Device Synchronisation: A Practical Limitation on Reader Assisted Jamming Methods for RFID Confidentiality

Qiao Hu, Lavinia Dinca, Gerhard Hancke

Device Synchronisation: A Practical Limitation on Reader Assisted Jamming Methods for RFID Confidentiality

Qiao Hu[1], Lavinia Mihaela Dinca[1], and Gerhard Hancke[1]

City University of Hong Kong, Hong Kong
qiaohu2-c@my.cityu.edu.hk

Abstract. Radio frequency identification (RFID) is a core component of the Internet-of-Things. In certain cases the communication between the tag and the reader needs to be confidential. Some passive RFID tags have very limited computational power and can therefore not implement standard cryptographic mechanisms. This has led to several proposals where data sent by the RFID tag is 'hidden' by noisy signals generated by the RFID reader. The RFID reader can remove the noise but third-party adversaries cannot, thereby ensuring a confidential backward-channel for tag data without the need for cryptography. Although this is a promising research direction there are also some practical limitations on the effectiveness of such schemes. This paper shows that at least one recent scheme is vulnerable to data recovery despite varying the reader's transmission power if there is a slight difference in the phase of the reader's blocking signal and the tag's data. We experimentally verify our attack and conclude that our eavesdropping and data recovery approach is effective and realistic. Finally we test three possible mitigation methods and show that two of the three approaches can provide protection against our attack while having little impact on the bit error rate of the reader in decoding the tag data.

Keywords: RFID, jamming, eavesdropping, physical-layer security

1 Introduction

Radio frequency identification (RFID) is one of the main technologies enabling the Internet-of-Things. There are many types of RFID systems, which cover devices from contactless payment smart cards to item-identification tags. The latter type of inexpensive RFID tags have several limitations, including storage, computational capability and power [1]. Given the popularity of RFID technology in various types of systems, security services have become an important aspect of RFID systems, including within the Internet-of-Things [2],. There are generally two major kinds of security concerns [2]: privacy and authentication. In this paper we focus on mechanisms that provide data encryption for the purpose of ensuring data confidentiality and privacy. As RFID uses wireless communication, eavesdropping is potentially an effective attack to obtain tag

information and has been demonstrated against RFID systems [6, 5]. In general, to protect against eavesdropping attacks, we usually apply some cryptography to encrypt messages that will be transmitted over the air [7]. However, this approach obviously needs some computational ability, which adds costs to minimalist tags. This resulted in research work on how tags responses could be 'encrypted' without the need for dedicated cryptographic mechanisms on the tag.

Recently, Huo et. al. [3] has proposed a new physical-layer security method (we will refer to it as Power Varying in the rest of our paper). Passive tags derive their power from the radio carrier transmitted by the RFID reader. Tags also do not transmit their own radio signals, due to power constraints, but rather modulate their response data on the reader's carrier. The reader can observe this 'backscatter' approach to determine the tag's response. Huo's scheme requires the reader to vary the amplitude of the carrier during the tag's response. This means that the response is modulated onto a 'noisy' signal. The reader, as it is sending this signal can cancel it out and determine the tag's response. A third party, who observes the mixed signal, cannot recover the response. The basic concept had been proposed before [4, 12, 13] but this scheme used a simpler, non-random step function as the intentionally introduced noise.

In this paper, we show that under certain realistic conditions we can reliably circumvent the basic Power Varying scheme. If the reader noise signal and the tag's response are not exactly in phase, i.e. perfectly synchronized, we can successfully start to recover tag response data from the mixed signal. Although RFID tags are generally adapt at loosely synchronizing responses with each other and to the timings expected by the reader there are in practice still variations in the response times. In publishing our research we wish to illustrate that, even though this general approach shows some promise, designs should carefully take into account the actual channel environments and device characteristics of RFID systems. Not doing so could have unintended consequences that could compromise the security of the entire scheme.

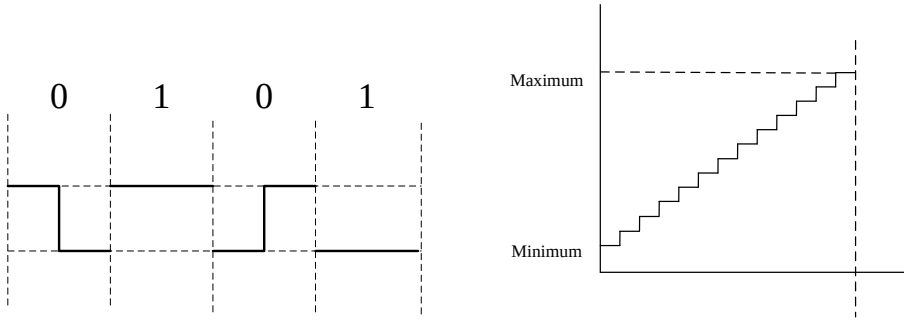
The rest of our paper is organized as follows: Section II provides a brief overview of related work and introduces the details of the Power Varying method by Hou et. al. We then describe how we can break this method with only one eavesdropper in section III, and demonstrate our attack through realistic simulation. In section IV, we show how the scheme could be improved using ideas from existing literature and show the effectiveness of mitigation methods on our earlier attack.

