKGROUND

2.1 Security issues in Bluetooth transmission

During the usage of Bluetooth, Bluetooth transmission can be deliberately jammed or block, which may lead to a number of safety hazard like data leakage, privacy invasion, identity impersonation etc. Security threats in Bluetooth can be branched into three major categories: The first one is disclosure threat. Under this threat, the information can leak from the target device to an unauthorized attacker. The second is integrity threat, which can compromise the integrity of the data by altering the information, so that the users of the system can be misled. The third one is Denial of Service (DoS) threat. The attacker would make the service unavailable or severely limit the service's availability to an authorized users to block the users from connecting the service [2]. In our study, we will focus on the spoofing attack, which is a kind of integrity threat as in spoofing attacks, attackers can impersonate legitimate devices to send false data, which undermines the integrity of the data.

2.2 Physical-layer identification

In wireless communication, physical fingerprint recognition technology is now widely used. There are many ways to identify devices, such as MAC address recognition or IP address recognition, but both of these methods have some limitations as both of these address can be identified or tampered easily. In contrast, the physical fingerprint is a unique character of the device, it comes from the differences of various hardware in the communication process, which is inevitable and cannot be changed. Therefore, using physical fingerprints to identify devices can improve the security and stability of the process.

But, as [3] mentioned, the attacker realizes this and bypasses the MAC address imitation step, instead using this unique physical-layer fingerprints which is introduced by hardware imperfections in mobile devices.

2.3 Description of I/Q offset and CFO

In the model that was built below, I/Q offset and CFO are the two physical fingerprints used to identify devices, so it is necessary to introduce what they are at first. DC offset is one of the causes of I/Q offset, which can be caused by many factors, like the asymmetry of the circuit or temperature changes. To think it more intuitively, just image a sine wave signal, its waveform is symmetric about the center line, which is 0. However, if there is a DC offset, the whole waveform will shift up or down and the distance it moves is the DC offset. The I/Q offset is the DC offset that exists in the I and Q components.

For the CFO(Carrier Frequency Offset), it is the mismatch between the frequency of the received signal and the frequency of the local oscillator at the receiver. The CFO may not change as often as the I/Q offset because it is due to the frequency offset of the local oscillator, and the aging of the hardware may cause it to change, but it is a slow process.

