A Framework to Securing RFID Transmissions by Varying Transmitted Reader's Power

Fei Huo [a], Chouchang Yang [b], Guang Gong [a] and Radha Poovendran [b]
[a] *Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada*
[b] *Network Security Lab, Department of Electrical Engineering, University of Washington, Seattle, WA, 98195, USA*

Abstract. RFID technology has gained tremendous popularity in the recent years. The tiny, inexpensive RFID tags can be easily attached to objects for seamless identification. However, one glaring weakness of RFID tags, especially passive RFID tags is its lack of capability for implementing strong crypto primitives for security purposes. When no or a weak crypto primitive is implemented, the adversary could easily eavesdrop to the communication session between the reader and the tag, he can potentially gain all the secrets about the tag. In doing so, the secrecy of the messages and the privacy of the tag is violated. In this paper, we introduce a new framework that would protect the messages transmitted from the tag to the reader. This framework makes use of the physical properties of RFID systems by sending a random time-varying waveform from the tag to the reader for power harvesting rather than a fixed amplitude waveform. We show theoretically this framework is secure against one eavesdropper by showing the eavesdropper's decoding error probability is very close to 50%. Furthermore, we have implemented our framework, the experimental results also confirm with our theoretical results. Finally, we will discuss two more stronger forms of attack.

Keywords. RFID, RFID Security, RFID Physical Layer

1. Introduction

Radio frequency identification (RFID) has gained tremendous popularity and research attention in the recent years. There are two distinct advantages with RIFD systems [6]: First, RFID provides unique identifications of each object. Each RFID tag contains an unique identification (UID) number that distinguishes itself from all other tags. Second, the reading range could potentially go up to tens of meters while no line of sight requirement is needed. Since its invention, the RFID technology has found a wide range of applications. This includes passport, driver's license, building access control and supply chain management just to name a few.

Based on the power source that drives communications between the reader and the tag, RFID tags can be classified into active, semi-active and passive three classes [4]. Active and semi-passive tags all have on-board batteries, which provide them with rea-

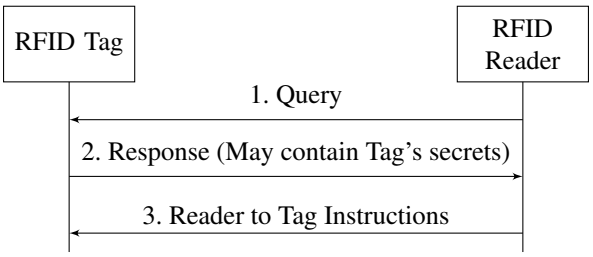

Figure 1. Reader Tag Communication

sonable computational capability. Passive RFID tags on the other hand can only harvest power from the reader. The first two classes of tags are powerful, implementations of secure cryptographic primitives on these tags are possible. Many RFID applications such as inventory control require the tag to be inexpensive, in these scenarios, only the passive RFID tags are applicable. However, passive tags are computationally constrained, their memory is generally also very limited. Therefore, one glaring weakness of the passive RFID system is its security and privacy concerns due to these constraints.

Different RFID standards employee different protocols for communications between the reader and the tag. However, in general, this process can be roughly depicted as shown in Figure 1. When a reader tries to communicate with a tag, it first sends a query to the tag. Upon receiving the query, the tag replies with its response. The response may include tag's secret information. The connection between them is also established. The reader then sends instructions to the tag to perform various tasks. It is imperative that the sensitive information such as a tag's UID to be protected. Therefore, our motivation is to find a good method to safeguard the messages transmitted from the tag to the reader without disclosing any information to the adversary in a passive RFID system.

There have been numerous attempts made in securing the transmissions between the reader and the tag. The most straightforward method is through the use of encryption. The computational complexity of public key cryptography is too high. Presently it is not feasible to passive tags. Generally, symmetric key cryptography is implemented. Due to the memory constraint, the key length is usually shorter than 80 bits, which is the presently accepted level for a symmetric key cryptography to be considered secure. Thus it cannot be considered to be secure. For example, the key length of popular EPCglobal Class 1 Gen 2 standard is only 32 bits [3]. This can easily be broken with the exhaustive search attack, and hence does not offer protection against a computationally powerful adversary. Consequently, other alternatives have been sought.