2 Background and Related Work

2.1 RFID System

In the Power Varying scheme the authors mention using a 915 MHz carrier as the signal from the RFID reader. We therefore assume that the scheme is primarily intended to work with RFID systems adhering to ISO/IEC 18000-6

(although the idea could feasibly also be applied to 13.56 MHz systems like ISO/IEC 14443/15693). As such, we will provide a brief overview of the communication channel specified in this standard in terms of the encoding and modulation characteristics of the response transmitted by the tag.



(a) FM0 Coding (b) Power Varying Reader Signal

Fig. 1: Basic concepts of RFID tag response and Power Varying

In ISO/IEC 18000-6, the tag transmits data to the reader through backscatter modulation, i.e. modifying and 'reflecting' the incident reader signals. Data that is transmitted by the tag is coded with the FM0 technique, as shown in Fig. 1.a, For logic bit 1, we can just see an instant electrical level change at the start of the symbol period. For logic bit 0, we can see not only an instant electrical level change at the start of the symbol period but also at the middle of the symbol period. The modulation method adopted is 10% Amplitude Shift Keying (ASK). If the logic bit is 1, the amplitude is α, otherwise it will be β. A modulation index of 10% means that $(\alpha - \beta)/(\alpha + \beta)$ is equal to 10%.

2.2 The Power Varying Method

Power Varying aims to prevent eavesdropping by changing the power/amplitude of the transmitted reader's signal. Huo et. al. [3] claims that the changing amplitude can effectively hide the backscattered signal transmitted by tags from eavesdroppers. Given that the reader is responsible for the power variation it can effectively cancel out this variation and reliably recover the noise. The basic format of the power varying signal is shown in Fig. 1.b. First, it will choose a minimum amplitude that satisfies the minimum power needed to activate and power the passive tags. Next, the amplitude of the signal will increase step-by-step until it reaches the maximum chosen amplitude. It will then return to the minimum amplitude and the cycle will start again.

The authors describes the variations of this step signal. In the first variation the period of the signal is equal to the bit period of the tag's response. The second variation uses a varying signal that has a period that is 10% of the bit period. The basic scheme defines that the changing step amplitude is equal to the difference between the amplitude of tag signals containing logic bit 0 or 1. In other words, when a symbol period of tag containing logic bit 0 arrives, the amplitude of the signal observed by eavesdropper will be the same as the amplitude of the signal during the previous step if the symbol period of the tag containing logic bit 1 arrived. We give an example of the first variation of this scheme in Fig. 2. From this figure, we can observe that amplitude differences between two continuous signals received by the attacker are different depending on the logic bit carried by corresponding tag signals. For example, the amplitude difference between two periods with logic bits sequence in 10 is near zero. And the amplitude difference between two periods with logic bits sequence in 01 is almost double of that with sequence in 11. This means that if we know which logic bit is carried during a step period, we can deduce the previous or next logic bit by the amplitude difference between these periods. How to know the logic bit? If we observe near zero amplitude difference, which happens quite often, we know that these two periods represent logic bits 00.

As this constant amplitude increasing method is vulnerable, its authors suggest to use random amplitude. Fig. 3.a illustrates this improved method in the first variation mentioned above. We can see that the amplitude difference between two continuous step periods has no relationship with the logic bit sequence. Even the logic bit sequence is 10, there is also a large amplitude difference. In other words, it is unclear whether the 2th bit is a large step with a logic 0 or a smaller step with a logic 1.This result demonstrates that the randomly increasing amplitude method has fixed the previous vulnerability.

2.3 Related Work

There are several works on physical-layer security and cryptographic-less encryption based on the general concept put forward by Wyner in the 1970s [16]. The foundation of all these schemes are that the legitimate receiver is less effected by, or can cancel out, noise. This allows for reliable reception of data while an eavesdropper cannot recover the data. At first schemes relied on environmental noise, but to ensure that there is sufficient noise to hide the data, schemes started introducing intentional noise. For example, the introduction of friendly jamming, where the system could either use multiple antennas in one node or multiple trusted nodes, could co-operate to transmit 'friendly' noise that is known to the receiver [9]. Subsequently many researchers tried to apply this idea to RFID technology, e.g [4, 10, 11], where either the reader or other tags would transmit noise to cover data signals transmitted by the tag of interest. There has also work been done on how to generate appropriate noise for jamming high-frequency RFID devices[13]. This method has also been applied to other technologies, such as short-range audio communication channels in mobile phones. In such cases,

one device would transmit data and the receiving device would transmit noise [14, 15].

There has not much work been done on attacking jamming schemes in practical environments. Hancke [12] showed that the natural variation in modulation index, which derives from the inherent impedance of the tags between the device transmitting the response data and the device transmitting the blocking noise, could reveal the hidden response. In this paper we investigate the effect of variations on the response time of the tags, i.e. difference in phase of the blocking noise and the response.

