# An Investigation into Long Range Detection of Passive UHF RFID Tags

Craig Valli
*Edith Cowan University*

Andrew Woodward
*Edith Cowan University*

Ken Wild
*Edith Cowan University*

Reino Karvinen
*Edith Cowan University*

# An investigation into long range detection of passive UHF RFID tags

Craig Valli
Andrew Woodward
Ken Wild
Reino Karvinen
School of Computer and Information Science
Edith Cowan University
c.valli@ecu.edu.au

## Abstract

*Radio frequency identification tags (RFID) have been in use for a number of years, in a variety of applications. They are a small computer chip like device that can range in size from a thumbnail to a credit card size device. They consist of a small silicon chip, and an antenna used to receive and transmit data. When a tag receives a signal from a valid reader it sends a response, typically a tag ID and any other requested/available data back to the reader device. The newer range of RFID chips that are coming into use now use higher frequencies (UHF) and are able to be detected, or transmitted to, from longer distances (1 – 10 m) with a conventional handheld reader. This increased distance alone presents many opportunities for users and misusers alike. These include but are not limited to passive scanning/sniffing of information in transit, deception, disruption of signal, and injection of malicious or false data into the broadcast envelope. There is no evidence currently in the literature of long-range scans or attacks on UHF RFID tag or supporting infrastructure. Given that these tags are now being used in military applications, an improved understanding of their vulnerabilities from long range scanning techniques will contribute to national security. An understanding of the long range scanning potential of these devices also will allow further study into the possible misuse of RFID technology in society by governments, business and individuals.*

**Keywords**

RFID, UHF tags, long range detection

## OVERVIEW OF RFID

Radio frequency identification tags (RFID) have been in use for a number of years, in a variety of applications. They are a small computer chip like device that can range in size from a thumbnail to a credit card size device. They consist of a small silicon chip, and an antenna used to receive and transmit data. When a tag receives a signal from a valid reader it sends a response, typically a tag ID and any other requested/available data back to the reader device.

RFID tags are similar to a bar code for much of their application, but they have several advantages. They do not need to be in line-of-sight like a conventional bar code, and they are less susceptible to environmental degradation. If a bar code gets wet or torn, or the lines in the code obscured, then it is no longer useful as it cannot be read anymore. In contrast, RFID tags can be coated in a protective resin rendering it less vulnerable to certain environmental factors. An advantage of the RFID tag system is that each has a unique identifying number and dependent on memory space can have an almost infinite range of numbers. For bar-codes, the range of numbers is limited by their use of numerical codes, which is also limited by the width of the label. Where bar-codes cannot store data, some RFID tags are able to store the equivalent of two pages ~ 4Kbytes of textual information on the chip that can be modified at will.

The greater robustness of RFID compared to other technologies is now seeing military application of this technology, particularly in the US (Gilbert 2003), as well as on a trial basis at a logistical level in Australia (Bushell 2004). The Australian Cattle Industry is now also using RFID to replace conventional cattle herd identifiers such as brands and earmarking (NLIS 2003). The mining industry also uses RFID for human resource and inventory tracking such as tyres for large earthmoving equipment. The healthcare industry employs RFID for the tracking of supplies and patients (Woodhead 2003; O'Connor 2005).

One of the most common types of RFID tag in use today are the so-called 13.56 MHz passives. These are powered solely by the signal emanating from the reader unit. Range for this type of tag may vary from 1cm to 1m, limited by the laws of physics, as well as by practical considerations. There are existing programs such as rfdump (www.rf-dump.org) that gather information from existing 13.56 MHz RFID tags, but this simply gathers information from the tags. There are similar programs to do this for other tags in existence and of course handheld readers essentially provide this functionality. The challenge is in combining this with accurate location of data at considerable distance

The newer range of RFID chips that are coming into use now use higher frequencies (UHF) and are able to be detected, or transmitted to, from longer distances (1 – 10 m) with a conventional handheld reader. This increased distance alone presents many opportunities for users and misusers alike. These include but are not limited to passive scanning/sniffing of information in transit, deception, disruption of signal, and injection of malicious or false data into the broadcast envelope.

There is no evidence currently in the literature of long-range scans or attacks on UHF RFID tag or supporting infrastructure. Given that these tags are now being used in military applications, an improved understanding of their vulnerabilities from long range scanning techniques will contribute to national security. An understanding of the long range scanning potential of these devices also will allow further study into the possible misuse of RFID technology in society by governments, business and individuals.

## OVERALL PURPOSE AND SIGNIFICANCE OF PROPOSED RESEARCH

The purpose of the research is to investigate long range location and scanning of RFID tags. Current UHF tag readers have an optimal distance of approximately 10 meters. It is hoped that this research will allow the detection of these tags at a range of up to 5 km.

The ability to detect RFID tags at long range has a wide range of legitimate and useful applications. These include tracking and movement of strategic assets such as personnel and inventory, herd management, disaster recovery, and asset control.