In [1] and [7], the authors proposed adding a separate source which randomly generate 8-bit level of noise to the reader's continuous waves to prevent the adversary from eavesdropping. Although the authors make the claim that the random noise amplitude is able to thwart an eavesdropper, no theoretical analysis supporting the claim was provided. Furthermore, the noise source and the reader requires perfect synchronization with each other in order to correctly decode the messages.

In this paper, we present on a new physical layer approach to address the problem of securing transmission of messages from the tag to the reader and to ensure the privacy of the tag. This scheme is very simple to implement, it requires no extra complexity, and no pre-sharing of any secrets between the reader and the tag is needed. We think this

framework can be implemented to the existing RFID networks to provide an additional layer of security against the various attacks.

The rest of the paper is organized as follows. In Section 2, we introduce the system as well as adversary models considered in this paper. In Section 3, we first present our framework, then we theoretically show this framework is secure against one eavesdropper. In Section 4, we implement our framework on a passive RFID system. We show the received and decoded messages for the legitimate reader and the adversary respectively. In Section 5, we explore two more stronger forms of attack. Namely *multiple passive adversaries colluding together* and *active eavesdropping*. Section 6 presents our conclusions and our future research.

2. System and Adversarial Model

In this section, we introduce the system and adversarial model used throughout this work.

2.1. System Model

In this work, we consider a passive RFID system where the tags are powered based on transmitted power of the reader. A simple passive RFID network consists of a reader and multiple passive tags. Each communication channel between a tag and a reader is independently secured. This can be achieved for example by ensuring that all tags share different keys at each run of the communication protocol. Therefore, our system model is of the simplest form, it is consisted of one reader and one tag. Furthermore, our scheme involves the reader generating a random, uniformly distributed time-varying waveform which would be send to the tag for the power harvesting purpose.

2.2. Adversarial Model

We assume that the adversary is a passive eavesdropper that can listen to local communication (not global). We further assume that the adversary can be mobile. He can freely move around or stay constantly as he wishes. He also has the complete knowledge of all the protocols and frequencies used between the reader and the tag. Furthermore, we assume that while the adversary has knowledge about the time varying nature of the waveform at any given instant, he does not have the specific values chosen for the "random" amplitude of the waveform.

3. Framework and Analysis

In this section, we first present our proposed framework. Then we present theoretical analysis showing that our proposed scheme is resilient against the passive eavesdropper.

3.1. Framework

The idea makes use of the physical nature of passive RFID systems. After a reader has sent an instruction to the tag, it needs to continuously send a waveform to the tag which is used to keep the passive tag active. The tag then performs backscattering modulations

by setting the impedance to either low or high to return a 0 or 1 respectively. The returned signal seen at the reader would be a superposition of its transmitted continuous waveform and the backscattering modulated signal. In this new approach, whenever after a reader has issued a command to the tag, instead of providing the constant amplitude continuous waveform to the tag, the reader sends a time-varying waveform whose amplitude changes after elapsed time. The time-varying waveform pattern is random only known to the reader. Assuming the minimum and maximum transmitted amplitudes are x_{low} and x_{high} respectively, then the distribution of the time-varying waveform is randomly uniformly distributed with a step size $\alpha\bar{x}$, where α is a constant which is a function of tag's impedance and $\bar{x}$ is the average amplitude given by:

$$\bar{x} = \frac{x_{low} + x_{high}}{2}.$$

Intuitively, by adopting our approach, the tag could still harvest the energy from this random waveform, the reader can cancel the effect of time-varying waveform before performing the decoding. However, the adversary without knowing the amplitude pattern of the transmitted waveform would not be able to cancel the noise, his intercepted signal reveals no information about he transmitted messages. Thus, the secrecy of the messages transmitted from the tag to the reader can be achieved.

