Impact of RF Interference between a Passive RFID System and a Frequency Hopping Communications System in the 900 MHz ISM Band

Michael R. Souryal[1], David R. Novotny[2], Daniel G. Kuester[3], Jeffrey R. Guerrieri[2], Kate A. Remley[2]
National Institute of Standards and Technology
[1]Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899
[2]Electronics and Electrical Engineering Laboratory
325 Broadway
Boulder, CO 80305
[3]University of Colorado
Electrical and Computer
Engineering Department
Boulder, CO 80309
{michael.souryal,david.novotny,daniel.kuester,jeffrey.guerrieri,kate.remley}@nist.gov

***Abstract*—We present experimental measurements and analysis of RF interference between a passive RFID system and a generic frequency hopping communications system in the 902 MHz to 928 MHz ISM radio band. Interference in both directions is considered, RFID to communications and vice-versa, and interference mitigation strategies are assessed. Variables of interest include transmission power, antenna locations and polarization, and frequency hopping channel bandwidth and dwell time. Among the findings are the susceptibility of the RFID backscatter link to sources operating within regulatory limits, characterization of the performance asymmetry between the systems, and the constructive effect of interference to RFID at low powers.**

I. Introduction

Passive radio frequency identification (RFID) in the ultra-high frequency (UHF) band is attractive due to the availability of low cost tags and adequate read range for supply chain and other applications. In the US, UHF RFID operates in an unlicensed radio frequency (RF) band, therefore RFID equipment must tolerate and be tolerated by other radiators sharing this band. As RFID becomes more commonly used in critical applications such as cargo and material identification, it is essential that system engineers and procurement officers understand under what circumstances various systems can be deployed reliably.

This paper investigates the effects of RF interference between a passive UHF RFID system and a communications system sharing the 902 MHz to 928 MHz industrial, scientific and medical (ISM) band. Communications devices in the ISM band are used for supervisory control and data acquisition (SCADA) applications, industrial automation and control, and wireless sensor networking. To comply with US regulatory rules for this band, the RFID and communications systems we have tested employ frequency hopping spread spectrum, whereby each device pseudo-randomly hops from one narrowband channel to another, transmitting for a given duration (or hop dwell time) on each channel. We measure and analyze the performance impact of the RFID system on the communications system and vice-versa, for varying transmission powers, antenna locations, antenna polarization, channel bandwidth and hop dwell time.

The Department of Homeland Security Science and Technology Directorate sponsored the production of this material under Interagency Agreement HSHQDC-09-X-00305 with NIST.

Prior work on interference with passive UHF RFID systems includes the analysis of reader-to-reader interference by Kim *et. al.* [1]; however this work addressed fixed, not hopping, channels. The work by Hong *et. al.* [2] identified conditions under which UHF RFID disrupted a nearby GSM downlink channel, while the work by Arnaud-Cormos *et. al.* [3] measured the effect of a GSM mobile device on the read range of a UHF RFID system. Novotny *et. al.* [4] analyzed the potential interference caused by UHF RFID emitters to nearby devices that satisfy standard minimum RF immunity levels. There have also been studies of interference with other types of RFID systems. Jiang and Ma [5] presented analytical and simulation results for the effect of microwave (2.4 GHz) RFID on an IEEE 802.11b link, and Chen *et. al.* [6] did the same for an IEEE 802.15.4 (Zigbee) link. Regarding high frequency (HF) RFID systems operating at 13.56 MHz, Novotny *et. al.* [7] investigated conditions under which continuous wave and modulated HF carriers can disrupt the RFID transaction.

