Computer Science and Artificial Intelligence Laboratory

Technical Report

MIT-CSAIL-TR-2013-001 January 12, 2013

Securing Deployed RFIDs by Randomizing the Modulation and the Channel

Jue Wang, Haitham Hassanieh, Dina Katabi, and Tadayoshi Kohno

massachusetts institute of technology, cambridge, ma 02139 usa — www.csail.mit.edu

Securing Deployed RFIDs by Randomizing the Modulation and the Channel

Jue Wang MIT
Haitham Hassanieh MIT
Dina Katabi MIT
Tadayoshi Kohno University of Washington

Abstract

RFID cards are widely used today in sensitive applications such as access control, payment systems, and asset tracking. Past work shows that an eavesdropper snooping on the communication between a card and its legitimate reader can break their cryptographic protocol and obtain their secret keys. One solution for this problem is to install stronger cryptographic protocols on the cards. However, RFIDs' size, power, and cost limitations do not allow for conventional cryptographic protocols. Further, installing new protocols requires revoking billions of cards in consumers' hands and facilities worldwide, which is costly and impractical.

In this paper, we ask whether one can secure RFIDs from such attacks without revoking or changing the insecure cards. We propose LocRF, a solution that changes the signal used to read the RFID cards but does not require any changes to the cards themselves. LocRF introduces a new approach that randomizes the modulation of the RFID signal as well as the wireless channel. This design protects RFIDs from eavesdroppers even if they use multi-antenna MIMO receivers. We built a prototype of LocRF on software-defined radios and used it to secure the communication of off-the-shelf cards. Both our analysis and empirical evaluation demonstrate the effectiveness of LocRF.

1. INTRODUCTION

Ultra-low power RFIDs are widely used in a variety of sensitive applications such as access control, payment systems, and asset tracking [35], [48], [12]. Some of the most well-known examples include the U.S. Passport Card, Zipcar key, MasterCard PayPass, RFID-equipped pharmaceuticals, and MBTA subway cards [28], [49], [31], [39], [30]. As a result of their ultra-low cost, ultra-low power requirements, these systems typically adopt weak encryption protocols [41], [24] or lack encryption altogether [43], leaving them widely exposed to security threats [32], [28].

Past attacks on commercial RFID systems have employed passive eavesdropping [6], [40], [13], [46]. In these attacks, an adversary snooping on the wireless medium intercepts the conversation between a legitimate RFID reader and an RFID card to obtain the sensitive data transmitted by the card. For example, the secret key in over 1 billion MIFARE Classic cards prevalently used in access control and ticketing systems today can be obtained in real-time from an overheard conversation [13]. Similarly, the cipher used in RFID-based anti-theft devices for modern cars has recently been broken in under 6 minutes based on eavesdropped information [46].

In theory, eavesdropping attacks can be addressed with more sophisticated encryption protocols than those typically used in RFIDs. Such an approach, however, would translate into more expensive, power-consuming cards, which goes against the main goal of the RFID industry, namely to dramatically reduce the cost and size of RFIDs [12]. More importantly, replacing the encryption on the cards requires revoking billions of RFIDs in consumers' hands and facilities worldwide, which is costly and impractical.

This paper introduces LocRF, a system that defends RFIDs against eavesdroppers, without modifying or revoking the cards. LocRF exploits that RFID cards do not generate their own transmission signal; they communicate by reflecting the signal transmitted by the RFID reader. In today's RFID systems the reader transmits a constant waveform $c(t)$, and a nearby card *multiplies* this waveform by its data x through reflection, producing $x \cdot c(t)$. The intuition underlying LocRF is that we can replace the reader's constant waveform, $c(t)$, by a random signal, $r(t)$. This will make the card's reflected message, $x \cdot r(t)$, appear random. Since the eavesdropper does not know the random waveform, he cannot extract the card's data from what he hears. In contrast, the reader is the one who generates the random waveform, and thus is able to decode by removing its effect.

To transform the above intuition into a practical system, we need to address a few challenges. First, simply multiplying each transmitted RFID bit by a random value does not work. The signal representing a "0" or "1" bit is not a single number; it has a pattern that differs between "0" and "1". A random multiplier per bit does not alter these patterns. Thus, in LocRF, the reader generates a random waveform $r(t)$ that destroys the internal pattern in an RFID bit, making individual bits look like white noise. We refer to this transformation of the reader's signal as random modulation.

Second, a multi-antenna MIMO adversary can still decode the RFID data. The rule of thumb in MIMO communication is: a MIMO receiver that has n antennas can decode n independent signals [45]. Thus a 2-antenna MIMO eavesdropper can decode the RFID bits despite the random multiplying signal from the reader. This is a known fundamental problem with physical layer solutions that try to hide a private signal with another signal [14], [26]. The current solution to this problem is to use at least as many antennas on the trusted device (here, the reader) as there are on the eavesdropper. This solution, however, creates an antenna battle between the reader and the eavesdropper. In this paper, we show that we can emulate a reader with many antennas by using a rotating antenna. The rotation randomizes the wireless channel from the reader to the adversary, making the reader look as if it had many antennas with different wireless channels. We demonstrate that the combination of random

channel and random modulation prevents a MIMO adversary from decoding, even if he has more antennas than the reader.

We implemented the LocRF reader on USRP software radios [23] and evaluated it with commercial RFID cards, in both the HF and UHF bands. Our evaluation reveals the following:

- Using our basic design of random modulation, a single-antenna eavesdropper that uses a maximum likelihood decoder (i.e., optimal decoder) experiences a mean bit error rate of 50% (and a standard deviation of 0.8% for HF and 2.3% for UHF), which is similar to the bit error rate when the eavesdropper is making a random guess.
- When LocRF reader transmits a random waveform, it can still decode the RFID data with the same accuracy –i.e., mean bit error rate – achieved with a constant waveform.
- Replacing the single-antenna eavesdropper by a MIMO eavesdropper reduces the adversary's mean bit error rate from 50% to 0.5%. Hence, we conclude that random modulation alone cannot secure RFID communication against a MIMO eavesdropper (who has more antennas than the reader).
- When the reader uses both random modulation and a rotating antenna, the mean bit error rate of a MIMO eavesdropper is 50%, which is no better than a random guess. This bit error rate stays at 50% even if the eavesdropper is allowed 3, 4 or 5 antennas. We conclude that the combination of random modulation and random channels protects against a MIMO eavesdropper (even if it has more antennas than the reader).
- Finally, we compare LocRF with the Noisy Reader [42], a related prior proposal that also changes the reader's signal and does not require modifying the RFID cards. We implemented the Noisy Reader on the same hardware as LocRF. Evaluation with commercial RFIDs shows that when the LocRF reader is replaced by a Noisy Reader, the mean bit error rate at the eavesdropper drops from 50% to just 0.3%. The reason is that the modulation signal used by the Noisy Reader cannot obscure the difference between the "0" and "1" patterns in the underlying data of the RFID card. As a result, the Noisy Reader does not work for most of today's commercial RFID cards, which use robust encoding schemes (e.g., Manchester encoding) that associate different patterns with "0" and "1" bits.

Contributions: This paper makes the following contributions:

- LocRF, to the best of our knowledge, is the first system that protects unmodified RFID cards from eavesdropping attacks. Alternative solutions to this problem either require revamping the encryption on existing cards [9], [1], [8], or prove insecure in practice [42].
- Further, this paper provides the first wireless system that prevents a MIMO eavesdropper from decoding the RFID signal even if it has more antennas than the total number of antennas on the trusted system.
- This paper also provides a comprehensive study of physical layer RFID security, shedding light on the communication model, and how inaccurate representation of the model causes a previous solution to be insecure in practice.

2. Threat Model

We address passive eavesdropping attacks against commercial RFID cards in the HF and UHF bands, including cards with cryptographic protection and those without. In this attack, an adversary listening on the wireless medium intercepts the conversation between a legitimate reader and an RFID card. The adversary may seek to obtain confidential information contained in the RFID card. In the simplest case, he can learn the ID of the card, threatening the privacy of the party carrying the card and opening doors for cloning attacks. Second, the adversary can obtain sensitive data transmitted by the card, such as biometric information and passwords. Further, the eavesdropper can intercept the cryptographic nonce transmitted by the card, and use it to reverse engineer the encryption and extract the secret key [13], [6].

The adversary may use standard or custom-built hardware to capture signals, including multi-antenna MIMO devices. Also, the adversary may be in any location with respect to the card and the reader. The adversary may be eavesdropping on his own card's conversation with the reader or someone else's card.

We assume the commands transmitted from the reader to the RFID do not contain sensitive information, i.e., by listening to the reader's commands alone, the eavesdropper cannot derive any confidential data. This assumption is justified since for HF cards (e.g., MIFARE), listening to the reader's messages alone does not allow the eavesdropper to extract the secret key and decode the rest of the card's encrypted data [13], [6]. For UHF cards, this assumption is satisfied as long as the reader acknowledges cards using only their temporary IDs, which are not confidential. This operating mode is readily available for today's UHF readers [11].

We also assume that the reflected signal from the RFID card is significantly weaker than the direct signal from the reader. This assumption is satisfied for both HF and UHF systems [3], [10], [37]. In practice, the reflection is one or two orders of magnitude weaker than the direct high power RF signal generated by the reader because the card's circuit reflects only a small part of the power it receives [34], [27].

What About Active Attacks?

Aside from passive eavesdropping, active scanning attacks are also frequently discussed in the RFID literature. In active attacks, an adversary repeatedly queries an RFID card in an attempt to infer the secret key from the responses or obtain confidential information.[1]

1. Man-in-the-middle attacks can be considered as a form of active attacks since they require the adversary to transmit his own signal.

There are multiple solutions for protecting deployed RFIDs from active attacks, including shielding sleeves which have proven successful in preventing active scanning and are commonly used in practice (e.g., in US Passport Cards [28] and RFID blocking wallets [44], [36]).

Active attacks are also relatively easier to address for three reasons: First, they have a shorter range [28], [18], [32], [19] since the attacker needs to power the RFID card (as opposed to the card being powered by the reader in eavesdropping attacks). For example, for HF RFIDs, an active adversary needs to be within a few centimeters from the card whereas a passive eavesdropper can be more than 4 meters away [18]. Second, active attacks are easier to detect because they require the adversary to transmit its own signal. This compounded with the fact that the active adversary has to be near the card means that one can use a friendly jammer co-located with the protected card (or the RFID deployment) to detect and jam unauthorized RFID commands. [24] presents a famous solution in this category. Third, while passive attacks succeed within seconds or minutes, active attacks can take multiple hours to retrieve the secret key [6], [46], [13].

We believe a solution that protects billions of deployed RFIDs against eavesdropping can address a remaining real threat and raise the bar for RFID security in general.

3. RFID Communication Primer

RFIDs mainly operate in two frequency bands: the High Frequency band (HF 13.56 MHz), where the communication range is about 10 cm, and the Ultra High Frequency band (UHF 915 MHz), where the range can reach a few meters. LocRF protects both types from eavesdropping attacks.