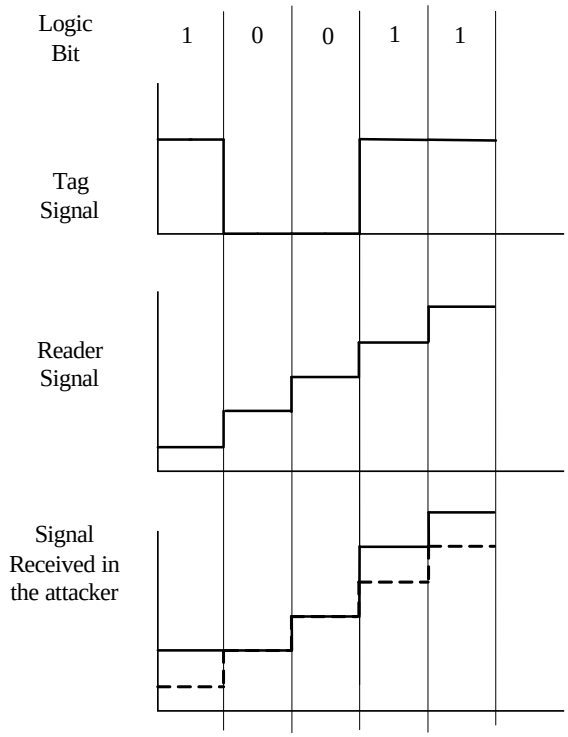


Fig. 2: Signals received by an attacker under the constant amplitude increasing method

3 Overview of Our Attack

3.1 Adversarial Model

In this subsection we introduce the adversarial model used throughout this work. In the rest of this paper we apply the increasing amplitude Power Varying scheme. We calculate the number of steps m by the following formula proposed in [3].

$$m = \frac{x_{high} - x_{low}}{\alpha \overline{x}} \tag{1}$$

x_{high} and x_{low} mean the maximum and minimum amplitude of the reader signal respectively. $\overline{x}$ is given by:

$$\overline{x} = \frac{x_{high} - x_{low}}{2} \tag{2}$$

We set α as 0.1, then m equals 21. Given that there is no standard prescribed in the Power Varying scheme we take two approaches. We attack the scheme assuming that no specific standard is used, i.e. non-return to zero encoding with basic amplitude modulation, and then analyse the scheme if it was implemented as per the ISO/IEC 18000-6 standard. In our adversarial model we have one RFID reader communicating with one passive RFID tag. The adversary is a passive attacker and only obtains the combined signal resulting from the tag response and the varying signal. We do not specify the position of the adversary relative to the tag and reader but assume that the attacker cannot derive any additional advantage from directional monitoring techniques to isolated reader and tag transmissions. Our attacker has knowledge of the standard used, i.e. the communication parameters, and of the Power Varying scheme. This means that the attacker knows that a step function is used to vary the power and he knows the period of the steps, but not necessarily the amplitude of the steps.

3.2 Analysis of Power Varying

1) General Attack

We first analyze the scheme taking into consideration no specific standard. We accept that the method is secure when the mixed signal received by the attacker is as shown in Fig. 3. We can see from Fig. 3 that the data is effectively hidden if the symbol period and the step period is synchronized, with the attacker unable to distinguish the response data as we talked about in Section 2. However, in reality it is unlikely that the reader would be able to perfectly synchronise his step function to the response of the tag. As shown is [11], even similar tags, i.e. same technology and manufacturer, exhibit slighlty different modulation and timing characteristics. We refer to this desynchronisation as the phase offset, or offset for short. The result of an offset on the combined signal is illustrated in Fig. 4, where the step period is not synchronized with the symbol period. In Fig. 3, there is no amplitude change during each symbol period. However, in Fig. 4, due to the desynchronization, the attacker could infer the effect of the step. For

example, if two logic 1's are transmitted we expect the second to have a higher amplitude due to the step, but ideally there should be an uncertainty whether it might also be a large step with a logic 0. If we notice that halfway through the first one the signal increases that is evidently the size of the step. If there is then an additional increase if the next bit period starts we also know that the bit is a one. Therefore, depending on these amplitude discontinuities caused by the offset we can distinguish the logic bits of the response.

