2007

A Single Channel Attack on 915MHz Radio Frequency Identification Systems

Christopher Bolan
Edith Cowan University

DOI: 10.4225/75/57b41c1130df8
Originally published in the Proceedings of 5th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, December 4th 2007.

A Single Channel Attack on 915MHz Radio Frequency Identification Systems

Christopher Bolan
School of Computer and Information Science
Edith Cowan University
c.bolan@ecu.edu.au

Abstract

There has been some speculation as to the protection offered by the Frequency Hopping Spread Spectrum utilised by RFID technology. This paper explores the construction of an attack based on the broadcast of an attack signal in a single channel. The study details an experiment on two groups of tags where the experimental group are exposed to an attack signal broadcast on a single channel. With consistent findings across both control and experimental groups the experiment clearly demonstrates that FHSS offers no protection against such an attack.

Keywords

Radio Frequency Identification, Attack, Frequency Hopping

INTRODUCTION

RFID tags or transponders may be either passive or active. Passive tags have no on tag power and are thus use the electromagnetic energy transmitted by the transceiver to power the microcontroller through inductive coupling or far field energy harvesting (Sarma *et al*., 2002). Inductive coupling uses the magnetic field of the communication signal to induce a current in the coiled antenna which charges an on-tag capacitor providing an operating voltage, and power (*ibid*). This means that inductive coupling is only feasible using the near-field communication signal.

Alternatively, far field harvesting uses the energy from the interrogation signal's far field signal to power the tag (*ibid*). The signal works upon the end terminals of the tag antenna inducing voltage which is used to charge a capacitor that in turn supplies an operating voltage. Due to their reliance on transmitted power passive RFID tags have only small transmission areas ranging from a few centimetres to around fifteen meters for the UHF tags. The price for passive tags is also comparably small with prices varying from around $0.10 (US) to $5.00 (US) per tag.

In a typical RFID system using passive tags, an interrogator (RFID Reader) receives data from an RFID Tag by first broadcasting a continuous-wave RF signal to the Tag (EPCglobal, 2005). Passive tags then use this signal to respond by modulating the reflection coefficient of its antenna, thereby backscattering an information signal to the reader. Due to this mode of operation, such systems are referred to as 'Interrogator Talks First' systems, as passive RFID Tags will only respond after direction from a Reader/Interrogator (*ibid*). The systems are also 'half-duplex', that is that Tags and Readers do not communicate simultaneously, rather switching roles of 'talking' and 'listening'.

Active tags have an additional power cell used to provide power to the RFID microcontroller. Such inclusion of an on-chip power source provides active tags with several advantages over their passive counterparts such as the ability to receive lower power signals or to output stronger signals than would otherwise be possible. The higher signal strength means that active tags are able to transmit over greater distances up to around 100 meters. With the added benefits that the active tags bring, also comes a shelf life. Modern tag battery life varies from one to ten years according to usage and data transfer settings. Also, while only slightly larger in size than their passive equivalents, active tags are considerably more expensive ranging from twenty to three hundred dollars per tag (Wild, 2005).

RFID DATA TRANSFER

At the basis of RFID systems is the need to transmit and receive data reliably, in order to do this, the data must be encoded in such a way to allow transmission. According to Sarma *et al*. (2002, p.5) there are two critical factors in RFID communication:

- "the encoding of the data"

- "the transmission of the encoded data" (the modulation).

The way in which the encoding and modulation are addressed will determine the bandwidth, integrity and power consumption of the RFID tags (*ibid*).