RFID cards do not generate their own transmission signals. Instead, they are powered and activated by the waveform coming from the RFID reader, through inductive coupling in the HF band [3] or backscatter communication in the UHF band [7]. In both UHF and HF systems, the reader continuously transmits a high power RF signal $c(t)$, and a nearby RFID card modulates the reader's signal with its data through a mechanism called load modulation. In particular, the card switches a load resistor on and off at its own antenna while reflecting the reader's signal. When the load resistor is off, the card's reflected signal on the air appears as $x_0 \cdot c(t)$; when the load resistor is on, the signal is $x_1 \cdot c(t)$, where x_0 and x_1 represent the reflection efficiency corresponding to the two impedance states of the card's antenna.

It is common practice to describe wireless systems in the baseband, that is after removing the carrier frequency.[2] Hence, in the rest of the paper, we focus on the baseband signals. In current RFID systems, during the card's reply, the reader's baseband signal is a constant waveform $c(t) = A$, where A is a constant amplitude.

A nearby receiver receives a weighted sum of the reader's signal and the reflected signal from the card:

$$y(t) = h_{reader \to receiver} \cdot c(t) + h_{card \to receiver} \cdot x(t) \cdot c(t) \quad (1)$$

$x(t)$ is the card's data message, $h_{reader \to receiver}$ is the wireless channel from the reader to the receiver, and $h_{card \to receiver}$ represents the channel coefficient of the card's reflected signal to the receiver. Note that the receiver in the above equation can be the reader itself or an eavesdropper.

4. LocRF: Randomized Modulation

In this section, we present LocRF's basic random modulation scheme, which defends RFIDs against single antenna eavesdroppers. The model and design discussed in this section hold true for both HF and UHF RFIDs.

In RFID systems, the reader transmits a query command to which a nearby RFID card replies with its data. During the card's reply, the reader needs to continue transmitting a high power RF signal on which the card modulates its data, as detailed in §3. LocRF randomizes this modulation of the card's data. To do so, instead of transmitting a constant signal as in today's RFID systems, a LocRF reader transmits a random signal $r(t)$ during the card's reply.

Two design goals need to be achieved. First, we need to ensure that an adversary cannot predict or learn the random modulation $r(t)$ to decode the card's data. Second, the LocRF reader should be able to decode with an accuracy comparable to the case where a reader uses a constant waveform to read the card. Below, we discuss how we address these two challenges.

4.1. Ensuring the Eavesdropper Cannot Decode

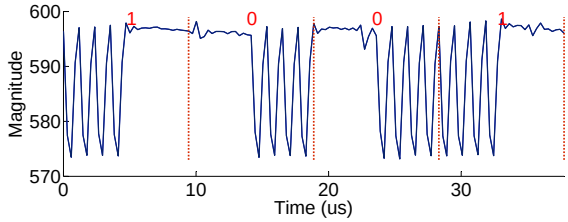
Recall from §3, that the eavesdropper receives:

$$y(t) = h_{reader \to eve} \cdot r(t) + h_{card \to eve} \cdot x(t) \cdot r(t) \quad (2)$$

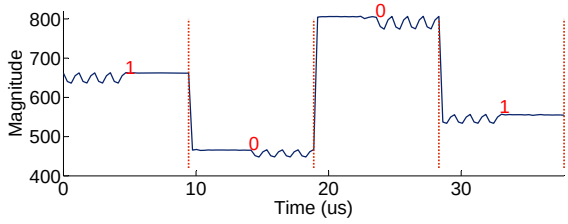
Thus, the eavesdropper hears the RFID data $x(t)$ multiplied by the reader's random signal, $r(t)$, in addition to hearing the random signal directly from the reader itself. So, how should we choose $r(t)$ such that the eavesdropper cannot decode $x(t)$ from its received signal?

At first, it might seem that the reader should transmit a different random number for the duration of each RFID bit in $x(t)$. Unfortunately, such a design does not work because the RFID card uses different *patterns* to disambiguate a "0" bit from a "1" bit (as opposed to a single scalar that differs between "0" and "1"). To better understand this issue, let us consider the Charlie subway card [30] as an example. Fig. 1(a) shows a few bits of the card's reply while communicating with a conventional reader. As shown in the figure, the card uses Manchester encoding, where a '0' bit is expressed as a constant value followed by switching

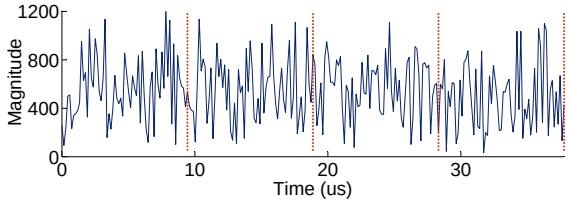
2. Wireless signals are transmitted using a carrier frequency f_c. At the receiver, the RF frontend removes the carrier frequency from the received signal $A\cos(2\pi f_c + \theta)$, which produces the baseband signal A.



(a) Charlie card



(b) One random number per bit



(c) Random modulation

Figure 1—The time signal at the eavesdropper during the Charlie card's reply: (a) shows the eavesdropper's received signal when the Charlie card communicates '1001' to a conventional RFID reader. Two patterns are used to disambiguate '0' and '1'. (b) shows the signal if the reader simply generates one random number per bit in the attempt to hide the card's data. Despite the randomness in magnitude, the received signal still exhibits two patterns, from which an eavesdropper can decode. (c) shows the received signal when the random modulation $r(t)$ varies much faster than the rate of the card. The received signal in this case resembles random white noise.

repeatedly between two states, whereas a '1' bit is expressed as switching state followed by a constant value.

Fig. 1(b) shows the eavesdropper's received signal, ($y(t)$ in Eq. 2), if the reader simply generates one random number per card data bit and uses a sequence of such numbers as $r(t)$. Clearly, the eavesdropper can still tell apart '0' bits and '1' bits based on the internal patterns, despite that each bit is multiplied by a random value. Thus, this design is insecure.

What we need is a design of $r(t)$ that can destroy these internal patterns. In particular, consider an alternative approach, where the LocRF reader's random signal $r(t)$ is changing rapidly within a bit of the card. Fig. 1(c) shows the signal received by the eavesdropper in this case for the same bits in Fig. 1(a). Now both the '0' bits and the '1' bits have the appearance of random white noise. Because the internal patterns are dispersed by the rapidly changing $r(t)$, the eavesdropper can no longer recognize them to decode.

But, how fast should the reader's random signal change? Consider again the card's data in Fig.1(a). $r(t)$ should change faster than the fastest transition in the card's data signal (i.e., the spikes in Fig.1(a)). The fastest transition in the card's signal is by definition limited by the signal's highest frequency component. Fig. 2(a) plot the Charlie card's signal in the frequency domain. The fastest frequencies spanned by the card's signal are around +/-1 MHz. Further the bandwidth is approximately 2 MHz (i.e., -1 MHz to 1 MHz). For $r(t)$ to hide even the fastest transitions in the card's data signal, $r(t)$ needs to have a bandwidth of at least 2 MHz, i.e., it should take 2 million random values per second.

Based on the above discussion, the LocRF reader generates its random signal $r(t)$ as follows. The reader generates a sequence of 2 million random complex samples per second. These random samples are drawn from a zero-mean complex Gaussian distribution with a variance equal to the average transmission power of the reader. The samples are then quantized to a resolution of 32-bit (to match the resolution of the digital-to-analog converter). The sequence of samples in the random modulation $r(t)$ during each message of the card is not used again by the LocRF reader.

We plot in Fig. 2(b) the frequency profile of the LocRF reader's random signal, $r(t)$. The figure shows that $r(t)$ spans 2 MHz of bandwidth and overlaps with the entire profile of the card's data in Fig. 2(a). Note the flat frequency profile characterizing white noise. The frequency profile of the eavesdropper's received signal in this case is shown in Fig. 2(c). Clearly, the two figures are similar which shows that the signal received by the eavesdropper is dominated by the reader's random signal and resembles the frequency profile of white Gaussian noise in this 2 MHz band.

The above provides an intuition to why the eavesdropper cannot decode. Next, we derive the optimal decoder and show that, even with the optimal decoder, the eavesdropper experiences a bit error rate close to that of a random guess.

4.2. Eavesdropper's Optimal Decoder

The eavesdropper receives the signal $y(t)$ in Eq. 2. Since $h_{reader \to eve}$ is constant, we can normalize $y(t)$ by it to get:

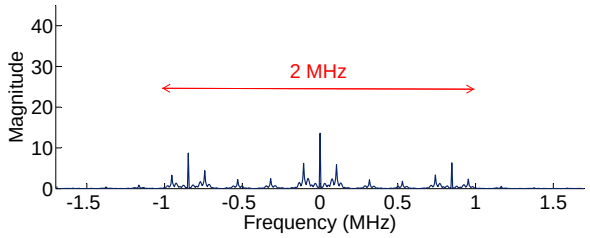
$$y'(t) = r(t) \cdot \left[1 + \frac{h_{card \to eve}}{h_{reader \to eve}} \cdot x(t)\right] \tag{3}$$

The RFID card's signal $x(t)$ has two states: x_0 when the load resistor is off and x_1 when load resistor is on. To convey a '0' or '1' bit, the card transmits different patterns of x_0's and x_1's of length k. Thus, for each card bit b the eavesdropper receives k samples in $y'(t)$ denoted as $\{Y_1, Y_2, \cdots, Y_k\}$:

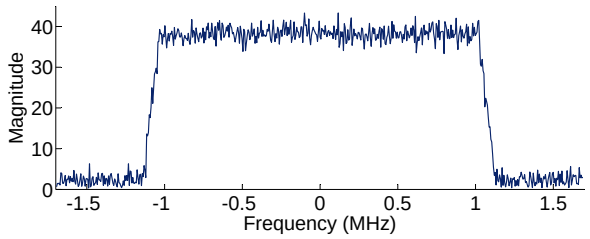
$$Y_i = \begin{cases} R_i \cdot (1 + p_i^0) & \text{if } b = 0 \\ R_i \cdot (1 + p_i^1) & \text{if } b = 1 \end{cases} \tag{4}$$

where $\{p_1^0, ..., p_k^0\}$ is the pattern when the card transmits a '0' bit and $\{p_1^1, ..., p_k^1\}$ is the pattern when the card transmits a '1' bit.[3] R_i is a sample in the reader's random signal $r(t)$ which is drawn from a complex normal distribution with zero mean and standard deviation σ, the received sample Y_i is

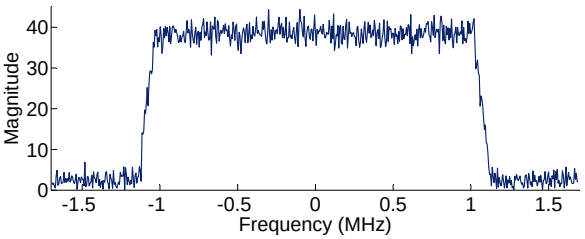
3. $p_i^0 = \frac{h_{card \to eve}}{h_{reader \to eve}} x_0$ or $\frac{h_{card \to eve}}{h_{reader \to eve}} x_1$ depending on the pattern used by the RFID card. The same holds for p_i^1.



