KCA UNIVERSITY

SCHOOL OF COMPUTING AND INFORMATION MANAGEMENT

RFID HAND HELD DEVICES TRACING AND RECOVERY

BY

JOHN GITHIARI KANYONI

REG.NO: KCA 12/02508

Supervisor: Prof. Ddembe Williams

A Research project submitted in partial fulfillment of the requirement for the award of the degree of Masters of Science in Data Communication.

DECLARATION

I declare that this research project is my original work and has not been published previously or submitted elsewhere for award of a degree. I also declare that this research project contains no material written or published by any other persons expect where due citation is made and author duly acknowledged

Students Name: John Githiari Kanyoni Reg. No. 12/02508

Sign: _____ Date _____

I do hereby confirm that I have examined this master's research project of

John G. Kanyoni

And have certified that all revisions that the research panel and examiners recommended have been adequately addressed.

Sign: _____ Date: _____

Prof Ddembe Williams

Supervisor.

RFID HAND HELD DEVICES TRACING AND RECOVERY

ABSTRACT

Hand held devices such as laptops, mobile phones and tablets are small in size and therefore easily concealable. They have a ready market and a high resale value making them an easy target for theft for their hardware value (resale) or data stored. Their use has increased as a result of computer literacy, Governments bridging the ICT divide and reduction in the cost of these devices. There is more reliant on these devices to store everything that is important and many a times without back up. As such the loss of any of these devices is not only the economic loss but the loss of valuable personal or corporate data and risky because your personal information, your email is now in the hands of a stranger – as is your internet history, which probably contains details of where you shop and bank

When a device is stolen, the process of recovery is tedious costly and time consuming. The police who give an abstract once a device is stolen have challenges of the necessary tools of recovery and are also overwhelmed by the high number of thefts making the recovery rate is very low. 1 in 10 laptops will be stolen within their lifetime according to the FBI that estimates that 10% of all laptops purchased in the US will be stolen within the first year of ownership. Of those, only 3% will be recovered. (Bruce Verduyn, 2005)

Barcode technology which has been used over the years for identification is now being replaced by Radio Frequency Identification (RFID) (Want, 2004). Bar coding requires a line of sight to scan a printed label to identify the object whereas RFID is omnidirectional and interrogates a tag using radio frequency signals.(Davis, Geiger, Gutierrez, Heaser, & Veeramani, 2009)

Key words: Radio Frequency Identification, tags, readers, tracking

DEDICATION

This research is dedicated to my wife wanjiru and children Peter, Saiya, Harun, Myles and Samuel and to all those who have had their hand held devices lost or stolen.

ACKNOWLEDGEMET

First I want to thank God for provision health and grace which has been more than sufficient to me.

I owe my deepest gratitude to my lecturer and supervisor Prof. Williams Ddembe for his guidance, corrections and encouragement that enabled me to complete this research.

In a special way I express my appreciation to Maxwell for helping me with the programming and development of the source code.

I want to thank the following; my wife Wanjiru for the financial support encouragement and prayers, my son Peter for coming in handy when I required consultation in IT, Saiya for helping during the testing and my classmates for encouragement and sharing.

Table of Contents

LIST OF ABBREVIATIONS

GIS	Geographical Information Systems
GPS	Global Positioning Systems
IP	Internet Protocol
MAC	Medium Access Communication
RFID	Radio Frequency Identification
RTLS	Real Time Locating System

LIST OF FIGURES

LIST OF TABLES

CHAPTER ONE

1.0 Introduction

1.1 Background of problem

Hand held devices like iPads, mobile phones, and laptops are highly susceptible to theft because they small in size thus easily concealable, portable, and provide connectivity through wireless allowing users to work as they travel. The more frequent use of these devices and the more the data stored, then the greater the loss. Barcode technology which has been used over the years is now being replaced by RFID(Want, 2004). Bar coding requires a line of sight to scan a printed label to identify the object whereas RFID interrogates a tag using radio frequency signals.(Davis et al., 2009)

The use of personal portable hand held devices (HHDs) like iPads, mobile phones, tablets and laptops has increased as a result of computer literacy, Governments bridging the ICT divide and reduction in the cost of these devices. Today people are relying more on these devices to store everything that is important to them and many a times without back up. As such the loss of any of these devices is not only the economic loss but the loss of valuable personal or corporate data which causes a major setback and risky because your personal information, your email is now in the hands of a stranger – as is your internet history, which probably contains details of where you shop and bank. The worst-case scenario is that your hand held device if on auto login, will automatically log the thief to social sites such as Facebook, which is a treasure trove of valuable personal information

Hand held devices are small in size making them easily concealable, have a ready market making them an easy target for theft and have capacity to store enough sensitive data and

confidential data of value higher than hardware that if stolen or misused could affect customer trust or dent image of organization. They are mobile by design presenting the same computing capacity and software as many desktop computers, and provide connectivity through wireless-allowing users to work outside office thus enabling staff who travel to keep in touch and work as they travel.

