How To Develop Clairaudience – Active Eavesdropping in Passive RFID Systems

Qi Chai and Guang Gong
Department of Electrical & Computer Engineering
University of Waterloo
Waterloo, ON, Canada N2L 3G1
{q3chai,ggong}@uwaterloo.ca

Daniel Engels
Revere Security
4500 Westgrove Drive, Suite 335
Addison, TX 75001, USA
daniel.engels@reveresecurity.com

***Abstract*—The large operation range of passive RFID systems and the ubiquitous deployment of passive tags introduce growing security and privacy threats such as tag skimming/tracking/cloning, in which eavesdropping the communication between the legitimate reader and the victim tag to obtain raw data is a basic tool for the adversary. However, given the fundamentality of eavesdropping, there are limited work investigating its intension/extension for passive RFID systems.**

In this work, we identify a brand-new attack at physical layer, called *Unidirectional Active Eavesdropping*, which defeats the customary impression that eavesdropping is a "passive" attack. In this attack, the adversary transmits an un-modulated carrier at a certain frequency, while a valid reader and a tag interacts at another frequency. When a passive tag modulates the amplitude of reader's signal, it causes fluctuations on the blank carrier as well. By carefully examining the amplitude of the backscattered version of both blank carrier and reader's carrier, the eavesdropper is able to recognize tag's responses more confidently. Besides the formalization and the theoretic analysis, we set out to fill the literature's gap by demonstrating this new attack towards a popular family of passive RFID systems, namely EPCglobal UHF Class-1 Gen-2, using software-defined radio devices and a programmable passive tag. Our empirically results further confirm that the active eavesdropping achieves a significant improvement in the reliability of the intercepted communication.

***Keywords*-RFID systems; passive tags; active eavesdropping;**

I. Introduction

Passive Radio Frequency IDentification (RFID) is an emerging technology, which enables contactlessly identification of physical objects more than ten meters away without requiring line-of-sight. However, the large operation range of passive RFID systems and the ubiquitous deployment of passive tags introduce growing security and privacy concerns regarding the possible release of the bearers' information. Some of the attacks identified in the literature, e.g., [6], [7], [9], are *tag skimming*, *tag tracking*, *tag cloning* and *mafia-fraud*. Thus far, to launch these attacks, *eavesdropping* the communication between the legitimate reader and the victim tag to obtain raw data is a basic tool for the adversary.

Nevertheless, given the fundamentality of eavesdropping attacks, there are limited prior work investigating its intension and extension for passive RFID systems. One possible reason is that the stereotyped thinking patterns lead people to believe that eavesdropping can be simply solved by encryption and decryption. However, while they are indeed sound paradigms to protect majority wireless communication systems from eavesdroppers, they may fail to work for passive RFID systems, because of the following three factors: (1) due to the modest computation/storage capabilities and the necessity to keep its prices low, passive tags are unlikely to perform even symmetric encryptions in the recent future. Although dedicated designs of lightweight block/stream ciphers are under development, e.g., [1], [10], the practical security they can offer is not very clear to date [11], [2]; (2) encrypting plaintext before transmission introduces the key management – key generation/distribution/storage/revoking/updating, which seems overkill for low-cost tags; and (3) providing a tag responds a reader with symmetric-encrypted data, the reader has to go through the entire key set to find a valid key for authentication and decryption, which, known as *key search problem* [6], results in a poor scalability. Considering the facts above, the de facto standard of passive RFID systems, called EPCglobal UHF Class-1 Gen-2 (known as EPC Gen2) [4], does not include encryption/decryption as a part. Therefore, *eavesdropping attack in this specific scenario seems like an animal with no natural enemies*, and better understanding of how a smart eavesdropper works and how powerful he could be is quite necessary.