One should notice that the power level of various continuous waveform from the reader is much larger than the power level of tag's backscatter signal since tags can only backscatter partial energy from reader's continuous waveform. Hence, an adversary always experience non-neglected interference from various continuous waveform which is larger than tag's signal such that an adversary cannot decode tag's data signal at any location alone. Unless the frequency of the time-varying waveform from the reader is much slower than the frequency of tags' signal, in this case, each time varying amplitude spans over multiple tag's data symbols. The adversary could treat this amplitude as a constant DC amplitude and remove it. Then he would potentially be able to decode the tags' signal. However, in our scheme, we consider the frequency of time-varying waveform to be always same or faster than tag's rate. Consequently, the adversary cannot separate the time-varying waveform and then decode the tag's signal.

3.2. Analysis of the Proposed Scheme

In the previous subsection, we have intuitively reasoned why our frame is secure against the eavesdropper. In this subsection, we provide detailed theoretical analysis to prove the security of our framework.

Let the transmitted waveform by the reader be x_i at time i, in an ideal situation, the received signal y_i by the same reader when the tag's backscattered signal is 0 or 1 can be modeled respectively by:

$$y_i = \begin{cases} \beta x_i, & \text{Tag returns 0} \\ \beta(x_i + \alpha x_i), & \text{Tag returns 1,} \end{cases} \tag{1}$$

where β is the channel gain and α is a constant due to impedance of the tag. This implies when 0 is returned, no added amplitude is returned. When 1 is returned, some proportional amplitude will be superimposed on top of the existing waveform.

Ideally, x_i in (1) should be dependent on the time-varying amplitude at time i. However, if the difference between the minimum amplitude x_{low} and the maximum amplitude x_{high} is small relatively to $\bar{x}$, then (1) can be reasonably approximated as follows:

$$y_i = \begin{cases} \beta x_i, & \text{Tag returns 0} \\ \beta(x_i + \alpha\bar{x}), & \text{Tag returns 1.} \end{cases} \tag{2}$$

In our framework, we have chosen our step increment size to be $\alpha\bar{x}$. This matches the difference in the returning value of 0 and 1. Then there would be a total of m steps given by:

$$m = \frac{x_{high} - x_{low}}{\alpha\bar{x}} + 1,$$

we further assume the system is designed such that m is an integer.

Consequently, for all $m-2$ intermediate levels of transmitted amplitudes other than x_{low} and x_{high}, if the tag returns an 0, then the tag whose input waveform is one step below with a return value of 1 would also have the same amplitude. Likewise, if the tag returns an 1, then the tag whose input waveform is one step above with a return value of 0 would also have the same amplitude. Assuming the probability of returning 0 and 1 by the tag is equally at 50% each, in the absence of the noise, the tag's maximum likelihood detector will be unable to make a decision or the decoding error probability $P_e = 50\%$.

For the transmitted waveform is x_{low}, the decoding error probability is :

$$P_e = \begin{cases} 0, & \text{Tag returns 0} \\ \frac{1}{2} & \text{Tag returns 1,} \end{cases} \tag{3}$$

The first line is because the returned signal is uniquely decoded into 0, no error is introduced. The second line is due to the reason mentioned earlier.

Similarly, for transmitted waveform x_{high}, the decoding error probability is just the reverse of (3) due to the symmetry:

$$P_e = \begin{cases} \frac{1}{2}, & \text{Tag returns 0} \\ 0, & \text{Tag returns 1,} \end{cases}$$

The overall total error probability P_t of our framework where the transmitted time-varying waveform is uniformly randomly distributed with m steps is:

$$\begin{aligned} P_t &= \frac{m-2}{m}\frac{1}{2} + \frac{1}{2}\frac{2}{m}\frac{1}{2} \\ &= \frac{1}{2}\frac{m-1}{m} \end{aligned} \tag{4}$$

Equation (4) is a lower bound of the error probability for adversaries, by taking noise into account. We expect the attackers' decoding performance to be further degraded. Namely, at any location, the bit error probability for adversaries is at least the same or higher than given in equation (4). With the reasonable value of m, i.e., $m > 20$, (4) results in an decoding error probability close to $\frac{1}{2}$, this guarantees that the eavesdropper would be indistinguishable of tag's response regardless of the attacker's location, channel quality and noise level.

