ATCZ175 InterOP PROJECT

Interference Analysis of Passive UHF RFID Systems

Institute of Electrodynamics, Microwave and Circuit Engineering
Technische Universität Wien

Advisor:
Assoc. Prof. Dipl.-Ing. Dr.techn. Holger Arthaber

by
Ahmet Baris Gok

October 18, 2019

Contents

Abbreviations

ASK amplitude-shift keying

CW continuous wave

EIRP effective isotropic radiated power

ISM industrial, scientific, and medical

RF radio frequency

RFID radio frequency identification

UHF ultra high frequency

1 Introduction

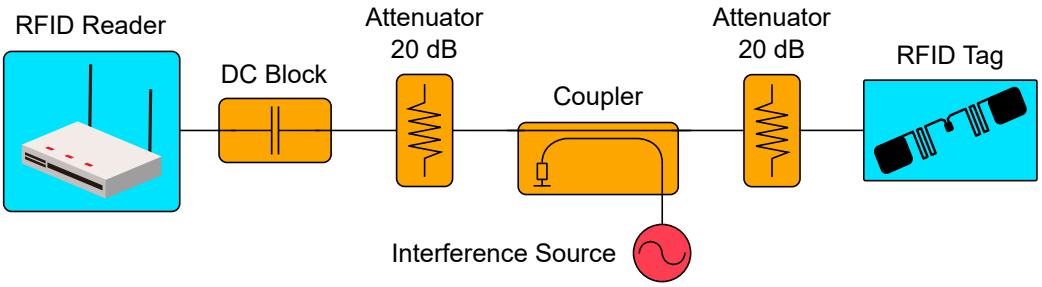
Nowadays, ultra high frequency (UHF) radio frequency identification (RFID) is a widely deployed wireless technology for identifying and tracking individual objects. Because of this versatile range of applications, RFID has gained more and more attention over the last years. Popular applications are, for instance, supply chain management, item tracking, and localization. As UHF RFID systems utilize the industrial, scientific, and medical (ISM) band (865 MHz–868 MHz) for data exchanges, perturbances through other communication standards become an important issue. Therefore, with this report the behavior of passive UHF RFID systems, affected by interference, is investigated.

An RFID system generally consists of two parts called reader and tag. The tag is the object which should be identified over the air by the reader. The on-board logic of RFID tags can be supplied passively, actively, or semi-actively. In this work, the focus lies on passive tags, supplied by the electro-magnetic waves sent by the reader. The reader-to-tag communication works with an amplitude-shift keying (ASK) modulation and the tag replies by changing the matching impedance of the antenna. As this data stream is encoded by different procedures (Miller, FM0), it will be examined if interference effects can be mitigated using different data rates and coding techniques.

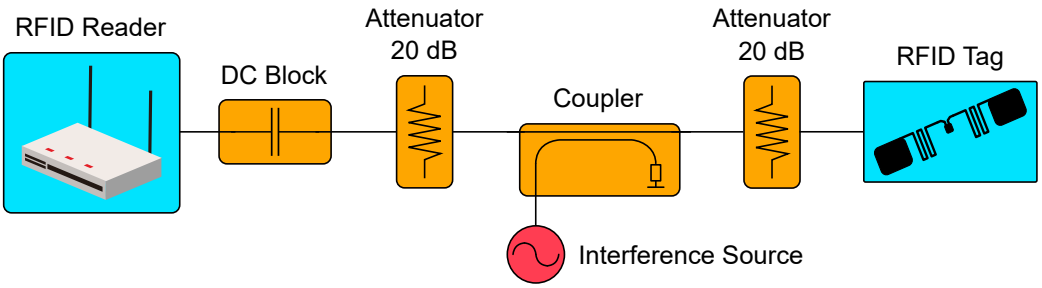
2 Interference Measurement Setup

In order to measure interference effects, an RFID communication system, consisting of a reader, a connectorized tag, and additional radio frequency (RF) equipment, has been created. The channel between reader and tag has been realized by a wired combination of a DC block, two attenuators (20 dB), and a directional coupler to connect the interference source. UHF RFID communications cover the frequency range between 865 MHz–868 MHz at a relatively small channel bandwidth of 200 kHz (Europe) [1]. Because of this narrow-band characteristic, the interfering signal is realized by a continuous wave (CW) signal, variable in frequency and power. Basically, two setups have been utilized differing on the coupling direction of the interference source. The first one (Figure 1(a)) is intended to investigate the influence of CW interference seen by the tag and the second one (Figure 1(b)) does the same towards the reader. One can find the utilized components in Table 1.