Contribution: In this work, we investigate the eavesdropping attack for passive RFID systems where encryption/decryption is unavailable. To this end, we constrain ourselves to the tag-to-reader channel, since a reader-to-tag channel can be viewed as a conventional broadcast communication which is more well-understood. Besides, we treat EPC Gen2 as a representative of passive RFID systems in our research and we focus more on its physical layer rather than its logic layer. To be specific:

- We identify a brand-new attack, called *Unidirectional Active Eavesdropping*, which defeats the customary impression that eavesdropping is a "passive" attack. During the active eavesdropping attack, the adversary transmits an un-modulated carrier (call it *blank carrier* hereafter) at a certain frequency $f_{\mathcal{E}}$, while a valid reader and a tag are talking at another frequency channel

978-1-4673-1239-4/12/$31.00

$f, f \neq f_{\mathcal{E}}$. When the tag modulates the amplitude of reader's signal, it causes fluctuations on the blank carrier as well. By carefully examining the amplitude of the backscattered version of both blank carrier and reader's carrier, the eavesdropper is able to recognize tag's responses more clearly.

- We set out to fill the literature's gap by demonstrating the active eavesdropping towards the passive RFID system in compliant with a popular standard, namely EPC Gen2 [4], through software-defined radio devices and a programmable passive tag. Our experimental results show a significant improvement in the bit error rate (BER) of the intercepted communication as long as active eavesdropping is mounted.

Organization The rest of this paper is structured as follows. Section II introduces preliminaries and summarizes the related work. In Section III, we formalize the active eavesdropping attack and provide the theoretic analysis. Empirical study of this attack is exhibited in Section IV. Section V concludes this paper.

II. Preliminaries and Background

Before an in-depth discussion of the eavesdropping problem, we present the system model and attacker model, and introduce the backscattered communication that forms the basis of our attack. At last, we summarize the related work.

A. System Model and Adversary Model

System Model: Our system encompasses three roles: a legitimate reader $\mathcal{R}$, a victim tag $\mathcal{T}$ and a computationally-bounded adversary $\mathcal{E}$. The mutual distance between the tag and the reader (adversary resp.) is $D_{\mathcal{T},\mathcal{R}}$ ($D_{\mathcal{T},\mathcal{E}}$ resp.). We assume that $\mathcal{R}$ and $\mathcal{T}$ with public configuration parameters involved in the RF communication do trust each other and are not compromised. In addition, $\mathcal{R}$ and $\mathcal{T}$ communicate over a frequency f choosing from a set $\{f_1, ..., f_K\}$. Since there is only a single tag in our system, the signal collision caused by multiple and simultaneous responses from different tags are ignored.

Adversary Model: The goal of $\mathcal{E}$ is to acquire or intercept tag-to-reader communication, i.e., $\mathcal{E}$ receives, demodulates and decodes analog RF signals backscattered by $\mathcal{T}$ by using its RF receiver (call it $Rx_{\mathcal{E}}$ hereafter) working at a proper frequency. We assume that $Rx_{\mathcal{E}}$ has a fixed gain throughout the rest. Additionally, $\mathcal{E}$ is free to "actively" transmit any well-designed signals (without concerning about the energy cost) by using its RF transmitter (call it $Tx_{\mathcal{E}}$ hereafter). Note that there could be more than one $Rx_{\mathcal{E}}$ and more than one $Tx_{\mathcal{E}}$, which are not necessary to situate in one physical location. That is saying, the adversary deploys/distributes (a set of) $Rx_{\mathcal{E}}$ and (a set of) $Tx_{\mathcal{E}}$ at his will, while all of these devices can be centrally coordinated.

However, unlike a Dolev-Yao attacker, $\mathcal{E}$ cannot control the communication channel between $\mathcal{R}$ and $\mathcal{T}$, i.e., $\mathcal{E}$ cannot insert and remove messages to/from the tag-to-reader communication channel and $\mathcal{E}$ cannot relay the tag-to-reader communication. Moreover, we assume that, $\mathcal{E}$ desires to keep the entire eavesdropping procedure undetected.

B. Backscattering Communication

Passive RFID system is principally a radar system in which the reader provides the RF signal for communications in both directions. The tag has no power source, but harvests the impinging power from the reader's carrier waves and also on which to modulate its responses. To be formal, the reader initially broadcasts an amplitude-modulated carrier, say, $CW(t) = A(t)\cos(2\pi ft + \theta)$, where f is the carrier frequency in $\{f_1, ..., f_K\}$ and θ is a constant phase of the carrier. $A(t)$, constituting of a high level and a low level, carries the binary command to be issued to the tags. Once a command is propagated, the reader keeps $A(t)$ at the high level expecting the tags' responses.

