# Electromagnetic Emissions and Performance for Proximity RFID

Jeff R Guerrieri[1] David R. Novotny[1], Michael H. Francis[1], Kate Remley[1]

[1]*Electromagnetics Division, National Institute of Standards and Technology*

*325 Broadway, Boulder, CO 80305, USA*

[1]guerrieri@boulder.nist.gov

novotny@boulder.nist.gov

francis@boulder.nist.gov

remley@boulder.nist.gov

*Abstract*— **We examined the electromagnetic emissions, and performance of commercial High-Frequency (HF) proximity Radio Frequency Identification (RFID) systems including their susceptibility to jamming and eavesdropping. These proximity RFID systems are used in an increasing number of financial, identification, and access control applications. We performed investigations of whether transactions can be detected and read at a distance. The measurements were performed to determine the power radiated by commercial systems and how they perform in adverse electromagnetic (EM) environments.**

## I. INTRODUCTION

High Frequency (HF) proximity Radio Frequency Identification (RFID) systems are used in an increasing number of critical applications such as financial transactions (credit cards), access control, identity verification, and inventory tracking. Some of these applications involve the transfer of proprietary or biometric information. The privacy of information and reliability of the transmission link is very important. These preliminary measurements show how detectable these transactions are at certain distances 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 primarily governed by International Standards Organization (ISO) standards 14443, 15693, 18000-3 and 18092 [1-4]. This ISM band also contains systems such as high power plasma generators, medical telemetry equipment, and other unlicensed communication equipment. Operational compatibility with these types of systems is necessary for low-power RFID to function correctly.

HF proximity RFID systems are designed to operate at a range of 10 cm or less. This range is limited by the level of field available to power a passive tag. Limits are placed on allowable transmitted 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 at greater distances [5].

The measurements in [6] highlight the operating conditions in which these commercial RFID systems can be used. Some basic issues regarding security and the range at which a transaction can be detected are reported in [7, 8]. Note that eavesdropping is defined for this paper as remotely detecting and deciphering a legitimate reader-to-tag transaction using another system. Skimming, which refers to 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: vicinity and proximity. Proximity tags generally require more power to operate, but they can involve much more information and functionality (for example: active encryption, limited amounts of processing power, data storage and retrieval). The power requirements for activation and operation limit the operating distance to less than 20 cm. Vicinity tags are a simple read device that will send back a limited number of bits (1 to 64) at lower data rates. They are employed in scenarios such as inventory control and theft deterrence systems. Their limited functionality requires less power and can be used in the 2 to 5 meter range. This study focuses on proximity systems. Consequently, HF RFID is assumed to be HF proximity RFID from this point forward in the paper.

There are many types of proximity systems operating at 13.56 MHz. They usually differ in communication protocol: the ISO compliant "type A" and "type B" systems, the "GO-card" used in some fare and transit systems, and the "type C" card used mostly in Asian fare and tariff systems. We will further focus our study on the analysis of the "type A" and "type B" tags, as they are more widely used and utilize ISO conformance standards.

## III. HF PROXIMITY EMISSIONS and SUSCEPTIBILITY

### *A. RFID Emissions*

HF proximity reader/interrogators transmit a carrier frequency, $f_c$, of 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 $f_s = f_c \pm f_c/16$ = 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. We recognize that the lower side-band modulation falls into a maritime-mobile band, and the upper side-band modulation falls into an aviation band. Furthermore, the relatively wide modulation bandwidth of the carrier frequency can smear energy from the reader over a bandwidth of 13.56 MHz $\pm f_d$. Similarly, the tag radiates in the 12.7125 MHz $\pm f_d$ to 14.4075 MHz $\pm f_d$ 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. It comes very close to the prohibited radio astronomy band between 13.36 and 13.41 MHz. Patents are now being issued for ISM communications and nonstandard tagging systems that suppress effects of RFID sidebands and limit system susceptibility [9].

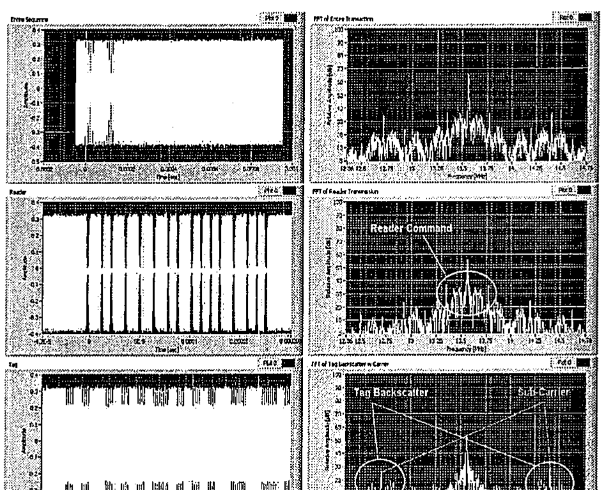


Figure 1. Typical ISO 14443 type A emission spectrum. The top graphs show the entire two-way communication in both the time domain (left) and frequency domain (right). The reader-to-tag query is in the middle, and the tag-to-reader response is at the bottom. Note that the reader must maintain the carrier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