The measurement procedure works as follows: The reader starts a typical identification sequence with the tag at a center frequency of 867.5 MHz. Meanwhile, the interference source is perturbing the data exchange with a CW signal at a certain frequency and power level. In order to gain stable results, this procedure is repeated up to a total time of 500 ms. Within this time interval it is measured how often the tag identification failed or worked out.



(a) Interference source coupled to the tag.



(b) Interference source coupled to the reader.

Figure 1: Interference measurement setup realizations.

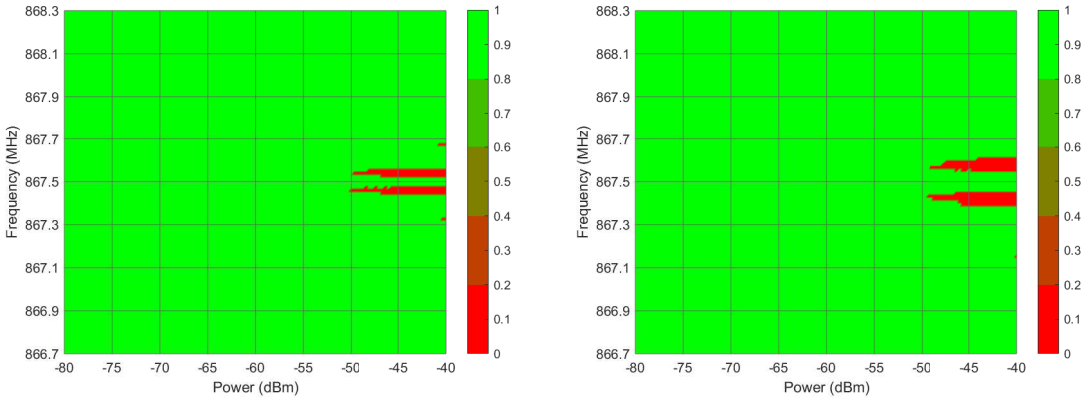
Component	Manufacturer	Description
RFID Reader	Kathrein	RRU 4500
RFID Tag	NXP	UCODE 7
Interference Source	Rohde und Schwarz	SMBV100A
Coupler	Krytar	MODEL 1850
DC Block	Mini Circuits	BLK-18-S+
Attenuator	Mini Circuits	VAT-20+

Table 1: Interference measurement setup: list of utilized components

3 Measurement Results

For the following results, the interference source's frequency and power level has been varied. Therefore, the results are presented in a contour plot, indicating under which conditions a valid tag identification can be established. The interference power levels have been calibrated with an RF power meter to compensate the influence of utilized RF

components. In Europe, UHF RFID readers are allowed to transmit with a maximum power level of 3 dB W (EIRP). In order to compare the transmit power relative to the interferer, one can roughly assume a setup (Figure 1) attenuation of 40 dB.

