HF RFID Electromagnetic Emissions and Performance

David R. Novotny Jeffrey R. Guerrieri Michael Francis Kate Remley
Electromagnetics Division
National Institute of Standards and Technology
325 Broadway
Boulder, Colorado 80305

***Abstract*— We examined the emissions of commercial HF (High-Frequency) proximity RFID (Radio Frequency Identification) systems and the performance of a typical RFID system in the presence of electromagnetic (EM) interference. Some initial investigations into security and reliability were also performed. These investigations highlight detectability and readability of an RFID transaction at a distance. We performed measurements to determine the power radiated by some commercial systems and monitored the RFID transaction in adverse EM environments.**

***Keywords*—RFID, HF, ISO 14443, jamming, communication, eavesdropping**

I. INTRODUCTION

HF proximity RFID systems are being used in an increasing number of critical applications such as financial (credit cards), access control, identity verification, and inventory tracking. Some of these applications involve the transfer of proprietary or biometric information, and the privacy of any information as well as, the reliability of the transmission link can be very important. These preliminary measurements discuss how detectable these transactions are at a distance and their resistance to interference from outside sources.

HF proximity RFID systems operate in the 13.56 MHz Industrial, Scientific, and Medical (ISM) band and are governed primarily by ISO standards 14443, 15693, 18000-3 and 18092 [1-4]. This ISM band is also populated with a large number of HF systems such as high-power plasma generators, medical telemetry equipment and unlicensed communication equipment. Operational compatibility in the presence of other ISM systems must be maintained for lower-power HF proximity RFID to function correctly.

HF proximity RFID systems were designed to operate at a range of 10 cm or less. This range is limited by the power available to energize a passive tag. Limits are placed on allowable transmitted magnetic field levels at a given distance (7.5 A/m at 37.5 mm from the antenna).

The practical effect is that standard-compliant HF proximity RFID has a limited transaction range on the order of 10 to 20 cm. However, the information transmitted by a remotely powered tag and reader can be detected from quite a bit farther [5].

These measurements [6] hope to highlight the operating conditions in which these commercial RFID systems can be used and some basic issues regarding security and range at which a transaction can be detected. Note that eavesdropping is defined here as detecting and inferring data from a legitimate reader-to-tag transaction using another remote system. Skimming, the use of a remote reader to surreptitiously query a tag at a long distance (possibly without the tag holder's consent), is not addressed in this paper.

II. PROTOCOL AND BACKGROUND

HF RFID systems operating at 13.56 MHz come in two forms: proximity and vicinity. Proximity tags generally require more power to operate, but generally have much more information and functionality (for example: active encryption, limited amounts of processing power, and data storage and retrieval). The power requirements for tag activation and operation generally limit operation to less than 20 cm. Vicinity tags are typically a simple read device that will send back a limited number of bits (1 to 64) at lower data rates than proximity tags. They are more generally employed in scenarios such as inventory control and theft deterrence systems. The limited functionality of these devices requires less power and can be used in the 2-5 meter range. As proximity tags generally contain more information and are used in more critical applications, this study focuses on proximity systems. The term "HF RFID" will be assumed from this point forward to mean HF proximity RFID.

There are at least four kinds of proximity systems that operate at 13.56 MHz. They differ in the communication protocol: the ISO compliant "type A" and "type B" systems, the "GO-card" employed in some transportation, transit and fare systems (the DC transit system is a notable example), and the "type C" card used mainly in Asia in fare and tariff systems. We will further focus our study on an analysis of the ISO compliant "type A" and "type B" tags, as they are used in a wider scope of applications and utilize ISO conformance standards.

III. HF Proximity Emissions and Susceptibility

A. HF RFID Emissions

HF proximity reader/interrogators transmit a carrier frequency f_c=13.56 MHz, modulated at a data rate, f_d, of f_c/128=105.9375 kHz, f_c/64=211.875 kHz, f_c/32 = 423.75 kHz, or f_c/16=847.5 kHz. The HF RFID tags modulate a backscattered carrier to produce sub-carrier transmissions back to the reader at f_s =f_c ± f_c/16=13.56 ±0.8475 MHz = 14.4075 and 12.7125 MHz. These sub-carriers are modulated at one of the data rates available to the interrogator. One should note that the lower side-band modulation falls into a maritime-mobile band. The upper side-band modulation overlaps with an aviation band. Furthermore, the relatively wide modulation bandwidth of the carrier frequency can smear energy from the reader at 13.56 MHz ± f_d. Similarly, the tag radiates in the 12.7125 MHz ±f_d to 14.4075 MHz± f_d range.