This study differs from the aforementioned studies in that we examine the mutual interference between frequency hopping RFID and communications systems in the UHF ISM band. Furthermore, in measuring the performance impact of interference, we utilize "soft" performance metrics—the read success rate and read throughput of RFID, and the packet reception rate of communications—rather than a hard on/off metric. Through experimental measurements, we find that, though the effects of interference are demonstrable in both systems, the RFID system is more sensitive to emissions of the communications system than vice-versa, likely owing to the greater susceptibility of the weaker backscattered tag-to-reader signal. However, we also find, interestingly, that under certain conditions RFID read performance can actually improve in the presence of another signal, as the communications signal appears to provide additional RF energy to help activate the passive tag. Interference mitigation through cross-polarization and strategic antenna location are also assessed.

The remainder of the paper is organized as follows. Sec-

tion II provides an overview of the systems that were used in our testing and the parameters that were varied. Section III details the experimental set-up, performance metrics, and results for interference caused to the RFID system, while Section IV does the same for interference caused to the wireless communications system. Section V summarizes the key findings.

II. Systems Overview

This section provides an overview of the systems that were employed in testing and the parameters that were varied.[1]

A. RFID System

The RFID system consists of a UHF reader (or interrogator) and one or more passive-backscatter tags (or transponders). In a passive RFID system, the tag is not powered independently but rather harvests energy from the RF field generated by the reader. The tag responds by modulating a backscattered carrier with identifying information. The air interface protocol between the reader and tags follows the EPCGlobal UHF Class 1 Gen 2 (ISO 18000-6C) standard.

The specific reader used for these tests is the Impinj UHF Gen 2 Speedway Reader. As an FCC Part 15 UHF ISM emitter, it transmits on one of 50 channels between 902 MHz and 928 MHz with 500 kHz channel spacing, and hops pseudo-randomly among the 50 channels. The reader was configured to use a Type A Reference Interval (Tari) of $6.25\,\mu$s and the EPC Gen 2 dense-interrogator spectral mask [8]. The forward link modulation (reader-to-tag) is Phase-Reversal Amplitude Shift Keying (PR-ASK). One port of the reader was connected to a linearly polarized patch antenna with 8 dBi gain. Tags are dual-dipole Rfidium Choctaw passive UHF tags. Reverse link encoding (tag-to-reader) is FM0.

Considering use of the 8 dBi antenna and an estimated 1 dB of cable loss, the maximum output power allowed by the FCC in this configuration is 29 dBm. Reader powers above FCC limits were used in some cases to mimic shorter reader-tag distances. The uncertainty in the radiated power of the reader is estimated to be 1.1 dB.

B. Communications System

The communications system is based on the DNT900 series of frequency hopping wireless industrial transceivers by RF Monolithics, Inc. This system can operate in a variety of configurations varying in data rate, channel bandwidth, and hop duration. Table I lists six profiles of selected values of these variables that were employed in the tests. For each profile, the system hops over 51 channels in the 902 MHz to 928 MHz band. Data is transmitted with filtered nonreturn-to-zero (NRZ) encoding modulated onto a carrier with binary frequency shift keying (FSK). Each transceiver uses a 2 dBi dipole antenna. The transmitter's nominal RF output power settings are 1, 10, 100, 250, 500, and 1000 mW. Measured output power was an average of 2.5 dB below nominal with an approximate uncertainty of 0.5 dB.

Profile No.	Data Rate (kb/s)	Channel BW (kHz)	Hop Duration (ms)
1	200	410	5.00
2	115.2	258	9.90
3	115.2	258	19.95
4	115.2	258	39.10
5	38.4	100	40.05
6	38.4	100	60.05

TABLE I
Communication system profiles

C. Variables

Due to the variety of scenarios and configurations that are possible in practice, this study aims to ascertain the degree to which the impact of interference is affected by a number of variables. The RF output power of both the RFID reader and the communication system is varied. The antenna polarization of the reader and the communications device is also varied. With the flexibility of the transmission parameters of the communications system, the channel bandwidth and hop duration of that system are varied as indicated in Table I, both when the communication system serves as the source of interference to the RFID system and when it is the recipient of interference from the RFID system. Finally, we consider two extremes of antenna topology when the communications system is the source of interference to the RFID system.

