SECURE TRACKING SYSTEM FOR NEXT GENERATION CIT PRODUCTS

by

CHRISTOPHER WILLIAM KOSMAS

A thesis submitted to Plymouth University
in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

School of Computing and Mathematics

Faculty of Science and Environment

In collaboration with
Spinnaker International Ltd

March 2014

Abstract

Secure Tracking System for Next Generation CIT products

Christopher William Kosmas – BEng (Hons)

The Cash in Transit (CIT) industry demands reliable and innovative products from its suppliers to ensure safety and reliability within the industry. Product innovation has been directed at a bespoke tracking system for the Cash in Transit industry, which can meet its stringent requirements and excel above the capabilities of standard, readily available tracking systems.

The presented research has investigated the state of the art in tracking and localisation systems and has highlighted Wi-Fi as a potential novel Cash in Transit tracking solution. With research into 2.4GHz Wi-Fi and the effects in a CIT environment, the technology has been understood and demonstrated in terms of its advantages and weaknesses when applied to CIT.

The research has shown that 2.4GHz Wi-Fi is a novel and viable solution for both wide area tracking and localised tracking of a Cash in Transit security box by testing innovative ways of detecting theft using 2.4GHz Wi-Fi in a set of specific real-world scenarios. An embedded tracking system was developed and a thorough evaluation undertaken using a series of practical usage scenarios. The results show the proposed tracking capability is very effective and ready for initial effective use within a Cash in Transit security box.

Table of Contents

Acknowledgements

The author would like to thank the Technology Strategy board, Spinnaker International Ltd and its employees who contributed to this work. Thank you to Dr Cen Tjhai for his early contributions and to all at the University of Plymouth who supported this in their various ways.

A special thanks to Nick Tripp for his insight, belief, leadership and friendship during this study. Thank you for choosing me in the interview.

Much gratitude is extended to Dr Nathan Clarke of the University of Plymouth for his guidance, professionalism and kindness to the author throughout this work.

Without Dr Nathan Clarke, Nick Tripp and Spinnaker International Ltd, this work would not have been possible.

To my mother Alwin and my father Marios. Yet another thing to make you a little bit prouder.

Finally, this thesis is for my wife Charlotte. Thank you for supporting me and pushing me hard enough to achieve this and for believing in me and us. Perseverance and hard work got us both where we are and it will take us further. Thank you.

AUTHOR'S DECLARATION

At no time during the registration for the degree of Master of Philosophy has the author been registered for any other University award without prior agreement of the Graduate Committee.

Work submitted for this research degree at the Plymouth University has not formed part of any other degree either at Plymouth University or at another establishment.

This study was financed with the aid of a Knowledge Transfer Partnership from the Technology Strategy Board, Spinnaker International Ltd and partly self-funded.

Publications:

Christopher Kosmas et al. "A Security Container and Security Systems." GB Patent No. GB2472632. 16 Feb. 2011

Presentation and Conferences Attended:

Guest Lecturer and Workshop on GSM technologies at the University of Plymouth

External Contacts: Spinnaker International Ltd
Saltash Parkway
Saltash
Cornwall
PL12 6LF

Word count of main body of thesis: 43,246 Words

Signed

Date 06/03/2014

1. Introduction

1.1 The Demand for Tracking

As computing and handheld electronics have taken hold of our lives, the word ‘Tracking’ or to ‘Track’ is very commonplace with its uses expanding rapidly. The Oxford Dictionary defines the verb ‘Track’ as ‘follow the trail or movements of (someone or something), typically in order to find them or note their course’ (Oxford Dictionaries, 2013). As a result, the interpretation of ‘Tracking’ in this modern world varies and as examples of its broad nature, one use is associated with tracking of parcel deliveries and another is portrayed by the film industry as a very wide area, global, accurate and easy way of locating an individual of interest.

This author’s experience of tracking has varied from parcel deliveries to a small tray of product being tracked through a manufacturing process in a production facility. These two extremes each provide their own challenges; one a more wide area solution referenced to global mapping systems and the other is a bespoke system tracking a tray of parts passing through a conveyor belt production line, which is recording each stage in the manufacturing process. This latter tracking system that the author has experienced is a more localised tracking method which serves a bespoke purpose.

This thesis and the research contained within it is in collaboration with Spinnaker International Ltd, a UK based company designing products for the protection of cash in the Cash in Transit (CIT) industry. There is little academic research within the CIT industry with Spinnaker International Ltd driving such research and the absence of research in this field provides challenges to this thesis which attempts to act as a baseline for future research by including the experience and expertise of Spinnaker International Ltd in this industry. Smith and Louis (2010) state that there are three types of robbery offenders, amateurs, intermediates and professionals, the former being opportunistic while the latter are rigorous and motivated in their approach to CIT robberies. These typologies provided by Smith and Louis (2010) provide an insight into the person that performs Cash in Transit robberies and this supports the views and experiences of Spinnaker International Ltd as experts within this industry. As such, tracking and the Cash in Transit (CIT) industry meet within this thesis as a way of combating the theft of Spinnaker CIT products and catching CIT robbers.

This thesis will highlight the challenges faced by the suppliers to the Cash in Transit (CIT) industry such as Spinnaker International Ltd, so they can provide the reliable products and services that the CIT industry demands. These challenges form the platform which this research is based on, which is research into cost effectiveness and robust solutions for tracking a CIT box, a device used to transport cash safely where the cash would normally be vulnerable. The reader will also see that these challenges push the definition of tracking in this context into a system that combines wide area tracking and a more localised tracking concept of theft detection of a CIT security box. The research in the following chapters will focus on developing a bespoke tracking system that fulfils the requirements of the Cash in Transit industry.

1.2 Aims and Objectives

The aim of the research in this thesis is to determine the extent to which Wi-Fi 802.11 networking technologies could be utilised to track objects, in this case, objects for use within the CIT industry. Objectives of this research are to:

- Understand the current state of the art in tracking technologies.
- Theoretically evaluate the feasibility of 802.11 Wi-Fi technologies in a tracking application.
- Evaluate the properties of a CIT box in the context of its effects on Wi-Fi technologies.
- Experimentally evaluate 802.11 Wi-Fi technologies for tracking properties.
- Practically validate an 802.11 Wi-Fi tracking system within a practical scenario.

1.3 Structure of the Thesis

Chapter 1 has introduced the definition of tracking, its links to the CIT industry and the aims and objectives set out for this research and its thesis.

Chapter 2 introduces the Cash in Transit industry and the demands that it places on its customers. The CIT box and its functionality are presented as well as design constraints resulting from the CIT industry's demands. The chapter then researches the current state of the art in tracking technologies.

Chapter 3 introduces Wi-Fi as a novel way of tracking CIT boxes. It researches the services available for determining location based on a Wi-Fi access point and quickly evaluates their potential in this application before discussing the vulnerabilities to this tracking technology.

Chapter 4 presents the experimentation of Wi-Fi as a tracking technology by evaluating 2.4GHz signal characteristics including Wi-Fi. This forms the physical layer and foundation for using 2.4GHz Wi-Fi signals for the CIT tracking.

Chapter 5 presents experimentation into the effects of the CIT box on Wi-Fi technologies, providing vital information on how this technology might perform with an integrated system within the CIT box.

Chapter 6 presents core research and experimentation of tracking a CIT box using 802.11 Wi-Fi technology. It introduces several tracking concepts including theft detection where experiments are performed to prove the worth of these concepts. Finally, the results are presented and the outcomes of this research are discussed.

Chapter 7 shows the experimentation and practical validation of an embedded 802.11 Wi-Fi tracking device from the tracking concepts introduced in Chapter 6. It presents comparative and more in depth experiments into the 802.11 Wi-Fi tracking concepts using realistic scenarios, environments and hardware including that of an embedded purpose-built tracker fully integrated into a CIT box.

Finally, Chapter 8 draws all aspects of the research to a conclusion by examining the achievements of this research and discussing the practical and physical limitations of this work.

2. The Cash in Transit industry

2.1 The Cash in Transit Industry and its Environment

The Cash in Transit (CIT) industry focuses on delivering and collecting cash from a diverse range of customers. These range from small independent high street shops to large customers such as supermarket chains or banks. If cash is required to be collected from a customer, the CIT industry supports this requirement by collecting the cash and transferring it across the pavement in a secure container to a secure vehicle. At that point, the cash is considered safe as it is secured within the vehicle.

If cash needs to be delivered to a customer, the cash is transferred into a secure container within the transport vehicle and is then carried across the pavement to the customer and delivered. This cash transferred between the customer and the CIT supplier can take the form of notes or coins.

Given the industry, there is little academic literature available and therefore Gill (2001) and Smith and Louis (2010) are of the most reliable sources to correlate with existing industry expertise. Robbing CIT vans is not preferred over stealing the cash during a delivery because the complexities of robbing a CIT van far outweigh the risks, especially if the van is not guaranteed to be carrying large amounts of cash (Gill, 2001). It is also this author’s opinion from experience of the industry and the vehicles, that the security surrounding these purpose built delivery vehicles outweighs the majority of threats from robbers.

Gill (2001) identifies that 75% of robbers carried a gun that was capable of firing a lethal shot but the majority of robbers did not wish to hurt the victims. Smith and Louis (2010) support this with their profile of Australian CIT robbers with 62% of robberies involving a handgun as a weapon, thus making the likelihood of robbing the guard across the pavement preferable, less risky and more flexible for the robber (Gill, 2001).

Across the pavement protection systems for CIT deliveries offer the guards a safer alternative to carrying bags of cash. The protection system that has been the focus of this research is a product developed by the collaborating partner of this research. Spinnaker International Ltd is the leading UK and EU manufacturer for Cash Security protection systems offering multiple solutions for cash transportation needs throughout the United Kingdom and Europe. The industry expertise mentioned previously is founded from the knowledge and experience of Spinnaker International Ltd, its employees and engineering excellence, supporting the literature and knowledge available through Gill (2001). The protection system used in this research is a cash security box (hereby referred to as CIT Box) which provides the necessary protection of the cash across the pavement by not allowing the guard to open the CIT Box until they have reached the delivery destination or returned to the safety of the delivery vehicle.

Nick Tripp, Engineering Manager of Spinnaker International Ltd, stated during the author's induction at Spinnaker International Ltd that In the event of an attack, guards are instructed to relinquish possession of the CIT Box and not try to defend it. This approach carries a lot of sense as the protection of the cash is under the control of the CIT Box rather than the guard whose job is only to transport the cash box across the pavement to the destination, where it can then be opened by combining the Guard's ID and the Customer's ID. Nothing else will allow the CIT Box to open once the CIT Box has been removed from the Vehicle. This applies in reverse during a cash collection from the destination where an empty CIT Box is carried across the pavement, opened only at the destination and loaded with cash to be returned to the delivery van. Only when inside the van can the CIT Box be opened.

There are many demands placed on companies supplying to the Cash in Transit (CIT) industry. During the author's induction at Spinnaker International Ltd, he was advised of the requirements of CIT companies. A cash security container must adhere, but is not limited, to the following criteria:

- High reliability in abusive environments
- Qualify to industry standards for attack and degradation of the contents
- Qualify to legislative standards for Electromagnetic Compatibility, CE, WEEE, R&TTE and Health and Safety lifting requirements
- Cost effective products

The latest demands from Spinnaker's CIT customers are that the CIT boxes must not be rechargeable and must run for at least a year on their internal, non-rechargeable batteries. By implementing a non-rechargeable solution, the reliability of the CIT box is increased by ensuring that the CIT box is never exposed to a situation where its state of charge can fall below operational levels whilst it is in service. Another demand, which is important to this research, is that CIT boxes must be reliably tracked for recovery and detection of theft.

2.2 Asset Tracking, CIT's requirements and environmental conditions

Hazas et al (2004) found that numerous factors have driven the development of coarse asset tracking and location based services. Their research suggests that Wi-Fi, Bluetooth and other wireless sensing technologies, which are embedded in end-user devices, would accelerate the adoption of location based services. Since then, location based services are available on most smartphone devices using wireless technologies such as Wi-Fi, Assisted GPS and Cellular positioning, as supported by the work of Zandbergen (2009).

With such developments in technologies, which now provide the potential to track people and assets and provide services from these locations, it is only natural that CIT adopt these services for their industry. Tony Westington, Managing Director of Spinnaker International Ltd stated in a meeting with the author that it is easier for the CIT industry if an attacked CIT Box is recovered. For insurance reasons, this is true as it is easier to explain the loss or destruction of cash if there is physical evidence that it was in an attack. This evidence is conclusive with a recovered CIT Box.

Corruption of CIT guards is not an uncommon occurrence as suggested by Gill (2001) and Nick Tripp, Engineering Manager of Spinnaker International Ltd. CIT Guards have been bribed by robbers for information on deliveries (Gill, 2001) and experience at Spinnaker International Ltd has unveiled instances where CIT guards were prosecuted with collaborating conspirators in the form of customers who claimed that the guard was attacked, the CIT Box stolen and the customer and guard shared the contents of the CIT Box before disposing of it. With this corruption in mind, the CIT industry is keen to track these valuable assets to aid insurance claims and avoid fraudulent activities by CIT employees. The tracking of these assets can also provide a good method of detecting theft of a CIT box before the CIT Box is attacked.

During the author’s time at Spinnaker International Ltd, conversations and project meetings with management at Spinnaker International Ltd have focussed on the requirements of tracking within the CIT industry in order to achieve one or more of the following:

- Locate the CIT Box to recover it for insurance purposes
- Locate the CIT Box in order to assist the Police in apprehending and convicting the offenders
- Respond quickly to the act of theft of the CIT Box so that the Police can respond rapidly and be guided to the offender

- Maintain the quality standards demanded by Spinnaker International Ltd and the CIT industry
- Maintain the service lifetime of the CIT Box with the demand to not re-charge it.

During early discussions between the Author, Spinnaker International Ltd and CIT customers, the requirements placed on tracking a CIT box are that it must be quick to track when a theft or breach has been detected, detecting a theft before breach is an advantage, and tracking must be robust. This last requirement from Spinnaker's CIT customers provides the greatest challenge because as research will show later on, there is no ideal tracking technology for all circumstances or environmental conditions.

The author's experience of the CIT industry has shown many ways by which offenders will attempt to break in to a CIT box. Attacks have been seen where lethal weapons such as axes, angle grinders and ram attacks have been used to gain access to the CIT Box. More elaborate measures that have been used to attempt to defeat the protection measures of CIT Boxes have been to drop the boxes from extreme heights, ram cars on to the boxes, submerge the boxes in water or even liquid nitrogen in order to defeat the protection systems of the CIT Box.

During normal use, the CIT box will be subjected to the misuse by CIT guards who do not respect the property and asset that they are transporting. As a result of the above, environmental and handling conditions that the CIT Box is exposed to are brutal attacks, extreme forces, shock, extreme temperatures and water ingress. Therefore, a tracking system used within CIT must withstand the extreme abuse because unlike the CIT Box itself, the tracking system's main job starts when the CIT Box has reached the end of its functional purpose which is to degrade the contents of the box when a breach is detected. The tracking system's main job starts once the abuse has finished and the CIT Box is no longer of use. In short, the tracking system must withstand abuse and still function and report location information to perform its primary functions.

2.3 Tracking technologies within CIT

As discussed in 2.2, robust tracking is a requirement placed on companies supplying the CIT industry. The research below investigates the latest technologies available to assist in this requirement for robust tracking.

2.3.1 GNSS

The best known navigation system today is GNSS or Global Navigation Satellite System. It is the general term for what is better known as GPS or Global Positioning System. The term GPS as a technology is misleading as GPS is the name of the US owned NAVSTAR Global Positioning System which started development in 1973 and declared operational at the end of 1993 (Bonnor, 2012). Developed in parallel to NAVSTAR GPS was the Russian GLONASS which achieved full operational capability globally in October 2011 with the first satellite launched in 1982 (Bonnor, 2012).

GNSS is a cost effective way to provide tracking for devices that have view of the sky as demonstrated by the early work of Wahab et al (1997). The most developed and readily available tracking and navigation systems use the NAVSTAR GPS (hereby shortened to GPS) but as mentioned by Zandbergen and Barbeau (2011), the limitation of GPS is the inability to determine position indoors, underground or anywhere else where a solid object obstructs the view of the sky such as dense tree growth or urban canyons.

Wahab et al (1997) demonstrated that it is possible to track a vehicle using a cost effective GPS receiver with reasonable accuracy. What they also discovered are the disadvantages of using this system which are the accuracy of the system due to the ionospheric errors and multipath errors which arise from the atmospheric conditions (Wahab et al, 1997). They comment that improvements to the accuracies that they achieved could be improved using the DGPS system where ground stations collect information from the visible satellites and compute correctional information to transmit to the GPS receiver (Wahab et al, 1997). This technique has been proven to defeat ‘Selective Availability’ (SA) which was introduced by the US military to deny civilian users the full accuracy of GPS (Bonnor, 2012).

Another issue which Wahab et al (1997) comment on, is the time to first fix which is an inherent issue with GPS systems. This promoted the development of the Assisted GPS or A-GPS system. Zandbergen and Barbeau (2011) describe how a modern GPS enabled smart phone receives an up to date ephemeris, an approximate last known location and the current time to eliminate sections of the signal search space. This reduces the time to first fix and devices are available on the market which can support an embedded A-GPS system.

The latest advance in GPS systems is the use of a ‘High Sensitivity’ GPS receiver. Zandbergen and Barbeau (2011) describe how A-GPS enabled devices allow the High Sensitivity receiver to narrow the search space with A-GPS data and therefore permit a longer dwell time per unit search space. This allows the A-GPS High Sensitivity receiver to search for 10 times longer with the potential of picking up a weaker signal within that extra time.

Use of GNSS systems do however come with commercial risks. One risk is that both of the fully functional systems available, GLONASS and Navstar GPS, were primarily designed for military use and have been allowed for civilian use. This risk, combined with Europe’s lack of GNSS led to the development of Galileo, Europe’s first and the next generation of global satellite navigation (Bonnor, 2012). One advantage of Galileo over other generations of GNSS is that once functional, Galileo will have a Safety of Life (SoL) service which provides the standard level of performance but has integrity performance parameters for safety critical applications which require certain margins of accuracy (Trautenberg et al, 2004).

For the use of GNSS in CIT, Galileo is not quite ready, GLONASS receivers are not easily available but GPS receivers are readily available, cheap and have DGPS systems built in. It is also possible to purchase GPS receivers with assisted GPS which has the advantage of providing the faster start times required by the CIT industry.

One significant advantage of using a GNSS system in CIT is that a GPS receiver in a CIT Box is self reliant and can record locations without the need for other support devices. This means that the tracking system can lose communications with a remote server and still track its location by recording to any available internal memory in preparation for upload at a time when communications can be re-established between the CIT Box and the remote server. The challenge with GPS in CIT is balancing the tracking time with power consumption as GPS devices consume reasonable amounts of power when compared to what a CIT Box consumes.

2.3.2 GSM

Mainstream mobile services came about in the UK with the Global System for Mobile communications (GSM) standard in the early 1990's as a digital mobile communications system which provides voice and low rate data services (Küpper, 2005)**.** Due to its robust infrastructure, availability of embedded parts and cost effectiveness of those parts, GSM networks are ideal candidates for tracking systems. The immediate application is the wireless relaying of location data from a remote tracking device that has been deployed in the field.

Bshara et al (2011) discuss that localisation can be performed using cellular networks by measuring the physical quantities of a signal travelling between the mobile device and a base station of the network. This allows mobile cellular devices such as GSM phones and embedded GSM modules to provide location using the existing infrastructure. The physical quantities relating to the signal between the mobile device and the base station that Bshara et al (2011) discuss are received signal strength (RSS), time of arrival (TOA), time difference of arrival (TDOA) and Cell ID.

The first positioning method that was used by GSM operators is the Cell ID technique which utilises the unique identifier of the serving Base Station to approximate the location of the mobile device based on the location of the Base Station. This location is cheap, fast but lacks accuracy as GSM cells can cover large areas up to 3km^2 for 95% of cells (Bshara et al, 2011). The technique of Timing Advance discussed by Trevisani and Vitaletti (2004) provides the ability to increase the accuracy of the Cell ID technique. Each mobile device needs to maintain a timing slot on the network and to eliminate propagation delays, the base station calculates and instructs the mobile device to advance its transmission to account for these delays. This advance of transmission is known as Timing Advance and with this information a very rough estimate of distance from the base station can be calculated. Each unit of Timing Advance can be approximated to 500m (Trevisani and Vitaletti, 2004).

Other techniques to estimate location of mobile devices on a GSM network are to measure the Time Difference of Arrival (TDOA) of a signal transmitted from a mobile station and received at several base stations. Venkatraman and Caffery (2004) describe an algorithm that uses this TDOA with three base stations to locate the mobile device. Furthermore, these algorithms developed utilise the Angle of Arrival (AOA) on the serving base station to optimise the locations derived from the networks (Venkatraman and Caffery, 2004).

Chitte et al (2009) noted that a common source of positional information is the Received Signal Strength (RSS). A simplified model that they reference shows how distance from the source can be calculated based on the current received signal strength and a known path loss coefficient. The model that they review shows that it is affected by log-normal shadowing (Chitte et al, 2009). This is explained further by Wang and Zhu (2008) as they describe two major sources of error when using RSS to estimate distance from a source as multipath fading and shadowing. Multipath fading is caused by multiple signals with different amplitudes and phases arriving at the receiver and causing constructive or destructive interference (Wang and Zhu, 2008). The shadowing effect that Wang and Zhu (2008) describe is much simpler as it is the attenuation or loss of signals due to obstructions and environmental effects.

With this information, the use of GSM positioning techniques in CIT is welcomed as it is highly likely that a tracking system suitable for use in the CIT industry will include a GSM modem to deliver the remote tracking capability of the device. As this modem is likely to exist, using the location information from the wireless network providers adds value to the tracking solution. Tracking methodologies such as TOA, TDOA and AOA are not yet available in the UK but using methods such as Cell ID enhanced by Timing Advance are available with a commercial agreement through Vodafone UK under the branding of LBS, where the author has seen it demonstrated.

At the time of demonstration, the services were priced at 10p per location request which can add significant running costs to the customer if it was to be used as the primary method of tracking. Equally, implementing a path loss model to estimate distance would be subject to non-repeatable errors depending on the environmental conditions, the location of the tracker and surrounding obstructions as mentioned by Wang and Zhu (2008). This makes the Cell ID the most likely option for providing an approximate location of the device when no other method is capable of providing a location of the CIT Box.

2.3.3 Inertial Navigation

Inertial Navigation is a well-established method of estimating position. It involves the use of sensors to estimate the location and orientation of the object in question. It is frequently used to guide missiles, ships and spacecraft and does so by measuring angular velocity and acceleration using three orthogonal gyroscopes and accelerometers (Woodman, 2007).

The application of Inertial Navigation to a CIT Box would involve knowing the start location of the CIT Box and would involve the use of gyroscopes and accelerometers to estimate the distance travelled in 3D space. Developments in Micro-Electromechanical systems or MEMS have seen the introduction and development of MEMS Gyroscopes and Accelerometers. The physical size of these devices makes the use of Inertial Navigation possible for a CIT Box.

Inertial Measurement Units (IMU's) combine all the sensors required for Inertial Navigation and two such units were evaluated by Brown (2005) in an effort to evaluate the error in such systems. The evaluation performed used a land vehicle equipped with a GPS aided IMU following a pre-set path. Results showed that the quality of sensors within the IMU's played a big role and that performance of a GPS aided IMU was reasonable; however the errors quickly built up and they concluded that another source of information was required to keep the errors down with a MEMS IMU (Brown, 2005).

Accuracies of IMU sensors can be increased by moving away from MEMS sensors but the costs quickly make the use of such sensors unfeasible without even considering the size of such alternatives. As a result of this information and although MEMS sensors are improving constantly, they are still not suitable for use with Inertial Navigation systems for prolonged periods without correction data being fed back to the system from external sources (Woodman, 2007).

Despite this, the advantages of such a system within CIT are that the system is fully stand alone and does not require view of the sky, nor does it rely on radio signals to navigate. It can be enclosed in a sealed unit with its own internal power and without the need for antennas. The final aspect for consideration with using MEMS IMU's is that the power needed to process the information from the IMU is above the capabilities of a small efficient processor. This makes Inertial Navigation a target for the future but not very practical for CIT's current requirements.

2.3.4 Radio tracking using RF beacons

The technique of using radio signals to track animals in the wild is well established but not very well academically researched. The principle uses a transmitter with a battery pack and an antenna to transmit pulsed or constant signals (Mech and Barber, 2002). The transmitted signals are received using a handheld portable receiver which is capable of adjusting its receiving frequency to account for multiple transmitters transmitting at different frequencies.

The use of a pulsed radio tracker is known in CIT as an RF beacon and their use is relatively recent within CIT. The devices used are a proprietary ISM band transmitter, a battery pack and an interface to the CIT box which turns the beacon on automatically when a breach of the CIT Box is detected. Use in conjunction with the transmitter is an off the shelf receiver used to track dogs or animals fitted with transmitters. These handheld receivers have integrated high gain directional antennas to allow the user to determine the direction of the transmitting beacon.

This tracking technology within CIT provides many advantages. The transmitters are relatively low cost and do not consume power until it is time to track the CIT box. The author's experience of these transmitters is that a non line-of-sight of approximately 400m can be achieved on an industrial estate which makes this tracking method excellent for pinpointing a CIT box.

The disadvantages of this system mean that there is no global reference so getting within 400m of the CIT box initially is a near impossible challenge with this tracking method. The transmitter is within the Industrial, Scientific and Medical band which means that no license to transmit within this band is needed; however it means that a lot of other devices use this license free band. Interference is quite likely, making the task of locating the CIT box more difficult. The most significant disadvantage of tracking using RF beacons is that the tracking method is labour intensive. The operator using the receiver must be skilled in tracking using this technology so the time taken to locate the CIT box combined with the costs of hiring a skilled tracking operator make it costly to locate a stolen CIT box.

2.3.5 Tracking indoors

The requirements for tracking in CIT have been described above including the different technologies that can help to fulfil the requirements for a robust tracking solution for CIT boxes. The weakest link in tracking of any form is the ability to track in an indoor environment. As Zandbergen and Barbeau (2011) have stated, GNSS is poor when used indoors but the global reference capabilities of GNSS tracking make it the most favourable tracking method for any system that has a clear visibility of the sky.

When indoors, more novel tracking solutions should be considered in order to provide the positional information required to track a CIT box. Liu et al (2007) describe a host of radio based systems and techniques for indoor localisation. Some of these techniques they describe, such as the GSM methods for positioning, have already been discussed above, however they discuss other methods, the most interesting being the use of narrowband IEEE 802.11 signals, Bluetooth, proprietary UHF solutions and positioning using multiple media (Liu et al, 2007).

The techniques described by Liu et al (2007) for WLAN positioning are for localisation. The techniques described that use signal strength and TDOA would need a global reference associated with the transmitting stations so that any tracking system implemented by a CIT box would be capable of determining approximate location of the box.

Fuchs et al (2010) describe a fingerprinting method using WLAN signals to provide a position estimate of the system based on signal maps of each transmitting WLAN station. This is a simple system which is flawed by two main factors. The first being the amount of work needed to create the fingerprints for each transmitting station and the second is that if the station is not under proprietary control, it is possible that it can change position or that the structures surrounding it can change (Fuchs et al, 2010).

Liu et al (2007) mention the use of proprietary solutions in the UHF band, including 2.4GHz which is one of the signal frequencies used by WLAN systems. These proprietary solutions provide advantages to an indoor tracking system as techniques such as Time Difference of Arrival (TDOA) can be implemented and control over the transmitting stations can be achieved. This does however mean that these proprietary indoor location systems will be placed in strategic locations and do not provide a global indoor tracking capability that is most in demand for CIT. The costs of implementing and maintaining a proprietary network in a multitude of locations means that the CIT industry will need to be convinced that the system provides them with the solution that they require at the right price. As is described later on in this thesis, it is a combination of proprietary and commercial systems that provide this novel tracking solution to the CIT industry. The tracking components from competitive suppliers within the CIT industry were reviewed and of those technologies, none were Wi-Fi based while one was reliant on GPS for location, another was reliant on GPS and cell location information and the final device was based on a proprietary system that is predicted to use a combination of cell mast data, antenna direction, received signal strength and a path loss model as proposed by Hata (1980).

2.3.6 Conclusions

To date, the most utilised tracking technology within CIT has been a combination of GNSS solutions backed up with GSM based tracking systems. Table 2.1 compares the technologies discussed in this chapter with the parameters most important to the CIT industry.

	Start-up time	**Outdoor Accuracy**	**Indoor Accuracy**	**Energy Consumption**	**Cost**	**Package Size**
GNSS	Very Slow	Very High	Very Low	Medium	Low	Small
GSM	Medium	Low	Low	High	Medium	Small
Inertial Navigation	Always Running	Decreasing with Time	Decreasing with Time	Very High	Very High	Large
Radio Frequency Beacons	Fast	Low	Low	Low	Low	Small

Table 2.1: Technology comparison to CITs importance criteria

None of the tracking technologies described here provides the solution required by the CIT industry. Indicative of this is the Indoor Accuracy which is at best, low. None of the solutions in Table 2.1 provide a small package size, low cost with high indoor accuracy which start-up fast. As such, this is the target for a bespoke tracking solution in the CIT industry.

3. Tracking Technology Review

The previous chapter has introduced the tracking technologies used within the CIT industry; however there are many applications that either require tracking or utilise a form of tracking to perform their functions. As an example, the early work of Bahl & Padmanabhan (2000) showed that radio frequencies can be used to determine the location of an individual equipped with a wireless transceiver to within 2 to 3 metres. This work was able to track users inside a building using radio frequency signals and provide location aware services using this technology. Bajaj et al (2002) have dated the importance of location tracking back to World War II for its uses with navigating and targeting, but they have identified modern applications to name but a few, as emergency response, resource management and stolen vehicle recovery (Bajaj et al, 2002). It was considered prudent to review this work within the context of this research. This chapter aims to explore these by researching into the different tracking and location technologies that allow the user or device to navigate, recover lost property, provide services or manage supply chain and manufacturing systems.

3.1 Vehicle Applications

Before the turn of the century, motor industry experts estimated that 800 million vehicles would be registered worldwide by 2005 (Powers, Nicastri, 2000). Their expertise and research has also shown that major future components in vehicles would be GPS and multiple sensors in order to enable the vehicles to become safer and smarter (Powers, Nicastri, 2000). With this foresight and research, modern day applications for tracking and location of vehicles have developed, however the underlying research into GPS systems for vehicle navigation has been reinforced by early research by Hunter et al (1990) who showed that significant accuracy can be achieved using an in-vehicle differential GPS unit for navigation. More recently, Duan and Wang (2013) successfully navigated a test vehicle equipped with differential GPS and an Inertial Navigation System (INS) accurately, proving that intelligent vehicle navigation and positioning is possible.

Another application for vehicle location and navigation is to use vehicle tracking data to assess and predict traffic conditions. This work by Brakatsoulas et al (2005) identifies the measurement errors of GPS and the sampling time of the measurement system as a source of measurement errors in their system. This in part supports the research by Duan and Wang (2013) on their selection to integrate an Inertial Navigation System with a differential GPS system in order to improve accuracy.

One of the most expected vehicle applications for tracking is stolen vehicle recovery. Addressing vehicle crime is a large part of the Automotive industry and electronic immobilisers are a large part of vehicle security since their mechanical alternatives were relatively easy to bypass (Farrell et al, 2011). Early immobilisation systems were developed with a transponder inside the vehicle key (Khangura et al, 1993) whereas later immobilisation combined Remote Keyless Entry as legislation mandating some form of immobilisation was introduced in Germany requiring all 1998 and later vehicles to comply in order to deter theft (Davis and DeLong, 1996).

Modern day vehicle trackers can consist of a GPS device with a GSM device to relay the tracking information back to a centralised location. This is supported by Maurya et al (2012) who describe the design of such a device and its uses as a stolen vehicle recovery aid and an anti-theft system. This is complemented by Guha et al (2012) and their AutoWitness system which can track a vehicle once motion is sensed, by using Inertial Navigation and a GSM/GPRS modem to transmit data remotely. The Inertial Navigation and Dead Reckoning of the AutoWitness system give it the advantage of being tolerant to GPS outages (Guha et al, 2012) however Inertial Navigation is subject to divergence due to error stack ups which can adversely affect the primary function of the AutoWitness device.

Since its UK launch in 1993, the TRACKER system developed for locating stolen vehicles, has been an alternative to GPS based tracking systems. The system works on the basis of a vehicle mounted transponder transmitting a tracking signal on a dedicated frequency. Police cars equipped with a Police Tracking Computer can then receive the signal and proceed to recovering the vehicle (Wheatley, 1993). The U.S.A variant of this system that first became available in 1986 (Wheatley, 1993) is known as LoJack and operates in the same manner as the TRACKER system available in the United Kingdom and are known to have deterrent effects regarding vehicle theft (Mitra et al, 2009). An alternative to the LoJack and the TRACKER system is proposed by Song et al (2008) who have identified that the LoJack system has a high initial cost and high maintenance costs. They have also identified that GPS systems are easy to defeat and therefore have proposed a sensor based network with nodes installed within vehicles and a base station in each parking area. Neighbouring nodes are monitored with each node reporting a status periodically. If the vehicle and its allocated node are removed without appropriate authentication, the neighbouring nodes will ensure that they report this to the base station (Song et al, 2008). To track a vehicle, nodes are deployed on the roadside, this giving a tracking capability as well as theft detection capabilities (Song et al, 2008). This is a novel and different tracking approach to vehicle recovery.

The proven effectiveness of the LoJack system was evaluated by Gonzalez-Navarro (2007) where the outcome showed that vehicle thefts of a specific Ford vehicle fitted with LoJack fell by 50% in Mexico where as LoJack claim a 90% recovery rate which is typically within a few hours (Roberts, 2012). However, the way in which LoJack is marketed to the public in different countries was determined as important by Gonzalez-Navarro (2007). If the LoJack system is sold on known models then it is proven that thefts of these models are significantly reduced (Gonzalez-Navarro, 2007) thus showing the deterrent benefits of vehicle tracking.

A study on vehicle antenna performance and reliability has been performed by Scogna and Wang (2008) with the location of the antenna in the rear wheel arch of the vehicle. Their modelling revealed that the vehicle's body also forms part of the antenna system as currents are excited in the body shell. Wheatley

(1993) stated that the antenna placement within TRACKER and LoJack equipped vehicles is selected at random on the vehicle and can be in one of 30 different locations. Scogna and Wang (2008) through their modelling have shown good results with antennas fitted to vehicles.

Vehicle security has an impact on insurance costs. This is documented by Shaw and Pease (2010) who mention that the organisation that provides the basis for security rating which directly influences vehicle insurance premiums is the Thatcham organisation. The test data provided by Thatcham is fed directly into vehicle manufacturers and there is a significant element of confidentiality when physically determining the security rating of vehicles (Shaw and Pease, 2010).

Abdullah (2011) has concluded that present vehicle alarm systems are no match to the well-equipped car thief and introduces a mobile controlled car security system which has the capability to remotely control any of the car’s security features and location is provided using GSM positioning. In theory this system would enhance the security features of the vehicle; however there would be concerns around the safety of such systems in practice. Within the automotive industry, such safety concerns are highlighted by the ISO26262 standard on Road Vehicle Functional safety (ISO26262 Parts 1-9, 2011; ISO26262 Part 10, 2012) which aims to assess the potential hazards due to malfunction for automotive electrical and electronic devices (Kafka, 2012). Permitting control of the vehicle’s security systems such as the alarm, locking and potentially the vehicle immobiliser will be subject to an Automotive Safety

Integrity Level (ASIL) assessment under the ISO26262 standard which can hinder the potential introduction of the system proposed by Abdullah (2011) due to cost and development investment.

Vehicle location and tracking can also assist in the event of road traffic collisions through detection and automatically contacting the emergency services. Such an idealised system has been mentioned by Acharya et al (2008) who have said that such automated systems would provide a more rapid response over responses relying on human input. Their work focusses on the research into design of a general purpose automatic emergency notification system for vehicles (Acharya et al, 2008). Such systems exist that are integrated into vehicles and have been analysed by the work of Verma et al (2007) of the General Motors Corporation. The system introduced by OnStar into General Motors vehicles incorporates Advanced Automatic Crash Notification (AACN) which automatically calls the OnStar centre when an airbag is deployed, a maximum detected rate of change of velocity exceeds safety criteria or if a roll-over of the vehicle is detected; the location of the vehicle is provided by a GPS receiver on-board the vehicle (Verma et al, 2007). Such other OEM systems in existence that are GNSS based are provided by BMW and Mercedes Benz (Quddus et al, 2006). Such systems as described above can be termed 'Mayday systems' for their abilities to perform automatic notifications in the interests of safety (Zhao, 2002) but they also serve another purpose, which is the merging of telecommunications and information processing for use in vehicles (Ai et al, 2007). This field of Telematics encompasses Navigation and services such as Yellow Pages listings as well as potential for Automatic Crash Notifications described above (Ai et al, 2007). Hossain et al (2010) have broken down vehicle telematics into three applications. The first application has been described above which is the safety aspect but building on this, Hossain et al infer further applications such as collision warnings in the event that there are multiple chain collisions ahead, road conditions such as slippery roads and the potential of approaching emergency vehicles. The second application described is a Traffic Information System, which informs the driver of congestion and directs the driver to an alternative route with minimum delays (Hossain et al, 2010). The third application described by Hossain et al is the comfort and entertainment application where the infotainment system can provide multimedia streaming, local information such as refuelling stations, rest stops and restaurants. All these applications require the use of a location determining device or system and Hossain et al (2010) have mentioned that WiFi, WiMAX, 3G and satellite technologies are vital to support vehicle telematics.

With everything that has been mentioned so far with regards to vehicle security and the associated location related elements, no mention has been made to the infrastructure surrounding these systems. Modern vehicles are sophisticated with multiple electronics control modules networked together by various network communication systems and architectures (Wolf et al, 2004). The networks, of which these control modules are connected to, can be accessed through the On-board diagnostics connection in the vehicle which was mandated by the United States government and has since become a standard interface into vehicle networks (Koscher et al, 2010). These control modules can influence vehicle systems such as the Anti-lock brakes, engine control and more safety critical systems such as Electric Power Assisted Steering and Dynamic Stability Control. External access to the vehicle networks, the most popular being the Controller Area Network or CAN (ISO11898-1, 2003), is becoming more common as aftermarket devices such as audio equipment, Telematics and safety devices such as the research of Acharya et al (2008) with their general purpose automatic emergency notification system for vehicles and Abdullah (2011) with the researched device that would enhance vehicle security. Such devices and the access to the vehicle networks can bring rise to errors and to malicious attempts to circumvent security and safety systems. This is reinforced by the investigations of Koscher et al (2010) who demonstrate the ability to ignore driver input and control automotive functions. Such vulnerabilities can lead to incorrect notification of vehicle location after a collision, navigation issues through a compromised infotainment system or even compromise vehicle safety.

One of the other considerations relating to modern vehicles is the EMC aspects that can affect the vehicle but also the radio devices, which the Mayday systems and infotainment are reliant upon. Borgeest (2012) has researched and documented interfering elements such as PWM converters and DC/DC converters which are commonly found on hybrid and electric vehicles, which can impact on devices that rely on radio frequency signals for their function. Such systems can be as simple as radio and television reception or interference could possibly affect the GPS reception this compromising the Mayday systems on vehicles. The EMC of a modern vehicle is not well researched however

Borgeest (2012) has provided the ability to assess risks in order to be aware of the effects EMC may have on the function of the systems mentioned in this section.

Mustafa et al (2006) have presented a system which can provide the identification of a vehicle and permit stolen vehicle recovery by forming an ad-hoc network with police cars and other cars in the vicinity. The proposals and prototype implementation by them is based on a short range wireless network and this short range factor means that for the stolen vehicle to be visible to another vehicle in the vicinity, it has to be within a minimum distance from the stolen vehicle. Mustafa et al (2006) mention that GPS systems are expensive and therefore are cost restrictive but if a GPS receiver is also included within their prototype system, the approximate stolen vehicle's location could be sent to the police vehicles if the identity of the stolen vehicle was reported to the police vehicle via another vehicle in the vicinity which was equipped with a location enabling device.

Other more sophisticated location tracking techniques are those that utilise vision systems. In 1985, Alvin, the Autonomous Land Vehicle, performed its first outing and in subsequent years its navigation capabilities were improved (Turk et al, 1988). Some of the basic goals of an Autonomous Land Vehicle as described by Turk et al (1988) include road following, position estimation and obstacle detection. Obstacle detection is important as it can also feed into the driver safety of modern vehicles as Sun et al (2006) describe in their review of On-Road vehicle detection. Their review highlights that tracking is important for high speed and low speed driving where vehicles are within close proximity to each other where the target is to alert drivers of the driving environment and potential collisions (Sun et al, 2006).

The final vehicle application researched for this chapter is Automatic Number Plate Recognition (ANPR) technology. Using neural networks, characters on a vehicle’s number plate are recognised (Tatale and Khare, 2011) and therefore this means that vehicles can be tracked by virtue of them being identified. There is documentation of its uses in Law Enforcement in the United States (Gordon and Wolf, 2007) and in India for traffic tracking (Kulkarni et al, 2009). ANPR in the United Kingdom has developed into a sophisticated network of over 3000 cameras linked to a database which can detect vehicle license plates and identify the vehicle at speeds of up to 100 miles per hour (Evans-Pughe, 2006). This vehicle tracking system can allow law enforcement officers to track down criminals and Evans-Pughe (2006) has indicated that this tracking system can help improve the efficiency of police operation as the number of arrests by ANPR officers is around 100 per year where the non-ANPR officers average around 30 arrests per year. Such ANPR cameras are placed in gantry’s, on poles or are vehicle mounted (Evans-Pughe, 2006; Gordon and Wolf, 2007) and feed information directly into roadside officers to help track criminals and offenders.

3.2 Supply Chain and Manufacturing

As of 2008, Martinez-Sala et al (2009) reported that the world's largest pallet and container leasing company had more than 285 million units. Knowing the magnitudes involved, it is clear that Supply Chain would benefit from tracking and this is what is explored by this section. A technology used for tracking in Supply Chain and Manufacturing is presented by Martinez-Sala et al (2009) who describe the introduction of RFID systems into the fresh fruit and vegetable supply chain as a revolutionary technology for capturing data. They describe the legacy barcode system as error prone and the perception of RFID is that of a barcode substitute rather than a reliable value-added service. This is supported by Michael and McCathie (2005) who identify the ultimate aim of RFID in Supply Chain Management as the capability for item-level tracking with the advantages of providing non-line-of sight scanning, reduced labour levels and improved inventory management. The negatives as told by Michael and McCathie (2005) are that RFID is clouded by privacy issues, lacks standardisation, robustness, and is costly.

A tracking technique researched by Holmström et al (2009) described as Item Centric Tracking is an approach that can be taken to improve Supply Chain Management. The basic principle that they describe is to treat the tracked item as the entity with the location as a property of the item. This method differs from the approach of location based control of an item with the advantage of the former being that the focus of control is on the item rather than control being on inventory and asset accounts in pre-defined locations (Holmström et al, 2009).

RFID tags are the technology of choice within this sector and they consist of an antenna and an Application Specific Integrated Circuit (ASIC). RFID tags can be active or passive with the difference being powered or unpowered. A passive tag is read by the means of a reader which transmits a modulated signal which is received by the tag's antenna. The voltage created by the tag's antenna is used to power the ASIC which then responds by varying its input impedance and thus modulating the back-scattered signal (Rao et al, 2005). The advantages for RFID tags have been mentioned previously, however in detail, non line-of-sight scanning does have advantages over its predecessor, the barcode, as the orientation of the object is no longer a factor when scanning items which means that extensive human intervention or rigorously controlled environments are no longer required (Juels, 2006). This also means that RFID works effectively in harsh environments where visibility is impaired, and response times are rapid; around 50 milliseconds, and passive tags can be read at distances of up to 6 feet away (Tuttle, 1997) although reliability at this distance is questionable.

More recent advances in RFID systems can monitor temperature, light and humidity integrated into an RFID tag as demonstrated in the fresh fish logistic chain by Abad et al (2009). This system can not only feed into the logistics of tracking because of its RFID capabilities, it can also monitor the condition of the merchandise without having to disturb it because of the non line-of-sight capabilities of RFID (Abad et al, 2009). Another similar technique used in the supply of perishable foods to provide monitoring of refrigerated goods is discussed by Jedermann, Ruiz-Garcia and Lang (2009). They describe the use of this semi-passive RFID system as capable of ensuring the quality of these goods delivered to the customer as well as tracking their location, where the objectives of their study were to use this RFID system to locate weaknesses in the supply chain which too involves identifying and tracking where the goods are within the chain.

Angeles (2005) describes 6 cases of RFID use within this environment with the most interesting case being the port of Singapore which has invested significantly in the installation of RFID transponders in the port shipyard to manage and track the location of thousands of cargo containers that are moving in and around the shipyard daily. The use of RFID in this scenario is in agreement with the harsh environments that Tuttle (1997) has discussed, however the cost of tags in 2005 was quite high (Angeles, 2005) which subdues the enthusiasm of businesses to invest in this technology. As with all technologies, maturation gives the opportunity for costs to reduce and CMOS technologies as studied and discussed by Glidden et al (2004) are helping the costs of RFID come down to the levels that will spark industry’s interest in greater numbers.

Much like Supply Chain Management, Manufacturing can benefit from the intelligence of tracking product. Brewer et al (1999) describe intelligence in manufacturing as the automatic gathering of information which improves the efficiency of the process. This early work shows consideration of the benefits of intelligence in manufacturing with an eye on the use of GPS to assist this process as well as RFID technologies (Brewer et al, 1999) which are more favoured by the Supply Chain and Manufacturing sectors as a means of locally tracking products rather than globally tracking the location of the product on demand.

Min et al (2007) have identified High Frequency (HF) RFID tags as the most appropriate for use in manufacturing because of the read speeds and penetration of the Radio Frequency waves while Brusey and McFarlane (2009) mention the problem of keeping track of the identity and location of objects in their example of a complex assembly process. They identify that a system that tracks an object must provide location, state and identity information on demand (Brusey and McFarlane, 2009). Providing and utilising this information in a manufacturing process can certainly enhance the efficiency of the operation and influence the end quality of the product. Wang et al (2007) describe the setup for line-side RFID readers with each object having a tag attached to be read by the reader in due course. Using this configuration, it has been shown that objects in an assembly line can be tracked using RFID technology with a note made by Wang et al (2007) that the use of GPS and GPRS tracking technologies being not applicable in manufacturing which is in contrast to the early work of Brewer et al (1999).

3.3 Aircraft Navigation

The navigation of an aircraft requires the pilot to determine the location of the aircraft and adapt or correct the course of the aircraft from this data. There are many ways that are used to locate an aircraft in order to permit global navigation and this section serves to research these methods and their application to modern aircraft navigation.

Star tracking has provided a way of navigating for many centuries however its flaws are simple and apparent as cloud, fog or rain can obstruct visibility of the sky (Getting, 1993). To combat this, Inertial Navigation is the alternative (Getting, 1993); however as described in Chapter 2, Inertial Navigation suffers from divergence of which the divergence rate is directly related to the quality of the sensors (Koifman and Bar-Itzhack, 1999). The sensors required for Inertial Navigation are explained in detail by King (1998) where he describes the requirement for three accelerometers and three integrating-type gyros mounted in a set of three gimbals. The gyros, connected to servo motors keep the inner most gimbal in a constant orientation in space, thus providing the aircraft with an azimuth, pitch and roll (King, 1998). The accelerometers provide the means of determining acceleration, velocity and finally, distance through integration (King, 1998). Tan and Park (2005) challenge the need for gyroscopes in Inertial Navigation systems citing cost, size and accuracy as the main factors for gyro-free Inertial Navigation. Using six accelerometers in a cube configuration, they proved that gyro-free Inertial Navigation is possible; however it is also prone to divergence (Tan and Park, 2005).

Interesting research by Allerton and Jia (2005) has provided a review on the design of Inertial Navigation systems in aircraft, focussing on fault tolerance in such systems. They propose three redundancy strategies being hardware, software and analytical redundancy to improve fault tolerance as a result of independent systems providing cooperation (Allerton and Jia, 2005). Divergence is a common problem seen in all research and it has been suggested early in the development of GPS that Inertial Navigation is combined with GPS in order to counter and correct this divergence (Cox, 1978). Unmanned aircraft have had assistance with their navigation through use of vision systems to correct Inertial Navigation errors (Wu et al, 2005) but the use of GPS to correct inertial errors is the recommended approach recently by Tan and Park (2005) as well as King (1998) with the existence now of a fully developed and proven GPS constellation.

GPS provides good navigation capabilities and this has been researched well in Chapter 2. Its applications to aircraft navigation seem logical and early research by Wang et al (1996) suggests a GPS based architecture for navigation of unmanned GPS based aircraft. There are issues with GPS based aircraft navigation that need to be understood and these are described by Ochieng et al (2003), who review the integrity of GPS and its impact on civil aviation safety. Integrity, in this instance, is the level of trust that can be placed on the information provided by the GPS navigation system. Several errors contributing to integrity concerns have been noted by Ochieng et al (2003) where a clock failure on a GPS satellite in 2001 caused range errors of thousands of meters, incorrect modelling of orbital parameters in 1993 caused a steadily increasing range error, and command uplink errors in 1995 caused a 6 second loss of lock on a specific satellite. Such events can impact the navigation of an aircraft that on approach or preparing to land and Walter et al

(2008) show that by 2020, such events will be reduced due to improvements to the GPS constellation but also as a result of the introduction of other satellite navigation constellations from Europe, Russia or China.

Correcting Inertial Navigation errors is useful to aircraft navigation. Very early research has been performed to integrate legacy systems such as VHF Omnidirectional Range (VOR) and Distance Measuring Equipment (DME) as Bryson and Bobick (1973) show in their research. The VOR and DME systems which operate at 108-118MHz and 962-1215MHz respectively (Hawthorne and Daugherty, 1965), were used extensively in the early days of aircraft navigation and VOR allowed the navigator to determine the aircraft's bearing relative to a base station within 1.5° and DME permitted the navigator to determine the distance of the aircraft to the base station within 1000 feet of error (Bobick and Bryson, 1972). These single beacon systems serve as an example of early systems that were used to determine location of aircraft but their resolution was limited, hence the work of Bryson and Bobick (1973) to integrate VOR and DME results into Inertial Navigation systems onboard aircraft.

Other radio navigation systems which supported the location and navigation of aircraft before Inertial Navigation and GPS became dominant were the Tactical Air Navigation System (TACAN) (Garfield, 1958), Automatic Direction Finders (ADF) (Cleaver, 1947) and DECCA (Powell, 1958). TACAN combined Distance measurement and bearing from a base station where early ADF systems used rotating antennas on-board aircraft to detect direction from a fixed and known base station that is transmitting an omni-directional beacon (Umpleby, 1946).

The DECCA system constantly compared the phase of signals received from separate base stations and comparing the phases against a hyperbolic curve to determine the intersection point of these signals and thus the location of the aircraft or ship is determined (Powell, 1958). The DECCA system is one of the few early radio navigation systems that extended to marine navigation as well as aircraft navigation, however it was more used for ship navigation than aircraft with installations on 25,000 ships but only a few hundred aircraft (Powell, 1982). These old and well established navigation aids allowed aircraft navigators to determine their locations and navigate aircraft for over 30 years before Inertial Navigation started to become more widespread in the 1970's as mentioned by Bobick and Bryson (1973).

White (1962) states that an aircraft can be navigated between two points using three parameters; heading, drift angle and ground speed. Heading can be determined from flux compasses and Caruso (2000) describes a method of determining heading from solid state magnetic sensors and a tilt sensor to determine heading. Caruso (2000) states that heading and attitude reference systems for commercial aircraft are very expensive and therefore this proposed heading and attitude reference system is more cost effective for small aircraft with compromises being the sensor's sensitivity to position on the aircraft sensitivity to EMI and a 0.14° error in heading.

With consideration of interference of radio signals for navigation, Bastide et al (2004) supported by Gao (2007) show how modern and future systems are now conflicting with the legacy navigation systems previously described. GPS L5 and Galileo E5 signals encroach on and have the capability to interfere with the

TACAN and DME legacy systems which are still in use today. This is not the only issue with modern aircraft navigation as a more common concern is the constantly changing Electromagnetic environment that aircraft flight systems are exposed to (Ely, 2005) such as mobile phones and in flight communication services that are being introduced. Wireless devices are now more common place and Carter (2012) states that the challenges to EMC engineers is to develop test procedures capable of handling modern avionics in this environment, which is not cost or time prohibitive as although Kuriger et al (2003) showed that CDMA, GSM and other mobile phone systems transmitting spuriously from the fuselage of an aircraft did not affect the instruments they tested, modern phones in 2014 have moved on and Kuriger et al (2003) place a caveat on their conclusion as limited to the avionics that they tested in their study.

3.4 Localisation in Mining

In this section we explore the tracking systems that are available to the mining industry, which is an established industry that has to deal with modern health and safety legislation and requirements. Salvador et al (2011) mention statistics that show that workplaces such as construction sites and steel manufacturing are dangerous working environments due to among other factors, heavy machinery, high heat, explosive areas and fast moving environments. This description fits with Hebblewhite (2009) although he describes mining as a constantly changing environment but the alarming numbers presented by Feng et al (2010) state that 130,000 people a year die from safety related accidents in China alone.

Nutter (2007) discusses the need for a mine tracking system based on renewed interest as a result of an explosion at the Sago mine in 2006. He states that mine tracking systems require each miner to carry an electronic device which along with the established infrastructure, will help to provide individual tracking in a mine. Ke-fei et al (2009) present the different indoor tracking technologies available to the mining industry, describing Radio based systems, ultrasonic, infra-red and even inertial navigation systems; their focus being on an RFID and Inertial Navigation system. In the United States, the Mine Safety and Health Administration (MSHA) have recently established guidelines for the resolution of which miners should be tracked to (MSHA, 2011). Sunderman and Waynert (2012) have mentioned these resolutions as within 61 meters in working sections and to within 610 meters in escapeways and, with these guidelines, it is possible to evaluate technologies that can meet these criteria.

Kennedy and Foster (2006) have researched into the propagation characteristics and performance of wireless networks with mesh capabilities in order to increase mine safety by designing a communications network that is rapidly deployable, flexible and scalable for use in mines. Their research has done so with a platform based on the 2.4GHz IEEE 802.15.4 (IEEE 802.15.4, 2011) standard, which is the standard for wireless personal area networks, including ZigBee technology. The use of ZigBee to locate miners is proposed by Huang et al (2010) and is supported by Li-min et al (2008), Yang and Huang (2007) and Wei and Li-Li (2009) show the many advantages of mesh networking for use within mines. Huang et al (2010) propose a tracking system that utilises an Ethernet backbone for data transmission to the surface and several ZigBee sub networks inside the mine tunnels for localisation. It is proposed that each miner wears a helmet with a ZigBee enabled sensor device and the individual miner is located periodically by position calculation based on a received signal strength (RSSI) algorithm; the information is then sent to the surface over the Ethernet network (Huang et al, 2010). The use of ZigBee enabled helmets is supported by Qiang et al (2009) who present a solution for a ZigBee based helmet for use in wireless positioning mine systems which incorporates humidity, temperature and gas sensors into the helmet. The advantages of monitoring sensors wirelessly are detailed by Wang et al (2007), where localisation of miners and ease of deployment are among the main factors for easy deployment of the wireless sensor network. They too introduce a mesh network based system for use in mining.

Hind (1994) describes the use of RFID systems used in mining to detect the presence of personnel on conveyor systems that are not designed for transportation of personnel. The concerns with deployment of RFID systems in the hazardous environment of a mine is detailed by Hind (1994), stating that the lack of certified reading equipment impacted the widespread deployment of RFID in the early days of mining. Tian and Zhu (2011) present a modern implementation of an RFID positioning system for use in mining that would work well with existing mine communications systems. The principle of their implementation is a distribution of readers throughout the mine with tags attached to the subject to be tracked. Upon reading of the tag, a surface located computer with management software will provide the tracking capabilities for the subjects. An alternative approach to RFID tracking is presented by Ni et al (2011) who show that a distribution of reference tags with known locations deployed in the field will provide a reference point. When tracking tags are present, the RFID reader picks up the reference tags in the vicinity of the reader as well as the tracking tags. With the system presented by Ni et al (2011), analysis of the received signal strength allows post processing to determine where the tracking tag is in relation to the reference tag and hence the location of the tracking tag can be determined with good accuracy and fewer RFID readers than in the system that Tian and Zhu (2011) presented.