While the very low power emissions from the tag are probably of little concern to maritime or aviation applications, the modulation spill over from the reader can be much higher and may extend beyond the ISM limited 13.56 MHz ± 7 kHz and comes very close to the prohibited radio astronomy band from 13.36 to 13.41 MHz. Patents are now being issued for ISM communications and non-standard tagging systems that suppress effects of RFID sidebands and limit system susceptibility to wideband interference [7].

B. HF Eavesdropping and Transaction Interupption

From Fig. 1 and Fig. 2 we see that the 13.56 MHz carrier is on during the entire transaction to deliver power to the tag. The carrier is modulated to send information to the tag(s). Since the tag lacks a power source and only modulates the load on its loop antenna to scatter back information, the returned signal is small compared to the carrier (typically 60 dB less than the carrier at a distance beyond 10 cm).

Eavesdropping systems must be able to distinguish the very weak tag response from the relatively strong carrier signal. Aggressive filtering needs to be done to detect the tag in the presence of the reader at moderate distances (over several meters).

Since HF RFID systems typically rely on relatively low power transmissions, they may be prone to interference from intentional jamming and unintentional sources. Jamming can occur either by interrupting tag-to-reader communications, by interfering with the carrier or the reader information, or by interfering with the reader-to-tag transaction. As the reader is transmitting several watts and is in the very near-field of the tag, to overcome the carrier at the tag requires a considerable amount of power if an interfering source is at a distance. Because tag-to-reader power levels are orders of magnitude less than the carrier, it is easier to upset the transaction by overpowering the weakest link in the RF power budget.

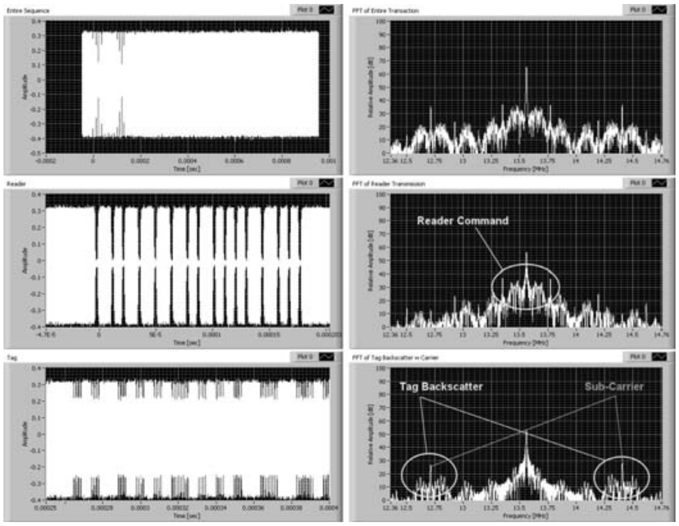

Figure 1. Typical ISO 14443 Typt A emission spectrum. The top graphs show the entire two-way communication in both the time-domain (left) and frequency-domain (right). The reader-to-tag query is in the middle and the tag-to-reader response is at the bottom. Note that the reader must maintain the carrier for the passive tag to recieve power.