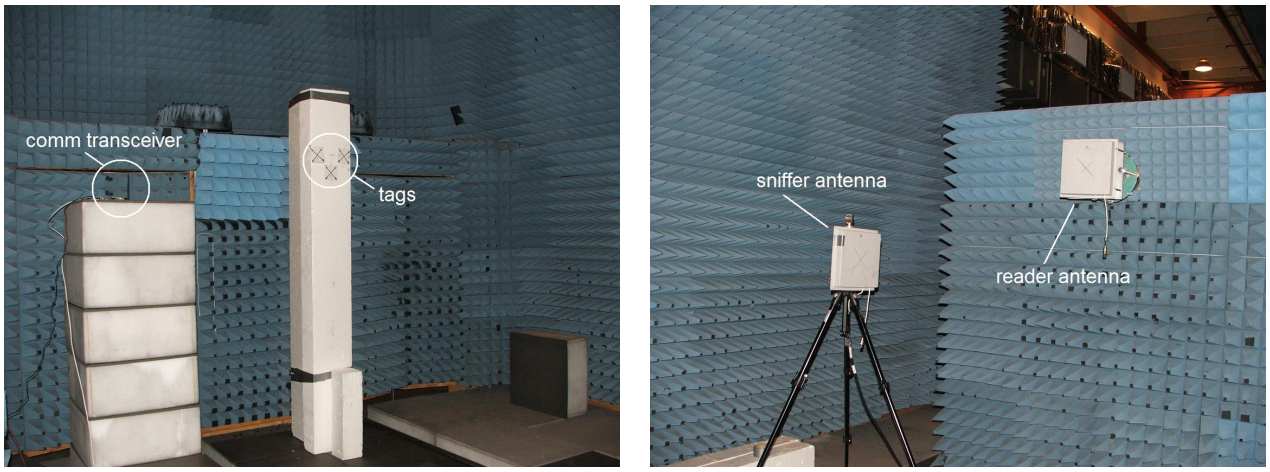
III. Communication System Interference to RFID

This section describes the test procedures and results for assessing the effect of communications device interference to a UHF RFID transaction. In the parlance of the IEEE 1900.2 recommended practice for interference analysis [9], here, the communications device serves as the *source* and the RFID system as the *recipient* of RF interference.

A. Experimental Set-up

The RFID reader antenna, tags, and a communications device were placed in an anechoic facility. Three tags were placed directly in front of the reader antenna at a reader-tag distance of 3.5 m. For the initial set of tests, the communications device was placed 3.7 m from and in the main beam of the reader antenna (see Figure 1). In this topology, the communications device illuminated the reader antenna but not the tags. In a second topology, the communications device illuminated the tags but not the reader antenna (see Figure 2). Figure 3 shows photographs of the experimental set-up for the first topology. In addition to the reader antenna, tags, and communications device, a sniffer antenna connected to a spectrum analyzer was used to monitor RF emissions.

[1]Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.



(a) (b)

Fig. 3. (a) Communications device (left) and RFID tags; (b) Sniffer and RFID reader (right) antennas