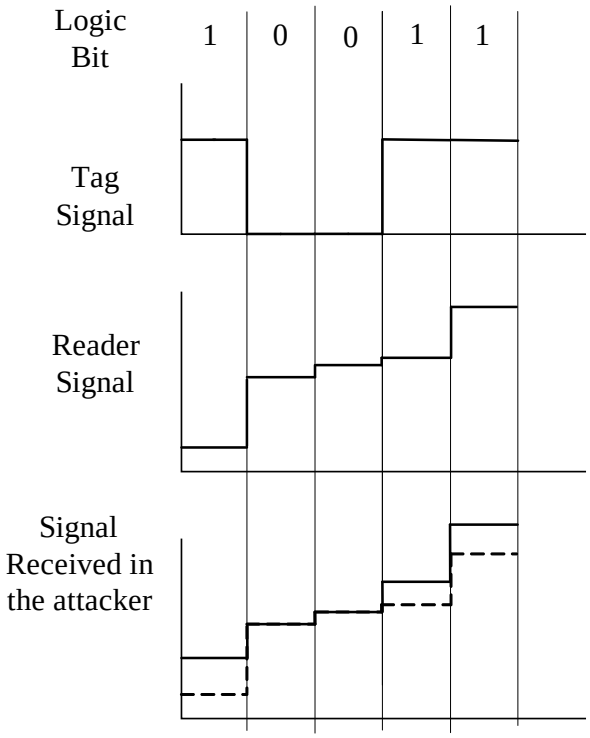
2) Results of the General Attack

We simulate the general attack in Matlab. In this experiment, we consider no specific standard and the tag signal is as shown in Fig. 4. And we also assume that there is no additional environmental noise. Between the minimum amplitude and the maximum amplitude there are 10 step periods (we use this setting at the rest of our experiments). This means that the power signal is a periodic signal with a 10 step cycle (with step period equal to either the bit period or 10% of the bit period). The only factor that may effect the result of our attack is the degree of desynchronization (or phase offset) between the two signals. For step equal to bit period, we set the offset from zero to a step period with interval equals to one fifth of a step period. For the step period 10% of the bit period, we set the offset from zero to two and a half step periods with interval equals to half of a step period. We use bit error rate(BER) to evaluate our experimental results. Our results show that apart from the case where the offset is 0 the resultant BER was always 0 for any amount of offset.

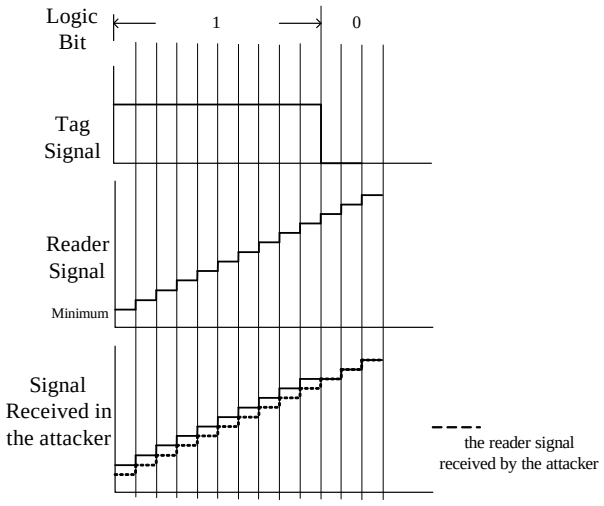
3) Specific Attack under ISO/IEC 18000-6

We then attempted the same attack as in the previous section, but we use the FM0 coding scheme as per ISO 18000-6. This means there is a slight variation in the signal when a logic 0 is encoded in that there is a signal change in the middle of the period, which results in a slightly different combined signal as shown in Fig. 5. Although this case appears at first similar there is now some uncertainty as to whether a discontinuity in the middle of the bit period is caused by the step of the logic 0 transition in some cases. If there is an instant level change at the beginning of each symbol period or at the middle of the period then the symbol represents logic 0. If the step period and the symbol period are not well synchronized, during one step period, we may also observe a similar level change.

We therefore need two steps to recover logic bits. First, we need to find the start of the tag response signal. If there is no tag signal, then there is no amplitude difference in one step period. Because we know the time of all step periods, we can distinguish whether the amplitude difference is caused by the tag signal or by the power signal. So we assume that the first amplitude difference means the start of the tag signal. Then we can calculate the middle area of each symbol period to search for the level change to judge the logic bit of this symbol period, as each symbol period has the same length. These two steps seem the simplest to find amplitude differences caused by electrical level changes.