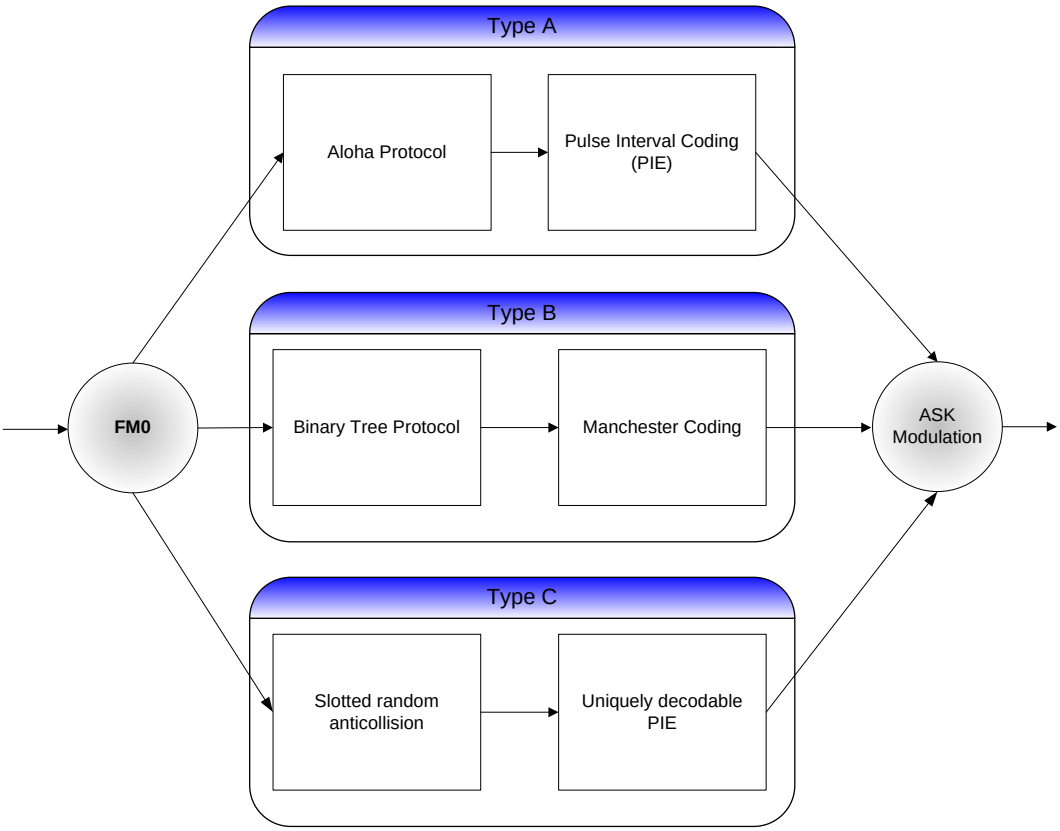


Figure 1. Possible Communication Architectures for RFID Systems (ISO/IEC, 2006)

The 2004 version of the ISO18000-6 specified two communication types for RFID systems, namely Type A and Type B (ISO/IEC, 2004). The standard was updated in 2006 to include a Type C architecture (ISO/IEC, 2006). The three architectures are illustrated in figure one.

Coding

Two categories of data coding are used in RFID systems namely level coding and transition coding. Level coding uses two different voltage levels to represent the communication bits (one and zero), whereas transition coding represents the communication bits as transitions in the level of the voltage. The coding scheme (is chosen on the basis of three considerations (Sarma *et al*., 2002):

- The amount of power required to transmit the code.
- The bandwidth required by the code.
- Whether the code allows for the detection of collisions.

Most modern RFID systems use PPM or PWM for reader to tag communication (transceiver → transponder) and Manchester or NRZ for tag to reader communication (transponder → transceiver).

Modulation

Modulation refers to how the coded bits are transmitted between the transponder and transceiver and visa versa. This is achieved through one of three schemes (Sorelles, 1998, p.4) namely Amplitude Shift Keying (ASK), Frequency Shift Keying (FSK) and Phase Shift Keying (PSK). The modulation scheme chosen for a particular implementation is dependant upon (Sarma *et al*., 2002):

- Power consumption constraints.
- Amount of reliability required.
- The available bandwidth.