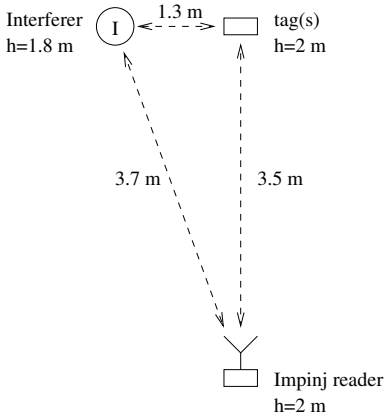


Fig. 1. Communications device illuminating RFID reader antenna

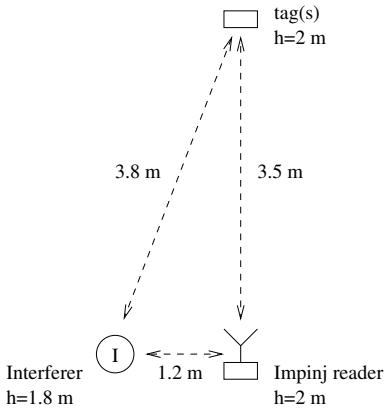


Fig. 2. Communications device in null of RFID reader antenna

B. Source Characteristics

The communications transceiver transmits packetized data continuously with signal characteristics as described in Section II-B and using one of the profiles in Table I. For example, transmissions using profile 1 hop over 51 channels with a hop dwell time of 5 ms and utilizing a channel bandwidth of 410 kHz. A single packet is transmitted during each hop, and the packet size is chosen to fully occupy the hop dwell time. By continuously transmitting with a full duty cycle, the source signal creates a worst-case interference scenario using the given channel-bandwidth/hop-duration profile.

C. Recipient Metrics

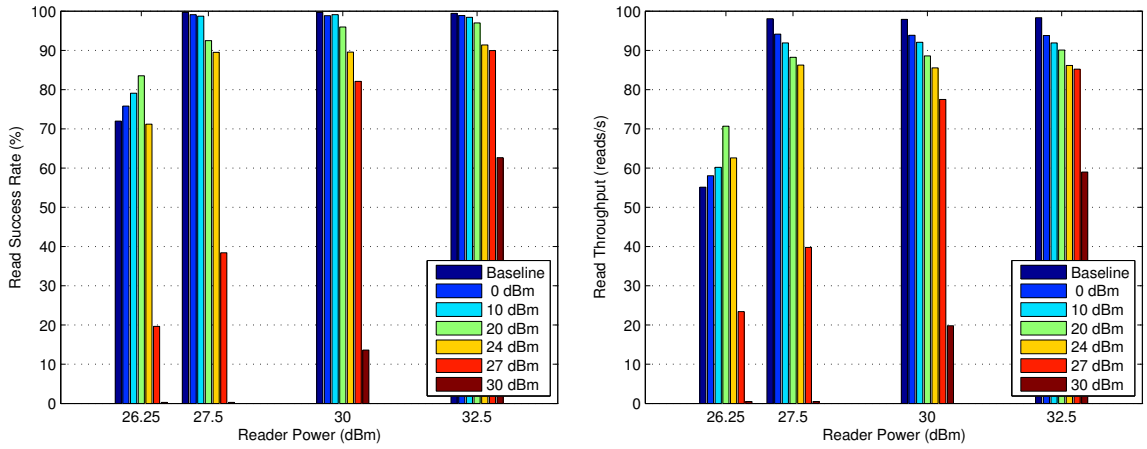
The RFID system was programmed to execute 1000 read attempts in succession and to record the number of times each tag was successfully read, the total number of successful reads, and the duration of the successive read attempts. From these measurements, two metrics are computed. The *read success rate* is defined as $n_s/(n_a n_t)$ where n_s is the total number of successful reads, n_a is the number of read attempts, and n_t is the number of tags in the field. With the duration, we also compute the *read throughput* in reads per second, which is simply the ratio of successful reads to the time it took to complete them. These two RFID performance metrics are used to evaluate the impact of various interference scenarios.

D. Experimental Results

Results are presented, first, for the topology of Fig. 1 in which the communications device is in the main beam of the reader antenna. For each set of results, a baseline measurement of RFID performance is made in the absence of the interfering signal for comparison (i.e., with the communications device present in the field but in an inactive state).

1) Interferer Power: Fig. 4 illustrates representative results for the read success rate and read throughput at different reader powers (horizontal axis) and interferer powers (legend).[2] Here, the communications device transmitted using communications profile 5 (100 kHz channel bandwidth, 40 ms dwell time). At reader powers of 27.5 dBm and higher, the expected reduction in read success rate and throughput with increasing interferer power is apparent. Interestingly, at the lowest examined reader

[2]Quoted power levels are the device's nominal settings for the RF output port prior to antenna gain.