The tag, after receiving the operating energy from $CW(t)$, uses an envelope detector to obtain and decode the command in $A(t)$ if there is any. To response, the tag maps the source message bits into baseband codewords using a Manchester-alike-code to enable the collision detection on the reader's side. For example, FM-0 code, as specified in [4], uses two bits $(0, 1)$ and $(1, 0)$ alternatively to represent a "0" bit, and uses $(0, 0)$ and $(1, 1)$ alternatively to represent an "1" bit.

In order to backscatter the encoded response, the tag next switches the reflection coefficients by changing its antenna impedance within two states (Δ_0, Δ_1), $0 < \Delta_0 < \Delta_1 < 1$, at a given rate. The backscattered signal can be written as:

$$BCW(t) = \Delta_i \sqrt{2E_{\mathcal{T}} v_{\mathcal{T}}} \cos(2\pi ft + \theta), \quad i = 0, 1,$$

where $E_{\mathcal{T}}$ is the energy per bit presented at the tag's antenna when $CW(t)$ with $A(t)$ at the high level is transmitted by the reader, $v_{\mathcal{T}}$ is the tag's data rate and $\Delta_1 > \Delta_0$ implying more power is backscattered when transmitting a "1" of the codeword. The reader, centering its receiver at f, coherently detects the responses by correlating the amplitude of $BCW(t)$ to potential codewords and comparing the resulting correlations with a particular threshold, which allows the establish of the backscatter communication.

C. Related Work

Hancke in [5] experimentally confirmed that two NFC standards, namely, ISO 14443A/B and ISO 15693, where the designed operational range is less than 10cm, are eavesdroppable even the attacker is 3.5m away. Dobkin in [3] reported testing results of intercepting a regular EPC Gen2 tag's reply approximately 7m away in an office environment. Our work follows Dobkin's preliminary research and discloses more. Recently, Koscher *et al.* in [8] particularly examined the security, under skimming attack, towards the United States Passport Card and Washington State enhanced drivers license, both of which incorporate EPC Gen2 tags. In their

demonstrations, the maximum distance a tag can be read by a rogue reader radiating 36dBm power is measured. However, skimming is different from eavesdropping in the sense that the skimmer does provide energy to the tag through the carriers it propagates. Thus, testing results on the skimming does not provide convincible results on the eavesdropping.

III. Unidirectional Eavesdropping: From Passive To Active

In this section, we introduce our novel concepts in eavesdropping by providing theoretic analysis of both passive eavesdropping and active eavesdropping. To produce meaningful results, we make use of the bit error rate (BER) as the main metric to evaluate the communication reliability.

A. Passive Eavesdropping

Let us first consider the BER of an RF receiver in general. In the current setting, this RF receiver is a passive eavesdropper. However, the results derived here are also applicable to the case where the RF receiver is the legitimate RFID reader itself. Assume the energy per bit at $\mathcal{R}$'s antenna is $E_{\mathcal{R}}$, the backscattered signal received by the eavesdropper is, if a bit $i \in \{0,1\}$ is sent,

$$\begin{aligned} BCW_{\mathcal{E}}(t) &= \Delta_i \sqrt{2E_{\mathcal{R}} v_{\mathcal{T}}} \cos(2\pi f t + \theta) \\ &= \Delta_i \sqrt{2E_{\mathcal{T}} v_{\mathcal{T}} \times \frac{\eta}{D^2_{\mathcal{T},\mathcal{E}}}} \cos(2\pi f t + \theta). \end{aligned}$$

The last equality is from the Friis transmission equation, i.e., $\frac{E_{\mathcal{R}}}{E_{\mathcal{T}}} = \frac{\eta}{D^2_{\mathcal{T},\mathcal{E}}}$, where η is a constant proportional to the multiplication of antenna gains of both parties and the square of the wavelength. Unsurprisingly, the attacker could keep employing antennas with higher gains to compensate for the loss of η because of the increase of $D_{\mathcal{T},\mathcal{E}}$. However, we treat η as a constant to simply the analysis.