It is important to note that when it comes to signal modulation RFID systems suffer from a unique problem, which is the vast difference in signal power between the transceiver and the transponder. This may mean that while a passive RFID tag may detect and use the signal given by the transceiver, its return signal may be too faint for the transceiver to detect. The ISO 15693 standard suggests that the return signal be modulated to a lower sub carrier to militate against this problem.

Frequency

The frequencies at which RFID transmissions operate are set by various standard bodies and affect the general operating potential of the technology. Most RFID technology work in the Industrial/Scientific/Medical (ISM) bands which are freely available for use by low-power/short-range systems as designated by the International Telecom Union (ITU) (Scharfeld, 2001). The ITU divides the world into three regions for the purpose of telecommunication bandwidths (figure 2).

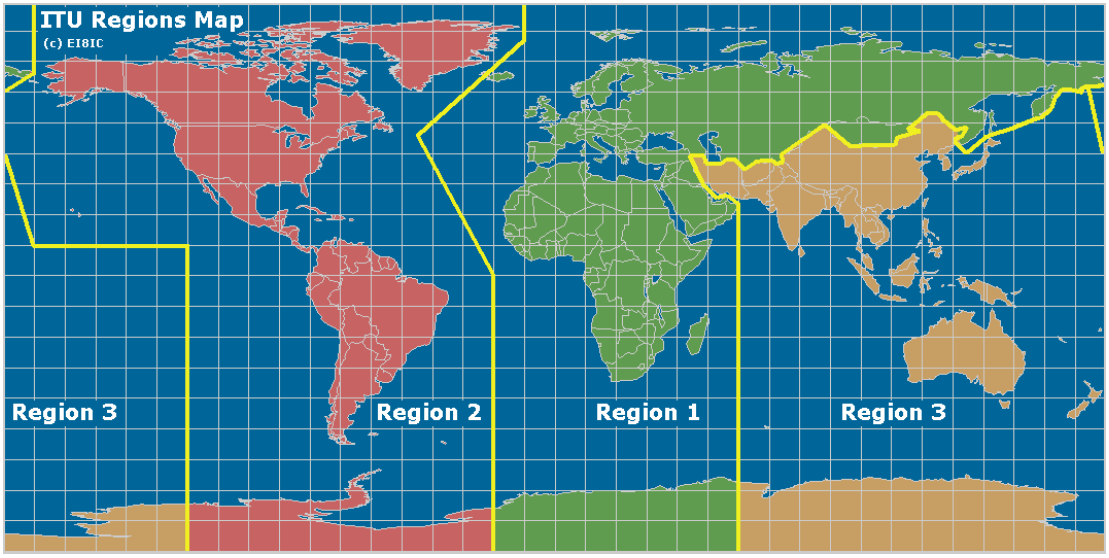


Figure 2. ITU Regions (EI8IC, 2002)

Within these regions the ITU specifies the following bands for use in ISM technologies such as RFID. While higher frequencies allow for greater bandwidth and thus greater data transfer rates, they also become more susceptible to interference from external materials such as water or metal.

Frequency Hopping Spread Spectrum

Frequency-hopping spread spectrum (FHSS) transmission provides a means to prevent radio signals from being monitored or blocked by hostile parties and other interferences. This is achieved through changing the frequency of a transmission at regular intervals within a given spectrum. Thus, a receiver that knows the spectrum and channels that frequency-hopping pattern will occur in and may thus receive an entire transmission.

In order to overcome possible interference in RFID systems, the RFID reader transmits its signal on a single channel within its spectrum (as shown in figure 3) and then hops to another channel within the spectrum for its next attempt at transmission. Over time the reader will use channels across the entire available spectrum, which in the case of 915 MHz will be 902 MHz – 938 MHz. This is shown in figure 4 which illustrates the cumulative waveform.