(a) (b)

Fig. 4. (a) RFID read success rate and (b) read throughput vs. reader power, by interference power; 100 kHz interferer with 40 ms dwell time

power of 26.25 dBm, when the baseline read success rate is already marginal, an increasingly powerful interfering signal *improves* reader performance up to a point (24 dBm interferer power), after which reader performance is adversely affected. This result suggests that at low reader power the interfering signal provides additional RF energy to help activate the tag, and that there is a tradeoff between the beneficial effect of activating the tag versus the harmful effect of interfering with the reader.

At reader power levels (or reader-tag distances) of practical interest, for which the baseline read rate is near $100\,\%$, we observe from Fig. 4(a) that read rates fall to below $50\,\%$ when the output powers of the devices are comparable. This observation suggests that despite the use of frequency hopping to mitigate interference, the relatively weak backscattered tag-reader link can be effectively disabled by an interferer operating within regulatory limits in this configuration.

These results are for the reader-tag and reader-interferer distances of this particular configuration. The effect with other distances can be predicted knowing that in free space the signal-to-interference ratio at the reader, which determines the ability of the reader to decode the tag's backscattered signal, is proportional to $(P_R G_R d_I^2)/(P_I G_I d_T^4)$, where P_R and P_I are the RF output powers of the reader and interferer, respectively, G_R and G_I are their antenna gains in the direction of the source, and d_I and d_T are the reader-interferer and reader-tag distances, respectively.[3]

2) Antenna Polarization: The graph in Fig. 5 compares the read success rate with a vertically versus horizontally polarized reader antenna. In both cases, the interferer antenna is vertically polarized, it transmits with the same hopping profile as above, and the reader power is 27.5 dBm. RFID performance improves somewhat when the reader antenna is cross-polarized with respect to the interferer antenna. For example, at an interferer power of 27 dBm, cross-polarized operation increases the read success rate from $38\,\%$ to $65\,\%$.

[3]To be more accurate, this proportionality would also account for the nonlinear power dependence in the tag [10].

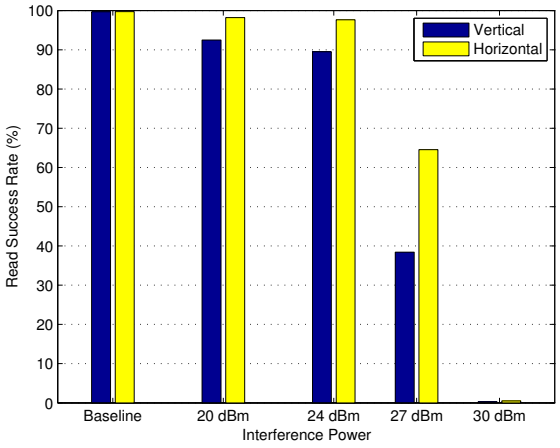


Fig. 5. RFID read success rate vs. interference power *by reader antenna polarization*; 27.5 dBm reader; 100 kHz interferer with 40 ms dwell time

Nevertheless, cross-polarized operation is insufficient to protect the RFID link at 30 dBm interferer power.

3) Interferer in Reader Antenna Null: When the interferer is repositioned as shown in Fig. 2 to be in the reader antenna's null and to illuminate the tags, RFID performance improves significantly. The graph in Fig. 6 illustrates the read success rate versus reader power by interference power in this configuration. The interferer signal has the same characteristics as above. Whereas a 30 dBm interferer disabled the RFID link in the previous configuration, it only reduces the read rate to about $90\,\%$ in this configuration. We also observe, once again, an ameliorative effect of the communications signal on RFID performance at low reader power.

The improved RFID performance in this configuration supports the notion that performance is limited by the backscattered link, even in frequency hopping systems. Controlling the RFID-interferer topology to protect that link, even if it means exposing the forward link, mitigates the impact of the interference to a large degree.