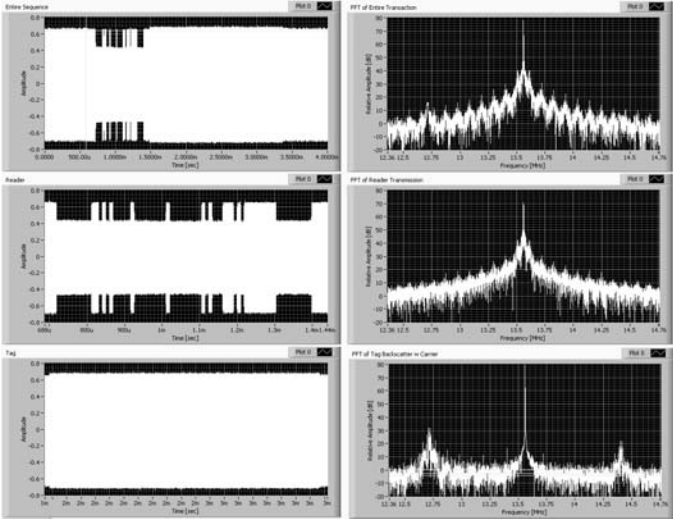

Figure 2. Typical ISO 14443 Type B emission spectrum. The top graphs show the entire two-way communication in both the time-domain (left) and frequency-domain (right). The reader-to-tag query is in the middle and the tag-to-reader response is at the bottom. The tag responds with a constant phase-modulated CW return signal at f_c ±f_d =13.56 ± 0.8475 MHz.

IV. Measurement Setup

A. Eavesdropping

We attempted to eavesdrop on a commercial-off-the-shelf (COTS) reader and COTS tag. We chose several tags including a type A tag with 16 kB of memory to perform these initial tests. This type of tag is being suggested for RFID financial transactions and this tag has a processor capable of performing fairly complex computational and encryption tasks.

The reader and the tag are coupled loops that are typically axially aligned (see Fig. 3). To study the RFID emissions, the orientation of the reader and tag was kept constant and the eavesdropping antenna was moved relative to them. Since the reader and the tag antennas are electrically small loops, it can be assumed that the radiation pattern of the system conforms to the simple loop fields given by Harrington [8]:

$$H_r = \frac{IS}{2\pi} e^{-jkr} \left(\frac{jk}{r^2} + \frac{1}{r^3} \right) \cos\theta,$$

$$H_\theta = \frac{IS}{4\pi} e^{-jkr} \left(\frac{-k^2}{r} + \frac{jk}{r^2} + \frac{1}{r^3} \right) \sin\theta, \qquad (1)$$

$$E_\phi = \frac{\eta IS}{4\pi} e^{-jkr} \left(\frac{k^2}{r} - \frac{jk}{r^2} \right) \sin\theta,$$

where $\boldsymbol{r}$ is the distance from the tag to an outside point, $\boldsymbol{\theta}$ is the elevation angle (see Fig. 4), $\boldsymbol{I}$ is the current in the loops, $\boldsymbol{S}$ is the surface area, $\boldsymbol{\eta}$ is the impedance of free space, and $\boldsymbol{k}$ is the wave number.

For small distances, $\boldsymbol{r}$, the axial magnetic field, $\boldsymbol{H_r}$, is stronger than the $\boldsymbol{\theta}$-directed field, $\boldsymbol{H_\theta}$. But, as distance increases, the $1/\boldsymbol{r}$ dependence of $\boldsymbol{H_\theta}$ dominates. So we expect that at close distances $<\lambda/4$, eavesdropping is easier directly above the reader (Fig. 5) and at larger distances $>\boldsymbol{\lambda}$, eavesdropping should be easier in the plane of the reader antenna (orientation of Fig. 6).

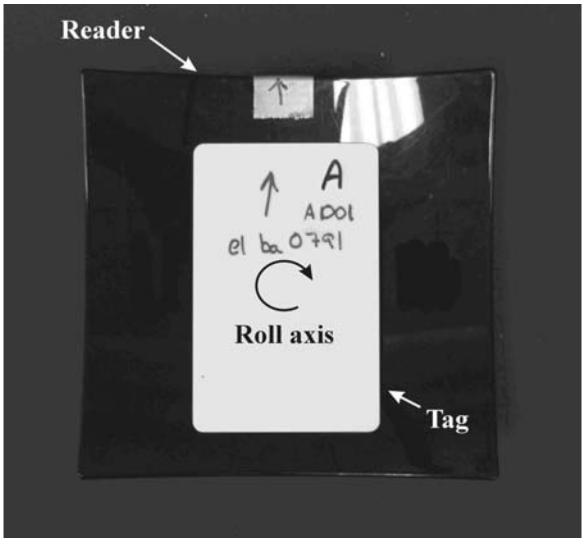

Figure 3. Orientation of the reader and tag. The tag was kept in the plane of the reader to allow for optimal communication.