Hence, according to the minimum distance detection method, the BER of the backscatter modulation, the main metric for the reliability of the eavesdropper, is given by

$$\begin{aligned} p_E &= Q\left(\frac{\Delta_1\sqrt{E_{\mathcal{T}} \times \frac{\eta}{D^2_{\mathcal{T},\mathcal{E}}}} - \Delta_0\sqrt{E_{\mathcal{T}} \times \frac{\eta}{D^2_{\mathcal{T},\mathcal{E}}}}}{\sqrt{N_o}}\right) \\ &= Q\left(\frac{(\Delta_1 - \Delta_0)\sqrt{\eta E_{\mathcal{T}}/N_o}}{D_{\mathcal{T},\mathcal{E}}}\right), \end{aligned} \quad (1)$$

where Q is the one minus the cumulative distribution function of the standardized normal random variable and N_o is the noise power density in the channel. As can be seen, as long as Δ_0, Δ_1, η, $E_{\mathcal{T}}$ and N_o are given and fixed, the errors in the intercepted messages grows rapidly when $D_{\mathcal{T},\mathcal{E}}$ increases. This observation corresponds the intuition that the greater the distance between the tag and the passive eavesdropper, the less reliable the intercepted communication is.

B. Active Eavesdropping

To combat the loss of reliability, a strategic adversary may consider *active eavesdropping*, which is effective towards the backscatter communication. Through the sequel, we formalize this attack and demonstrate how the eavesdropper obtains a better BER performance.

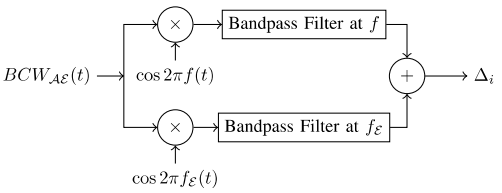

Figure 1. Receiver Structure for Active Eavesdropping.

In addition to the aforementioned RF receiver, the eavesdropper, denoted as $\mathcal{AE}$, has an RF transmitter working at $f_{\mathcal{E}}$, $f_{\mathcal{E}} \neq f$, which produces a *blank carrier* while a valid reader-tag communication is ongoing, i.e.,

$$CW_{\mathcal{AE}} = \sqrt{2E_{\mathcal{AE}} v_T} \cos(2\pi f_{\mathcal{E}} t + \theta')$$

where $E_{\mathcal{AE}}$ is a constant to make the amplitude of the blank carrier (presented at the tag's antenna), i.e., $\sqrt{2E'_{\mathcal{T}} v_{\mathcal{T}}}$, suitable. When the tag amplitude-modulates reader's signal as aforementioned, it causes fluctuations on the blank carrier as well, which can be written as:

$$\begin{aligned} BCW_{\mathcal{AE}}(t) &= \Delta_i \sqrt{2E_{\mathcal{T}} v_{\mathcal{T}} \times \frac{\eta}{D^2_{\mathcal{T},\mathcal{AE}}}} \cos(2\pi f t + \theta) \\ &+ \Delta_i \sqrt{2E'_{\mathcal{T}} v_{\mathcal{T}} \times \frac{\eta(f_{\mathcal{E}})}{D^2_{\mathcal{T},\mathcal{AE}}}} \cos(2\pi f_{\mathcal{E}} t + \theta'), \end{aligned}$$

where $E'_{\mathcal{T}}$ is the energy per bit at $\mathcal{T}$'s antenna resulted by the blank carrier. It is worthy to mention that $\eta(f_{\mathcal{E}})$ is no longer a constant as, even the eavesdropper could keep his gain at a constant level (by switching to a proper antenna), the tag's antenna is unlikely to maintain the same gain under different $f_{\mathcal{E}}$. For example, if $f_{\mathcal{E}}$ is totally out of the effective region of the tag's antenna, e.g., $f_{\mathcal{E}} = 10$KHz, $\eta(f_{\mathcal{E}})$ decreases to 0. Different tags may results in different $\eta(f_{\mathcal{E}})$ (which can be obtained through the VSWR graph of its antenna). A crucial observation here is that, for most of the antennas, although optimized for a particular frequency band, e.g., 902-928MHz, the gain remains almost the same if $f_{\mathcal{E}}$ is not too far away from this designed band, e.g., $860 \leq f_{\mathcal{E}} \leq 960$MHz. Principally, if the tag has a quadband UHF antenna, we could even actively eavesdrop it with $f_{\mathcal{E}} = 1.8$GHz. In the rest, we say $f_{\mathcal{E}}$ is *effective* iff $\eta(f_{\mathcal{E}}) \approx \eta(f), f \in \{f_1, f_2, ..., f_K\}$.