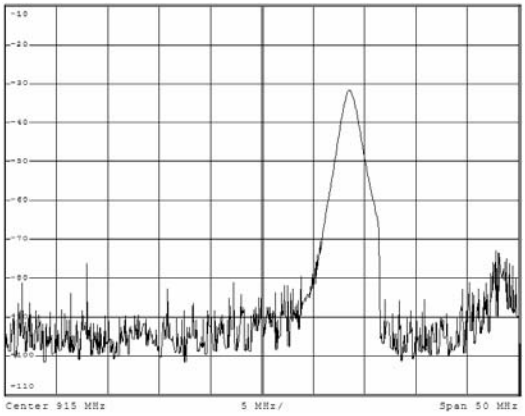


Figure 3. Reader communication on a single channel in the 915 MHz spectrum

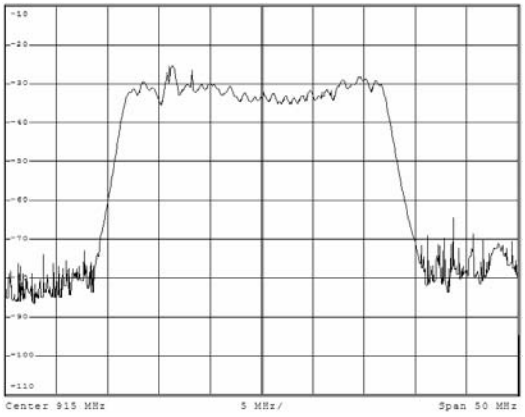


Figure 4. Cumulative waveform of RFID Communication on the 915 MHz spectrum

Both the Air Interface for EPC tags and the ISO18000-6 standards allow for Frequency Hopping Spread Spectrum (FHSS) for reader to tag communications. Utilising this allowance a number of countries, including the U.S. and Australia, have permitted the use of FHSS for RFID implementations. This means that an RFID reader may, in a pseudo-random sequence, hop between channels within the operating band of frequencies.

A critical reason behind the usage of FHSS is the assertion that it provides some immunity to Denial of Service (DoS) from in-band interference. Such assertions seem to stem from the use of FHSS in typical 'symmetric' systems. In symmetric FHSS implementations, both transmitter and receiver lock step, that is the receiver hops with the transmitter to each new channel within the operating frequency. In contrast, RFID systems employ 'asymmetric' FHSS, with only the transmitter hopping between channels and the RFID tag, due to processing limitations and lack of continuous power, regarding the *entire band* as a single channel. This means that while a Reader may avoid a noisy channel by hopping to the next, an RFID tag is unable to do this. The tag effectively listens on all channels at once and thus, will attempt to react to *a* signal occurring anywhere within the entire band.

THE EXPERIMENT

Design of the Experiment

At first sight it would appear that DoS interference for a UHF Gen 1 based Reader, being based on a frequency-hopping protocol, would need to occur within the current channel (or every channel) to be effective. Due to the asymmetric operation of FHSS in RFID systems, it was considered likely that a signal on a single channel within the operating band of an RFID tag would interfere with the successful operation of the system. In order to verify this assertion a hypothesis was created: "*An interfering signal on a single fixed channel anywhere within a Frequency Hopping RFID band will disrupt Reader-Tag communications, causing DOS*".

This attack builds upon the effect of interference on a single channel, as stated by ISO18000-6b (2004, p. 2). Such interference will cause the tag (or target reader) to enter a communication fault state. The standard states that when a tag receives a modulated signal that it does not recognise, it remains silent. As the 915Mhz tags used in this experiment operate on the 860 to 960MHz spectrum, any carrier modulation on any channel within this range of frequencies should either engage the tag in communications, or occupy the tag in a communications error state. US regulations state that Gen 1 RFID systems must operate within the 902 to 928MHz band. Hence a correctly modulated carrier operating on any single channel within this range of frequencies should either engage the tag in communications, or occupy the tag in a communications error state.