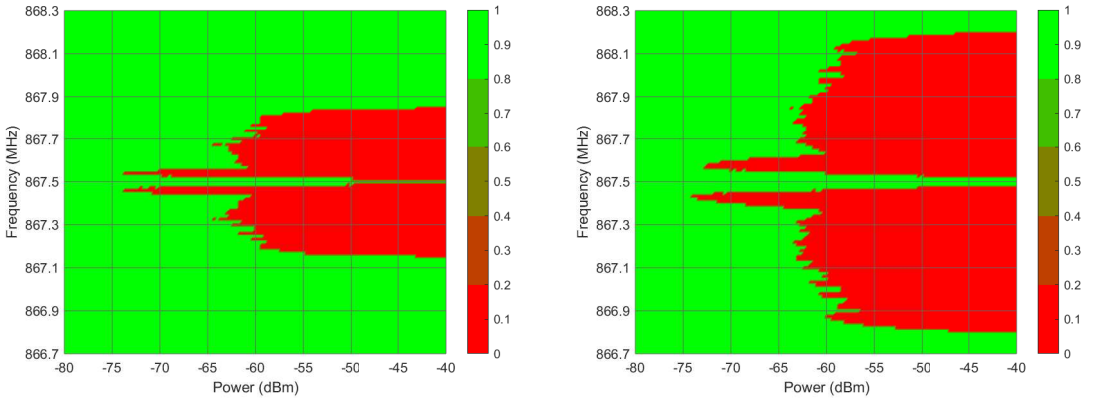


(a) Rx: 160 kbit/s, FM0

(b) Rx: 320 kbit/s, FM0

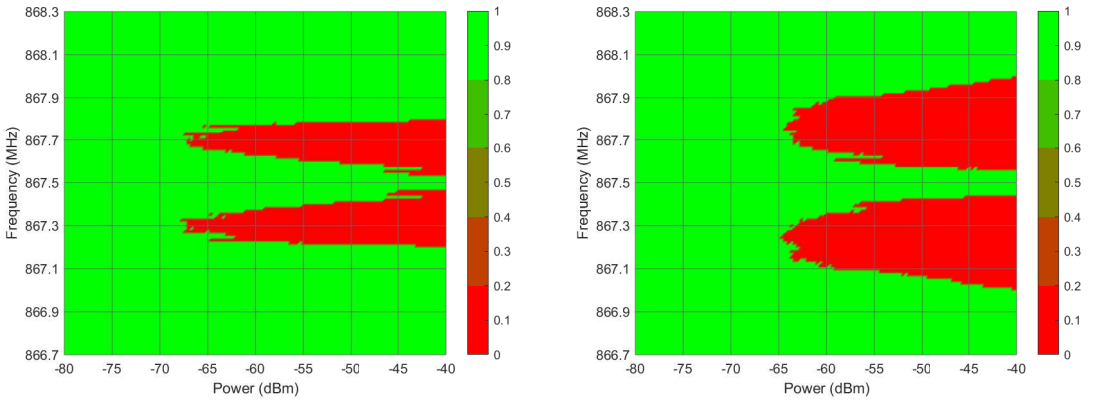
Figure 2: Measurement resutls, interference source coupled to tag (Figure 1(a)), Tx: 80 kbit/s (reader-to-tag), $f_c = 867.5$ MHz, tag-to-reader data rate denoted with Rx.

Figure 2 depicts the contour plots for measurement setup one (Figure 1(a)) using different back-scatter modulations and coding schemes. First of all, the reader may be surprised about the digital behavior of valid (green) and invalid (red) identification communications. Indeed it turned out that the RFID system is sensitive to a certain CW interference power level. As a result of this clear behavior, it is not strictly necessary to investigate such a long reading time (500 ms) in this configuration. In addition to this, interference coupled towards the tag causes perturbances only for high power levels. Concerning this matter, the measurement results of the second setup, indicated by Figure 3, where the interference signal is coupled towards the reader yield a more relevant output. In this configuration, the back-scattered signal suffers heavier from interference. Obviously, all subplots have one thing in common. The contour plots show a symmetric outage, mirrored around the center frequency (867.5 MHz). This behavior can be explained through the spectral mask of the back-scattered signal. As ASK just modulates the carrier by a rectangular signal, equidistant modulation products around the center appear. Depending on the utilized encoding scheme, these spectral lines are broadened. The simplest coding technique is the *FM0*. Hence, modulations using this method are the most disadvantaged in terms of interference vulnerability. *Miller* coding, for instance, raises subcarrier cycles per symbol (M = 2, 4, 8) and consequently the link reliability as well [2]. Because of the higher frequency content, the spectral lines distance gets larger (compare Subplot 3(a) and Subplot 3(f)).