### *B. HF Eavesdropping and Jamming*

In Figure 1 and Figure 2, we see that the 13.56 MHz carrier is on during the entire transaction, delivering power to the tag. The carrier is modulated to send information to the tags. Since the tag lacks a power source and only modulates its loop antenna load 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 response. Aggressive filtering allows an eavesdropper 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 susceptible to interference from intentional jamming and unintentional sources. Jamming can occur by interrupting the reader-to-tag communications by interfering with the carrier and/or the reader information. Jamming can also occur by interfering with the tag-to-reader transaction. The reader transmits at several watts and is in the very near-field of the tag. Therefore, to overcome the carrier signal at the tag requires a considerable amount of power if jamming is done at a distance. As 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.

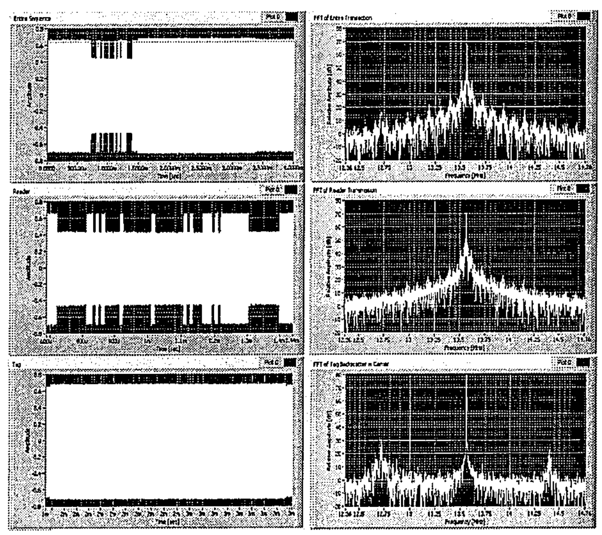

**Figure** 2. Typical ISO 14443 type B emission spectrum. The top graphs show the entire two-way communication in both the time-domain (left) and frequency-domain (right). The reader-to-tag query is in the middle, and the tag-to-reader response is at the bottom. The tag responds with a constant phase-modulated CW return signal at $f_c \pm f_d$ = 13.56 ± .8475 MHz.

## IV. MEASUREMENTS and RESULTS

### *A. Eavesdropping*

The eavesdropping research was performed on a commercial off-the-shelf (COTS) reader and COTS tags. We chose several tags including a type A tag with 16 kB of memory that has a processor capable of performing fairly complex computational and encryption tasks used for RFID financial transactions.

The reader and the tag are coupled loops that are typically axially aligned in the same plane. 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 patterns of the reader and the tag antennas are those of small loops, we can assume that the radiation patterns conform to the simple loop fields given by Harrington [10]:

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

Here $r$ is the distance from the tag to an outside point and $\theta$ is the elevation angle, both illustrated in Figure 3. $I$ is the current in the loops, $S$ is the surface area, $\eta$ is the impedance of free space, and $k$ is the wave number.

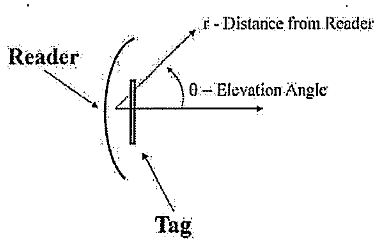


Figure 3. Relative directions for eavesdropping on an HF RFID system. When close to the reader, coupling is best at low elevation angles *(θ=0°)*. When farther away (approaching a wavelength (20m)), eavesdropping should be more efficient at *(θ=90°)*.

For short distances, $r$, the axial magnetic field, $H_r$, is stronger than the $\theta$ directed field, $H_\theta$. At larger distances, the $1/r$ dependence of $H_\theta$ dominates. So, we expect that at close distances (<λ/4) eavesdropping is easier directly above the reader (Figure 4) and at larger distances (>λ) eavesdropping should be easier in the plane of the reader antenna (Figure 5).

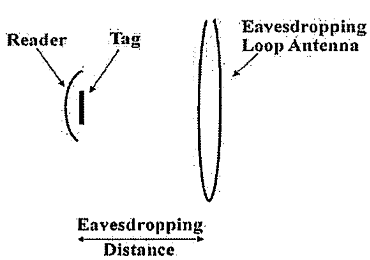


Figure 4. Orientation for short distance (<λ/4) eavesdropping *(θ=0°)*.