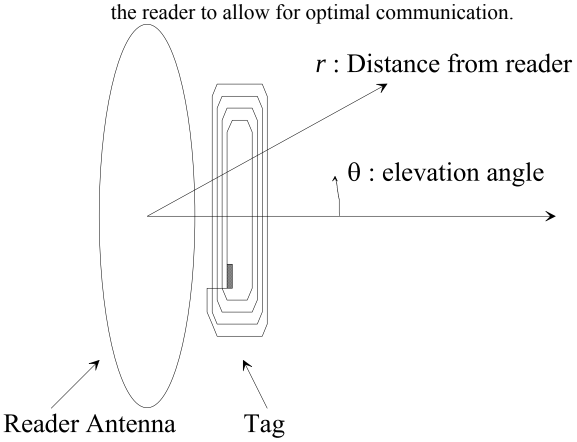

Figure 4. Relative directions for eavesdropping on an HF RFID system. When close to the reader, coupling is best at low elevation angles *(θ=0°)*. When farther away (approaching a wavelength ~20 m), eavesdropping should be more efficient at *θ=90°*.

We used a single 1 m loop with a capacitive bridge to match to the 50 Ω input of the receiving system. The receiver nominally had 60 dB of gain at the sub-carrier $f_c + f_c/16$ and had 70 dB of relative rejection at the carrier frequency f_c. This allowed for detection of the carrier modulation and the tag response while suppressing the carrier power. Our tests showed that, if we found the tag response to be 6 dB above the noise floor of the system, the information in the signal could be reliably decoded. This provided the criterion for a successful eavesdropping session.

Fig. 7 shows the raw output of the eavesdropping antenna at 2 m. Without filtering, the reader modulation can easily be distinguished; however, the tag response cannot. Fig. 8 shows the effect of the receiver filtering. The tag and reader are both distinguishable and information can be decoded.

Table 1 shows the results of the eavesdropping tests. Other groups have reported considerably longer range results in more idealized testing environments [5]. We limited these tests to using low-cost COTS equipment, "small" antennas, and performed these tests in a non-ideal, RF cluttered environment. By placing the tag at an optimal distance from the reader antenna, the RFID system can be tuned to maximally radiate outward (which was not done for this test). It can be inferred from the results in Table 1 that the eavesdropping distance is strongly tied to tag design. We saw little variation in the activation field (field level to turn on the tag) between these tags, but we had appreciable eavesdropping distance variations.

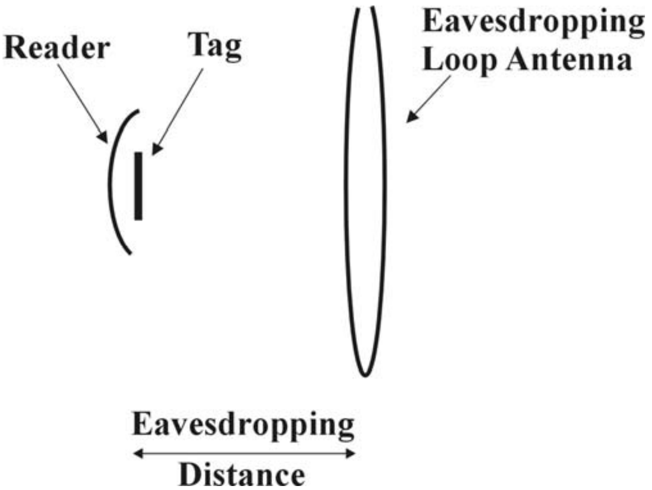

Figure 5. Orientation for close in eavesdropping *(θ=0°)*.

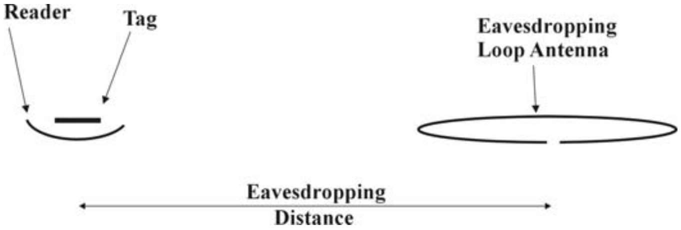

Figure 6. Orientation for long distance eavesdropping *(θ=90°)*.