To guide the experimentation a Quasi-Experimental approach was been selected. The first consideration for the experiment was the selection of an appropriate sample population. The Quasi-Experimental method allows for 'the selection of the target population via the use of non-random or otherwise strict sampling techniques, which may not accurately reflect an entire population'. To satisfy this requirement a sample population of twenty compliant EPC Generation One RFID tags were 'non-randomly' selected from a population of one thousand tags and labelled from 1 - 20. After the sample selection, and in accordance with classical 'pre test – post test' experimental design, the tags were further separated into two groups. The first group consisting of tags the odd numbered tags was selected as the 'Experimental group'. The remaining even numbered tags were then put into the 'Control Group'.

The next step was to plan the setup for the experiment and in so doing, discover and declare the independent, dependant and confounded variables along with any constants. To effectively the hypothesis required that the experiment be as controlled as possible, to this end the setup was designed to limit or eliminate any variations in subsequent tests other than the sample tag being tested and the state of the attack. The overall setup for this experiment is illustrated in figure 5.

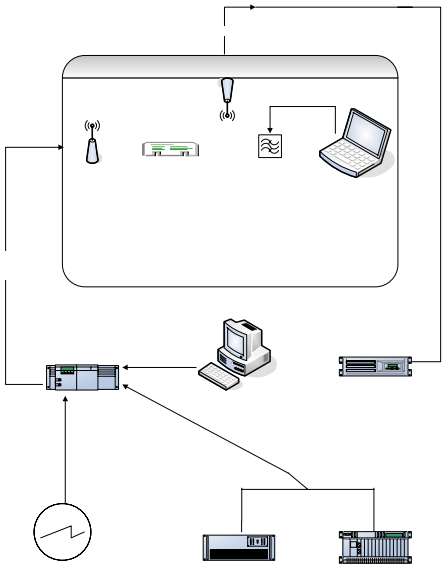


Figure 5. Experimental Setup

For this experiment there were two 'independent variables'. Firstly, the status of the 'interfering signal' or 'attack signal' is a binary state variable with the attacking signal either 'on' or 'off'. The second independent variable is which RFID tag from the experimental sample was being tested. As dependent variables are the measurable factors which occur as a result of a change in one or more independent variables, there was only one for this experiment, namely the 'Tag read status'. The status of a Tag read for this experiment is also a binary state variable with either the Reader unit being able to successfully read the Tag or alternatively no Tag being read. These variables are explicitly stated along with their possible values in table one.

Table 1. Independent and Dependant Variables

Type	Name	Values
Independent Variable	Interference Signal Status	ON | OFF
Independent Variable	RFID Tag Number	1 .. 20
Dependent Variable	Tag Read	YES | NO

The 'confounding variables' facing this experiment was the manufacture and operating status of the RFID tags in the sample and interference from 'background noise'. Given the simple physical nature of an RFID tag it is impossible to determine wether a tag is functioning or suffering from a manufacturing fault by pure observation. To limit the influence of this variable, every tag in the sample of 20 was tested for operation both prior and post experiment. In addition the sample size and the number of tests selected also minimise the impact of this factor.

The possibility of 'background noise' interfering with the experiment was mitigated through the use of a Faraday Cage which effectively reduced all 'background noise' to a negligible level. The use of pre-test post-test design also meant that if 'background noise' was the cause of any observed result then it would be likely that the event would occur across both the 'control' and 'experimental' groups and thus be detected. The remainder of the experimental setup was kept 'constant'. This included the physical location of the hardware, the hardware itself and the software setup.

Experimental Process

The purpose of the 'control group' was to illustrate the base/normal behaviour of the system without the attack, which could then be used for comparison against the results of the 'experimental group'. A conceptual map of the 'control group' process is given in figure 6. In this process the RFID system is monitored and logged without interference to ensure that in a protected setup that the reader and tag can communicate without interruption.