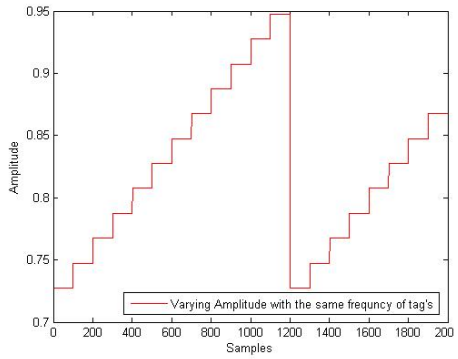

Figure 2. Reader's transmitted continuous wave at slow rate

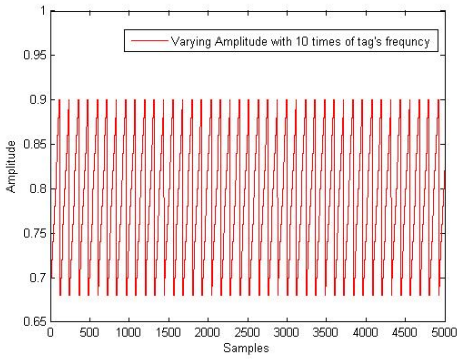

Figure 3. Reader's transmitted continuous wave at fast rate

4. Experiment

In this section, we will verify our scheme through experiments. We have implemented our own RFID system on two USRP N210 with 900 MHz daughter board and Intel WISP tags. We have configured one USRP to be the legitimate reader, and the other to be the adversary. The antenna we used for both URSPs are near-field antenna specially designed for RFID signal measurements [5]. In setting up the experiment this way, we ensure that the legitimate reader and the adversary have equal capabilities. The Intel WISP tag is configured to be a pure passive tag.

In these experiments, a baseband signal of regularly increasing step function is used as a various amplitude waveform with cosine carrier at 915MHz. We chose regularly increasing step function for easy demonstration purpose. In reality, random step functions should be used instead. This random time-varying waveform is known only to the reader, the adversary has no knowledge of this waveform pattern. We chose two different periods of each step function. For the first experiment, the period of each step function matches the tag's data rate. This implies that each returned step wave contain no more than one bit of backscattered information. For the second experiment, the period of each step waveform is $\frac{1}{10}$ of the tag's data period. This implies 1 bit of tag's backscattered signal is spread over 10 step waveforms. The two transmitted waveforms are shown in Figures 2 and 3 respectively. Furthermore, we fix the tag's backscattering modulated response to be a 16-bit response 0101, 0011, 0001, 0010. Once the response length exceeds this length, it will stop to sending for 5 symbol periods and repeat again from the first bit. This guarantees the comparability of our results under different settings.

We will examine the received baseband signals for both the reader and the adversary. We will show for the case of the reader, after removing his own transmitted continuous wave, he can successfully decode the message. However, for the case of the adversary, without knowing the continuous wave pattern, the received signal in the eyes of the adversary would look like noise, thus he could not successfully decode it into messages.