The principles and the technology presented by Tian and Zhu (2011) and Ni et al (2011) can be considered effective; however more modern systems such as the ZigBee systems discussed by many other industry experts such as Huang et al (2010) have the capability of providing more benefits to the mining industries such as sensor monitoring and the advantages of mesh networking. Mishra et al (2012) have suggested that the lack of emergence of RFID systems in mines is due to the restrictions placed on systems that are certified for use in the mining industry. Mishra et al (2012) present a new technology, RuBee (IEEE Std 1902.1-2009), which they believe to be beneficial for use in the mining industry. The capabilities of RuBee as described by Mishra et al (2012) suggest that the low frequencies used can ensure that personnel and equipment within mines can be detected through rock and even steel as the magnetic properties of the signal can be enhanced and environmental detuning can be compensated for. The advantages of RuBee such as the capability to read through metal, rocks and liquids, long battery life and large read ranges (Mishra et al, 2012) mean that RuBee has a future use in the mining industry.

3.5 People Tracking and Personal Location

RFID is a popular technology in many tracking applications and this is clear from earlier tracking applications in this chapter. This popularity continues into a different section of tracking as Sangwan et al (2005) present the potential to track patients and their charts in a medical environment with the target of improving efficiency and avoiding errors. The further advantages for such a system is real time data which is beneficial to doctors and nursing staff for the correct administration of medication (Sangwan et al, 2005) as well as applications for tracking usage of medical equipment and outpatient compliance with treatment plans after discharge (Wicks et al, 2006).

Other technologies used in people location systems such as presented by Gaukel (2000), utilise GPS and a mobile phone to provide location. Such systems can be used to track prison inmates but, as with all GPS systems that have been discussed in some detail, the ability to track indoors is not a strength of a GPS based system. Alternative systems can be radio based such as that described by Richards et al (2002), who describe a pulse radio based system, which alarms when an inmate moves out of a specified area.

Koshima and Hoshen (2000) discuss six technologies that a personal location system can use. They involve the use of GPS and radio based technologies that implement fingerprinting, signal direction, Time Difference of Arrival (TDOA) and the use of signal strength information. These technologies have in several forms been described in this chapter and in Chapter 2, but it is their exploitation in personal location that is of interest here. Early research into personal location, such as presented by Hewat and Cheek (1993), describe the benefits of GPS tracking for use in lone worker systems. Lone worker systems can help to reduce staffing levels by decreasing the number of workers whilst still maintaining the safety standards required by law. Brennan (2010) provides an insight into the hazards of lone workers with a worst possible example given of the death of a health support worker in 2006. Needless to say, such events are a threat to carer and nursing staff and the use of lone worker systems exist within the NHS as indicated in a case study by Curran and Pluta (2008).

A final consideration for Personal Location is presented by Michael et al., (2006) in their paper on the ethics of human centric tracking. They raise many questions relating to the accuracy of tracking data, consent for tracking rented vehicles and more interestingly, the ethics of use of tracking data by the Police in the event of suspected illegal activity. Several cases in the United States have seen the placement of tracking devices on vehicles and defended such activities in court, while there are services available for parents to track their children and employers to monitor their employees. The ethical discussions on the use of the data and accuracy of it continue and are much debated (Michael et al.,2006).

3.6 Robot Tracking

Robots are the ultimate indication of human technological progress with the drive towards replicating human activities. There are many applications for robots in society today but some of the best and most common applications are mentioned by Leow and Shang (2010) in their paper on Mobile Robot Tracking. Applications such as search and rescue and military surveillance are among those mentioned by Leow and Shang (2010); however their description of the tracking problem is simple in that it requires accurate location of the moving target. Early robot navigation has seen the use of rotating laser scanners with barcodes at known locations and retro-reflective strips in combination with ceiling lights that act as beacons detected by infrared and vision systems (Leonard and Durrant-White, 1991). Leonard and Durrant-White’s work on Robot Localization mostly focussed on the use of Sonar for location determination while Kuang and Morris (1999) present the use of Ultrasonic Doppler as a better alternative to Time of Flight Ultrasonic systems. Their research demonstrates the advantages of Doppler over Time of Flight as an improvement over sample resolution, accuracy and tracking speed (Kuang and Morris, 1999).

Recently, robots have been navigating outdoors in unknown environments with the use of vision systems as presented by Ravari et al (2009). Much research has been performed in this field and, using a fuzzy logic system, Ravari et al (2009) have been able to direct a robot towards safe areas using their algorithm for outdoor robot navigation. Similarly, other visual navigation systems as researched by Meng and Kak (1993) and Tangruamsub et al (2009) use neural networks to interpret visual information and assist in the visual navigation of robots. The advantage of vision based systems is the ability to process an image rather than sensor data, which is likely to have accumulated noise. An example of this would be an odometer reading that is sensitive to the path surface and the distance travelled (Tangruamsub et al, 2009). As such, vision systems can give advantages in this aspect.

Another vision based tracking system with a different perspective is presented by Kobilarov et al (2006) and similarly by Dai et al (2008). This research uses cameras and laser direction finders in an effort to track humans. Kobilarov et al (2006) present two methods; the first being a camera based system, which was only proven to perform well in controlled environments; however their second and most researched method used a laser scanner to detect the presence of humans and the camera is used in conjunction with the laser scanner. Dai et al (2008) also use a laser range finder in conjunction with a camera and the person is identified by correlating a target person model against the images captured by the board camera, while the laser range finder detects the presence of people in order to work in conjunction with the camera. With this human tracking aspect, Aggarwal and Cai (1997) present early work performed with vision systems to track human motion. This work, although not entirely location related, presents efforts to track the motion of a human with interests in surveillance, athletic performance and man-machine interfaces. In their work, they describe strategies which follow a general framework for feature extraction, feature matching and further processing and with this framework, they describe two separate methodologies; a priori based shape model and a model based system, both which fit with this framework.

The lighter side of robotics is presented by Thrun et al (1999) who present Minerva; a robotic tour guide, which was deployed in a Smithsonian museum with the aim of entertaining and educating visitors. The environment that Minerva operated within is a very dynamic and fast changing environment and therefore multiple sensors were incorporated on the robot. Laser range finders, sonar and cameras were all used on Minerva, with the cameras and lasers used to provide localisation as well. Intelligently, Minerva used ceiling mosaics detected by the on board ceiling cameras to provide localisation and when cross referenced against the on board maps, location estimation was possible (Thrun et al, 1999). On a similar theme, Helpmate is presented by Engelberger (1993) as a robotic healthcare assistant to provide transportation services and couriering of items such as medical records within the hospital environment. Within this very early work, Helpmate navigated by using a combination of dead reckoning, ultrasound for obstacle detection, vision systems based on cameras and infrared sensors detecting passive strips on the ceilings.

In 2002, the DARPA Grand Challenge was announced which required entrants to have a land vehicle capable of navigating autonomously from Los Angeles to Las Vegas without human input beyond the start of the race (Behringer et al, 2004). The teams were provided with waypoints before the race which were entered into the entrant's navigation computers and following that, no human input was allowed. The main stipulation for the DARPA Grand Challenge was that no technologies developed with United States Government funding were allowed to be used (Behringer et al, 2005).

The RASCAL vehicle presented by Behringer et al (2004) for the 2004 and 2005 DARPA Grand Challenge incorporated the use of laser sensors to detect obstacles as well as vision systems for this purpose as well as lane limitations for the vehicle (Behringer et al, 2005). For localisation and position estimation, GPS and inertial navigation were used to navigate the vehicle between waypoints (Behringer et al, 2004). Other entrants support the RASCAL vehicle's navigation architecture in the use of vision and laser based navigation systems such as Redmill et al (2006) and Broggi et al (2006), which is different to the approach taken by Bacha et al (2004), where their architecture had the capabilities to use laser, radar and vision based systems but, in their 2004 DARPA attempt, the vehicle was only operated with laser range finders. The variation in navigation approach to this challenge is impressive as in 2005, the first winner of the DARPA Grand Challenge was a robot called 'Stanley' from

Stanford University (Thrun, 2006) whose achievements saw the 132 mile off road autonomous challenge achieve a winning place with an average speed of 19.2 miles per hour (Hoffmann et al, 2007) to win the 2 million dollar DARPA Grand Challenge first prize as evidence of the achievements in robot navigation.

4. Wi-Fi as a tracking technology

The concept of indoor tracking has been introduced and how it may be beneficial to the robust tracking solution sought by the CIT industry. Chapter 2 introduces and evaluates the different technologies available to build a tracking system for the CIT industry but it intentionally does not describe one particular radio technology, which this author believes can provide a promising solution to the challenges of a CIT tracking system.

This aforementioned radio based technology uses the widespread availability of IEEE 802.11 radio systems, better known as Wi-Fi. Wi-Fi mainly utilises the 2.4GHz ISM band but variants of the 802.11 standards, in particular the 802.11a standard, uses the 5GHz frequency band. 802.11b & g use the established and popular 2.4GHz band where 802.11n has the capability of using both 2.4GHz and 5GHz (IEEE 802.11-2007 Amendments 1, 2 & 4).

Wi-Fi is a popular domestic communication technology and Zandbergen (2009) describes it as a now popular technology for positioning. This chapter will discuss the many advantages that Wi-Fi positioning has to offer and how it can fit in to the CIT industry.

4.1 Localisation Using Wi-Fi

The use of proprietary solutions to implement indoor tracking systems has previously been discussed. This extends to the use of proprietary Wi-Fi systems to provide location information either indoors or outdoors. Pandey and Agrawal (2006) stipulate that measurement of distance dependent parameters of a radio link should be measured to determine the distance from the transmitter. These parameters are Signal Strength, Time of Arrival and Connectivity (Pandey and Agrawal, 2006). Time of Arrival (ToA), which has already been discussed in Chapter 2, adds significant cost to the hardware (Pandey and Agrawal, 2006). Using the ToA method within CIT serves as an example where it cannot be used in a Wi-Fi based system due to costs and the associated hardware complexity.

Turner et al (2011) utilise received signal strength and trilateration to estimate location of a client based on the known location of 4 Wi-Fi access points in their experimental setup. This use of proprietary access points is very popular in research (Turner et al, 2011), Serrano, Canas, Matell´an, and Rodero (2004)) but it relies heavily on knowing the location of the transmitting stations. This particular issue is what makes proprietary Wi-Fi access points desirable in terms of location accuracy but very undesirable when it comes to cost.

Proprietary access points infer that there is control over the availability and use of the access points. Control in the case of the CIT industry means upfront costs and maintenance of any proprietary networks. Discussions with Nick

Tripp, Engineering Manager at Spinnaker International Ltd, stated that the use of proprietary networks would only be justified with an innovative tracking solution that can convince the CIT industry that it is a solution that can fulfil many of its tracking or security requirements. This in turn would then justify the development program and associated development and deployment costs.

The alternative to proprietary access points is to use publically available Wi-Fi information. Such information is available via the service announcement beacon transmitted from Wi-Fi access points (AP's). Through their work in autonomous creation of radio maps using smart phones, Koo and Cha (2012) classify Wi-Fi positioning systems into two categories: RF Fingerprint-based and AP Position based. The most accurate localisation method is to use RF fingerprinting which splits a signal map into grids. Each grid can then be cross referenced with a location and hence the location of a Wi-Fi enabled device can be determined based on the signal at the Wi-Fi receiver (Koo & Cha, 2012). The alternative to RF fingerprinting is AP based positioning. Here, Koo & Cha (2012) mention that the advantages of this approach are that the look-up database required for AP based Wi-Fi positioning is smaller than the RF fingerprinting approach. AP positioning as described by Koo & Cha (2012) uses the single and sometimes estimated location of a Wi-Fi access point to allow a Wi-Fi enabled device to determine its location from the pre-existing database. This method is however less accurate than the RF fingerprinting method described (Koo & Cha, 2012). Such systems exist as commercial services and are discussed in 4.2, and the use of these commercial systems allows positioning on a metropolitan scale using Wi-Fi as the technology as Zandbergen (2009) has demonstrated.

4.2 Available Commercial Wi-Fi Positioning Services

Zandbergen (2009) shows that here are four Wi-Fi positioning services available; these are from the following companies: Skyhook Wireless, PlaceEngine, WeFi and Navizon. PlaceEngine services cover Japan (PlaceEngine Coverage Area, 2011), which serves little purpose for the UK CIT industry.

All these systems maintain a database containing locations and Medium Access Control (MAC) addresses of each Wi-Fi access point at that location (Tippenhauer et al, 2009). The MAC address of a Wi-Fi device is available from the Wi-Fi service beacon without having to establish a connection to the Access Point. Storing MAC addresses and geographic locations is what provides services like Skyhook Wireless with the capability of providing a Metropolitan wide solution to positioning, using freely accessible Wi-Fi signals. To access this database, a remote device equipped with a Wi-Fi transceiver listens for Wi-Fi beacons and records the MAC addresses from these beacons. The remote device then sends the MAC addresses to the Wi-Fi positioning service provider and is returned with position information if a valid MAC address matches one on the provider’s database.

Between all the companies mentioned by Zandbergen (2009) that provide Wi-Fi positioning services, Skyhook Wireless is the only company that maintains and populates their own database using a fleet of data collectors. Navizon state that they use crowdsourcing to populate their database (Navizon Features, 2012) which can be at a disadvantage to the solution provided by Skyhook Wireless's actively maintained database, as Navizon's information can be sporadic due to its reliance on user contributions and the inevitable security implications associated with the reliability of the user contributions.

The advantages of using a Wi-Fi location system are that indoor positioning can be implemented and evidence by Zandbergen (2009) shows that Skyhook boast an accuracy of 20m outdoors and indoors using their Wi-Fi system. This cannot be verified in 2013 because Skyhook have revised their accuracy figures to reflect a combined AGPS, Wi-Fi and cell tower positioning service. This is claimed to be accurate to within 10-20m 99.8% of the time (Skyhook Location Performance, 2013).

Disadvantages of using Skyhook's Wi-Fi positioning system are well documented by Tippenhauer et al (2009). Tippenhauer et al (2009) proved that it is possible for an attacker to prevent localisation of the Wi-Fi device or to convince the device that it is at a location different to its actual location. This was done by impersonating Wi-Fi access points and feeding the remote device a fake MAC address. This MAC address would then be looked up by on Skyhook's database and provide position information that is in conflict with the actual location of the remote device.

The system that is evaluated in section 4.3 below is Skyhook's Wi-Fi Positioning System which has been in use by Apple's iPhone since 2008 and provides one of three levels of location information for the iPhone (Zandbergen, 2009) and Apple products such as the iPod (Tippenhauer et al, 2009) and the iPad. As a result, Skyhook's Wi-Fi positioning system is well established and proven commercially.

4.3 Skyhook tracking evaluation

Figures 4.1 and 4.2 show the results of a brief experiment that was performed to evaluate the Skyhook Wireless service. Wi-Fi signals were scanned for and the MAC addresses were extracted from the Wi-Fi broadcast beacons. This was performed at a fixed number of locations as shown by Figure 4.1 below. Some of the MAC addresses are shown on the plot and due to overlapping of the Wi-Fi signals because of the proximity of the physical scanned locations, some of the Wi-Fi beacons were observed in more than one of the physical locations.

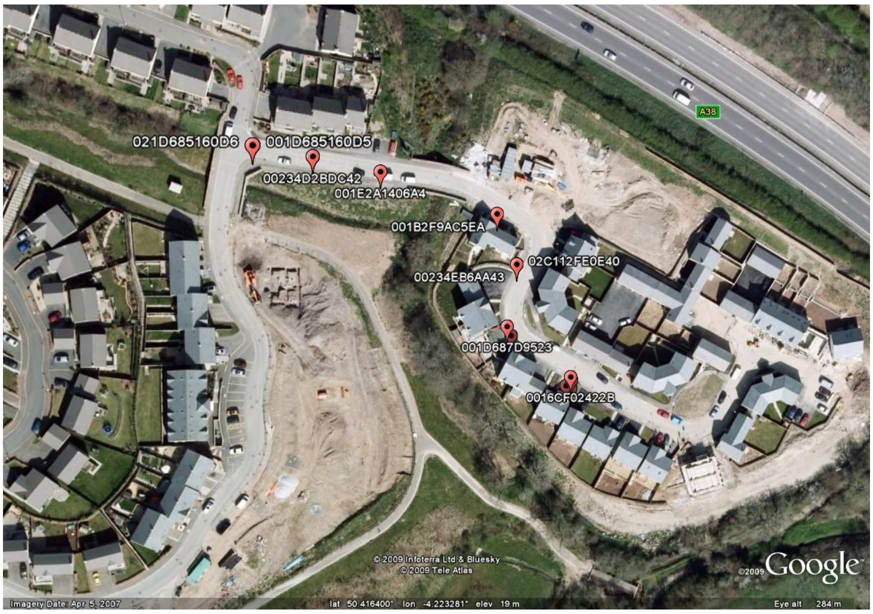
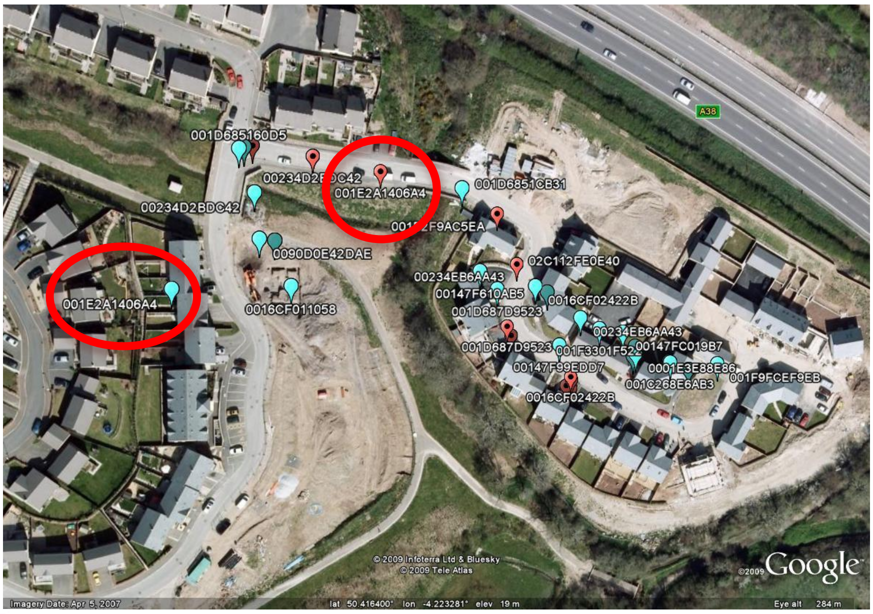


Figure 4.1: Wi-Fi MAC addresses at multiple points of scan.

The scanned MAC addresses were then fed into Skyhook's database using a script. The script operated by modifying the MAC address of the computer's wireless LAN card to the MAC address' that were manually collected. Skyhook's standard SDK then allowed the Skyhook database to return any corresponding location information associated with that MAC address. The location information returned from Skyhook's location database is shown in Figure 4.2. The interrogated information shown by the blue markers is overlaid with the original scanned data shown by the red markers. The interrogated locations plotted on the image are more than in Figure 4.1 for reasons explained previously.

With reference to Figure 4.2, the MAC address '001E2A1406A4' circled was scanned in a location that differs to the Skyhook result. The distance between the two locations is approximately 50m, which raises two questions; is the location information from Skyhook correct and was fingerprinting used by Skyhook with this result? The distance between the two locations would yield a very low RSSI if the transmitter was exactly where Skyhook indicates on its geolocation data. It is suspected that in this instance, RSSI was not used to calculate this location and fingerprinting was not employed. This is supported in some instances by investigations by Zandbergen (2009), where he has noted that some Wi-Fi positions appear “snapped” to the road, indicating the fingerprinting was not reliable in those instances.



Skyhook retrieved location   Wi-Fi scanned location

Figure 4.2: Wi-Fi positions overlaid with the scanned locations of the MAC addresses.

The results of this brief experiment show that it is possible to use Wi-Fi as a method of geolocation and it has highlighted the risks associated with this practice, as we were able to spoof the MAC addresses of all the access points that were collected. We have also noted that the information retrieved from Skyhook's database may not always utilise advanced techniques such as fingerprinting to determine the location stored in Skyhook's database.

4.4 Spoofing and methods of countering

It is beyond the scope of this thesis to investigate the different methods of spoofing a Wi-Fi access point, but Tippenhauer et al (2009) have demonstrated various methods of impersonating a Wi-Fi access point. This has a direct effect on the reliability of information from the Skyhook location service. The Skyhook location service is reliant on reliable database information and no malicious attacks such as spoofing or jamming. This makes a Wi-Fi tracking system for CIT very vulnerable to a Wi-Fi attack which impacts the reliability and accuracy of the tracking solution. As a result, methods of overcoming these weaknesses must be considered and are discussed below.

The first way to decrease the vulnerability of any Wi-Fi access points used by a Wi-Fi tracking system designed for CIT is to use the existing encryption of 802.11 systems such as WEP or WPA2. The use of 802.11 encryption ensures a proprietary access point which means that authentication will also need to take place. This means there will be an increased time to first fix with these proprietary access points and all the disadvantages of proprietary access points previously discussed. Proprietary access points also guarantee that coverage will no longer be widespread enough to provide a good tracking system and Skyhook location services cannot be used.

Another way of decreasing the vulnerability is to run a parallel system to Wi-Fi positioning. By using commercially available Wi-Fi positioning services such as those provided by Skyhook Wireless, a parallel system such as GSM positioning can be used to provide a degree of confidence in the location returned by the Wi-Fi positioning system. For example, if a returned Wi-Fi position is more than 400m from the base station which is serving the tracker, then the Wi-Fi location is likely to be unreliable.

Other parallel systems, such as GPS based systems, can be used in more intelligent ways. For example, if the last fix was 60 seconds old and the latest Wi-Fi position was within a nominal distance from the last fix, the Wi-Fi location data can be considered valid. Using these parallel systems, a scoring system for degrees of confidence can be implemented. The factors affecting the confidence score are time of the last GPS fix and the distance from the serving base station. This means that the Wi-Fi location can be fed to the individual tracking the CIT box accompanied by a degree of confidence factor calculated using the above methods.

5. 2.4GHz Wi-Fi Signal Characteristic Research

With Chapter 4 investigating the use of 2.4GHz Wi-Fi as a tracking technology, this chapter investigates characteristics of the 2.4GHz radio spectrum using the 2.4GHz Wi-Fi technology as its base. The purpose is to investigate the limits of 2.4GHz signals to help determine how robust a Wi-Fi tracking solution could be for the CIT industry. The presented research investigates and starts to present the CIT box into the research on:

- The physical effects of the 2.4GHz Wi-Fi signals within an indoor environment.
- The physical effects of the 2.4GHz Wi-Fi signals in an outdoor environment.
- The effects of 2.4GHz constant wave interference on the Wi-Fi signals.
- The effects of different materials on the performance of 2.4GHz Wi-Fi signals.
- The effects of vehicle types on the received signal strength of 2.4GHz Wi-Fi signals.
- The feasibility and effects of receiving 2.4GHz Wi-Fi signals from within a moving vehicle.

5.1. Evaluation Methods & Experimental Setups

The testing methods described below utilise a commercially available 2.4GHz 802.11b/g wireless access point as the transmitting source with a combination of 3 different antennas attached to the transmitter in some tests. When evaluating 2.4GHz interference, two different devices were used to generate the interfering signals.

5.1.1. Indoor Signal Characteristic Evaluation

The objective of this research is to evaluate the performance characteristics of Wi-Fi in an indoor scenario, which will assess the indoor broadcast range of the signal and the effect of obstacles on Received Signal Strength (RSS). To investigate the performance of 2.4GHz Wi-Fi in an indoor environment, a typical mezzanine office was selected to perform this evaluation. This environment was made up of desks, partitions and other smaller partitioned offices.

A 2.4GHz Edimax branded access point was installed at one side of the office with three different antennas available for testing. These antennas were:

A. Standard Antenna provided with the access point (AP)

B. 8dBi Omni-Directional Antenna

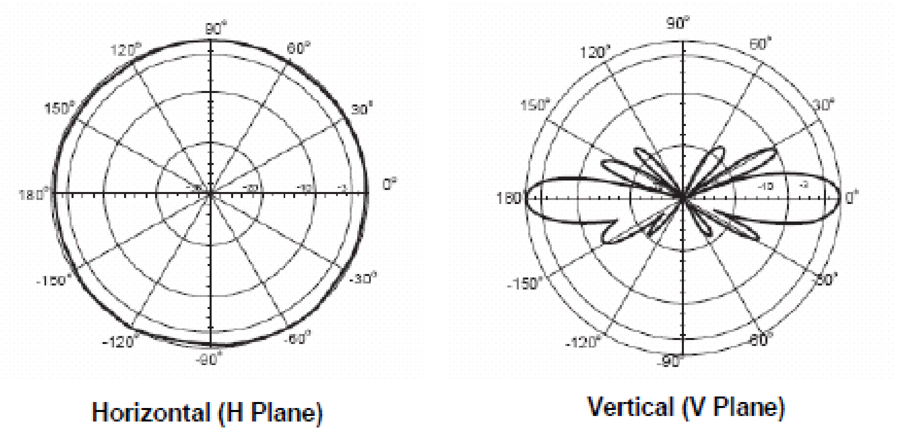


Figure 5.1: 8dBi Omni-Directional antenna propagation pattern

C. 14dBi Directional Antenna

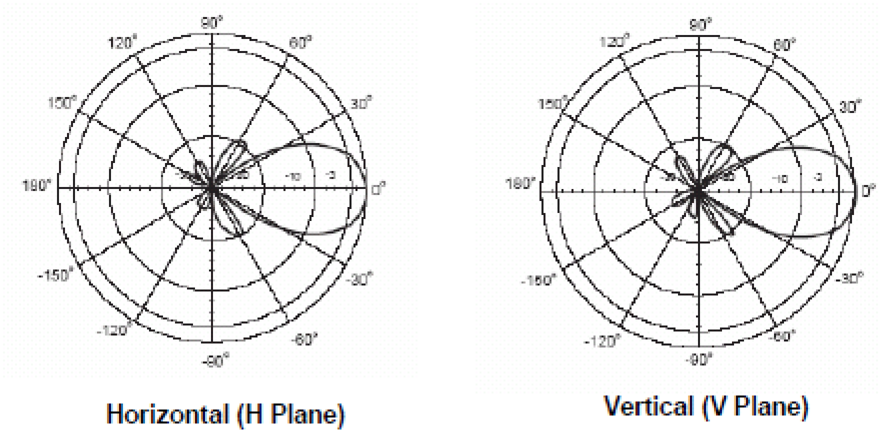


Figure 5.2: 14dBi Directional antenna propagation pattern

The purpose of these different antennas was to evaluate if different antenna gains affect the received signal strength in this indoor environment. The 8dBi omni-directional antenna provides the capability of eliminating dead spots in the signal, whilst providing an omni-directional radiation pattern. The 14dBi directional antenna gives a different radiation pattern altogether by providing a high gain 60° beam width, which focusses the radiating power from the wireless access point.

Using a laptop equipped with a Wi-Fi receiving USB dongle, 25 locations were sampled throughout the office environment. Figure 5.3 below shows the layout of the office environment where the tests were performed.

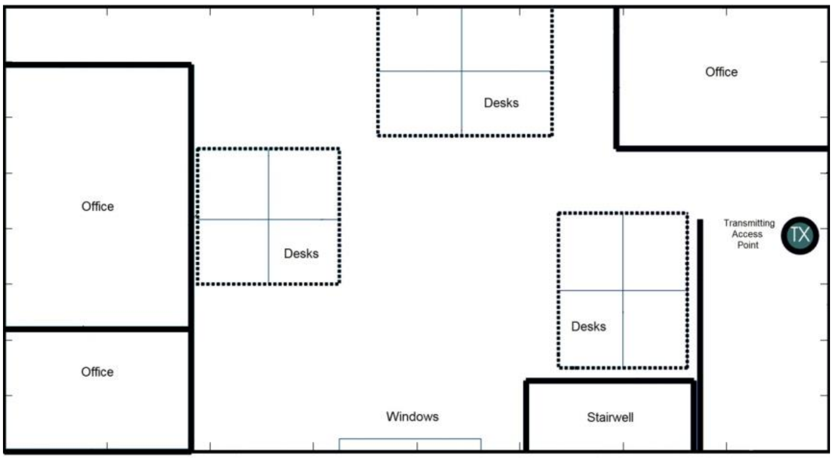


Figure 5.3: Office layout for indoor 2.4GHz Wi-Fi testing

5.1.2. Outdoor Signal Characteristic Evaluation

The objective of this research is to evaluate the performance characteristics of Wi-Fi in an outdoor scenario. There are two studies which detail the outdoor signal characterisation:

A. Assessment of maximum broadcast range with a direct line of sight
B. The effects of moving obstacles on received signal strength

Study A evaluates signal strengths with different antennas and a direct line of site to establish an understanding of the signal attenuation through air and a maximum practical achievable reception radius. The three different antennas used were the standard antenna provided with the access point, an 8dBi omni-directional antenna and a 14dBi directional antenna. These three antennas were the same ones used for evaluating the indoor characteristics and the propagation characteristics of the 8dBi and 14dBi antennas are shown above in Figures 5.1 and 5.2 of section 5.1.1.

The research was achieved by installing a wireless access point in an outdoor location. There were no obstacles placed within 15m of the access point. The received signal strength was measured in 10m increments for the three different antenna types up to a maximum distance from the antenna of 160m. The setup is shown in Figure 5.4.

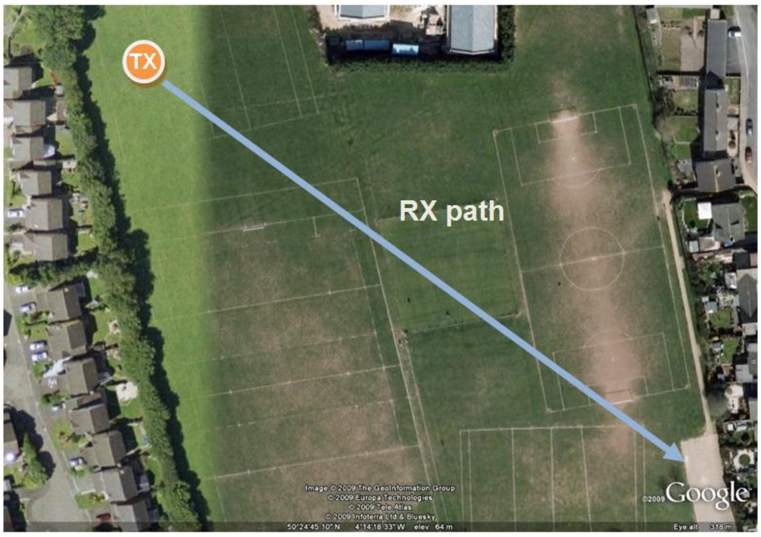


Figure 5.4: Study A outdoor setup

Study B evaluates the effects of moving obstacles on received signal strength outdoors. The objective is to assess how obstacles such as vehicles affect the transmitted signal as they pass in front of it. As with Study A, three different antennas were used to provide an assessment of how antenna directionality and gain affects the signal. The antennas used were those used in Study A; the standard antenna provided with the access point, an 8dBi omni-directional antenna and the 14dBi directional antenna.

The research was performed by installing the access point outdoors with vehicles passing between the transmitter and the receiver. The received signal strength was recorded for 20 minutes at 1 second intervals using a laptop equipped with a wireless dongle. The samples were taken at peak afternoon traffic times with an approximation of 50-55 cars passing between the transmitter and the laptop over the 20 minutes. The evaluation setup is shown in Figure 5.5.

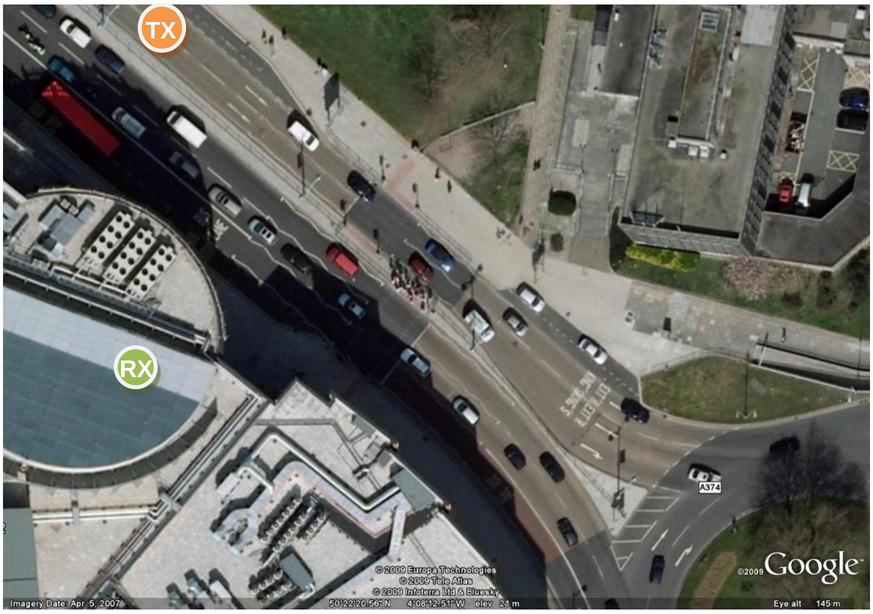

TX
RX
A374
© 2009 Europa Technologies
© 2009 Tele Atlas
© 2009 Infoterra Ltd & Bluesky
©2009 Google
Imagery Date: Apr 5, 2007
50°22'20.56" N 4°08'12.51" W elev 21 m
Eye alt 145 m

Figure 5.5: Study B setup

5.1.3. 2.4GHz Wi-Fi Interference Testing

The objective of this research is to evaluate how other devices on the 2.4GHz frequency band affect the operation of Wi-Fi in that same frequency band. This will provide an understanding as to how a tracking system using Wi-Fi might be affected by a commercially available device using the 2.4GHz frequency band.

The technology used was a 2.4GHz wireless TV sender, which is representative of a 2.4GHz ISM band wireless CCTV camera or wireless TV sender. To evaluate the effects of this device on Wi-Fi signals, two studies were performed.

A. TV sender at a height to simulate a wireless CCTV camera

B. TV sender on ground level by a window to simulate a home TV installation

In both studies, data was gathered in a different manner by carrying a laptop in a simulated cash box. This setup was chosen as a medium to transport the laptop was required and the simulated cash box was the most sensible option as this would yield more realistic results. The receiving antenna was placed on the outside of the cash box and the laptop used a Wi-Fi dongle with an external antenna connection point. The receiving setup was carried along a pre-determined path past the suspected interference point whilst scanning and recording visible access points. A control evaluation with the suspected interference switched off formed the base line signal levels for the access points in the vicinity. Figure 5.6 below shows the pre-determined path that the receiving setup followed.

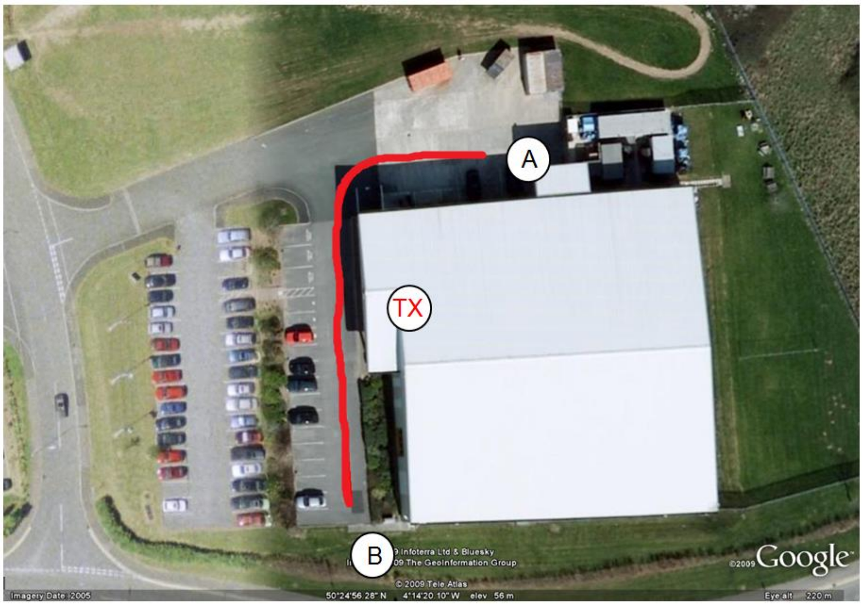


Figure 5.6: Route followed for 2.4GHz interference testing

5.1.4. Effects of Materials on Wi-Fi Received Signal Strength

This research evaluates the performance of 2.4GHz Wi-Fi signals with various obstacles between the transmitter and receiver. The data acquired from this research will provide understanding of the effects of various commonly found materials on 2.4GHz Wi-Fi. This in turn can allow prediction of signal characteristics when a Wi-Fi access point is statically set up in indoor environments surrounded by these materials. This research will also provide understanding of a practical environment where these materials are used. There are two studies associated with this research as described below:

A. Evaluation of received signal strength with a building between the transmitter and receiver

B. Evaluation of 4 obstructive mediums – Glass, Metal, Concrete wall, office partition

Study A uses a transmitting access point in the centre of a metal clad building with film coated windows and signal strength results were measured outside the building. As with other tests, 3 different types of antennae were used to gather 3 sets of results for this study. The antennae used were the same ones used in section 5.1.1; the standard antenna provided with the wireless access point, the 8dBi antenna and the 14dBi antenna. Figures 5.1 and 5.2 of section 5.1.1 can be referred to for the propagation characteristics of these antennas. Data was gathered at 20 locations around the building and repeated three times to complete the study with the three different antennas.

Study B uses an access point set up outdoors in a central location with no surrounding obstacles within 100m. To evaluate the effects of the aforementioned materials, concrete blocks were used for the wall and 6mm aluminium sheet was used as the metal material. A twin sheet glass window was used as the glass divider and the partition was made of MDF wood. For each evaluation, the transmitting access point was placed 1m from the receiving laptop which was equipped with a wireless dongle to record the signal strength. The obstructing media were placed between the transmitter and receiver and 50 samples were taken for each. A control sample with no medium between the transmitter and receiver formed the baseline for comparison.

5.1.5. Detection of Wi-Fi Signals From a Moving Vehicle

This research evaluates the likelihood of detecting a specific Wi-Fi access point from a vehicle, which is moving at speed. By evaluating the received signal strength of the wireless access point in question from a moving vehicle, the research intends to provide an understanding as to whether the signal can be detected from the vehicle and, if so, how this signal strength will vary at different speeds.

This information will help to assess whether a tracking system moving at speed can detect low signal strength static Wi-Fi access points in order to acquire a location. For this testing, the Wi-Fi access point was placed in an open space with a road running perpendicular to the radial field of the antenna. Figure 5.7 below shows the setup graphically.

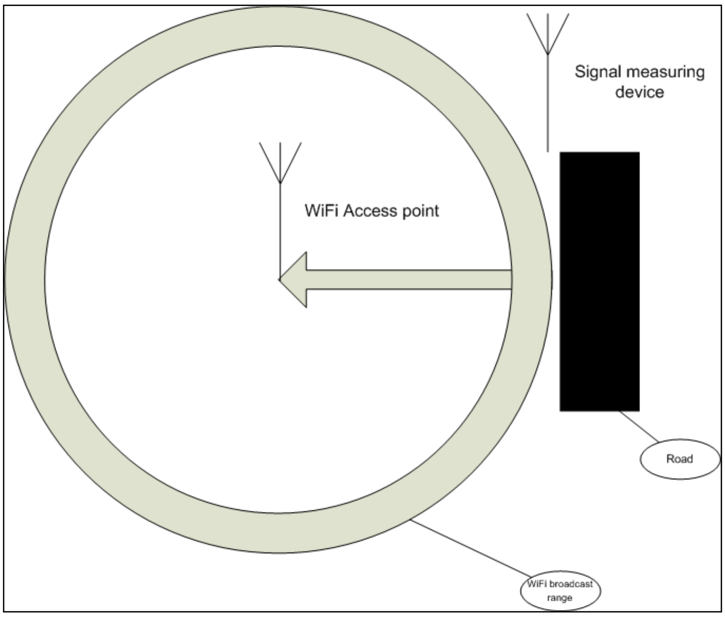


Figure 5.7: Setup for detection of Wi-Fi signals from a moving vehicle

The data was recorded using a laptop equipped with a Wi-Fi dongle, which was situated within a vehicle moving along the road in a manner described by the blue arrow in Figure 5.8. Signal data was gathered with the vehicle moving at speeds of 20, 30, 40 and 50mph. A control evaluation was taken at the side of the road at a distance of 160m from the transmitting access point to provide a baseline for comparison. The sample location for the control evaluation is indicated by the green dot in Figure 5.8 and the location of the transmitter is shown by the orange dot.

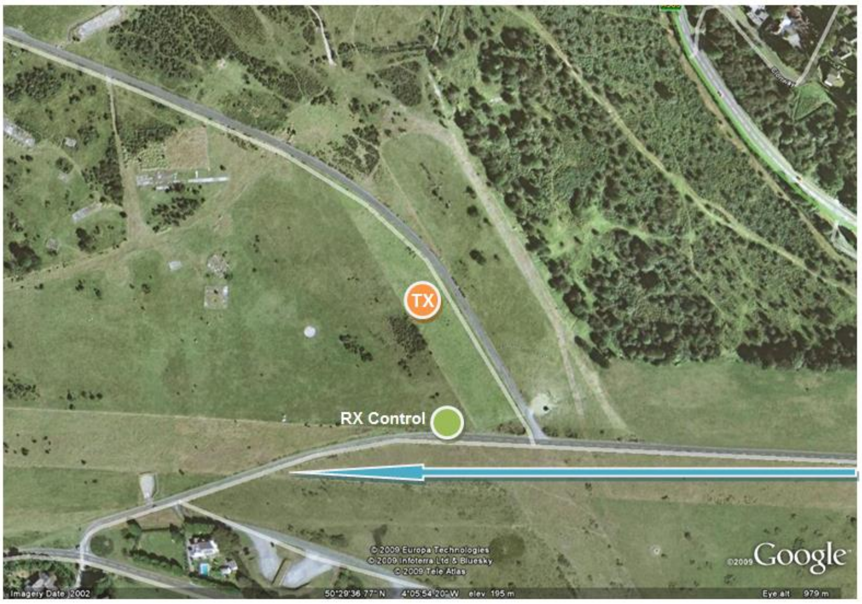

TX
RX Control
© 2009 Europa Technologies
© 2009 Infoterra Ltd & Bluesky
© 2009 Tele Atlas
©2009 Google
Imagery Date 2002
50°29'36.77" N 4°05'54.20" W elev 195 m
Eye alt 979 m

Figure 5.8: Control evaluation location and vehicle route for section 5.1.5

5.1.6. Evaluation of Wi-Fi Received Signal Strengths From Within Vehicles

This research provides an understanding of how different vehicle types can affect the received signal strength of a Wi-Fi access point. The purpose of this is to understand how a 2.4GHz Wi-Fi tracking system will perform when stolen and placed in the boot of a vehicle. By evaluating the vehicle types, this knowledge can help to predict how the tracking performance will be affected and could potentially help determine what type of vehicle the tracking system is located within when tracking is active.

The hardware setup for this evaluation was similar to that in 5.1.3 where a laptop was placed in a cash security box. For this evaluation, two 2.4GHz antennas were installed on the left and right hand exterior of the cash security box in areas as shown in Figure 5.9 below. Data was sampled using both the left and right hand antennas and was recorded separately.

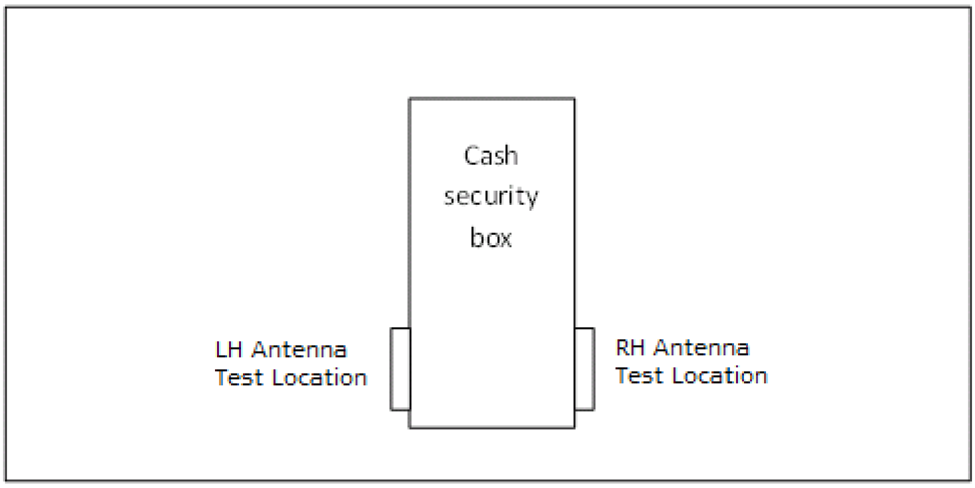


Figure 5.9: Cash security box antenna setup

The physical setup for the data collection is illustrated by Figure 5.10. The transmitting access point was placed on the upper floor near a window. It is worth mentioning that the window was covered with a film to attenuate the light and as a result, this may affect the transmitter's range. This is acceptable as for the purposes of this evaluation no absolute range is required, just relative signal levels.

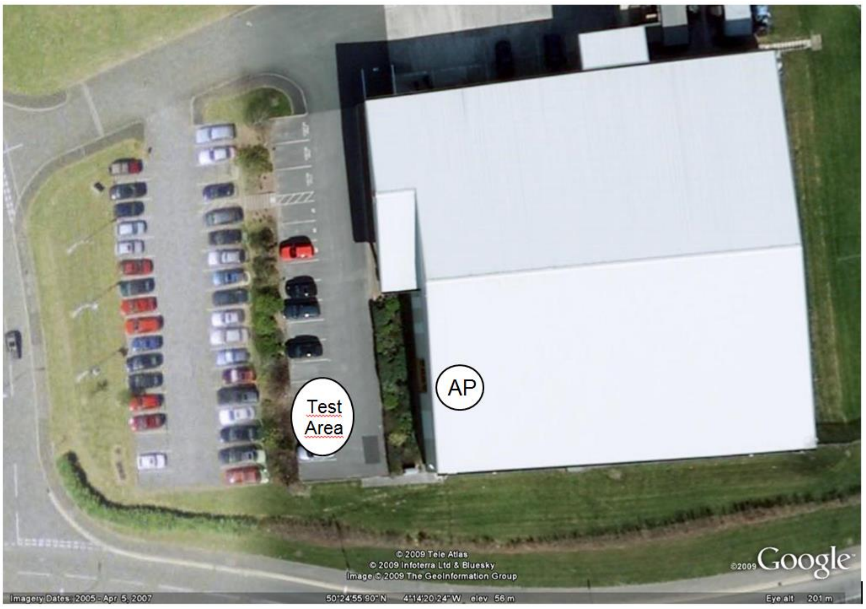

Test
Area
AP
© 2009 Tele Atlas
© 2009 Infoterra Ltd & Bluesky
Image © 2009 The GeoInformation Group
©2009 Google
Imagery Dates: 2005 - Apr 5, 2007
50°24'55.90" N
4°14'20.24" W
elev 56 m
Eye alt 201 m

Figure 5.10: Setup for 5.1.6 data collection

For each evaluation, the cash security box with its acquisition hardware was placed in the boot of each vehicle with the front of the cash security box facing the rear of the vehicle. The rear of the vehicles always faced towards the building. Samples were taken across both Wi-Fi antennas for a 60 second period. Control readings were taken from the left and right antennas with the cash security box in the same orientation as when in the vehicle, but with no vehicle present. Table 5.1 shows the vehicle types used for these tests.

Type	**Make**	**Model**	**Year**
Saloon	Volvo	T5	1994
Hatchback	Honda	Civic 5dr	1998
Small Hatchback	Suzuki	Swift	1999
Estate	Audi	A4	2008
4x4	Land Rover	Freelander I (TD4)	2006
Small Van	Ford	Transit Connect	2005
Large Van	Ford	Transit	2008

Table 5.1: Different vehicle types used for 4.1.6 research

5.2. Evaluation of Results

As the experiment setup and testing has been described in 5.1, the results of each experiment are presented below. These results will provide an understanding of the characteristics of 2.4GHz Wi-Fi and the performance of portable 2.4GHz Wi-Fi devices.

5.2.1. Indoor Signal Characteristics

Received signal strength results were recorded by taking ten samples for each of the 25 locations within the indoor office environment. The set of 10 samples were averaged and the results for each of the 25 locations were plotted using a contour plot generated in Matlab. The contour plot was overlaid with the office layout to produce a signal map show the varying signal strength in dBm within the office environment. Three signal maps were generated for each of the 3 antenna types. The resulting signal maps have the same scaling and are shown in Figures 5.11-5.13 below.

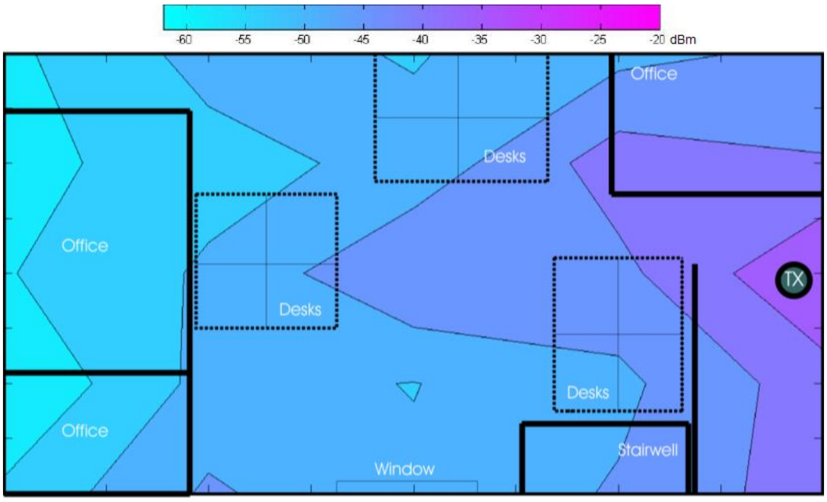


Figure 5.11: Standard Antenna Signal Map

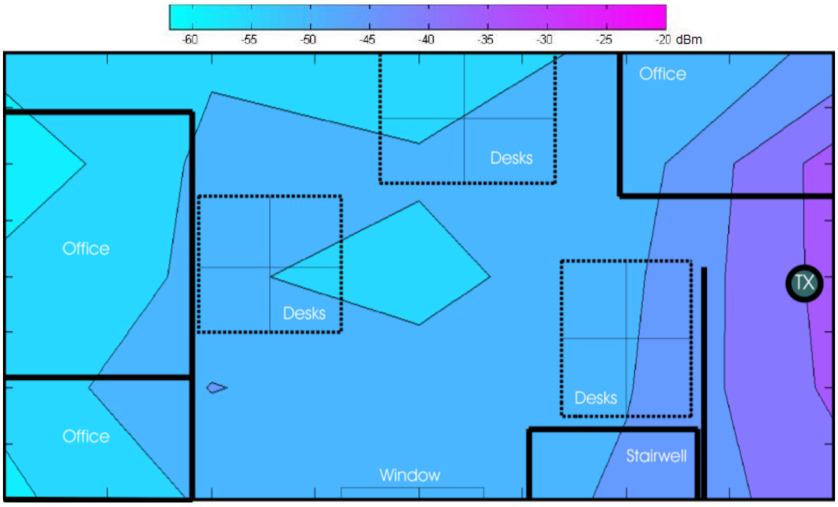


Figure 5.12: 8dBi Antenna Signal Map

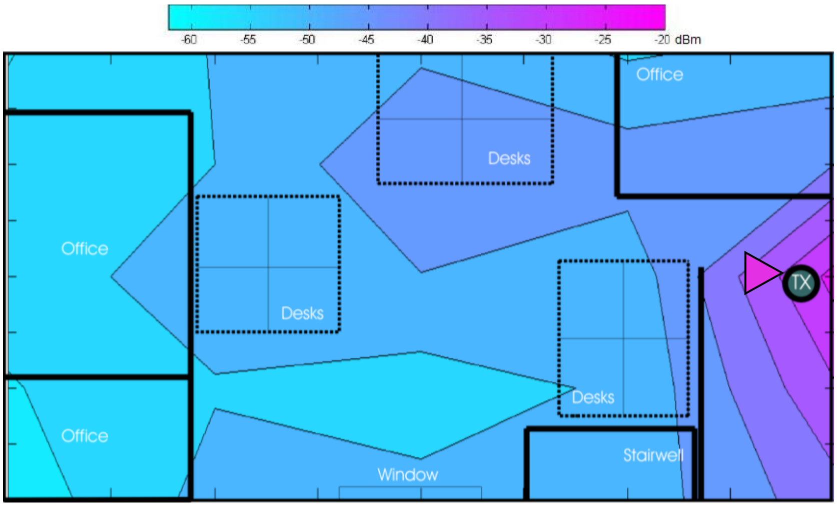


Figure 5.13: 14dBi Antenna Signal Map

Figure 5.14 below provides a graphical view of the averaged received signal strengths for each of the three antennas. The averaged received signal strength samples from each of the 25 locations were plotted on a box plot for each antenna type to provide a comparative view from antenna to antenna. This is useful to determine if using a high gain antenna within an indoor environment provides a significant advantage over lower gain omni-directional antennas like the standard antenna used in this testing.

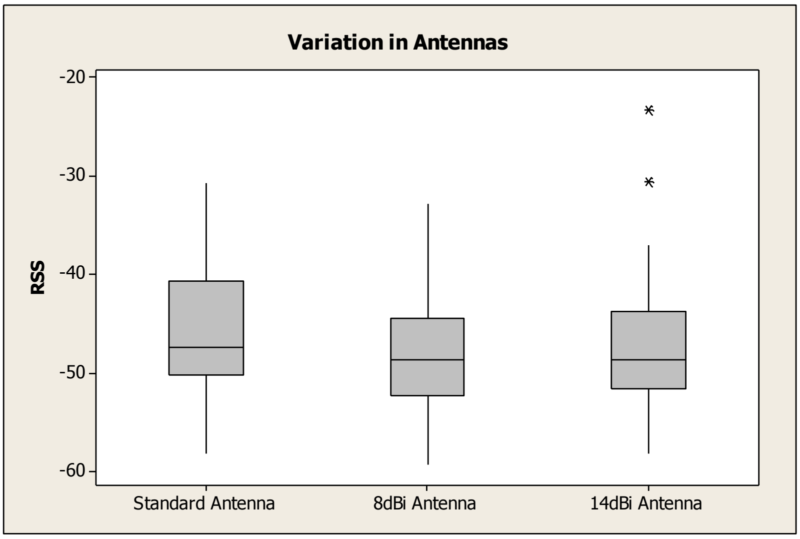


Figure 5.14: Variation in RSS (in dBm) between each of the antennas

Figures 5.15-5.17 use box plots to graphically demonstrate the variation in the 10 samples acquired across the 25 locations in the indoor environment. This is repeated for the 3 different types of antenna to provide a comparative view between the antennas but it also highlights which areas of the indoor environment provide the greatest variation in received signal strength.