(a) Frequency profile of Charlie card's reply



(b) Frequency profile of the LocRF reader's random signal



(c) Frequency profile of eavesdropper's received signal

Figure 2—Randomized modulation in the frequency domain: The frequency profile of the random modulation in (b) is as wide as the card's data bandwidth in (a), and can hide the transitions associated with the card's signal in the time domain. The frequency profile of the eavesdropper's received signal in (c) is flat and resembles that of random white noise. All frequency profiles are plotted in baseband, i.e. centered at 0 Hz.

also complex normal with zero mean and standard deviation $\sigma|1+p_i^0|$ for $b=0$, or $\sigma|1+p_i^1|$ for $b=1$.

The eavesdropper needs to decide whether $b=0$ or 1 based on the k samples $\{Y_1, Y_2, \cdots, Y_k\}$ he receives. The optimal decoder is a maximum likelihood decoder [4], [25] defined by the following hypothesis test:

$$Pr(b=1|\{Y_1,\cdots,Y_k\}) \underset{0}{\overset{1}{\gtrless}} Pr(b=0|\{Y_1,\cdots,Y_k\})$$

In Appendix A.1, we show this maximum likelihood test can be reduced to:

$$\sum_i^k \left(\frac{|Y_i|}{\sigma_i^1}\right)^2 \underset{0}{\overset{1}{\lessgtr}} \sum_i^k \left(\frac{|Y_i|}{\sigma_i^0}\right)^2, \quad (5)$$

where $\sigma_i^0 = \sigma|1+p_i^0|$ and $\sigma_i^1 = \sigma|1+p_i^1|$.

Security Analysis: We analyze the bit error rate (BER) at the eavesdropper given that he uses the above optimal decoder. We derive the BER formula for both HF and UHF cards in Appendix A.2. The BER depends on the ratio of the reader's direct signal power to the RFID's reflected signal power. For a typical power ratio of 30 dB (i.e., the card's reflected signal is 30 dB weaker than the reader's high power RF signal), the eavesdropper's BER assuming no channel noise is around 47%. Further, the empirical measurements in §7.1 which result from running the system over real wireless channels show that, in practice, the eavesdropper's mean BER is 50% (the same as a random guess). This is because in practice channel noise exacerbates the BER.

4.3. How Does the LocRF Reader Decode?

The goal of the LocRF reader's decoder is to retrieve the card's data $x(t)$ from the received signal $y(t)$. As explained in §3, the reader receives:

$$y(t) = h_{reader\to self}\cdot r(t) + h_{card\to reader}\cdot x(t)\cdot r(t), \quad (6)$$

where $h_{reader\to self}$ is the channel of the reader's self-interference,[4] and $h_{card\to reader}$ is the channel of the card's reflection to the reader.

To decode, the LocRF reader needs to eliminate the effect of the random signal $r(t)$ in Eq. 6 to obtain $x(t)$. The first term in the above equation, $h_{reader\to self}\cdot r(t)$, is the reader's self-interference and is independent of the card's data. Removing self-interference is a known procedure in wireless full-duplex systems [21]. It is done as follows: We partially eliminate self-interference in the analog domain using a device called circulator [21]. Second, we further process the signal in the digital domain to eliminate any residual self-interference. This is done by subtracting $h_{reader\to self}\cdot r(t)$ from the received signal $y(t)$. The reader knows $r(t)$ since he generated the random signal. As for the channel, $h_{reader\to self}\cdot r(t)$, it can be estimated using standard channel estimation methods.[5]

After removing the self-interference term from Eq. 6:

$$\widehat{y}(t) = h_{card\to reader}\cdot x(t)\cdot r(t) \quad (7)$$

Next, the reader divides $\widehat{y}(t)$ by $h_{card\to reader}\cdot r(t)$, which will produce $x(t)$. This is possible since the reader knows $r(t)$ and can compute the channel $h_{card\to reader}$ using the known preamble in the card message (as customary in wireless channel estimation). Once the reader has $x(t)$, it can decode the data bits using typical RFID decoding.[6]

5. LocRF: Randomized Channel

In this section, we consider the problem of defending against an emerging class of powerful adversaries: MIMO (multi-input multi-output) eavesdroppers. MIMO is an advanced wireless technology that relies on multi-antenna systems. A good description of MIMO is available in [45].

4. Since the reader is receiving at the same time while transmitting, it hears its own transmission. This phenomenon is commonly referred to as self-interference.

5. The reader can estimate the self-interference channel, $h_{reader\to self}$, by transmitting a known signal and observing how the signal changes as it is received, which is a standard approach in wireless systems [20].

6. Dividing a noisy received signal by $r(t)$ can potentially increase the noise variance, due to the random structure of $r(t)$. One way to refine the decoding at low SNRs is to use a matched filter and correlate with $r(t)$ [15].

For the context of this paper, however, it is sufficient to know the following high-level rules about MIMO capabilities [45]:

- An n-antenna MIMO receiver receives signals in an n-dimensional space. For example, a 2-antenna receiver receives signals along two dimensions: the first dimension is the signal received on his first antenna, and the second dimension is the signal received on his second antenna.
- A MIMO receiver with n antennas can separate (and independently decode) n signals transmitted concurrently on the wireless medium. The ability of the MIMO receiver to perform this separation, however, is subject to the condition that the channels over which it receives these n signals are sufficiently different.

Let us consider the implications of these rules for eavesdropping on RFID transmissions.

MIMO in the HF Band: As stated above, the ability of a MIMO eavesdropper to separate the reader's random signal from the RFID's signal hinges on the channels he perceives from the reader and the RFID being sufficiently different. However, in HF (13.56 MHz) RFID systems, the operating distance between the card and the reader is within 10 cm, significantly smaller than half of a wavelength (11 meters). In this case, it is well-known that MIMO techniques cannot separate their signals [45]. Hence, the eavesdropper cannot exploit MIMO to decode the RFID's data in the HF band.

MIMO in the UHF Band: In UHF RFID systems, half of a wavelength is only 16 cm while the operating distance between the card and the reader can be multiple meters. Thus, MIMO becomes a powerful tool that can be employed by eavesdroppers to decode the confidential RFID data. Addressing MIMO adversaries is important since UHF RFIDs are predicted to gradually replace HF RFIDs [22], and they are already used in asset tracking, the U.S. Passport Card, and the Enhanced Driver License.

Addressing MIMO eavesdroppers has long been a difficult problem in wireless systems [14], [26]. Below, we explain in detail the challenge brought in by MIMO, and our solution.

5.1. Challenge: The Antenna Game

MIMO transforms the RFID eavesdropping problem into an antenna game: if the eavesdropper has more antennas than the reader, it can separate the reader's random signal from the RFID's signal and decode the latter. Thus, currently, to win this game, the reader needs to keep adding transmit antennas (with different random signals) to match or exceed the number of receive antennas on the eavesdropper. For example, in §4, we demonstrated that a single-antenna reader transmitting a random signal, $r(t)$, can protect against a single-antenna eavesdropper. Let us examine, what happens if the reader continues to use one antenna but the eavesdropper upgrades to a 2-antenna MIMO receiver.

A 2-antenna eavesdropper receives two signals, $y_1(t)$ and $y_2(t)$ on his two antennas:

$$\begin{aligned} y_1(t) = &\quad (h_{reader\rightarrow eve1} + h_{card\rightarrow eve1} \cdot x(t)) \cdot r(t) \\ y_2(t) = &\quad (h_{reader\rightarrow eve2} + h_{card\rightarrow eve2} \cdot x(t)) \cdot r(t), \end{aligned} \tag{8}$$

where $h_{reader\rightarrow eve1}$ and $h_{reader\rightarrow eve2}$ represent the channels from the reader to the eavesdropper's first and second antennas respectively, and $h_{card\rightarrow eve1}$ and $h_{card\rightarrow eve2}$ the channel coefficients of the card's reflected signal at the eavesdropper's first and second antennas.

The MIMO eavesdropper can first eliminate the random multiplier $r(t)$ by dividing the two signals he receives:

$$\frac{y_1(t)}{y_2(t)} = \frac{h_{reader\rightarrow eve1} + h_{card\rightarrow eve1} \cdot x(t)}{h_{reader\rightarrow eve2} + h_{card\rightarrow eve2} \cdot x(t)}. \tag{9}$$

Next, the eavesdropper tries to decode $x(t)$ from Eq. 9, which has no random multiplier.

Recall that the card's message $x(t)$ has only two states: $x(t) = x_0$ when the card's load resistor is *off*, and $x(t) = x_1$ when the card's load resistor is *on*. Hence, distinguishing these two states enables the eavesdropper to fully decode the card's transmitted data $x(t)$ (including the patterns within the "0" and "1" bits). As a result, the ratio of the received signals in Eq. 9 only takes two values corresponding to the $x(t) = x_0$ state and the $x(t) = x_1$ state. We denote these two values of the ratio y_1/y_2 as α_0 and α_1.

After computing the ratio y_1/y_2, the only ambiguity the eavesdropper has is in mapping the two observed values α_0 and α_1 to states x_0 and x_1. To resolve this ambiguity he checks which of the two mappings allows the decoded RFID message to satisfy the checksum [11]. Thus, a 2-antenna eavesdropper can win the antenna game over a single-antenna reader, even if the latter uses random modulation.

We can gain a deeper insight into this antenna game by looking at the received signal in the 2-dimensional space created by the two antennas on the eavesdropper. Recall that a 2-antenna eavesdropper receives signals in a 2-dimensional space, where one dimension is $y_1(t)$, the signal received on his first antenna and the other dimension is $y_2(t)$, the signal received on his second antenna. Thus, at any point in time t, the received signals $(y_1(t), y_2(t))$ can be represented as one point in this 2-dimensional space. When $x(t) = x_0$, we know from above that $y_1 = \alpha_0 y_2$, which defines a *line* in this 2-dimensional space. Similarly, when $x(t) = x_1$, the received signals lie on a different line defined by $y_1 = \alpha_1 y_2$.