As long as $BCW_{\mathcal{AE}}(t)$ is intercepted, it is passed through two filters centered at f and $f_{\mathcal{E}}$ respectively as shown in Figure 1. The resulting baseband signals are then added up.

From the signal constellation's point of view, the eavesdropper obtains a constellation of two points (representing signals for bit "1" and bit "0" respectively), that are separated by a minimum distance of

$$(\Delta_1 - \Delta_0)\left(\sqrt{E_{\mathcal{T}} \times \frac{\eta}{D^2_{\mathcal{T},\mathcal{AE}}}} + \sqrt{E'_{\mathcal{T}} \times \frac{\eta(f_{\mathcal{E}})}{D^2_{\mathcal{T},\mathcal{AE}}}}\right).$$

C. Reliability of Active Eavesdropping

In parallel to Eq. (1), the active eavesdropper's BER performance is

$$p_{\mathcal{AE}} = Q\left(\frac{(\Delta_1 - \Delta_0)(\sqrt{\eta E_{\mathcal{T}}/N_o} + \sqrt{\eta(f_{\mathcal{E}})E'_{\mathcal{T}}/N_o})}{D_{\mathcal{T},\mathcal{AE}}}\right) \quad (2)$$

which suggests that, for an effective $f_{\mathcal{E}}$, the eavesdropper is always able to tune $E_{\mathcal{AE}}$ to get a suitable $p_{\mathcal{AE}}$.

IV. Implementation and Testing of Active Eavesdropping Attack

A. System Design

To validate our concept of unidirectional active eavesdropping, we developed a prototype system, as shown in Figure 2, that encompasses four roles: one legitimate reader, one legitimate tag, one $Rx_{\mathcal{E}}$ for the eavesdropper and one $Tx_{\mathcal{E}}$ for the eavesdropper. Note that our system evaluates two basic topologies as shown – in Scenario I, all components are located in a straight line; in Scenario II, the reader and the tag reside on the y-axis while $Tx_{\mathcal{E}}$ and $Rx_{\mathcal{E}}$ are located on the x-axis. In what follows, we detail each component.

Gradients from Software Defined Radio: To enable flexibility, the *Universal Software Radio Peripheral* (USRP) is employed to build up programmable transmitters/receivers working at UHF band. Roughly speaking, the USRP, in conjunction with the daughterboard `RFX900` it carries, constitutes a low-cost RF transceiver with freely available schematics and drivers. In the receiving path, `RFX900` captures raw UHF signals and converts them to the intermediate frequency (IF) band and passes them to the USRP board, which further samples/converts them to baseband signals by an analog-to-digital converter and a digital-down-converter. The baseband digital signals out of USRP are sent via USB 2.0 (for USRP-1) or Ethernet cable (for USRP-2) to the laptop running GNU Radio, a toolkit for signal processing. The transmitting path proceeds in a similar way.

RFID Reader: We used an USRP-N210, in conjunction with one `RFX900` carrying two VERT900 dipole antennas, to play the role of the legitimate reader. We developed a script to create and control a signal flow graph to enable this reader: (1) querying a tag by propagating a constant sine wave working at 915MHz with maximum possible power that does not result in RF clipping, i.e., 23dBm, through one dipole antenna; and (2) collecting the reflected signal through another dipole antennas. The script runs on a MacBook MC516LL with OS X 10.4 and communicates