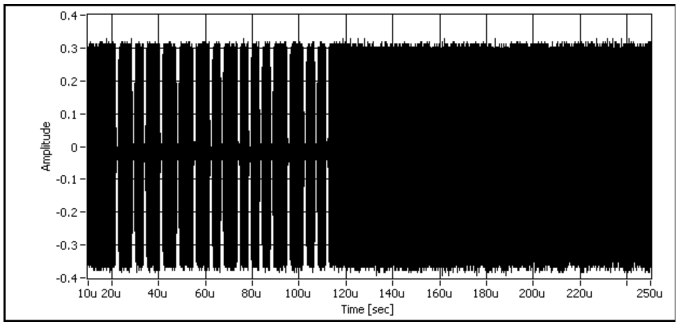

Figure 7. Raw signal out of the eavesdropping antenna at 2 m. Note the tag response cannot be readily distinguished.

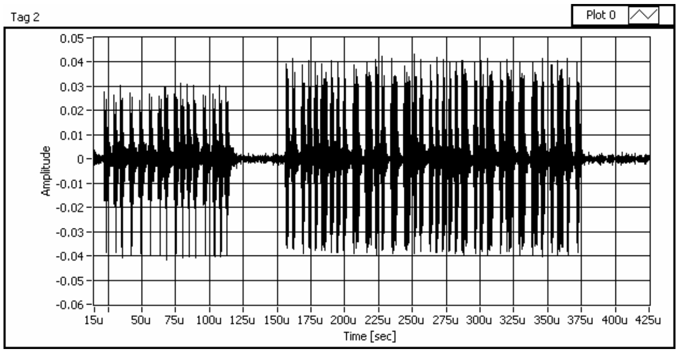

Figure 8. Results of an eavesdropped Type A transaction at 2 m distance after processing by the receiver. The burst on the left is the transitions in the carrier modulation. The burst on the right is the tag response.

TABLE 1.
Eavesdropping Results for Type A Tags

Manufacturer	Tag number	Eavesdropping distance (θ=0°) (see Fig. 7)	Eavesdropping distance (θ=90°) (see Fig. 8)
1	A001	6.5 m	15 m
1	A002	6.5 m	15 m
2	A003	5 m	9 m
2	A004	5 m	9 m
2	A005	5 m	9 m
3	A006	6 m	8 m
4	A007	6 m	8 m

.

B. *Jamming*

To test the communications reliability of these HF RFID systems, they were subjected to in-band interference. Previous swept-frequency measurements showed they were most vulnerable to upset only near the frequency band of operation. It seems reasonable that jamming at the carrier and sub-carriers would provide the opportunity to upset the communication between the reader and tag.

We used three types of antennas (see Fig. 9): a set of dual 1 m loop antennas, a single 15 cm ISO 10373-6 standard proximity coupling device (PCD) loop, and a set of dual 15 cm ISO 10373-6 standard PCD loops. Each antenna was tuned to the frequency of the jamming signal (retunes between tests were required). The 1 m loops represent an easily deployable and relatively efficient transmit configuration. The 15 cm loops represent a small device with less radiation efficiency or a nearby RFID system.

Several interference scenarios were studied: jamming at the carrier or reader transmit frequency f_c, and the upper and lower sub-carriers or tag backscatter frequency f_s. Previous studies using broadband frequency sweeps have shown much lower susceptibility of typical commercial RFID systems at frequencies other than f_s and f_c.

To ensure maximum readability of the signal by the reader and to present the most difficult upset scenario, the tag was placed in close proximity to the reader antenna (within the limits of the reader geometry < 0.5 cm). If the tag is farther from the reader, but still within its nominal operating range (<10 cm), the transaction is much easier to upset, as the tag backscatter falls off very rapidly with near-field distance.

Three basic waveforms were used to mimic probable threat scenarios: a continuous wave (CW) source at f_c (another RFID reader or other ISM equipment), a CW carrier at the sub-carrier frequency $f_c + f_s$ (a generic CW interference source), and a CW carrier at the sub-carrier frequency $f_c + f_s$, modulated at f_d (a nearby tag or intentional interference).

The power delivered to the antenna was monitored to ensure that tuning was correct (Fig. 10). As some HF RFID systems have robust data failure and retry algorithms, only when consistent data failures were noted was jamming of the RFID transaction considered successful.