We confirm this point empirically by letting a 2-antenna MIMO adversary (implemented using USRP2 software radio) eavesdrop on a conversation between a commercial UHF RFID and a USRP2-based LocRF reader. Details of the experimental environment are described in §6. Fig. 3 shows a scatter plot of what the eavesdropper receives on his two antennas. Here we plot the magnitude of the received samples, i.e., each point in the figure represents $(|y_1(t)|, |y_2(t)|)$ for a specific t. We then use our ground truth knowledge of the actual bits transmitted by the RFID card

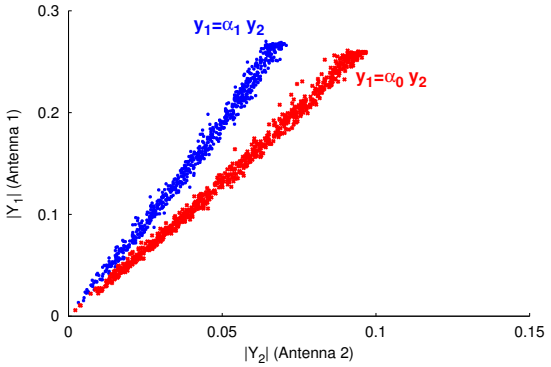


Figure 3—Antenna space of a 2-antenna MIMO eavesdropper in LocRF's basic randomized modulation scheme: The figure shows a scatter plot of the digital samples received by a 2-antenna eavesdropper. Despite random modulation, a 2-antenna eavesdropper facing a single-antenna reader sees two lines that correspond to the two states of the RFID card, x_0 and x_1. Hence, it can decode the RFID state at any point in time.

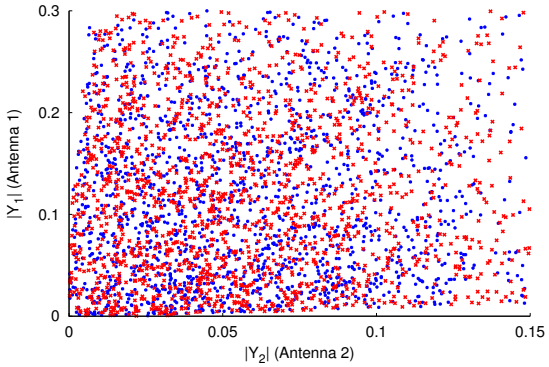


Figure 4—Antenna space of the 2-antenna MIMO eavesdropper when the reader uses a rotating antenna: When the reader transmits the same random signal $r(t)$ as in Fig. 3 using a rotating antenna, the eavesdropper's received samples $(|Y_1|, |Y_2|)$ almost span the entire antenna space because the channels are randomly changing. No subspace is unique to the card's x_0 state (red), as opposed to the x_1 state (blue), which prevents the reader from distinguishing the x_0 and x_1 samples to decode.

to label samples corresponding to x_0 in blue and x_1 in red. Despite the fact that the received signal at each antenna is random, together $y_1(t)$ and $y_2(t)$ span only *lines* instead of the entire 2-dimensional space at the eavesdropper. Since the card's data has only two states, we see two lines in the figure and hence the eavesdropper can decode by checking which line the received samples lie on.

The above can be generalized to more antennas on the reader and the eavesdropper. If the eavesdropper has n antennas, he receives signals in an n-dimensional space. If the reader has k antennas, where $k < n$, and transmits k independent signals from them, these signals will only span a k-dimensional *subspace* (lines, planes, etc.) in the eavesdropper's n-dimensional space. Since the card only has two states x_0, x_1, the eavesdropper will observe two unique subspaces and hence he can decode. Thus, it comes down to an antenna game between the RFID reader and the eavesdropper. No matter how many antennas the reader uses, the eavesdropper can win the game by using more antennas.

5.2. Change the Game: A Rotating Antenna

To overcome the antenna game and ensure that an n-antenna eavesdropper cannot decode, the reader needs to span the entire n-dimensional space in which the eavesdropper receives. This guarantees that no particular subspace is unique to the $x(t) = x_0$ state of the card as opposed to the $x(t) = x_1$ state. An infinite number of antennas at the reader will achieve this goal, yet it is infeasible in practice.

Instead, in LocRF, we emulate the behavior of a very large (i.e., virtually infinite) number of antennas by using a rotating antenna. This design choice is based on the observation that a small change in the position and direction of a transmitter's antenna can dramatically change its channels to different receiving antennas. This phenomenon is due to the multi-path effects in wireless communications and has been extensively studied in RF propagation [38], [47]. Since antennas in MIMO decoding are identified by the set of channels they create [45], a rotating antenna, which creates a different set of channels at each point in time, can make the reader look as if it had many antennas.

Fig. 4 plots the signal received by a 2-antenna eavesdropper when the reader's single static antenna is replaced with an antenna that rotates (the antenna is fixed to an off-the-shelf motor that rotates at 1725 rpm). Apart from replacing the static antenna with a rotating antenna, the experiment is no different from that in Fig. 3. In contrast to Fig. 3, now the received signal samples span the entire space, instead of being confined to two lines. Hence, the eavesdropper in this case cannot tell apart the blue points and the red points.

To better understand the difference between Fig. 4 and Fig. 3, recall that the slopes of the two lines in Fig. 3, α_0 and α_1, depend only on the channels; if the channels stay constant, the two lines $y_2 = \alpha_0 y_1$ and $y_2 = \alpha_1 y_1$ in Fig. 3 do not change over time. However, if the antenna rotates, it randomizes the channels, and hence the slopes of the two lines α_0 and α_1 will change randomly across time samples, preventing the eavesdropper from separating the samples that correspond to x_0 from those for x_1.

The above discussion is in the context of a 2-dimensional eavesdropper. In Appendix B, we generalize the argument to show that a reader with a rotating antenna can emulate a transmitter with at least n antennas to an n-antenna eavesdropper. We also verify this behavior empirically in §7.2 for MIMO eavesdroppers with $3-5$ antennas.

5.3. LocRF's Rotating Antenna Extension

A rotating transmit antenna overcomes the antenna game and prevents a MIMO eavesdropper from decoding. However it also poses a challenge for decoding at the reader. Specifically, the reader receives:

$$y(t) = h_{reader \to self}(t) \cdot r(t) + h_{card \to reader}(t) \cdot r(t) \cdot x(t). \quad (10)$$

In this equation, although the reader knows $r(t)$, the varying channels $h_{reader \to self}(t)$ and $h_{card \to reader}(t)$ act as random

multipliers for $r(t)$. Hence, the reader no longer knows the actual random modulation happening on the air, and ends up facing the same challenge as the eavesdropper.

To enable the reader to decode while ensuring the eavesdropper cannot decode, we need to increase the knowledge gap between the reader and the eavesdropper. To do so, we create a design in which the reader can process the digital signal samples it receives so that these samples (after processing) have a higher variance when the card is in state x_1 than when it is in state x_0. The difference in variance appears only post-processing; the samples on the air have equal variance, and hence are received by the eavesdropper with equal variance. Further, the processing done by the reader cannot be done by the eavesdropper because it requires knowing the random waveform. Below we describe our design in detail.

The LocRF reader uses two antennas: a rotating antenna and a static antenna. The reader transmits $r_1(t)$ on its rotating antenna and $r_2(t)$ on its static antenna, where $r_1(t)$ and $r_2(t)$ are two independent random waveforms. To decode, the reader uses only the signal that it receives on its static antenna, which can be written as:

$$\begin{aligned} y(t) = \quad & h_{rotate}(t) \cdot r_1(t) + h_{c\_rotate}(t) \cdot r_1(t) \cdot x(t) \\ + \quad & h_{static} \cdot r_2(t) + h_{c\_static} \cdot r_2(t) \cdot x(t), \end{aligned} \tag{11}$$

where $h_{rotate}(t)$ and $h_{c\_rotate}(t)$ are the direct channel from the reader's rotating antenna and the indirect channel via the reflection off the card. Note $h_{c\_rotate}(t)$ varies with time because it is the composite channel from the rotating antenna to the card and from the card to the reader's static antenna. h_{static} is the self-interference channel of the static antenna, and h_{c_static} is the card's reflection channel for the signal transmitted by the static antenna.

The LocRF reader does not know the changing channels $h_{rotate}(t)$ and $h_{c\_rotate}(t)$. However, the LocRF reader knows $r_1(t)$ and $r_2(t)$ as it is the one who generates them in the first place. The reader also estimates the value $h_{static} + h_{c\_static} \cdot x_0$ when $x(t) = x_0$, as follows: The card starts its reply with a known preamble, i.e., a known sequence of x_0's and x_1's. The reader picks one of the x_0's in the preamble at random, and does not transmit from the rotating antenna during that x_0 interval. As a result, for that particular x_0 interval, the reader receives $h_{static} + h_{c\_static} \cdot x_0$, which is the value it wants to estimate. The eavesdropper cannot distinguish when the rotating antenna transmits and when it does not because its channel is random and the wireless medium always has randomly modulated power from either or both antennas.

The reader leverages its knowledge of the variables $r_1(t)$, $r_2(t)$, and $h_{static} + h_{c\_static} \cdot x_0$ to decode. First, it removes the self-interference from its static antenna by subtracting from the received signal in Eq. 11 $(h_{static} + h_{c\_static} \cdot x_0) \cdot r_2(t)$. Then it normalizes the residual with the signal transmitted from its rotating antenna $r_1(t)$. The resulting signal $\widehat{y}(t)$ becomes:

$$\begin{aligned} \widehat{y}(t) =& \frac{y(t) - (h_{static}(t) + h_{c\_static}(t)x_0) \cdot r_2(t)}{r_1(t)} \\ =& \begin{cases} h_{rotate}(t) + h_{c\_rotate}(t)x_0 & \text{if } x(t) = x_0 \\ h_{rotate}(t) + h_{c\_rotate}(t)x_1 + h_{c\_static}(x_1 - x_0)\frac{r_2(t)}{r_1(t)} & \text{if } x(t) = x_1 \end{cases} \end{aligned}$$

During an $x(t) = x_0$ interval, the variation of $\widehat{y}(t)$ depends only on the variation of the channels h_{rotate} and h_{c_rotate}. On the other hand, during an $x(t) = x_1$ interval the variation of $\widehat{y}(t)$ depends on the variation in the channels as well as the variation of term $\frac{r_2(t)}{r_1(t)}$. Since $r_1(t)$ and $r_2(t)$ change very quickly (each takes 2 million different values per second as explained in §4), the reader observes a much higher variation in $\widehat{y}(t)$ when the card is in state x_1.

Thus to decode, the reader uses the values of $\widehat{y}(t)$ during the card's preamble to estimate the variance of $\widehat{y}(t)$ in x_0 state and x_1 state. During the card data transmission, the reader distinguishes $x(t) = x_0$ from $x(t) = x_1$ based on whether the variance of $\widehat{y}(t)$ during that interval is closer to the variance of x_0 state or x_1 state as computed during the preamble. An eavesdropper on the other hand cannot decode using the same procedure because it does not know the random waveforms and hence cannot compute $\widehat{y}(t)$.

5.4. Security Discussion

Deriving the eavesdropper's optimal decoder under unknown channel conditions caused by the rotating antenna is a difficult problem and quickly becomes intractable for MIMO receivers. Instead, we will discuss potential strategies that an eavesdropper may attempt to use to decode the RFID data. For the discussion below, we consider an n-antenna eavesdropper. We assume that in each cycle, the rotating antenna exhibits $m \geq n$ distinct channel values to each of the n antennas on the eavesdropper, and that the channels are independent of the state of the card. We also assume that due to rotation the channels exhibit some change (though it may be small) over intervals comparable to how often the card changes state.