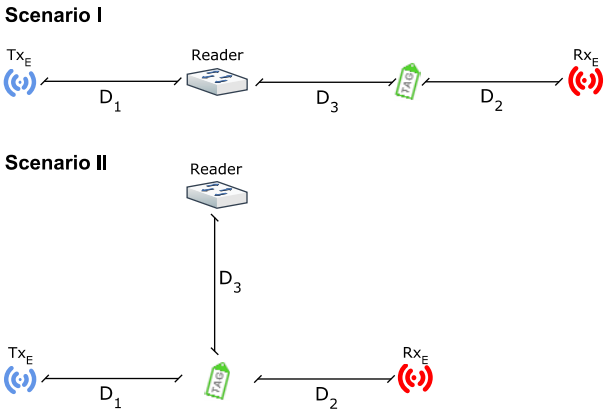

Figure 2. Our prototyping system to evaluate eavesdropping attacks.

with the USRP-N210. Note that, we intentionally keep this reader as functionally simple as possible, since, in this work, we do not care much about how the reader interacts with a tag at the logic layer.

Eavesdropper's Transmitter: This transmitting part is realized by another USRP-N210 in conjunction with one `RFX900`, where the later carries a circular polarity panel antenna. Similarly, in our script, we enable this $Tx_{\mathcal{E}}$ propagating a sine wave with a tunable center frequency $f_{\mathcal{E}}$ and a tunable amplitude amp. Furthermore, $Tx_{\mathcal{E}}$ connects to a Thinkpad T410 laptop. Note that USRPs use a positive number, called *scale factor*, to represent the amplitude of a signal without unit. The actual measures of the output voltages at port `TX/RX` of `RFX900` (without antenna) w.r.t. the scale factors are provided in Table I.

Table I
Actual measures of the output voltages at port `TX/RX` of `RFX900` w.r.t. the scale factors of USRP-1/USRP-N210.

scale factor (USRP-1)	scale factor (USRP-N210)	output voltage
1000	0.01	396mv
2000	0.05	864mv
3000	0.1	864mv
5000	0.2	2.124v
6500	0.5	2.400v
10000	0.8	2.880v

Eavesdropper's Receiver: To build a powerful $Rx_{\mathcal{E}}$, we make use of an USRP-1 together with two `RFX900`s carrying an dual polarization horn antenna effective from 700MHz-6GHz each. A script is created to parse and process the received signals according to the two-branch receiver as shown in Figure 1. For each branch, the gain of the receiver's antenna is set to 20dB, and the received signal is decimated by the USRP-1 with a factor of 32. In addition, the decimated signals are again filtered by an 8-th order low-pass filter with gain 2 and cutoff frequency 400KHz, respectively. Finally, the two baseband signal are added and stored for the later analysis. Note that, to enable the

collaboration between $Tx_{\mathcal{E}}$ and $Rx_{\mathcal{E}}$, we connect $Rx_{\mathcal{E}}$ to the same Thinkpad T410.

Passive RFID Tag: The unique properties owned by a passive tag are the key for our experiments. To this end, we made use of WISP v4.1 tag [12] – a full-fledged passive tag not only supports energy harvesting, ephemeral energy storage and backscatter communication, but also provides programmability. Each WISP is operated by a 16-bit general purpose microcontroller, MSP430F2132, the programs for which were written in embedded C and compiled, debugged and profiled using IAR Embedded Workbench 5.10.4. As an additional benefit, WISP is shipped with the firmware, which implements a significant portion of EPC Gen2 commands. For our purpose, we tweaked this firmware and let the tag transmit a random binary sequence (further encoded by Miller-4 code) at 64kbps as long as there is available power.

Environment: In reality, multi-path effects and interferences from other RF transmitters nearby is an enemy for our proof-of-concept experiments. We primarily reduced the communication range of regular passive RFID systems (by controlling the energy level of the reader and the eavesdropper), and conducted the experiments in a microwave anechoic chamber of size 2.7m(L) $\times$ 1.5m(W) $\times$ 1.9m(H), which is a shielded room insulated from exterior sources of noise, and whose walls have been covered with a material that scatters or absorbs so much of the incident energy to simulate free space. In addition, we placed the devices on a horizontal surface in the chamber and let $D_1 = 65\text{cm}, D_2 = 83\text{cm}, D_3 = 48\text{cm}$ for Scenario I; $D_1 = 89\text{cm}, D_2 = 107\text{cm}, D_3 = 48\text{cm}$ for Scenario II.