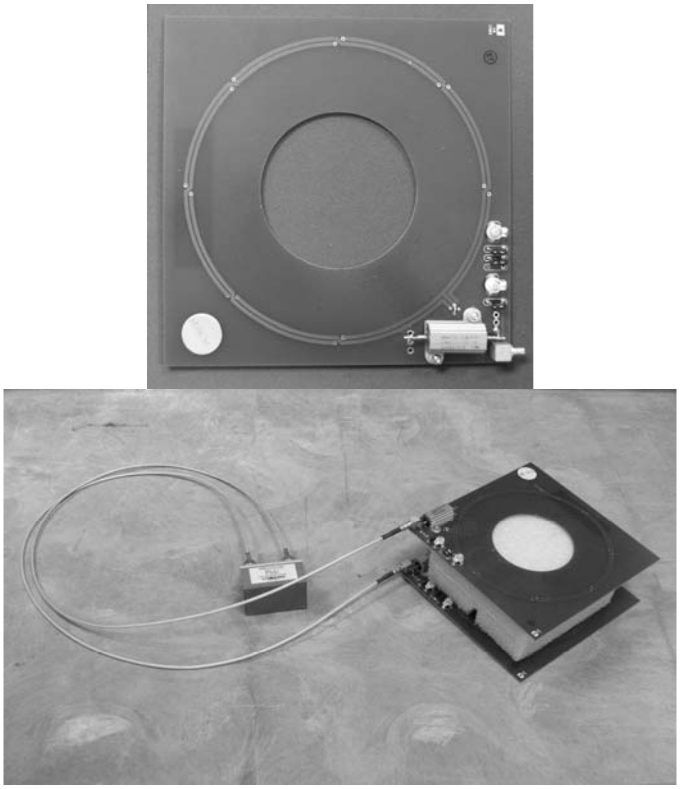

Figure 9. Single PCD loop antenna (top and stacked PCD loop antennas (bottom).

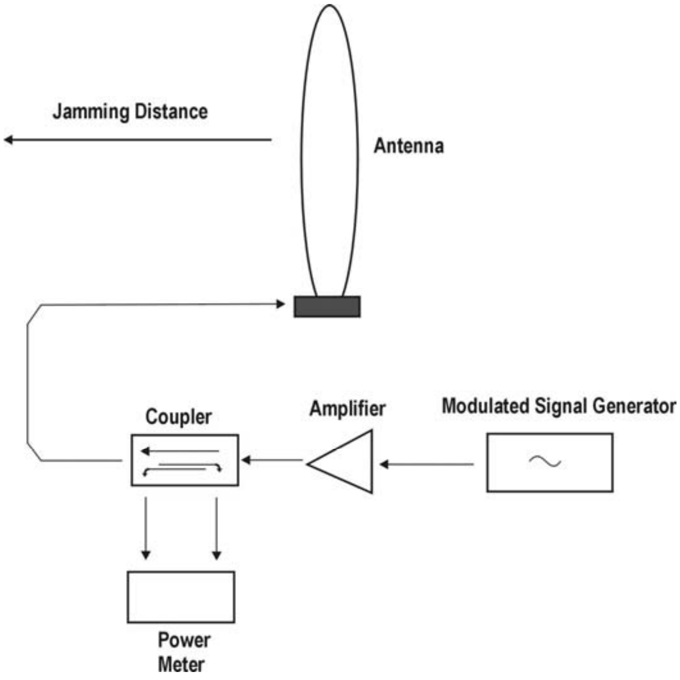

Figure 10. Jamming system overview.

Tables 2-4 show results for jamming at selected distances and powers. The 13.56 MHz CW signal is representative of another piece of ISM equipment or another RFID reader. This becomes a concern if readers are stacked too closely together or operating near other unlicensed equipment. The sub-carrier signals are less likely to be encountered randomly and represent a concerted attempt to interfere with the transaction. It should be noted that the power required to disrupt the transaction at the lower sub-carrier (12.7125 MHz) was generally slightly greater (~10 %) than the power required to disrupt the transaction at the upper sub-carrier frequency. We attribute this mainly to the slightly less efficient nature of the antenna at the longer wavelength.