4.1. Reader's Recovered Signal

The received results for each different rate are shown in Figures 4 and 5 respectively. Since the legitimate reader know the varying amplitude waveform and frequency rate,

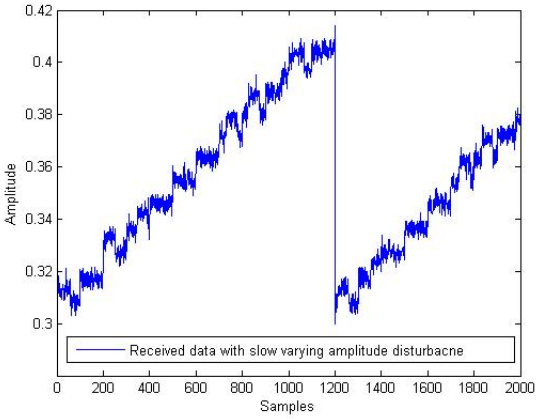

Figure 4. Received signals with slow rate disturbance

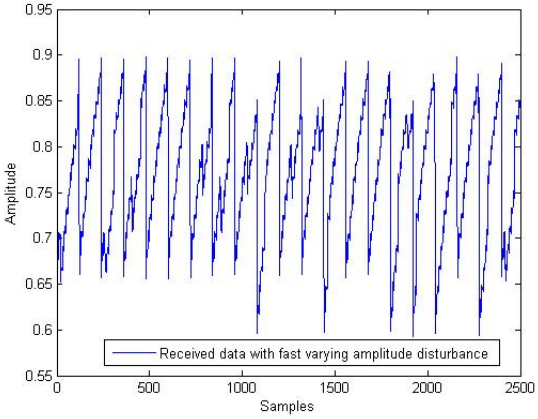

Figure 5. Received signals with fast rate disturbance

the reader is able to remove the disturbance. Hence, the reader can recover tag's data as shown in Figure 6.

Figures 4 and 5 illustrates the received signals by the reader with the slow and high disturbance rate respectively. Figures 6 and 7 demonstrates the recovered results after removing the time-varying results. This is done by a signal processing script written in Matlab which automatically removes the effect of the transmitted time-varying waveform. From Figures 4 and 5, one can easily distinguish 0 and 1 (1 has a higher amplitude and 0 has lower amplitude). Using standard decoding algorithms, the waveforms started from samples 660 in Figure 4 and samples 700 in Figure 5 would be decoded into 0101, 0011, 0001, 0010, which matches our expected return response. There exists big fluctuations in the amplitude of the reader's recovered signal as shown in Figures 6 and 7, it is more noticeable in Figure 7. This is due to the steep instantaneous change in the amplitude of the transmitted signal from the one period to another. It would take some

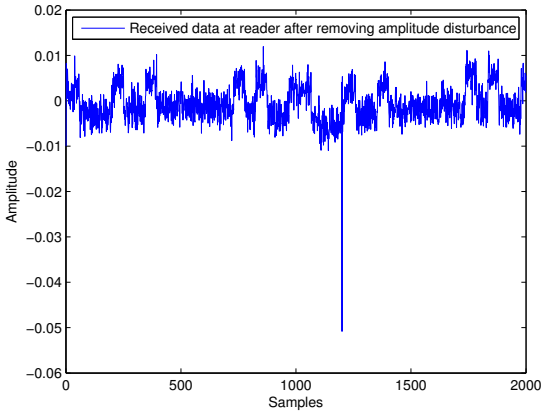

Figure 6. Recover tag's signal from slow disturbance

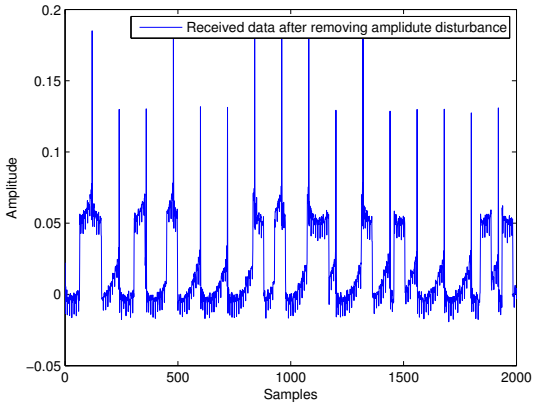

Figure 7. Recover tag's signal from fast disturbance

time for the tag to react to this change. This suggests the random waveform containing steep amplitude changes should be avoided as this may cause decoding errors.