Common hand held device are laptops which are portable, one of the key concerns is their movement in and out of office or campus usually on a daily basis, they are easy to remove and conceal and therefore highly susceptible to theft. They have a ready market, and are stolen for their hardware value (resale) or data stored.

Organizations open to the public, such as government offices, colleges and universities, are easy targets for laptop thieves, since every day hundreds of people staff, students and visitors walk in and out of the premises.(Dimkov, Pieters, & Hartel, 2010)

In colleges and universities, theft of HHDs is increasing by the day with laptops being stolen from libraries, lecture halls, hostels, offices etc. Once stolen, they are either taken out of the compound immediately or hidden in other offices and hostels until a later date when the heat has cooled off.

Bruce avers that a predictable more than two million laptops are stolen, or lost in the United States yearly. 1 in 10 laptops will be stolen inside their lifetime as indicated by the FBI that gauges that 10% of all laptops obtained in the US will be stolen in the first year of proprietorship. Of those, the recovered will be about 3%. (Bruce Verduyn, 2005)

As per the 2011/12 Crime Survey for England and Wales, around 2% of cellular telephone owners have had their phone mugged in the past 12 months. The increment in the volume of

cellular telephones stolen in episodes of individual robbery is prone to reflect both their expanded worth and attractive quality to cheats and the way that more individuals own high valued cell phones. As late as in 2011 the extent of robbery from the individual and theft episodes including a cellular telephone expanded to 46% from 31% in 2010/11. (date et al., 2013)

Johnson assert that the burglary of HHDs is an inexorably genuine issue in cutting edge society(johnson & Kudek, 2003). With the ascent of the 24 hour worldwide economy, Laptop computers are in consistent utilization to help organizations around the globe. To give round-the-clock service to internet users, , communication jacks, web networks and USB ports have been installed at coffeehouses and stands, air transport terminals, voyage ships, airlines and subways.(johnson & Kudek, 2003)

Radio frequency identification (RFID) is a technology used to track and trace and identify a person/object using radio frequency transmission. An RFID system includes tags, readers, and an application system. Information is exchanged wirelessly between a tagged object and a reader when they are tuned to the same radio frequency.

RFID has been used in a number of tracking applications such as to reduce search times for files (Swedberg, 2014), track assets (Violino, 2011)(Wood, 2003), tag and track baggage at airports(O'Connor, 2005b)(Mishra & Mishra, 2010), tracking people during pilgrims (Mohamed Mohandes, 2013) (Amer, 2011), tracking new born babies in hospitals (Haskell-Thomas, 2013)(Collins, 2005), track animals and pets (Ahsan, Shah, & Kingston, 2010)(McGrath, 2008), tracking books in a library (Zaino, 2008) and in security applications (Hunt V. Daniel, Puglia Albert, 2007)

Of all the physical assets, hand held devices are the most troublesome to protect because they are portable and can be easily concealed. Current method of tracking and recovering lost hand held devices mainly through manual verification and surveillance by security personnel at the entry and exit points. The serial number of their devices are recorded and registered to the owner at the entry point and these records are compared at the time of exit. Such manual process is wastage of employees or visitors time as well as a big irritant. This brings in the need of an auto identification of hand held devices to ensure the "Right Person carries the Right device".

Some stolen hand held devices don't ever leave the compound or building where they can be detected through physical searching or scanning methods , but are used within the compound or building that makes detection very difficult or impossible.

1.2 Causes of problem in tracing and recovering HHDs

A hand held device can be tracked and recovered by using pre-installed or embedded software that allows the device to broadcast its presence and sometimes location when it is connected to the internet.

However, this method does not work at all times and with expected accuracy, as only 6% of stolen laptops are ever recovered(Griebenow, 2005)If the installed software is meant to disable the laptop, then one is likely to loose the data forever, whether or not a thief can exploit it. It is therefore advantageous to track and locate a stolen hand held devices before it leaves the area of use say a building

In his review on laptop theft tracking, Bahade observes that the greatest challenge for the security personnel face is to protect and recover laptops stolen in public organizations or buildings that are heavily populated (Bahade, 2014b). It is tedious to manually locate a lost or

stolen device by physically searching every employee, student or guest walking past or driving through the gate to ensure he / she is not carrying a hand held device that is not allocated or belong to him/her.