We note that in practice a small change in an antenna's position or orientation can cause a significant change in the channel [38], [47]. Hence, m can be fairly large. Further, for RFIDs, the card's reflected power is much lower (e.g., 30 dB lower) than that of the reader. Thus, even a small change (a fraction of a percent) in the reader's channel can cause enough noise to obscure the card's state at the eavesdropper.

Given the above, we consider the following strategies:

Strategy 1: The eavesdropper tries to track the changing channels by considering the LocRF reader's rotating antenna as static over short time intervals. As described at the end of §5.1, if the reader has two static antennas, the received signal would span two separate planes in the eavesdropper's antenna space, one for x_0 and one for x_1. The eavesdropper may consider short intervals on the order of a few states, assume channels are static for that duration, and try to

identify the two planes. To do this, the attacker needs to receive signals for enough x_0 and x_1 states to approximate the planes. In our empirical evaluation in §7.2, we implement this strategy and show that due to the fast fading channels and the random modulation, such a MIMO eavesdropper experiences bit error rates close to 50%, equivalent to when he makes a random guess.

Strategy 2: The eavesdropper tries to decode by exploiting that, in every cycle, the rotating antenna spans the same positions, and hence the same sequence of channels. The eavesdropper may try to group and decode together the card's states that are a full cycle apart because they experience the same channel values. This strategy is significantly hard to implement in practice for the following reasons: A full cycle is typically longer than a UHF RFID message which lasts for less than 20 millisecond. Also, the reader can randomize its rotating speed and keep that information secret from the adversary. Further, even with full knowledge of the setup, we could not identify clear repeated channel states in our experiments (see specifications of the rotating antenna in §6). We believe the reason is due to small mechanical variations, which are not deterministic across cycles.

Strategy 3: The eavesdropper may use $n > m+1$ antennas, in which case the received signal will span two $(m+1)$-dimensional subspaces in the eavesdropper's n-dimensional space, where each subspace refers to either x_0 or x_1. While this attack is plausible it is likely impractical. As explained above the number of distinct channel instantiations m can be fairly large. In practice, building a very large-scale MIMO system is difficult. For example, commercial WiFi MIMO receivers are limited to 4 MIMO antennas [33]. While it is possible to build a larger MIMO receiver by using multiple devices and synchronizing them with an external clock, as we did in our experiments, this setup however is quite bulky and does not scale to a very large number of antennas.

6. IMPLEMENTATION

We built a prototype of the LocRF reader using software-defined radios. Our implementation is a customized version of the USRP implementation of an RFID reader developed in [7]. The customization involves the use of a random waveform during the RFID card transmission instead of a constant waveform, and an extension to the code to cover also the HF band (since the original implementation was for UHF only). The eavesdropper is also implemented on the USRP software radio. Additional information regarding the hardware and the setup is provided below.

A. HF Devices and Setup

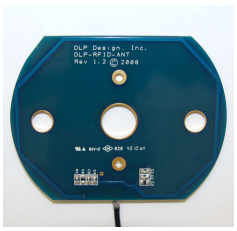
Reader: The HF LocRF reader is implemented on USRP1 software radio [23] using LFTX and LFRX daughterboards operating in the 0-30 MHz frequency range. The reader's antenna is the DLP-RFID-ANT antenna shown in Fig. 6(a).

(a) MBTA Charlie Card

(b) General Purpose RFID

(c) UMASS Moo RFID

Figure 5—RFID cards used in experiments: (a) MBTA Charlie subway card in the HF band (ISO14443), (b) the Alien Squiggle General Purpose commercial RFID tags in the UHF band, and (c) the Moo UHF computational RFID with a micro-controller.



(a) HF Antenna

(b) UHF Antenna

(c)

Figure 6—Antennas used in experiments: (a) the DLP-RFID-ANT antenna in HF band, (b) the Cushcraft 10x10 inch panel antenna in the UHF band and (c) the VERT900 6 inch vertical antenna in the UHF band.

RFID Card: We use the MBTA Charlie card shown in 5(a) as an example of MIFARE Classic cards. The typical operating range of these commercial cards is within 10 cm. We vary the distance between the HF LocRF reader and Charlie card in a range of [2, 10] cm.

Eavesdropper: The adversary is implemented using the same hardware (USRP and antenna) as the LocRF reader. The location of the eavesdropper varies across runs but stays within [5, 10] cm away from the tested RFID card. To decode, the eavesdropper uses the optimal decoder based on maximum-likelihood described in Appendix A.1.

B. UHF Devices and Setup

Reader: The UHF LocRF reader is implemented on USRP n210 [23] with rfx900 daughterboards in the 902-928 MHz range and a Cushcraft panel antenna [29] shown in Fig. 6(b).

RFID Card: We use the Alien Squiggle General Purpose RFID Tags [2] in Fig. 5(b), and the Moo tags in Fig. 5(c). The distance between the reader and the tag is varied in a range of [1, 5] meters, matching the typical operating range in current UHF RFID systems.

Rotating Antenna: In LocRF's MIMO extension, the reader's rotating antenna is implemented by mounting a VERT900 antenna shown on Fig. 6(c) on a 1725-rpm fan motor. The antenna is tilted and thus rotation changes both the position and the direction. We note that this rotating antenna is smaller than the static antenna used by the reader and the eavesdropper's multiple antennas. The lightweight nature of the rotating antenna allows us to easily mount it on an off-the-shelf fan motor.

Eavesdropper: The adversary is implemented using the

same hardware as the LocRF reader, and uses the same antenna type as the reader's static antenna. The only difference is that, in the MIMO experiments, the eavesdropper uses multiple (up to 5) of the panel antennas in Fig. 6(b). For the single antenna evaluation, the eavesdropper decodes using the maximum-likelihood decoder in Appendix A.1. For the MIMO evaluation, the eavesdropper decodes using Strategy 1 in §5.4. This strategy is based on the intuition that a rotating antenna can be approximated for every short interval by a different static antenna. Thus, the eavesdropper first uses the card's known preamble to learn two planes that correspond to x_0 and x_1 and best fit the data. He initializes his decoder to these planes. He keeps updating the planes in real time by using a few consecutive samples. We tried update intervals that span the duration of one, two, three and ten RFID state transitions, and found that the eavesdropper was slightly better off using an update interval roughly matching the duration of two state transitions.

C. Security Metric

We use the bit error rate (BER) experienced by the eavesdropper as our security metric. A perfectly secure system should maintain a 50% bit error rate at the eavesdropper with an optimal decoder, which is equivalent to a random guess. For both HF and UHF experiments, we run the experiment in a variety of locations and we then average across 1000 runs to compute the average BER.

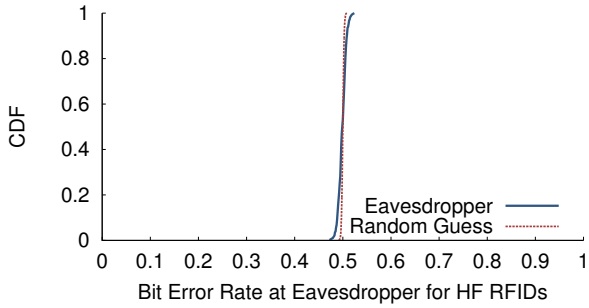


Figure 7—HF eavesdropper's bit error rate: CDF of the eavesdropper's BER over all runs of the Charlie card. Each run (CDF point) includes 1000 traces. The security of LocRF against HF eavesdroppers closely matches the result of random guess.

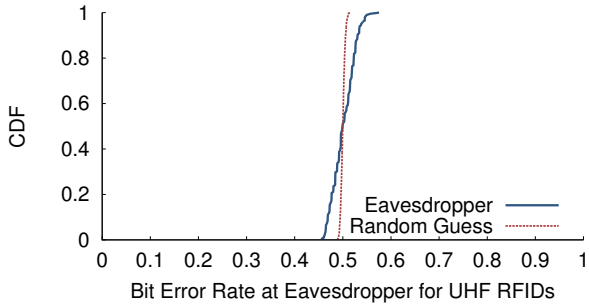


Figure 8—UHF eavesdropper's bit error rate: CDF of the eavesdropper's BER over all runs of commercial UHF tags. Each CDF point includes 1000 traces from the same location. The average BER is 50% with a standard deviation of 2.3%. The BER has a slightly bigger variance than the HF systems, because the operating range in the UHF band is significantly larger.

7. Performance Evaluation

7.1. Evaluation of LocRF's Randomized Modulation

We evaluate the effectiveness of LocRF's random modulation in protecting HF and UHF RFIDs from a single-antenna eavesdropper.

Experiment: In this experiment, the LocRF reader queries the Charlie card or the commercial UHF tag for 1000 times in each run. To match the operating range in current RFID systems, the distance between the LocRF reader and the RFID card is varied between [2, 10] cm in the HF case, and [1, 5] meters in the UHF case. During the RFID's reply, the reader continuously transmits a random signal generated using the method in §4. In the case of the Charlie card (HF), the eavesdropper is placed [5, 10] cm away from the card. In the UHF case, he is placed in a range of [0.2, 5] meters away from the RFID card. He has a single antenna and decodes using the maximum-likelihood decoder in §4.2.

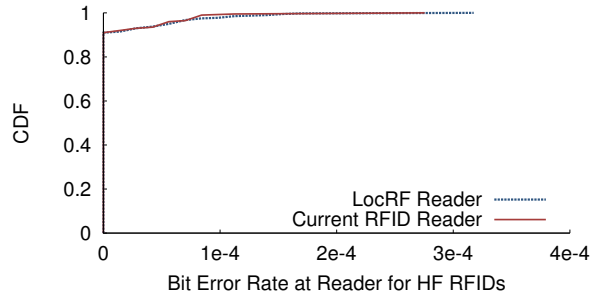
Results 1 (BER at eavesdropper): Fig. 7 plots the CDF of the eavesdropper's bit error rates when the Charlie card is communicating with a LocRF reader. The CDF is taken over all positions of the reader, Charlie card, and eavesdropper. For comparison, the red dashed curve is the CDF of the eavesdropper's BER when he randomly guesses the bits without trying to make use of the eavesdropped information.

The figure shows that when the LocRF reader randomizes the modulation, the eavesdropper's BER is 49.8% on average, with a standard deviation of less than 0.8%, closely matching the results for a random guess.

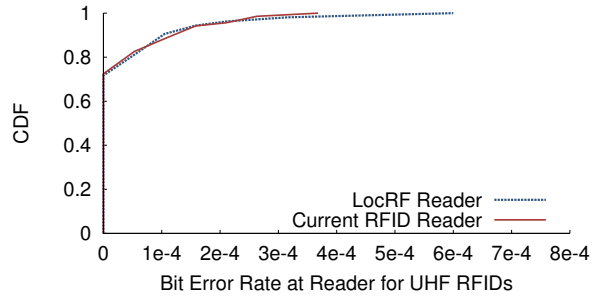
Similarly, Fig. 8 plots the CDF of the UHF eavesdropper's BER. Due to the significantly larger range in UHF systems, the BER has a slightly bigger standard deviation than HF systems. Overall, the UHF eavesdropper's BER is still 50% on average with a standard deviation of 2.3%. This result indicates that random modulation renders the decoding of the eavesdropper about as good as a random guess.