Comparing Figure 4 with Figure 6, one can observe that the magnitude of the reader's transmitted signal is much greater than the tag's backscattered signal. Therefore, the actual data containing signal are buried in the time-varying amplitude. Consequently, no decoding can be performed without removing the time-varying continuous wave.

4.2. Eavesdropper's Intercepted Signal

For the adversary who lacks the knowledge of the time-varying waveform cannot subtract the transmitted waveform to obtain tag's signal, since our varying amplitude is equal or faster than tag's data rate. As shown in Figure 8 and 9, the tag's signal are collided with readers varying amplitude signal. Note that the recovery of these collided signal waveforms can be viewed as the collision problem. Since attackers may only know step

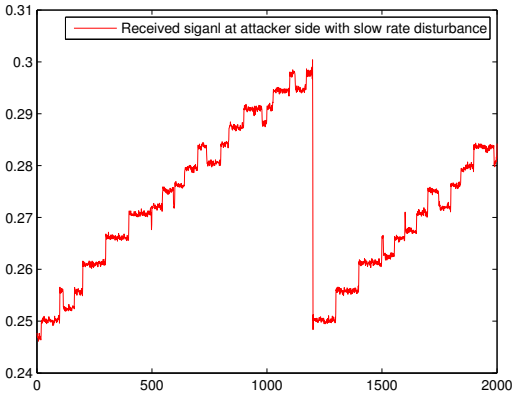

Figure 8. Received signals with slow rate disturbance

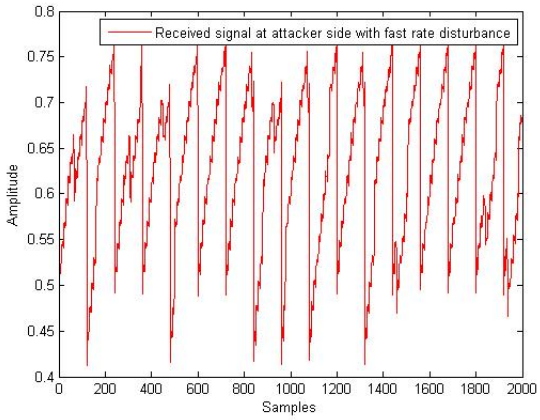

Figure 9. Received signals with fast rate disturbance

function time period for each step, the uncertainty to remove disturbance in this scenario will be related to the numbers of level which step function can achieve. In here, we use 12 levels increasing step function for illustration purposes. In reality, randomly amplitude step functions should be used that comply with our framework.

As discussed earlier, the more number of amplitude levels for continuous waveforms readers can have, the closer it is for the adversary to have a decoding error rate of 50%. However, there exists tradeoffs between the number amplitude levels and the system performance of the legitimate parites. For example, having amplitudes below a certain threshold would cause tags to unable harvest the energy, because it is below the detection range of the tag. This tradeoff will be studied in our future work.

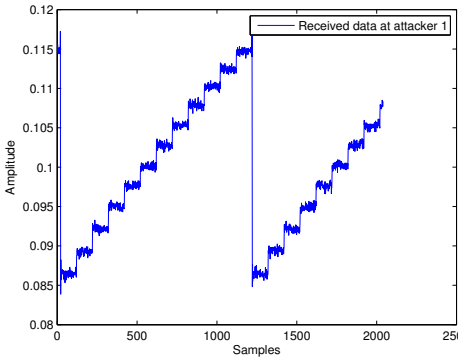

Figure 10. Attacker 1's received signal

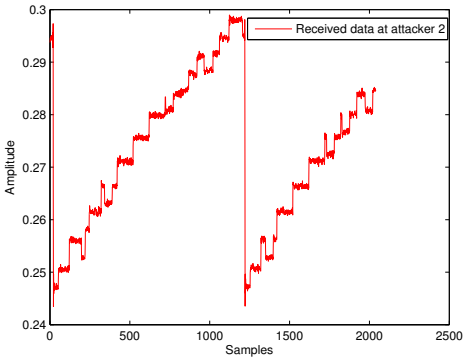

Figure 11. Attacker 2's received signal

5. Discussions on Stronger Attacks

In this section, we explore two stronger forms of attackers. The multiple passive colluding eavesdroppers and the active eavesdropping attack.