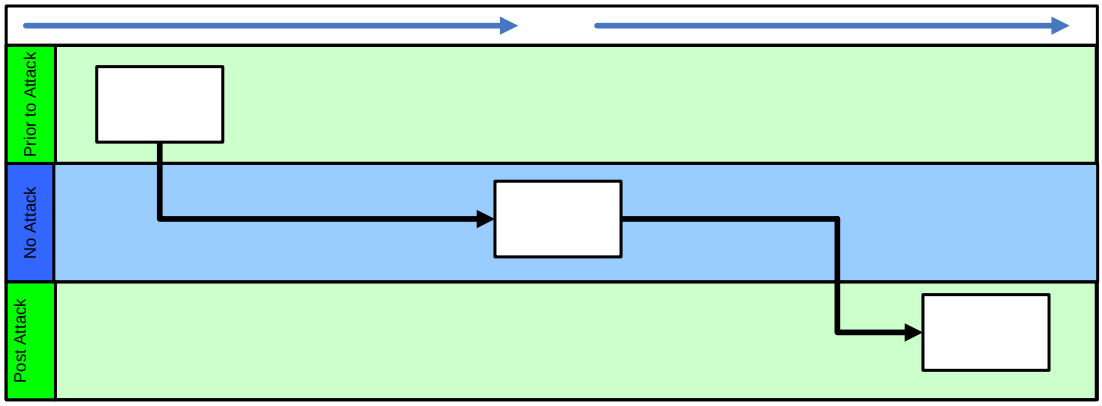


Figure 6. Conceptual Process for the Control Group

The experimental group follows a slightly modified process with the 'No Attack' section of the 'control group' replaced by the injection of the attack signal. To ensure that a tag in the 'experimental group' is functioning normally the tags operation is tested before and after the attack. This process is outlined in figure 7.

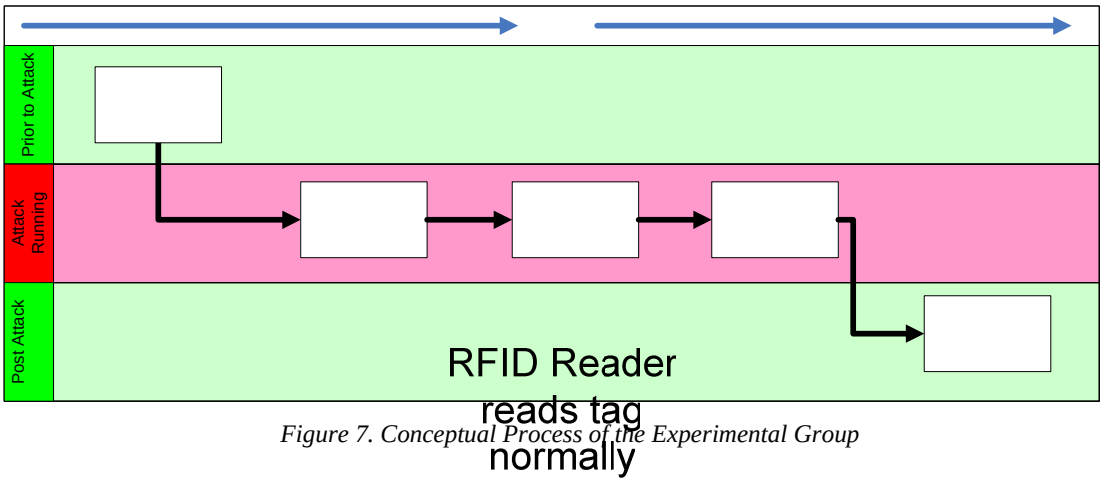


Figure 7. Conceptual Process of the Experimental Group

CONCLUSION

The findings from this experiment were conclusive, with every experiment across the 100 tests in both the control and experiment groups reacting as hypothesised. However due to the volume of data produced from the experiment this section will only discuss one tag and one experiment from each group with the complete result. The diagram below illustrates a test set from the control sample group which follows the procedure from figure 8.