The initial stage of the research will aim to produce a proof-of-concept implementation which demonstrates that long range location of tags is possible. Currently, no system exists for the long-range detection of UHF RFID tags using ground based radio signal location techniques. There are systems available that use GPS devices in every tag to achieve location services (Jansen 2003). However, this is an added expense that could be eradicated by the development of the proposed system. The removal of GPS services also means that in the same design, the space, power and computation gained could be used for other tasks. An RFID based location system that is solely dependent upon ground based location methods provides a potentially cheaper and usable alternative. Furthermore, by using location based on radio signal propagation the problem of GPS black spots such as buildings, warehouses or other structure that block access to the sky will be mitigated against. This is not to say that ground based location services are not also susceptible to black spots, it is just that these are likely to be less of a problem.

## STUDY DESIGN

The methodology used for the conduct of the research will use a quasi-experimental method. The research will involve practical experimentation and theoretical modelling to examine long range detection and location for RFID UHF tags using an empirical learning approach. There are several stages to the study each being cumulative and building empirically on the previous stages

Stage 1 – Long Range Detection - will involve initial trials to simply detect the tags via signal resonance at range using a high powered antennae. This stage will be achieved with a custom built antennae that gives theoretically 15Dbi gain and placement of a small cluster of tags.

Stage 2 – Long Range Identification - This will be the placement of a small number of UHF RFID tags within an open field in a geographical area where there is relative radio silence, such as in rural Australia. Tags will be evenly distributed in a grid pattern at heights of 1m, and their location recorded using a GPS. This experiment

Stage 3 – Long Range Scanning – This will involve scanning and reading the tags as discrete tags at range.

Stage 4 – Location - Two RFID Reader stations will be placed at fixed points a set distance apart, adjacent to the tag field. Each reader station will include a GPS unit to determine absolute location. Each location station will include a rotating directional antenna, and computer controlled UHF radio transceiver. One station will transmit a series of short bursts of radio-frequency energy in a narrow radio beam into the field. The second station will receive the radio echo of any tags caught in the radio beam-path. These low level echoes will be accumulated by using averaging techniques over a large number of bursts to lift the signal above the background noise. The first station will then rotate its directional antenna array to the next sector of the field, and the process will repeat until the entire field is scanned. The two stations will then swap transmit and receive roles, and the process will be repeated. Signal responses from each will then be recorded, to hopefully permit triangulation and location of the RFID tags within the field.

## ANALYSIS AND TESTING

By using an empirical learning approach as the analysis framework, the data gathered from these field experiments will be analysed using established radio location methods and techniques to identify possible methods for location of UHF RFID tags. Finding the appropriate method for the system will be exploratory in nature.

It is envisaged that the data will have to be analysed through a series of cycles and levels of precision and accuracy to find the best balance between accurate location of RFIDs and cost of actual computation of location. This modelling will be achieved through the use of the existing radio location algorithms such as Time Difference On Arrival (TDOA) and relevant statistical calculations and methods. This stage of the process should easily be handled by the utilised hardware. However, it intended that some of the project will use modelling to examine various aspects, which is computationally intensive in nature. The use of existing compute cluster architectures to process and run models will garner significant time advantage for the researchers when processing these models.

## INTENDED OUTCOMES

This research should provide the rudiments of a system which allows for the long range location of UHF RFID tags in the field. If successful as a proof of concept then this research will have significant potential and implication. The effective long range scanning of UHF RFID will open up a wide range of good use and misuse applications. Good use could be in the mining sector to track humans in hostile work environments. A use in the livestock sector could see farmers being able to monitor and account for stock with the strategic placement of antennae around their property. This would add extra benefit as RFID technology is being used for herd identification in Australia already.

The defence sector is currently deploying this type of technology which means that this proof of concept has great intelligence and counter-intelligence potential. In addition the ability to scan at long range will have major combat implications if personnel and ordinance are tagged for inventory management and asset tracking.

From a misuse perspective it could be possible to scan a competitors inventory and gather critical business intelligence hence garnering significant arbitrage from this malfeasance of the technology.

## REFERENCES

Bushell, S. (2004). TAGS, You're it! URL: http://www.cio.com.au/index.php/id;648258786;fp;4;fpid;19 accessed 8/4/05

Gilbert, A. (2003). U.S. military expands radio-wave tracking. URL: http://news.zdnet.com/2100-1009_22-984391.html accessed 8/4/05

Jansen, S. (2003). Alternative Positioning: GPS is not the only way to determine position, RFIDs have a place too. URL: http://www.gisuser.com.au/POS/content/2005/POS16/pos16_feature/pos16_feature_3.html

NLIS (2003). Policy paper: Livestock identification and traceability. URL: http://www.aahc.com.au/surveillance/nlis_policy.pdf accessed 8/4/05

O'Connor, M.C. (2005). IBSS launches Healthcare Tracking. URL: http://www.rfidjournal.com/article/articleview/1318/1/131/ accessed 8/4/05

RF-Dump (nd). RF-Dump.org. URL: http://www.rf-dump.org/ accessed 12/4/05

Woodhead, B. (2003). Electronic tags: are we next? URL: http://afr.com/articles/2003/07/28/1059244557388.html accessed 8/4/05.

## COPYRIGHT