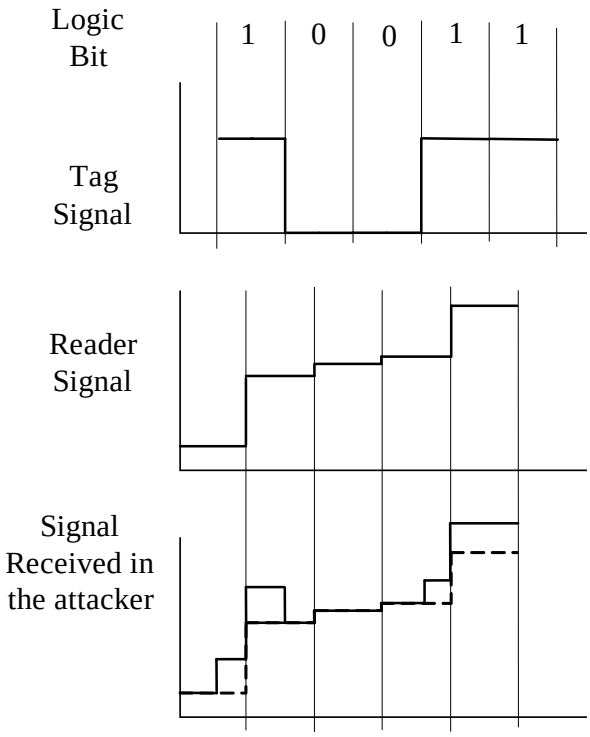


(a) Step period equal to bit period

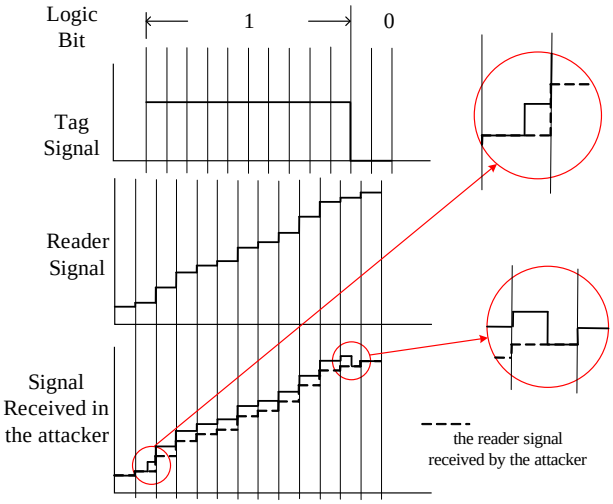


(b) Step with period equal to 10% of bit period

Fig. 3: Signals received by an attacker with perfect synchronization

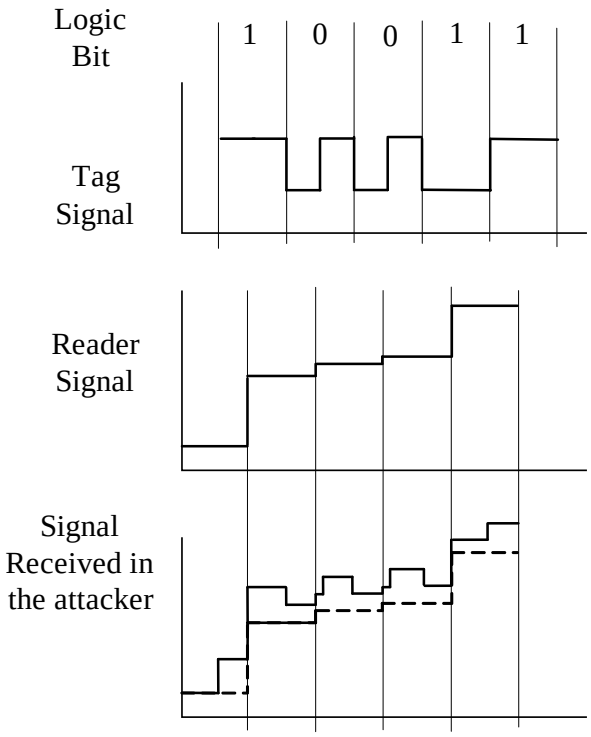


(a) Step period equal to bit period

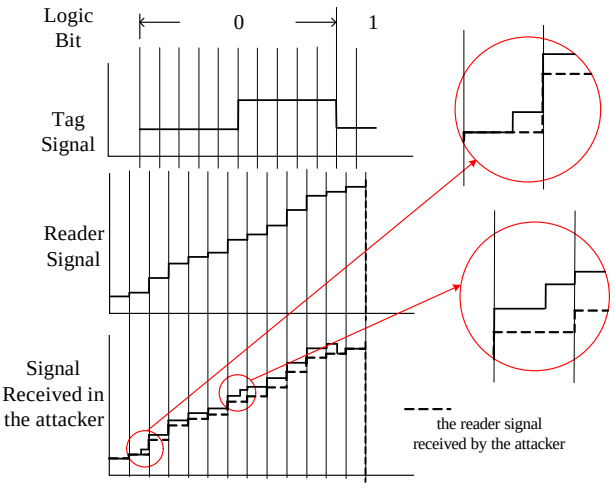


(b) Step with period equal to 10% of bit period

Fig. 4: Unsynchronized signals received by the Attacker



(a) Step period equal to bit period



(b) Step with period equal to 10% of bit period

Fig. 5: Unsynchronized signals received as per ISO/IEC 18000-6

4) Results of the Specific Attack under ISO/IEC 18000-6

We also simulate the specific attack in Matlab. In this experiment, we have the same configuration as with the previous experiment. We also do the experiment under one or one tenth of a symbol period situation. We set the offset as we do in the general attack experiment. Interestingly the results differ from the general case as shown in Figure 6. Let's first see the result of a situation with a period ratio equals to 1, which means a step period is equals to a symbol period shown in Fig 5.a. We can observe three high BER periods. The first and the last period happen when the offset nears zero or one step period, which means the starting point of a symbol period is overlapping with the beginning of a step period. The second period happens with a 1/2 step period offset, which represents the overlap between the middle point of a symbol period and the beginning of a step period. The result of a period ratio equal to 10 has a similar but a little different reason as the previous result. The difference is that the distance between the starting point and the middle point of a symbol period can be divided by a step period, which is illustrated in Fig 5.b. If the starting point of a symbol period is overlapping with the beginning of a step period, we may get a high BER at the attacker. We can observe that except for the area of overlapping, the BER is 0, which means the attack is a success.