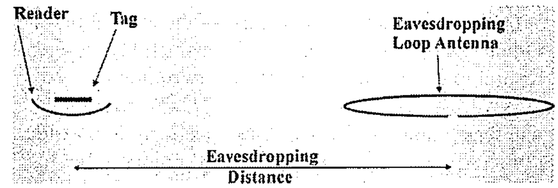


Figure 5. Orientation for large distance (>λ) eavesdropping *(θ=90°)*.

We used a single 1 m loop with a capacitive bridge to match 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 a tag response of 6 dB above the noise floor is captured the information in the signal could be reliably decoded. This set the criterion for a successful eavesdropping session.

Figure 6 shows the raw output of the eavesdropping antenna at 2 m. Without filtering, the reader modulation can easily be distinguished, but the tag response cannot. After receiver filtering, shown in Figure 7, the tag and reader are both distinguishable and the information can be decoded.

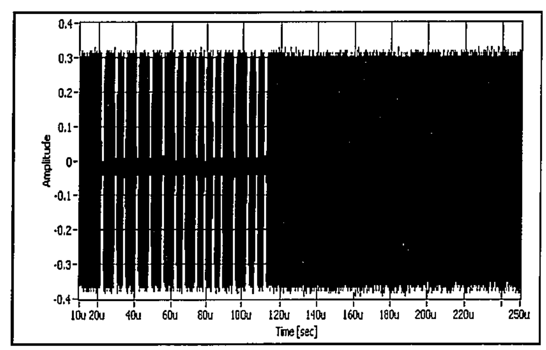


Figure 6. Raw signal received by the eavesdropping antenna. Here, the tag response cannot be distinguished.

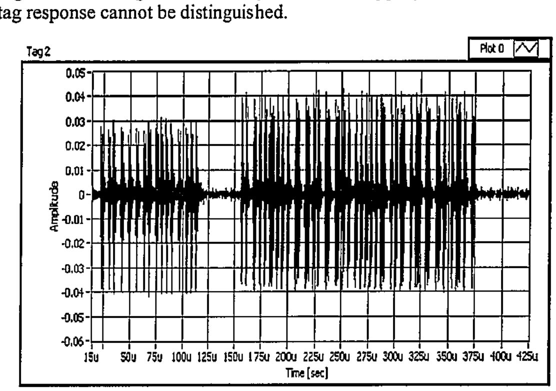


Figure 7. Results of an eavesdropped type A transaction at 2 m distance after filtering out the carrier. The burst on the left is the transitions in the carrier modulation. The burst on the right is the tag response.

Table I summarizes the results of the eavesdropping tests. Other groups have reported considerably longer range results in more idealized testing environments. We limited these tests to using low-cost COTS equipment, small antennas, and performed these tests in a non-ideal, RF cluttered environment. Also, 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). Table I also shows that the eavesdropping distance is strongly tied to tag design. We saw little variation between these tags in the activation field (field level to turn on the tag), but we saw appreciable variations in the eavesdropping distance.

TABLE I
EAVESDROPPING RESULTS for TYPE A TAGS

| Manufacturer | Tag number | Eavesdropping distance t ($\theta$=0°) (see Fig. 5) (m) | Eavesdropping distance at ($\theta$=90°) (see Fig. 6) (m) |
|---|---|---|---|
| 1 | A001 | 6.5 | 15 |
| 1 | A002 | 6.5 | 15 |
| 2 | A003 | 5.0 | 9 |
| 2 | A004 | 5.0 | 9 |
| 2 | A005 | 5.0 | 9 |
| 3 | A006 | 6.0 | 8 |
| 4 | A007 | 6.0 | 8 |

*B. Jamming*

To test the communications reliability of these HF RFID systems, they were subjected to in-band energy. Previous swept frequency measurements indicate vulnerabilities only near the frequency band of operation. We show that jamming at the carrier and sub-carriers would provide the best opportunity to upset the communication between the reader and tag.

We used three types of antennas: (1) a set of dual 1 m loop antennas, (2) a single 15 cm ISO 10373-6 standard Proximity Coupling Device (PCD) loop, and (3) a set of dual 15 cm ISO 10373-6 standard PCD loops, shown in Figure 8. Each antenna was tuned to the frequency of the jamming signal (retuning 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.

One scenario studied was jamming at the carrier or reader transmit frequency, $f_c$. Other scenarios include jamming at the upper and lower sub-carriers or the tag backscatter frequency, $f_s$.

To ensure maximum readability of the tag signal by the reader and to present the most difficult upset scenario for the jammer, 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 further 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 distance in the near-field.