TABLE 2
Jamming Results CW Carrier at f_c (13.56 MHz)

Antenna	Distance	Power to disrupt transaction
Dual 1m loops	5m	10 W
Single PCD antenna	2m	12 W
Dual PCD antenna	2m	10.5 W

TABLE 3
Jamming Results for CW Sub-Carrier at $f_c + f_s$ (14.4075MHz)

Antenna	Distance	Power to disrupt transaction
Dual 1m loops	8m	3.7 W
Single PCD antenna	3m	7 W
Dual PCD antenna	3m	6.9 W

TABLE 4
Jamming Results for "Data-Like" Modulated Sub-Carrier at $f_c + f_s$ (14.4075MHz)

Antenna	Distance	Power to disrupt transaction
Dual 1m loops	8m	0.3 W
Single PCD antenna	5m	3 W
Dual PCD antenna	5m	2.8 W

Many ISM transmission systems operating at this frequency deliver in the range of 5 to 7 watts to the antenna, even with the low efficiency of these small antennas, ISM system interference can be a problem and should be considered.

Table 5 lists the approximate magnetic field level needed to disrupt the RFID transaction when a typical tag is located very close to the reader. If the tag is farther from the reader, then transaction interruption could possibly occur at lower levels.

TABLE 5.
Approximate Magnetic Field (***H***) Required at the Reader to Jam a Transaction.

Antenna	***H*** Field @ tag to disrupt transaction
13.56 MHz	1.1 mA/m rms
14.4075 MHz	300 µA/m rms
Modulated 14.4075 MHz	75 µA/m rms

V. Conclusion and Insights

HF RFID systems may transmit sensitive data and may be vulnerable to common interference or malicious RF attacks. We explored the ability to eavesdrop on an HF RFID transaction at a distance. Our findings show that detection of information can be performed. The use of strong encryption can greatly diminish the potential for loss of critical information. RFID communications can be disrupted with by either unintentional interference or with much lower power by "RFID-like" waveforms. While the waveforms are not likely encountered from unintentional sources, they can easily be generated and used in a malicious manner to disrupt critical systems depending on the RFID transaction.

Many RFID systems do employ various levels of encryption. However, many building access and inventory systems are based on un-encoded data on the tags. These may be vulnerable to eavesdropping and replay style attacks. We have noted that properly shielded RFID readers, while being more expensive, have been shown to reduce the potential of eavesdropping and are generally less vulnerable to jamming. Further efforts are being made to reduce eavesdropping potential by introducing variations in the carrier; these alterations may increase the difficulty of synchronizing to the data and thus harder to retrieve useful information [9]. The security of data and system integrity should be considered when deploying RFID systems in critical applications.

Results for a limited number of RFID devices were shown; however, basic trends for eavesdropping and susceptibility to upset have been seen in a number of other unshielded HF proximity RFID systems

Acknowledgments

We acknowledge the sponsorship and support of Tom Karygiannis of the Computer Security Division of the Information Technology Laboratory at NIST for this work.

References

[1] ISO/IEC 14443 Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards.

[2] ISO/IEC 18000-3 Information technology -- Radio frequency identification for item management -- Part 3: Parameters for air interface communications at 13,56 MHz.

[3] ISO/IEC 15693 Identification cards - Contactless integrated circuit(s) cards - Vicinity cards.

[4] ISO/IEC 18092 Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1) and ISO/IEC 21481 Information technology -- Telecommunications and information exchange between systems -- Near Field Communication Interface and Protocol -2 (NFCIP-2).

[5] Finke, T., Kelter, H., Radio Frequency Identification - Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems, Bonn 2004.

[6] Guerrieri, J and Novotny, D, NIST Internal Report 818-7-71,"HF RFID Eavesdropping and Jamming Tests, September 2006", Sept 2007.

[7] European Patent EP1033669

[8] Harrington, R.F., "Time-Harmonic Electromagnetic Fields", McGraw-Hill, New York, 1961, pg. 93.

[9] Hancke, G., "Modulating a noisy carrier signal for eavesdropping-resistant HF RFID", e & i Elektrotechnik und Informationstechnik, Volume 124, Number 11 / November, 2007, pp 404-8.