5) Eavesdropping in a Noisy Environment

Up to now the attack implementation did not consider any additional noise. However, this is not a realistic assumption in real operating environments. Therefore we also consider our attack against Power Varying in the presence of background noise. Such noise should in theory hinder the attacker and the valid receiver. We only analyze the impact of noise for the attack scenario against ISO 18000-6. As noise will change the amplitude of signals, we should calculate the average amplitude to deduce the impact of noise. To evaluate the impact of additional background noise, we add Additive White Gaussian Noise (AWGN) to our simulation. We set the SNR (Signal to Noise Ratio) of the received signal in the attacker as ∞ (no noise), 20dB and 30dB. These are realistic noise figure in radio environments, e.g. WiFi under normal conditions operates at around 40 dB. We again run the experiment with the two kinds of step period length. The final result, as shown in Fig. 7, is as expected. It shows the BER of the attacker increasing but large parts of the message could still be recovered.

4 Mitigation Methods

In this section we consider ways to mitigate the weaknesses of the basic scheme. As we only analyze the randomly increasing amplitude method, we try to analyze the random amplitude method that allows the amplitude increasing or decreasing. We will refer to this as the random amplitude method. Another approach is to use the reader signal and a phase shifted version of the reader signal as the reader's signal. This is similar to the approach in [4] where noise and

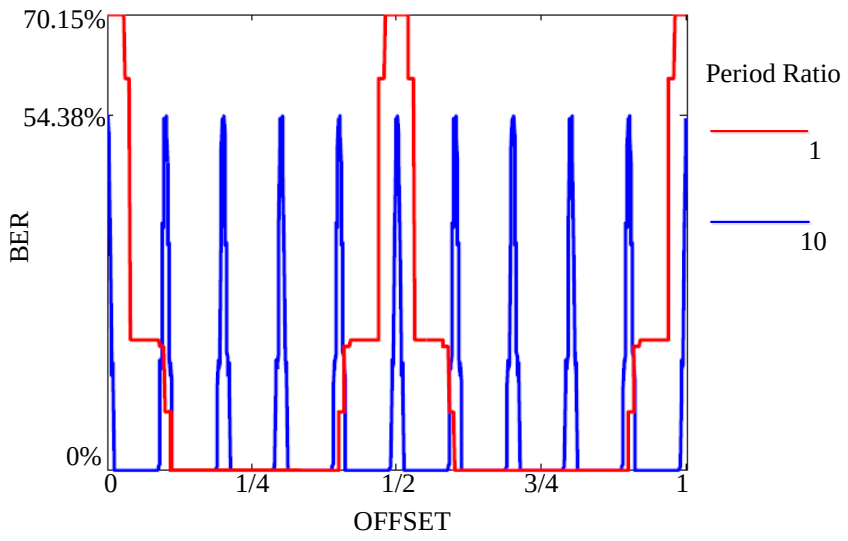


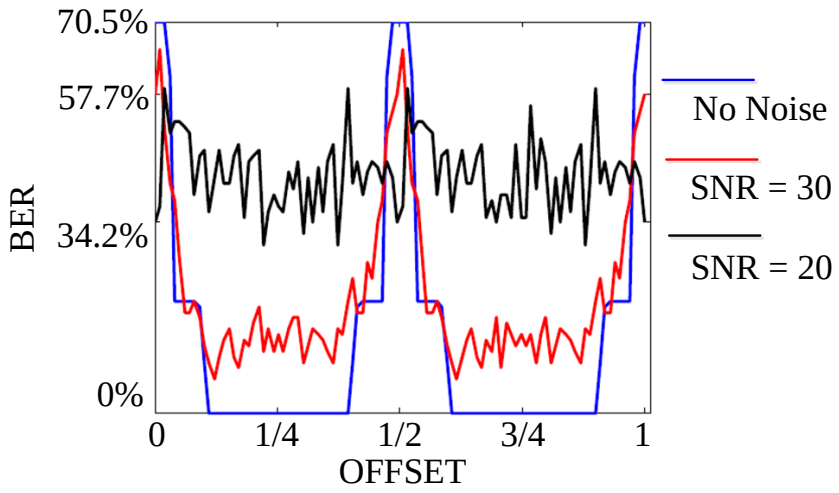
Fig. 6: Results of the attack on ISO 18000-6

noise phase shifted by $\pi/2$ are used to hide the data. We randomly create two reader signals with just one cycle from the minimum amplitude to the maximum amplitude. So these two randomly created signals have different amplitudes even in the same step period. Then we multiply one reader signal by the normal carrier and the other one by the carrier phase-shifted by $\pi/2$. We add them together to form a new reader signal. During one step period, α and β are the amplitude of two reader signals, and the amplitude of the new reader signal in this step period can be calculated by:

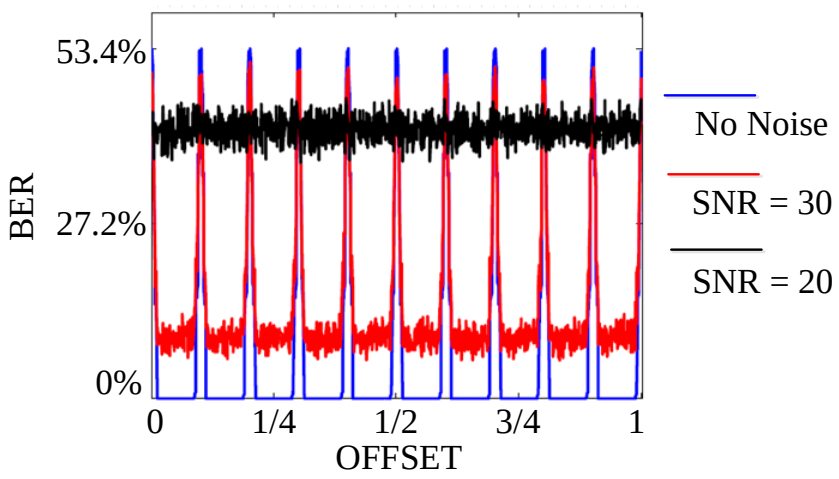
$$Amp = \alpha cos(2\pi * 915000000 * t) + \beta cos(2\pi * 915000000 * t - \frac{\pi}{2}) \qquad (3)$$

This formula tells us that the new reader signal is a cyclic signal with a period of 2π during one step period. We refer to this as the artificial noise method. Finally, we propose that we can improve the random amplitude method by also adding a random variation of the step length. In other words, choose the step period length randomly. We call it the random step period and amplitude method. We implement these three methods for the ISO/IEC 18000-6 standard and repeat the attacks tests in the previous sections. In experiments on the first two methods, we set the period ratio as 1. We also evaluated these methods if the SNR of the received signal at the attacker are ∞ (no noise), 30db and 20db.

Results of these tests are shown in Fig 8. Thise figure show that when the energy of noise is very low compared to the mixed signal, the first two methods increase the BER by a small amount but the third method utilizing both the random step size and random step amplitude works much more effectively. We