Some causes of problems in RFID tracking are:

- Metals block RFID signals The antennas on a UHF RFID tag are tuned to receive signals within the UHF spectrum. Placing a tag close to metal reflect energy away from the tag and detunes the antennae blocking the signal from being received (Roberti, 2012)
- Electromagnetic interference from wireless devices such as and wireless computer or network and cordless and mobile phone
- Security and privacy – Since RFID tags can be hidden inside objects without the knowledge of consumers, there are security and privacy concerns. Not many people would like being tracked or their personal data being compromised. (Reuven R. Levary, David Thompson, 2005)(Albrecht, 2003)

- Cloning of RFID tags – RFID tags are vulnerable to cloning, since counterfeiters can read the unique Electronic Product Code (EPC) in a tag and program it into a different one that is indistinguishable to that reader. The manufacturer's tag identifier (TID) can also be cloned.(Traub, 2014)
- Reader collision caused by readers overlapping. The tag is incapable to retort to concurrent queries.
- Tag collision caused by the crowding of many tags in a small area. A misread occurs one when two tags are in the magnetic field at the same time

- Signal strength limited to a required distance
- An antenna of high power can be used to detect sensitive tags by an authorized persons from much further away, compromising privacy.

A number of methods used to track missing or lost hand held devices require that the device being tracked be connected to the Internet for it to broadcast its position(Bahade, 2014b). However, the location given by most methods especially software related are too general and cannot be used by law enforcement officers to track and recover the devices. The an-authorized user or thief could keep changing location making recovery difficult.

In this research choice will be made of antennae less RFID tags that transform metal into antennae to prevent interference of any surrounding metal with the radio signals.

1.3 Definition of terms

1.3.1 Radio Frequency Identification (RFID) – Is a technology that describe a method used to transmit the unique identity of an object by means of using radio waves. This is occasionally referred to as contact-less technology and a having a label or tag, a reader and a computer for the database, control and interface.

1.3.2 Hand held: Any mobile device Small enough to be operated while you hold it in your hands and with the capacity to communicate either by wireless or through a local area network (LAN) or both

1.3.3 Trace –Follow or discover the location or description of the whereabouts of a device in relation to other reference points or known objects.

1.3.4 Recovery – retrieving or regaining a device that was lost or in danger of becoming lost.

1.3.5 Global Positioning System (GPS) is a space-based triangulation system that delivers time and location data in all climatological conditions, anyplace on Earth as long as there is an unhindered line of sight to at least four GPS satellites

Devices such as cellular phones, and portable and hand-held computers, are designed to be mobile, and additional information is needed in order to draw inferences about their location at the time of a particular event. Some kinds of location definition may be limited to a line or cone (e.g. those relying on directional mechanisms), or an area bounded by three or more lines (e.g. those relying on triangulation). Differential and augmented GPS systems have improved GPS services through the use of additional data from terrestrial reference-points.(Clarke & Wigan, 2011)

The main feature of RFID technology is its ability to identify, locate, track, and monitor people and objects without a clear line of sight between the tag and the reader.

An RFID system has three parts: a scanning antenna or tag which is embedded on the object to be identified, a transceiver with a decoder to interpret the data and a transponder (RFID tag) pre-set with information. The scanning antenna sends out a radio-frequency signal providing a means of communication with the RFID tag. When the RFID tag passes through the frequency field of the scanning antenna; it detects the activation signal and can transfer the information data in holds to be picked up by the scanning antenna. RFID tags carry a lot of data (read/write) and can read multiple items without requiring a line of sight.

In this research, an RFID tag that will contain the serial number of the device, the owners name etc will be embedded in the hand held device to be tracked. Readers which will pick up the radio signals from the embedded tag identifying the device will be placed at strategic

positions of monitoring.

1.4 Problem statement

The commonly use method of physically checking for hand held devices at exit points to authenticate ownership is tedious, annoying and time consuming causing huge bottlenecks especially at peak times. Tracking and recovery of mobile hand held devices is quite a challenge and the greater risk in not even of the physical cost of the device which can be met by an insurance company, but that of the data stored therein. There was a case where a laptop belonging to the US state department was stolen and this incident was kept secret for a long time. If this laptop had contained sensitive classified information and fallen to the wrong people, the result could have disastrous.(Johnson & Kudek 2003)

It is not always possible to trace and recover a stolen HHD by simply employing some software embedded in the device. Some tracking softwares provide data wipe facilities to remotely delete sensitive data. However wiping a hard drive deleted important data and applications that could be used for tracking thus limiting recovery chances.