4) Interferer Signal Bandwidth/Dwell Time: The graph in Fig. 7 shows read success rate versus reader power with a

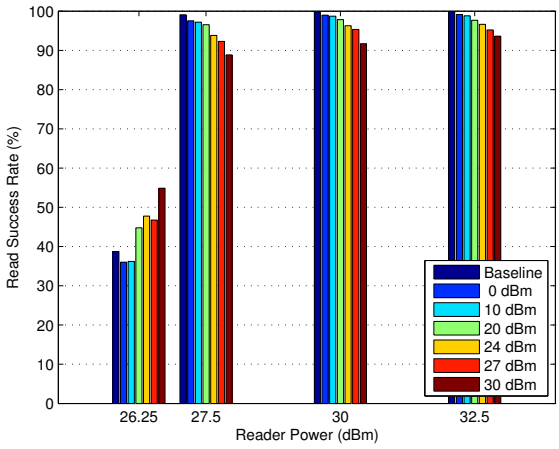


Fig. 6. RFID read success rate vs. reader power, by interference power; 100 kHz/40 ms interferer *in reader antenna's null*

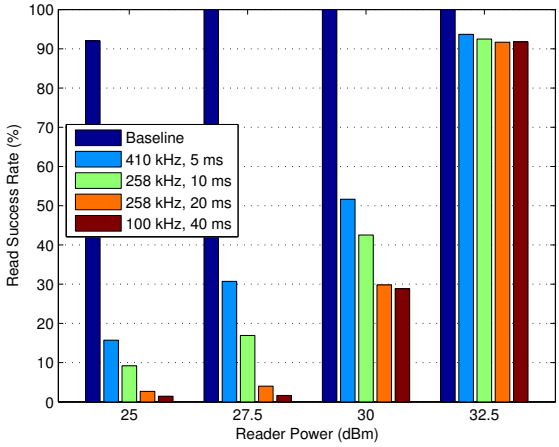


Fig. 7. RFID read success rate vs. reader power *by interference profile*; 30 dBm interferer; single tag one-half wavelength from aluminum plate

single tag one-half wavelength in front of an aluminum plate to improve read performance. The topology is as shown in Fig. 1 with the interferer illuminating the reader. At each reader power, the interferer power was held at 30 dBm and its frequency hopping profile was varied. The results indicate that RFID performance in our test system is more sensitive to the hop dwell time than the channel bandwidth of the interference.

IV. RFID Interference to Communication System

This section describes the test procedures and results for assessing the effect of RFID interference on the frequency hopping communications system. Here, the RFID reader and tags serve as sources of interference, and the communications system is the recipient system.

A. Experimental Set-up

The topology is as shown in Fig. 8. The reader, three tags, and one communications device (labeled 'B' for base) are in the same positions as in Fig. 1. However, here a second communications device, labeled 'R' for remote, is located behind RF absorbers with respect to the reader but with a

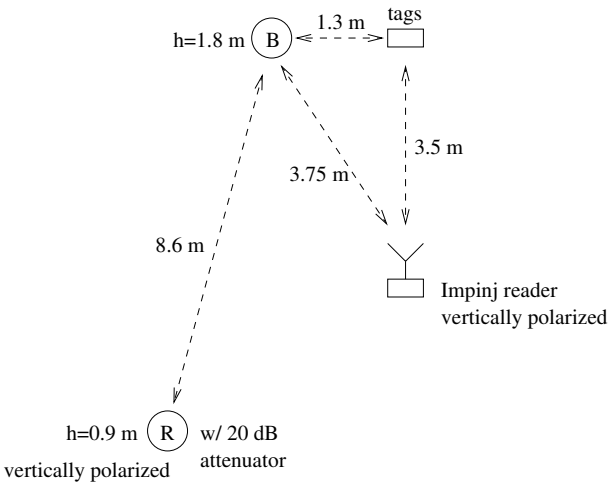


Fig. 8. RFID reader illuminating communications antenna

line of sight to the base. In this way, the base is exposed to the reader's signal, but not the remote. The base and remote communications device hardware are identical except for a 20 dB attenuator inserted between the RF output of the remote and its dipole antenna to prevent overloading of the receivers.