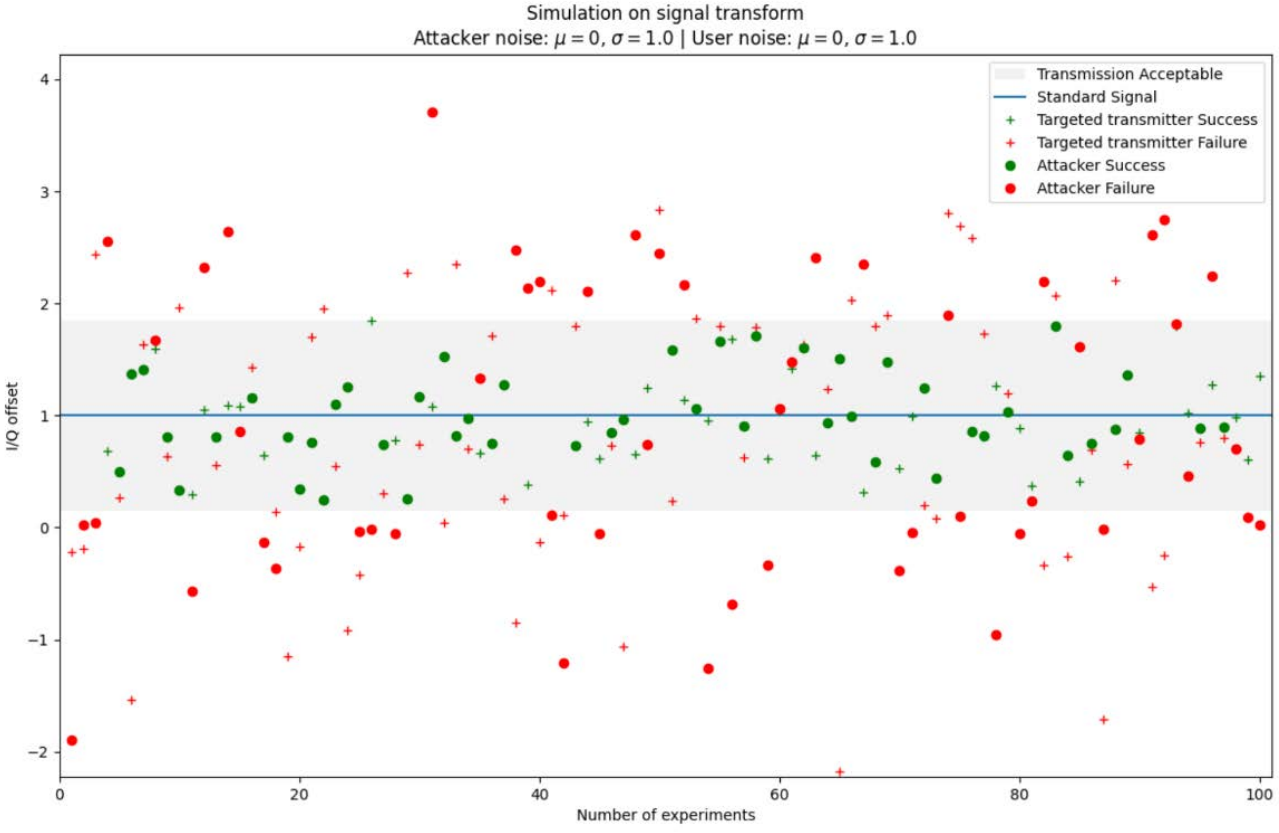

Figure 1. The identification of I/Q offset from transmitter and attacker's signals.

3. THREAT MODEL

In reality, the identification of the physical-layer fingerprinting of a Bluetooth signal can be influenced by many factors like Signal Noise and temperature, on the grounds that these factors are able to shift the fingerprinting from its original value. Therefore, receivers need to set a threshold of the physical-layer fingerprinting to determine whether a signal is from the target transmitter. Specifically, if the values of the fingerprinting of a signal are all within the threshold set, the signal can be considered as being sent by the target transmitter.

3.1 I/Q offset physical-layer identification and attack

3.1.1 Settings of the I/Q identification model

In our model, we consider that there is spoofing attack in our Bluetooth communication system. The attacker makes the physical-layer fingerprinting of his signal be as like that of transmitter's signal as possible, leading to the possibility that the physical-layer fingerprinting is within the threshold, so that the attacker can pretend to be the transmitter. This attack mode is also specified in [4]. As shown in Figure 1, the first physical-layer fingerprinting that we studied was In-phase/Quadrature offset (I/Q offset). A threshold is set around the standard I/Q offset of the transmitter. A certain number of experiments are carried out, and there are two signals received in each experiment, one is from the attacker and one is from the transmitter. Taking into the account the effect of noise, the I/Q offsets of the transmitter signals received by the receiver are equal to the standard value of I/Q offset plus the random noise which is in Gaussian distribution. Since the attacker does not know the exact value of the I/Q offset of the target transmitter signal, he would set the I/Q offset of his signal randomly around the standard I/Q offset value. In addition, due to the influence of the random noise in Gaussian distribution, the I/Q offset fingerprinting of the attacker's signal will be further affected and fluctuates.

3.1.2 I/Q offset identification process of the receiver

The signal which has the I/Q offset, firstly, is within the threshold and, secondly, is closer to the standard I/Q offset compared with the other signal in the same experiment can be recognized as the signal from the transmitter. However, in this identification process, it is possible that the I/Q offset. from the attacker's signal is closer to the standard I/Q offset than that from the transmitter's in the threshold. This would be considered a successful spoofing attack for the attacker as the receiver would recognize the signal with closer I/Q offset to the standard one as the signal from the transmitter. In our security evaluation process, we will use the variance of the random noise to present the noise interference resistance of signals from the transmitter and the receiver. We will alter the noise variance to explore the success rate of the attacker under different noise interference resistances of the attacker and receiver, the two variance are our variables.