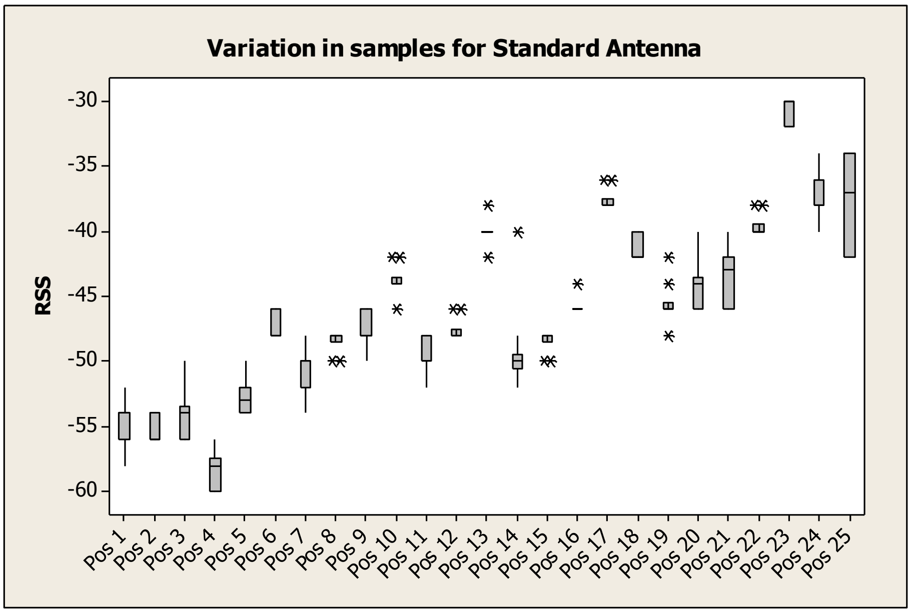


Figure 5.15: Variation in recorded signal strength (dBm) for the Standard Antenna

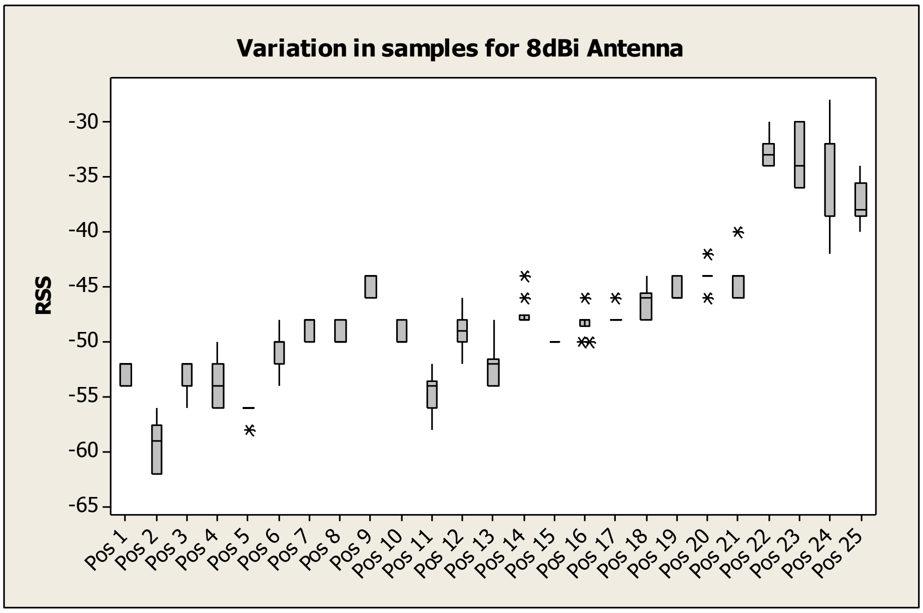


Figure 5.16: Variation in recorded signal strength (dBm) for the 8dBi Antenna

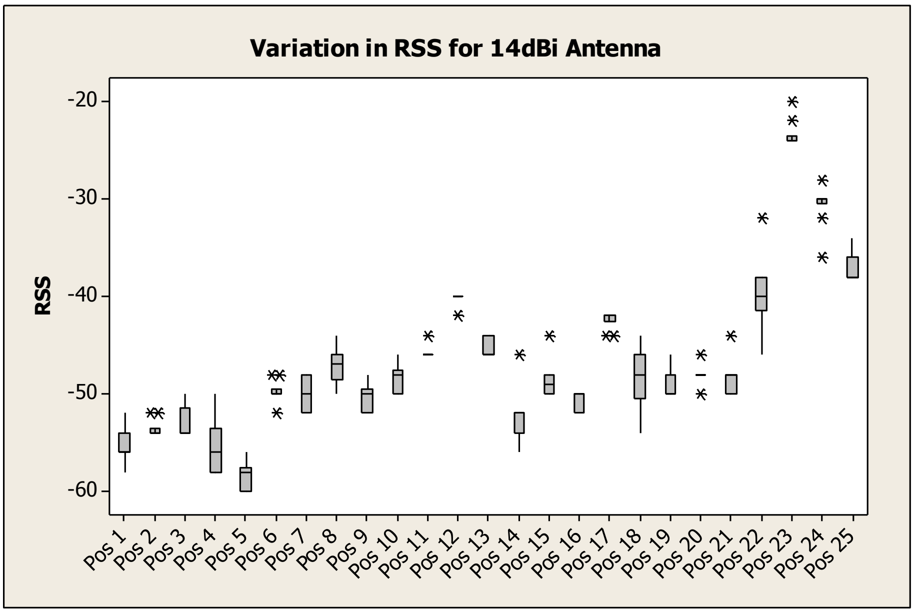


Figure 5.17: Variation in recorded signal strength (dBm) for the 14dBi Antenna

5.2.2. Outdoor Signal Characteristics

As described in section 5.1.2, two studies were performed to determine the performance of 2.4GHz Wi-Fi in an outdoor environment. Study A investigates the capabilities of 2.4GHz Wi-Fi with direct line of site while Study B evaluates the effects of moving obstacles on received signal strength in this outdoor environment.

Study A

For this study into outdoor performance with direct line of sight, Figures 5.18-5.20 show the average recorded signal strength in dBm vs distance for each of the three antenna types across the full 160m distance.

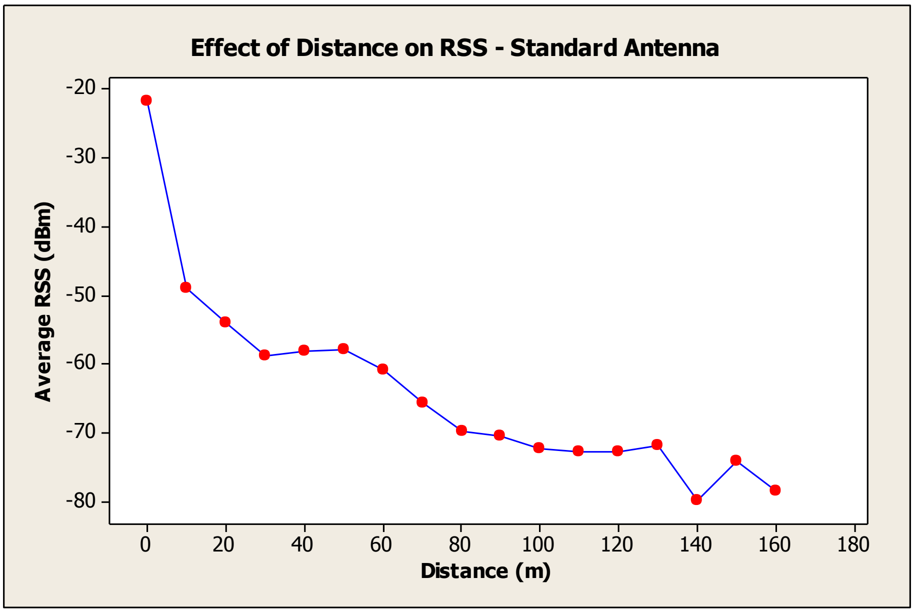


Figure 5.18: The effect of distance on the received signal strength using the standard antenna

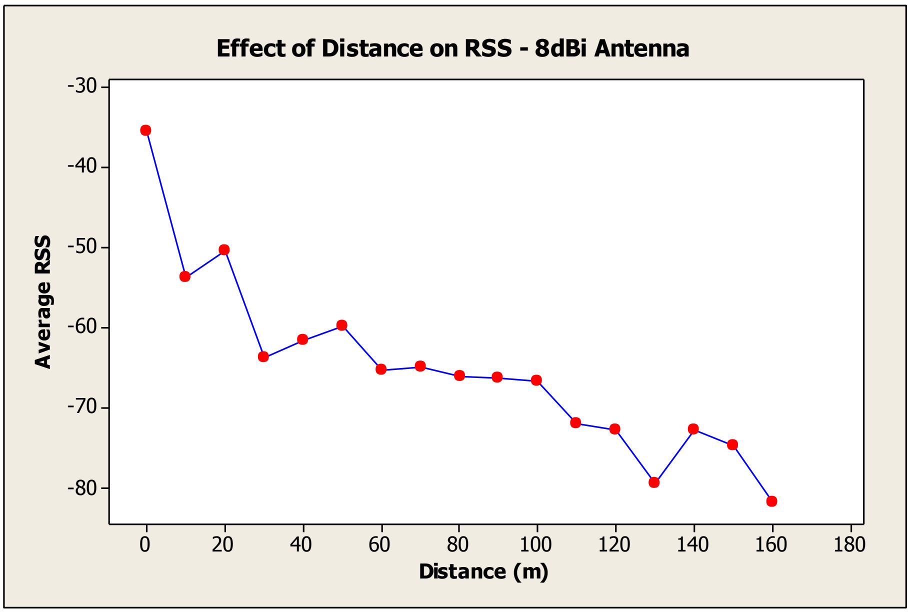


Figure 5.19: The effect of distance on the received signal strength using the 8dBi antenna

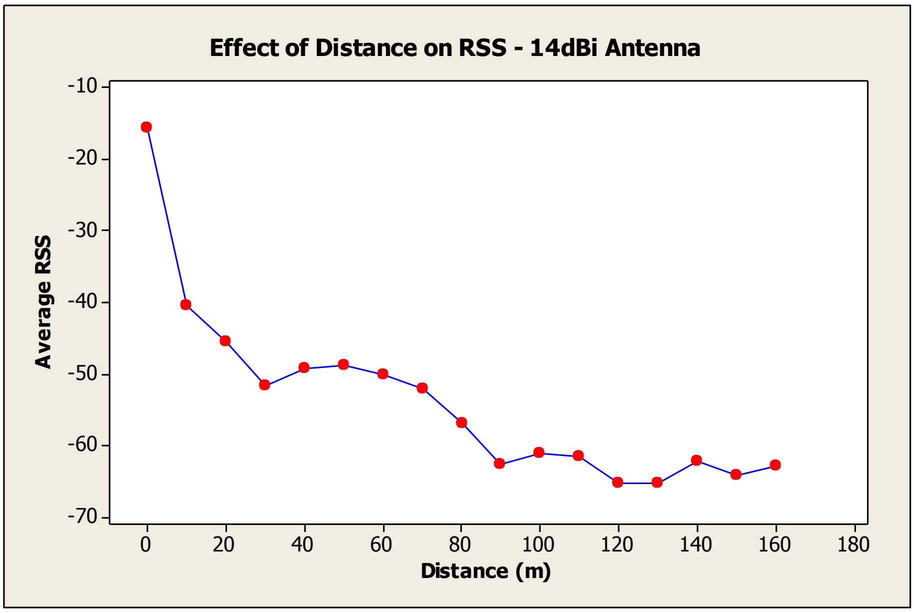


Figure 5.20: The effect of distance on the received signal strength using the 14dBi antenna

The graphical data presented below in Figures 5.21-5.23 show the scatter in the 10 samples at each of the sampled distances. This is displayed for each of the three antenna types tested to provide an understanding of the variance in each of the antennas in this environment so that a better understanding of the mathematical models can be achieved.

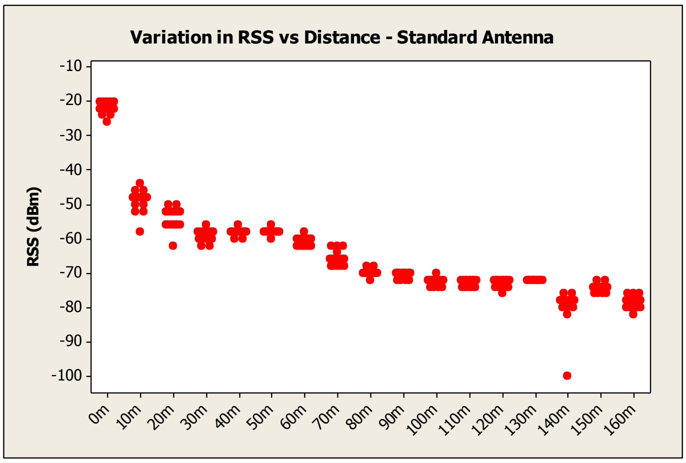


Figure 5.21: The variation in samples using the standard antenna

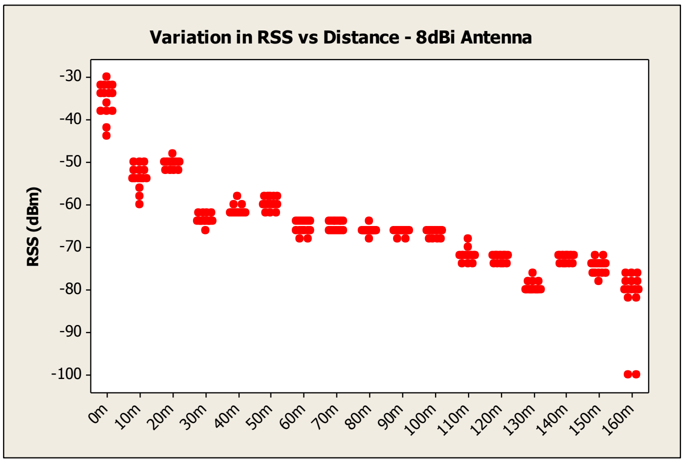


Figure 5.22: The variation in samples using the 8dBi antenna

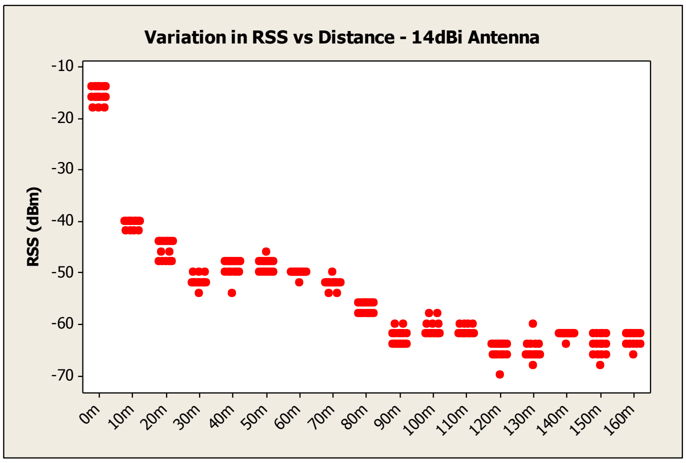


Figure 5.23 The variation in samples using the 14dBi antenna

Study B

For this study into the effects of moving obstacles on received signal strength, Figures 5.24-5.26 illustrate the results of the signal strength over the 20 minute evaluation periods for each antenna.

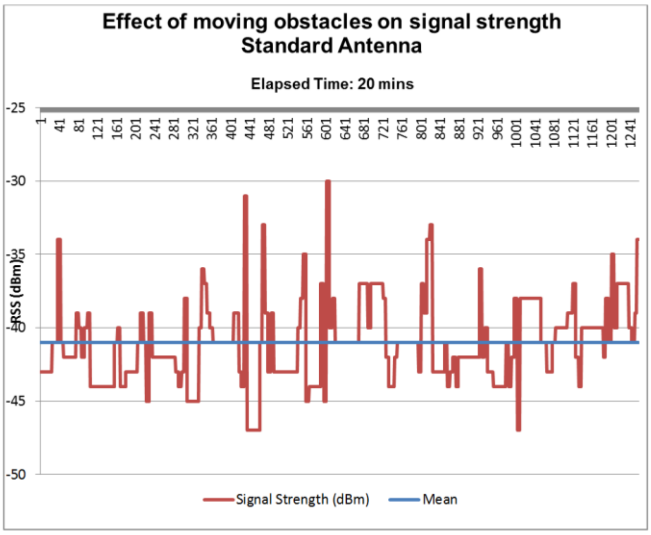


Figure 5.24: Effects of moving obstacles on received signal strength using the standard antenna

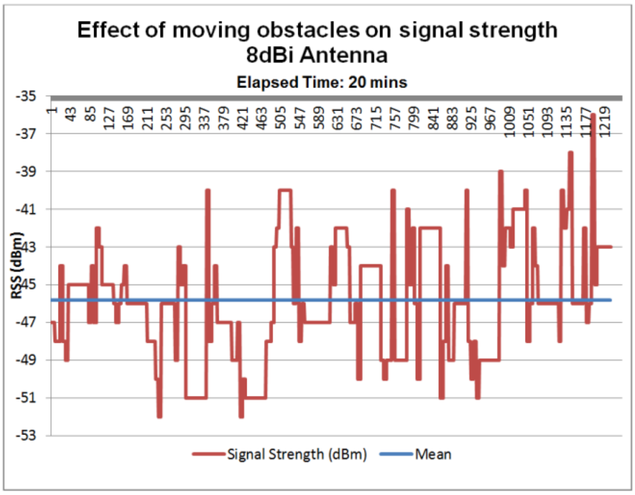


Figure 5.25: Effects of moving obstacles on received signal strength using the 8dBi antenna

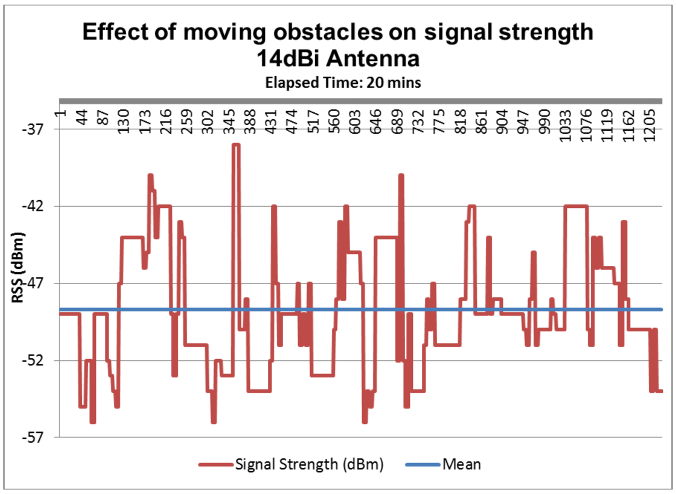


Figure 5.26: Effects of moving obstacles on received signal strength using the 14dBi antenna

Further to the preceding graphical illustration of Study B's results, Table 5.2 below shows a comparative span and the mean of the received signal strengths for these three types of antenna during this testing.

Antenna	Max RSS	Min RSS	RSS Span	Mean RSS
Standard Antenna	-30dBm	-47dBm	17dBm	-41dBm
8dBi Antenna	-36dBm	-52dBm	16dBm	-46dBm
14dBi Antenna	-38dBm	-56dBm	18dBm	-49dBm

Table 5.2: RSS Span for each antenna

5.2.3. 2.4GHz Wi-Fi Interference

Section 5.1.3 introduces and explains the setup of the two studies performed on this investigation of interfering devices on the 2.4GHz Wi-Fi band. Study A provides learning of 2.4GHz Wi-Fi performance when exposed to 2.4GHz wireless CCTV setups as a potential source of interference, which are mounted at height, whereas Study B provides the information into potential interference when 2.4GHz Wi-Fi is obstructed by a wireless TV sender located at ground level.

Study A

Figure 5.27 shows the control evaluations where the 2.4GHz CCTV simulator was turned off so Wi-Fi signals along the route could be recorded as a baseline.

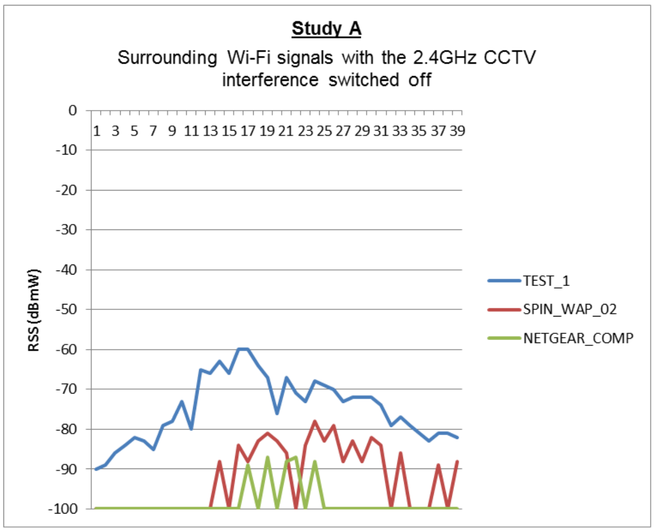


Figure 5.27: Control evaluation for Study A with the CCTV simulator switched off

Figure 5.28 shows the resulting interference that occurs when the 2.4GHz wireless CCTV setup is switched on and signals along the evaluated route are recorded.

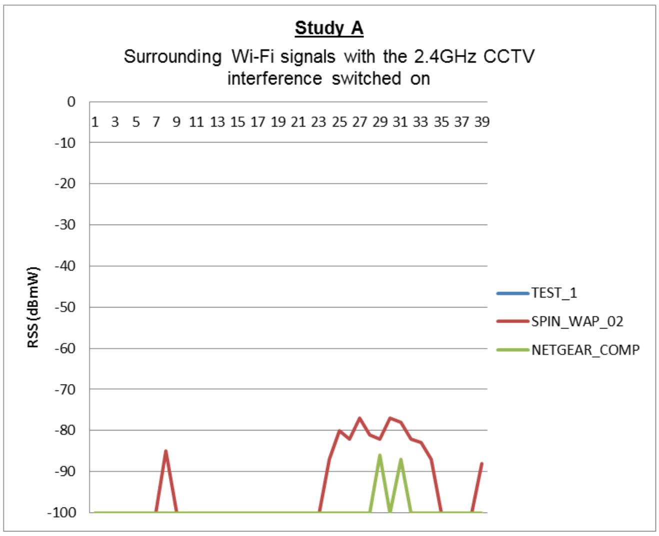


Figure 5.28: Surrounding Wi-Fi signals with the CCTV simulator switched on

Study B

Figure 5.29 shows the control evaluation where a 2.4GHz wireless TV sender simulator was switched off so that a baseline of surrounding Wi-Fi signals could be established along the route defined in 5.1.3. Figure 5.30 shows the resulting interference and the effect on the strength of the surrounding received Wi-Fi signals when the 2.4GHz wireless TV simulator was turned on and that same route was followed.

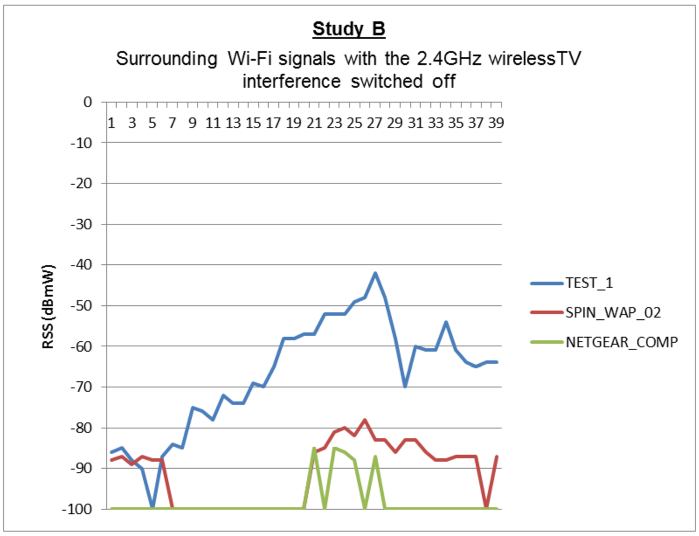


Figure 5.29: Control evaluation for Study B with the wireless TV simulator switched off

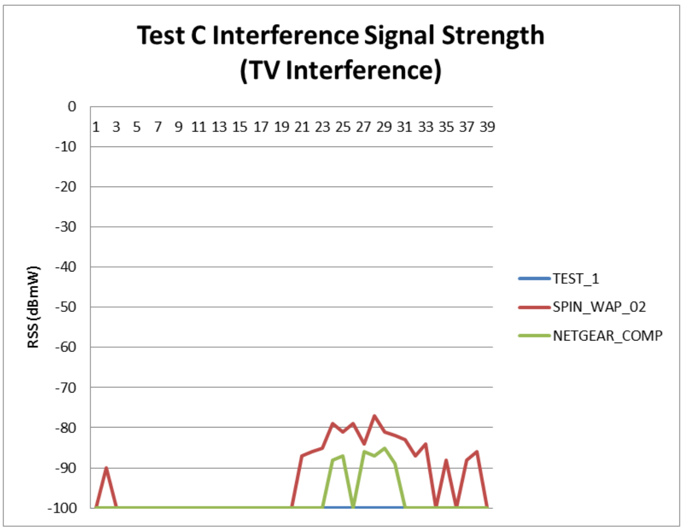


Figure 5.30: Surrounding Wi-Fi signals with the wireless TV simulator switched on

5.2.4. Effects of Materials on Wi-Fi Received Signal Strength (RSS)

Section 5.1.4 explains how the testing was performed to evaluate the effects of materials on Wi-Fi received signal strength. The results of the testing described in 5.1.4 are illustrated in their respective studies in this section.

Study A

Figure 5.31 below illustrates the signal strength in dBm resulting from the transmission of the 2.4GHz Wi-Fi access point with the standard antenna. The data from the 20 sample locations around the building were averaged and plotted on the contour plot of Figure 5.31.

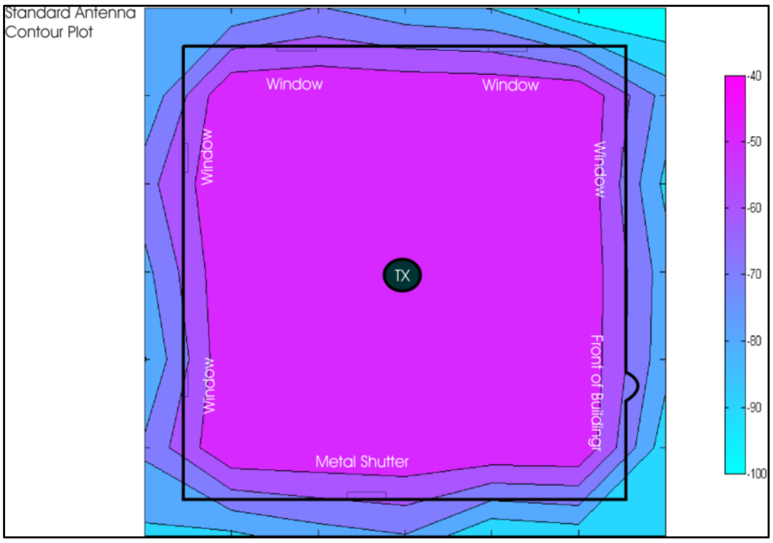


Figure 5.31: Contour plot showing the signal strength received around the building with the standard antenna

Figures 5.32 and 5.33 show the equivalent data for the 8dBi and 14dBi antennas respectively. Please note the direction of the 14dBi antenna shown in Figure 5.33.

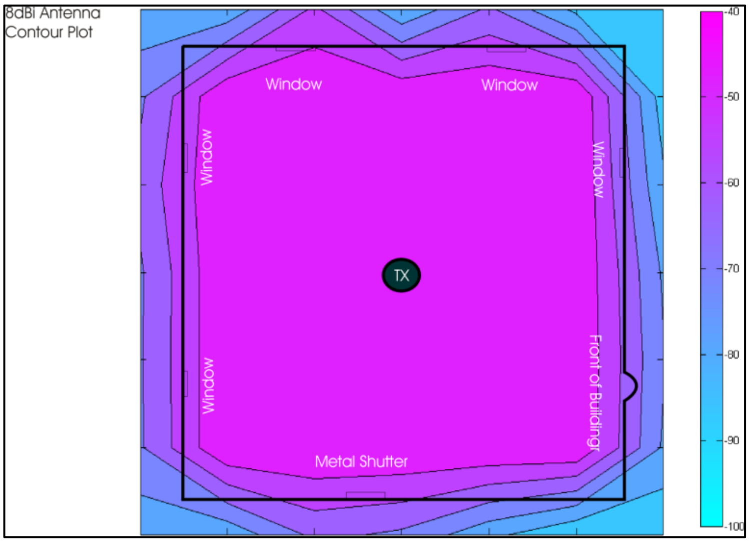


Figure 5.32: Contour plot showing the signal strength received around the building with the 8dBi antenna

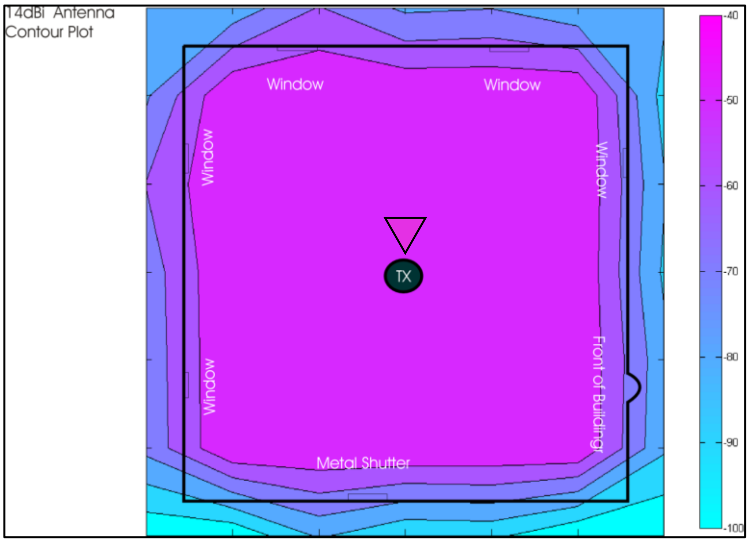


Figure 5.33: Contour plot showing the signal strength received around the building with the 14dBi antenna. Please note the direction of the antenna.

Study B

The two figures 5.34 and 5.35 graphically illustrate the resulting averaged effects of placing different materials between a transmitter and receiver as stipulated by the setup in 5.1.4. Figure 5.34 shows the absolute signal strength whereas Figure 5.35 shows the attenuation of the signals referenced to the control measurement.

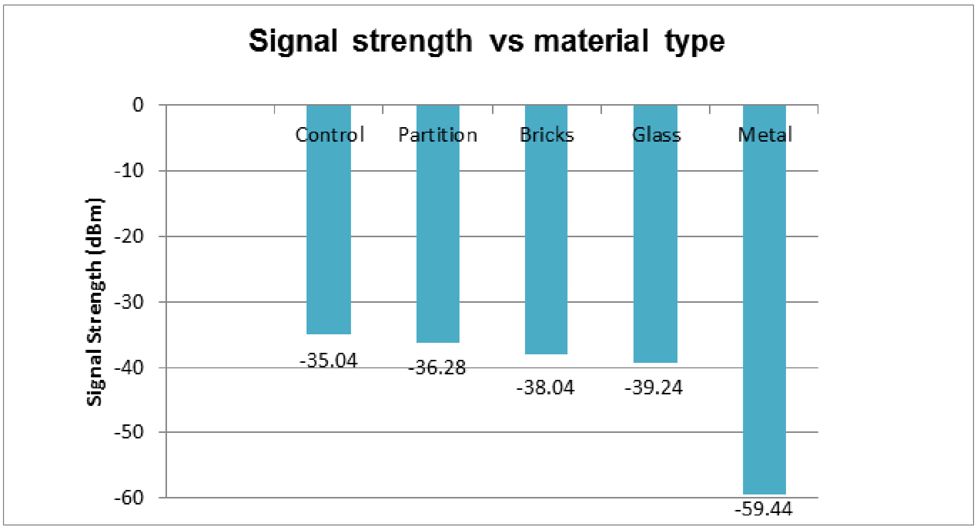


Figure 5.34: Average signal strength of the control and various materials obstructing the receiver

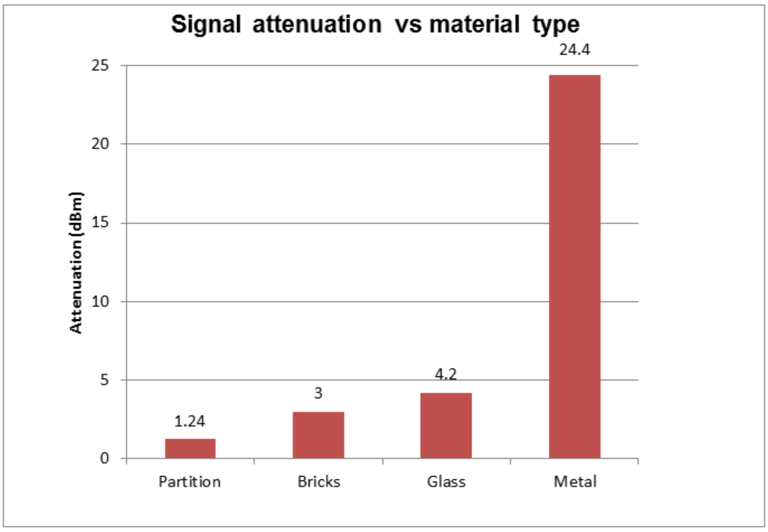


Figure 5.35: Attenuation effects of the material types referenced to the control

5.2.5. Detection of Wi-Fi Signals From a Moving Vehicle

The setup described in 5.1.5 shows how data from a moving vehicle was gathered in order to assess how the speed of a vehicle affects the capability of a receiver to receive Wi-Fi signals. The results of this evaluation are illustrated by Figure 5.36 which shows the average received signal strength for the stationary control evaluation and each of the speed tests performed.

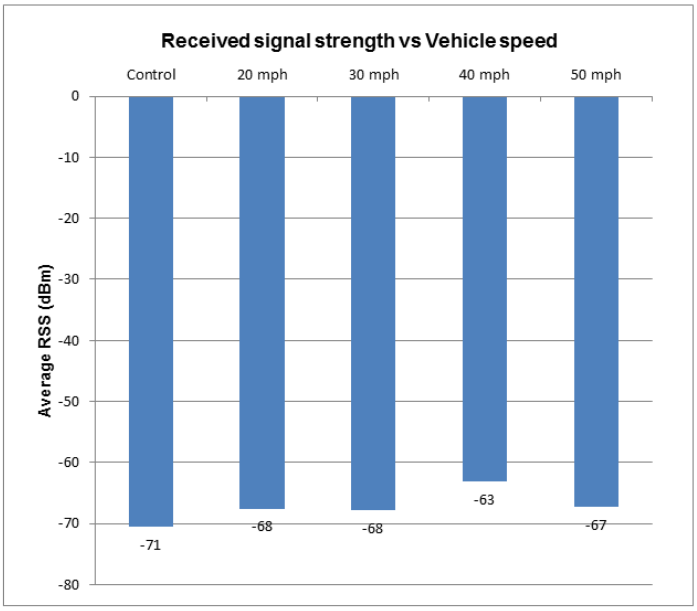


Figure 5.36: Results of signal strength from a moving vehicle

5.2.6. Wi-Fi received signal strengths from within vehicles

Figure 5.37 provides a visual result of the average received signal strength across both the left and right antennas from within each vehicle. The setup for this testing is described in section 5.1.6. The control shows the average signal strength received across both antennas with no vehicle present. This provides a reference to assess the attenuation caused by each vehicle. Figures 5.38 and 5.39 show the attenuation results for the left and the right antennas individually. This data shows how the structure of the vehicle affects signal strength as well as the attenuation caused by the vehicle itself referenced to the control.

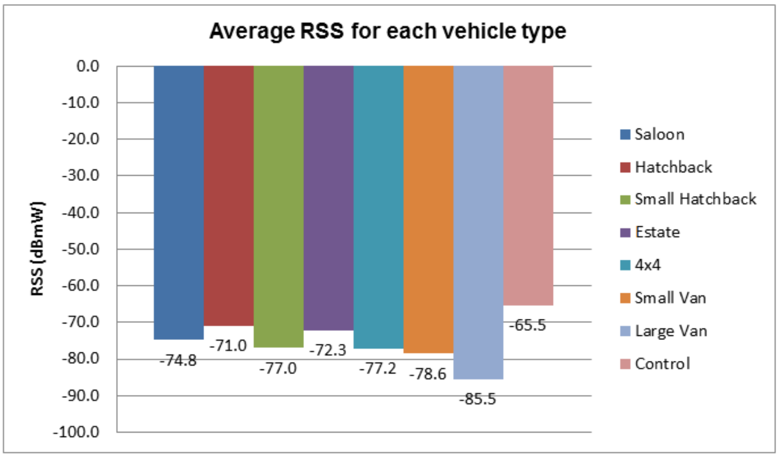


Figure 5.37: Average signal strengths recorded across both antennas for each vehicle and the control

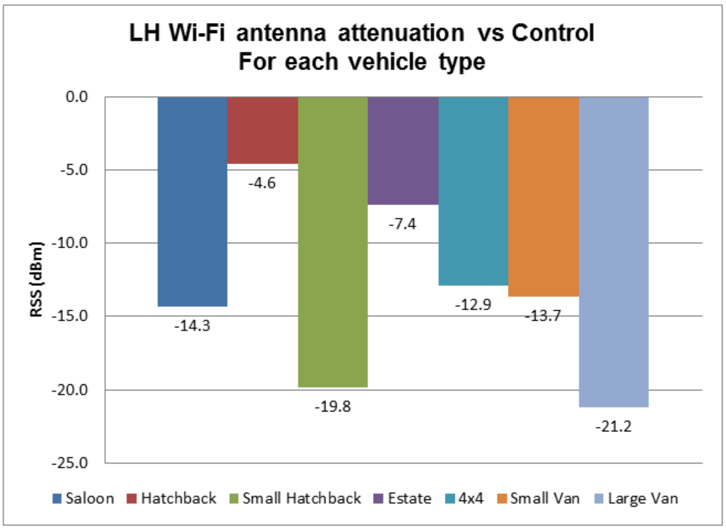


Figure 5.38: Attenuation effects of each vehicle as seen by the left hand antenna

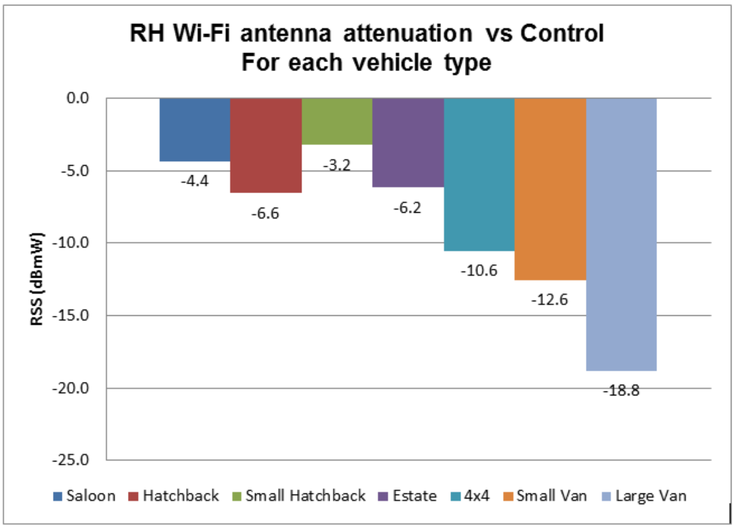


Figure 5.39: Attenuation effects of each vehicle as seen by the right hand antenna

5.3. Discussion of Results

The research that has been introduced in the previous sections of this chapter has described in detail the methods by which the testing of 2.4GHz Wi-Fi signals has taken place. The testing has covered a broad review of the signal characteristics by investigating indoor and outdoor signal propagation, but it has also investigated situations which will provide useful data for a tracking system. This final section of Chapter 5 will review and discuss the results of the research into these characteristics by following the order by which they are introduced and presented in the previous sections.

For the indoor signal characteristics, Figures 5.11-5.13 illustrate the effects that the indoor office environment has on the transmitted signal strength. From Figure 5.11, we can see that the partition on the far right bottom corner of the contour plot has quite a marked effect on the signal strength at the bottom of the plot. It appears solely from viewing Figure 5.11 that the partition and proximity to windows provides enough attenuation to lower the signal strength across the bottom of the office as viewed by the plot. This effect can be correlated with the findings of Win & Scholtz (2006) in their investigations into Ultra-Wide bandwidth signal propagation where they observed that measurements made in offices located at the edge of buildings see in increase in the noise floor attributed to radio and television stations, EMI and cellular towers (Win & Scholtz, 2006).

The plot also shows that desks have a minimal but notable attenuation effect but the partition, windows and also the smaller internal offices have the greatest effect on signal strength in that environment. Using the 8dBi antenna, Figure 5.12 reveals that the desks appear to have a greater effect than with the standard antenna that was used to plot Figure 5.11. The same attenuation effects with the partition and the offices are noted but, with this antenna, the desks appear to provide that bit more attenuation than with the standard antenna.

Figure 5.13 provides the highest signal strength in close proximity to the antenna than any of the other two antennas tested. Peaking at -20dBm in testing, this high power is to be expected as Dai et al (2011) explain, due to the increased power density of directional antennas. The directionality of the antenna provides higher signal strengths towards the back of the office with the 14dBi antenna. Figure 5.14 shows that the 14dBi antenna provides the most consistent results which can be explained by the conclusions of Dabin et al (2003) who indicate that directional antennas reduce the effects of multipath and the RMS delay spread due to their limited beam width.

The results of the outdoor signal characteristic research can conclude from Study A that the strongest signal at maximum distance was achieved by the 14dBi antenna. These findings are supported by the conclusions of Dai et al (2011) who conclude that directional antennas in wireless networks provide benefits such as reduced interference and extended communication range. Table 5.3 below shows the average received signal strengths between the three types of antenna which demonstrates along with Figures 5.18-5.20 that the received signal strength at the receiver was highest for the 14dBi antenna.

Antenna type	**Average RSS**
Standard Antenna	-64.1dBm
8dBi Antenna	-65.1dBm
14dBi Antenna	-53.8dBm

Table 5.3: Average received signal strengths for the three antenna types in Study A

Figures 5.21-5.23 show that the variation in sample strength was more for the standard and 8dBi antenna within the first 30m for the antenna. This variation in signal strength is believed to be due to the location of the transmitter in proximity to other obstacles which increases the interference as a result of the multipath propagation due to the environment and omni directional antennas used in these tests. Cichon & Wiesbeck (1994) support this with their statement of multiple reflections from building walls, building edge diffraction and radio penetration into buildings are dominant propagation mechanisms with outdoor propagation.

Study B can conclude that variation in received signal strength is affected by moving obstacles that pass between the transmitting and receiving antennas. Figures 5.24 -5.26 show a substantial variation in received signal strength and the lowest points in these Figures represent vehicles that stopped and obstructed the line of sight of the antennas.

Table 5.4 shows the average received signal strength for the three antenna types and it is clear from this that the 14dBi antenna is more susceptible to obstacles due to the narrow beamwidth. The results show that the two omni-directional antennas increase the average received signal strength when obstructing the line of sight of the antenna.

Antenna type	**Average RSS**
Standard Antenna	-41dBm
8dBi Antenna	-46dBm
14dBi Antenna	-50dBm

Table 5.4: Average received signal strength
affected by moving obstacles.

Park et al (2003) describe experiments on radio interference in the 2.4GHz ISM band, similar to the testing that took place in section 5.2.3. In particular, Park et al. (2003) investigate interference with a video transmission device operating in the 2.4GHz band. Testing performed with this device showed that it blocked WLAN transmissions up to 100m from the wireless access point on channels 9, 10 & 11 of the Wi-Fi band. The testing performed in section 5.2.3 showed that in both Study A and Study B there was a complete loss of the wireless access point TEST_1 which was positioned within 1m of the wireless TV sender simulator. Other wireless access points were affected but less so than TEST_1 access point which was operating on channel 6 and close to the wireless TV sender simulator. This testing agrees with the findings of Park et al. (2003) and finds no differences between a CCTV device at height and a wireless TV sender.

Study A of 5.2.4 demonstrates the effects of a building on received signal strength. Figure 5.31 clearly shows that windows attenuate the signals less, as the signal strength increases around those areas. The lowest recorded signal strength was -100dBm where the access point beacon was not visible at all to the receiver. Figure 5.32 shows the effect of the 8dBi antenna which performed better than the standard antenna as there was better signal reception overall. The lowest average signal strength was -86.8dBm.

The evaluation of signal strength received with the 14dBi antenna reflects the propagation characteristics of the antenna, with the highest signal strengths visible in the direction of propagation of the antenna. Resulting from this, the attenuation effects of metal skins in this style of building have a substantial effect on the received signal strength when measured from outdoors. Windows permit signals to leak indicating that metal is a greater attenuator than film coated glass.

Study B in section 5.2.4 concludes from Figures 5.34 and 5.35 that metal attenuates a 2.4GHz signal the most. Glass is the second greatest attenuator in this experiment and the top two results are confirmed by the results of Study A above in 5.2.4. The metal clad building in Study A showed that glass attenuated the signal less than the metal cladding of the building which is confirmed by this more direct evaluation in Study B. Using these results, an estimation of signal strength in an indoor environment can be made by generating signal models using the data in this study. This can provide insight into the placement of transmitters and estimate the signal strength at key locations in the environment.

Figure 5.36 in section 5.2.5 shows that there is very little effect on average signal strength when travelling in a vehicle. The transmitting access point was always visible and had good signal strength which is comparable to that of the control evaluation. The small difference in signal strength on the 40mph evaluation appears to be an anomaly which is likely to be down to environmental factors such as presence of another vehicle at the time of testing and potential changes to the antenna setup by repositioning of the recording laptop. `From this testing, it can be concluded that there is minimal effect on 2.4 GHz Wi-Fi signal strength received from a moving vehicle.

The final part of this chapter's research evaluated the effects of different vehicles on received 2.4GHz signal strength. This unique research showed the attenuation due to different vehicle structures. It is evident from all the tests that the large van attenuated the signal the most. This further confirms the results of 5.2.4 Study B which showed that metal attenuates a 2.4GHz signal more than glass. The results show a strong correlation between the amount of metal on the vehicles which is determined by vehicle size, and the strength of the received signal. This is true for the large van, the small van and the 4x4 vehicle.

Different results are seen with the hatchback and the saloon vehicle. The Hatchback had a very large glass boot which did not attenuate the received signal as much as the previously assessed vehicles. The signal strengths on the left and right antennas were different which can be explained by the depth of the boot compartment on both of these vehicles. The boot compartments on small vehicles are small, confined and use depth to maximise boot space. As there is a large lip surrounding the boot, combined with a small compartment, the transmitted signal has less chance of reaching the receiver without significant attenuation. With the saloon car, this also applies although the boot compartment is larger which explains the higher received signal strength at the receiver. The left hand antenna received signal strength on these two vehicles also differed and this is due to the structural differences of the vehicles which affect how the signal approaches each antenna, either by reflection or line of sight.

5.4. Conclusions

This unique research shows the advantages of using antenna diversity to receive the best possible signal and how the differences in received signal strengths from within vehicles can be improved by using this technique. In the real scenario of a stolen CIT box, this research has shown that applying antenna diversity techniques to a CIT box within the boot of a getaway vehicle can help to counter the attenuation effects of the vehicle’s structure.

6. Factors Affecting Cash Security Box Antenna Received Signal Strength

This chapter introduces the CIT cash box and discusses the physical aspects that may have an effect on the performance of any Wi-Fi antennas placed outside or near the CIT box. The design of the CIT box is already fixed and hundreds of thousands of pounds in development, testing, validation and re-tooling is required to re-design the CIT box with an integrated tracking system in mind. Given this expense, a tracking solution must integrate into this existing design which is not the ideal situation in terms of general integration and seamless function where the best outcome for an integrated tracking system is to design the CIT box itself with the tracking solution in mind. As the CIT box is an existing product, this ideal situation is not possible and therefore this chapter investigates the issues, discusses methods of circumventing the issues and identifies compromises that may have to be made with this tracking system.

6.1 The CIT Box And Antenna Arrangement

The image below in Figure 6.1 shows an example of a Spinnaker CIT box that has been used for this research. It serves as a visual indicator of challenges that are faced with integrating a tracking system into this type of product. The image shows the CIT box components comprising a hinged lid, fixed handle, LCD display and two interface buttons on each side of the handle.

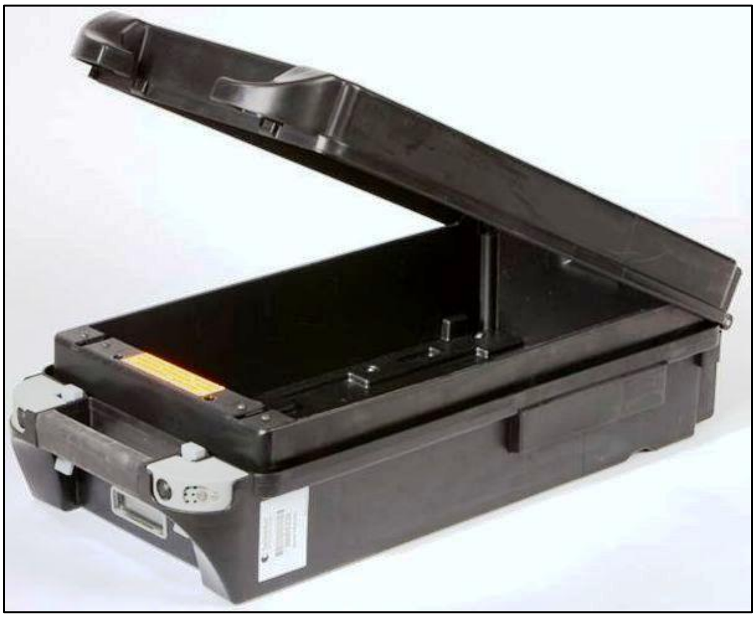


Figure 6.1: An example of a Spinnaker CIT box

Chapter 5 has already introduced the concept of antenna locators on the CIT box and the use of these external locators is due to constraints that exist as a result of the construction of the CIT box. Details of these constraints are confidential but they restrict the placement of antennas such that no antennae can be placed inside the lid and no antennae can be placed in the base of the box; the surface opposite the lid. This leaves three surfaces, the two sides and the top face of the box where the handle exists. First thoughts are that antennae used for the purposes of this tracking system are best placed on the top face of the box, or even within the handle, but with further consideration, antennae within the handle of the CIT box is not a manufacturable solution due to the construction of the CIT box but also, an operator’s hand on the handle would only adversely affect the performance of any antennae placed within the handle. External locators for antennae are the preferred choice for this research as they provide the best solution for manufacturability and they offer flexibility for antenna diversity which has been previously discussed and will be further discussed in this chapter.

The following research investigates the effects of placing Wi-Fi antennae against the CIT box in the external locators. The research also investigates antenna diversity techniques which provide the capability of switching between Wi-Fi antennas installed in the left and right antenna locations. The final part of this chapter’s research is evaluating Wi-Fi antenna performance and antenna diversity in a practical scenario not uncommon to stolen CIT boxes.

6.2 Evaluation Methods And Experimental Setups

The evaluation methods and experimental setups described in this section evaluate three types of antennas and a bespoke designed RF switching device which is capable of electronically switching between two antennas. With these devices, this research aims to establish knowledge of the effects of the CIT box on three types of antennae when placed in the antenna locators and to evaluate the effectiveness of antenna diversity. Three antennas were selected for this research; a stubby omnidirectional antenna, a high quality PCB mounted chip antenna from Antenova, and a cost effective chip antenna from Murata.

6.2.1 Stubby Antenna

This stubby antenna is a readily available 2.4GHz dipole antenna and has a gain of 1.8dBi matched at 50Ω and is designed for use with WLAN equipment. It is cost effective and doesn’t require any supporting hardware such as a PCB. The stubby antenna is shown in Figure 6.3 below.

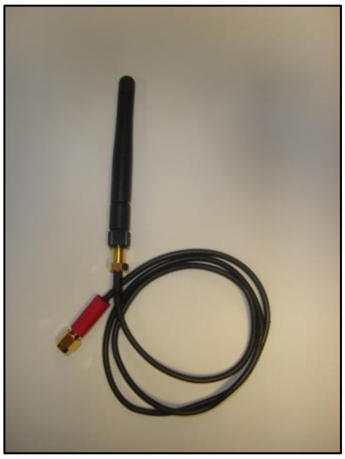


Figure 6.3: Stubby Wi-Fi antenna

The stubby antenna was evaluated in three scenarios: free standing, inside the Acetal antenna locator and installed on the CIT box (Acetal antenna locator screwed to the CIT box). In each of the three scenarios, the antenna was connected to a Vector Network Analyser and the return loss S11 parameter was measured.

6.2.2 Antenova Antenna

This antenna was selected for its compact size and stated good performance within the Wi-Fi band. It is centred at 2.45GHz with 0.8dBi gain. Its design requires the antenna to be mounted on a PCB with a ground plane under the antenna to radiate effectively and as a result, the PCB on which the antenna is mounted needs to have specific dimensions. Figure 6.5 below shows the implemented design of the Antenova antenna, which was designed by the author for this evaluation.

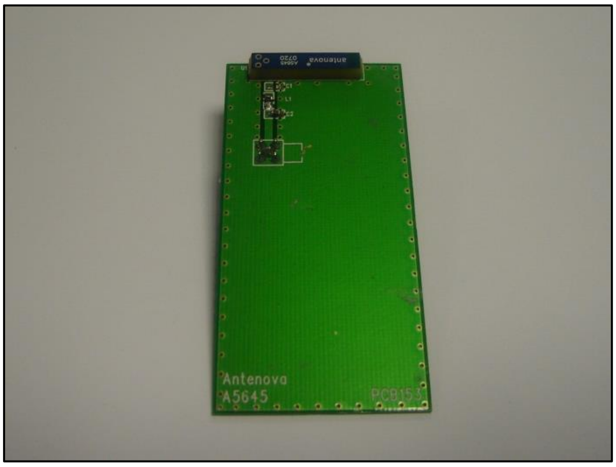


Figure 6.5: Designed Antenova Antenna board

The antenna was designed on 0.8mm thick FR4 board with dimensions 64x32mm. The transmission line was matched to 50 ohms using a coplanar waveguide as described by the application note. Space was left for a matching network to tune the antenna when in place in the CIT box to optimise performance. Figure 6.6 shows the layout of the Antenova PCB.

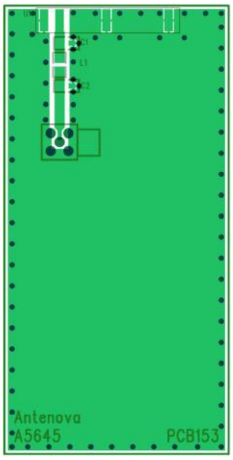


Figure 6.6: Antenova Board Layout

The Antenova antenna assembly was evaluated in three scenarios: free standing, inside the Acetal antenna locator and installed on the CIT box (Acetal antenna locator screwed to the CIT box). In each of the three scenarios, the antenna was connected to a Vector Network Analyser and the return loss S11 parameter was measured. To provide a good baseline for testing, the Antenova antenna was tuned freestanding using the Vector Network Analyser to match as close as possible the return loss characteristics specified by the antenna datasheet. These tuned values were a 1pF capacitor at C2 and a 0R link at L1.

6.2.3 Murata Antenna

This antenna was chosen for its cost and flexibility. It is also the smallest antenna out of all those tested. Its centre frequency is variable and is easily configured using a coarse tuning element and a fine tuning element such as a capacitor or inductor. Its design requires the antenna to be mounted on a PCB with a ground plane under the antenna to radiate effectively. The coarse tuning element is etched into the PCB by removing a small section of the copper from the ground plane near the antenna. The fine tuning element can vary the antenna's peak radiation frequency by up to 100MHz without having to alter the coarse tuning. This allows the antenna to be finely tuned to optimise performance when installed on the CIT box. Figure 6.7 below shows the implemented design of the Murata antenna which involved the design of a bespoke PCB for this application by the author.

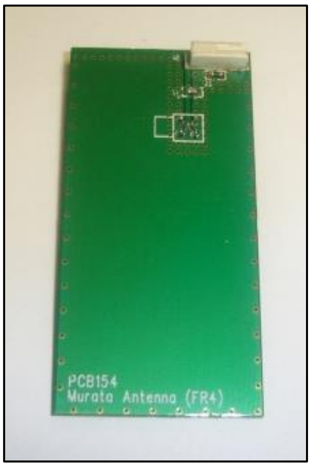


Figure 6.7: Murata Antenna PCB

The antenna was designed on 1.6mm thick FR4 board with dimensions 64x32mm. The transmission line was matched to 50 ohms (1.1mm) using a Microstrip. Space was left for a fine tuning element and a matching network to tune the antenna when installed on the CIT box. Figure 6.8 below shows the design of the Murata PCB antenna.

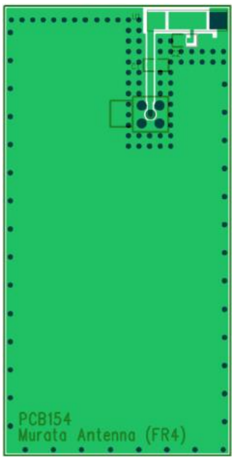


Figure 6.8: Murata Board Layout

The Murata antenna assembly was evaluated in three scenarios: free standing, inside the Acetal antenna locator and installed on the CIT box (Acetal antenna locator screwed to the CIT box). In each of the three scenarios, the antenna was connected to a Vector Network Analyser and the return loss S11 parameter was measured. To provide a good baseline for testing, the Murata antenna was tuned freestanding using a similar method to the Antenova antenna. The difference between the two tuning strategies is that the Murata antenna requires a fine tuning element to tune the antenna as well as tuning of the transmission line. The tuning was performed with a Vector Network Analyser and the fine tuning was achieved with a 3.3nH inductor at location C2 and the matching network was tuned using a 2.2pF capacitor at C1.

6.2.4 Antenna Diversity Evaluation

The objective of this research is to provide information relating to the locations of antennas on a CIT box and to also prove the effectiveness of antenna diversity with a CIT box in a practical situation. The selected locations for the antennas are in both the left and right hand antenna locators located on the sides of the CIT box as previously described. The research was performed using a bespoke designed RF switch to switch the input of the receiver between the left and right hand antennas located on the CIT box. This RF switch device was designed by the author on a 2 layer PCB in the Mentor Graphics PADS CAD package for this application, and is shown below in Figure 6.9.