B. Transmission Characteristics and Recipient Metric

The RFID reader inventories the tags continuously while the base and remote communication devices exchange packetized data. The communications link is symmetrical; each device transmits at a fixed rate determined by one of the communications profiles in Table I and with an RF output power of 30 dBm. The base and remote each transmit one packet per hop, evenly splitting the hop duration between them. When a packet is successfully received, the receiver immediately replies with an acknowledgment. Packets are not retransmitted if an acknowledgment is not received.

Each transceiver logs and maintains counts of the packets sent, the packets successfully received, and the acknowledgments received. The packet reception rate, the ratio of packets received to packets transmitted, is the metric used to evaluate the impact of interference from the RFID system. Each measurement of packet reception rate is based on 60 s of continuous packet transmission.

C. Experimental Results

1) Bandwidth/Dwell Time: Fig. 9 illustrates the measured packet reception rate at the base transceiver for different frequency hopping profiles and at different RFID reader powers. The baseline measurement of the packet reception rate in the absence of an RFID emission (not shown in the figure) was $100\,\%$ in each case. Furthermore, the packet reception rate at the remote transceiver was $100\,\%$ in each case, as the remote was shielded from the RFID emission.

Overall, the results indicate that the communications system is relatively robust to the interference generated by the RFID system. For example, at 30 dBm reader power—which, when accounting for the 20 dB attenuator, the differing antenna

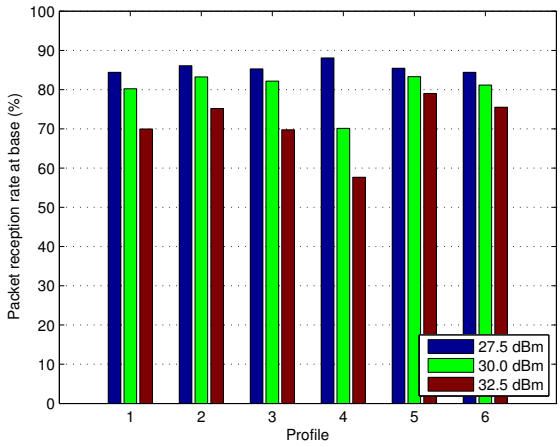


Fig. 9. Packet reception rate at base vs profile, by reader power

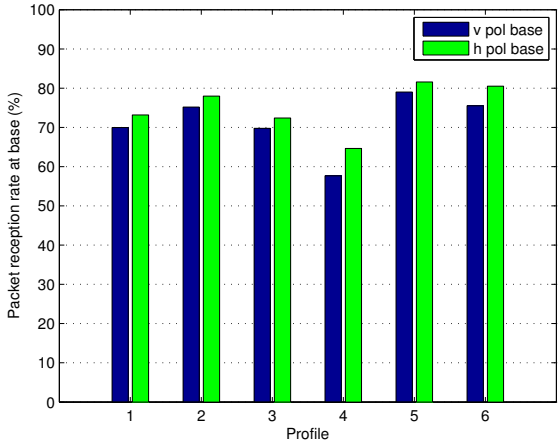


Fig. 10. Packet reception rate at base vs profile, by base antenna polarization; 32.5 dBm reader; vertically polarized reader antenna

gains, and differing distances, translates to an interfering signal at the base receiver that is 35 dB greater than the communications signal—the base is still able to receive from 70 % to over 80 % of the remote's packets without packet retransmission. In practice, most data links use retransmission for error recovery, and with only three retransmissions, a 70 % reception rate (30 % error rate) would translate to 99 % reliability. Thus, frequency hopping largely protects the communications link from interference in this configuration.