B. Testing Results

In the testings, we varied the center frequency $f_{\mathcal{E}}$ of $Tx_{\mathcal{E}}$ and $Rx_{\mathcal{E}}$ around 915MHz and tuned the transmitting power of $Tx_{\mathcal{E}}$, e.g., by setting the scale factor from 0.1 to 0.5. The partial results for Scenario I and Scenario II are recorded in Figures 4 and 5 respectively. Note that, to enable clear analysis, we independently plot the signals go through the two branches in our receiver in these two figures: (1) the signals go through the upper branch (that mixing $\cos 2\pi f(t)$ and filtering at f) are exhibited in Figure 3, which can be seen as the results of a conventional passive eavesdropping; (2) the signals go through the bottom branch are exhibited in Figures 4 and 5, which are the results of eavesdropping using the blank carrier only. Note that the results obtained by the attacker should be the addition of signals in both branches. Moreover, each short column represents a backscattered signal from the WISP tag that contains a random binary sequence of 16 bits.

As can be seen in these figures, active eavesdropping is surprisingly effective as, for example, in Scenario I, the eavesdropper could get a view of the tag's response at $f_{\mathcal{E}} = 875\text{MHz}$ with $amp = 0.5$ as clear as the ones he gets by passively eavesdropping at $f_{\mathcal{E}} = 875\text{MHz}$, which implies, when adding up these two signals, the minimum distance in his signal constellation regarding the tag's responses is doubled, which results in a significant decrease (increase resp.) in his BER (reliability resp.). A similar phenomenon happens in Scenario II, which further confirms our theoretic analysis in the previous section.

By a vertical comparison of these plots, we can see clearly that the antenna of the WISP performs best when $f_{\mathcal{E}} = 875\text{MHz}$ and 900MHz. Besides, as we tested (but omitted from the figures due to the space limit) , it can work at $f_{\mathcal{E}} = 960\text{MHz}$ if a strong stimuli is given and a regular reader-tag communication can be jammed if $Tx_{\mathcal{E}}$ works at 915MHz. This observation ensures our previous definition and discussion about the effective region of UHF tags. By a horizontal comparison of these plots, we can see clearly that the amplitude of the backscattered signals do not have a simple linear relation with respect to the amplitude of the blank carrier. For example, the second row in Figure 4 indicates when $amp = 0.5, 0.2, 0.1$, the amplitude of the backscattered signals are almost the same, albeit the amplitude of the blank carrier as received by $Rx_{\mathcal{E}}$ show significant difference. In addition, if the signal emitted by $Tx_{\mathcal{E}}$ is to weak, e.g., $amp \leq 0.1$, it gets lost during the propagating and hardly results in meaningful responses in $Rx_{\mathcal{E}}$. By scenario-wise comparison, we found, although it is intuitive that attacker in Scenario I could achieve better benchmarks, there is essentially no much difference. A possible explanation is that: we can consider the reader and the tag as one unit – an active tag, which is interrogated by $Tx_{\mathcal{E}}$ and $Rx_{\mathcal{E}}$. Since $Tx_{\mathcal{E}}$ and $Rx_{\mathcal{E}}$ are always placed in one line and both of them use directional antennas, two scenarios can be essentially reduced to one more basic scenario.

V. Concluding Remarks

In this paper, we introduce, formalize, analyze and demonstrate a novel physical-layer attack called unidirectional active eavesdropping, which takes advantage of the unique characteristics of the passive RFID systems and brings the eavesdropper to his full potential.

Due to the space limit, the following results will be given in the full version of this work: (1) the attacker's strategies to perform active eavesdropping; (2) a lightweight countermeasure of a particular kind of active eavesdropping (though it is not trivial to be prohibited in general); and (3) more quantitative results based on our current settings.

Acknowledgement

The experiments on active eavesdropping attacks are conducted in the RF chamber of DBJay Ltd., and the first two authors wish to thank Dr. Fred Yu for his tremendous help and support for conducting those experiments. This research is supported by NSERC SPG and ORF-ER.