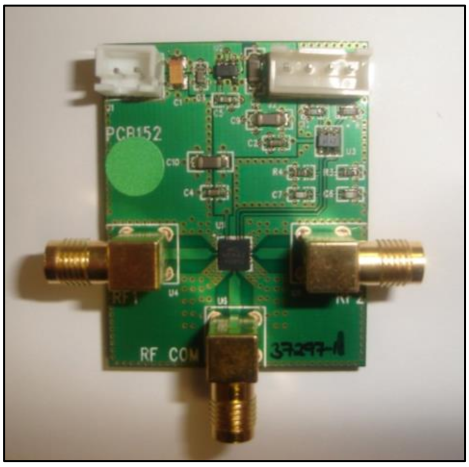


Figure 6.9: The bespoke designed RF switch device

6.2.4.1 Static Evaluation

A static evaluation was first performed to evaluate the received signal strength at each antenna. The setup is shown in a top view in Figure 6.10 below and shows a CIT box at a fixed distance from a transmitting Wi-Fi access point. The three antennas in 6.2 were used so results show the received signal strength at the Stubby antennas, Antenova antennas and the Murata antennas each in the left and right hand antenna locator. Eight samples of signal strength were averaged across the left and right hand antenna locator for each of the three antenna types.

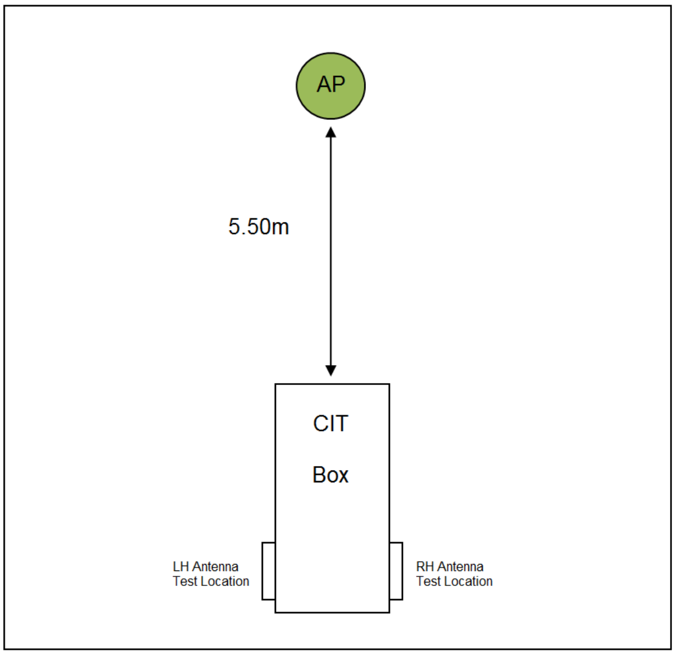


Figure 6.10: General setup for the static evaluation of antenna diversity

6.2.4.2 Practical Evaluation

Further research evaluates the effectiveness of antenna diversity in a more practical environment, which a CIT box is exposed to when stolen. A stolen CIT box is often thrown into a bush or shrubbed area where it is concealed, or into a skip where it will hopefully end up in landfill without being noticed. In these two likely scenarios, antenna diversity is evaluated to establish whether it is worthwhile implementing such a technique in a bespoke tracking system utilising Wi-Fi signals. For completeness, the three types of antennas introduced in the preceding research are also used in this research.

In the evaluation of the scenario of the CIT box thrown in a shrub, tests were performed with each of the three antenna types and data was sampled from the antennas firstly with the left hand test location facing upwards and then the right hand test location facing upwards. The transmitting wireless access point was placed at a location where the CIT box would see very low signal strength; around -80dBmW. Three samples were taken which consisted of a control experiment, LH antenna facing the ground and RH antenna facing the ground. The control samples were taken with the CIT box at the evaluation area but with neither antenna obstructed. This method helps to prove the benefits of antenna diversity in a worst case when one of the CIT box antennas is facing the ground. The setup for the experiment is shown in Figure 6.11 below showing the location of the transmitting Wi-Fi access point and the location of the CIT box in the shrubbery.

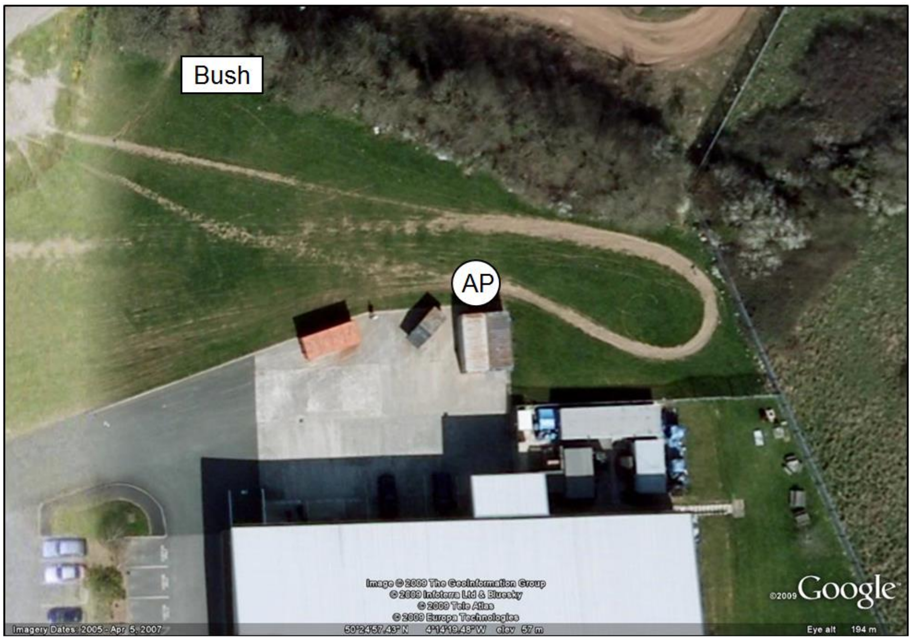

Bush
AP
Image © 2009 The GeoInformation Group
© 2009 Infoterra Ltd & Bluesky
© 2009 Tele Atlas
© 2009 Europa Technologies
©2009 Google
Imagery Dates: 2005 - Apr 5, 2007
50°24'57.43" N 4°14'19.48" W elev 57 m
Eye alt 194 m

Figure 6.11: Setup for evaluating antenna diversity effectiveness in a scenario with a CIT box thrown in shrubbery

The final piece of research for this chapter evaluates the scenario of a CIT box thrown in a metal skip and follows a similar setup to that used to evaluate the scenario of a CIT box thrown in shrubbery. All three antennas were evaluated with one antenna type present in the antenna test location for a given evaluation. The tests again featured sampling with the left hand antenna test location facing upwards and then the right hand antenna facing upwards. The control experiment was performed with the CIT box outside the skip and both antennas unobstructed. The wireless access point was placed at a location where the CIT box would see very low signal strength; around -80dBmW. The setup for the experiment is shown in Figure 6.12 below showing the location of the transmitting Wi-Fi access point and the location of the skip where the CIT box was placed for testing.

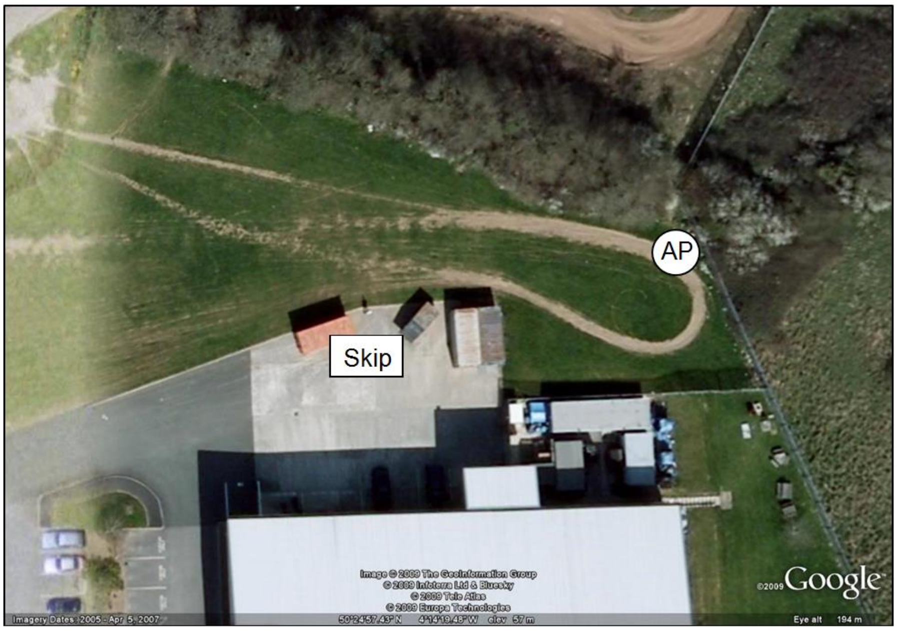
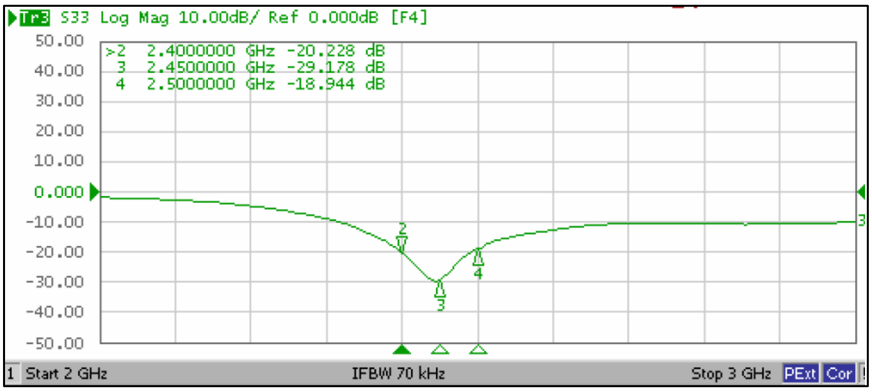


Figure 6.11: Setup for evaluating antenna diversity effectiveness in a scenario with a CIT box thrown in shrubbery

6.3 Evaluation of Results

6.3.1 Stubby Antenna

Following the experiment setups in 6.2.1, Figure 6.13 below shows the specified performance of the stubby antenna as a 2.4GHz Wi-Fi radiator.



```
Tr3 S33 Log Mag 10.00dB/ Ref 0.000dB [F4]
>2  2.4000000 GHz -20.228 dB
 3  2.4500000 GHz -29.178 dB
 4  2.5000000 GHz -18.944 dB
1 Start 2 GHz          IFBW 70 kHz          Stop 3 GHz PExt Cor
```

Figure 6.13: Stubby Wi-Fi antenna return loss as shown on its datasheet

Figure 6.14 shows the return loss results from the Vector Network Analyser when the stubby antenna is installed in the acetal antenna locator. When installed, the stubby antenna is detuned and its peak return loss moves to 2.34GHz which is far from Wi-Fi Channel 1 at 2.41GHz.

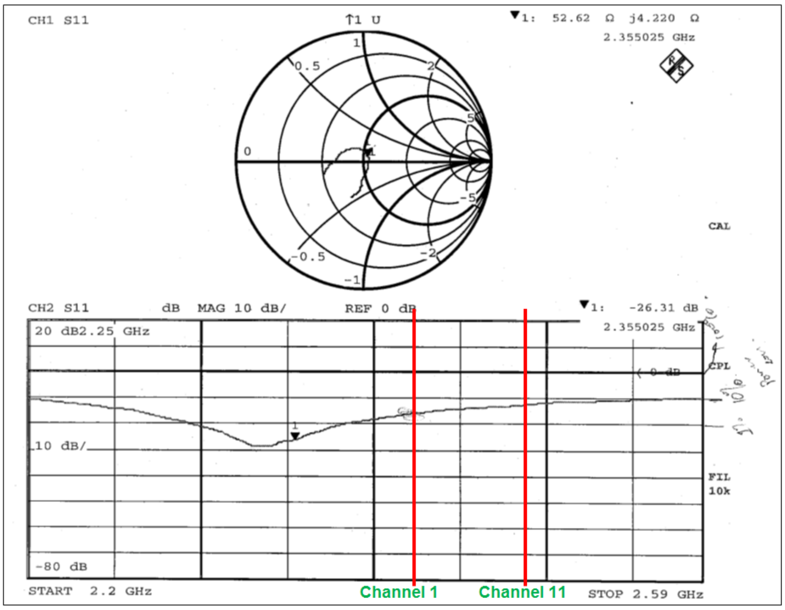


Figure 6.14: Stubby Wi-Fi antenna return loss when installed in the Acetal antenna locator.

The final results for the stubby antenna are shown in Figure 6.15, which shows the effect of placing the stubby antenna in its locator onto the CIT box. The peak return loss is decreased but it also drifts lower down the frequency band to around 2.2GHz.

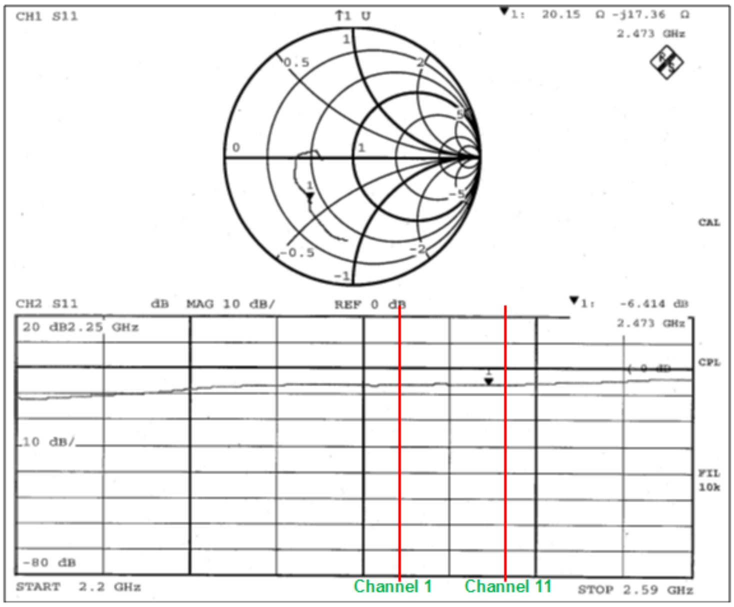


Figure 6.15: Stubby Wi-Fi antenna performance when installed on the CIT Box

6.3.2 Antenova Antenna

Figure 6.16 below shows the pre-tuned antenova antenna in free space. It does not appear to be as particularly well tuned to the 2.4GHz Wi-Fi bands as a free standing antenna when compared to the return loss characteristics of the datasheet as shown by Figure 6.17.

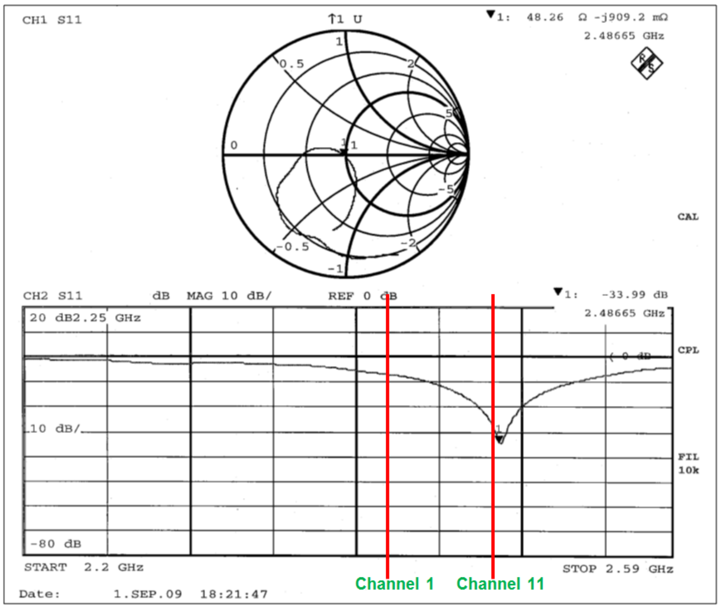


Figure 6.16: Antenova antenna tuned (Free Standing)

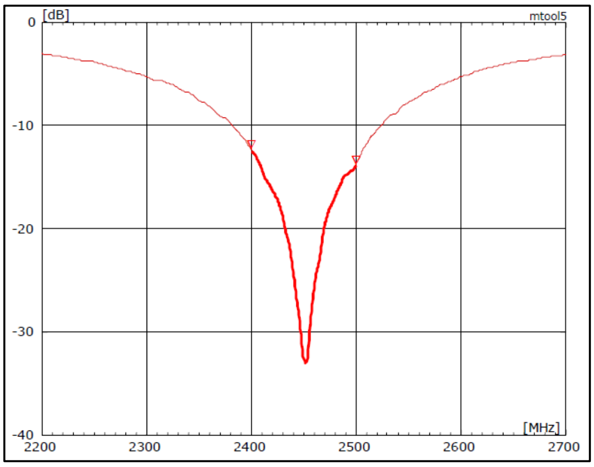


Figure 6.17: Antenova antenna return loss as shown on its datasheet

Figure 6.18 shows the return loss results from the Vector Network Analyser when the Antenova antenna is installed in the acetal antenna locator. When installed, the antenna appears to be re-tuned by the characteristics of the Acetal and the peak return loss frequency shifts lower down the band, closer to Channel 1 where it was weak when free standing.

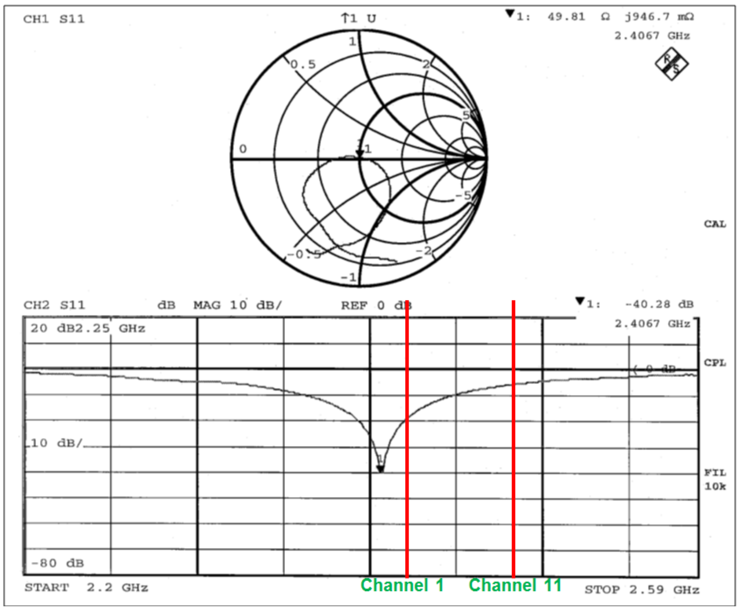


Figure 6.18: Antenova antenna's response when installed in the Acetal locator

When the Antenova antenna is installed on the CIT box, it appears to re- tune the antenna and brings the peak return loss frequency around Channels 1 to 2. This benefits the tracking system by being most effective at receiving weak signals on Wi-Fi channels 1 and 2. Figure 6.19 shows this result.

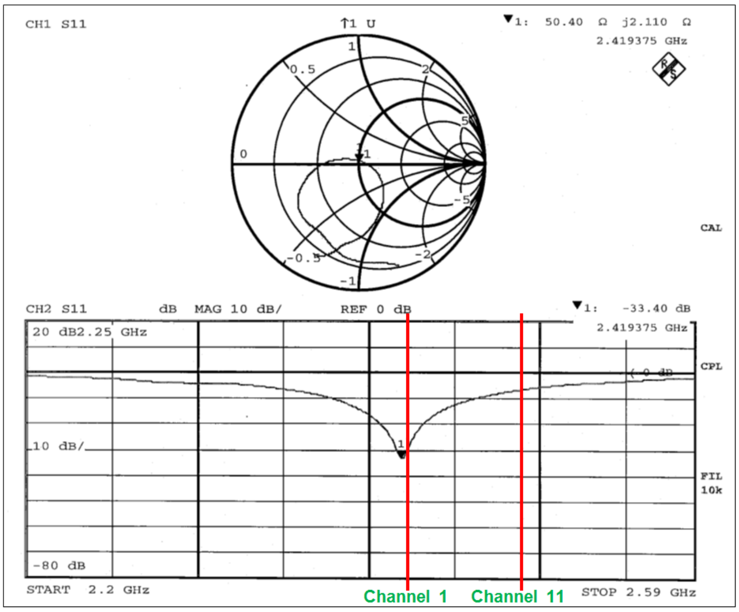


Figure 6.19: Antenova antenna’s response when installed on the CIT Box

6.3.3 Murata Antenna

Figure 6.20 below shows the pre-tuned Murata antenna in free space. It appears to be tuned to the higher Wi-Fi channels and reflects the Murata datasheet return loss characteristics as depicted by Figure 5.21, albeit shifted more towards the higher Wi-Fi channels.

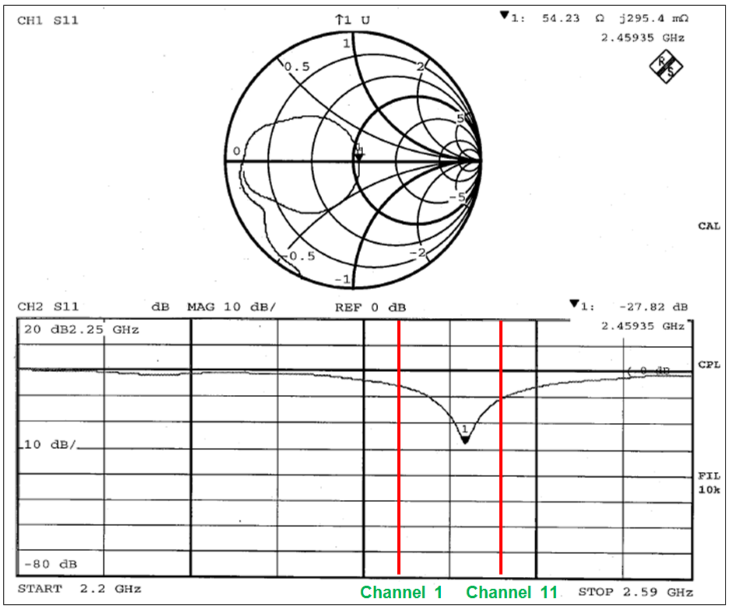


Figure 6.20: Murata antenna when tuned (Stand alone)

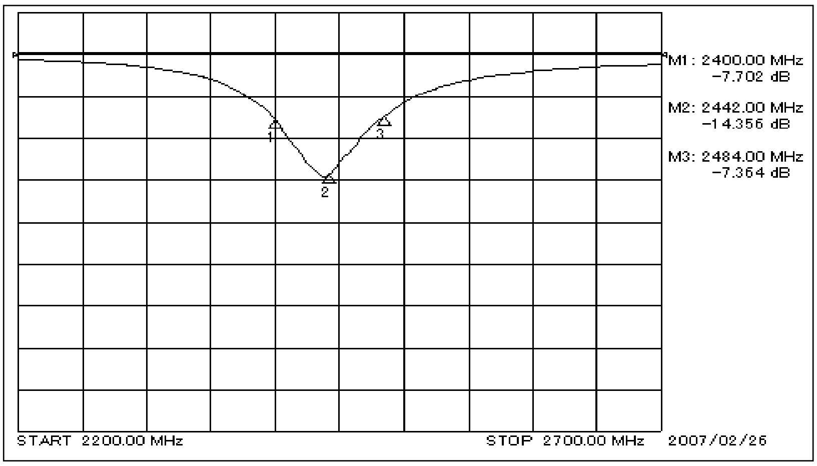


Figure 6.21: Murata antenna theoretical return loss from datasheet

Figure 6.22 shows the return loss results from the Vector Network Analyser when the Murata antenna is installed in the acetal antenna locator. When installed, the antenna's tuning is significantly compromised by the Acetal's characteristics. The sharp and well pronounced return loss curve is broadened and the peak return loss frequency is moved away from the frequencies of interest.

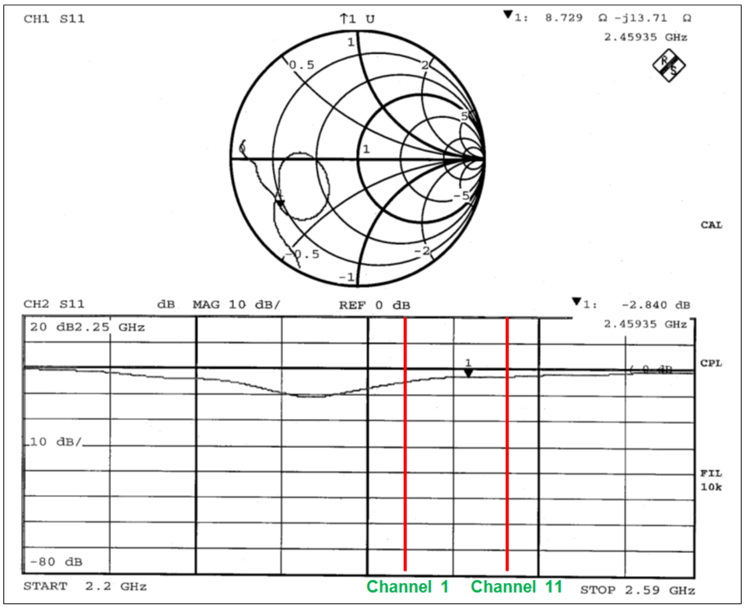


Figure 6.22: Murata antenna's response when installed in the Acetal antenna locator

When the Antenova antenna is installed on the CIT box, it appears to have little further effect on the antenna. As a result, the antenna's performance is only slightly more compromised than when not placed on the CIT box. Figure 6.23 shows this result.

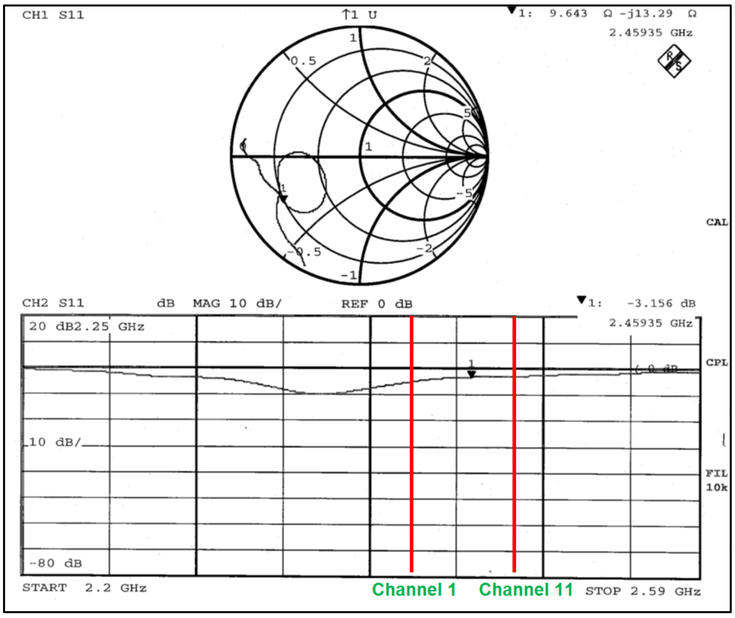


Figure 6.23: Murata antenna's performance when installed on the CIT Box

6.3.4 Antenna Diversity Evaluation

6.3.4.1 Static Evaluation

The results for this experiment described in 6.2.4 and 6.2.4.1 are shown below in Figures 6.24 - 6.31. The results compare the received signal levels at the left, right and control antennas for each antenna type (Stubby, Antenova & Murata). In some figures the received signal strength at the left and right antennas are subtracted from the control signal to show the level of attenuation at that antenna.

Figure 6.24 & 6.25 show the results of the Stubby antennas and in particular, Figure 6.24 shows the received signal strength at the left antenna and right antenna along with the control antenna which was placed freestanding outside the CIT box. Figure 6.25 shows the attenuation of each antenna vs the control as the signal strength at each antenna is subtracted from the signal seen at the control to provide the loss on each antenna due to the CIT box.

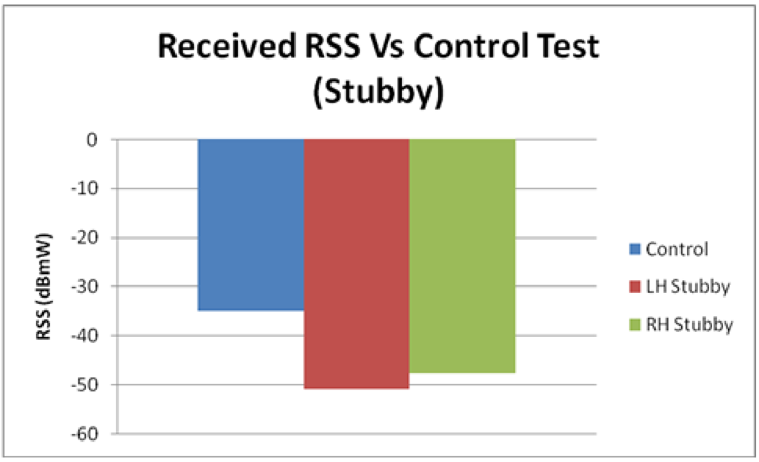


Figure 6.24: Received Signal Strength at each Stubby antenna

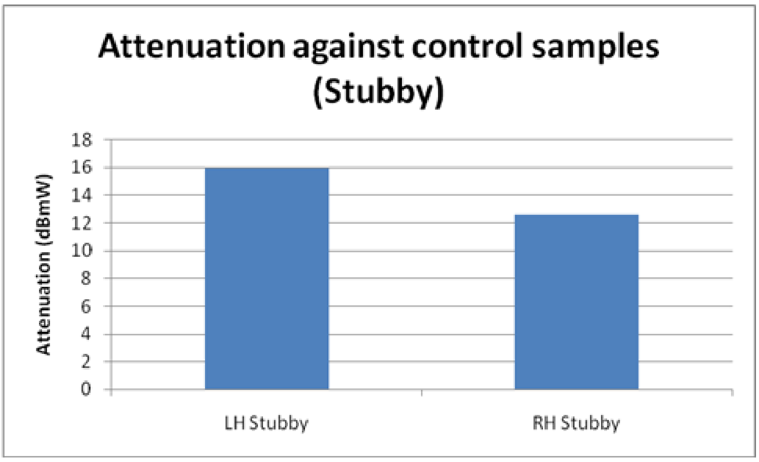


Figure 6.25: Attenuation at each Murata antenna vs the control samples

Figure 6.26 shows the measured results of the Antenova antennas against their respective control measurements, which were taken with the control antenna outside the CIT box. Figure 6.27 shows the attenuation of each antenna vs the control for the Antenova antennas. As with the stubby antennas, signal strength at each antenna is subtracted from the signal seen at the control antenna to provide the loss on each antenna due to the CIT box.

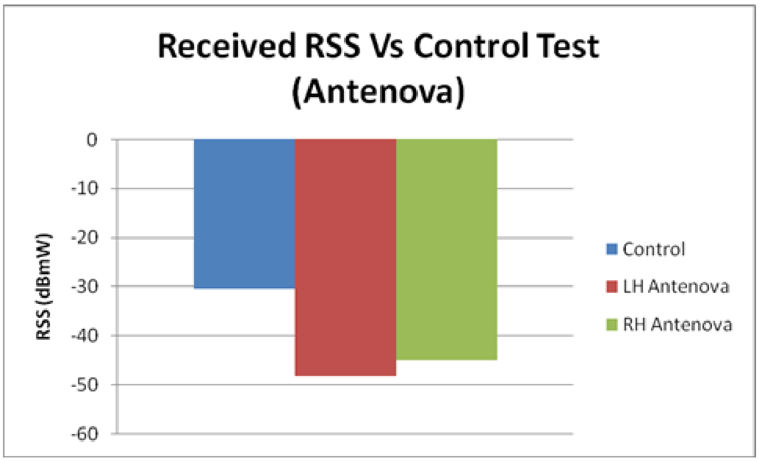


Figure 6.26: Received Signal Strength at each Antenova antenna

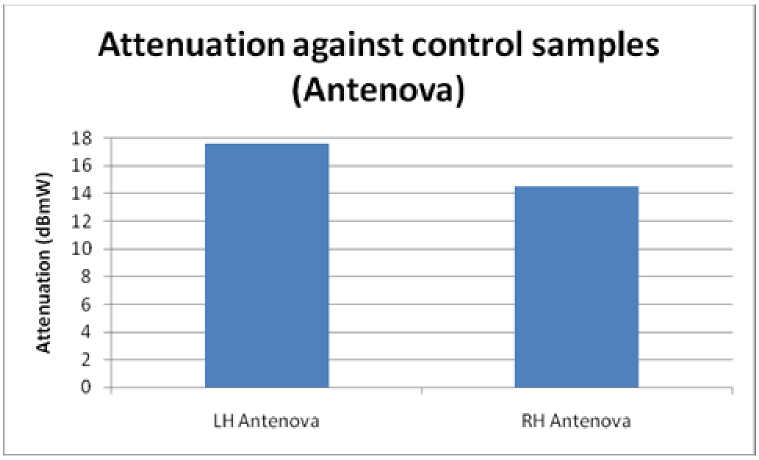


Figure 6.27: Attenuation at each Antenova antenna vs the control samples

The final measurements for this evaluation are shown in Figures 6.28 and 6.29. They show the received signal strength for the left hand and right hand Murata antennas vs the control antenna placed outside the CIT box. As with the two previous antennas, the signal strength at the left and right antennas is subtracted from the control antenna strength to show loss at each antenna due to the CIT box.

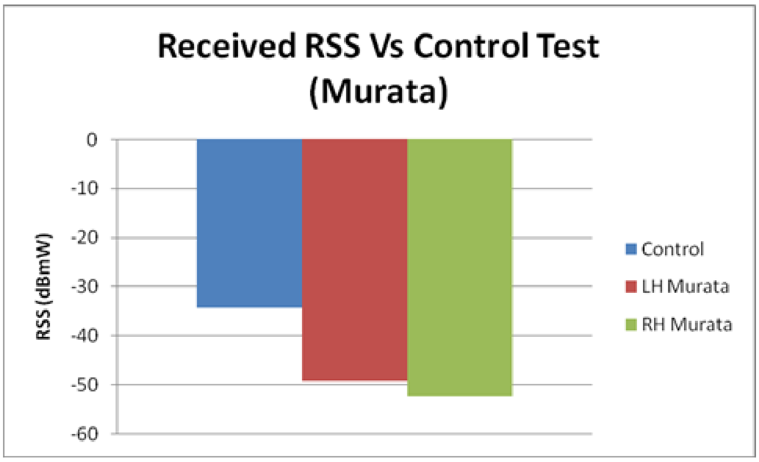


Figure 6.28: Received Signal Strength at each Murata antenna

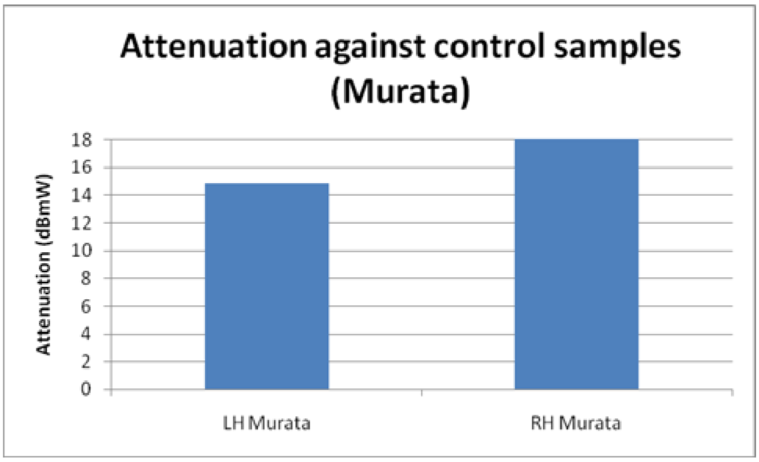


Figure 6.29: Attenuation at each Murata antenna vs the control samples

The following figures 6.30 and 6.31 show a comparison between each of the three antennas compared by left and right. The intention of this is to provide direct comparison between each of the antenna types to determine the best antenna to use for further testing in later research.

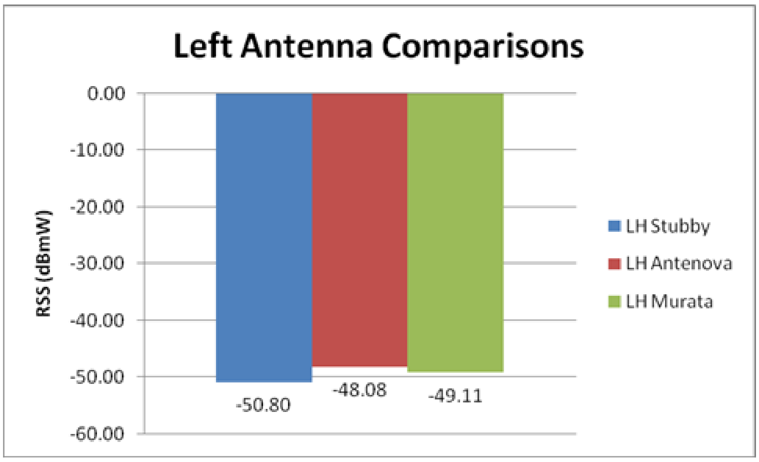


Figure 6.30: Comparing the left hand antennas by type

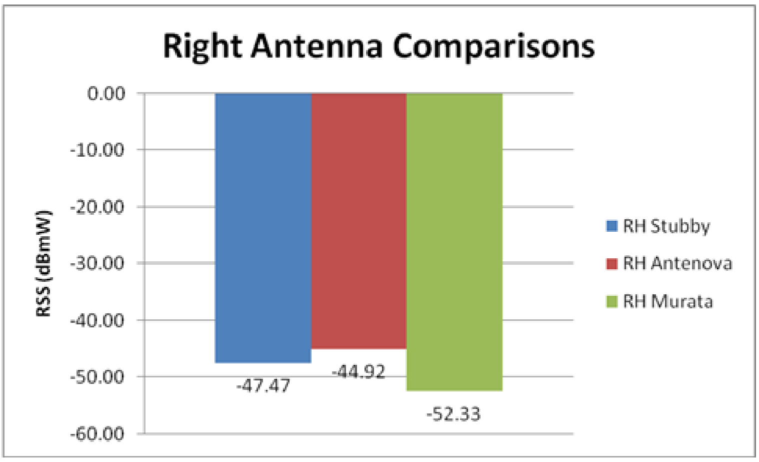


Figure 6.31: Comparing the right hand antennas by type

6.3.4.2 Practical Evaluation

The results of the two practical scenarios tested and described in 6.2.4 and 6.2.4.2 are shown below. For the testing with the CIT box in shrubbery, Figures 6.32 and 6.33 show the received signal strength for the left and right Stubby antennas, Figures 6.34 and 6.35 show the signal strength with the Antenova antennas and Figures 6.36 and 6.37 show the signal strength for the Murata antennas within the shrubbery.

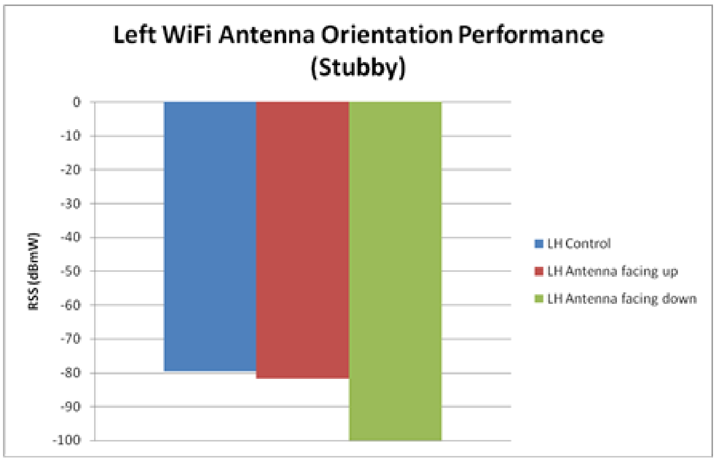


Figure 6.32: Left Hand Wi-Fi Stubby Antenna performance in the shrubbery experiment

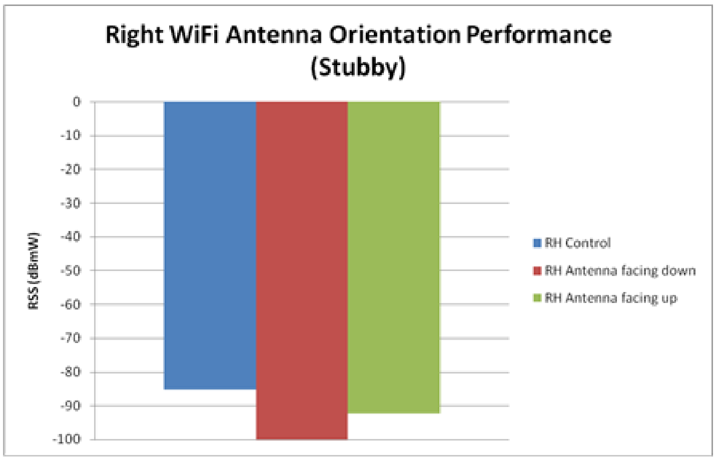


Figure 6.33: Right Hand Wi-Fi Stubby Antenna performance in the shrubbery experiment

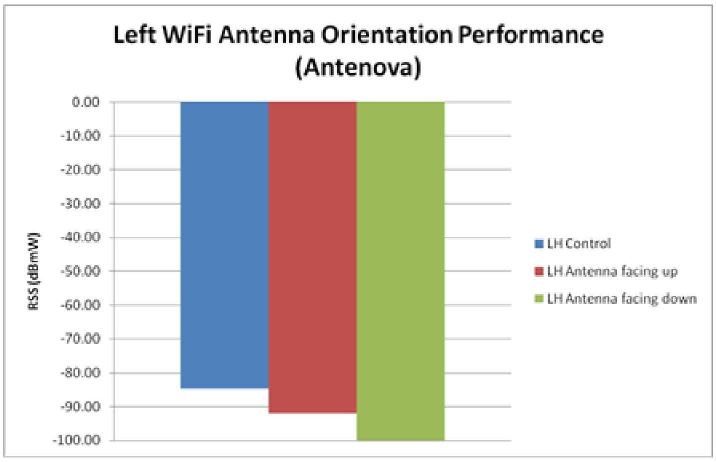


Figure 6.34: Left Hand Wi-Fi Antenova Antenna Performance in the shrubbery experiment

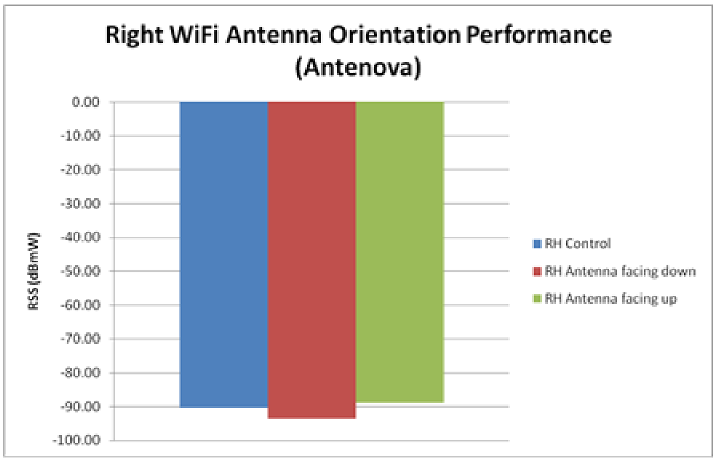


Figure 6.35: Right Hand Wi-Fi Antenova Antenna Performance in the shrubbery experiment

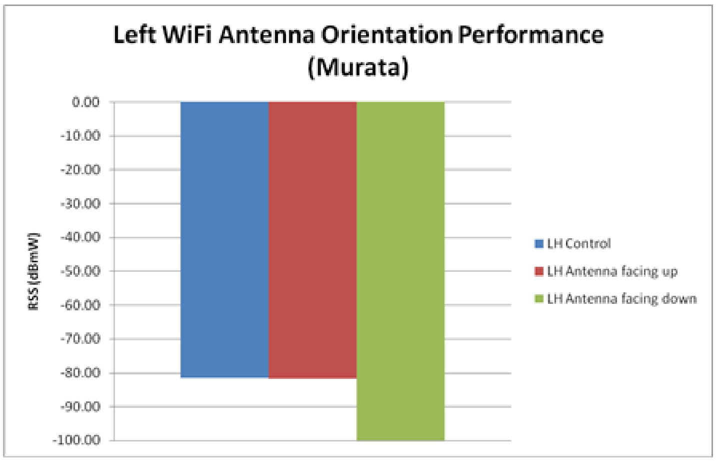


Figure 6.36: Left Hand Wi-Fi Murata Antenna performance in the Shrubbery experiment

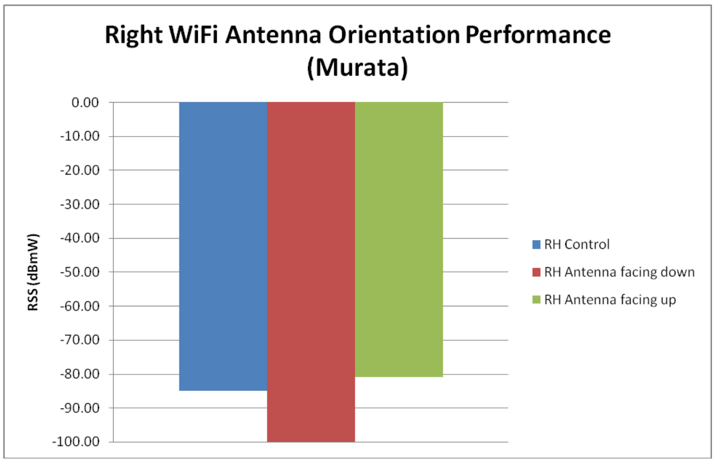


Figure 6.37: Right Hand Wi-Fi Murata Antenna Performance in the Shrubbery experiment

The results of the practical scenario evaluation involving a skip are shown below. As above, Figures 6.38 and 6.39 show the received signal strength for the left and right Stubby antennas, Figures 6.40 and 6.41 show the signal strength with the Antenova antennas and Figures 6.42 and 6.43 show the signal strength for the Murata antennas within the skip experiment.

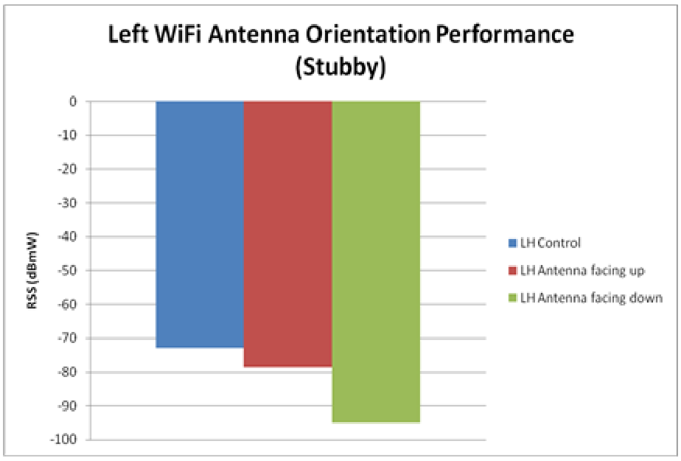


Figure 6.38: Left Hand Wi-Fi Stubby Antenna Performance in the Skip experiment

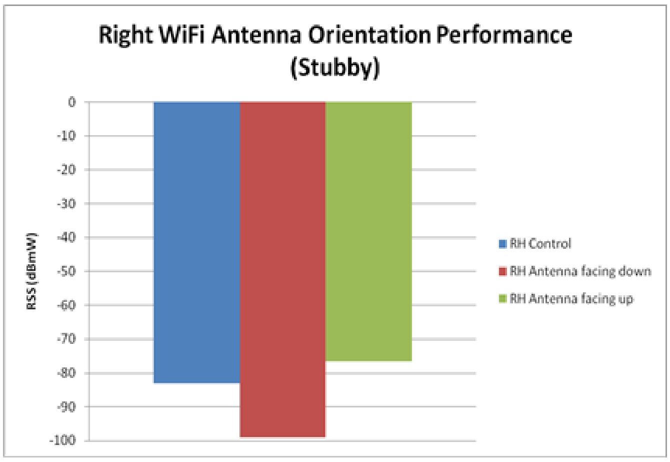


Figure 6.39: Right Hand Wi-Fi Stubby Antenna Performance in the Skip experiment

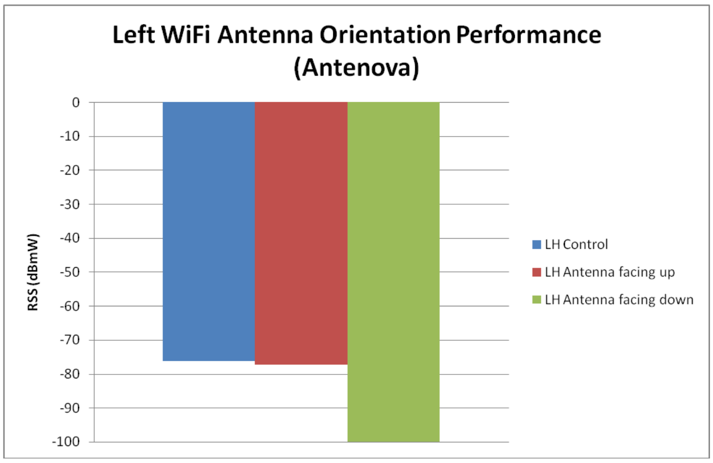


Figure 6.40: Left Hand Wi-Fi Antenova Antenna Performance in the Skip experiment

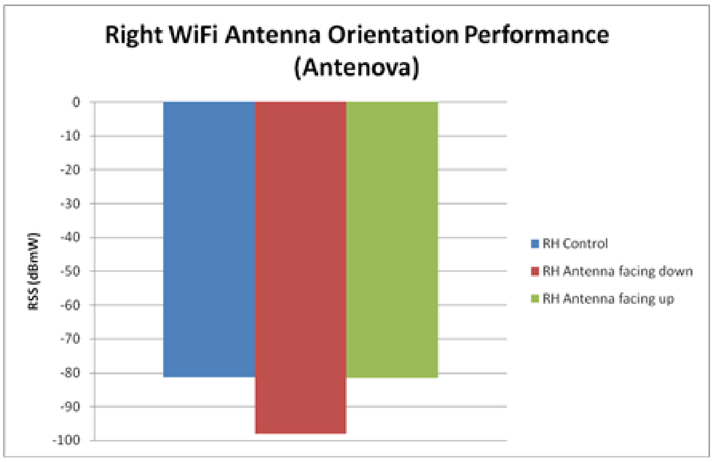


Figure 6.41: Right Hand Wi-Fi Antenova Antenna Performance in the Skip experiment

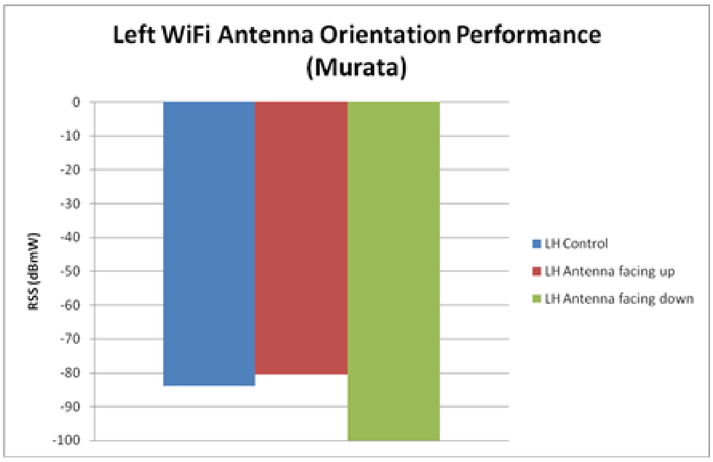


Figure 6.42: Left Hand Wi-Fi Murata Antenna Performance in the Skip experiment

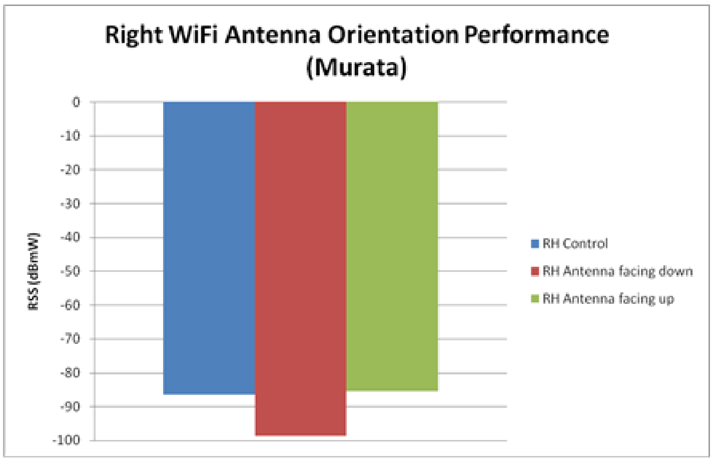


Figure 6.43: Right Hand Wi-Fi Murata Antenna Performance in the Skip experiment

6.4 Discussion of Results

The research that has been presented in the preceding sections of this chapter has demonstrated factors that can affect antennas placed on CIT cash boxes. The research has also shown the advantages of using antenna diversity switching to enhance Wi-Fi signal reception with CIT boxes. This final section of Chapter 6 will discuss the results from the research presented above and will provide recommendations for forthcoming research based on these results.

With the antenna evaluations in sections 6.2.1 and 6.3.1, comparisons of Figures 6.12 and 6.13 show that the free standing stubby antenna appears to perform close to the datasheet’s specifications. A minor discrepancy appears between peak return losses, as the datasheet shows the peak return loss at 2.45GHz where the practical tests show the peak return loss at 2.46GHz. This can be due to manufacturing differences but is more likely to do with differences between the experimental setup used in this study and the experimental setup used by the manufacturer. Regardless, this antenna is matched at 50Ω and is an effective radiator at most of the Wi-Fi bands which are shown by the two red vertical lines in Figure 6.12.

When the Stubby antenna is placed in the acetal locator, the antenna appears to be detuned and the bandwidth of the antenna increases. However, even with this detuning, the stubby antenna is not a bad performer between 2.41GHz and 2.46GHz where Channels 1-11 reside. At Channel 1 the return loss is -19dB which means only around 2-3% of the power is reflected. At Channel 11 this return loss is around -16dB which means 6-7% of the radiated power is reflected. These are not terrible performance figures and the Acetal locator naturally tunes the antenna to operate more efficiently towards Channel 1 of the Wi-Fi band where it would naturally perform best at Channel 11 according to Figure 6.12.

When installed on the CIT box, the Stubby antenna’s performance is further compromised. Across Channels 1-11 23% of the power is reflected and hence the antenna’s efficiency is significantly reduced. Where 23% of the power is reflected just by mounting the antenna to the CIT box, there is no tolerance for practical situations where the CIT box might be placed near a device that detunes it further. This will reduce the antennas performance further which makes it less useful in practical situations.

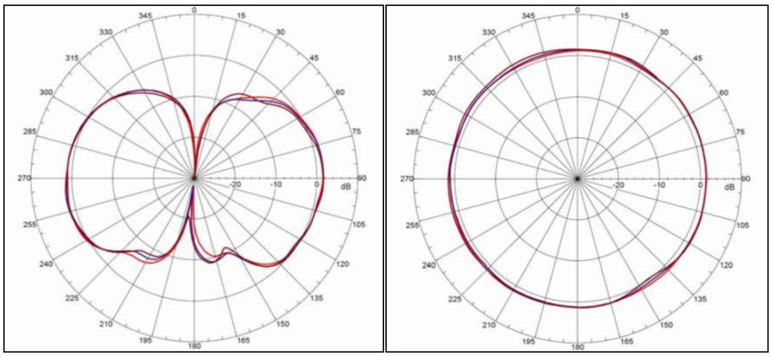


Figure 6.44: Stubby Wi-Fi antenna radiation pattern

Figure 6.44 above shows the propagation characteristics of the Stubby antenna. This information is extracted from the component’s datasheet and is not subject to research by this thesis but it serves as an indication of the capabilities of the antenna which is another factor in antenna selection. The radiation pattern for this antenna is not too bad when compared to an isotropic antenna. It would appear to be a very effective radiator but it is beyond the scope of this thesis to determine the radiation characteristics of this antenna when installed on the CIT box.

The second type of antenna that was tested is the Antenova antenna. Figure 6.16 shows the Antenova antenna tuned as close to 50Ω as possible. This data is compared to Figure 6.17 which is the return loss specified by the manufacturer’s datasheet. The measured return loss in Figure 6.16 is around -34dB and that figure is comparable to the -33dB from the product datasheet shown in Figure 6.17. A noticeable difference is the frequency at the peak return loss shown in Figure 6.16 is at 2.48GHz where the datasheet shows the return loss peaking at 2.45GHz. At this return loss the reflected power is less than 0.001%, making it a very efficient antenna, albeit not at the optimum frequency in this setting.