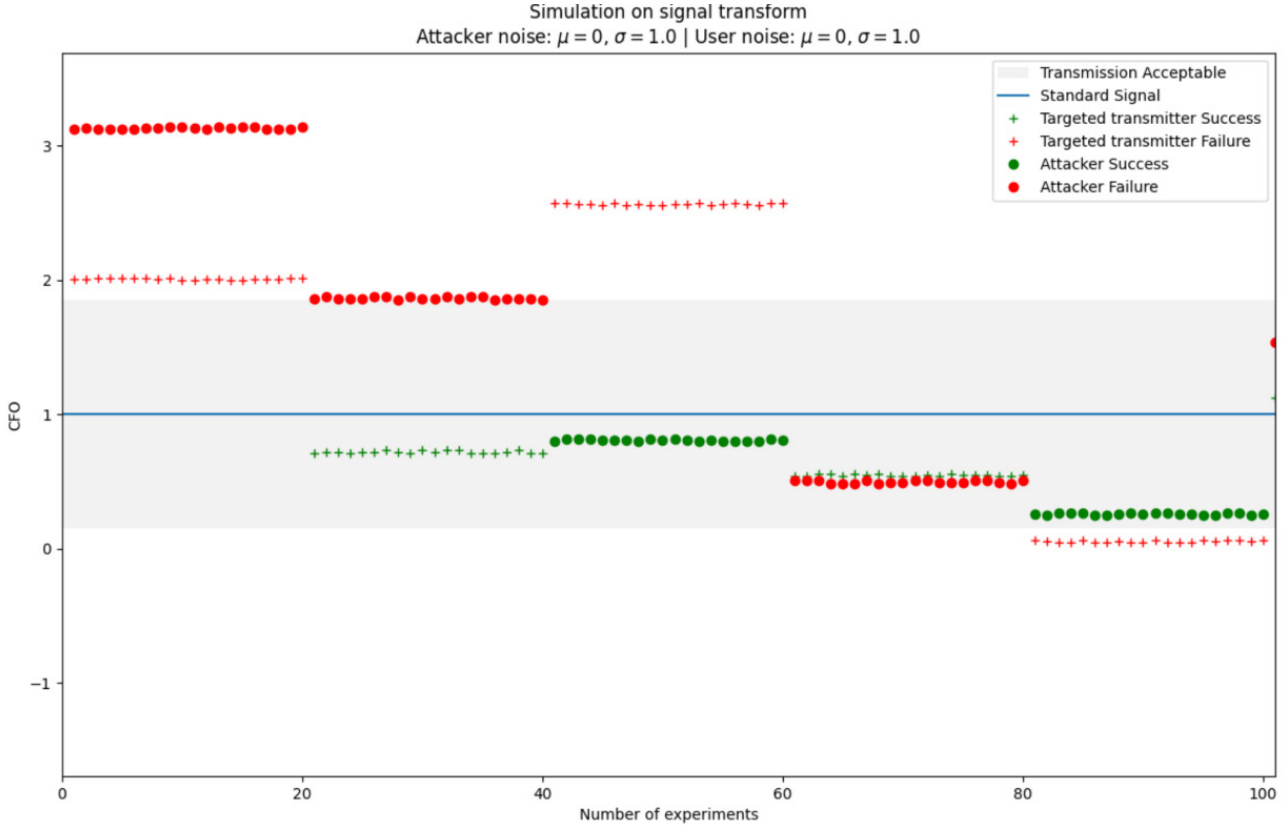

Figure 2. The identification of CFO from transmitter and attacker's signals.

3.2 CFO physical-layer identification and attack

3.2.1 Settings of the CFO identification model

The other physical-layer fingerprinting that we used in identification in Bluetooth system was CFO. As shown in Figure 2, this CFO identification model is quite similar to the I/Q offset identification model in Figure 1. A certain number of experiments are carried out as well, and there is also a threshold for the receiver to identify where signals are from. In each of the experiment, there are two signals from both the transmitter and the attacker. Due to the attacker's uncertainty of the exact standard CFO value, he will set his CFO value of his signal randomly. The values of the CFO of the transmitter signals and the attacker signals received are all set as their original CFO values plus the random change in Gaussian distribution. The receiver would have a comparison about how close is the signals' CFO to the standard CFO, which is the original CFO of the transmitter signal, between the receiver signals and the transmitter signals received to choose signals of trust. However, the difference is that the CFO of a signal would be changed very slowly, and in a short time, it can be considered unchanged, so we set the CFO of the signals from the attacker and the transmitter to be roughly constant over a certain number of experiments.