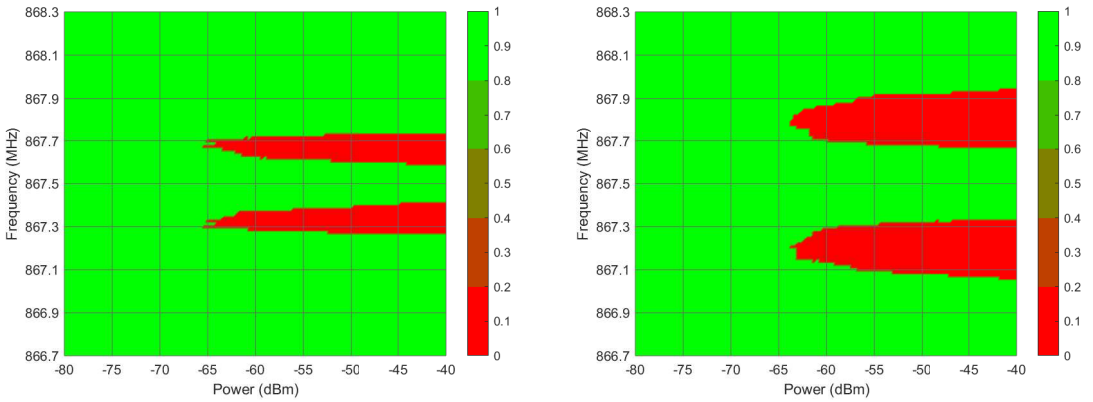
(a) Rx: 160 kbit/s, FM0

(b) Rx: 320 kbit/s, FM0



(c) Rx: 80 kbit/s, Miller2

(d) Rx: 160 kbit/s, Miller2



(e) Rx: 40 kbit/s, Miller4

(f) Rx: 80 kbit/s, Miller4

Figure 3: Measurement resutls, interference source coupled to reader (Figure 1(b)), Tx-rate: 80 kbit/s (reader-to-tag), $f_c = 867.5$ MHz, tag-to-reader data rate denoted with Rx.

Depending on the bandwidth of the interfering signal, the following approaches can be made. If the interferer is narrowband ($\leq 10\,\mathrm{kHz}$), it would make sense to align the reader's center frequency with the interferer. In this scenario, high data rates and a low complexity encoding scheme (*FM0*) could be conceivable. For a bandwidth $> 10\,\mathrm{kHz}$ it would be a solution to use *Miller* coding and further enlarge the spectral lines distance by higher data rates. It is remarkable that enhancing the throughput leads to an improved robustness against interference.

4 Conclusion

Building the measurement setup enabled the characterization of UHF RFID systems in terms of interference. As these systems are narrowband, a CW signal was utilized to jam the identification communications between reader and tag. Regarding the setup realizations (Figure 1), it turned out that coupling the CW signal towards the reader was the most error-prone scenario. Furthermore, the contour plots showed a binary behavior of the communication outage, indicating that the system is very sensitive to a certain interference power level.

Investigating the measurement results in more detail (Figure 3), it comes to mind that one simple solution to mitigate perturbances is to align the center frequencies of the interferer and the desired signal. Depending on the interferer's bandwidth, different coding schemes (i.e., *FM0* and *Miller*) can be utilized to further enhance the communication robustness. In addition to this, in some cases it is even useful to enhance the data rate as well.

Lastly, it must be mentioned that this setup does not consider free space propagation effects, such as fading. As the setup was realized by wired components, it must be considered that raising the throughput is not always an option for a reliable link.

References

[1] RFID Journal, FAQ. `https://www.rfidjournal.com/faq/` 1

[2] Specification for RFID Air Interface, Protocol for Communications at 860 MHz–960 MHz, Version 2.0.0 Ratified, 2013. *EPC^{TM} Radio-Frequency Identity Protocols Generation-2 UHF RFID*. 3