When installed in the acetal locator, this antenna remains well tuned with no evidence of compromise of the antenna’s bandwidth as shown by Figure 6.18. The compromise for this installation is that the peak return loss frequency has shifted to 2.40GHz and the return loss at 2.45GHz is -10dB. This does mean that 10% of the power will be reflected back at 2.45GHz and this only gets worse as Wi-Fi channel 11 is approached. Overall, the acetal locator may not compromise the antenna’s bandwidth but it does affect the efficiency of the antenna towards the higher Wi-Fi bands.

With the Antenova antenna installed on the CIT box there is a small but positive effect on the antenna as the peak return loss frequency is shifted from 2.40GHz to 2.42GHz, as Figure 6.19 shows. Looking at the return loss of this setup, the antenna would perform best between Channels 1 and 9 but Channel 11 would see a 10% power loss. This 10% power loss is not ideal but it is not a bad compromise for this antenna.

Although the research performed with this antenna does not cover investigations into the propagation characteristics of the Antenova antenna, they are worth discussing. The characteristics of this antenna are not far from the ideal isotropic antenna if the datasheet holds true. Figure 6.45 below shows the radiation pattern for this antenna according to the datasheet. Properly tuned, this antenna looks quite promising given its radiation pattern and the performed research as the CIT box seems to have a lesser and more predictable and effect on its performance when compared to the Stubby antenna.

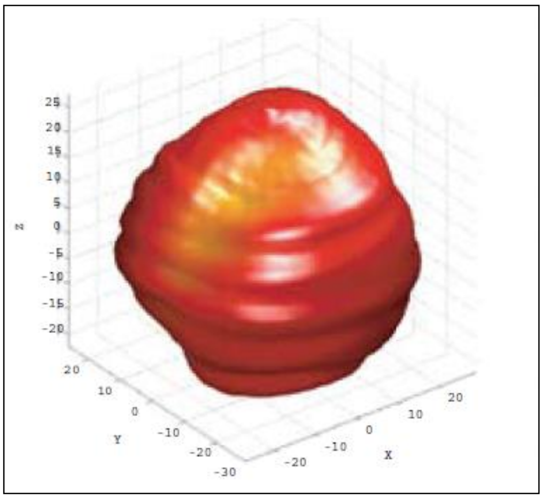


Figure 6.45: Antenova antenna’s radiation pattern

The third and final type of antenna researched is the Murata antenna. Evaluation results shown in Figure 6.20 show that the return loss characteristics of the Murata antenna reflect those of the datasheet reasonably well; however, the tuning of the antenna is towards the higher Wi-Fi channels, thus compromising the antenna’s performance at Wi-Fi Channel 1. Figure 6.21 shows the device datasheet’s radiation characteristics of the Murata antenna. The practically measured return loss shows at 2.46GHz only 0.2-0.3% of the power is reflected back to the transmitter which comparable with the return loss at that frequency shown by the product datasheet.

When installed in the acetal antenna locator, the Murata antenna is detuned even after already being tuned with an inductor on the fine tuning element. This effect of the Acetal locator is so pronounced that the return loss at 2.46GHz drops to -2.8dB from -27.8dB when the antenna was free standing. This means that nearly 53% of the signal is being reflected back to the transceiver device. Figure 6.22 shows this effect. It is possible that the antenna can be re-tuned but with such a large shift from the required band the coarse tuning element would need altering which would have required a PCB modification.

Figure 6.23 shows the effect of the CIT box on the Murata antenna when installed. There appears to be minimal improvement to the antenna’s function, which means the CIT box does not particularly affect this antenna and the Acetal locator affects the antenna the most. The performance of this antenna at best appears to reflect 25% of the power with 50% reflection being the worst as the frequency increases toward Wi-Fi Channel 11. This is far from optimal and these tests show that the Murata antenna will not perform well in field testing.

As with the Antenova and Stubby antennas, it is worth mentioning the propagation characteristics of the researched antenna. Figure 6.46 below shows the radiation pattern for the Murata antenna and it does not appear to be as good as either the Antenova antenna or the Stubby antenna, which, combined with its performance when installed on the CIT box, makes this antenna the least favourable antenna for further research.

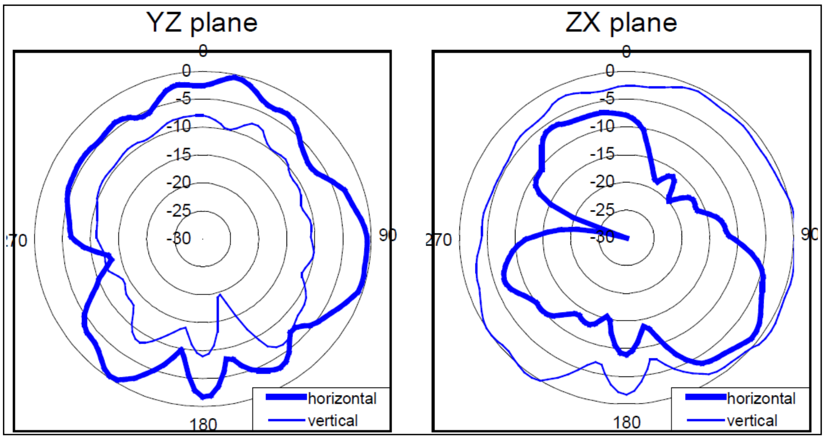


Figure 6.46: Murata antenna's radiation pattern

In conclusion to this portion of the research, it is obvious that the CIT box and antenna locators have a big effect on the performance of Stubby antennas. These effects can be accounted for by tuning the stubby antenna when in the CIT box but this would require additional hardware and cost.

The Murata antenna's performance is degraded by the introduction of the Acetal locator to its near field. The return loss measurements performed on the Vector Network Analyser show that a large amount of transmitted power is reflected back to the transceiver affecting its sensitivity. It also has the worst radiation pattern of the three antennas tested.

The best performer of all is the Antenova antenna. It seems relatively unaffected by the Acetal and re-tunes to a useable frequency when introduced to the CIT box. It is heavily reliant on the ground plane under the Antenna and it so it has the largest form factor of the two PCB mounted antennas. Properly tuned, good performance can be expected from this antenna because of its radiation pattern.

Section 6.3.4.1 evaluates the effectiveness of antenna diversity when used with a CIT box. The first experiment with the stubby antenna reveals a 3dB difference in signal strength when comparing the RSS of the two antennas. This 3dB difference in the RSS between the two antennas can be a result of surrounding obstacles reflecting the signal or the location of the CIT box combined with the propagation characteristics of the antenna when installed on the CIT box.

With the Antenova antenna, there is also a 3dB difference between the two antennas. There is also 17dBs of attenuation at the left antenna compared to the control but like the stubby antenna there is less attenuation at the right antenna compared to the control which provides consistency and confidence between the two tests.

The Murata antenna exhibits the same 3dB difference between the left and right hand antennas but the difference between the Murata antenna and the other two researched antennas is that the left hand antenna is the better performer in this case rather than the right hand antenna. This can potentially be explained by reflections from surrounding obstacles or more likely, propagation characteristics of the antenna.

Figures 6.30 and 6.31 show the Antenova antenna performs better when using the same setup. Comparing the Antenova antennas to the stubby antenna there is a 2.5-2.7dB improvement by using that antenna. Comparing the Murata antenna to the stubby, there appears to be a 1.8dB increase in RSS on the Murata antenna but on the right antenna there is a -5dB loss in the Murata antenna. This could be due to environmental factors or the propagation characteristics of the antenna.

In 6.3.4.2, the evaluation of the practical scenarios, the results of the tests that involved placing the CIT box in shrubbery show that the antennas not facing the ground record a signal strength comparable with that of the control tests. What is observed is that there is a significant advantage with using an RF switching device to switch between two Wi-Fi antennas. The results show that in the instances where no signal was detected on the antennas facing the ground, the antennas on the opposing side were able to detect a signal. What this means for the tracking system is that in a worst case where one antenna is compromised completely, the other antenna would be able to provide enough function to perform what is required of it in the tracking solution. This helps with the requirement to make a robust tracking system for CIT. Between antenna types, the results show that reception with the Antenova antenna is better than the Stubby and the Murata antennas and in situations where there is low signal strength the Antenova antennas may provide an advantage over the others.

With the testing that involved placing the CIT box in a skip, there were issues that affected the results of the antenna type comparisons. Variations in the weather at the time of testing did not allow for reliable comparisons to be made. The tests were not re-run as this information serves to prove a point that environmental conditions can affect wireless signals which in turn can affect the capability of Wi-Fi receivers to detect weak signals or provide repeatable results.

Despite this environmental setback, the benefits of using the RF switching device can still be evaluated. In all instances but one, the Wi-Fi antennas facing the skip enclosure would not detect the transmitting access point and would certainly not permit any data transfer through this antenna. The antennas facing away from the skip enclosure detected the transmitting access point and the signal strength was comparable with that of the control antenna; in the case of the right stubby antenna facing away from the skip enclosure, its performance was better than that of the control.

6.5 Conclusions

This Chapter introduces the CIT box and the effects that it has on the 2.4GHz Wi-Fi Radio Frequency. Several antennas have been evaluated with the Antenova antenna providing the best performance when installed in the Acetal locator on the CIT box. The overall outcome from the Antenna diversity practical shrubbery and skip testing showed that significant attenuation is seen on the antenna that is facing the ground or metal skip as expected. With Antenna diversity it was shown that Wi-Fi signals could be detected on the opposing antenna therefore making Antenna diversity an invaluable asset that can assist with providing the robust tracking solution that the CIT industry requires.

7. Tracking and Theft Detection of a CIT Box

7.1 Tracking and Theft Detection Concepts

The preceding chapters talk about tracking solutions for CIT, the requirements of a tracker, state of the art technologies that are used in tracking today and how antennas can affect a CIT box. This chapter introduces novel tracking solutions for the CIT industry that will provide them with the solution that they demand. Furthermore, preliminary testing has been performed to evaluate the practical feasibility of each of these new and novel methods of tracking a CIT box, and the testing is detailed in this chapter. Below are four methodologies of tracking a CIT box.

Each concept is introduced and the testing method to prove the concept is described. The evaluation results show that each concept provides novelty to the CIT industry as well as a capability for location detection of the CIT box. Only one of these concepts focuses entirely on a wide area and global solution but all concepts focus on the use of Wi-Fi technologies to implement the tracking solution.

The reason that this chapter does not focus on location technologies such as GNSS or GSM location is because these technologies are proven entities and are easily implemented as a bolt-on modular solution to any tracking system that CIT may require. The purpose of this chapter is to demonstrate novel research that goes beyond the current state of the art. In fact, Chapter 7 will show that the use of a GSM communication module is required to transmit data back wirelessly to a central server which can then process data acquired through the Wi-Fi tracking methods.

Four concepts are presented and evaluated below in the work in this chapter and are the:

- *Theft Detection* Concept
- *Safe Zone* Concept
- *Profile Tracking* Concept
- *Non-Proprietary Access Point Tracking* Concept

These four concepts add Novelty to the CIT industry’s bespoke tracking solution through the concepts developed, introduced and tested below while the four concepts are supported by a published patent (Kosmas et al, 2011) and a pending Wordwide patent.

7.1.1 *Theft Detection* Concept (Delivery From Van to Destination and Reverse)

The first of the four concepts is designed to detect the theft of a CIT box. The concept is shown in Figure 7.1 and involves using two Wi-Fi transmitting access points and a Wi-Fi transceiver within the CIT box. The first transmitting Wi-Fi access point is placed in the delivery vehicle with the antenna mounted externally to the vehicle for good coverage. The second transmitting Wi-Fi access point is located at a delivery location in an area where the CIT box will be opened such that the cash contents can be handled. CIT box is equipped with a small laptop installed inside it which was in constant communication with a Wi-Fi device which converts serial communications to Wi-Fi. The CIT box is equipped with antennas installed on the CIT box within the antenna locators as described in Chapter 6. This laptop based setup within the CIT box is known as the tracker.

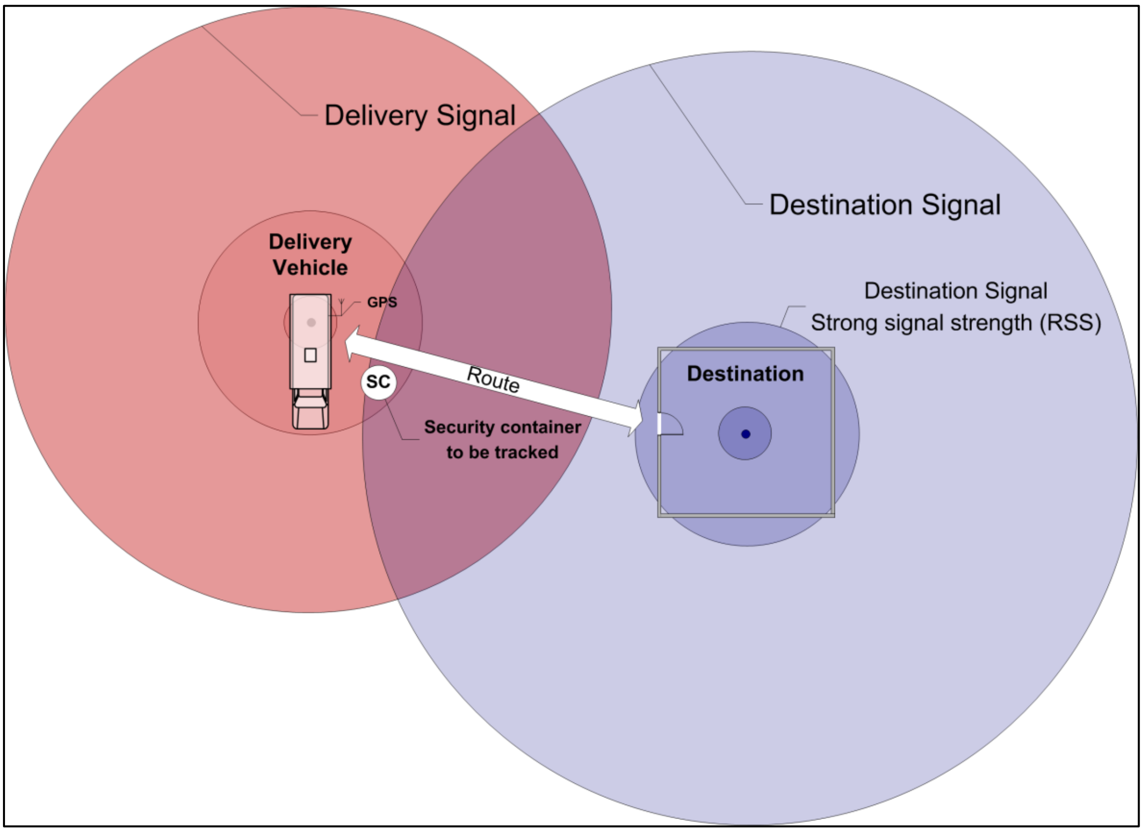


Figure 7.1: *Theft Detection* concept (Van to Destination)

The operation of this *Theft Detection* concept is simple and involves the delivery vehicle parking at the delivery location and the Wi-Fi tracker within the CIT box is woken once the CIT box is ready to be removed from the vehicle. This is ideally performed automatically by the CIT box. Once awake, the tracker starts scanning for visible wireless access point broadcast beacons. It extracts the Medium Access Controller (MAC) address from each of the beacons and compares them to a list of ‘Friendly’ MAC addresses within the tracker’s internal database. As the tracker is within the delivery vehicle, it detects the delivery vehicle’s MAC address through the Delivery signal’s broadcast beacon and it classes itself as ‘Safe’ because it is within the range of the delivery vehicle’s access point.

The same procedure is performed with the Destination signal which is found through proximity of the CIT tracker to the delivery destination which as mentioned, also has a transmitting Wi-Fi access point. The tracker separates the Destination signal into two classes: ‘Safe’ and ‘Not Safe’. The ‘Not Safe’ classification means that the tracker has detected the presence of the Destination signal but it does not believe it is close enough to the destination to class itself as ‘Safe’. The ‘Safe’ classification is where the tracker believes that it is close enough to the Destination signal to know that it is at the point of delivery where the contents of the CIT box will be handled safely.

Regarding the security status of the tracker, the tracker does not consider itself under threat if it can detect the Delivery Signal or the ‘Safe’ Destination signal. If the tracker see’s the ‘Not Safe’ classification, it does not consider itself under threat but it is at a heightened level of security as it knows that it is in transition.

This situation only occurs when the tracker is far enough from the delivery vehicle to not see the Delivery Signal.

If the tracker does not see either the Delivery signal or the Destination signal, it assumes a security breach and that it has been stolen. The tracking system can then enable more wide area and global tracking systems that it has as part of the bespoke solution and will allow a remote operator to start tracking the CIT box, pre-empting that it is under attack. Using this methodology and proprietary equipment, the tracking system can detect where it is between two trusted entities and intelligently implement a theft detection system. It is also capable of tracking its path between two locations.

The weakness in this methodology is the spoofing of wireless access points. As we have mentioned in previous chapters, it is relatively easy to spoof a wireless access point and this poses a significant issue with this *Theft Detection* concept. If the Delivery signal is spoofed then the CIT box can be stolen and the tracker will not appreciate that it is in this situation. This will allow an attacker to take the CIT box to a location where they can attack the CIT box without fear of interruption. This is a worst possible situation for a CIT box to be in because it allows the attacker the grace of time to try and defeat the CIT box's primary defence mechanisms.

A cost effective way around this spoofing is to implement a timeout with the expectation of seeing the destination within a maximum time. This is not an unreasonable solution as the timeout would act as a secondary security feature in the event that a CIT box is abandoned within the confines of the Delivery Signal.

Another technique that would eliminate the weakness due to spoofing is to introduce a handshaking procedure between the access points. As the Delivery and Destination access points will be CIT proprietary access points, connecting and authenticating them will not be an issue. This will eliminate the spoofing weakness but it will add cost to each proprietary access point and will also add timing overheads to the delivery which can make the solution less desirable.

The inherent strengths of this *Theft Detection* concept are that attacks to the radio system will fail safe and the CIT box will elevate its security level and prepare its wider area tracking systems. Such attacks are signal jamming attacks as tested with Wi-Fi signals in Chapter 5, and sabotage of the power systems to the Delivery and Destination transmitters. The fail safe in these cases are the removal of the transmitting signal and the CIT box will react by assuming a security breach.

An advantage of this *Theft Detection* concept is that it helps maintain the CIT industry's requirement to maintain the service lifetime of the CIT box by reducing power consumption of the tracking system. A good indication of this advantage is that the local tracking of the CIT box through the *Theft Detection* concept allows the wider area tracking systems to remain in a powered down state, thus reducing power consumption as they are not necessary. As mentioned above, when a security breach is detected using this local tracking *Theft Detection* concept, the tracker's wider area tracking systems are enabled as they are now required. This concept shows how a bespoke local tracking system operating in a manner that detects its location through proprietary access points and can add value to enhance the bespoke tracking solution that the CIT industry requires by detecting theft.

7.1.2 *Safe Zone* Concept

Having introduced the concept and operation of the *Theft Detection* concept, the next concept to introduce is that of the *Safe Zone*. This has already been touched upon when introducing the destination signal in the *Theft Detection* concept. The concept is shown visually in Figure 7.11.

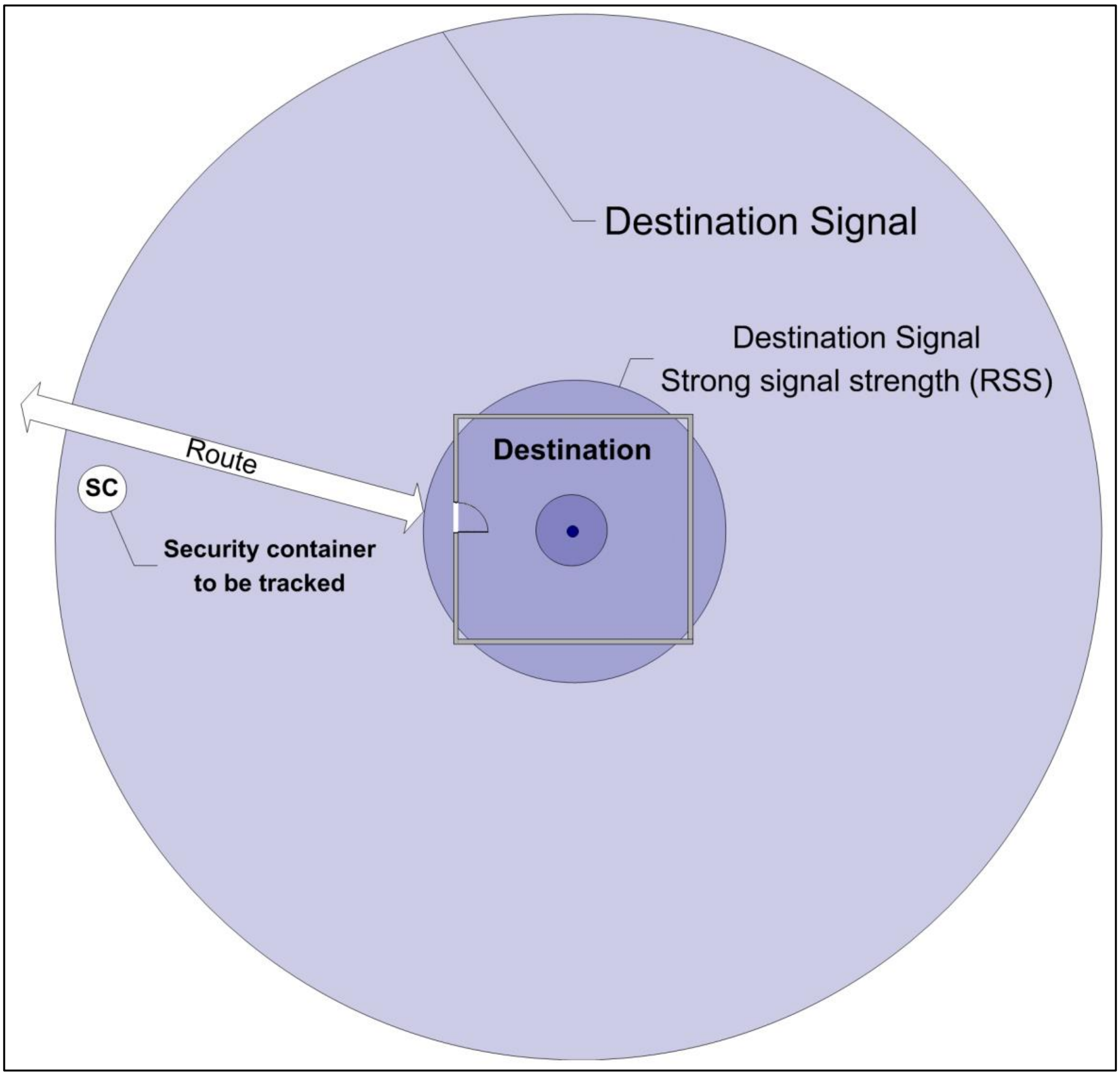


Figure 7.11: *Safe Zone* concept using the Destination signal strength

The concept is that the destination signal has a dual use for the tracking system where the first use is that described by the *Theft Detection* concept. The second use is where the signal is strong enough for the tracker within the CIT box to have enough confidence that it is close to the Destination transmitter. When the tracker establishes that it is close enough to the Destination transmitter, it initiates communication with it to establish its authenticity. If the tracker successfully authenticates with the Destination transmitter, it believes that since the signal strength of the Destination signal is high and that it is a valid proprietary transmitter, then the CIT box is very close to the point of delivery where the contents of the CIT box will be handled.

The tracker considers itself ‘Safe’ as the cash is about to be handled and it can reduce its tracking rate or suspend its tracking activities altogether. The advantages of using this *Safe Zone* system are that it helps to reduce the power used by the tracking system when it is not required. There is no need for the tracking system to be checking for the Delivery signal or the Destination signal if it knows it is in a safe environment. In this case, the safe environment is determined by the fact that the cash is being handled by the CIT guard in the presence of the customer; therefore the customer is assuming responsibility for the cash. Reducing the power used by the tracker helps to achieve the on-going requirement for maintaining the service life of the CIT box.

The other less direct advantage is that it can enhance the functionality of the CIT box itself by integrating the tracker’s functions into those of the CIT box. In the Destination *Safe Zone* there is no reason why the tracking system cannot signal to the CIT box to automatically unlock as it is in the presence of the customer. If the customer doesn’t want this automatic unlock feature, then the Destination *Safe Zone* can act as a verification that the CIT box is at the destination and this verification can be used by the CIT box’s controller as yet another assurance that it can unlock and expose the cash. This assurance would be used alongside the CIT box’s current authentication system which instructs the CIT box to unlock for the customer’s delivery or cash pickup.

The disadvantages of this *Safe Zone* concept are that the authentication with the destination access point can take time and impact the delivery time. Also, if the delivery access point fails, the CIT box would not allow itself to unlock and the delivery could fail. These disadvantages have to be weighed up against the advantages of the added security features from integrating the tracker with the CIT box, and maintaining a good lifetime out of the tracker by reducing power consumption. The added value of the *Safe Zone* concept uses a tracked single point location alongside intelligence within the tracker's controller to enhance the CIT box's security and to help achieve the demands placed upon the designers of the CIT industry's tracking system.

7.1.3 *Profile Tracking* Concept

This concept expands further on the *Theft detection* concept by adding flexibility to the way the concept of the localised tracking system operates. With the *Theft Detection* concept, the Delivery signal had to overlap the destination signal to ensure that the tracker did not experience a situation where it could not see either signal. In this instance, it would assume a theft and start enabling its wide area tracking systems. There are situations where it is likely that the delivery signal is far from the destination signal and the coverage area of these signals would not be adequate to ensure that the tracker does not start enabling wide area tracking systems and presuming a theft.

Such examples are deliveries to multi storey buildings or to shopping centres that have multiple outlets within a large structure. It is not possible for a delivery vehicle to park inside a shopping centre, therefore the tracking solution required by the CIT industry must be able to accommodate such deliveries without assuming that its security has been compromised.

The introduction of *Profile Tracking* is a novel way of expanding the range of the localised tracking by utilising existing non-proprietary access points to the advantage of the CIT box. The concept in Figure 7.13 below shows the CIT box (marked as AF) leaving the coverage of the delivery signal and travelling along the pre-determined delivery route. As it travels along that route, it passes a series of non-proprietary Wi-Fi access points which the CIT box detects as it is continually scanning for access points looking for the destination signal. The concept is that delivery routes are pre-determined and unlikely to change therefore the CIT box should see the same non-proprietary access points when travelling that route.

The tracker within the CIT box will have a database containing all non-proprietary access points associated with each destination. Before leaving the delivery vehicle, the appropriate destination is selected which loads the corresponding profile. The profile is a list of wireless access points that the tracker should see along its route to the Destination. As the tracker leaves the coverage of the Delivery signal, it places itself in an elevated threat state and starts looking for the non-proprietary access points associated with its destination. If it detects a number of them, it assumes it is on course and does not start enabling its wider area tracking systems as it is still within reasonably familiar territory. When the tracker approaches the Destination signal and detects this signal, it enters its ‘Non-safe’ state as it does not believe it is close enough to the destination to start enabling any *Safe Zone* functions. Once it is closer to the Destination signal it can then start authenticating with the Destination access point in accordance with the *Safe Zone* process in 7.1.2 above.

In the event that the tracker cannot associate any non-proprietary access points, it assumes a credible threat and starts to enable wider area tracking systems before it times out and finally enters full tracking and starts reporting its location to the control centre.

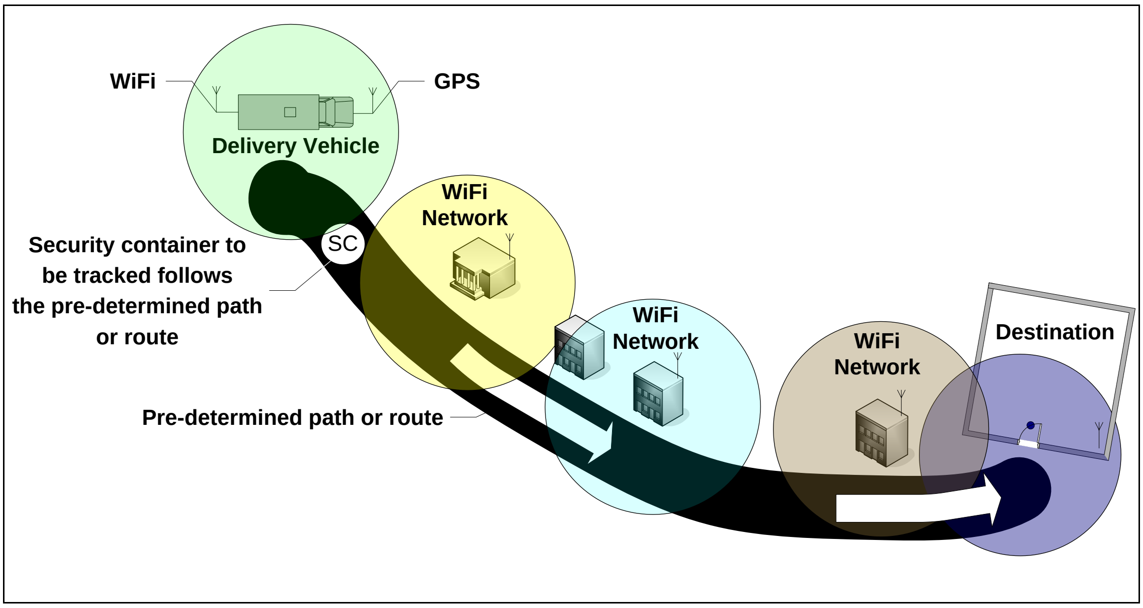

WiFi
GPS
Delivery Vehicle
WiFi Network
SC
Security container to be tracked follows the pre-determined path or route
WiFi Network
WiFi Network
Destination
Pre-determined path or route

Figure 7.13: The visual representation of the *Profile tracking* concept.

This concept has a few disadvantages associated with it. It requires a destination input to the tracker in order to load the profile, but it also requires profiles to be built and maintained in a master database. The weakness in this solution is that changes to the non-proprietary access points can affect each delivery so it is important that the *Profile Tracking* remains flexible in a manner that does not require each access point in the profile to be seen in order to function. The best solution to these issues are to make a self-adapting database where the tracker records any new access points seen along its route, waits until it has successfully completed the route and then forwards these to the command centre for approval and addition to the profile on the master database. Redundant access points along a profile would then expire automatically within the central profile database. When a tracker has its database updated, these redundant access points will no longer exist and thus a reasonably strong self-maintaining database of non-proprietary access points based Delivery profiles is built.

The benefit of this tracking method is that it expands the range of the local tracking system without using additional proprietary access points which would be expensive and physically vulnerable to attack. To ensure that the *Profile Tracking* concept is as secure and robust as possible, an overall timeout for the delivery is best implemented as soon as the tracker can no longer see the Delivery signal which is that last point at which it can assume it is safe. This will ensure that if a CIT box is stolen and the criminals have replicated the access points along the profile in an attempt to convince the CIT box that it has not deviated from its route, an overall timeout will ensure that the CIT box assumes it is under threat if it has exceeded a reasonable time for delivery. This will then cause the normal process to resume, which starts wider area tracking systems in order to assist recovery of the CIT box as quickly as possible.

7.1.4 Non-Proprietary Access Point Tracking

The concept of tracking non-proprietary access points was introduced in Chapter 4 with the introduction and evaluation of the Skyhook commercial Wi-Fi positioning service. Here we will look at how it can be utilised for the CIT industry. The purpose of this method is to use Wi-Fi access points to the advantage of the CIT box, which allows the Wi-Fi receiver to be used as a wide area and global tracking device.

With this concept, the CIT box is equipped with a GSM module and a SIM card which is capable of transmitting data over the GSM network using the General Packet Radio Service. The GSM module is used to relay the data extracted by the Wi-Fi device within the CIT box to a remote server. The remote server then handles the heavy processing and communication to the Skyhook service. From there, any location information returned from Skyhook will be handled by the back end systems as the tracker only provides unprocessed data to the back end systems.

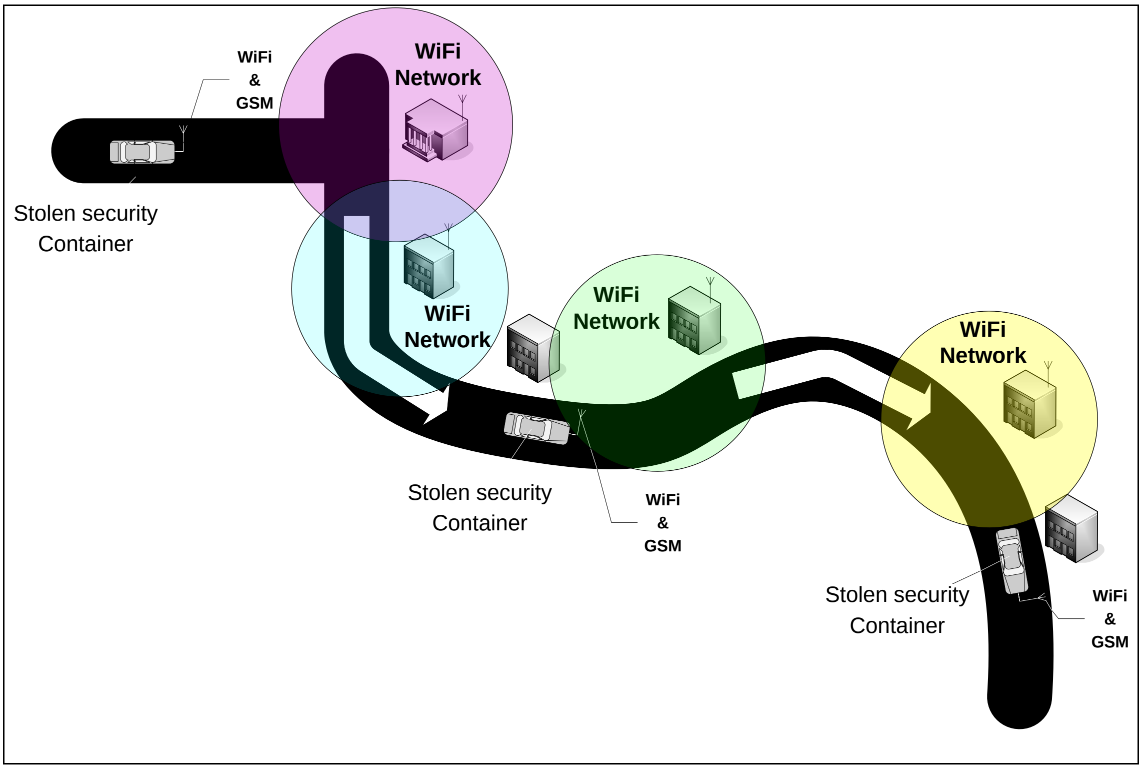


Figure 7.18: Non-proprietary wireless access point tracking of a CIT box

Figure 7.18 above visually demonstrates the concept of using the Wi-Fi receiver within the CIT box to perform *Non-Proprietary Access Point Tracking*. As it passes by several non-proprietary Wi-Fi access points, it detects the transmitting service announcement beacons, extracts the MAC addresses and uses the GSM network to send this information to a central server. The server then handles the communication with Skyhook and retrieves the necessary coordinates of the Wi-Fi access point that was near to the CIT box at the time of scan.

The greatest advantage of this tracking method is that it allows dual use of the Wi-Fi device within the CIT box. The Wi-Fi device can be used to detect theft as detailed by the concepts in 7.1.1 through to 7.1.3, and when the tracker is required to use wider area tracking methods it is able to do so with the advantages described in Chapter 4, such as indoor tracking.

7.2 Evaluation Methods for the Tracking and Theft Detection Concepts

7.2.1 Evaluation Method for the *Theft Detection* Concept

The testing for this tracking methodology required the use of a CIT box with a small laptop installed inside it. The laptop was running a custom script to communicate with a serial to Wi-Fi device also installed in the CIT box, which was instructed to scan continuously for surrounding Wi-Fi service broadcast beacons. The script running on the laptop then extracted the MAC addresses from the service broadcast beacons and logged them along with the received signal strength.

The testing involved the evaluation of 8 different delivery routes to evaluate feasible transit distances between the van and the delivery location for this concept. The delivery routes chosen for evaluation are grouped into three categories and are labelled from A through to H:

- Short distance from the delivery location (Locations: A, B)
- Medium distance from the delivery location (Locations: C, D, H)
- Long distance from the delivery location (Locations: E, F, G)

The Stubby Wi-Fi antenna was installed in the left hand antenna locator of the CIT for these tests. Two identical access points were used; one installed at the delivery location and the other installed on the delivery van. The antenna installed on the delivery van was mounted externally. For each evaluation, the van was parked where indicated in Figure 7.2, and the CIT box was carried along the delivery routes shown in Figures 7.3 to 7.10 through to the delivery point which is indicated in Figure 7.2 by the symbol ‘TX’. This is all in accordance with the short, medium and long distance delivery routes detailed above.

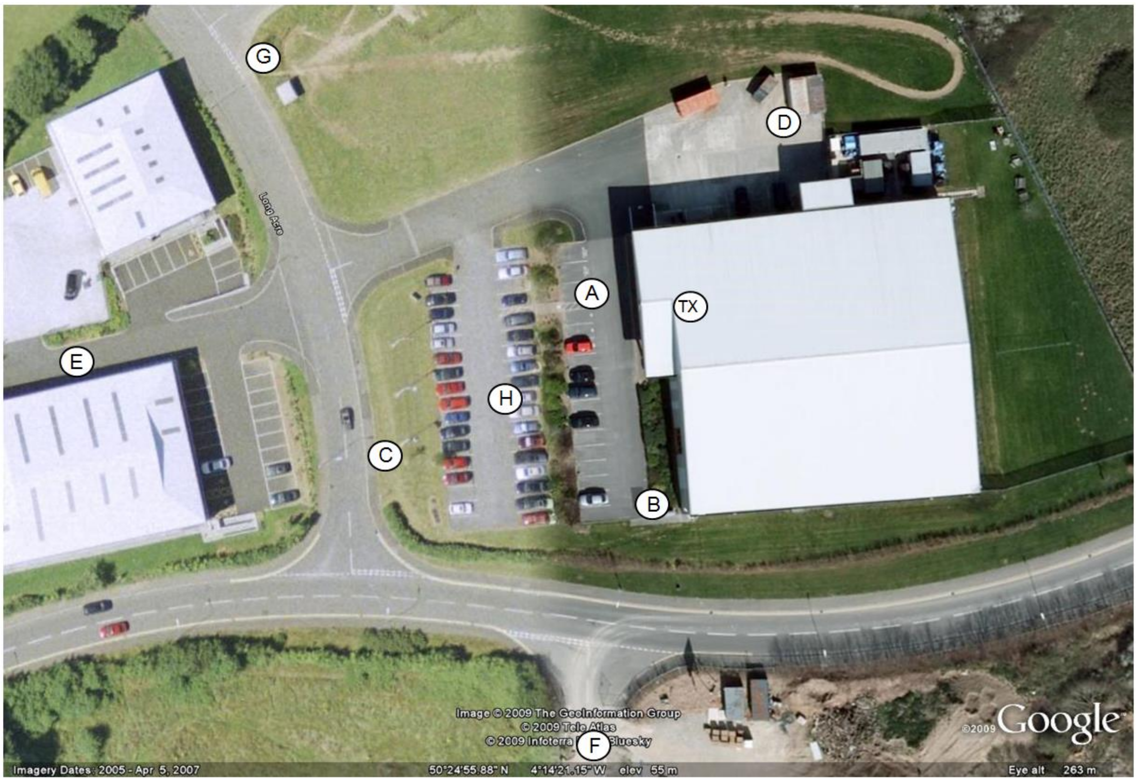

G
D
Long Acre
A
TX
E
H
C
B
Image © 2009 The GeoInformation Group
© 2009 Tele Atlas
© 2009 Infoterra Bluesky
F
©2009 Google
Imagery Dates: 2005 - Apr 5, 2007
50°24'55.88" N 4°14'21.15" W elev 55 m
Eye alt 263 m

Figure 7.2: Delivery vehicle (Van) evaluation locations

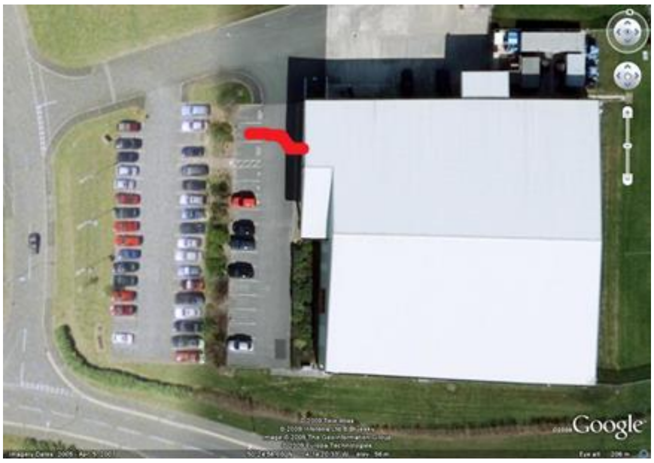


Figure 7.3: Route A

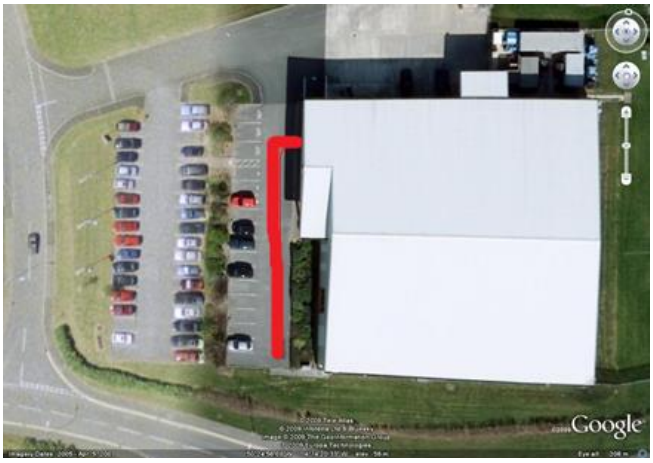


Figure 7.4: Route B

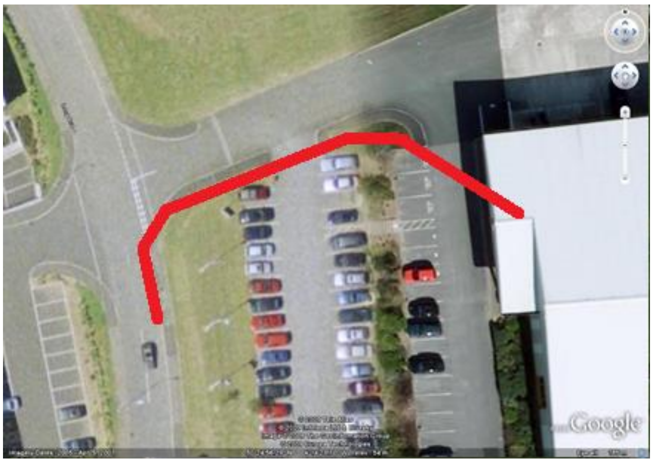


Figure 7.5: Route C

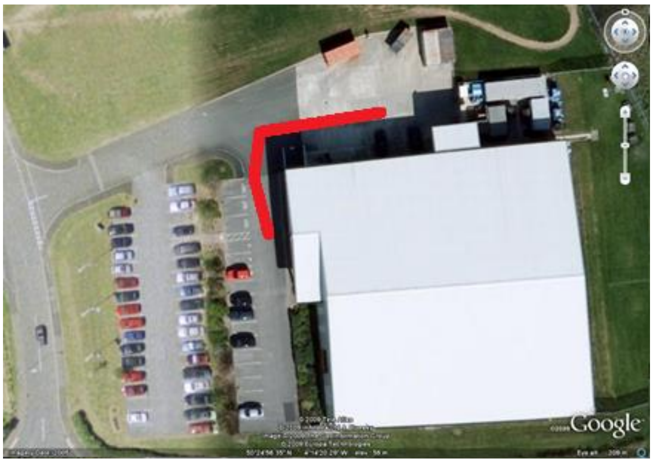


Figure 7.6: Route D

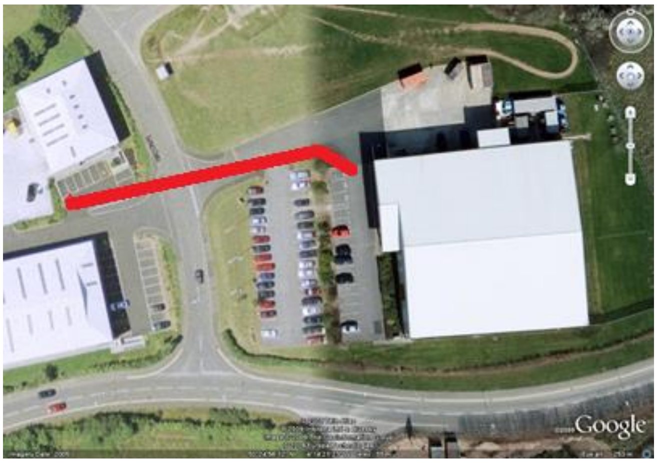


Figure 7.7: Route E

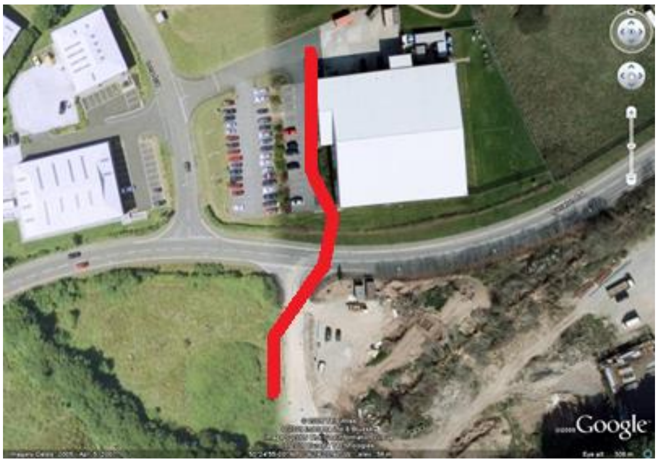


Figure 7.8: Route F

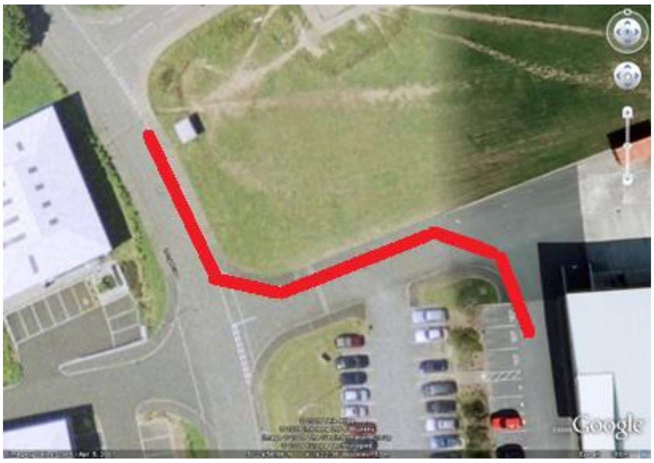


Figure 7.9: Route G

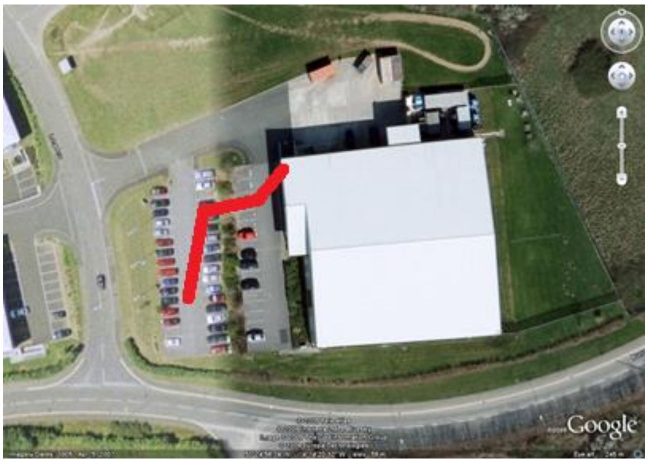


Figure 7.10: Route H

7.2.2 Evaluation Method for the *Safe Zone* Concept

The experimental setup for evaluating this *Safe Zone* concept involved the use of the same hardware setup used in 7.2.1. The purpose of the testing is to evaluate the signal strength of the destination wireless access point as the CIT box approaches it. This replicates a guard's practical routine as they approach the cash delivery point. Evaluating the signal strength will allow a profile to be established which will feed into the research for Chapter 8.

A wireless access point simulating the delivery point was installed on the ground floor of the building shown in Figure 7.12. An antenna was installed on the outside of the CIT box and an additional antenna was installed inside the CIT box. The antenna inside the CIT box is used to assess if there are any benefits of installing the antenna inside the CIT box for this application. Both antennas were connected to the Antenna diversity switching device as used in 6.2.4 and the Wi-Fi receiver within the CIT box was set to scan and record visible access points as rapidly as possible using the laptop installed with the CIT box.

During the testing, the CIT box was moved from the start point to the destination where the lid of the CIT box was then opened to simulate the cash being removed from the CIT box. Tests were performed at the following distances from the destination:

- 40m
- 20m
- 15m
- 10m
- 5m

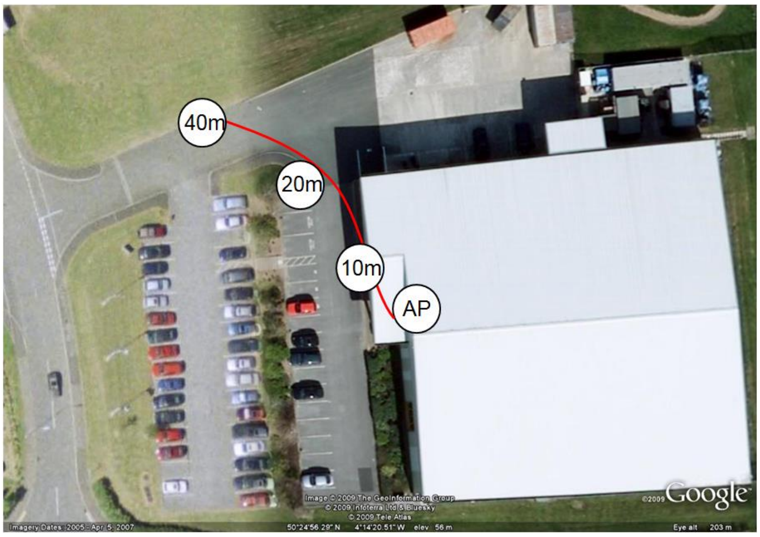

40m
20m
10m
AP
Image © 2009 The GeoInformation Group
© 2009 Infoterra Ltd & Bluesky
© 2009 Tele Atlas
©2009 Google
Imagery Dates: 2005 - Apr 5, 2007
50°24'56.29" N 4°14'20.51" W elev 56 m
Eye alt 203 m

Figure 7.12: Setup for evaluating the *Safe Zone* concept

A final evaluation was performed with this setup where the signal strength was recorded at both antennas (outside and inside the CIT box) with the transmitter at a distance of 3m from the CIT box. Signal strength was recorded with the CIT box lid closed and with the lid opened to establish a magnitude of attenuation for the antenna inside the CIT box.

7.2.3 Evaluation Method for the *Profile Tracking* Concept

The testing for this tracking method involved three tests being performed. Each evaluation was an assessment of a route which involved recording the wireless access points along the route, then using the route to extend the range of the localised tracking system. The final element of each evaluation was to start following the route from the Van and divert from that route whilst noting the response of the tracker. The idea is to gauge how far the CIT box would travel before it detects that it has diverted from its designated route.

The first test is shown in Figure 7.14 below. The van was parked and the route was recorded. The route was then retraced as shown.

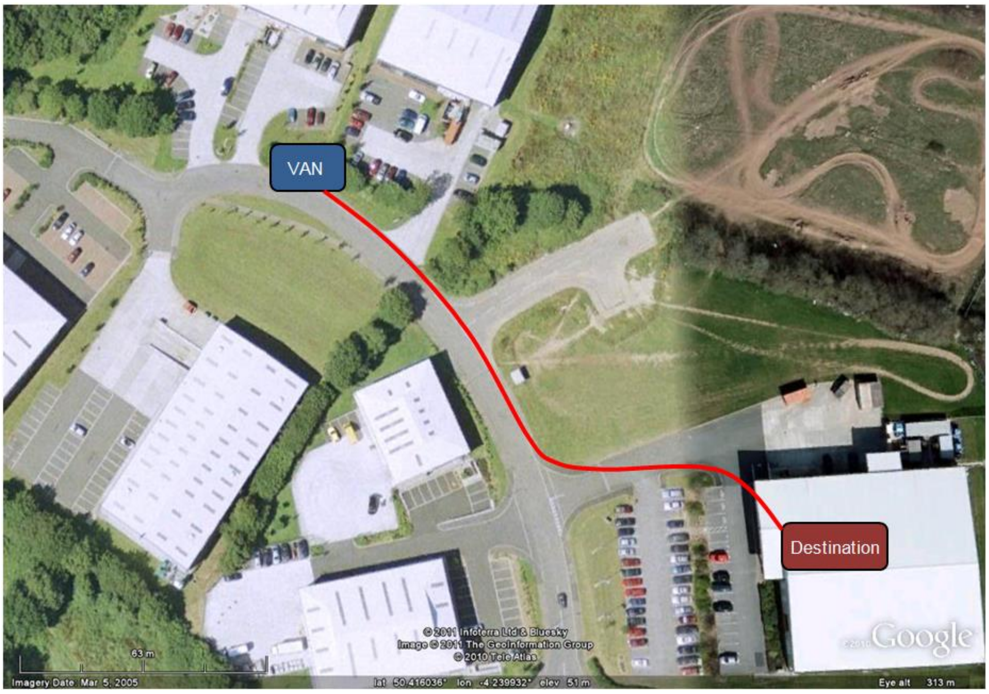

VAN
Destination
© 2011 Infoterra Ltd & Bluesky
Image © 2011 The GeoInformation Group
© 2010 Tele Atlas
Google
63 m
Imagery Date Mar 5, 2005
lat 50.416036° lon -4.239932° elev 51 m
Eye alt 313 m

Figure 7.14: *Profile Tracking* Evaluation 1 route

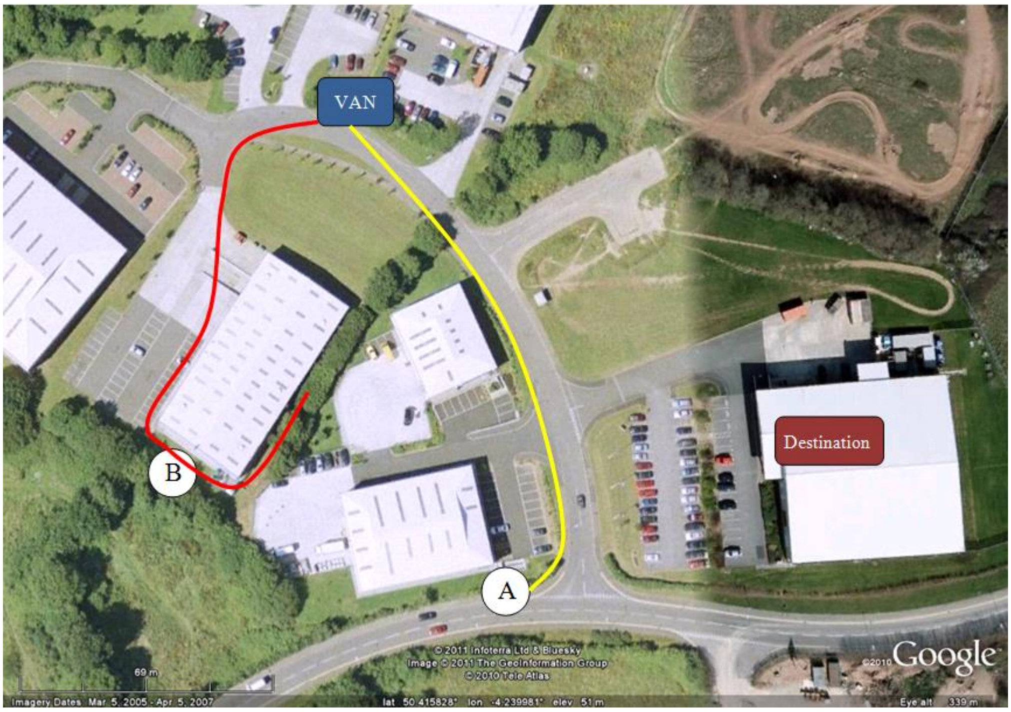

VAN
Destination
B
A
© 2011 Infoterra Ltd & Bluesky
Image © 2011 The GeoInformation Group
© 2010 Tele Atlas
©2010 Google
69 m
Imagery Dates Mar 5, 2005 - Apr 5, 2007
lat 50.415828° lon -4.239981° elev 51 m
Eye alt 339 m

Figure 7.15: *Profile Tracking* Evaluation 1 diversions

Figure 7.15 above shows two diversions from the route in evaluation 1 and the points where the CIT box indicated that the threat level was high. These two diverted routes are realistic examples of what a CIT box robber would do. In the example of the yellow route, the robber would attack the CIT guard and run to a waiting car or motorcycle. This is a more organised approach and attack. In the example of the red route, the robber would attack the CIT guard and take the CIT box to a nearby secluded area where they would try to get into the CIT box quickly in order to get as many notes as possible. This is a more desperate and disorganised attack. This evaluation uses both these examples to see if the tracking system can detect theft quickly. The markers A and B show the point at which the tracking system detected a theft.