Results 2 (Decoding performance at the LocRF reader): Next, we check that replacing the constant waveform with LocRF's randomized modulation does not negatively impact decoding at the reader, in both HF and UHF RFID systems. We use measurements from the same experiment above but we focus on the BER at the reader.

Fig. 9(a) and Fig. 9(b) plot the CDFs of the bit error rates at the LocRF reader for the HF and UHF experiments respectively. For reference, the figure also shows the bit error rate of existing RFID readers that use a constant waveform instead of the random modulation. The HF LocRF reader has an average decoding BER of less than 0.01% and a maximum BER of 0.03%, whereas the UHF LocRF reader has an average bit error rate of less than 0.01% and a maximum of 0.06%. These values are typical for RFID systems and in line with current RFID reader's performance.



(a) HF LocRF reader decoding with random modulation



(b) UHF LocRF reader decoding with random modulation

Figure 9—Decoding performance of LocRF reader: CDFs of the LocRF reader's BER. (a) For the Charlie card placed in the range [2, 10] cm away from the reader, the average BER is less than 0.01% with a maximum of 0.03%. (b) For a commercial UHF RFIDs [1, 5] meters away from the reader the average BER is less than 0.01% with a maximum of 0.06%. For both HF and UHF RFIDs the decoding performance of the LocRF reader is on par with that of existing readers, for the typical RFID operating ranges.

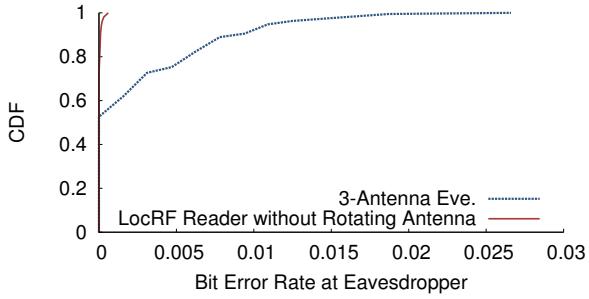


Figure 10—MIMO eavesdropper's BER without rotating antenna: CDF of the 3-antenna eavesdropper's BER when the LocRF reader uses two static antennas. The BER is on average less than 1% which means that the eavesdropper recovers 99% of the RFID card's bits correctly.

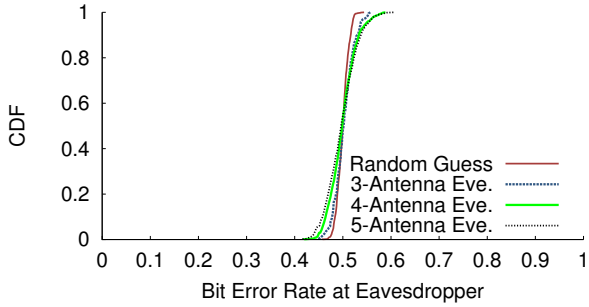


Figure 11—MIMO eavesdropper's BER in LocRF's rotating antenna extension: CDF of the MIMO eavesdropper's BER when the LocRF reader uses one static antenna and one rotating antenna to transmit two independent random signals. The BER is on average 50% and is very close to a random guess even if the eavesdropper uses 3, 4, or 5 antennas to try to decode.

7.2. Evaluating LocRF's Randomized Channel

We empirically evaluate the effectiveness of LocRF's rotating antenna scheme in protecting RFIDs against multi-antenna eavesdroppers. Since multiple antennas do not help eavesdroppers in HF systems, here we focus on UHF RFIDs.

Experiment 1 (MIMO & Static Antennas): First, we would like to empirically confirm that a MIMO eavesdropper with more antennas than the reader can decode despite the random modulation. Thus, we repeat the same experiment performed with the single antenna system in the previous section, after replacing both the reader and the eavesdropper with MIMO devices. In this experiment, the reader has two static antennas each transmitting an independent random signal $r_1(t)$ and $r_2(t)$. The eavesdropper uses a 3-antenna MIMO receiver and decodes by identifying the two planes corresponding to the card's x_0 and x_1 states in its 3-dimensional space, as described in Appendix B.

Result 1 (MIMO & Static Antennas): Fig. 10 plots the CDF of the BER experienced by a 3-antenna MIMO eavesdropper when the LocRF reader uses 2 static antennas with random modulation. Consistent with our analysis in Appendix B, the MIMO eavesdropper can successfully decode the UHF tag's data (BER $< 3\%$). This is because the samples corresponding to '0' bits of the card lie on one plane in the eavesdropper's 3-dimensional space, while the ones corresponding to '1' lie on another plane. The few bit errors the eavesdropper has are caused by the channel noise.

Experiment 2 (MIMO & a Rotating Antenna): We repeat the above experiment after replacing one of the antennas on the reader with a rotating antenna. The MIMO eavesdropper again uses three antennas to capture signals and decodes using Strategy 1, which tries to learn the planes that best fit the data for every short interval, as explained in §6. We repeat this experiment with 4- and 5-antenna eavesdroppers. Adding antennas on the eavesdropper while keeping the reader with two antennas confirms that the rotating antenna can protect against a very powerful MIMO eavesdropper.

Result 2 (MIMO & a Rotating Antenna): Fig. 11 plots CDFs of the BER experienced by 3- 4- and 5-antenna MIMO eavesdroppers when the LocRF reader uses its rotating antenna extension. For reference, the BER result of a random guess is also plotted. The figure shows that the eavesdropper experiences a bit error rate close to 50%. The eavesdropper's decoding in face of LocRF's rotating antenna scheme is equivalent to a random guess. This is because the samples corresponding to x_0 and x_1 states are now indistinguishable in the eavesdropper's multi-dimensional space.

Result 3 (Reader Decoding with a Rotating Antenna): Finally, we check that the rotating antenna and the resulting channel randomization do not prevent the trusted RFID reader from decoding. Fig. 12 plots the BER from the same

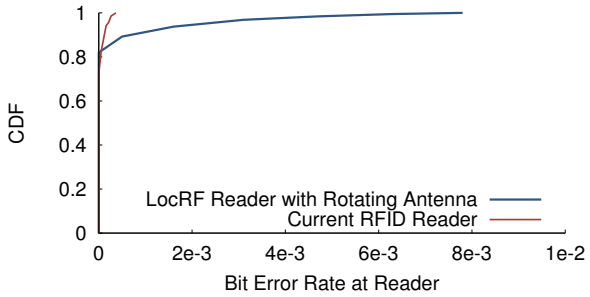


Figure 12—Decoding performance of LocRF reader with rotating antenna: The average BER at the LocRF reader with a rotating antenna is 0.03% which is fairly close to the performance of current RFID readers.

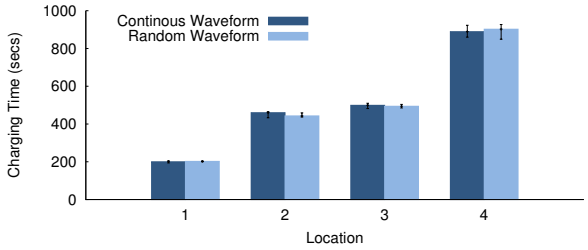


Figure 13—Energy harvesting efficiency: The amount of time it takes to charge the large attached capacitor to the wakeup threshold is similar for both the random modulation and the constant waveform of the same RMS voltage.

experiment as above but as perceived by a LocRF reader that decodes the signal using our design in §5.2. The figure shows that the LocRF reader has an average decoding bit error rate of 0.03%, and a maximum BER of 0.78%. This is slightly worse than the single static antenna case, because the variance-based decoder here is more sensitive to noise. However, an average BER of 0.03% is quite common and considered negligible in RFID systems. If certain applications require an even lower BER, the reader can request the tags to transmit their data using longer codes, an option readily available in today's commercial RFIDs [11].

In summary, the results of the MIMO experiments show that LocRF's randomized channel scheme using a rotating antenna achieves the goal of defending commercial RFIDs against multi-antenna MIMO eavesdroppers, even when the reader has less antennas than the eavesdropper.

7.3. RFID Energy Harvesting Efficiency

Since the reader's RF signal acts as the energy source for the RFID cards, here we investigate whether replacing the constant waveform with LocRF's random waveform affects the card's efficiency in energy harvesting.

Experiment: We want to measure the charging time; however, the capacitor on the battery-free passive RFIDs is typically small (e.g. 5 pF), which does not allow us to obtain robust time measurements. As a workaround, we attach a large capacitor (i.e., 0.1 F) to the Moo RFIDs and record the time it takes for the voltage between two pins of the Moo's energy harvesting circuit to reach 2.2 V, the wakeup threshold. We position the RFID tag at four different locations which are 1, 2, 3, and 4 meters away from the reader, and repeat the charging experiment five times at each location, both for the constant and random waveforms.

Results: Fig.13 shows the time it takes the RFID's capacitor to charge to 2.2V at each location. At all locations, the power efficiency of LocRF's random modulation is on par with the constant waveform. The small differences in the charging time are insignificant and do not consistently favor either of the two waveforms. Thus, we conclude that using a random waveform instead of a constant waveform as the reader's signal has no measurable impact on the power harvesting efficiency of the RFID cards.

7.4. Evaluation of the Noisy Reader Proposal

The Noisy Reader [42] makes the reader vary its own signal in an attempt to hide the HF card's data. To do so, it generates one random number per card bit and uses it as the magnitude of the reader's signal. Further, the Noisy Reader recognizes that the card has an underlying bit pattern, which changes between two states x_0 and x_1. It tries to imitate the card by making the reader periodically switch the phase of its signal by 180 degrees at the same frequency the card uses to switch between two states.

Recall how the HF Charlie card conveys '0' bits and '1' bits in Fig. 1(a): A '0' bit is expressed as a constant value followed by switching repeatedly between two states, whereas a '1' bit is expressed as switching state followed by a constant value. Fig. 14 shows the same bits in the received signal at a single-antenna eavesdropper, when the Noisy Reader is protecting the Charlie card. Although each bit is scaled differently, we can still see that all the '0' bits have the same shape, while the '1' bits have a different shape. Hence, the eavesdropper can still observe two patterns in the message and use them to decode.

The security of the Noisy Reader was studied analytically but we are unaware of any prior implementation or empirical evaluation. We have implemented the Noisy Reader using the same USRP setup as LocRF. We conduct the same experiment as in §7.1, except that here we replace the LocRF reader with the Noisy Reader. Fig. 15 plots the CDF of the single-antenna eavesdropper's BER when the Charlie card is communicating with the Noisy Reader. For comparison, the figure also plots the reader's BER. The figure shows that the difference between the eavesdropper's and the reader's average bit error rates is below 0.3%. This means that the eavesdropper can almost perfectly decode the Charlie card's data despite the Noisy Reader.