All the software related tracking methods require that the device be connected to the internet to broadcast their location and this poses a great challenge since one must have another device to use to connect with and also where the connectivity is poor. Besides, not all softwares are open source. According to FBI, 97% of stolen laptops that are not installed with tracking software are never recovered. (Bruce Verduyn, 2005)

A lost device presents two challenges; that of recovery (whose cost is insurable) and the loss of important and sometimes confidential personal data stored within. Unfortunately, device recovery is not straightforward since having some information about the possible location of a device doesn’t guarantee recovery by police. Most tracking methods will give a general

location of the device which cannot even be used by law enforcement officers to get a search warrant or accurate recovery.

There is no way of completely preventing the theft of hand held mobile devices and therefore various organizations and institutions must invest in methods of tracing and recovering these devices.

Tracking a mobile or hand held device maybe is easy through available open source or proprietary softwares but recovery is a big challenge.

Handheld device users have installed softwares to track their devices with a view that in the event of a theft, it should be easy to recover. This also does give straightforward since police need adequate information to obtain a search warrant, which may not be possible with GPS information alone.

1.5 Aims and objectives of the project

(a) **Aims**

The goal of this research is to investigate how RFID technology can be used to enhance object tracking and develop an artifact for identification by radio frequency for tracking and recovering hand held devices.

(b) Specific Objectives

- Identify factors that can lead to the security of hand held devices
- Define components of an RFID tracking system
- Design an artifact for a RFID hand held devices tracking system
- Implement the artifact
- Test and evaluate the application

1.6 Significance of the study

When a hand held device is lost the owner required to provide the serial number of the device to help in its recovery. However most owners of these devices do not keep a record of the

serial numbers and that makes it difficult to trace and recover or claim ownership once the device is found.

Tracking and recovery of mobile hand held devices is quite a challenge and the greater risk in not even of the physical cost of the device which can be met by an insurance company, but that of the data stored therein. There was a case where a laptop belonging to the US state department was stolen and this incident was kept secret for a long time. If this laptop had contained sensitive classified information and fallen to the wrong people, the result could have disastrous.(Johnson & Kudek 2003)

1.6.1 IMPORTANCE OF THE RESEARCH

This research will culminate in the development of an artifact that will be used to track and recover a stolen hand held device.

The industrial contribution of this research will lead to the tracking and tracing of a hand held devices. This will lead to the reduction of theft of these devices and thus increased security. It will also lead to prevention of loss sensitive personal data

The scientific contribution of this artifact a basis for further research

CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 State of the art in RFID tracing and recovery

When a device is stolen or lost, the technique and time taken to track and recover it is of extreme importance to the achievement of the recuperation. Throughout the years, various methods have been utilized to label, distinguish and track gadgets and stock things. Some of these strategies are:

2.1.1 Barcode

As observed by Xiao, the most broadly embraced strategy for item identification has long been barcode technology (Xiao et al. 2007). Barcode, a standardized identification is a visual representation of information that is filtered and deciphered for data. Every standardized tag contains a certain code which is used for tracking for items; and is represented by an arrangement of lines or different shapes. Initially it was embodied by the breadth and spaces sandwiched between parallel lines that were one dimensional. This later graduated into other shapes like rectangles and hexagons that were two dimensional. This barcode technology can be scanned by barcode readers along with newer technology on devices such as smartphones and desktop printers

Figure 1 Barcode

2.1.2 QR CODE

The two-dimensional scanner tags, known by their exchange imprint code name QR Code or Quick Response Code are otherwise called matrix bar codes. Two-dimensional scanner tags comprise of a white square foundation printed with little dark squares. A QR code is eventually a two dimensional bar code that stores information both evenly and vertically and can hold significantly more data contrasted with an one dimensional scanner tag. They are regularly utilized in advertising, for example, magazine and daily paper advertisements, and additionally on bulletins and business cards. They might be utilized to track assets, as well as office equipment and machinery.