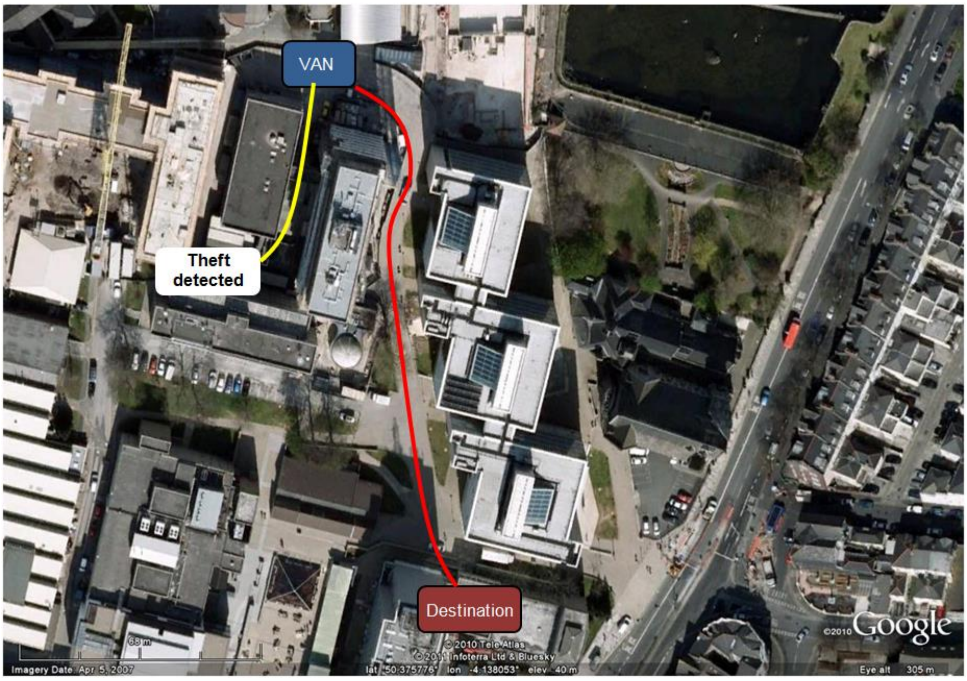

VAN
Theft detected
Destination
© 2010 Tele Atlas
© 2011 Infoterra Ltd & Bluesky
©2010 Google
Imagery Date: Apr 5, 2007
lat 50.375776° lon -4.138053° elev 40 m
Eye alt 305 m
68 m

Figure 7.16: *Profile Tracking* Evaluation 2 route and diversion

Figure 7.16 shows the second profiled route within a denser environment which provided a realistic scenario that demonstrates the concept in a shopping centre or high street. This scenario involves the device detecting a large number of Wireless Access Points and therefore testing if the tracker and the *Profile Tracking* algorithm can work within this environment. It is also worth noting that the tracker was restricted to a maximum of 30 profiles in its memory due to the software design. The route recorded and followed to the destination is shown by the red line. The diversion from the route is illustrated in Figure 7.16 as well by the yellow line.

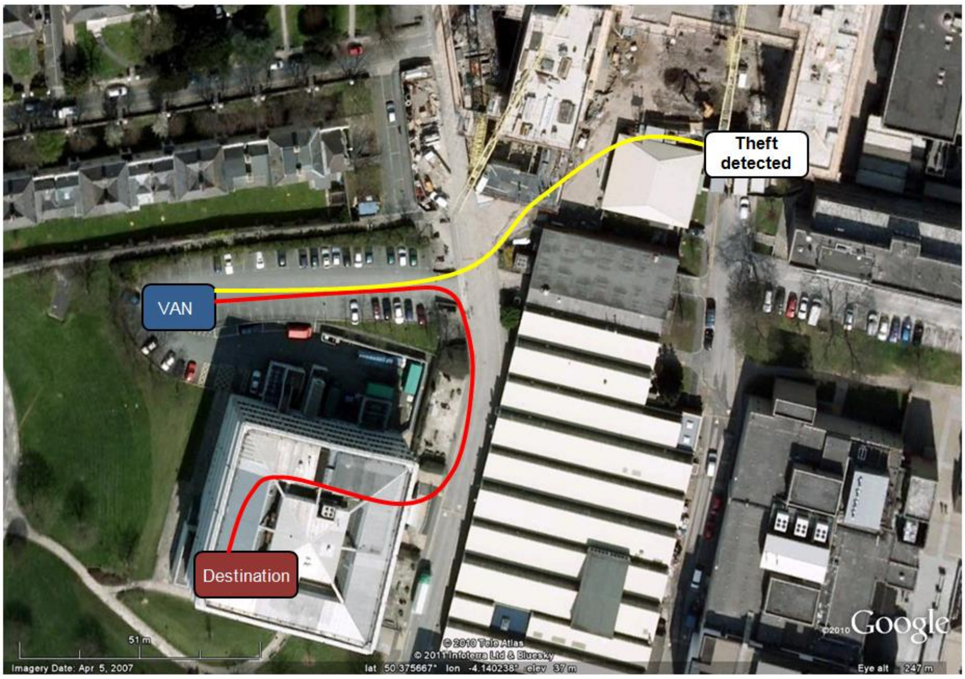

Theft detected
VAN
Destination
51 m
Imagery Date: Apr 5, 2007
© 2010 Tele Atlas
© 2011 Infoterra Ltd & Bluesky
lat 50.375667° lon -4.140238° elev 37 m
Eye alt 247 m
©2010 Google

Figure 7.17: *Profile Tracking* Evaluation 3 route and diversion

The route for Evaluation 3 shown in Figure 7.17 was selected for its length which totals 290m. It involved entering a building as the red route in Figure 7.17 shows. This was introduced to provide information on how the *Profile Tracking* concept would perform inside a building. As with the previous evaluation, the profiled delivery route is shown by the red line where the yellow line shows the diversion from the intended delivery route.

7.2.4 Evaluation Method for *Non-Proprietary Access Point Tracking*

Three experiments were performed to evaluate *Non-Proprietary Access Point Tracking*. The hardware used was a prototype system which comprised of a GSM modem, serial to Wi-Fi device as used previously and a host controller which communicated with these two devices and was limited in software to the storage of up to 30 profiles. The first experiment evaluates an urban area which is mostly pedestrianised and therefore it was walked during this evaluation. This second experiment evaluates a suburban area whilst walking, while the final of the three experiments evaluates a wider area whilst driving in a vehicle.

During the testing, a 6 second scan time was implemented for the Wi-Fi device as this was considered a reasonable tracking speed. The tracking device was kept in constant communication with the server and the results of the 6 second Wi-Fi scan would be transmitted once the necessary data such as MAC address and signal strength was extracted. The server, which was running a script developed by Spinnaker International Ltd, would then look up each Wi-Fi MAC address on Skyhook's database starting with the MAC address with the strongest signal strength. This lookup process on Skyhook's database is continued until a match is found and it was then recorded on the local database containing the latitude and longitude of each Wi-Fi location. If no match was found then no data was recorded to the database.

Figure 7.19 below shows the route followed during the first evaluation which evaluates the urban route. The route followed is shown in red and it was recorded with a hand held GPS receiver. The area itself is in the middle of Plymouth City Centre and it starts inside the city's largest indoor shopping centre and then follows the two most popular shopping streets. This is a good route for evaluating the effectiveness of Wi-Fi positioning in an area where Skyhook's vehicles are not allowed to go. This route is also representative of a situation that a robber may take advantage of as there are many CIT deliveries that take place in this area and the pedestrianised area can act in the robber's favour.

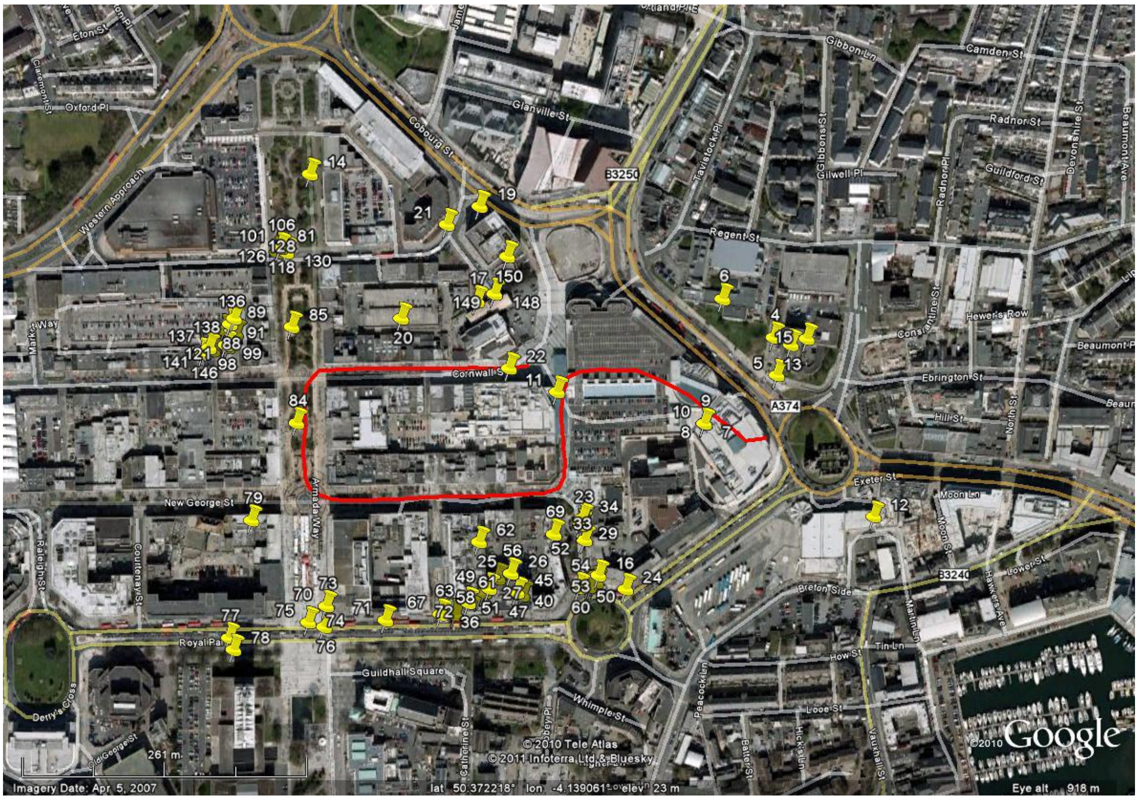


Figure 7.19: Evaluation route for the urban Wi-Fi tracking evaluation

Figure 7.20 shows the second evaluation route that was evaluated for this *Non-Proprietary Access Point Tracking System*. This route is a good evaluation of the non-proprietary Wi-Fi tracking as it gives an opportunity to see how Wi-Fi signals in suburban areas can provide viable location information for a CIT box that has been stolen and taken to such an area. The route evaluated is shown by the red line which was recorded by a GPS receiver during the experiment.

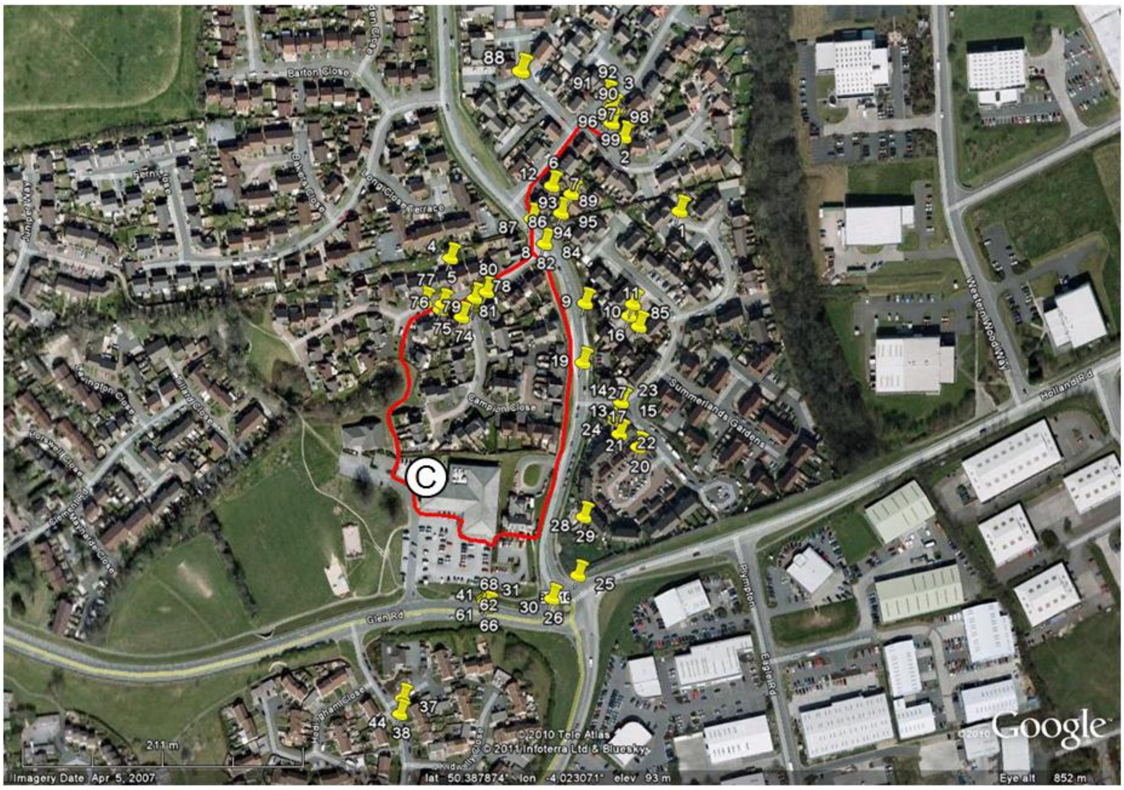


Figure 7.20: Evaluation route for the suburban Wi-Fi tracking evaluation

The final evaluated route is shown by Figure 7.21 and shows how Wi-Fi tracking can perform whilst being recorded from a vehicle moving at speeds of up to 70mph. Due to the large area covered during this evaluation, urban and suburban areas were explored again but the newest addition is an evaluation of the performance of Wi-Fi tracking on a dual carriageway whilst leaving the city and its suburbs. The recorded GPS route is shown in yellow in Figure 7.21, where the actual route followed is plotted in red. The differences between these two graphs will are discussed in 7.2.1.

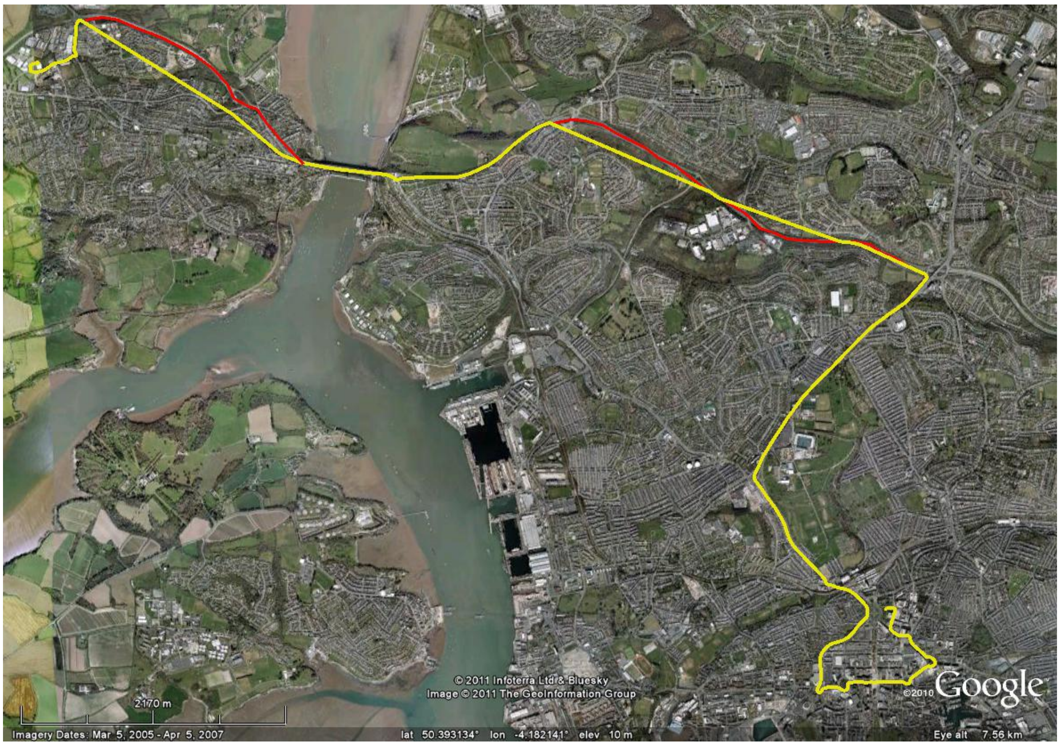

© 2011 Infoterra Ltd & Bluesky
Image © 2011 The GeoInformation Group
2170 m
Imagery Dates: Mar 5, 2005 - Apr 5, 2007
lat 50.393134° lon -4.182141° elev 10 m
Eye alt 7.56 km
©2010 Google

Figure 7.21: Evaluation route for the Wi-Fi tracking evaluation whilst driving

7.3 Evaluation of Results

7.3.1 *Theft Detection* Concept

The results of the evaluations performed in 7.2.1 are shown graphically in the figures following. Each of the figures relates to the results of an evaluation performed on a specific route which is shown at the bottom of each graph. The results are slightly smoothed to remove any abrupt changes which can be attributed to noise factors while each graph is also separated into 5 areas in the time domain which depict the physical location and action of the CIT box at that moment in time.

The expected output is that the signal strength of the van's transmitter decreases as the CIT Box moves away from the van. It is also expected that the signal strength of the delivery location's transmitter increases as the CIT Box approaches it.

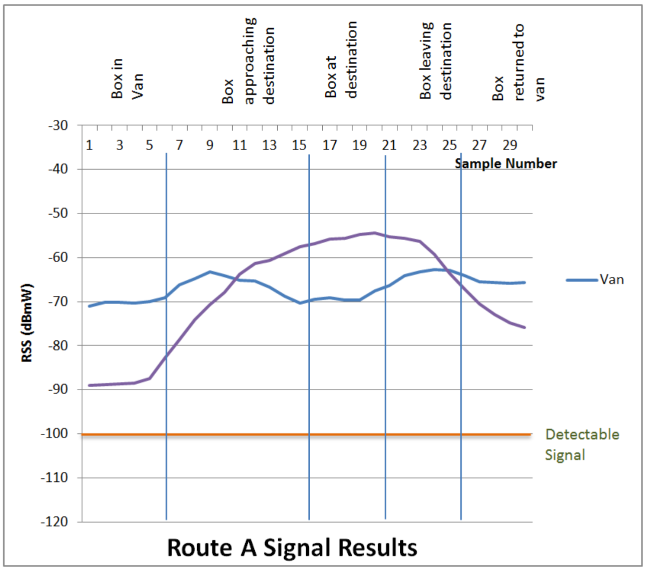


Figure 7.22: Route A evaluation results

Route A is the first of the two short distance tests. The results of this study show that, as the CIT Box approaches the destination, its transmitter's signal strength increases markedly. It is worth noting that the destination's signal was visible from the point of the CIT box leaving the van and this is because the destination for this route is within 10 metres of the van. When the CIT Box is at its destination, the van's signal is still visible with good signal strength.

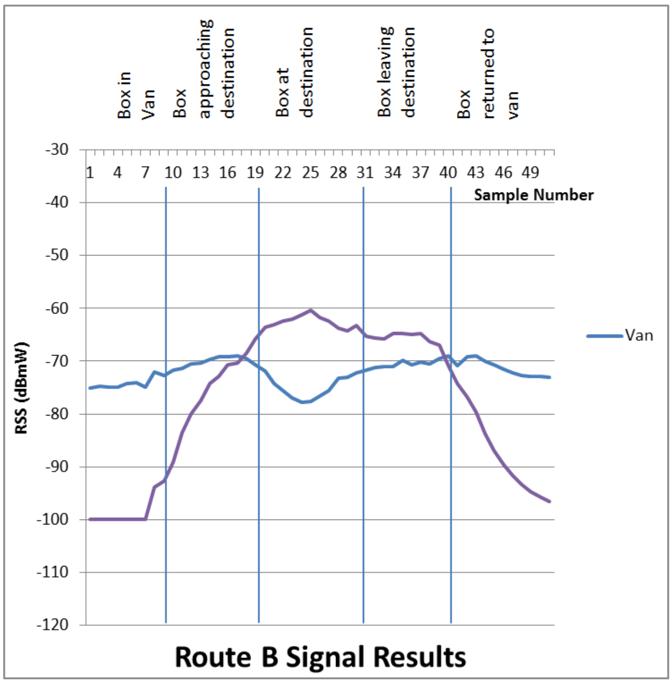


Figure 7.23: Route B evaluation results

Route B shows similar characteristics to Route A but the delivery location's signal cannot be seen for the first 7 samples. This can be explained by the CIT Box being inside the van at this point and the attenuation effects of the Van are dominant at this distance from the destination access point. Apart from this, the signal trends during transport are comparable to those expected and predicted.

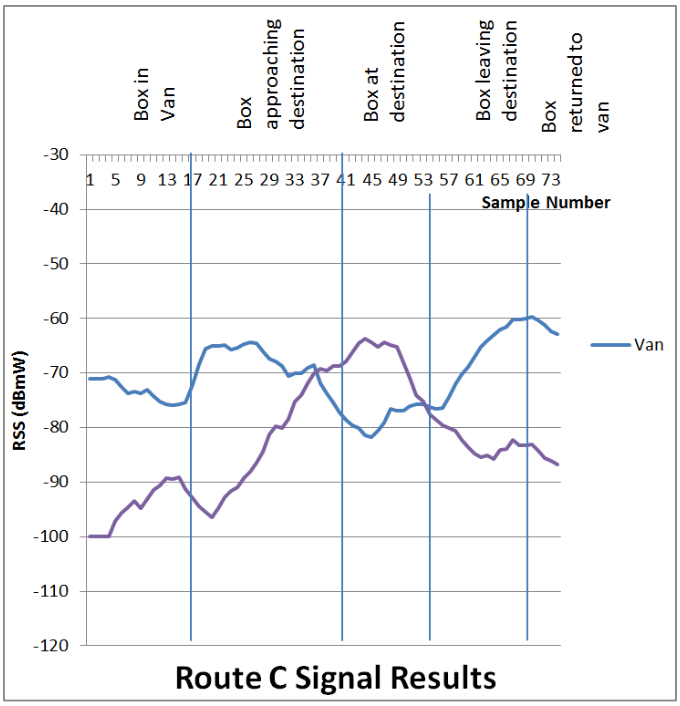


Figure 7.24: Route C evaluation results

Route C is the first of the medium distance studies and the results are rather ragged which diverge slightly from the expected. Because the results are smoothed to remove any noise, these results show that there is significant variation in the received signal strength and this is due to the route taken and obstacles in the way when assessing this route. It is worth noting that, for the first four samples, the delivery location's signal was not visible as the attenuation effects of the van and the surroundings are dominant.

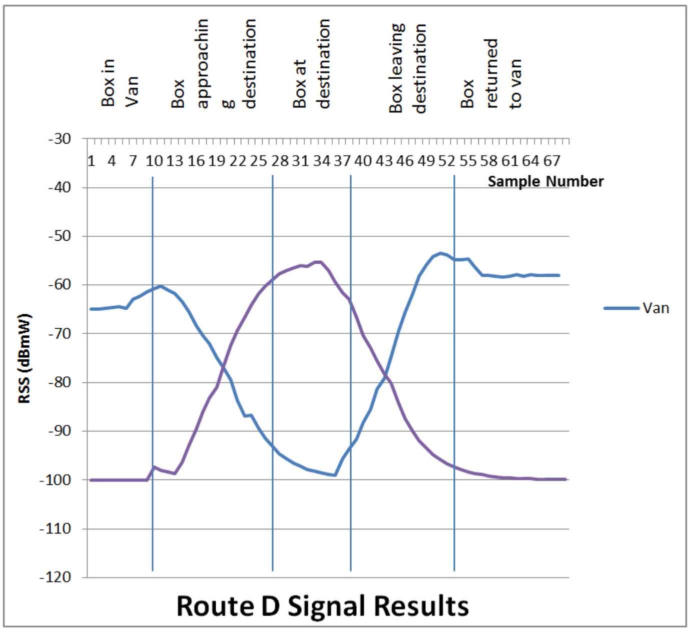


Figure 7.25: Route D evaluation results

Route D is a good example of the expected trend. The destination access point was not visible for the first samples and also in this case the van's signal was not visible when the CIT Box was at its final destination. This is to be expected as the distance between the delivery location and the van increases.

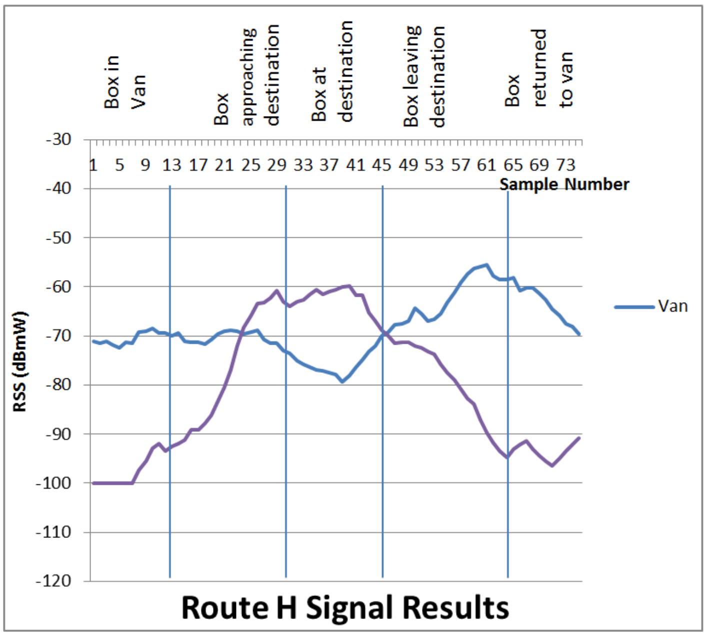


Figure 7.26: Route H evaluation results

Location H is directly in front of the transmitting access point and as a result the van's signal remains visible even when the CIT Box is inside the delivery building. This provides good evidence of the benefits of placing the Wi-Fi antenna on the outside of the van as the destination signal is weaker than that of the delivery van.

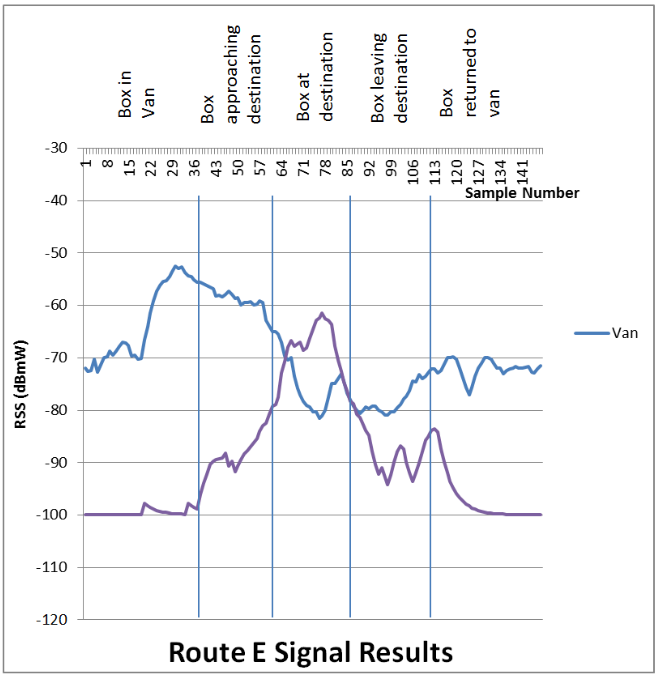


Figure 7.27: Route E evaluation results

Route E is the first of the longer distance tests and this is confirmed as the destination signal is not properly visible for the first 30 samples. This is to be expected because of the large distances between the van and the delivery location. At the delivery location the van's transmitted signal is still visible and this is because at location E, the van is directly in front of the destination, once again reinforcing that the van's transmitting antenna is best placed externally to the vehicle.

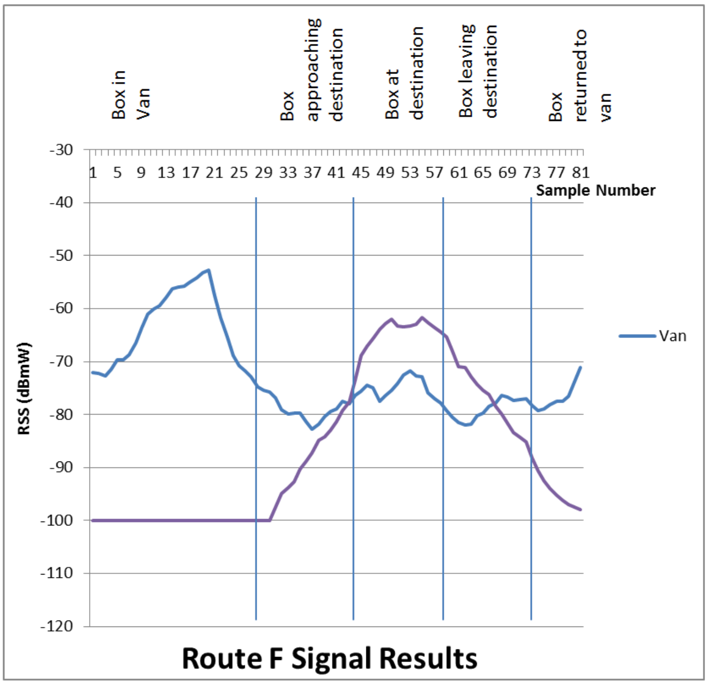


Figure 7.28: Route F evaluation results

Route F presents some unexpected results as the destination access point is not visible for at least 1/3 of the CIT Box's journey. This is expected as the transmitter is located indoors and the van is very far from the delivery location. One important fact is that the van's transmitter is always visible to the CIT Box which means that during the box's journey it was always within the coverage of one Wi-Fi access point.

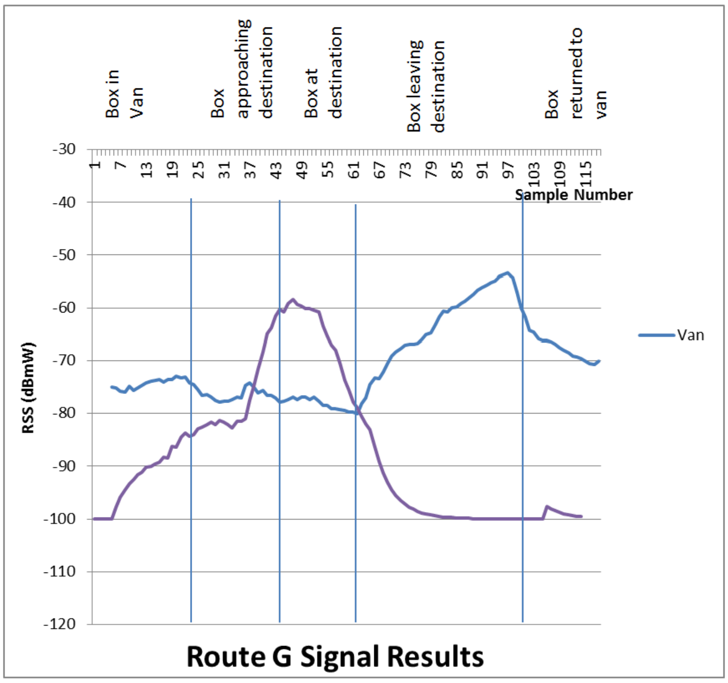


Figure 7.29: Route G evaluation results

In terms of the expected trend, Route G's results are similar to those seen in Route F above. The differences between them are minor but it is worth mentioning that on the return journey, the destination's signal disappears quicker than on the outbound journey. This trend is the opposite of the van's signal which is stronger on the return journey than on the outbound journey. This is a characteristic that shows that the single antenna within the CIT box has better performance characteristics when the CIT box is in a particular orientation. This characteristic can certainly be overcome by utilising the antenna diversity techniques tested and developed in Chapter 5.

7.3.2 *Safe Zone* Concept

The results of the evaluations performed in 7.2.2 are shown graphically below.

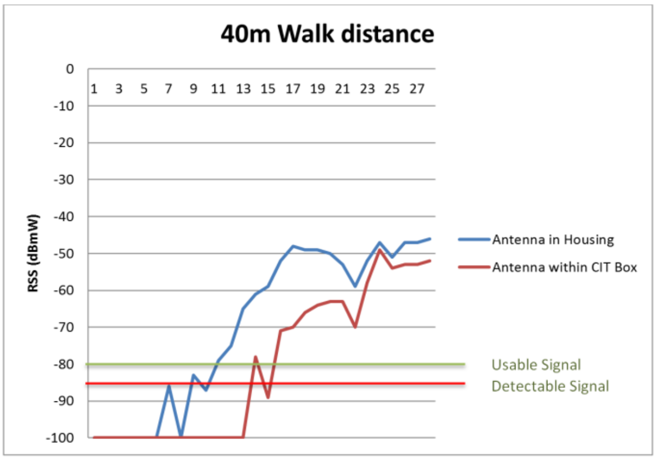


Figure 7.30: 40m Walk distance towards the Delivery transmitter

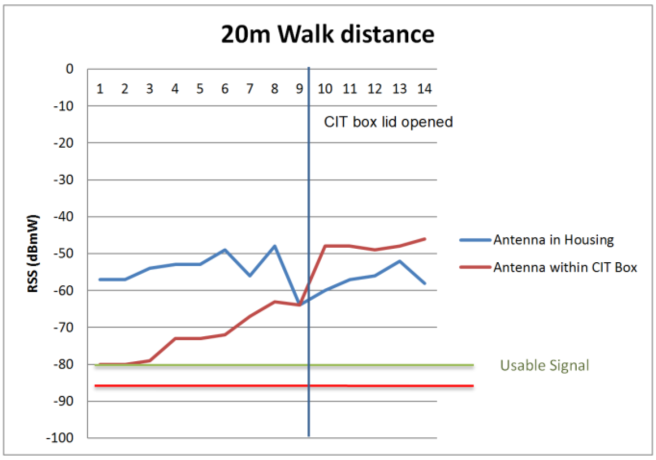


Figure 7.31: 20m Walk distance towards the Delivery transmitter

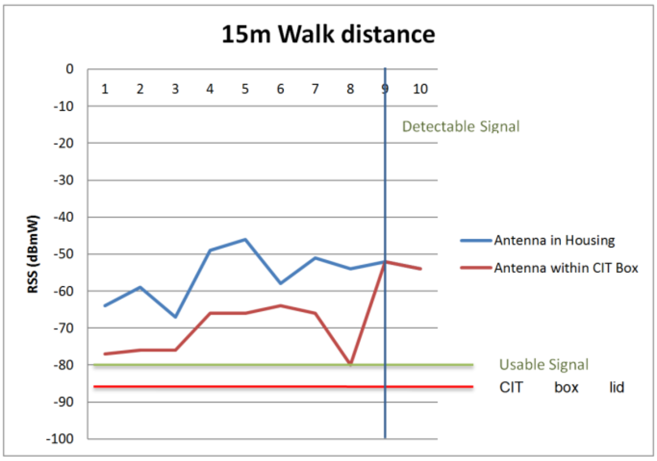


Figure 7.32: 15m Walk distance towards the Delivery transmitter

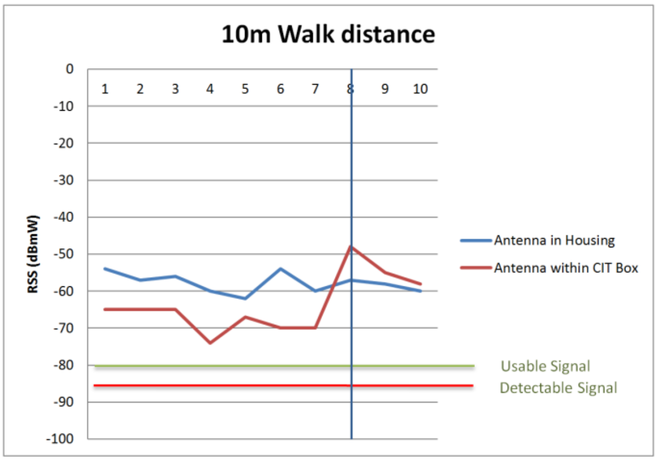


Figure 7.33: 10m Walk distance towards the Delivery transmitter

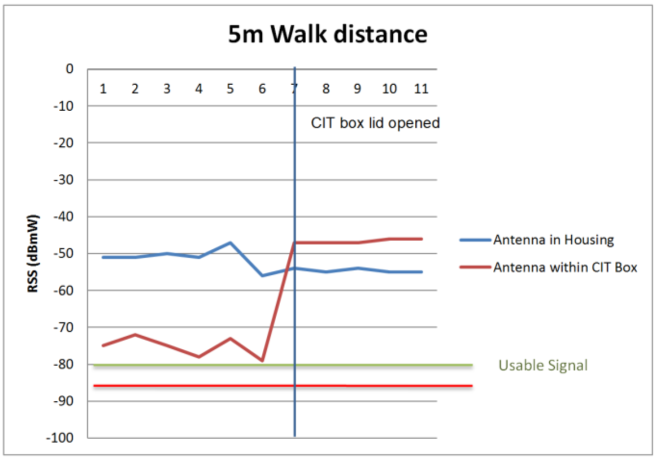


Figure 7.34: 5m Walk distance towards the Delivery transmitter

With a walk distance of 20m or less the signal strength recorded on the antenna locator is fairly constant but at 40m, increasing signal strength can be detected.

For the final evaluation where the CIT box was placed 3m from the Delivery transmitter, the RSS at the antenna locator averaged -54.6dBmW at that distance. The maximum recorded signal strength was -46dBmW and the minimum recorded was -60dBmW. For this setup and at this distance from the transmitting access point, -60dBmW is around the expected RSS at any orientation given the performance of the antenna used and any losses from the antenna locator. The results are shown graphically in Figure 7.35.

The attenuation effects of the CIT box are clearly visible as there is a big difference in the two signal strengths recorded. Once the CIT box lid is opened, the signal strength at the antenna within the CIT box is stronger because the attenuating factors have been removed. The antenna within the antenna locator is now the worst performer because the antenna locator has an attenuating effect as evaluated in Chapter 6.

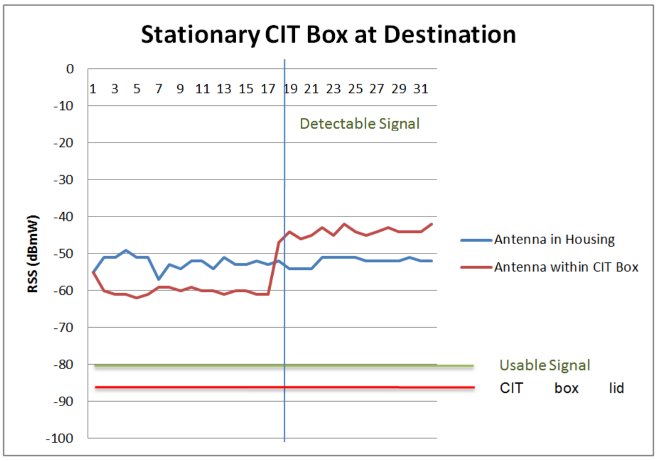


Figure 7.35: Stationary CIT box 3m from the Delivery transmitter

7.3.3 *Profile Tracking* Concept

The results of the evaluations described in 7.2.3 are discussed below. The first evaluation depicted by Figures 7.14 and 7.15 was split into two routes that simulated two different types of attacks; one organised and the other less so. The yellow route in the first evaluation detected theft at marker A which was 138m from the van. The red route managed to detect a theft at marker B which was 106m from the van. These distances were extended by the presence of the Profile but due to the nature of the area where the tests were being performed this extension is probably a worst case as it is fairly open with minimal RF reflections. This gives the transmitted signals the best possible range.

Another factor is the time taken to cover these distances. The time to cover these distances in this simulated scenario is minimal as the open areas allow for easy escape in the event of a theft. With multi-storey buildings, the time taken to cover these distances is greatly increased. The time to detection of theft in this scenario is approximately 15 seconds if the CIT box was stolen straight from the Van. Anything between this takes less time to detect assuming that all other variables remain unchanged.

In the second evaluation depicted by Figure 7.16, which simulates a dense urban environment, the tracker recorded the 30 maximum profiles that the software would allow and achieved this before the return route (returning to the van) was completed. As the journey to the destination was completed before the memory allocation (the 30 profiles) was filled, the route was deemed suitable for testing.

The results from the simulated delivery on this evaluation, depicted by the red route, showed that the route could be followed safely up to the destination without any indication from the tracker that the threat level was high. The diversion from this route, as shown by the yellow route, shows that the tracker detected theft at a distance of 55m. This short distance was due to the dense environment and an assumed simulated attack at the Van.

The final evaluation shown by Figure 7.17 revealed an issue with the limit of 30 profiles that could be recorded to the tracker's memory. During the recording of the profile, the 30 memory allocations were filled approximately 10m from the end of the destination on the outbound journey. This highlighted the weakness with the limited recording space for the profiles.

The simulated delivery route for this evaluation shown by the red route in Figure 7.17 was tested despite falling 10m short of the destination. The route was declared OK for testing because the tracker was in view of the destination access point and therefore the tracker was not expected to react adversely. Despite this shortfall, the tracker managed to extend the route acceptably using the recorded profile and did not exhibit any instances of a high threat level.

The route was then repeated and the diversion took place away from the Van in this situation. The tracker managed to get almost 127m from the Van before the threat level was raised by the tracker.

7.3.4 Non-Proprietary Access Point Tracking

Results for the testing of the *Non-Proprietary Access Point Tracking* using Wi-Fi as introduced in 7.2.4 are described below. During the testing of the urban environment route, the results showed that it was not easy to visually decipher a route from the data. This is due to many factors, one of which is the number of samples and the speed at which the tracker was travelling, which is a walking speed. Indoor location does not appear to yield the best results with this track either and this can be partially attributed to the large area that the indoor shopping centre covers.

The Urban environment route shown by Figure 7.19 exposes a weakness in the *Non-Proprietary Access Point Tracking* method in this environment. As the area tested is pedestrianised and the Wi-Fi scanning service acquires its data from the road, the results are skewed towards the road or buildings close to the road which the Wi-Fi scanning service provided by Skyhook used to gather the location data. This is the major contributing factor to not being able to decipher a route which correlates with the red GPS track.

As a way of providing a pinpoint location, the Wi-Fi location system does however work well. In the majority of cases, it places a recovery team within 120 meters of the route and at the worst recorded case, the furthest recorded distance from the route was 171m. This technology allows a recovery team to get within 171m of the tracker to start the recovery process. This shows that there is significant value to a CIT tracking system that uses this non-proprietary Wi-Fi tracking system in this environment.

The second tested route shown by Figure 7.20 is within the suburban environment and yet again, the greatest weakness of this tracking system is exposed. It is clear that it is not easy to decipher a route from this data but again, it is possible to use this system as a pinpoint location service. The worst distance recorded between the actual route and the Skyhook estimated position was 125m but this was a minority figure. In the majority of cases, the distance between the estimated position and actual position was 50m which is due to the density of access points in the area. This accuracy is also reinforced by the densely populated area as the buildings do a good job of attenuating other Wi-Fi signals which may dilute precision. The limits to Wi-Fi positioning in this area are shown by marker C in Figure 7.20. This marker lies within a local shopping area where it is apparent that there are no Wi-Fi access points.

The third and final evaluation of this technology reinforces all the predicted strengths and weaknesses of this tracking technology. It is clear from the GPS route that reception was lost at two locations and they had to be corrected. The first loss of signal is the longest duration and was due to concrete canyons on the dual carriageway at a large underpass. The second loss of signal is due to a tunnel and the GPS receiver was slow to recover from the signal loss.

Despite these GPS results, Figure 7.36 below shows the results of the *Non-Proprietary Access Point Tracking*. The results did not deviate dramatically from the expected. They followed a trend where urban and suburban areas yielded good results yet the more rural areas such as the A38 dual carriageway yielded very few results by comparison.

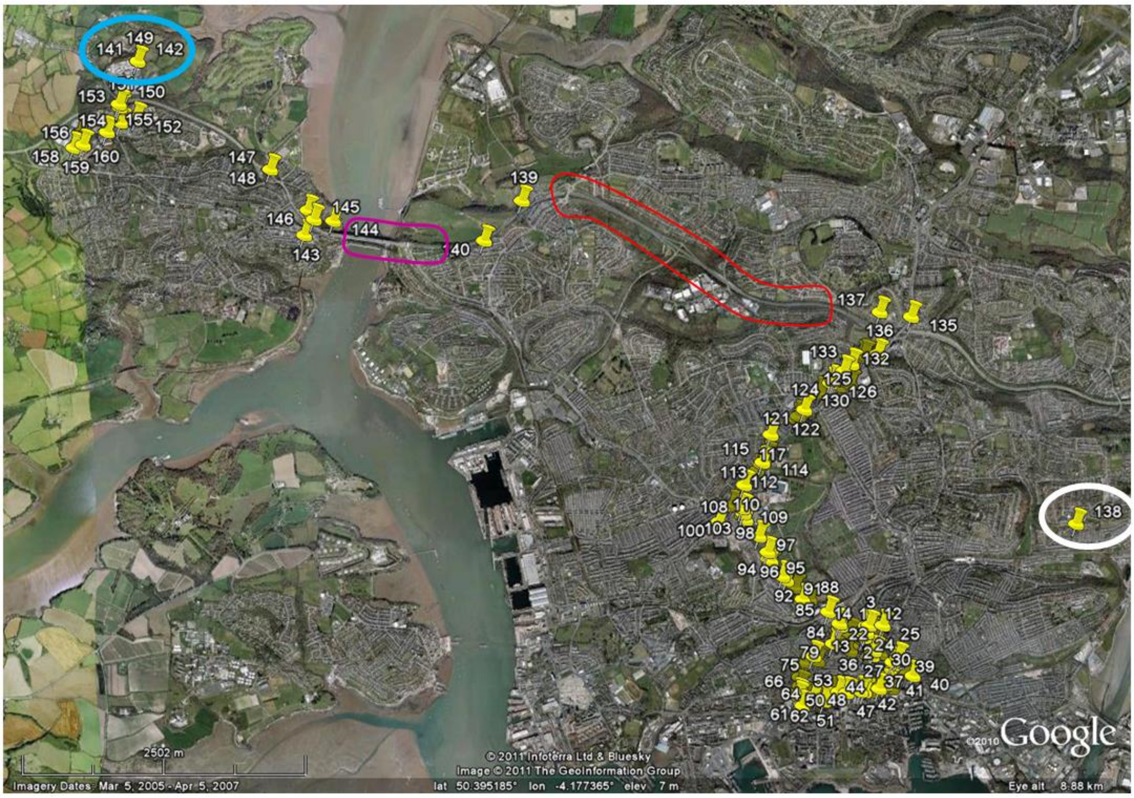


Figure 7.36: Wi-Fi results of the *Non-Proprietary Access Point Tracking* with a vehicle in motion

This route identified the potential issues with the *Non-Proprietary Access Point Tracking* system. Marker 138 circled in white the far right of Figure 7.36 is out of place as this access point was actually scanned on the A38 between markers

137 and 139 shown by the red shape. The resulting retrieved location is indicative of an ageing Wi-Fi database as the access point has changed location.

The same situation is highlighted by the Blue circle at the top left of Figure 7.36. Markers 141 and 142 were actually scanned somewhere within the violet coloured shape. Analysis of the raw data shows that locations 141 and 142 are the same MAC address therefore the total number of errors in this whole evaluation is 2 out of 160 locations returned from Skyhook. This gives a total error of:

$$\text{Error} = \frac{2}{160} \times 100\% = 1.25\%$$

As Figure 7.21 encompasses all the tested environments in one drive, the Urban and Suburban environments have been extracted and are magnified and shown below in Figures 7.37 and 7.38. The actual routes have been overlaid and the results show the resolution that can be achieved using this non-proprietary Wi-Fi location system. The Wi-Fi routes can easily be distinguished and by comparison with the actual route overlaid, the results are nearly always within 30 metres of the GPS location. In the majority of cases, the location was visible from the point of scanning. It must also be noted that these results were achieved from a vehicle which was in motion at speeds between 20 and 60mph.

This proves that the non-proprietary location technology can be used when the CIT box is in motion.

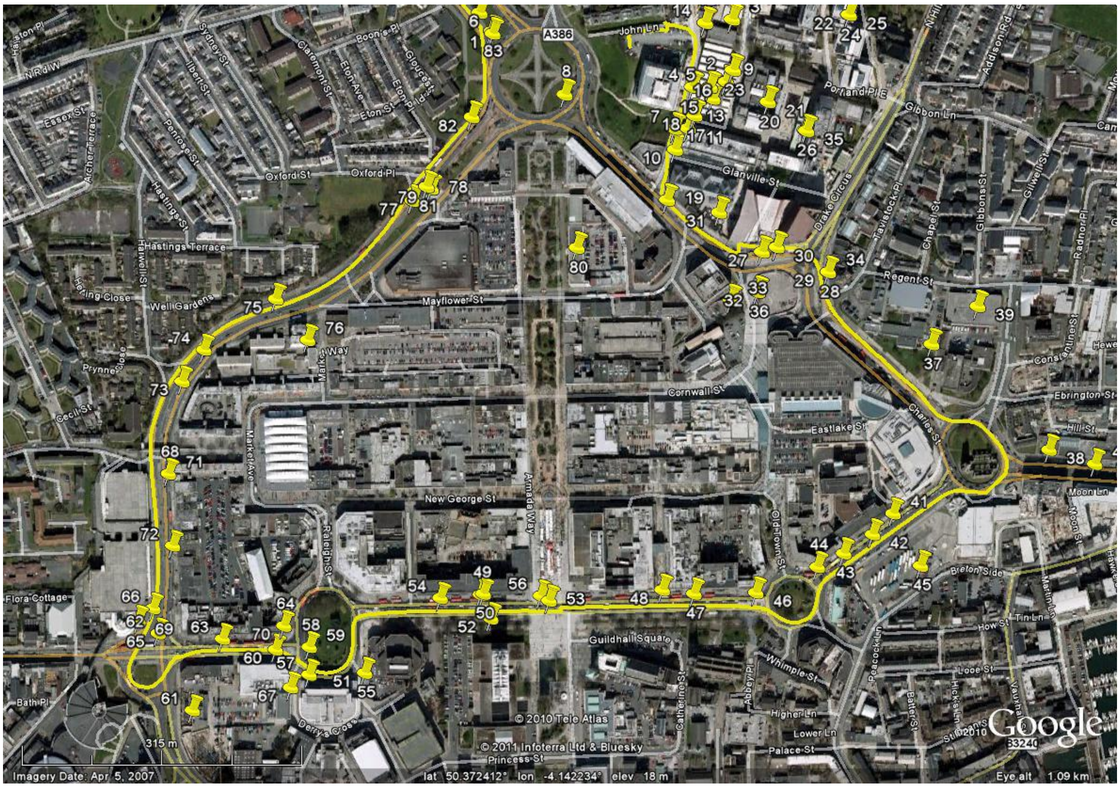


Figure 7.37: Magnified urban environment with a vehicle in motion

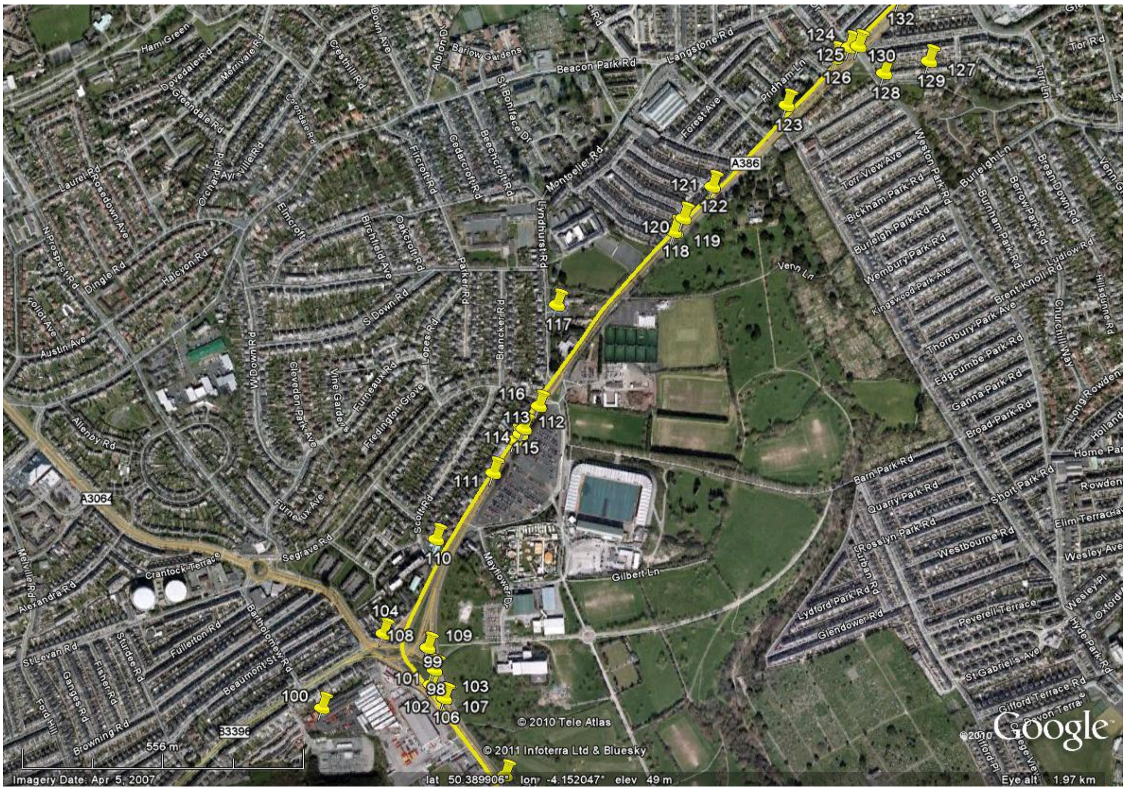


Figure 7.38: Magnified suburban environment with a vehicle in motion

7.4 Discussion

This chapter has introduced four new methods of tracking a CIT box. Each of these new methods is unique but they can be split into two types of tracking; tracking that uses proprietary Wi-Fi access points, and tracking that uses non-proprietary Wi-Fi access points. The differences between the two have been discussed but it is clear that for the CIT application, there is a substantial benefit to implementing a proprietary network that each tracking system can use to enhance the operation of the tracker. It is defined as a localised tracking system.

The greatest justification for the proprietary access point tracking is that this architecture will allow most of the tracker hardware to be in a sleep state. For CIT customers, this means that they can be reassured that the batteries powering the tracking system will last long enough to recover the device as all the potential wide area tracking modules such as GSM, GPS and RF beacons are not switched on until such time comes that they are required. With this architecture, this hardware remains turned off until the main core of the tracker detects that the CIT box is not where it is expected to be. The *Theft Detection* concept introduced in 7.1.1 is a robust way of tracking the CIT box locally and detecting if it is off course.

The results of evaluating this *Theft Detection* concept presented in 7.3.1 have shown that there is a signal profile that emerges from each evaluation. The signal strength of the delivery vehicle decreases as the CIT box moves away from the van and the signal strength of the Destination increases. The testing did not yield any unexpected results but it did reinforce the fact that there can be instances where the Delivery signal is not visible and the CIT box is solely reliant upon seeing the Destination signal which is classed as ‘Not Safe’.