3.2.2 CFO identification process of the receiver

The receiver would also choose the signals with closer CFO to the standard value of CFO as a signal of trust. If the CFO of the attacker's signal is more like the CFO of the standard signal than that of the transmitter's, the attacker is successful in the attack. In this simulation, the variances of the noise for the receiver and the transmitter will also be altered, and we will explore how the attacker's success rate changes with the change of the variance.

4. RESULTS AND DISCUSSION

Based on the model and the experiment method introduced above, the variables for our experiment are the variances of the factors that cause I/Q offset and CFO change. For the I/Q offset, the factor is the noise that satisfies Gaussian distribution. For the CFO, it is the aging of hardware.

The I/Q offset of both the targeted transmitter and the attacker varies from 0.1 to 1, and there are 100 sets if each set is considered: for example, when the variance of noise that affected the targeted transmitter is 0.1, that of the attacker can be 0.1, 0.2, 0.3, 0.4…1.

For the two situations (before and after the combination of CFO to identify devices), the difference between the targeted transmitter success rate and the attacker success rate will be calculated respectively.

Diff_SucessRate_Before = Target_SucessRate_Before – Attacker_SucessRate_ Before

Diff_SucessRate_After = Target_SucessRate_After – Attacer_SucessRate_ After

And then the mean of these differences will be measures, this number is used to evaluate the safety of the identification process.

$$Mean = \frac{1}{N}\sum_{i=1}^{N}(Difference)$$

Finally, the standard deviation of the success rate difference is calculated to examine the stability of the entire system.

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(Difference - Mean)^2}$$

4.1 Results

Before the combination of CFO, I/Q offset is only used as a physical fingerprint to identify devices. We got these results:

Mean of the success rate difference: -0.0017333333333333437

Standard deviation of the success rate difference: 0.2079134022222222

After the combination of CFO which means we used both physical fingerprints, the I/Q offset and the CFO, to identify the device. We got these results:

Mean of the success rate difference: 0.00010666666666665492

Standard deviation of the success rate difference: 0.20093300195555555

4.2 Discussion

First, there is an increase in the mean of success rate difference, which proves that the combination of physical fingerprint identification with CFO can make the success rate of target transmitter greater than that of attacker, regardless of the influence of ambient noise and other factors. This means the security of the identification process increases when more physical-layer fingerprints is used to recognize the device. Then, the standard deviation does not change too much, which proves that the system is very stable even when CFO is added as one of the factors for device identification, which proves that the process of using physical fingerprints to identify devices is robust.

5. CONCLUSION

In conclusion, through the establishment of the model, the whole process of physical fingerprint identification is introduced. Then, by considering the data obtained by two experiments, physical fingerprint device identification is

proved to be a safe and robust method. And by quantifying security and robustness, if more physical fingerprints are referenced to identify devices together, it will be harder for attackers to attack our devices, and in Bluetooth communication, the transmission between devices will be more secure. In the future, people need to enable the device to recognize more physical devices to improve the security of Bluetooth communication, but this may require a higher cost and the device needs higher power, which is the future research direction.

6. Acknowledgment

Fengting Fei, Zhuohang Lai, Changhe Li, and Jiayue He contributed equally to this work and should be considered co-first authors.

References

[1] Vainio, J. T. (2000, May). Bluetooth security. In Proceedings of Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory, Seminar on Internetworking: Ad Hoc Networking, Spring (Vol. 5).

[2] Rijah, U. M., Mosharani, S., Amuthapriya, S., Mufthas, M. M. M., Hezretov, M., & Dhammearatchi, D. (2016). Bluetooth security analysis and solution. International Journal of Scientific and Research Publications, 6(4), 333-338.

[3] Givehchian, H., Bhaskar, N., Redding, A., Zhao, H., Schulman, A., & Bharadia, D. (2023, October). Practical Obfuscation of BLE Physical-Layer Fingerprints on Mobile Devices. In Proc. of IEEE S&P (Vol. 23, pp. 73-73).

[4] Danev, B., Luecken, H., Capkun, S., & El Defrawy, K. (2010, March). Attacks on physical-layer identification. In Proceedings of the third ACM conference on Wireless network security (pp. 89-98).