In this test a tag from the sample group was placed in the faraday cage in accordance with the experimental setup described previously. Once the cage was closed the tags placement was registered and recorded by the reader software as indicated by the number 1 label in the figure. Two readings from the oscilloscope are then captured and marked on the diagram as 6 and 7. This reading shows only normal communication is taking place with no spike of transmission from the attacking signal. After a period of time the tag is then removed with the reader registering the tag removal at point 3 of the diagram. The lack of any further 'tag removal' or 'tag added' logs demonstrates that at no point during the normal operation of the tag and reader was communication disturbed. This is inline with the expected behaviour in a shielded system

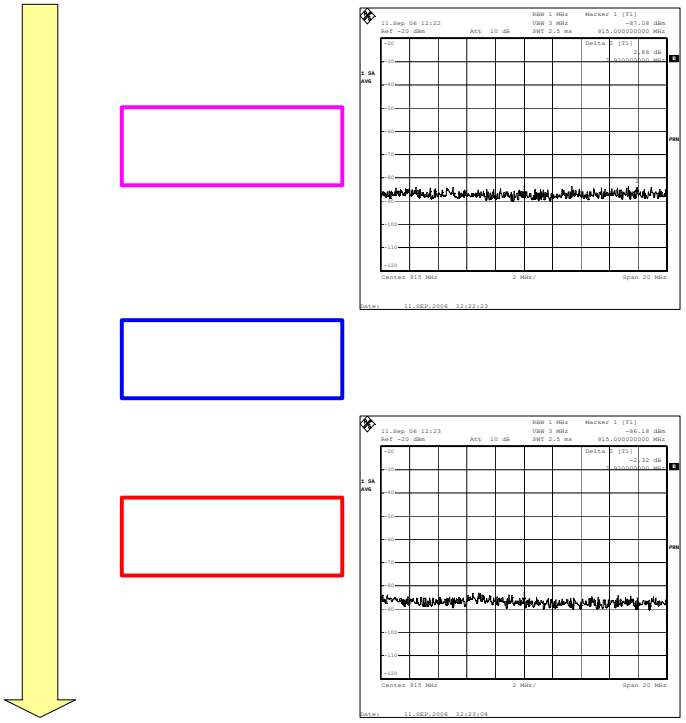
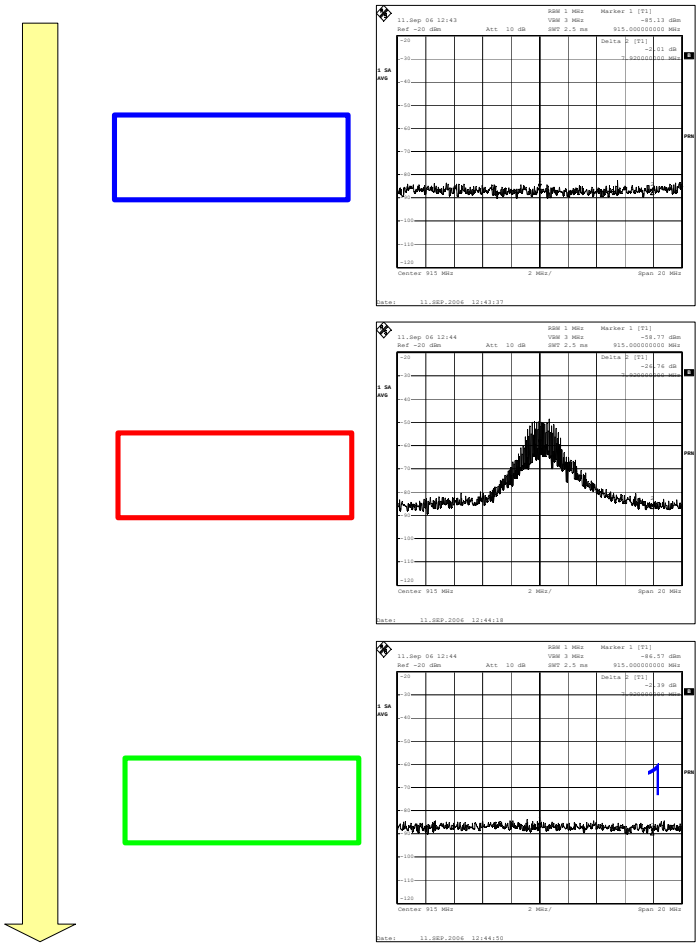