Comparing the results for different profiles shows that the packet reception rate decreases with increasing hop duration (see profiles 2–4 and 5–6) as well as increasing channel bandwidth (profiles 4–5). In fact, profile 4, which has the largest time-bandwidth product, shows the greatest sensitivity to increasing interference power.

2) Base Antenna Polarization: Fig. 10 compares the packet reception rate at the base when the base antenna is vertically polarized versus horizontally polarized. In both cases, the remote antenna and the reader antenna are vertically polarized. As in the case with the RFID system, cross-polarized operation with respect to the interferer only modestly improves the communications link performance. It is possible that some of the gains of cross-polarizing with respect to the interferer are offset by a weaker cross-polarized base-receiver link.

V. Conclusions

This paper presented experimental measurements and analysis of the impact of mutual RF interference between a passive UHF RFID system and a frequency hopping communications system sharing the same band. The key findings are summarized below.

- Despite the use of frequency hopping to mitigate interference, the relatively weak backscattered tag-reader link can be effectively disabled by an interferer illuminating the reader within regulatory limits (Section III-D1).
- Controlling the RFID-interferer topology to protect the backscattered link, even if it means exposing the forward link, mitigates the impact of the interference to a large degree (Section III-D3).
- At low reader powers, when the baseline read rate is already marginal, an interfering signal can *improve* the read rate by helping to activate the passive tag (Sections III-D1 and III-D3).
- The impact of RFID emissions on a frequency hopping communications system increases with the channel bandwidth and hop duration of the communications signal; but overall, the communications system is much less sensitive to interference than the RFID system (Section IV-C1).
- Using polarization isolation is minimally effective in reducing interference (Sections III-D2 and IV-C2).

References

[1] D.-Y. Kim, B.-J. Jang, H.-G. Yoon, J.-S. Park, and J.-G. Yok, "Effects of reader interference on the RFID interrogation range," in *Proc. European Microwave Conference*, Oct. 2007, pp. 728–731.

[2] W. Hong, R. Kan, and S. Li, "Electromagnetic compatibility of UHF-RFID to GSM," in *Proc. International Symposium on Electromagnetic Compatibility (EMC)*, Oct. 2007, pp. 63–66.

[3] D. Arnaud-Cormos, T. Letertre, A. Diet, and A. Azoulay, "Electromagnetic environment of RFID systems," in *Proc. European Microwave Conference*, Oct. 2007, pp. 1652–1655.

[4] D. R. Novotny, J. R. Guerrieri, and D. G. Kuester, "Potential interference issues between FCC part 15 compliant UHF ISM emitters and equipment passing standard immunity testing requirements," in *Proc. International Symposium on Electromagnetic Compatibility (EMC)*, Aug. 2009, pp. 161–165.

[5] W. Jiang and Y. Ma, "Interference analysis of microwave RFID and 802.11b WLAN," in *Proc. International Conference on Wireless Communications, Networking and Mobile Computing (WiCom)*, Sep. 2007, pp. 2062–2065.

[6] J. Chen, J. Zeng, and Y. Zhou, "Packet error rate of Zigbee under the interference of RFID," in *Proc. International Conference on Advanced Computer Control (ICACC)*, Jan. 2009, pp. 581–585.

[7] D. R. Novotny, J. R. Guerrieri, M. Francis, and K. Remley, "HF RFID electromagnetic emissions and performance," in *Proc. International Symposium on Electromagnetic Compatibility (EMC)*, Aug. 2008.

[8] "EPC radio-frequency identity protocols: Class-1 generation-2 UHF RFID protocol for communications at 860 MHz – 960 MHz," version 1.2.0, EPCGlobal, 2008.

[9] "IEEE recommended practice for the analysis of in-band and adjacent band interference and coexistence between radio systems," IEEE Std 1900.2-2008, New York: IEEE, 2008.

[10] S. Skali, C. Chantepy, and S. Tedjini, "On the measurement of the delta radar cross section (ΔRCS) for UHF tags," in *Proc. IEEE International Conference on RFID*, Apr. 2009, pp. 346–351.