5.1. Multiple Passive Colluding Eavesdroppers

Up till this point, we have assumed that there exists only one adversary in the system. We have already shown our proposed scheme is resilient against this attack model. Now, we consider the attack model where there exist multiple passive colluding eavesdroppers. First, we consider the presence of two passive colluding eavesdroppers in the system. Other assumptions remain unchanged.

We have re-conducted the experiment by adding another reader as the second eavesdropper with the exact same setup as the legitimate reader and the eavesdropper 1. We have used the same step functions for transmitted time-varying signal used by the reader as shown in Figure 2. The expected return response from the tag is still 0101, 0011, 0001, 0010. Furthermore, we placed the eavesdropper 1's receiving antenna close to the reader's transmitting antenna and attacker 2's receiving antenna close to the tag. We hypothesize this setup provides the two eavesdropper with the best chance. The reason is when the receiving antenna is placed close to the reader, the intercepted signal is highly correlated to the time-varying signal, the signal strength of the backscattering modulation from the tag is considerably weaker. From this, the adversary 1 has the complete knowledge of transmitted time-varying waveform. When the receiving antenna is placed close to the tag, then the signal of tag's backscattered data should be very strong. From this, the adversary has the complete knowledge of superimposed signals. Decoding is possible when the two adversaries collude together.

Figures 10 and 11 are intercepted signals by the adversary 1 and 2 respectively. By observing Figures 10 and 11, we see that our hypothesis is true.

When two adversaries are able to collude together and assuming their clocks are fully synchronized, from the intercepted the signals, they make an attempt to remove the time-varying signal as shown in Figure 12. The two eavesdroppers would decode the waveform in Figure 12 into binary data which exactly matches the tag's returned data. Therefore, it is possible to decode the messages. When even more eavesdroppers are

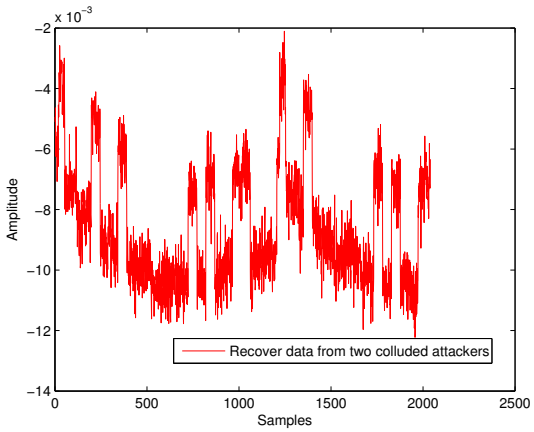

Figure 12. Recovered data by two colluding attackers

present in the system and they all can freely collude with each other, then we expect their decoding ability to be even greater. Thus, this scheme is vulnerable to multiple colluding eavesdroppers. However, if we add the detection functionality in the reader which can detect the adversaries that are present using the method in [8], then this attack can be prevented.

5.2. Active Eavesdropping

We now consider a scenario where the attacker no longer just passively eavesdrops the communication session, but rather he is actively sending out signals in hopes to obtain useful information. This attack was first introduced in [2]. The attack targets the vulnerability in the RFID system design. The two most important criterion of a RFID system are: 1). It needs to be very convenient (the tag can be easily read and accessed by the reader). 2). The tags needs to be inexpensive. By design, RFID tags respond to whoever makes the query through a simple backscattering modulation. The adversary could exploit this property, after the reader has issued command to the tag, the adversary sends out his own continuous waveform at a different frequency than the legitimate reader's frequency. This frequency however has to be within the allowed range of the tag. The tag's received waveform would be the superposition of the two signals. However, the tag does not check the existence of the signal from the adversary. He simply performs the backscattering modulation and returns the data signal. Once the eavesdropper receives the backscattered signal, he first use a bandpass to filter out the legitimate reader's signal, leaving only his own frequency component of the signal. The adversary can then successfully recover the response of the tag. Thus, this scheme is also vulnerable to this attack theoretically.