We note that the Noisy Reader still works for cards that do not have internal patterns for "0" and "1" bits. However, more than 80% of the HF cards today (ISO 14443 Type A [35]) use the same patterns as the Charlie card (called Manchester encoding), and the UHF cards use a different

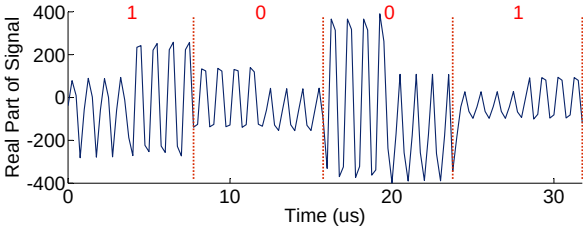


Figure 14—Noisy Reader trace: The eavesdropper's received signal of the Charlie card communicating with the Noisy Reader still exhibits two clear patterns corresponding to the '0' bits and '1' bits. Despite the random magnitude in each bit and the phase shifting, the eavesdropper can still decode by comparing the first half and the second half of each bit. The '0' bits have the same shape, while the '1' bits have a different one.

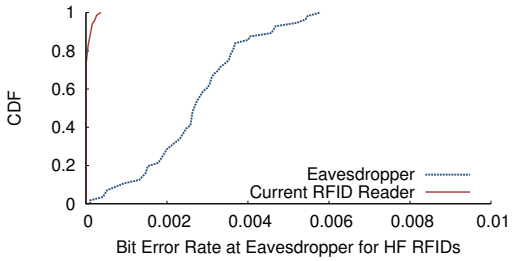


Figure 15—Single-antenna eavesdropper's BER in Noisy Reader scheme: The eavesdropper can almost perfectly decode the RFID card's message (BER $<$ 1%), which is far from the 50% eavesdropper BER expected from a secure scheme. In fact, in this case the eavesdropper's average BER is within 0.3% of the trusted reader.

pattern based on Miller code.

8. Related Work

Past work on defending RFIDs against eavesdroppers mostly focuses on improving their cryptographic protocols [5], [9], [1]. These schemes, however, are difficult to build in practice due to severe cost and size constraints on RFID cards. Hence, commercial RFIDs continue to use weak encryption schemes known to be vulnerable [28], [35], [43].

LocRF belongs to the class of physical layer security mechanisms. Our work is closest to the Noisy Reader scheme [42], which we discussed in detail in §7.4. Other physical layer solutions to eavesdropping attacks, such as the "noisy tag" [8], require modifying the cards to use physical layer signals to exchange a key with the reader. Further, none of these solutions deals with MIMO eavesdroppers.

Finally, we are inspired by recent advances in jamming-based security using full duplex radios [16], [17]. However these jamming solutions deal with wireless devices that transmit their own signal, in which case the jamming signal *adds up* to the protected data. RFIDs on the other hand simply reflect the reader's signal without transmitting a signal of their own. Hence their communication model is *multiplicative*. More importantly, except for [16], none of these systems addresses MIMO. The work in [16] assumes the jammer and the transmitter of the protected signal are within a few centimeters of each other, and does not work otherwise. In contrast, LocRF can overcome a MIMO eavesdropper that has more antennas that the trusted system without imposing constraints on device locations.

9. Conclusion

Recent eavesdropping attacks have compromised the security of billions of deployed RFIDs worldwide. This paper asks the question whether one can secure these simple RFIDs from eavesdropping attacks, without modifying the cards. By only implementing changes on the RFID reader, LocRF introduces the idea of randomized modulation and its rotating antenna extension to overcome powerful MIMO adversaries. We analytically and empirically demonstrated that randomizing the modulation via reflection, and randomizing the wireless channels by using a rotating antenna can effectively protect today's widely used commercial RFIDs from eavesdroppers. Further, we believe the rotating antenna scheme can be combined with multiple existing security primitives, which will open doors to a variety of new designs in wireless security beyond the scope of RFID communication.

References

[1] M. B. Abdelhalim, M. El-Mahallawy, M. Ayyad, and A. Elhennawy. Design and implementation of an encryption algorithm for use in rfid system. In *IJRFIDSC*, 2012.

[2] Alien Technology Inc. ALN-9640 Squiggle Inlay. www.alientechnology.com.

[3] U. Azad, H. C. Jing, and Y. E. Wang. Budget and capacity performance of inductively coupled resonant loops. In *IEEE Trans. on Antennas and Propagation*, 2012.

[4] M. Barni, F. Bartolini, A. De Rosa, and A. Piva. Optimum Decoding and Detection of Multiplicative Watermarks. *IEEE Transactions on Signal Processing*, 2003.

[5] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede. Public-key cryptography for rfid-tags. In *PERCOM*, 2007.

[6] S. C. Bono, M. Green, A. Stubblefield, A. Juels, A. D. Rubin, and M. Szydlo. Security analysis of a cryptographically-enabled rfid device. In *USENIX Security Symposium*, 2005.

[7] M. Buettner and D. Wetherall. A software radio-based uhf rfid reader for phy/mac experimentation. *IEEE RFID*, 2011.

[8] C. Castelluccia and G. Avoine. Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags. In *CARDIS*, 2006.

[9] H.-J. Chae, D. J. Yeager, J. R. Smith, and K. Fu. Maximalist cryptography and computation on the WISP UHF RFID tag. In *Proceedings of the Conference on RFID Security*, 2007.

[10] D. M. Dobkin. UHF reader eavesdropping: Intercepting a tag reply, 2009. www.enigmatic-contulting.com.

[11] EPCglobal Inc. EPCglobal Class 1 Generation 2 V. 1.2.0. http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2.

[12] Frost & Sullivan. Global RFID Market 2011.

[13] F. Garcia, G. Gans, R. Muijrers, P. Rossum, R. Verdult, R. Schreur, and B. Jacobs. Dismantling MIFARE classic. ESORICS, 2008.

[14] S. Goel and R. Negi. Guaranteeing secrecy using artificial noise. *IEEE Trans. on Wireless Communication*, 2008.

[15] A. Goldsmith. *Wireless Communications*. Cambridge University Press, 2005.

[16] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu. They can hear your heartbeats: non-invasive security for implantable medical devices. In *SIGCOMM 2011*.

[17] S. Gollakota and D. Katabi. Physical layer wireless security made fast and channel independent. In *INFOCOM '11*.
[18] G. P. Hancke. Practical attacks on proximity identification systems. In *IEEE Symposium on Security and Privacy*, 2006.
[19] E. Haselsteiner and K. Breitfu. Security in near field communication (nfc). In *EURASIP J. Adv. Signal Process*, 2008.
[20] J. Heiskala and J. Terry. *OFDM Wireless LANs: A Theoretical and Practical Guide*. Sams Publishing, 2001.
[21] S. Hong, J. Mehlman, and S. Katti. Picasso: Flexible RF and Spectrum Slicing. In *SIGCOMM*, 2012.
[22] Impinj Speedway. R420 RFID reader. www.impinj.com.
[23] E. Inc. Universal Software Radio Peripheral. http://ettus.com.
[24] A. Juels, R. L. Rivest, and M. Szydlo. The blocker tag: selective blocking of rfid tags for consumer privacy. CCS'03.
[25] N. K. Kalantari, S. M. A. Ahadi, and H. Amindavar. A universally optimum decoder for multiplicative audio watermarking. In *ICME*, 2008.
[26] A. Khisti and G. W. Wornell. Secure transmission with multiple antennas: part II: the MIMOME wiretap channel. *IEEE Transactions on Information Theory*, 2010.
[27] H. Kortvedt and S. Mjolsnes. Eavesdropping near field communication. The Norwegian Info. Security Conf., 2009.
[28] K. Koscher, A. Juels, V. Brajkovic, and T. Kohno. EPC RFID Tag Security Weaknesses and Defenses: Passport Cards, Enhanced Drivers Licenses, and Beyond. CCS, 2009.
[29] Laird Technologies. Crushcraft S9028PCRW RFID antenna. http://www.arcadianinc.com/.
[30] Massachusetts Bay Transportation Authority. The Charlie Card Reusable Ticket System. www.mbta.com.
[31] MasterCard Worldwide. PayPass. www.paypass.com.
[32] National Institute of Standards and Technology. Guidelines for Securing Radio Frequency Identification Systems, 2007.
[33] NETGEAR. 3dhd wireless: Wifi technology for hd and 3dhd delivery, 2010.
[34] P. Nikitin and K. Rao. Effect of gen2 protocol parameters on rfid tag performance. In *IEEE RFID*, 2009.
[35] NXP Semiconductors. MIFARE Classic. http://mifere.net/overview/mifare-standards/.
[36] K. Paget. Credit Card Fraud: The Contactless Generation. ShmooCon, 2012.
[37] J. Park and T. Lee. Channel-aware line code decision in rfid. In *IEEE Communications Letters*, 2011.
[38] J. Parsons. *The Mobile Radio Propagation Channel*. 2000.
[39] Pfizer Inc. Counterfeit Pharmaceuticals. Tech. Report, 2007.
[40] R. Ryan, Z. Anderson, and A. Cheisa. Anatomy of a Subway Hack. DEFCON, 2008.
[41] S. Sarma. Some issues related to RFID and Security, 2006. Keynote Speech in Workshop on RFID Security.
[42] O. Savry, F. Pebay-Peyroula, F. Dehmas, G. Robert, and J. Reverdy. Rfid noisy reader how to prevent from eavesdropping on the communication? CHES '07, 2007.
[43] ThingMagic. RFID Security issues - Generation2 Security. www.thingmagic.com.
[44] Travelon, Inc. RFID Blocking. www.travelonbags.com.
[45] D. Tse and P. Vishwanath. *Fundamentals of Wireless Communications*. Cambridge University Press, 2005.
[46] R. Verdult, F. Garcia, and J. Balasch. Gone in 360 seconds: Hijacking with hitag2. In *USENIX Security*, 2012.
[47] K. Yazdandoost and K. Sayrafian. Channel Model for Body Area Network (BAN). IEEE P802.15 Wireless Personal Area Networks, 2009.
[48] T. Zimmerman. Assessing the capabilities of RFID technologies. Gartner, 2009.
[49] Zipcar, Inc. www.zipcar.com/how/technology.