The circumstance where the tracker can measure reliably high signal strength from the Destination signal is introduced and researched by the *Safe Zone* concept in 7.1.2. The uses of this tracking method may not be immediately apparent but they provide a way of enhancing the functionality of the tracking system and enhancing the functionality of the CIT box. When the tracking system believes it is safe as defined by this research, it can lower the security of the CIT box as it is expecting the box to be opened. This means the tracker can communicate directly with the CIT box and provide it with a ‘Safe’ signal. The tracker will now form an integral part of the CIT box’s security by not allowing the CIT box to open without seeing this ‘Safe’ signal. If it sees this signal it knows it is trying to be legitimately opened at a location that it recognises as safe. This functionality further secures the case where an organised robber steals the security keys from the guard and a customer and then tries to legitimately open the CIT box elsewhere.

The second additional functionality of the *Safe Zone* concept will cover an operational case where the CIT guard has the CIT box open at the delivery location and the customer is slow to remove the cash or deposit the new cash into the CIT box if it is a cash pickup. This situation occurs frequently as the CIT guard has to wait for the customer to find the cash or even wait for the individual responsible for handing the CIT guard the cash during a pickup. The Wi-Fi tracking system would be running all this time to ensure that its security has not been compromised but in reality, the CIT box is not moving and the lid is open waiting for the customer. As the CIT box knows it is safe, it would be possible for the CIT box to signal to the tracking system that the box is open and therefore the tracking system would be able to shut itself down as it is in the presence of the customer and the CIT box has been instructed to open. This is considered a safe location as the CIT box is not responsible for the safety of the cash in this situation. Once the lid of the CIT box is closed, the CIT box is responsible for the safety and integrity of its contents and the tracking system will resume the function of checking for the Delivery and Destination signals. By implementing this feature, the tracking system can further reduce its power consumption by turning off when it is not required. This would further bolster the requirements imposed by the CIT industry to ensure the lifetime of the CIT box without recharging.

The research in 7.3.2 showed that the tracker could be up to 20m away from the Destination transmitter and it would believe it is just as safe as if it was 5m from the Destination transmitter. This may appear to be a disadvantage to this *Safe Zone* tracking method but there is scope to improve on this. During the research in 7.3.2, the CIT box was simulating a delivery and the Destination transmitter was within 3m of the simulated delivery point where the CIT box was opened. In a practical scenario, the customer always has a specific location where they open the CIT box which is normally a back room out of the visibility of customers and especially, robbers. This provides consistency to the delivery process and a practical delivery could involve placing the CIT box within 1m of the Destination transmitter. This will increase the received signal strength to a level greater than the research in 7.3.2 as the CIT box would be close to the near field of the Destination's transmitting antenna. This is where the CIT box would consider itself 'Safe'. This gives the *Safe Zone* tracking method a more credible way of distinguishing if it is safe, especially if the Destination transmitter is ruggedized and fixed to a surface that is difficult to move such as a wall or bench.

The last concept researched is *Profile Tracking*. This is not considered to be *Non-Proprietary Access Point Tracking* despite it using non-proprietary access points. This is because the methodology is reliant on the *Theft Detection* concept and *Profile Tracking* is only implemented to cover the instances where the Delivery vehicle's signal is not visible and the Destination signal is not visible either. Under the *Theft Detection* concept, the routes indicated by *Profile Tracking* would be considered a theft situation and the tracking system would react accordingly. As explained in 7.1.3, there are credible situations where the loss of Delivery and Destination signals can occur and the results of the *Profile Tracking* research in 7.3.3 show that non-proprietary access points can fill this void.

The research is very positive however a few issues have been highlighted. The first area of concern is that whilst recording profiles, a large amount of memory is needed as dense urban environments will have a lot of Wi-Fi access points. The software limited the number of profiles to a maximum of 30 in but this constraint only exists as a result of the software design of the prototype system and not the memory limitation of the hardware. Large realistic profiles can be accommodated by removing this software restriction and by building in some intelligence into the profile recording. Filters could be implemented that reject Wi-Fi access points that have very low signal strength which means that they are far away from the delivery route but are weakly visible. This should cut down on memory required within the tracker, which is a premium, and can introduce delays if searching through large banks of memory.

Another issue is the complexity involved in implementing this practically. Practical implementation would involve knowing where the CIT box was going to be delivered to and then loading the appropriate profiled route to follow. This involves the CIT industry getting more involved and introducing intelligence into their planning and delivery management systems. This is less likely to happen soon in the UK market but it is something that Scandinavian markets already implement. It is in these markets that *Profile Tracking* will work well and prove its use. Once it is proven, other markets will be able to subjectively assess the use of *Profile Tracking* and make a business judgement as to whether they will implement it.

For markets that cannot yet implement *Profile Tracking* without significant immediate investment, a compromise can be implemented for lengthy delivery routes which will trigger a false theft situation. A preset time can be introduced where the tracker times the period between the loss of Delivery and Destination signals. If this preset time is exceeded, the tracker will then assume theft. This compromises the tracker’s response to a genuine theft situation but it can eliminate false triggering of the wider area tracking system and theft reporting. The best outcome is still to implement *Profile Tracking* in all situations as the research has showed that a theft was detected at most, 138m from the van.

So far the advantages of adding a Wi-Fi receiver to the CIT box for localised tracking and theft detection have been discussed. The final important advantage to using a Wi-Fi receiver within the CIT box is that it can be used in conjunction with a GSM module to track the CIT box on a more global, wide area scale rather than just a localised tracking system. The research introduced in 7.2.4 and performed in 7.3.4 has proved that non-proprietary Wi-Fi access points can be used successfully within urban and suburban environments to locate a tracker within 171m of its actual location. It has also been proven that this tracking system is not restricted by the device being indoors. Research in 7.3.4 shows that Wi-Fi as a Tracking technology is very viable and the cost of the Wi-Fi receiver is already accounted for because the hardware is already used for localised proprietary access point tracking researched earlier in this chapter. This positive outcome from non-proprietary Wi-Fi access point tracking further bolsters the research in Chapter 3 which helped lead to this new research.

The research in 7.3.4 has demonstrated that urban areas yield good tracking results using this technology but in urban areas that are pedestrianised, the location accuracy can be compromised. This is not considered significant because this urban research is a worst case. Large cities like the City of

London are not fully pedestrianised and therefore that type of urban environment would yield much more accurate results. From a CIT perspective, there are more attacks on CIT deliveries in the City of London than there are in Plymouth City Centre; therefore the location accuracy lost in 7.3.4 is not critical.

Another positive for this research is the number of location conflicts as a result of inaccurate information received from the Skyhook database. 7.3.4 shows a calculated error of 1.25% which is very low. As a reassurance however, it is unlikely but not impossible that a situation will arise where a CIT box will only see one Wi-Fi access point. If this instance does arise where only one Wi-Fi access point is seen, this information becomes critical and other measures can be taken to check the validity of the returned Wi-Fi data. A measure that can be taken is to cross check cell mast information from the tracker's GSM device with the location data received from Skyhook. This is expensive therefore should only be performed in a situation where the integrity of the received location information is critical.

Security aspects

Most Wi-Fi and non-proprietary security aspects have already been touched on in previous chapters, however they relate directly to this research. Each of the three non-proprietary tracking methods described here have utilised Wi-Fi signals which are vulnerable to spoofing attacks and jamming.

Spoofing a Wi-Fi access point would compromise the security of the *Theft Detection* concept and the *Safe Zone*. A good way to eliminate spoofing is to connect to the Delivery and Destination access points and authenticate using a Challenge – Response algorithm. Implementing such authentication techniques is possible as the access points are proprietary to Spinnaker and CIT customers, therefore this method will ensure that spoofing is not possible.

Spoofing with *Profile Tracking* would mean that an attacker could create their own profile and guide a CIT box to a place where they could attack it without the tracking system elevating its threat level. This is not desired but it can be easily overcome by introducing a timing feature which expects to see the destination signal within a certain timeframe. This is a simple solution to the concern.

Chapter 5 demonstrates the effects of jamming Wi-Fi signals and it is possible that this can happen with these newly researched concepts in this chapter. Signal jamming attacks are not a concern for any of the researched proprietary access point tracking concepts because a loss of Delivery or Destination signal will automatically trigger a theft and the tracking system will enable its wide area tracking systems. A worthy note is that an intermittent signal jam could cause the tracker to start its wide area tracking systems, but as there is a finite time required for these systems to start, the intermittent nature of the jamming attack might cancel the wide area tracking before the tracker has an opportunity to acquire its location or establish communications with the remote server. To overcome this, the tracker must simply latch the theft status in the first instance that it detects theft. This will overcome any intermittent signal jamming attacks.

The final security concern is the integrity of Destination transmitter. If these transmitters are stolen, they can be used to convince the CIT box that it is safe and an attacker can access the CIT box if they have stolen the access keys as well. To overcome this, the Destination transmitters will need to be designed to be rugged and only accessible by Spinnaker service personnel. The transmitters will also need to be installed in secure locations that are immovable or cannot be easily removed in the timeframe that an organised robber has.

7.5 Conclusions

This chapter has introduced four novel tracking methods and technologies while evaluating their performance. Value is also provided through the research that has already been performed and introduced such as Wi-Fi as a tracking solution combined with antenna diversity in Chapters 4 and 5.

These concepts have shown that Wi-Fi is a useful tool for detecting theft of a CIT box while the *Non-Proprietary Access Point Tracking* of a CIT box yields good results in Urban environments. The security aspects of both Proprietary and *Non-Proprietary Access Point Tracking* are discussed with mitigation techniques suggested. The following chapter details research and development of an embedded tracker that implements these researched concepts and researches them further in a more practical environment.

8. Embedded Tracking and Theft Detection

The research performed so far has introduced and tested concepts for a tracking solution that is bespoke to the CIT industry. So far, the research in this thesis has used and tested a mixture of hardware to determine the best performing setup for use with a CIT box. This final research chapter expands on the research performed in Chapter 7 by researching more realistic delivery routes and takes into account all the outcomes of the preceding chapters that are beneficial to making the best tracking solution for CIT. The research brings together the outcomes of Chapters 5, 6 and 7 and links them to show how the localised tracking and theft detection systems introduced in Chapter 6 fit into the final solution presented to Spinnaker as the bespoke tracking solution for the CIT industry.

As a result, this chapter presents a bespoke embedded tracking system that is designed to integrate into a CIT box. It integrates a GSM communication device, an embedded Wi-Fi transceiver, an integrated two port antenna diversity switching device, a microcontroller and some non-volatile memory for data storage.

8.1 Embedded Tracking and Theft Detection equipment

As the purpose of this research is to design a bespoke tracking system for CIT use, unique prototype hardware was designed in order to achieve the research presented in this chapter. The developed hardware is shown in Figure 8.1 and was designed over the space of 3 months by the author for this embedded tracking application. The electrical architecture was designed in the schematic capture package of Mentor Graphics PADS and the electrical layout onto an 8-layer PCB in the layout package of PADS followed the schematic capture.

The wireless communications equipment integrated on to this prototype tracker included a GSM modem device for transmitting data wirelessly to a central server, a Wi-Fi transceiver capable of interfacing to a microcontroller and an RF switch to evaluate and implement antenna diversity if required. There was also expansion for connecting an external GPS receiver. Supporting hardware for the tracker included an 8 bit microcontroller, 256kbits of non-volatile memory, an accelerometer, ambient temperature sensing and an on-board buck/boost switch mode power supply.

For the testing in this chapter, a tuned dual antenna PCB was designed which integrated the Antenova Wi-Fi antenna tested in Chapter 6 and a new Antenova GSM antenna. The two antennas were integrated on to the same board because this would be a more representative solution of a tracking system that would be integrated into a CIT box.

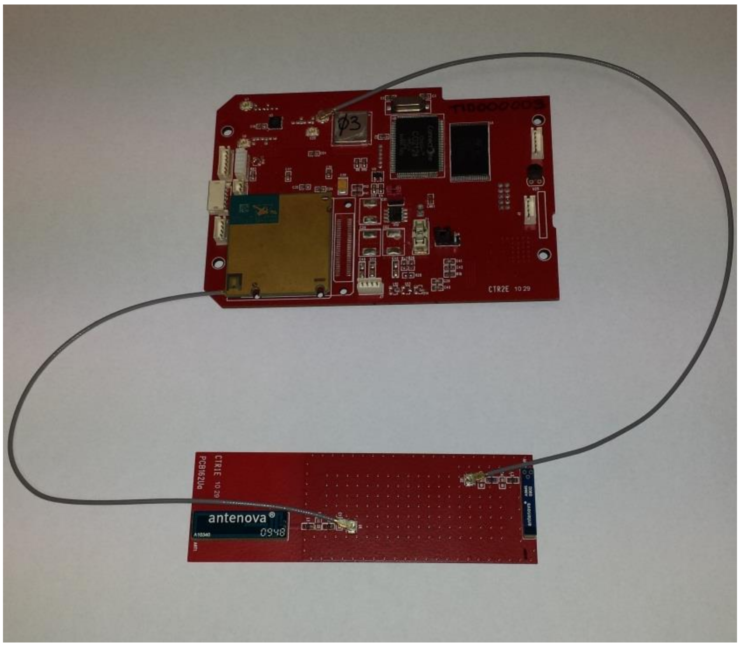


Figure 8.1: The bespoke embedded tracking system

Regarding the integration of the embedded tracking system, the designed tracker considered aspects of the CIT box’s design with the target of providing a level of integration into the CIT box. This integration was considered at design time; however a reasonable level of flexibility was maintained so that the research in this chapter could be performed. When installed, the tracker was not visible in the CIT box, thus showing a level of integration. The designed dual antenna was installed in the left hand antenna locator as researched in other chapters and both the Wi-Fi and GSM elements were tuned for best performance using a Vector Network Analyser. No GPS receiver was connected for the testing as a handheld unit was used instead.

The tracker was powered by a 3.6V primary lithium-thionyl chloride cell capable of delivering the required pulse current for GSM communications. The battery pack was placed inside the CIT box near the tracker for ease of access. A servo motor was also connected to the tracker and used to lock and unlock the CIT box to prove the following concepts described in 8.2 below.

User interface to the tracker was done via a push button on the CIT box that was connected to an input on the tracker. The purpose of this interface was to provide an instruction to the tracker to lock and unlock the CIT box.

Embedded software was written by the author in the C programming language to drive each of the subsequent tests performed in 8.2 below. The software development spanned approximately 3 months for this hardware. Using the GSM modem and its General Packet Radio Service (GPRS) function, the software opened a socket over TCP/IP to a remote server controlled by and supported by Spinnaker and a protocol was devised by the author, which sent structured tracking data to the server when research was being performed.

The tracking data was received from the Wi-Fi device which was programmed to extract MAC addresses and signal strength from surrounding Wi-Fi service broadcast beacons. The hardware operated right first time as the intended design and no hand modifications were necessary to ensure operation of the hardware. This hardware, software and surrounding infrastructure was used to further expand the tracking techniques and concepts introduced in Chapter 7.

8.2 Research methods

Based on the research of Chapter 7 and the concepts introduced, this section takes the concepts introduced in Chapter 7 and repeats some parts in order to determine if an embedded tracking system can replicate the results of the research performed in Chapter 7. Further research is then performed into more realistic delivery routes to determine how the tracking system responds.

Research in 8.2.2 investigates the effects of a delivery vehicle on signal strength in order to establish if the CIT box can detect if it is within a delivery vehicle or not. Section 8.2.3 researches the effects of orientation and position of the CIT box relative to the destination access point while the research in 8.2.4 evaluates the effect of placing a destination access point underneath a delivery table. The final research for this chapter is in 8.2.5 which will evaluate the trackers capability to exchange data with the destination access point and the time taken to perform this data exchange. This information will identify the overall timing impact if a tracker must authenticate with the destination access point in order to verify the legitimacy of its presence. These final elements of this chapter’s research evaluate the finer elements which will add robustness and value to the embedded tracking system required by the CIT industry.

8.2.1 Embedded Evaluation of the *Theft Detection* Concept

8.2.1.1 Evaluation Method for the Embedded *Theft Detection* Concept

In Chapter 7, the *Theft Detection* concept was introduced and in order to prove the effectiveness of this concept, section 7.3.1 presented a set of results that tested 8 different delivery routes of varying distances between the delivery vehicle and the destination. The following research revisits this and attempts to replicate the research performed in 7.2.1 with the embedded integrated tracking solution presented in 8.1. This is performed in order to establish if the embedded system performs as well as the evaluated equipment used previously in Chapter 6 and to evaluate if there are compromises with the use of this embedded tracker.

Figure 8.2 is a reminder of the delivery routes that were performed in section 7.2.1. The setup is almost identical to that in section 7.2.1 but with the embedded system including its antenna substituted as the tracking system. As a reminder, the testing involved the evaluation of 8 different delivery routes to evaluate feasible transit distances between the van and the delivery location for this concept. The delivery routes chosen for evaluation are grouped into three categories and are labelled from A through to H:

- Short distance from the delivery location (Locations: A, B)
- Medium distance from the delivery location (Locations: C, D, H)

- Long distance from the delivery location (Locations: E, F, G)

To avoid repetition, the individual detailed routes can be found in Figures 7.3 through to 7.10 in Chapter 7, section 7.2.1.

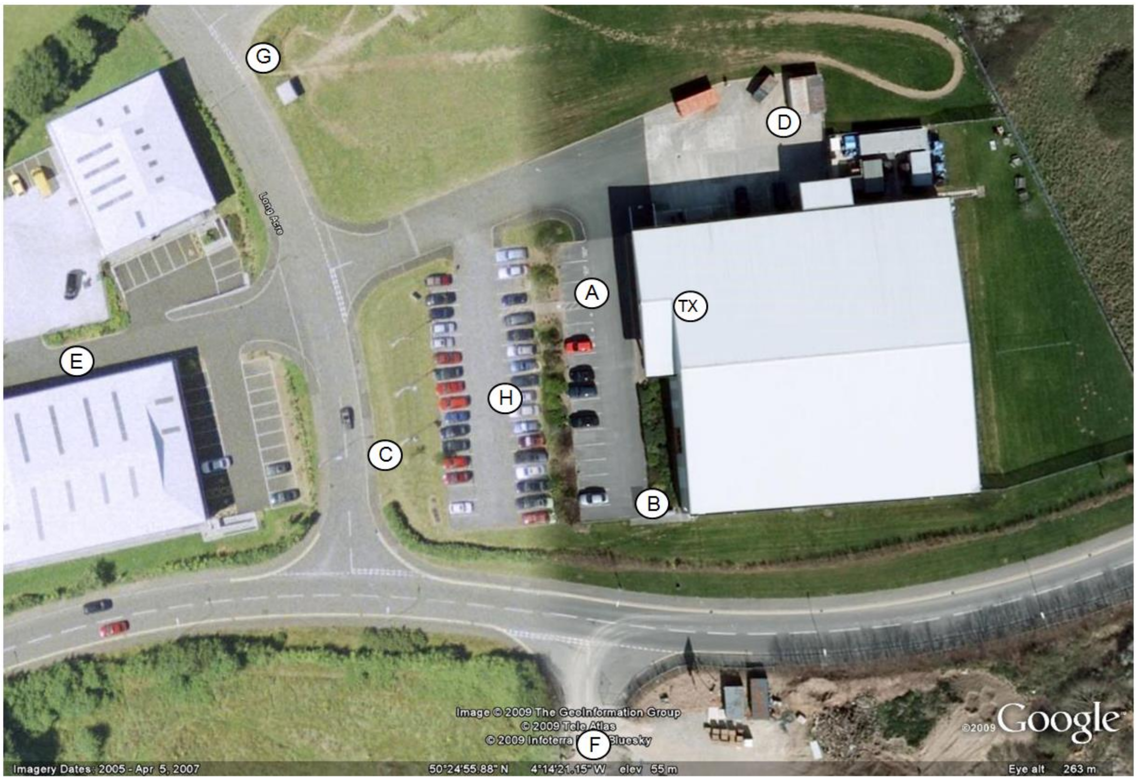

G
D
Long Acre
A
TX
E
H
C
B
F
Image © 2009 The GeoInformation Group
© 2009 Tele Atlas
© 2009 Infoterra Bluesky
©2009 Google
Imagery Dates: 2005 - Apr 5, 2007
50°24'55.88" N 4°14'21.15" W elev 55 m
Eye alt 263 m

Figure 8.2: Repeated delivery routes from section 7.2.1

8.2.1.2 Evaluation Method for Real World CIT Routes Using The Embedded *Theft Detection* Concept

This section of Chapter 8 also evaluates new routes which are more representative of CIT deliveries. Routes A to H introduced in Chapter 7 and revisited in 8.2.1.1, were designed to evaluate the feasibility of the *Theft Detection* concept and localised tracking. The following research evaluates 4 new tracks that evaluate the embedded tracking system installed in the CIT box in a more representative environment. This research is designed to highlight any new issues that arise from using this embedded *Theft Detection* and localised tracking system in a busy Radio Frequency environment and in more practical environmental surroundings. As the practical elements of this tracking solution are being researched, current consumption was also measured which allows battery lifetime calculations to be performed which will help to estimate the lifetime of the tracker's battery.

Each track has four sub tests which involved holding the CIT box in different ways, which represent how the CIT guards can hold the cash boxes. The purpose of these sub tests is to determine if the manner in which the CIT guard holds the cash box has an effect on the localised tracking system. The four manners selected for this research are:

a. CIT box held normally with the antenna facing the van.
b. CIT box held normally with the antenna facing away from the van.
c. CIT box held with antenna facing the guard's body.
d. CIT box held against the guard's body in a cradle position.

It is very likely that the CIT box will be held in one of these ways, especially held against the guard's body as the CIT box can be quite heavy when loaded with cash. The first of four tracks, Track 1, is shown below which followed a 224m round trip into a building from an open environment close to a road, as shown in Figure 8.3 below. The trip was repeated four times, each time the CIT box was held in the manners described above.

Throughout the research into these four localised tracks, current consumption of the tracking system was measured. The purpose of this is to model the current consumption of the embedded system in order to calculate battery lifetime. This current measurement was performed using a coulomb counter in series with the tracking system's battery.

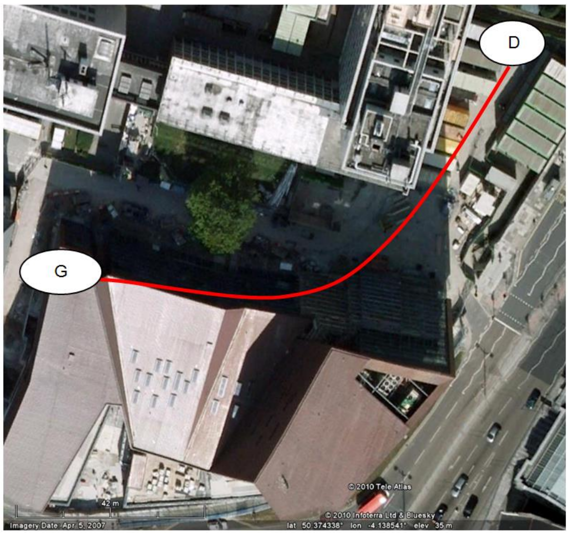

D
G
© 2010 Tele Atlas
42 m
© 2010 Infoterra Ltd & Bluesky
Imagery Date: Apr 5, 2007
lat 50.374338° lon -4.138541° elev 35 m

Figure 8.3: Track 1 – 224m route

The second track, Track 2, is shown n Figure 8.4. The track itself is a 72.2m round trip which replicates the exact cash delivery of a Loomis CIT vehicle. The delivery is to the ground floor of the Isaac Foot building at the University of Plymouth Cash Office. Permission was attained to enter the cash office and the destination transmitter was placed to the right of the cash safe in a location where the destination transmitter would most likely be installed. The research data was acquired by walking the route into the cash office to simulate a delivery behind the reinforced glass of the Cash Office.

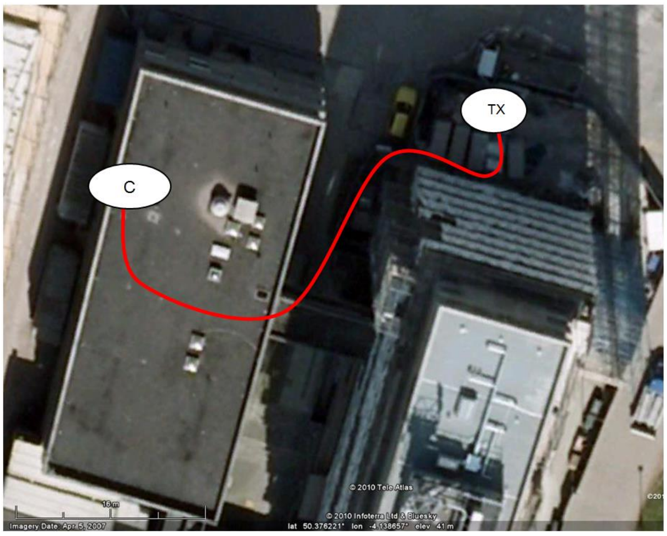

TX
C
© 2010 Tele Atlas
16 m
© 2010 Infoterra Ltd & Bluesky
Imagery Date: Apr 5, 2007
lat 50.376221° lon -4.138657° elev 41 m

Figure 8.4: Track 2 – 72.2m route

Track 3 as shown in Figure 8.5 is a 170m round trip which represents a cash delivery on the 3rd floor of a multi-storey building. Research data was collected by walking from the van into the lift on the ground floor, ascending to the 3rd floor and completing the delivery by walking to the south eastern corner of the office area where the destination transmitter was located.

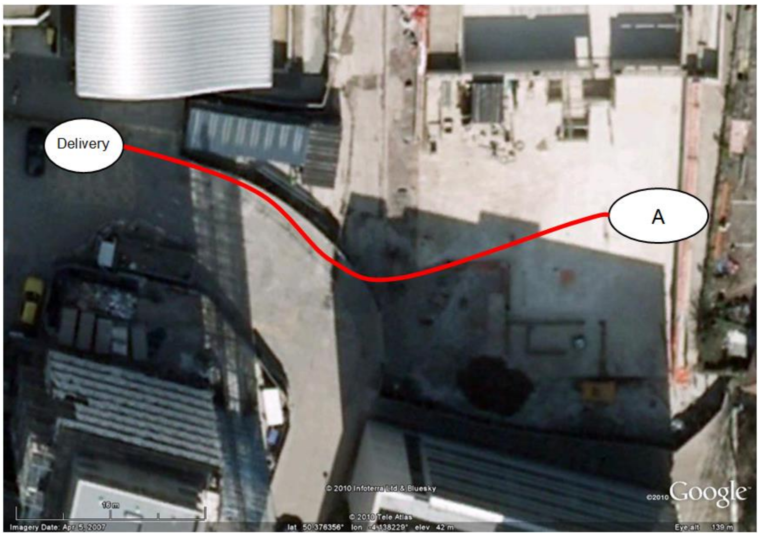


Figure 8.5: Track 3 – 170m route including 15m ascent in a lift

The final track, Track 4, was designed to investigate the effects of the tracking system without a direct line of site to the transmitter and with surrounding buildings. With a total round trip distance of 290m, it researches the practicalities of following the exterior walls of the destination’s building and the effects of a non-direct delivery point, meaning the CIT box moves away from the delivery point before it then starts approaching it.

The simulated delivery vehicle was located on the north face of the building and the delivery took place 5m inside the entrance on the east face of the building. The surrounding buildings to the east of the delivery point were a brick structure with a metal roof but the north, south and west areas surrounding the building were open spaces. This is shown in Figure 8.6.

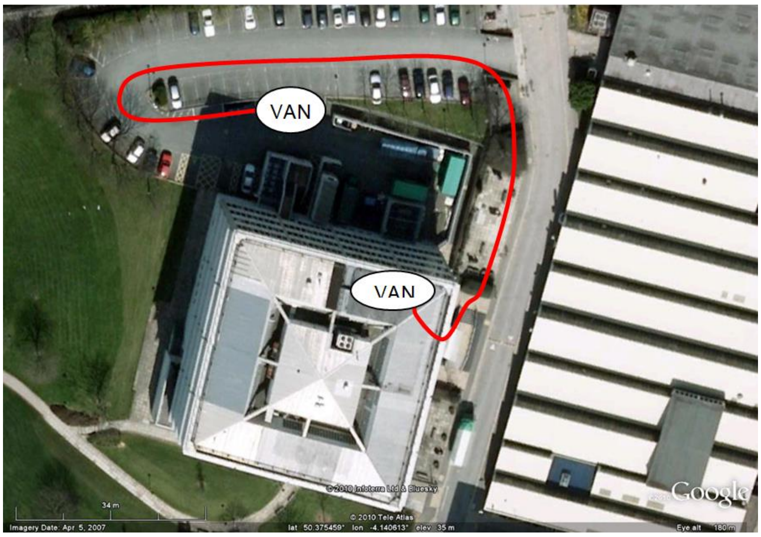

VAN
VAN
© 2010 Infoterra Ltd & Bluesky
Google
34 m
© 2010 Tele Atlas
Imagery Date: Apr 5, 2007
lat 50.375459° lon -4.140613° elev 35 m
Eye alt 180 m

Figure 8.6: Track 4 – 290m route

8.2.2 Evaluation Method of Signal Strengths in the Proximity of a Delivery Vehicle With an Embedded Device

The objective with this research is to evaluate the signal levels of the delivery access point within and around the delivery vehicle. These levels will determine if the tracking system within the CIT box can determine if it is inside the vehicle or outside it, with the intention of disabling the tracking system once inside. This functionality will give the tracking system an element of autonomy from the CIT box control system, with the intention of not having to receive instruction from the CIT box when it is about to exit the vehicle on a delivery or cash pickup. The research used a panel van to simulate the delivery vehicle and the radio setup involved the installation of the delivery access point antenna outside the delivery vehicle with an identical setup to all previous research using a simulated delivery vehicle. The delivery access point signal strength was measured around the vehicle at distances of 1, 5 and 10m. Measurements of the CIT box moving into the delivery vehicle's cargo area and shutting the door were taken to establish a signal profile as the CIT box approaches the delivery vehicle. Figure 8.7 visually shows the testing.

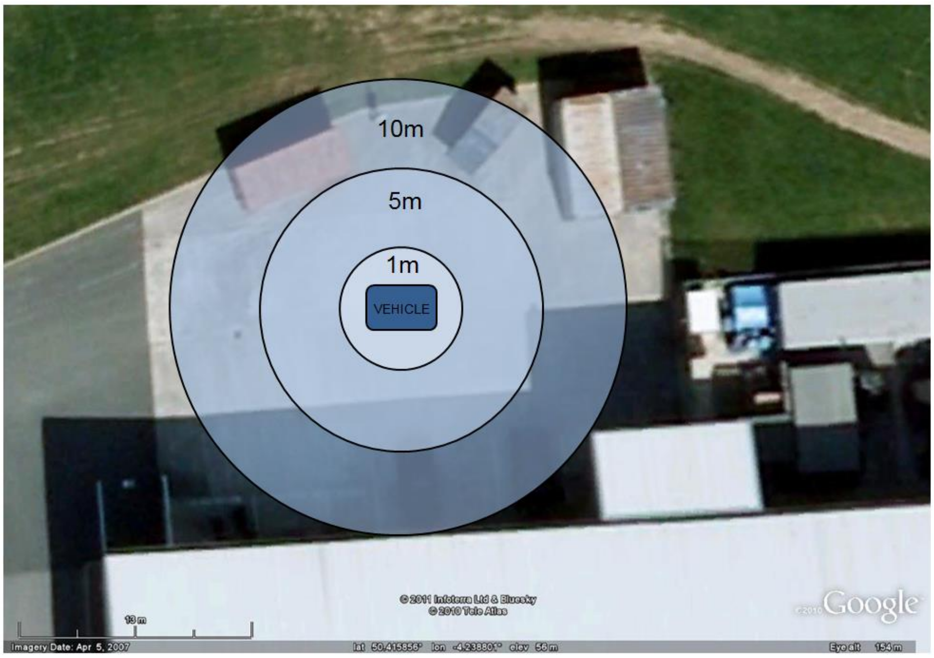

10m
5m
1m
VEHICLE
© 2011 Infoterra Ltd & Bluesky
© 2010 Tele Atlas
©2010 Google
13 m
Imagery Date: Apr 5, 2007
lat 50.415856° lon -4.238801° elev 56 m
Eye alt 154 m

Figure 8.7: Delivery access point signal evaluation

8.2.3 Evaluation Method for the Evaluation of Signal Effects Due to Orientation of a CIT Box in a *Safe Zone*

The purpose of this research is to determine how effective the *Safe Zone* concept will be with the addition of real world scenarios which simulate CIT guards who are normally in a rush. These two sets of data evaluate the impact of a guard placing the CIT box on the floor in a rushed delivery and the remaining evaluation is to simulate the more likely situation where there is a specific delivery point with a location for the CIT guard to open the box at a more manageable height.

The setup for this research requires the destination transmitter to be located in an open indoor environment with representative furniture such as desks and chairs with no obstructions from moving obstacles. The selected distance of the CIT box from the transmitting access point was set at 6m. The research required a control sample to be taken at the 6m distance with the CIT box being held. Following this control evaluation, two sets of data were gathered at this 6m distance from the destination access point with the CIT box placed on the floor and also placed horizontally on a desk at that distance. 46 samples were taken for each of these three scenarios; the control evaluation, the CIT box on the floor and the CIT box horizontally on a desk.

8.2.4 Evaluation Method for a Destination Transmitter Installed Under a Delivery Desk

This research supplements the research performed in 8.2.3 by evaluating the effects of placing a CIT box above the destination access point which is placed underneath a delivery desk. The testing involved measuring the signal strength variation over time in order to determine its effects. The purpose is to determine if there is a significant advantage to placing the CIT box in close proximity to the destination transmitter. It is possible to introduce delivery stations into the CIT delivery locations in order to implement these new concepts and assist with the robust implementation of the *Safe Zone* concept.

8.2.5 Evaluation Method for Embedded Data Exchange Methods and Simulated Authentication Timings

This following research investigates the capabilities of the embedded Wi-Fi device to connect to a proprietary wireless access point and exchange data with it. This will prove that data exchange can happen between two access points and it will evaluate the time taken for connection, data exchange and closing of the connection which simulates an authentication between the destination access point and the tracker.

The destination access point used for this evaluation differed from the standard access point that has been used in all the testing so far. This is because no data has been exchanged in any of the tests so far which means that the Wi-Fi service broadcast beacons have been used to extract signal strength and identity data. To perform this data exchange, two embedded Wi-Fi devices need to communicate with each other as only embedded devices will form part of a final CIT proprietary tracking solution. To exchange data for this research, a demo board with the embedded Wi-Fi transceiver was connected to a laptop which placed the destination Wi-Fi transceiver into Ad-Hoc mode. This function enables the Wi-Fi transceiver's service broadcast beacon. The tracker within the CIT box detected the ad-hoc network created by the destination Wi-Fi transceiver and joined with it.

The simulated transmission accounted for the following expected sequence:

a. Identifying the destination access point to connect to.
b. Establishing a physical connection to the destination access point.
c. Opening a communications channel between the tracker and the destination access point.
d. Transmitting data from the tracker to the destination access point. This data could be encrypted.
e. Receiving data from the destination access point. This data could be encrypted.
f. Closing the communications channel.
g. Unlocking the CIT box as a way of showing that authentication has been accepted.

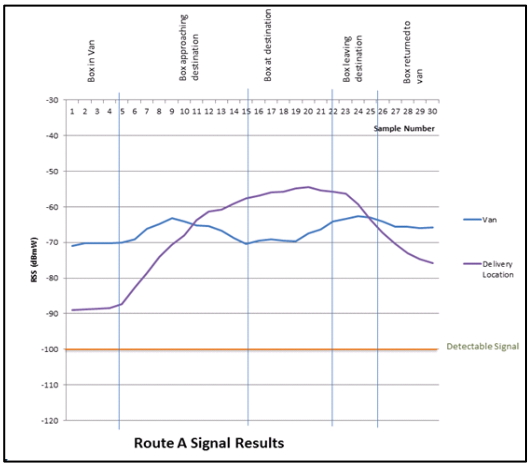
8.3 Evaluation of Results

8.3.1 Embedded Evaluation of the *Theft Detection* Concept Results

8.3.1.1 Summarises the results of the testing that was repeated with the embedded tracking system for the *Theft Detection* concept while 8.3.1.2 shows the results for the real world testing of new CIT delivery routes.

8.3.1.1 Embedded Re-Evaluation of the *Theft Detection* Concept

Figures 8.7 through to 8.22 show the results of the repeated routes described in 8.2.1.1 with the embedded tracking system. For ease of comparison, the results of the initial research performed in 7.2.1 are shown side by side with each corresponding embedded route that was re-traced. Each of the initial research results are shown on the left with the newly repeated embedded results on the right.



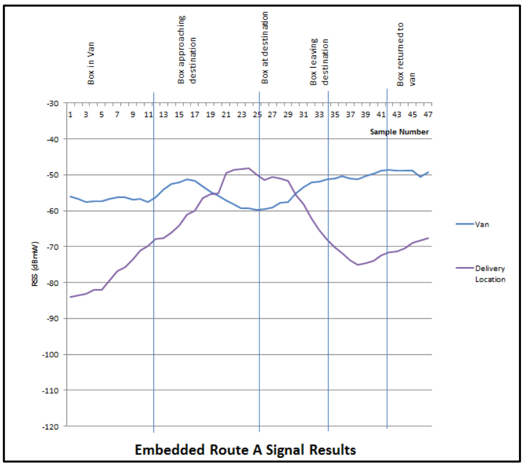
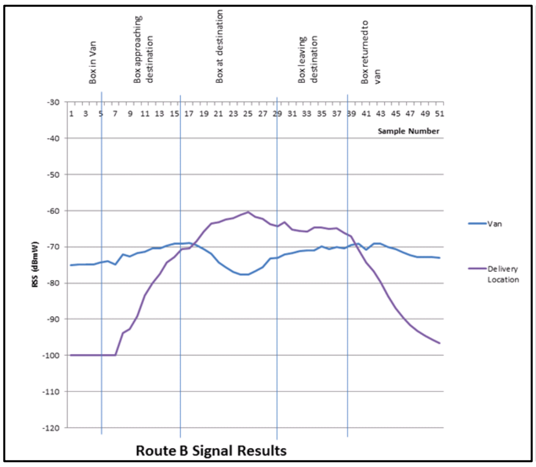


Figure 8.7: Route A Initial research Figure 8.8: Route A Embedded research



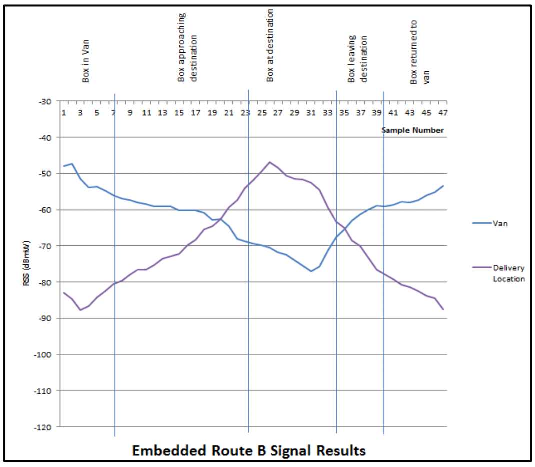
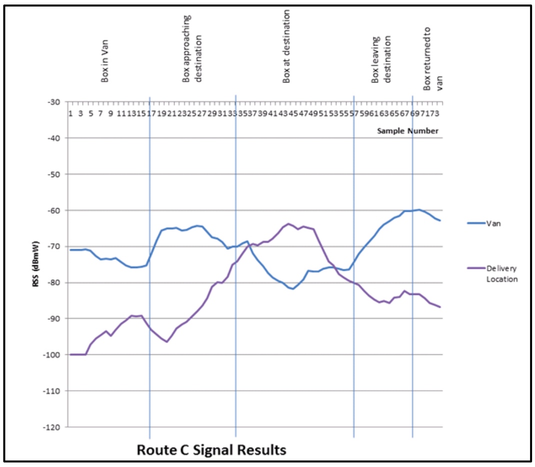


Figure 8.9: Route B Initial research Figure 8.10: Route B Embedded research



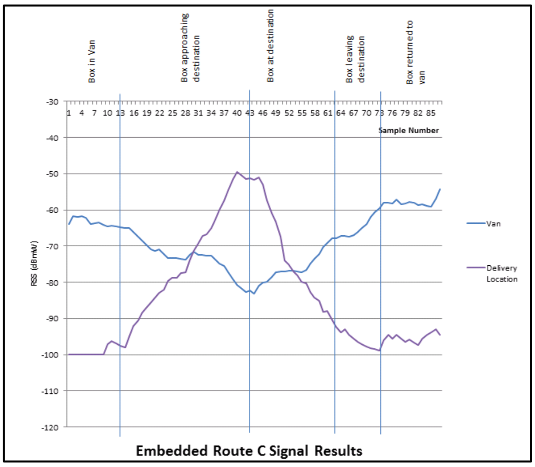
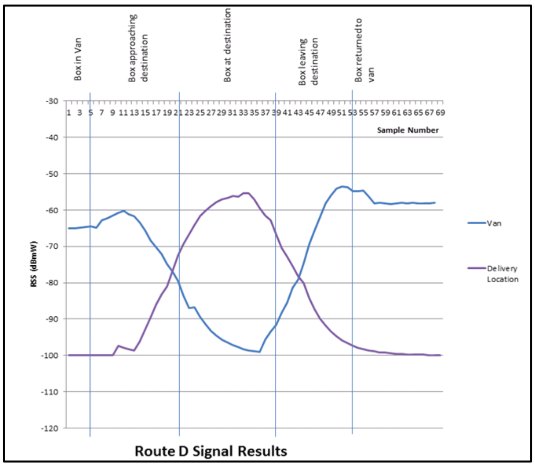


Figure 8.11: Route C Initial research Figure 8.12: Route C Embedded research



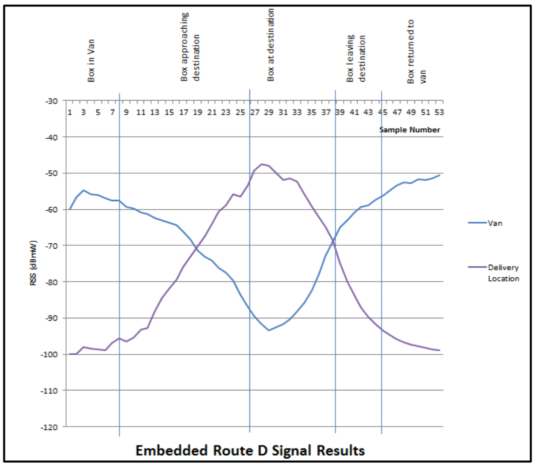
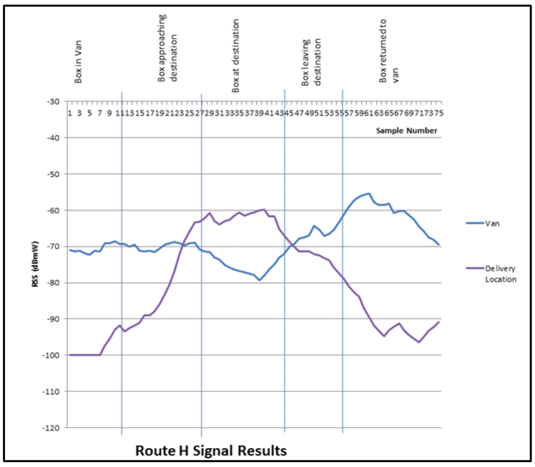


Figure 8.13: Route D Initial research

Figure 8.14: Route D Embedded research



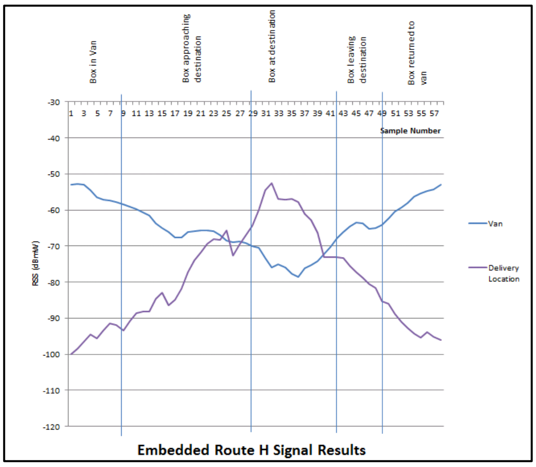
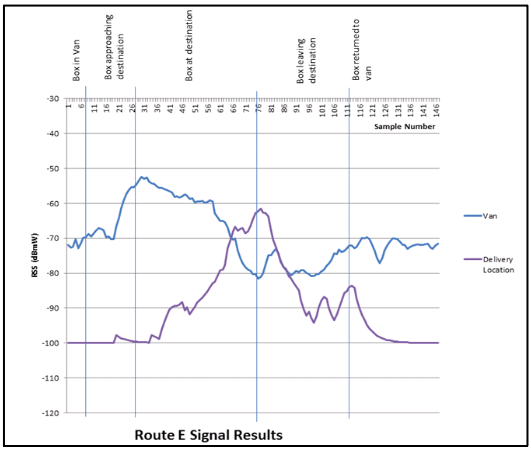


Figure 8.15: Route H Initial research

Figure 8.16: Route H Embedded research



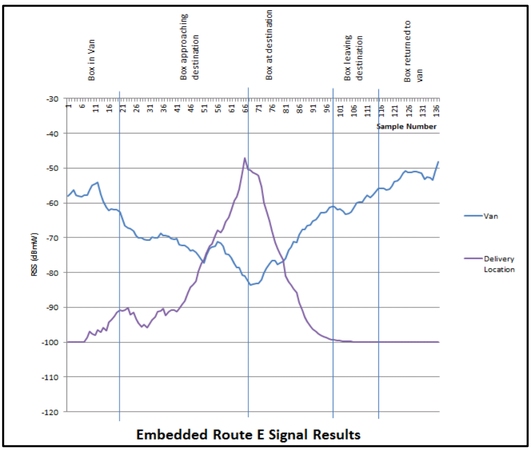


Figure 8.17: Route E Initial research

Figure 8.18: Route E Embedded research

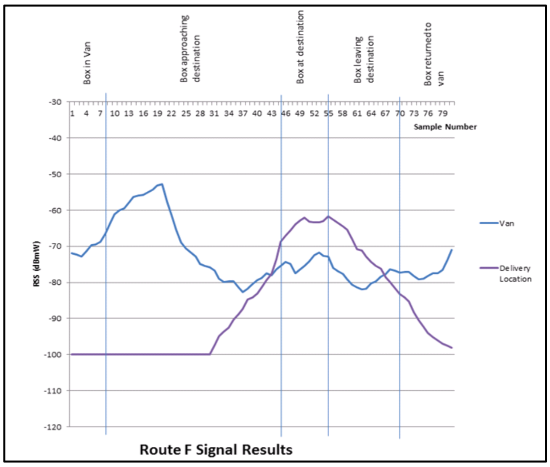


Figure 8.19: Route F Initial research

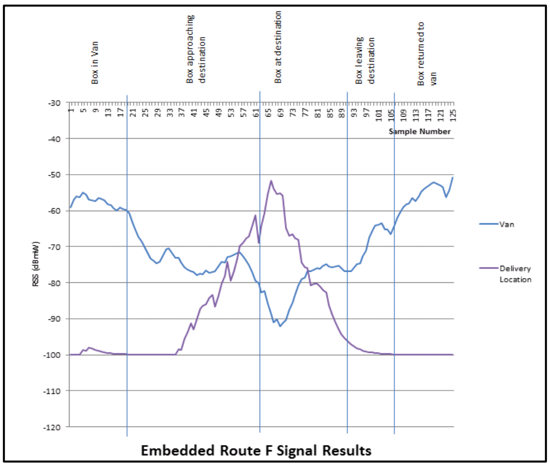


Figure 8.20: Route F Embedded research

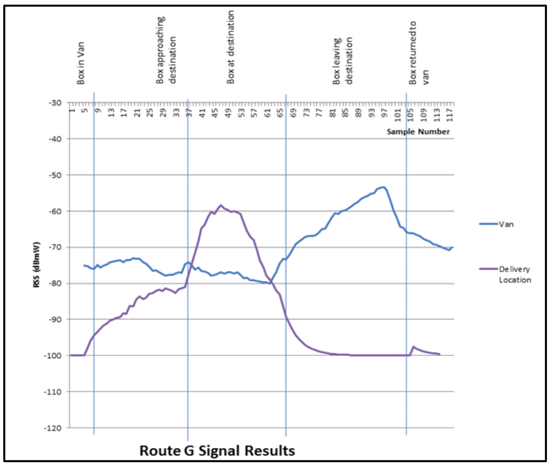


Figure 8.21: Route G Initial research

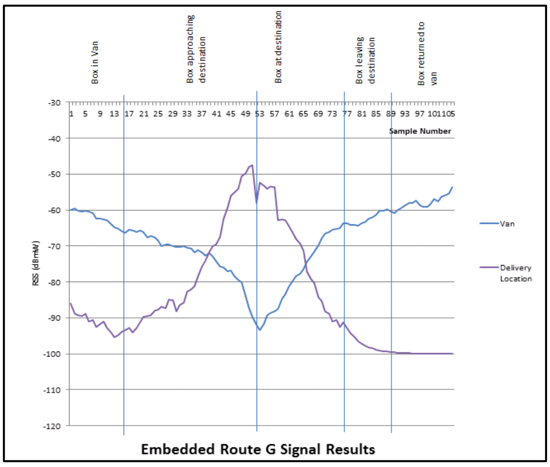


Figure 8.22: Route G Embedded research

The results show that the embedded system performs well with the resulting trends depicted by the embedded Route A research as expected. This provides confidence that valid results exist for a comparative evaluation. Comparing the new embedded research from Route A with the initial research, the embedded research performs better. The lowest recorded signal level of the simulated delivery vehicle, the van, was -60dBm which is a full 10dBm higher than the equivalent point on the initial research performed in 7.3.1. With Route B, the embedded results of both the simulated delivery van and the delivery location performed better than in the initial research. The destination was always visible with the embedded system and although the lowest recorded Van signal rivals the original Route B lowest, the overall mean Van signal is greater than the mean Van signal in the original research. There is also more clarity to the trend with the embedded results which shows that the antenna performance is better than that in the original research.

The embedded results for routes C, D and H follow a similar trend to Routes A and B. They have an overall mean signal level greater than the equivalent initial testing in 7.3.1 which means that the delivery vehicle and the destination are seen earlier and for longer. The trends are more clearly defined towards what is expected.

The embedded research results of Routes E, F and G differ to the results from the initial research in 7.3.1. The embedded results show lower signal troughs in the delivery van's signal but all the new research with the embedded systems show a clearer and better defined signal profile than in the research performed in 7.3.1. As a result, it is clearer when the destination is reached and the overall average signal strength of the delivery vehicle across all three routes was greater in the new embedded research. These more pronounced signal profiles provided by the embedded setup prove that a more reliable signal level can be achieved.

8.3.1.2 Real World CIT Routes Using the Embedded *Theft Detection* Concept

The results of each of these tracks showed promise for the embedded tracking system. The results for Track 1 are shown below in boxplot form in Figure 8.23 to visually compare the four orientations of the CIT box during this research. None of the signal levels dropped dramatically with the different orientations of the CIT box. As expected, the best performance was experienced with the CIT box facing the van with the worst performer expected to be when the CIT box was held in the guard’s arms but this was only marginally supported. The most surprising result was when the CIT box’s antenna was facing the guard as the performance of the antenna in this instance was comparable to the research performed with the CIT box facing the van.

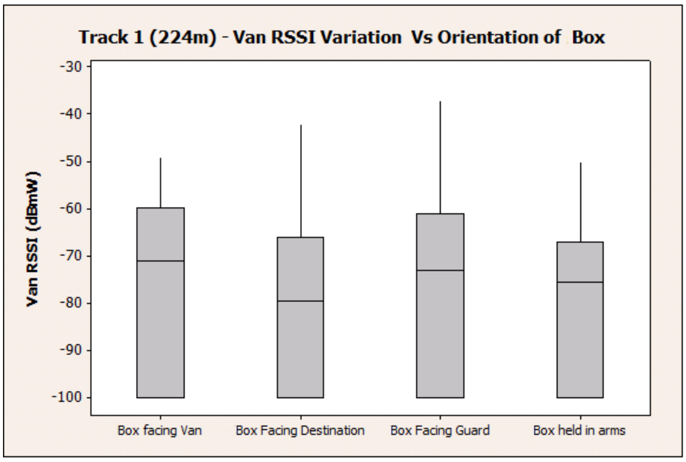


Figure 8.23: Boxplot of the results comparing Track 1 orientation

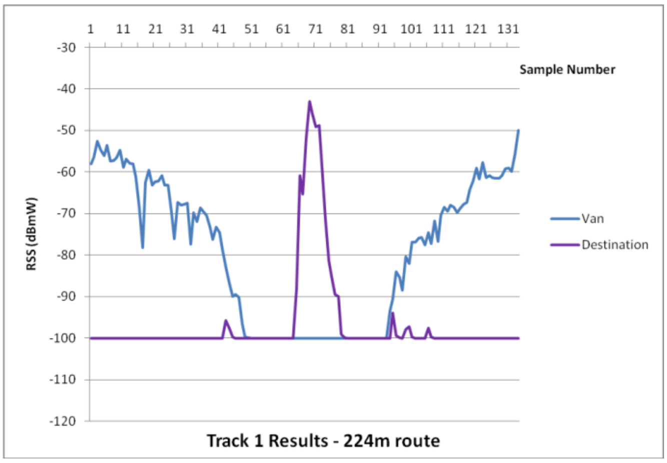


Figure 8.24: Track 1 signal results

The results of Track 2's research show that the signal strength was rarely undetectable as is shown by the outliers in the box plot below. This is because Track 2 is a short distance track. There is a clear trend visible from the box plots with the highest average signal strength achieved as expected, with the CIT box facing the van and the second highest signal strength achieved with the CIT box facing the guard. The worst signal strength is noted when the CIT box is held in the guard's arms but because of the short distance, the effectiveness of the tracking system was not compromised.

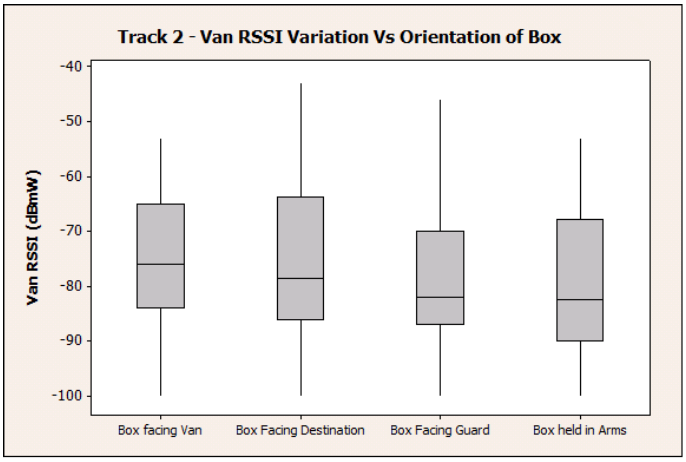


Figure 8.25: Boxplot of the results comparing Track 2 orientation

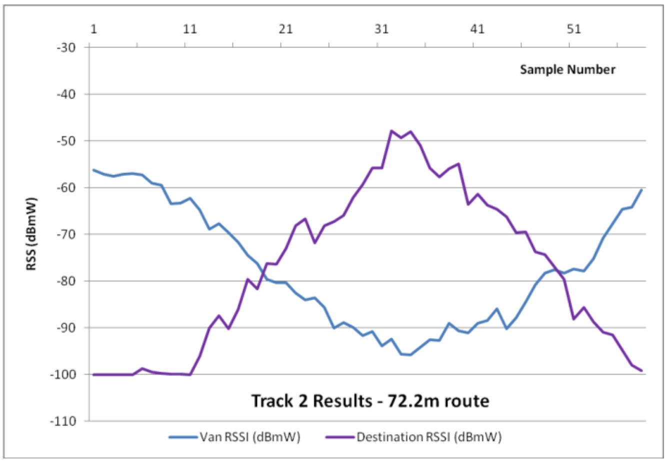


Figure 8.26: Track 2 signal results

The results from Track 3 below in Figures 7.27 and 7.28 show a different trend than those seen in any of the research so far. The medians of the three first tests (Facing van, Facing Destination and Facing Guard) are at the minimum of -100dBmW which shows that the majority of the samples were out of the range of the transmitter.

The mean signal strengths of these four tests were -82.84dBmW, -86.89dBmW, -87.77dBmW and -85.68dBmW respectively. This shows an odd trend where CIT box is held in the arms of the guard. The median for this evaluation was -

88dBmW and shows that with the CIT box held in the arms of the guard, better results were achieved than in previous tests. This is attributed to the amount of time that this last track took as waiting for the lift took less time in this instance, and therefore any conclusions drawn from the median result are not valid.