Figure 8. Annotated findings from a Control Group Tag

Each of the fifty tests conducted on the sample group demonstrated the same finding with no drop out during the period of experimentation. Such conclusive tests were deemed to indicate that without external interference the tag would respond to all reader requests and thus not be registered as 'removed' by the system until physically removed at the conclusion of the test period. The experimental group findings were compared to the bank of findings from the control group.



Added 1/09/2006 12 42 43 PM
00 27 32 20 00 00 00 00 00 01 90 01

Figure 9. Annotated findings from a Experimental Group Tag

The annotated figure above details the adding of a tag from the experimental group into the faraday cage following the same process as the control group in accordance with the procedure detailed previously in figure 8. The addition of the tag is logged by the reader and labelled with a number 1 above with an accompanying reading from the oscilloscope labelled number 5. The attack signal is then introduced and is recorded via a another capture from the oscilloscope which illustrates the spike of activity in label 6. The injection of the attack signal into the system is accompanied by a loss of tag to reader communication and this is recorded by the reader as the tag being removed from the communication field and logged in the diagram as label 2. After the period of attack is over the attack signal is then removed (label 7) and almost instantly the reader re-establishes communication and reregisters the 'adding' of the tag in label 3.

As with the control group all fifty tests from the experimental group followed the same pattern with the tag and reader communications being successfully disrupted via the injection of an attack signal. The experiment described in this paper clearly demonstrates that a single channel attack in completely clear conditions is effective despite the use of asynchronous Frequency Hopping Spread Spectrum communications. 915 MHz

Removed 1/09/2006 12 43 31 PM
00 27 32 20 00 00 00 00 00 01 90 01

TIME

RFID technology. RFID tags by their very nature are designed to be located remotely from the reader; this means that any tag not detected by the reader is not necessarily an availability issue as the tag may be assumed to be out of range. Thus the efficacy of this type of attack would suggest that implementations of RFID systems will require the development of systems to identify when such an attack may be occurring.

REFERENCES

EI8IC. (2002). ITU Regions Map. Retrieved 28/03/05, from http://www.mapability.com/ei8ic/index.html?http&&&www.mapability.com/ei8ic/maps/regions.html

EPCglobal. (2005). *EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960MHz* (No. 1.0.9): EPCglobal.

ISO/IEC. (2004). *Information technology - Radio frequency identification for item management - Part 6: Parameters for air interface communications at 860 MHz to 960 MHz* (No. ISO/IEC 18000-6): International Organization for Standardization.

ISO/IEC. (2006). *Information technology - Radio frequency identification for item management - Part 6: Parameters for air interface communications at 860 MHz to 960 MHz - Amendment 1: Extension with Type C and update of Types A and B* (No. ISO/IEC 18000-6): International Organization for Standardization.

Sarma, S. E., Weis, S. A., & Engels, D. W. (2002). RFID Systems and Security and Privacy Implications. In *Workshop on Cryptographic Hardware and Embedded Systems* (Vol. 2523, pp. 454-470).

Scharfeld, T. A. (2001). *An Analysis of the Fundamental Constraints on Low Cost Passive Radio-Frequency Indentification System Design.* Massachusetts Institute of Technology.

Sorrells, P. (1998). *Passive RFID Basics* (No. AN680): Microchip Technology Inc.

Wild, K. (2005). *3D Asset Location for Mobile Devices Using Passive RFID Tags.* Unpublished Masters Proposal, Edith Cowan University, Perth, Western Australia.

COPYRIGHT