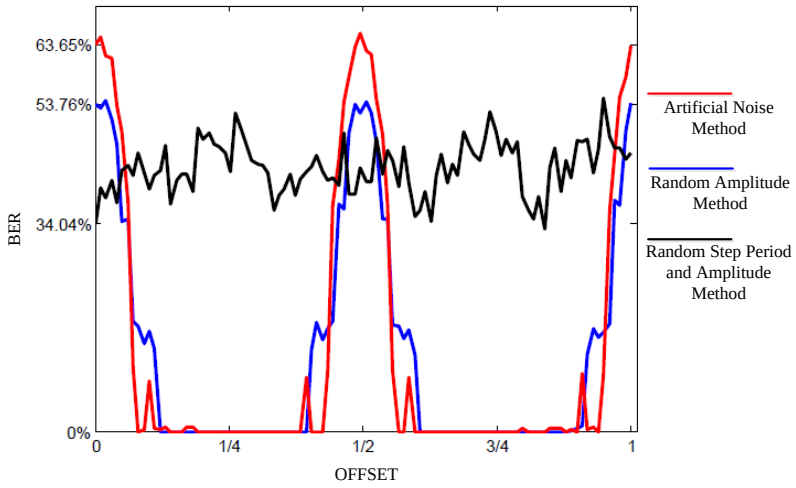


(a) Step period equal to bit period

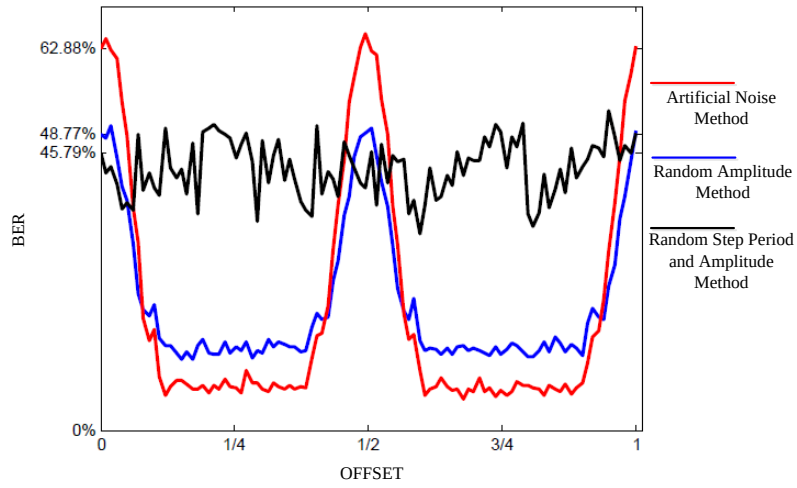


(b) Step with period equal to 10% of bit period

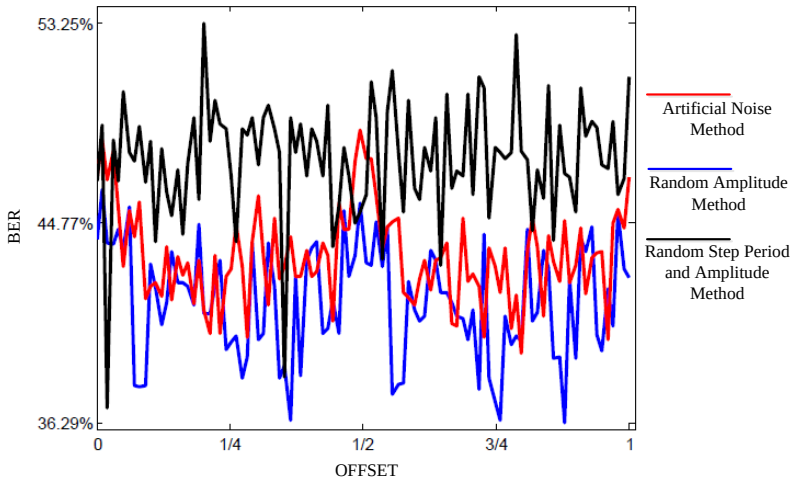
Fig. 7: Impact of noise on the attack



(a) BER at the Attacker of Three Methods with no noise



(b) BER at the Attacker of Three Methods with SNR equals to 30db



(c) BER at the Attacker of Three Methods with SNR equals to 20db

Fig. 8: Results of Noise Impact on Communication based on Specific Standard

believe this is because our attack depends mostly on the amplitude difference caused by the tag signal and the time of amplitude changes caused by the power signal can be calculated by us. As the first method only change the amplitude of the power signal and the second method only change the original power signal to another power signal with the same cycle time, these have minimal effect on our attack. The last method is also successful at causing the attack to calculate the incorrect start point which would lead to error decoding most of the message.

5 Conclusion

In this article, we analyze the vulnerability of Power Varying method proposed by Hou et. al. [3]. This method can be broken when the step period of the signal from a reader and the symbol period of the backscatter signal from a tag are not well synchronized. This desynchronization causes amplitude differences in the step period which can be used to distinguish tag signals. We describe our attack under general situation and for communication adhering to ISO/IEC 18000-6. Then we analyze factors including noise and phase offset that can affect our attack. Results show that our attack works well in less noisy environment and that even a small phase offset can result in effective recovery of the tag's response. Lastly, we test three mitigation methods: a random step amplitude method, artificial noise addition method and a combined random step period and amplitude method. Results show that the latter approach, which is propose by us, is the best mitigation method. The combined random step period and amplitude method can protect communication from recovery while have little impact on the bit decoding error rate of the tag signal at the reader.

References

1. Grover, A., Berghel, H.: A Survey of RFID Deployment and Security Issues. Journal of Information Processing Systems. vol. 7, pp. 561–580 (2011)
2. Hancke, GP., Markantonakis, K., Mayes, KE. Security Challenges for User-Oriented RFID Applications within the Internet of Things. Journal of Internet Technology 11 (3), pp. 307–313 (2010)
3. Huo, F., Yang, C., Gong, G., Poovendran, R.: A Framework to Securing RFID Transmissions by Varying Transmitted Reader's Power. In: 9th Workshop on RFID Security, pp. 57–68. IOS Press, Amsterdam (2013)
4. Archard, F., Savry, O.: Cross-Layer Approach to Preserve Privacy in RFID ISO/IEC 15693 systems. In: RFID-Technologies and Applications (RFID-TA), 2012 IEEE International Conference on, pp. 85–90, IEEE, (2012)
5. Hancke, G.: Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens. Journal of Computer Security. 19, 259–288 (2011)
6. Hancke, G.: Eavesdropping Attacks on High-Frequency RFID Tokens. In: 4th Workshop on RFID?Security, pp. 100–113 (2008)
7. Juels, A.: RFID security and privacy: A research survey. IEEE Journal on Selected Areas in Communications. 24, 381–394 (2006)
8. Bolic, M., Simplot-Ryl, D., Stojmenovic, I.: RFID systems: Research Trends and Challenges. John Wiley & Sons, Hoboken (2010)

9. Negi, R., Goel, S.: Secret Communication Using Artificial Noise. In: IEEE Vehicular Techonology Conference. vol. 62, pp. 1906–1910 (2005)
10. Castelluccia, C., Avione, G.: Noisy Tags: Pretty Good Key Exchange Protocol for RFID Tags. In: Smart Card Research and Advanced Applications Conference. pp. 289–299 (2006)
11. Haselsteiner, E., Breitfuss, K.: Security in Near Field Communication (NFC). In: Workshop on RFID security. pp. 12–14 (2006)
12. Hancke, G.: Noisy Carrier Modulation for HF RFID. In: First International EURASIP Workshop on RFID Technology, pp. 63–66,(2007)
13. Savry, O., Pebay-Peyroula, F., Dehmas, F., Robert, G., Reverdy, J.. RFID Noisy Reader How to Prevent from Eavesdropping on the Communication? In: Workshop on Cryptographic Hardware and Embedded Systems , pp. 334–345 (2007)
14. Nandakumar, R., Chintalapudi, K., Padmanabhan, V., Venkatesan, R.: Dhwani: Secure Peer-to-Peer Acoustic NFC. In: ACM SIGCOMM Computer Communication Review, Vol. 43, pp. 63–74 (2013)
15. Zhang, B., Zhan, Q., Chen, S., Li, M., Ren, K., Wang, C., Ma, D.: PriWhisper: Enabling Keyless Secure Acoustic Communication for Smartphones. IEEE Internet of Things Journal. vol. 1, pp. 33–45 (2014)
16. A.D. Wyner: The Wire-Tap Channel. Bell Systems Technical Journal, vol. 54, pp. 1355-1387, (1975)