Figure 3. Testing Results of Passive Eavesdropping (Scenario I/II) in an Anechoic Chamber

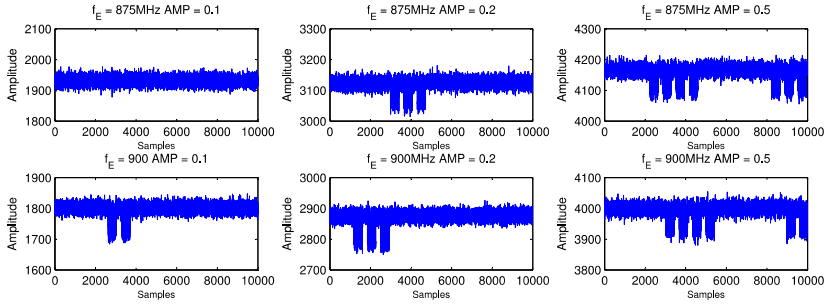

Figure 4. Testing Results of Active Eavesdropping (Scenario I) in an Anechoic Chamber

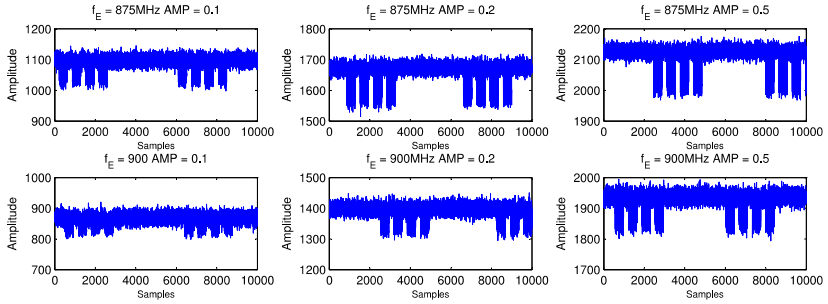

Figure 5. Testing Results of Active Eavesdropping (Scenario II) in an Anechoic Chamber

REFERENCES

[1] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin and C. Vikkelsoe, PRESENT: an ultra-lightweight block cipher, *Cryptographic Hardware and Embedded Systems, CHES'07*, LNCS 4727, pp. 450–466, 2007.

[2] N. Courtois, G. Bard and D. Wagner, Algebraic and slide attacks on KeeLoq, *Fast Software Encryption, FSE'08*, LNCS 5086, pp. 97–115, 2008.

[3] Daniel M. Dobkin, UHF reader eavesdropping: intercepting a tag reply, *http://www.enigmatic-consulting.com/ Communications_articles/RFID/Tag_intercept.html*.

[4] EPC Global, Class 1 Generation 2 UHF air interface protocol standard v1.2, *http://www.epcglobalinc.org*, 2008.

[5] G. Hancke, Eavesdropping attacks on high-frequency RFID tokens, *In Proceedings of the 4th Workshop on RFID Security, RFIDSec'08*, pp. 1–14, 2008.

[6] A. Juels, RFID security and privacy: a research survey, *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 2, pp. 381–394, 2006.

[7] T. Karygiannis, B. Eydt, G. Barber, L. Bunn and T. Phillips, Guidelines for securing radio frequency identification (RFID) systems, *NIST Special Publication*, vol. 80, pp. 1–154, 2007.

[8] K. Koscher, A. Juels, V. Brajkovic and T. Kohno, EPC RFID tag security weaknesses and defenses: passport cards, enhanced drivers licenses, and beyond, *In Proceedings of the 16th ACM conference on Computer and Communications Security, CCS'09*, pp. 33–42, 2009.

[9] Y. K. Lee, L. Batina, D. Singelée and I. Verbauwhede, Low-cost untraceable authentication protocols for RFID, *In Proceedings of the third ACM conference on Wireless network Security, WiSec'10*, pp. 55–64, 2010.

[10] Y. Luo, Q. Chai, G. Gong and X. Lai, WG-7, a lightweight stream cipher with good cryptographic properties, *IEEE Global Telecommunications Conference, GLOBECOM'10*, pp.1–6, 2010.

[11] K. Nohl, D. Evans, S. Starbug and H. Plotz, Reverse-engineering a cryptographic RFID tag, *17th USENIX Security Symposium, USENIX'08*, pp. 185–194, 2008.

[12] WISP Tag, *http://wisp.wikispaces.com*, 2011.