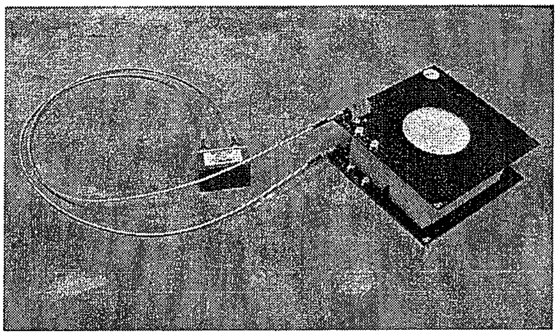

Figure 8. Stacked PCD antennas.

A diagram of the jamming system is shown in Figure 9. Three basic waveforms were used to mimic probable threat scenarios. A continuous wave (CW) source at, $f_c$, a CW carrier at the sub-carrier frequency, $f_c + f_s$ ,and a CW carrier at the sub-carrier frequency, $f_c + f_s$, modulated at $f_d$ to mimic a nearby reader or tag.

The power delivered to the antenna was monitored to ensure that the tuning was correct. The system was considered upset when consistent failures were noted. Some HF RFID systems have robust data failure and retry algorithms; only consistent data failures assure upset.

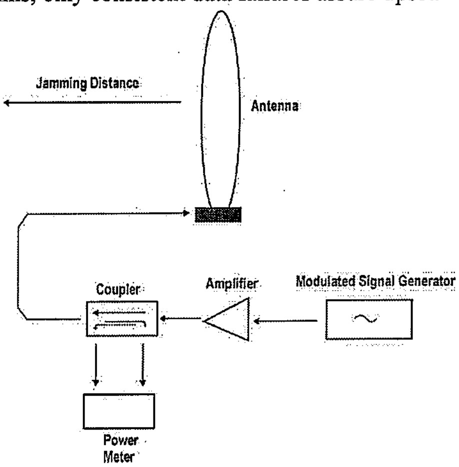


Figure 9.. Jamming system overview.

Tables II-IV 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 is 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. Note that the results at the lower sub-carrier (12.7125 MHz) were similar to the upper sub-carrier frequency.

TABLE II
JAMMING RESULTS CW CARRIER at $f_c$ (13.56 MHz)

| Antenna | Distance (m) | Power to disrupt transaction (W) |
|---|---|---|
| Dual 1 m loops | 5 | 10.0 |
| Single PCD | 2 | 12.0 |
| Dual PCD | 2 | 10.5 |

TABLE III
JAMMING RESULTS for CW SUB-CARRIER at $+f_s$ (14.4075MHz)

| Antenna | Distance (m) | Power to disrupt transaction (W) |
|---|---|---|
| Dual 1 m loops | 8 | 3.7 |
| Single PCD | 3 | 7.0 |
| Dual PCD | 3 | 6.9 |

TABLE IV
JAMMING RESULTS for "DATA-LIKE" MODULATED SUB-CARRIER at $+f_s$ (14.4075 MHz)

| Antenna | Distance (m) | Power to disrupt transaction (W) |
|---|---|---|
| Dual 1 m loops | 8 | 0.3 |
| Single PCD | 5 | 3.0 |
| Dual PCD | 5 | 2.8 |

Many ISM transmission systems in this frequency have a power delivery in the range of 5 to 7 W to the antenna. Even with the low efficiency of these small antennas, ISM system interference can be a real threat and should be considered.

Table V **TABLE** 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 jamming can possibly occur at lower levels.

TABLE V
APPROXIMATE MAGNETIC FIELD REQUIRED at the READER to DISRUPT a TRANSACTION

| Strategy | ***H*** Field @ tag to disrupt (μA/m rms) |
|---|---|
| 13.56 MHz | 1100 |
| 14.4075 MHz | 300 |
| Modulated 14.4075 MHz | 75 |

## V. CONCLUSIONS

RFID systems may transmit system data and may be vulnerable to common interference or malicious attacks.

We explored the ability to eavesdrop on an HF RFID transaction at a distance and 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 interfered with by either unintentional interference or with much lower power by "RFID-like" waveforms. While the waveforms are not likely to be 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 are vulnerable to eavesdropping and replay attacks. We have noted that 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 that make it more difficult to synchronize to and thus harder to decode data [11]. The security of data and system integrity should be considered when deploying RFID systems in critical applications.

## ACKNOWLEDGEMENTS

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] Guerrieri, J.; Novotny, D.; Francis, M. and Remley, K., "HF Proximity RFID Electromagnetic Emissions and Performance," *Proc. AMTA*, pp. 429-434, Nov. 2008.

[8] Novotny, David R.; Guerrieri, Jeffrey R.; Francis, Michael; Remley, Kate; "HF RFID Electromagnetic Emissions and Performance", Electromagnetic Compatibility, 2008. EMC 2008. IEEE International Symposium, 18-22 Aug. 2008 Page(s):1 – 7.

[9] European Patent EP1033669.

[10] Harrington, R.F., "Time-Harmonic Electromagnetic Fields", Mcgraw-Hill, New York, 1961.

[11] 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.