APPENDIX A.
ANALYSIS OF LOCRF'S RANDOM MODULATION

A.1. Eavesdropper's Optimal Decoder

For each bit b transmitted by the RFID card, the eavesdropper receives k samples $\{Y_1, \cdots, Y_k\}$ where

$$Y_i = \begin{cases} R_i \cdot (1 + p_i^0) & \text{if } b = 0 \\ R_i \cdot (1 + p_i^1) & \text{if } b = 1 \end{cases} \tag{12}$$

$\{p_1^0, p_2^0, ..., p_k^0\}$ is the pattern when the card transmits a '0' bit and $\{p_1^1, p_2^1, ..., p_k^1\}$ is the pattern for a '1' bit. Each element in these patterns can be equal to $\tilde{x}_0$ or $\tilde{x}_1$ depending on the pattern used by the RFID card where from Eq. 3, $\tilde{x}_0 = \frac{h_{card \to eve}}{h_{reader \to eve}} x_0$ and $\tilde{x}_1 = \frac{h_{card \to eve}}{h_{reader \to eve}} x_1$. R_i is the random sample drawn from a complex normal distribution with zero mean and standard deviation σ. Hence, each received sample Y_i is also complex normal with zero mean and standard deviation $\sigma|1 + p_i^0|$ for $b = 0$, or $\sigma|1 + p_i^1|$ for $b = 1$.

The maximum likelihood decoder is defined as:

$$Pr(b = 1|\{Y_1, \cdots, Y_k\}) \underset{0}{\overset{1}{\gtrless}} Pr(b = 0|\{Y_1, \cdots, Y_k\})$$

Because the card's bits have equal probability of being '0' or '1' [11], [35], we can rewrite the hypothesis test as:

$$Pr(\{Y_1, \cdots, Y_k\}|b = 1) \underset{0}{\overset{1}{\gtrless}} Pr(\{Y_1, \cdots, Y_k\}|b = 0)$$

Given $b = 0$, the k samples in $\{Y_1, \cdots, Y_k\}$ become independent Gaussians with zero mean and standard deviation $\sigma_i^0 = \sigma|1 + p_i^0|$. Hence, we can write:

$$Pr(Y|b = 0) = \frac{1}{(2\pi)^{k/2} \prod \sigma_i^0} \cdot \exp\left(- \sum_i^k \left(\frac{|Y_i|}{\sigma_i^0} \right)^2 \right) \tag{13}$$

A similar equation can be derived for $b = 1$. Assuming the two patterns have the same number of $\tilde{x}_0$ samples, then $\prod \sigma_i^0 = \prod \sigma_i^1$. The maximum-likelihood decoder becomes:

$$\sum_i^k \left(\frac{|Y_i|}{\sigma_i^1} \right)^2 \underset{0}{\overset{1}{\lessgtr}} \sum_i^k \left(\frac{|Y_i|}{\sigma_i^0} \right)^2 \tag{14}$$

Without loss of generality, assuming $|1+\tilde{x}_1| > |1+\tilde{x}_0|$, given the patterns p^0 and p^1 for HF RFIDs [42], we can simplify the hypothesis test to:

$$|Y_2|^2+|Y_4|^2+|Y_6|^2+|Y_8|^2 \underset{0}{\overset{1}{\lessgtr}} |Y_9|^2+|Y_{11}|^2+|Y_{13}|^2+|Y_{15}|^2$$

A similar hypothesis test can be dervied for UHF RFIDs.

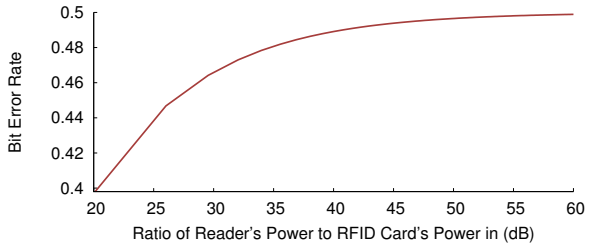


Figure 16—Theoretical BER at the eavesdropper as a function the ratio of the reader's signal to the RFID's reflected signal.

A.2. Bit Error Rate of Eavesdropper

Here we derive the bit error rate (BER) at the eavesdropper for the case of HF RFID cards. The analysis is the same for the UHF RFID cards. We define random variables $U = |Y_2|^2+|Y_4|^2+|Y_6|^2+|Y_8|^2$, $V = |Y_9|^2+|Y_{11}|^2+|Y_{13}|^2+|Y_{15}|^2$, and $Z = U - V$. Based on the optimal decoder in A.1 the bit error rate at the eavesdropper is calculated as:

$$BER = \frac{1}{2}Pr(Z < 0|b = 0) + \frac{1}{2}Pr(Z > 0|b = 1)$$

Given $b = 0$, $\{Y_2, Y_4, Y_6, Y_8\}$ are independent complex Gaussian random variables with zero mean and standard deviation $\sigma_U = \sigma|1 + \tilde{x}_1|$ while $\{Y_9, Y_{11}, Y_{13}, Y_{15}\}$ are independent complex Gaussian random variables with zero mean and standard deviation $\sigma_V = \sigma|1 + \tilde{x}_0|$. Thus, U and V have a Gamma distribution where $U \sim \Gamma(4, 2\sigma_u^2)$ and $V \sim \Gamma(4, 2\sigma_v^2)$. We derive $\Pr_Z(z|b = 0)$ and then calculate:

$$\begin{aligned} Pr(Z < 0|b = 0) &= \int_{-\infty}^{0} \Pr_Z(z|b = 0)dz \\ &= \frac{20\mu^3}{(1+\mu)^7} + \frac{10\mu^2}{(1+\mu)^6} + \frac{4\mu}{(1+\mu)^5} + \frac{1}{(1+\mu)^4} \end{aligned}$$

where $\mu = |1 + \tilde{x}_1|^2/|1 + \tilde{x}_0|^2$. One can further prove that $Pr(Z > 0|b = 1) = Pr(Z < 0|b = 0)$. Hence the eavesdropper's BER using the optimal decoder is:

$$BER = \frac{20\mu^3}{(1+\mu)^7} + \frac{10\mu^2}{(1+\mu)^6} + \frac{4\mu}{(1+\mu)^5} + \frac{1}{(1+\mu)^4} \quad (15)$$

As μ approaches 1, the BERbecome $1/2$. Since the RFID card's reflection is much smaller than the reader's signal, we have $|\tilde{x}_0|, |\tilde{x}_1| \ll 1$ and $\mu \approx 1 + \epsilon$ where $|\epsilon| << 1$. We can see from this equation that the BER depends on how much smaller is the RFID card's reflection as compared to the LocRF reader's signal. Fig. 16 shows the eavesdropper's BER as a function of the ratio of the reader's signal power and the RFID card's reflected power at the eavesdropper. For typical ratio of 30dB to 50dB, the BER is between 46.4% and 49.6%. This result is under the assumption of no wireless channel noise, which is favorable for the adversary.

APPENDIX B.
ROTATING ANTENNA IN HIGH DIMENSIONS

We discuss the impact of using a rotating antenna and a static antenna at the reader on a 3-antenna eavesdropper and then generalize to n-antenna eavesdroppers.

First, consider the case if the reader uses *two static* antennas to transmit $r_1(t)$ and $r_2(t)$. A 3-antenna eavesdropper receives the signals $y_1(t), y_2(t), y_3(t)$ on each of his antennas:

$$\begin{bmatrix} y_1(t) \\ y_2(t) \\ y_3(t) \end{bmatrix} = \left(\begin{bmatrix} h_{r_{11}} & h_{r_{21}} \\ h_{r_{12}} & h_{r_{22}} \\ h_{r_{13}} & h_{r_{23}} \end{bmatrix} + x(t) \cdot \begin{bmatrix} h_{c_{11}} & h_{c_{21}} \\ h_{c_{12}} & h_{c_{22}} \\ h_{c_{13}} & h_{c_{23}} \end{bmatrix} \right) \cdot \begin{bmatrix} r_1(t) \\ r_2(t) \end{bmatrix} \quad (16)$$

where $h_{r_{ij}}$ is the channel coefficient from the LocRF reader's i-th to the eavesdropper's j-th antenna. $h_{c_{ij}}$ is the channel of the card's reflection of $r_i(t)$ to the adversary's j-th antenna.

Recall that $x(t)$ has two states: x_0 or x_1. For the x_0 state, based on Eq. 16, one can prove the following:

$$\Delta_{2,3} \cdot y_1(t) - \Delta_{1,3} \cdot y_2(t) + \Delta_{1,2} \cdot y_3(t) = 0, \quad (17)$$

where

$$\begin{aligned} \Delta_{i,j} = \quad & (h_{r_{1i}} + h_{c_{1i}} \cdot x_0)(h_{r_{2j}} + h_{c_{2j}} \cdot x_0) \\ & - (h_{r_{2i}} + h_{c_{2i}} \cdot x_0)(h_{r_{1j}} + h_{c_{1j}} \cdot x_0), \end{aligned} \quad (18)$$

which defines a plane in a 3-dimensional space. When $x(t) = x_1$ a different plane can be derived. Since all channels are constant, the two planes corresponding to x_0 and x_1 are static. Hence, the eavesdropper can distinguish x_0 samples from x_1 samples by mapping them to one of the two planes.

Now consider the case where the first antenna of the reader is rotating. The channels $h_{r_{1i}}$ and $h_{c_{1i}}$ are changing randomly and hence the Δ_{ij} coefficients in Eq. 18, which define the planes will also change randomly. In this case, no particular plane in the eavesdropper space is unique to x_0, as opposed to x_1. Said differently, a sample corresponding to x_0 in the 3-dimensional space can also correspond to x_1 once the channel coefficients have changed. Thus, the eavesdropper will not be able to distinguish the x_0 samples from the x_1 samples to decode.

When the eavesdropper has n antennas, he receives n signals $y_1(t), \cdots, y_n(t)$ where:

$$\begin{bmatrix} y_1(t) \\ \vdots \\ y_n(t) \end{bmatrix} = \left(\begin{bmatrix} h_{r_{11}}(t) & h_{r_{21}} \\ \vdots & \vdots \\ h_{r_{1n}}(t) & h_{r_{2n}} \end{bmatrix} + x(t) \cdot \begin{bmatrix} h_{c_{11}}(t) & h_{c_{21}} \\ \vdots & \vdots \\ h_{c_{1n}}(t) & h_{c_{2n}} \end{bmatrix} \right) \cdot \begin{bmatrix} r_1(t) \\ r_2(t) \end{bmatrix}$$

Consider the samples received in one occurrence of the x_0 state:

$$\begin{bmatrix} Y_1 \\ \vdots \\ Y_n \end{bmatrix} = \begin{bmatrix} H_{r_{11}} + H_{c_{11}} \cdot x_0 \\ \vdots \\ H_{r_{1n}} + H_{c_{1n}} \cdot x_0 \end{bmatrix} \cdot R_1 + \begin{bmatrix} h_{r_{21}} + h_{c_{21}} \cdot x_0 \\ \vdots \\ h_{r_{2n}} + h_{c_{2n}} \cdot x_0 \end{bmatrix} \cdot R_2$$

We use capital letters to denote the random variables.

For any point in the n-dimensional antenna space $Y_1 \cdots Y_n$, a set of R_1, R_2 and $H_{r_{1i}}$'s and $H_{c_1 i}$'s exist that satisfy the above equation. In other words, the samples corresponding to x_0 state are not confined to a subspace, but rather can span the n-dimensional space. One can prove the same for x_1. Thus, the eavesdropper cannot distinguish the samples it receives during x_0 state from x_1 state.