6. Conclusions and Future Work

In this paper, we have presented a framework which exploits the physical nature of RFID system. This framework allows the messages to be securely transmitted from the tag to

the reader in the presence of one passive eavesdropper. Thus, the secrecy of the messages and the privacy of the tag is ensured. This framework is easy to implement and requires no pre-sharing of any secrets between the reader and the tag. We have conducted the theoretical analysis and demonstrated that the theoretical decoding error probability of the adversary without knowing the time-varying waveform is close to 50% for reasonable number of steps m. Two experiments were also performed, results from these two experiments confirm with our theoretical results. We think this framework can be implemented to the existing RFID networks to provide an additional layer of security against the eavesdropping attack.

This framework is still vulnerable to multiple colluding adversaries and active eavesdropper attacks, which are two stronger forms of attack. These two attacks can be prevented by secure encryption primitives. However, we have reasoned this is either infeasible in the case of public key encryption or insecure in the case of symmetric key encryption. Related works we presented earlier which add a separate noise source too are all vulnerable to these two attacks. As a future work, we intend to consider stronger attack model with multiple colluding adversaries who are capable to conduct active eavesdropping attack.

In addition to detecting passive eavesdroppers, another potential method to thwart the multiple colluding adversaries is to adopt the beamforming approach. Due to the constructive and destructive interferences of the signal, the adversary would only see a corrupted version of the signals, colluding between the different adversaries could prove to be much more difficult. Furthermore, adversaries do not know the amplitude variations of each of the legitimate reader's transmitting signals, this would greatly increases the attacker's decoding error probability. This is a future work we will consider.

Secondly, we can use this framework to design a protocol for sharing keys between the reader and the tag. When the reader needs to securely communicate with the tag, the proposed scheme can be changed to a key transport scheme, where the key obtained by the tag can be transported to the reader by hiding it in the time-varying waveform.

References

[1] F. Achard, O. Savry, A cross layer approach to preserve privacy in RFID ISO/IEC 15693 systems, *RFID-Technologies and Applications (RFID-TA)*, 2012 IEEE International Conference on , vol. 85, no. 90, pp. 5-7, Nov. 2012

[2] Q. Chai, G. Gong and D. Engels, How To Develop Clairaudience – Active Eavesdropping in Passive RFID Systems (invited), *3rd IEEE International Workshop on Data Security and Privacy in wireless Networks, D-SPAN'12*, San Francisco, CA, USA, 2012.

[3] EPCGlobal, UHF class 1 gen 2 standard v. 1.2.0. 2008.

[4] A. Grover and H. Berghel, A survey of RFID deployment and security issues. *Journal of information processing systems*, vol. 7, no. 4, pp. 561–580, Dec. 2011.

[5] Impinj, *RFID reader evaluation kit*, Available: http://www.impinj.com/Speedway_Reader_Evaluation_Kits.aspx.

[6] A. Juels, RFID security and privacy: A research survey. *Journal of Selected Area in Communication (J-SAC)*, vol. 24, no. 2, pp, 381–395, 2006.

[7] O. Savry, F. Pebay-Peyroula, F. Dehmas, G. Robert, The RFID Noisy Reader: How to prevent from the eavedropping on the communication?, *In P. Paillierand I.Verbauwhede, editors, CHES07*, vol. 4727 of LNCS,.Springer, 2007.

[8] B. Wild and K. Ramchandran, Detecting primary receivers for cognitive radio applications, In *Proc. IEEE Int. Symp. DySPAN*, pp. 124-130, Nov. 2005.