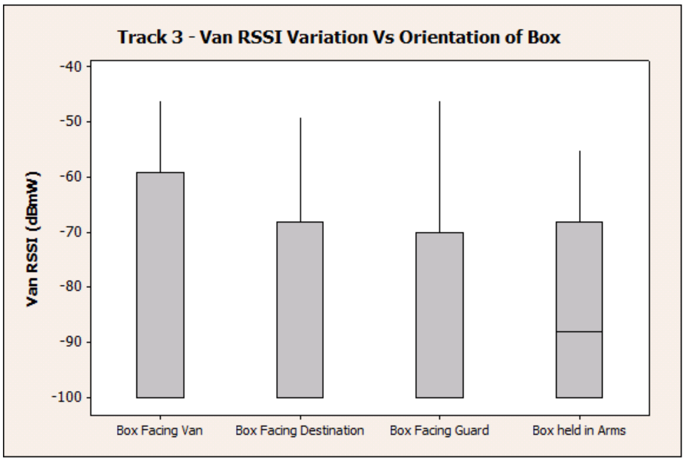


Figure 8.27: Boxplot of the results comparing Track 3 orientation

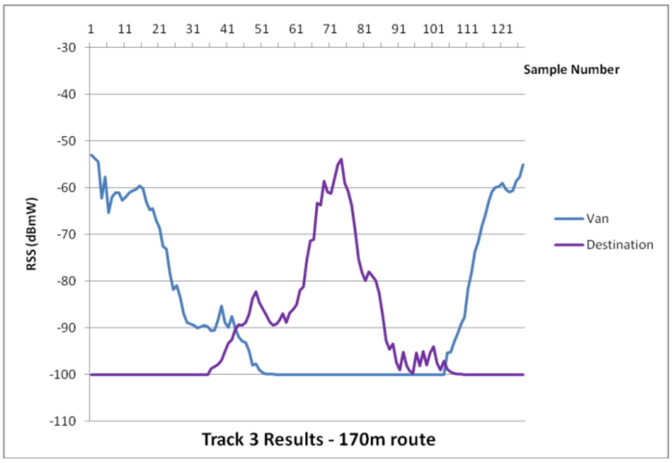


Figure 8.28: Track 3 signal results

The results of the final track, Track 4, show the best results are achieved with the CIT box facing the delivery vehicle. This has been true for the research into these four tracks thus far. Within this researched track, the results with the CIT box facing the destination proved to be very comparable to the results with the CIT box facing the van.

The worst performer was with the CIT box facing the guard. It is likely that the environment surrounding this setup produced these results. Comparatively, the CIT box held in the guard's arms performed as in the other tests; however the average signal strength with the CIT box in the guard's arms is 3dB lower which keeps the average signal quite high at -74dBmW. These results are shown graphically below.

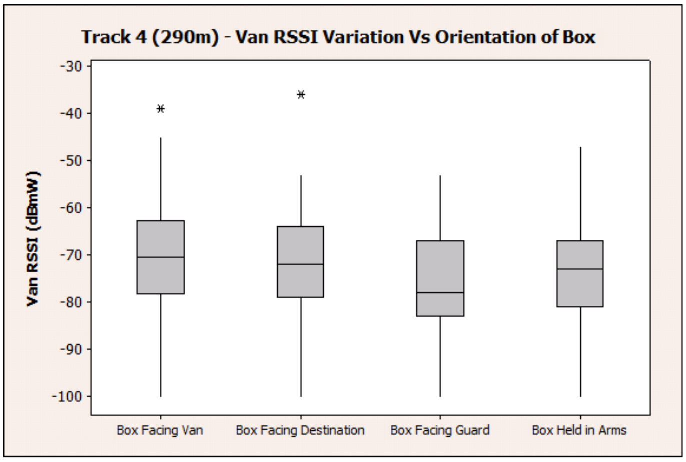


Figure 8.29: Boxplot of the results comparing Track 4 orientation

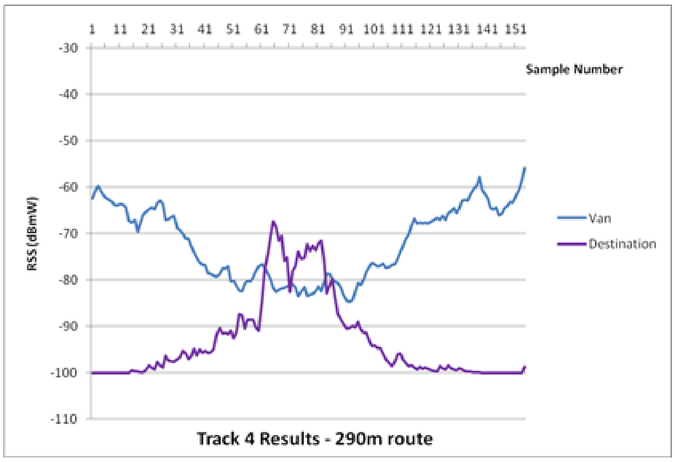


Figure 8.30: Track 4 signal results

Table 8.1 below shows the recorded current consumed by the tracking system for each track that was performed in the above research. Variations of the tracks are shown as a to d and they represent each method by which the CIT box was held during the research.

Track	Current (mAh)	Average
Track1a	10.236	10.6625
Track1b	11.942	
Track1c	11.089	
Track 1d	9.383	
Track2a	5.118	5.33125
Track2b	5.971	
Track2c	5.118	
Track2d	5.118	
Track3a	10.236	11.72875
Track3b	12.795	
Track3c	11.942	
Track3d	11.942	
Track4a	11.942	12.3685
Track4b	12.795	
Track4c	11.942	
Track4d	12.795	

Table 8.1: Currents for each track

The lowest recorded current consumption was 5.118mAh and as expected, this was observed on the shortest route of Track 2, 72.2m. The highest recorded current consumption was recorded on Track 4 as this was the longest track at 290m. There were no unexpected variations with the current measurements and the trends reflected the reality that current consumption increases with distance travelled.

Table 8.2 shows a calculated result of distance vs average current consumption for all four of the tracks researched above. The trend observed indicates that the shorter routes draw more energy per metre than the shorter routes. This is because the start-up time and therefore the start-up current of the embedded device from an off state is more dominant in the shorter distances. As the distance increases, the start-up time has less of an effect over the current consumed per metre travelled.

Average current consumed per metre distance	
Track Number	**Average current consumed per metre travelled**
Track 1 (224m)	48µAh/m
Track 2(72.2m)	74µAh/m
Track 3 (170m)	69µAh/m
Track 4 (290m)	43µAh/m

Table 8.2: Average current consumed per metre distance travelled.

8.3.2 Signal Strengths in the Proximity of a Delivery Vehicle With an Embedded Device

The results of this research are presented graphically below. The boxplot in figure 8.31 shows the variation in signal strength at the three selected distances from the delivery vehicle, supplemented by the descriptive statistics in 8.32 relating to the three distances from the delivery vehicle.

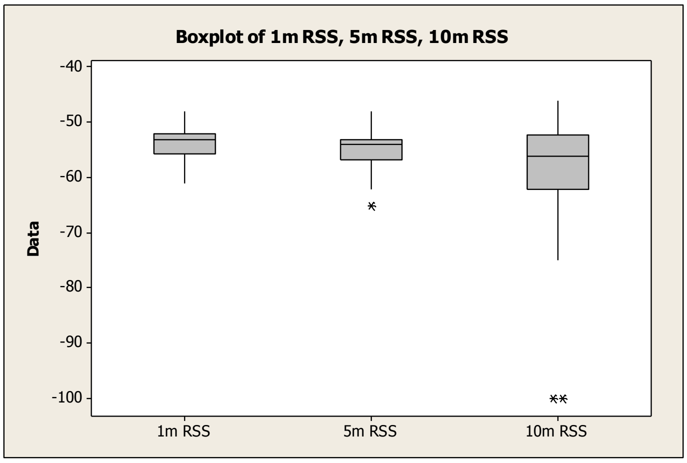


Figure 8.31: Variation in received signal strength over the 3 tested distances from the delivery vehicle

Variable	N	N*	Mean	SE Mean	StDev	Minimum	Q1	Median	Q3
1m RSS	44	0	-53.955	0.522	3.464	-61.000	-55.750	-53.000	-52.000
5m RSS	48	0	-54.646	0.494	3.424	-65.000	-56.750	-54.000	-53.000
10m RSS	96	0	-58.427	0.918	8.994	-100.000	-62.000	-56.000	-52.250

Figure 8.32: Descriptive statistics for the distances to the delivery vehicle

It is expected that the signal level will vary more with the increasing distance from the delivery vehicle and the trend shows this. This is due to increasing effect of Radio Wave reflections as the distance from the delivery vehicle’s transmitter increases. The 10m evaluated distance shows a few outliers that reveal the Van transmitter was not visible to the tracker. This can be attributed to nulls in the RF signal due to reflections or less likely, an error with the Wi-Fi transceiver not detecting the RF signal. The average signal at 10m is -4.5dB lower than at the 1m evaluated distance. At 5m the average difference in signal strength is -0.7dB. The medians for these evaluations show little skew to the distribution therefore there is confidence in the averages of the results.

The following Figures 8.33 and 8.34 show the signal strength over time as the CIT box approached the delivery vehicle and entered it. The cargo door of the delivery vehicle was shut and the recorded data is shown in 8.34.

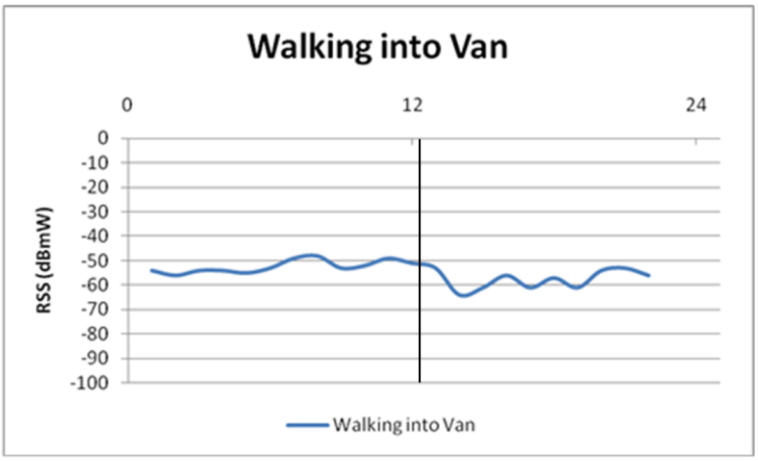


Figure 8.33: Signal results recorded whilst walking into the van

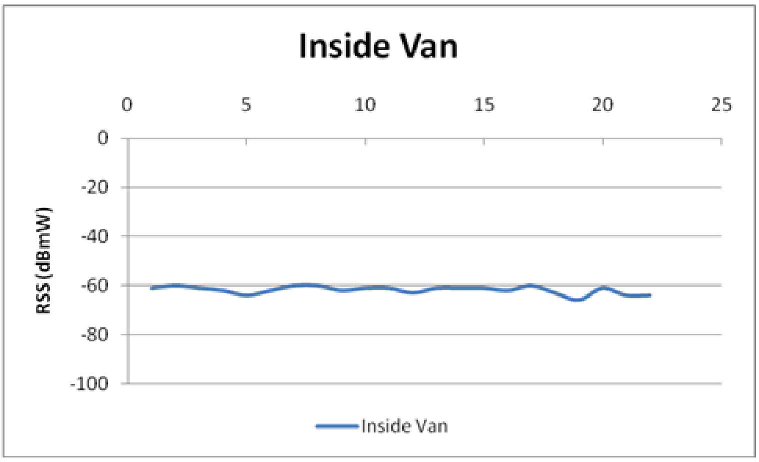


Figure 8.34: Signal results recorded whilst inside the van with the cargo door closed

Samples 0-12 in Figure 8.33 show the signal strength before entering the van. The transition is at sample 12 therefore all data after sample 12 is indicative of the tracker inside the van. The average signal strength whilst the CIT box was approaching the van was -54.5dBmW. This decreased after the tracker was inside the van. The average signal strength was then recorded at -57dBmW indicating a loss of -2.5dB.

With delivery vehicle door shut, the average received signal strength was recorded at -62dBmW which is a significant drop when compared to the average results seen with the van door open. When compared with the 1m mean result of -53.995 dBmW, the total loss between the CIT box being outside the delivery vehicle and moving inside the vehicle and shutting the door is 8dBmW.

8.3.3 Results for the Evaluation of Signal Effects Due to Orientation of a CIT Box in a *Safe Zone*

The results of the average signal strengths are shown in Table 8.3 below.

Control	On floor	Horizontal on desk
Average	Average	Average
-47.30	-42.83	-45.89

Table 8.3: Average signal strengths from the orientation research

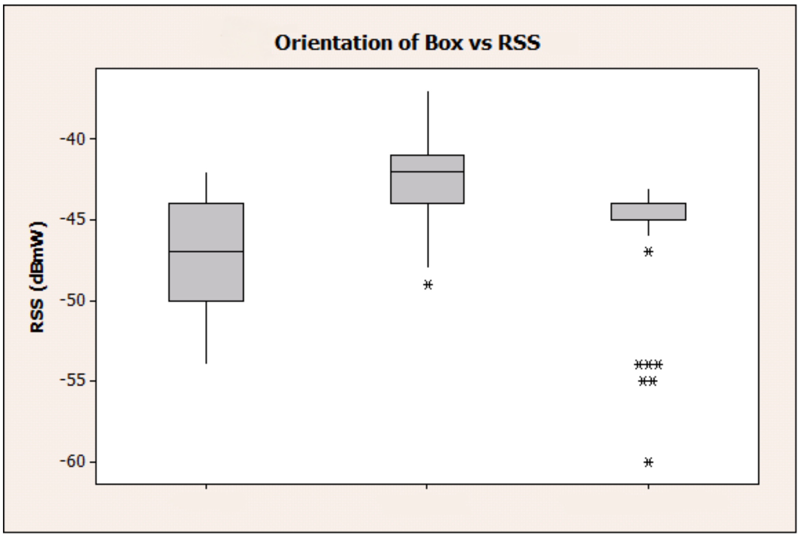


Figure 8.35: Boxplot showing the variation in signal strengths for the three tests performed

The box plot in Figure 8.35 graphically shows the variation between the three sets of data and the variation within each of these tests. The average signal strengths recorded over the 46 samples show that the best performance is achieved with the CIT box on the floor but the most stable results were achieved with the CIT box placed horizontally on the desk. This difference between the floor and the desk is due to attenuation of the signal at the desk and unfavourable RF reflections affecting the measurement. This difference is not considered significant. The control evaluation accounts for the circumstance where the CIT box is opened mid-air which is unlikely but not impossible. This data shows that the orientation of the CIT box will have little effect on the *Safe Zone* during delivery.

8.3.4 Destination Transmitter Installed Under a Delivery Desk

The two plots 8.36 and 8.37 below show the resulting signal variation in the recorded data for this evaluation. This data demonstrates that the horizontal orientation of the CIT box and the placement of the destination access point provide a high *Safe Zone* signal strength and stability of the received signal strength. Both of these factors are desirable for the *Safe Zone* signal characteristics.

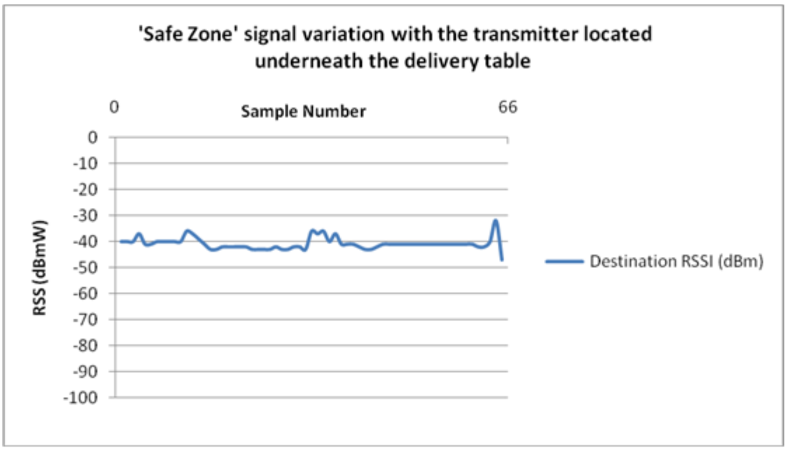


Figure 8.36: Signal characteristics over time with the CIT box placed above the transmitter

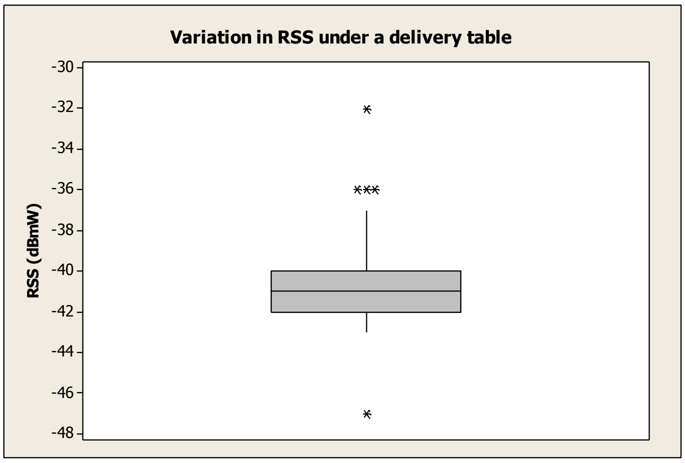


Figure 8.37: Variation in signal strength with the CIT box placed above the transmitter

8.3.5 Embedded data exchange methods and simulated authentication timings

The results of 6 connection attempts yielded the timing results are shown below in Table 8.4.

Connection Time (s)	Average Connection Time (s)
5.59	5.96
5.75	
6.15	
6.09	
6.09	
6.09	

Table 8.4: Results of the 6 connection timings

8.3.6 Discussion

This chapter has produced a tracking system for use in a CIT box. The designed hardware has been engineered to integrate into a CIT box with minimal intrusion and it has been used in this chapter to prove that an integrated tracking system can perform in the manner that supports the research in previous chapters. This chapter has focussed on the embedded evaluation of *Theft Detection* tracking and the *Safe Zone* concept. *Profile Tracking* has not been an embedded research focus as the application requires too much investment in order to be implemented in the UK market.

The designed hardware functioned as designed, and throughout the testing the hardware operated without issues. The mechanical integration into the CIT box also occurred without faults and it is due to confidentiality that this thesis cannot show the full extent of the integration and discuss the hardware more in depth. The new Antenova antenna designed for this testing was tuned using a Vector Network Analyser to operate with the selected network service provider in the GSM1800 band. The Wi-Fi antenna was also tuned to counter the effects that the CIT box has on Wi-Fi antennas. The embedded software was adjusted to suit the testing that was being performed at the time. Each revision of the embedded software was debugged and tested before research data was collected. This ensured that the software had no errors that could influence the research.

Section 8.2.1 used Chapter 7's research methods to prove that the embedded tracking system can function as well as the laptop that was used for the initial research in the previous chapters. The research in 8.2.1.1 yielded more repeatable results than its equivalent research in 7.2.1 which gave confidence that the embedded hardware was performing well. It is has also proven that a well tuned Wi-Fi and GSM combination antenna connected to a bespoke embedded tracker can perform the tasks required to provide the CIT industry with the bespoke tracking solution that the industry requires. The new research in section 8.2.1.2 proves that the system can function as designed with an actual CIT delivery route. It has also proved that there is an optimal orientation of a CIT box and optimal placement of the Wi-Fi antenna in the CIT box but this has not compromised the effectiveness of the tracking method. That research has proved that in order to get optimal range performance, two antennas using the antenna diversity techniques researched in Chapter 5 should be used on the final tracking solution.

The research in section 8.2.2 has shown that with the *Theft Detection* system proposed in this thesis, the tracker is not able to detect when it is inside or outside the delivery vehicle. In order for the tracker to identify it is safe within the delivery vehicle, an increase in signal strength is required. The research so far has shown that there is a decrease in signal strength and this alone is not enough for the tracker to reliably gauge that it is inside the delivery vehicle. Alternatives to this strategy would be to split the delivery vehicle's transmitted signal and install an antenna inside the van. This would provide the increase in signal strength required when inside the delivery vehicle but introduce a loss into the delivery vehicle's transmitted signal which would ultimately compromise the range of the *Theft Detection* tracking. This would be of no value to the overall system. The proposed solution would be to integrate the tracker with the CIT box's main controller and utilise existing CIT box docking systems to disable the tracker. This system requires communication between the CIT box and the tracker but it is more robust than using RF signals to determine when to shut down the tracker.

The embedded evaluation of the *Safe Zone* in 8.2.3 determined that the orientation of the CIT box is not too critical to the implementation of the *Safe Zone* concept. However, if the concept was to extend to an enhancement of the CIT box's core functionality, i.e. as a replacement for the customer's identity tag, it is best that the delivery point meets certain criteria. The criteria were determined through all of the research within 8.2.3 and can be readily used.

The resulting conclusions of the research in 8.3.4 are that the destination access point is best located underneath a bespoke delivery table and the CIT box opened horizontally on that table. It provides the CIT box with a strong and consistent signal. Additional support for this installation is that access points installed underneath a delivery tables will provide an element of security as it conceals the access point from the CIT guards, customers and most of all, robbers. As cash pickups and deliveries do not normally take place in open areas, this solution is not intrusive to CIT guards or customers.

The final research for this thesis presented in 8.3.5 demonstrates that it could take up to 6 seconds for the current embedded system to authenticate with a destination access point. CIT guards are normally in a rush to complete their rounds and therefore 6 seconds may appear to be an unacceptable length of time for a CIT guard to wait for the CIT box to authenticate with a destination transceiver. If this time is considered in the context of a delivery, longer times can be experienced in a cash delivery where the CIT guard has to wait for the customer to locate their identity tag and unlock the CIT box. With this considered, removing the customer’s tag from the equation has the potential to reduce delivery times despite the authentication time.

8.3.7 Conclusions

In conclusion to this chapter, the designed embedded tracking system has been tested and compared against results of previous non-embedded testing where the tracking methodologies were defined. This chapter has proved that the designed embedded tracking solution for CIT is feasible and a robust platform for future development beyond the prototype stage has been created.

9. Conclusion of the Research Study

The research presented in this thesis has been tailored to meet the specific tracking requirements of the Cash in Transit. The research has explored the state of the art in tracking technologies used both globally and some technologies specific to the CIT industry. With this research, underlying knowledge of the CIT industry and the input from Spinnaker International Ltd, this thesis has researched into the use of 2.4 GHz Wi-Fi technologies, discovered the limitations and further researched into the capabilities of a product that will provide the Cash in Transit industry with the tracking system that they require to meet their industry's demands.

9.1 Research achievements

The research into the tracking technologies available has unveiled that Wi-Fi based tracking is now one of the predominant location-based services around. With this information and the research into existing and alternative tracking technologies, this thesis has explored the capabilities of Wi-Fi systems as a suitable solution to the Cash in Transit industry's embedded tracking system. Although other tracking methods exist, they are nearly all Radio Frequency based systems with the exception of Inertial Navigation. With this knowledge, the first level of confidence is that Wi-Fi based tracking systems show promise simply by the fact this solution is RF based also.

With this confidence, this thesis has progressed into researching the capabilities of Wi-Fi as a tracking technology and this research has shown that there are several methods to provide localisation using Wi-Fi; however the most popular and widely available method uses commercially available Wi-Fi positioning services due to availability and simplicity of the techniques. A brief evaluation of the Skyhook Wireless Wi-Fi positioning service has led to further chapters evaluating 2.4GHz Wi-Fi signals in order to understand the effects when used within the CIT environment.

Knowledge of the effects of different material types and maximum range of 2.4GHz Wi-Fi has been achieved, which has provided this tracking system with a theoretical range. This allows a CIT tracking system operator to use that range as an estimator of the distance of the CIT box from the access point. Research into the effects of signal interference have revealed that the 2.4GHz Radio Frequency can be jammed using cheap commercially available devices and this has allowed the research to understand the vulnerabilities of the tracking system. As the nature of this tracking system is based around recovery after theft, research has been performed into the effects of different vehicles on the signal strength of 2.4GHz Wi-Fi to understand the losses that will be experienced when the tracking system is placed in that situation.

The research that has been performed into the effects of the CIT box on transmitting antennas has shown that optimisation can be performed that counters the negative effects that the CIT box has on antennas, therefore improving the capabilities of the CIT box to detect weak signals and improve its operating RF range.

The unique 2.4GHz Wi-Fi tracking concepts conceived for the CIT industry have demonstrated that Wi-Fi tracking can be used in a more local manner by ensuring that the CIT box is within a safe area defined by 2.4GHz Wi-Fi RF boundaries. These concepts have been proven to enhance the CIT box's security and provide a rapid, automatic theft detection system. Further to this, non-proprietary Wi-Fi access point tracking has been thoroughly researched and the limitations of this technology have been understood and compared against the GPS tracking method.

The research and development presented in the final research chapter has shown that an embedded tracking system created for the CIT industry demonstrates the capabilities of all this research. It has done so by performing comparative experiments and enhancing them with further research. This has provided validation towards the tracking systems use as a bespoke and unique embedded tracking system.

9.2 Limitations of the research

This section describes some limitations in the research that has featured in this thesis. With radio frequency testing, there are experiments that are best performed in an anechoic chamber in order to achieve the most accurate results. The signal evaluations and measurements performed in this thesis were not performed in an anechoic chamber but were performed with real world receivers and real world environments. What this means is that RF reflections can have an effect on results such as the maximum range of a 2.4GHz Wi-Fi signal. Signal measurements were taken with real world receivers rather than with calibrated receivers and antennas. The magnitude of these effects is unknown but the advantage for this research is that real world results are useful to this application.

The Antenova antenna tuning research that was performed has shown that the Antenova antenna can be tuned to function well within the CIT box' antenna locator. This research was performed on a sample of two antennas and it is likely that there will be differences in performance between antennas when in volume production. These differences can be due to the antennas builds, component tolerances and drifts over temperature, as well as mechanical differences such as increased thickness of antenna locators and variation in the moulding of the locators. It is possible that production solutions will involve manually tuning an antenna to match specific antenna locators and these two items will be paired as an assembly. It is also possible that production solutions may not want to implement antenna locators to antenna matching and therefore will allow the variation in tuning to be counted as an acceptable loss.

The limitations of Wi-Fi localisation have already been discussed; however a more general limitation is that commercial Wi-Fi positioning is not yet available in every country that restricts this technology's application to those countries that have this capability. Due to the increasing demand by smartphone users, this technology will continue to expand which will eventually make commercial Wi-Fi positioning feasible in more countries.

During this research, it has been suggested that there are vulnerabilities with using open Wi-Fi access points and that data transmission would have to be encrypted. This is indeed a limitation of this research and it would be diligent to ensure that all proprietary access points are adequately secured to ensure that they cannot be imitated. It has also been noted that data exchange with the Wi-Fi chipset used in the embedded research is difficult. It is likely that if a tracking solution was designed, based around the currently selected Wi-Fi chipset, there would be failures to initiate communications between the tracker and the authenticating party. A robust solution would need to be in place if there was to be authentication between the tracker and the van or destination.

The research performed in Chapters 7 and 8 has demonstrated concepts which have been proven to work well. The weakest of the concepts is the *Profile Tracking* concept which will require significant financial investment by the CIT companies in the UK. It is limited also by the resources to update each profile, which will require human involvement unless a sophisticated self-repairing algorithm can be implemented. This leads on to one of the greatest limitations which is the cost associated with creating these proprietary networks. There are many delivery destinations which will require a proprietary Wi-Fi based access point and this is a significant investment for the CIT companies. The costs for each node will be the key factor in the design of them.

9.3 Future work

With the limitations described above, there is potential for future work. The most significant piece of work would be to investigate how to integrate "intelligence" processing on the centralised system to provide more robust detection and correlation of information. Similar to existing *Security Event Management (SEM)* systems utilised within organisation networks, the system would be able to provide valuable centralised intelligence in order to be able to respond in a more timely and appropriate fashion. Future work would also need the weaknesses identified and appropriate countermeasures developed to ensure that the vulnerabilities in the tracking concepts are eliminated. This would also require researching optimisation techniques for authentication and researching the vulnerabilities in the Destination and Delivery access points.

With the understanding of vulnerabilities and the research into the security of these concepts as suggested above, further investigations can be performed into integration of the tracking system into the locking and unlocking mechanism of the CIT box. With this suggested future work, it is also feasible to investigate the effects of linking the tracking system and its *Theft Detection* concepts into the degradation system of the CIT box. This would substantially enhance the security of the CIT box and ensure that the contents were degraded before the attack began, thus deterring thieves from future theft attempts. The research would need to highlight the risks associated with false activations and be positioned to minimise those risks.

Since this research began, IEEE 802.11n-2009 specification has been released and has changed the wireless access point market. This specification now also applies to the 5GHz Wi-Fi band which opens further opportunities for research and use of the 5GHz Wi-Fi frequency for the concepts introduced in this thesis. The use of such high frequencies may open opportunities for reduced antenna sizes without the compromises from the losses of the acetal antenna locators on the CIT box. This research could help to optimise and future proof the tracking system.

With regards to the *Profile Tracking* concept, a desirable concept would be to have a self-healing database, which will account for the uncontrollable element of non-proprietary access points disappearing whilst the profile is expecting to see them. Future work could see an algorithm and process developed to automatically scan for new access points when a profile is being executed and send this data back to a central location to be verified before the route's profile is appended.

This research and the work presented in this thesis is believed to be unique and has achieved an innovative embedded tracking system which provides the CIT industry with improved local and global tracking capabilities.

References

802.11-1999. (2003). *IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.

802.15.4-2011. (2011). *IEEE Standard for Local and metropolitan area networks-Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)*.

Abad, E., Palacio, F., Nuin, M., Zárate, A., Juarros, A., Gómez, J. and Marco, S. (2009). RFID smart tag for traceability and cold chain monitoring of foods: Demonstration in an intercontinental fresh fish logistic chain. *Journal of food engineering*, 93(4), pp.394--399.

Abdullah, J. (2011). The Design of Mobile Control Car Security System. *IACSIT International Journal of Engineering and Technology*, 3(3).

Acharya, D., Kumar, V., Garvin, N., Greca, A. and Gaddis, G. (2008). A sun SPOT based automatic vehicular accident notification system. pp.296--299.

Aggarwal, J. and Cai, Q. (1997). Human motion analysis: A review. *Nonrigid and Articulated Motion Workshop*, pp.90--102.

Ai, Y., Sun, Y., Huang, W. and Qiao, X. (2007). OSGi based integrated service platform for automotive telematics. *2007 IEEE International Conference on Vehicular Electronics and Safety*, pp.1--6.

Allerton, D. and Jia, H. (2005). A review of multisensor fusion methodologies for aircraft navigation systems. *Journal of Navigation*, 58(03), pp.405--417.

Angeles, R. (2005). RFID technologies: supply-chain applications and implementation issues. *Information Systems Management*, 22(1), pp.51--65.

Bacha, A., Reinholtz, C., Wicks, A., Fleming, M., Naik, A., Avitabile, M. and Elder, N. (2004). The DARPA Grand Challenge: overview of the Virginia Tech vehicle and experience. *Intelligent Transportation Systems*, pp.481--486.

Bahl, P. and Padmanabhan, V. (2000). RADAR: An in-building RF-based user location and tracking system. 2, pp.775--784.

Bajaj, R., Ranaweera, S. and Agrawal, D. (2002). GPS: location-tracking technology. *Computer*, 35(4), pp.92--94.

Bastide, F., Chatre, E., Macabiau, C. and Roturier, B. (2001). GPS L5 and Galileo E5a/E5b signal-to-noise density ratio degradation due to DME/TACAN signals: simulations and theoretical derivation. *Proceedings of the 2004 National Technical Meeting of The Institute of Navigation, San Diego, CA*, pp.1049--1062.

Behringer, R., Sundareswaran, S., Gregory, B., Elsley, R., Addison, B., Guthmiller, W., Daily, R. and Bevly, D. (2004). The DARPA grand challenge-development of an autonomous vehicle. *Intelligent Vehicles Symposium*, pp.226--231.

Behringer, R., Travis, W., Daily, R., Bevly, D., Kubinger, W., Herzner, W. and Fehlberg, V. (2005). Rascal-an autonomous ground vehicle for desert driving in the darpa grand challenge 2005. *Intelligent Transportation Systems*, pp.644--649.

Bobick, J. and Bryson, A. (1973). Updating inertial navigation systems with VOR/DME information. *AIAA Journal*, 11(10), pp.1377--1384.

Bonnor, N. (2012). A Brief History of Global Navigation Satellite Systems. *Journal of Navigation*, 65(01), pp.1--14.

Borgeest, K. (n.d.). Practical papers, articles and application notes: EMC aspects of car communication systems. *Electromagnetic Compatibility Magazine, IEEE*, 1(1), pp.35--41.

Brakatsoulas, S., Pfoser, D., Salas, R. and Wenk, C. (2005). On map-matching vehicle tracking data. pp.853--864.

Brennan, W. (2010). Safer lone working: assessing the risk to health professionals. *British Journal of Nursing*, 19(22), p.1428.

Brewer, A., Sloan, N. and Landers, T. (1999). Intelligent tracking in manufacturing. *Journal of Intelligent Manufacturing*, 10(3-4), pp.245--250.

Broggi, A., Caraffi, C., Porta, P. and Zani, P. (2006). The single frame stereo vision system for reliable obstacle detection used during the 2005 DARPA grand challenge on TerraMax. *Intelligent Transportation Systems Conference*, pp.745--752.

Brown, A. (2005). Gps/ins uses low-cost mems imu. *Aerospace and Electronic Systems Magazine, IEEE*, 20(9), pp.3--10.

Brusey, J. and McFarlane, D. (2009). Effective RFID-based object tracking for manufacturing. *International Journal of Computer Integrated Manufacturing*, 22(7), pp.638--647.

Bryson, A. and Bobick, J. (1972). Improved navigation by combining VOR/DME information and air data. *Journal of Aircraft*, 9(6), pp.420--426.

Bshara, M., Orguner, U., Gustafsson, F. and Van Biesen, L. (2011). Robust tracking in cellular networks using HMM filters and cell-ID measurements. *Vehicular Technology, IEEE Transactions on*, 60(3), pp.1016--1024.

Carter, N. (2012). The past, present and future challenges of aircraft EMC. *Electromagnetic Compatibility Magazine, IEEE*, 1(1), pp.75-78.

Caruso, M. (2000). Applications of magnetic sensors for low cost compass systems. *Position Location and Navigation Symposium, IEEE*, pp.177--184.

Chitte, S. and Dasgupta, S. (2008). Distance estimation from received signal strength under log-normal shadowing: Bias and variance. pp.256--259.

Cichon, D. and Wiesbeck, W. (1994). Indoor and outdoor propagation modeling in pico cells. pp.491--495.

Cleaver, R. (1947). The development of single-receiver automatic adcock direction-finders for use in the frequency band 100-150 Mc/s. *Electrical Engineers-Part IIIA: Radiocommunication, Journal of the Institution of*, 94(15), pp.783--797.

Cox, D. (1978). INTEGRATION OF GPS WITH INERTIAL NAVIGATION SYSTEMS (MISCELLANEOUS TOPICS). *Navigation*, 25(2), pp.236--245.

Curran, I. and Pluta, S. (2008). Overview of machine to machine and telematics. *IET*.

Dabin, J., Ni, N., Haimovich, A., Niver, E. and Grebel, H. (2003). The effects of antenna directivity on path loss and multipath propagation in UWB indoor wireless channels. pp.305--309.

Dai, H., Ng, K., Li, M. and Wu, M. (2011). An overview of using directional antennas in wireless networks. *International Journal of Communication Systems*.

Dai, W., Cuhadar, A. and Liu, P. (2008). Robot tracking using vision and laser sensors. *Automation Science and Engineering, 2008. CASE 2008. IEEE International Conference on*, pp.169--174.

Davis, B. and DeLong, R. (1996). Combined remote key control and immobilization system for vehicle security. *Power Electronics in Transportation*, pp.125--132.

Duan, J. and Wang, F. (2013). The research and implementation of intelligent vehicle based on differential GPS and inertial navigation system. pp.4768--4772.

Ely, J. (2005). Electromagnetic interference to flight navigation and communication systems: new strategies in the age of wireless. *AIAA Atmospheric Flight Mechanics Conference and Exhibit*.

Engelberger, J. (1993). Health-care robotics goes commercial: The ’helpmate’ experience. *Robotica*, 11(6), pp.517--523.

Evans-Pughe, C. (2006). Ro4d W4tch. *Engineering Technology*, 1(4), pp.36-39.

Farrell, G., Tseloni, A. and Tilley, N. (2011). The effectiveness of vehicle security devices and their role in the crime drop. *Criminology and Criminal Justice*, 11(1), pp.21--35.

Feng, F., Shengyu, H. and Qi, X. (2010). The Research of the ZigBee and RFID Fusion Technology in the Coal Mine Safety. *3rd International Conference on Information Management, Innovation Management and Industrial Engineering*.

Fuchs, C., Aschenbruck, N., Martini, P. and Wieneke, M. (2011). Indoor tracking for mission critical scenarios: A survey. *Pervasive and Mobile Computing*, 7(1), pp.1--15.

Gao, G. (2007). DME/TACAN Interference and its Mitigation in L5/E5 Bands. *In ION Institute of Navigation Global Navigation Satellite Systems Conference*.

Garfield, W. (1958). TACAN: a navigation system for aircraft. *Proceedings of the IEE-Part B: Radio and Electronic Engineering*, 105(9S), pp.298--306.

Gaukel, J. (2000). *Apparatus and method for continuous electronic monitoring and tracking of individuals*. US Patent No. 6,100,806.

Getting, I. (1993). Perspective/navigation-the global positioning system. *Spectrum, IEEE*, 30(12), pp.36--38.

Gill, M. (2001). The craft of robbers of cash-in-transit vans: crime facilitators and the entrepreneurial approach. *International journal of the sociology of law*, 29(3), pp.277--291.

Glidden, R., Bockorick, C., Cooper, S., Diorio, C., Dressler, D., Gutnik, V., Hagen, C., Hara, D., Hass, T., Humes, T. and others, (2004). Design of ultra-low-cost UHF RFID tags for supply chain applications. *Communications Magazine, IEEE*, 42(8), pp.140--151.

Gonzalez-Novarro, M. (2007). It matters how you sell it: Lojack in Mexico. *Retrieved July*, 12, p.2010.

Gordon, A. and Wolf, R. (2007). License Plate Recognition Technology. *FBI Law Enforcement Bulletin*, 76(3), p.8.

Guha, S., Plarre, K., Lissner, D., Mitra, S., Krishna, B., Dutta, P. and Kumar, S. (2012). Autowitness: locating and tracking stolen property while tolerating gps and radio outages. *ACM Transactions on Sensor Networks (TOSN)*, 8(4), p.31.

Hatay, M. (1980). Empirical formula for propagation loss in land mobile radio services. *Vehicular Technology, IEEE Transactions on*, 29(3), pp.317--325.

Hawthorne, W. and Daugherty, L. (1965). VOR/DME/TACAN frequency technology. *Aerospace and Navigational Electronics, IEEE Transactions on*, 12(1), pp.11--15.

Hazas, M., Scott, J. and Krumm, J. (2004). Location-aware computing comes of age. *Computer*, 37(2), pp.95--97.

Hebblewhite, B. (2009). Mine safety--through appropriate combination of technology and management practice. *Procedia Earth and Planetary Science*, 1(1), pp.13--19.

Hewat, A. and Cheek, C. (1993). Possibilities of using satellites for lone worker alarms. *Satellite Distress and Safety Systems, IEE Colloquium on*, pp.8--1, 8--6.

Hind, D. (1994). Radio frequency identification and tracking systems in hazardous areas. *IET*.

Hoffmann, G., Tomlin, C., Montemerlo, D. and Thrun, S. (2007). Autonomous automobile trajectory tracking for off-road driving: Controller design, experimental validation and racing. *American Control Conference*, pp.2296--2301.

Holmström, J., Kajosaari, R., Främling, K. and Langius, E. (2009). Roadmap to tracking based business and intelligent products. *Computers in Industry*, 60(3), pp.229--233.

Hossain, E., Chow, G., Leung, V., McLeod, R., Mišic, J., Wong, V. and Yang, O. (2010). Vehicular telematics over heterogeneous wireless networks: A survey. *Computer Communications*, 33(7), pp.775--793.

Huang, X., Zhu, W. and Lu, D. (2010). Underground miners localization system based on ZigBee and WebGIS. *Geoinformatics, 2010 18th International Conference on*, pp.1--5.

Hunter, T., Kosmalski, W. and Truong, P. (1990). Vehicle navigation using differential GPS. pp.392--398.

IEEE Standard for Long Wavelength Wireless Network Protocol. (2009). *IEEE Std 1902.1-2009*, pp.1-25.

ISO11898-1 – Road Vehicles CAN. (2003). [online] Available at: http://www.iso.org.

ISO26262 – Road Vehicles Functional Safety. (2011). [online] Parts 1-9. Available at: http://www.iso.org.

ISO26262 – Road Vehicles Functional Safety. (2012). [online] Part 10. Available at: http://www.iso.org.

Juels, A. (2006). RFID security and privacy: A research survey. *Selected Areas in Communications, IEEE Journal on*, 24(2), pp.381--394.

Kafka, P. (2012). The Automotive Standard ISO 26262, the Innovative Driver for Enhanced Safety Assessment \& Technology for Motor Cars. *Procedia Engineering*, 45, pp.2--10.

Kennedy, G. and Foster, P. (2006). High resilience networks and microwave propagation in underground mines. *Wireless Technology, 2006. The 9th European Conference on*, pp.193--196.

Khangura, K., Middleton, N. and Ollivier, M. (1993). Vehicle anti-theft system uses radio frequency identification. pp.4--1.

King, A. (1998). Inertial navigation-forty years of evolution. *GEC review*, 13(3), pp.140--149.

Kobilarov, M., Sukhatme, G., Hyams, J. and Batavia, P. (2006). People tracking and following with mobile robot using an omnidirectional camera and a laser. *Proceedings 2006 IEEE International Conference on*, pp.557--562.

Koifman, M. and Bar-Itzhack, I. (1999). Inertial navigation system aided by aircraft dynamics. *Control Systems Technology, IEEE Transactions on*, 7(4), pp.487--493.

Koo, J. and Cha, H. (2012). Unsupervised Locating of WiFi Access Points Using Smartphones. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 42(6), pp.1341--1353.

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H. and others, (2010). Experimental security analysis of a modern automobile. *Security and Privacy (SP)*, pp.447--462.

Koshima, H. and Hoshen, J. (2000). Personal locator services emerge. *Spectrum, IEEE*, 37(2), pp.41--48.

Kosmas, C., Tripp, N., Westington, A., Clarke, N. and Tjai, C. (2011). *A container and security systems*. GB Patent No. GB2472632.

Kuang, W. and Morris, A. (1999). Ultrasonic Doppler distance measurement technique for robot tracking system. *Electronics Letters*, 35(11), pp.942--943.

Kulkarni, P., Khatri, A., Banga, P. and Shah, K. (2009). Automatic Number Plate Recognition (ANPR) System for Indian conditions. *RADIOELEKTRONIKA '09. 19th International Conference*, pp.111--114.

Küpper, A. (2005). *Location-based services*. 1st ed. Chichester, England: John Wiley.

Kuriger, G., Grant, H., Cartwright, A. and Heirman, D. (2003). Investigation of spurious emissions from cellular phones and the possible effect on aircraft navigation equipment. *Electromagnetic Compatibility, IEEE Transactions on*, 45(2), pp.281--292.

L Trautenberg, H., Weber, T. and Schafer, C. (2004). GALILEO system overview. *Acta Astronautica*, 55(3), pp.643--647.

Leonard, J. and Durrant-Whyte, H. (1991). Mobile robot localization by tracking geometric beacons. *Robotics and Automation, IEEE Transactions on*, 7(3), pp.376-382.

Leow, Y. and Shang, Y. (2010). Mobile robot tracking in wireless sensor networks. *Networking, Sensing and Control (ICNSC), 2010 International Conference on*, pp.313--318.

Li-min, Y., Anqi, L., Zheng, S. and Hui, L. (2008). Design of monitoring system for coal mine safety based on wireless sensor network. *Mechtronic and Embedded Systems and Applications*, pp.409--414.

Martínez-Sala, A., Egea-López, E., García-Sánchez, F. and García-Haro, J. (2009). Tracking of returnable packaging and transport units with active RFID in the grocery supply chain. *Computers in Industry*, 60(3), pp.161--171.

Maurya, K., Singh, M. and Jain, N. (2012). Real Time Vehicle Tracking System using GSM and GPS Technology-An Anti-theft Tracking System. *International Journal of Electronics and Computer Science Engineering (IJECSE, ISSN: 2277-1956)*, 1(03), pp.1103--1107.

Mech, L. and Barber, S. (2002). A critique of wildlife radio-tracking and its use in national parks. *A report to the US National Park Service*, pp.19--20.

Meng, M. and Kak, A. (1993). NEURO-NAV: a neural network based architecture for vision-guided mobile robot navigation using non-metrical models of the environment. *Robotics and Automation, 1993. Proceedings., 1993 IEEE International Conference on*, pp.750--757.

Michael, K. and McCathie, L. (2005). The pros and cons of RFID in supply chain management. pp.623--629.

Michael, K., McNamee, A. and Michael, M. (2006). The emerging ethics of humancentric GPS tracking and monitoring. *Mobile Business, 2006. ICMB '06. International Conference on*, pp.34--34.

Min, Z., Wenfeng, L., Zhongyun, W., Bin, L. and Xia, R. (2007). A RFID-based material tracking information system. *Automation and Logistics, 2007 IEEE International Conference on*, pp.2922--2926.

Mine Safety and Health Administration, (2011). *Program Policy Letter No. P11-V-13*.

Mitra, S., Zheng, Z., Guha, S., Ghosh, A., Dutta, P., Krishna, B., Plarre, K., Kumar, S. and Sinha, P. (2009). An affordable, long-lasting, and autonomous theft detection and tracking system. pp.351--352.

Mustafa, M., Behnam, M. and El-Tarhuni, M. (2006). A Wireless Embedded System for the Tracking of Stolen Vehicles. *Computer Systems and Applications, IEEE International Conference on*, pp.818--825.

Navizon, (2012). *Navizon Features*. [online] Available at: http://www.navizon.com/navizon-how-it-works.

Ni, L., Zhang, D. and Souryal, M. (2011). RFID-based localization and tracking technologies. *Wireless Communications, IEEE*, 18(2), pp.45--51.

Nutter, R. (2007). Underground Coal Mine Communications and Tracking Status SAGO Plus One Year. *IEEE Industry Applications Annual Meeting*, pp.2086-2089.

Ochieng, W., Sauer, K., Walsh, D., Brodin, G., Griffin, S. and Denney, M. (2003). GPS integrity and potential impact on aviation safety. *The journal of navigation*, 56(01), pp.51--65.

Oxford Dictionaries, (n.d.). *track: definition of track in Oxford dictionary (British & World English)*. [online] Available at: http://oxforddictionaries.com/definition/english/track [Accessed 21 Jul. 2013].

Pandey, S. and Agrawal, P. (2006). A survey on localization techniques for wireless networks. *Journal of the Chinese Institute of Engineers*, 29(7), pp.1125--1148.

Park, J., Park, S., Kim, D., Cho, P. and Cho, K. (2003). Experiments on radio interference between wireless LAN and other radio devices on a 2.4 GHz ISM band. 3, pp.1798--1801.

Placeengine, (2011). *PlaceEngine Coverage Area*. [online] Available at: http://www.placeengine.com/showe/about.

Powell, C. (1958). The Decca navigator system for ship and aircraft use. *Proceedings of the IEE-Part B: Radio and Electronic Engineering*, 105(9), pp.225--234.

Powell, C. (1982). Performance of the Decca Navigator on land. *Communications, Radar and Signal Processing, IEE Proceedings F*, 129(4), pp.241--248.

Powers, W. and Nicastri, P. (2000). Automotive vehicle control challenges in the 21st century. *Control engineering practice*, 8(6), pp.605--618.

Qiang, C., Ji-ping, S., Zhe, Z. and Fan, Z. (2009). ZigBee Based Intelligent Helmet for Coal Miners. *Computer Science and Information Engineering, 2009 WRI World Congress on*, 3, pp.433--435.

Quddus, M., Ochieng, W. and Noland, R. (2006). Map Matching Algorithms for Intelligent Transport Systems Applications.

Rao, K., Nikitin, P., Lam, S. (2005). Antenna design for UHF RFID tags: A review and a practical application. *Antennas and Propagation, IEEE Transactions on*, 53(12), pp.3870--3876.

Redmill, K., Martin, J. and Ozguner, O. (2006). Sensing and sensor fusion for the 2005 Desert Buckeyes DARPA grand challenge offroad autonomous vehicle. *Intelligent Vehicles Symposium*, pp.528--533.

Richards, J., Fullerton, L., Kelly, D., Meigs, D., Payment, T., Finn, J., Tucker, W. and Welch, W. (2002). *"System and method for tracking and monitoring prisoners using impulse radio technology*. U.S. Patent No. 6,489,893.

Roberts, A. (2012). Motor Vehicle Recovery A Multilevel Event History Analysis of NIBRS Data. *Journal of Research in Crime and Delinquency*, 49(3), pp.444--467.

Salvador, C., Zani, F. and Gentili, G. (2011). RFID and sensor network technologies for safety managing in hazardous environments. pp.68--72.

Sangwan, R., Qiu, R. and Jessen, D. (2005). Using RFID tags for tracking patients, charts and medical equipment within an integrated health delivery network. *Networking, Sensing and Control*, pp.1070--1074.

Sayed, A., Tarighat, A. and Khajehnouri, N. (2005). Network-based wireless location: challenges faced in developing techniques for accurate wireless location information. *Signal Processing Magazine, IEEE*, 22(4), pp.24--40.

Scogna, A. and Wang, J. (2008). Study of a conformal hidden wire antenna used for the detection of stolen cars. pp.1--6.

Serrano, O., Rodero Merino, L., Matell'an Olivera, V. and Canas, J. (2012). Robot localization using wifi signal without intensity map.

Seymour, S., Baker, R. and Besco, M. (2001). Inmate Tracking With Biometric and Smart Card Technology. *Corrections Today*, 63(4), pp.75--77.

Shaw, D. and Pease, K. (2010). Car security and the decision to recommend purchase. *Crime Prevention \& Community Safety*, 12(2), pp.91--98.

Skyhook Inc., (2013). *Skyhook Location Performance*. [online] Available at: http://www.skyhookwireless.com/location-technology/performance.php.

Smith, L. and Louis, E. (2010). Cash in transit armed robbery in Australia. *Trends and issues in crime and criminal justice*, (397), p.1.

Song, H., Zhu, S. and Cao, G. (2008). Svats: A sensor-network-based vehicle anti-theft system.

Spinnaker Product Range. (n.d.). [online] Available at: http://www.spinnaker.co.uk/products.html [Accessed 31 May. 2014].

Sun, Z., Bebis, G. and Miller, R. (2006). On-road vehicle detection: A review. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 28(5), pp.694--711.

Sunderman, C. and Waynert, J. (2012). An overview of underground coal miner electronic tracking system technologies. *Industry Applications Society Annual Meeting (IAS)*, pp.1--5.

Tangruamsub, S., Tsuboyama, M., Kawewong, A. and Hasegawa, O. (2009). Mobile robot vision-based navigation using self-organizing and incremental neural networks. *," Neural Networks, 2009. IJCNN 2009. International Joint Conference on*, pp.3094--3101.

Tatale, S. and Khare, A. (2011). Real time ANPR for vehicle identification using neural network. *International Journal of Advances in Engineering & Technology*, 1(4), pp.262-268.

Thrun, S., Bennewitz, M., Burgard, W., Cremers, A., Dellaert, F., Fox, D., Hahnel, D., Rosenberg, C., Roy, N., Schulte, J. and others, (1999). MINERVA: A second-generation museum tour-guide robot. *Robotics and Automation*, 3.

Thrun, S. (2006). Winning the darpa grand challenge: A robot race through the mojave desert. *Automated Software Engineering*, pp.18-22.

Tian, J. and Zhu, J. (2011). Positioning system for miners based on RFID. *Multimedia Technology (ICMT), 2011 International Conference on*, pp.626--629.

Tippenhauer, N., Rasmussen, K., Pöpper, C. and Čapkun, S. (2009). Attacks on public WLAN-based positioning systems. pp.29--40.

Trevisani, E. and Vitaletti, A. (2004). Cell-ID location technique, limits and benefits: an experimental study. pp.51--60.

Turk, M., Morgenthaler, D., Gremban, K. and Marra, M. (1988). VITS-A vision system for autonomous land vehicle navigation. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 10(3), pp.342--361.

Turner, D., Savage, S. and Snoeren, A. (2011). On the empirical performance of self-calibrating WiFi location systems. pp.76--84.

Tuttle, J. (1997). Traditional and emerging technologies and applications in the radio frequency identification (RFID) industry. *Radio Frequency Integrated Circuits (RFIC) Symposium*, pp.5--8.

Umpleby, K. (1947). Airborne automatic direction-finders. *Electrical Engineers-Part IIIA: Radiocommunication, Journal of the Institution of*, 94(15), pp.693--704.

Venkatraman, S. and Caffery, J. (2004). Hybrid TOA/AOA techniques for mobile location in non-line-of-sight environments. 1, pp.274--278.

Verma, M., Lange, R. and McGarry, D. (2007). A study Of US crash statistics from automated crash notification data. pp.18--21.

Wahab, A., Chong, T., Wah, N., Eng, O. and Keong, W. (1997). A low-cost yet accurate approach to a vehicle location tracking system. 1, pp.461--465.

Walter, T., Enge, P., Blanch, J. and Pervan, B. (2008). Worldwide vertical guidance of aircraft based on modernized GPS and new integrity augmentations. *Proceedings of the IEEE*, 96(12), pp.1918--1935.

Wang, J., Luo, Z., Wong, E. and Tan, C. (2007). RFID assisted object tracking for automating manufacturing assembly lines. *ICEBE 2007. IEEE International Conference on*, pp.48--53.

Wang, W. and Zhu, Q. (2008). RSS-based Monte Carlo localisation for mobile sensor networks. *Communications, IET*, 2(5), pp.673--681.

Wang, X., Zhao, X., Liang, Z. and Tan, M. (2007). Deploying a wireless sensor network on the coal mines. *," Networking, Sensing and Control, 2007 IEEE International Conference on*, pp.324--328.

Wang, Y., Li, X. and Huang, Y. (1996). Navigation system of pilotless aircraft via GPS. *Aerospace and Electronic Systems Magazine, IEEE*, 11(8), pp.16--20.

Wei, S. and Li-li, L. (2009). Multi-parameter monitoring system for coal mine based on wireless sensor network technology. *Industrial Mechatronics and Automation, 2009. ICIMA 2009. International Conference on*, pp.225--227.

Wheatley, S. (1993). Tracker-stolen vehicle recovery system. *Vehicle Security Systems, IEE Colloquium on*, pp.1/1 - 1/3.

White, R. (1962). Airborne Doppler Radar Navigation of Jet Transport Aircraft. *Aerospace and Navigational Electronics, IRE Transactions on*, (1), pp.11--20.

Wicks, A., Visich, J. and Li, S. (2006). Radio frequency identification applications in hospital environments. *Hospital topics*, 84(3), pp.3--9.

Win, M. and Scholtz, R. (2002). Characterization of ultra-wide bandwidth wireless indoor channels: a communication-theoretic view. *IEEE J. Select. Areas Commun.*, 20(9), pp.1613-1627.

Wolf, M., Weimerskirch, A. and Paar, C. (2004). Security in automotive bus systems. *In Proceedings of the Workshop on Embedded Security in Cars*.

Woodman, O. (2007). An introduction to inertial navigation. *University of Cambridge, Computer Laboratory, Tech. Rep. UCAMCL-TR-696*, 14, p.15.

Wu, A., Johnson, E. and Proctor, A. (2005). Vision-aided inertial navigation for flight control. *Journal of Aerospace Computing, Information, and Communication*, 2(9), pp.348--360.

Yang, W. and Huang, Y. (2007). Wireless sensor network based coal mine wireless and integrated security monitoring information system. *Networking, 2007. ICN '07. Sixth International Conference on*, pp.13, 22--28.

Zandbergen, P. and Barbeau, S. (2011). Positional accuracy of assisted gps data from high-sensitivity gps-enabled mobile phones. *Journal of Navigation*, 64(03), pp.381--399.

Zandbergen, P. (2009). Accuracy of iPhone Locations: A Comparison of Assisted GPS, WiFi and Cellular Positioning. *Transactions in GIS*, 13, pp.5-25.

Zhang, K., Zhu, M., Wang, Y., Fu, E. and Cartwright, W. (2009). Underground mining intelligent response and rescue systems. *Procedia Earth and Planetary Science*, 1(1), pp.1044--1053.

Zhao, Y. (2002). Telematics: safe and fun driving. *IEEE Intelligent Systems*, 17(1), pp.10--14.