Figure 2 QR Code

2.1.3 RADIO FREQUENCY IDENTIFICATION (RFID)

Radio frequency (RFID) technology currently the most discussed and researched auto identification and data capture (AIDC) technology. Once used the World War II to identify friendly aircraft, it is therefore not a new technology but is being applied in new ways which are necessitated by technological advances and reduced costs. RFID is now used in a variety of ways to identify, track and trace the location of objects without human intervention. Its for this reason that several world largest companies use this technology to add value to their

goods and services. RFID tracking is not only used by the Defense Department of the United States (DOD) but also Wal-Mart, United Parcel Service, General Motors, Delta Airlines, and Proctor & Gamble, Leanne C. McGrath observes that Proctor & Gamble has estimated that at a price of five cents per tag, it would cost approximately $110 billion to put RFID on its 2.2 billion cases and pallets shipped each year (McGrath, 2008)

Global retailers like Wal-Mart, Metro Group and Tesco are heading the improvement and have helped the presentation of RFID in logistics by ordering their biggest suppliers to actualize RFID on holders and pallets.(Amer 2011) Because of this, the retail division has turned into a worldwide advancement environment where the RFID results are continuously tried, steered and actualized. Different business areas are nearly after these trials and making preparatory work to use the new innovation. Powerful use of RFID may oblige expansive changes in the current methods, a truth that potential clients may not have considered.

As of recently, RFID applications have for the most part concerned separate, shut and in-house frameworks. The utilization of passive UHF RFID technology is expanding quite rapidly, because of the low value, great institutionalization circumstance and sufficient performance (3-4 m reading distance). Because of their expanded utilization, UHF RFID labels which are intended for particular applications (e.g. mounting on metal) have likewise gotten to be industrially accessible. A development in active RFID technology is predicted in RTLS (Real Time Location Systems), because of enhanced institutionalization, lower costs and the likelihood for integration with existing IEEE 802.11 (WLAN) foundation

2.1.4 ELECTRONIC PRODUCT CODE (EPC)

The electronic item code (EPC) put away in the tag chip's memory is composed to the tag by a RFID printer and takes the type of a 96-bit string of information. The initial eight bits are a header which distinguishes the adaptation of the convention. The following 28 bits distinguish

the association that deals with the information for this tag; the association number is allocated by the EPC global consortium. The following 24 bits are an article class, recognizing the sort of item; the last 36 bits are an interesting serial number for a specific tag. These last two fields are situated by the association that issued the tag. The aggregate electronic item code number could be utilized as a key into a worldwide database to extraordinarily distinguish that specific item

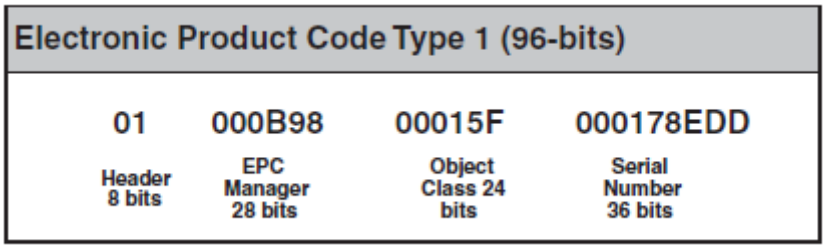


Figure 3 96-bit EPC

2.1.5 TRACKING USING MAC AND IP ADDRESS

This method is used for tracking portable computers and is focused around four modules; window application, web application, Image Capture and Data up loader. Window application runs automatically through window administration when a device is switched on. Web application is utilized for the portable device owner to dealing with the essential data like upgrading the status of smart device like laptops MAC address, adapter address and so forth. Whenever a device being tracked interfaces with the web, its location details and picture of person handling is sent to send on this web application which programmed recoup the vital information necessary for the recovery of the device (Bahade 2014).

Patrick Bertegna notes that with GPS innovation and the ever increasing use of smartphones, it implies that the location of anybody using a GPS empowered cell phone could be precisely followed at any time. Bartenga discloses GPS Tracking softwares that provide applications for

most smart phone operating system which can be used to locate each another on a position-based social networking portico and from one phone to another.(Bertagna, 2010) The tracking is centered on computing power levels and antenna configurations. Use is made of the theory that a cellular phone uninterruptedly converses wirelessly with the closest base stations. Therefore knowing the base station that the cell phone converses with, the location can be traced to that respective base station. There are advanced systems determine the sector in which the mobile phone resides and roughly estimate also the distance to the base station

2.2 STATE OF PRACTICE IN RFID TRACING AND RECOVERY

Kluth observes that several asset tracking frameworks exist that track the location of items and stock e.g. in health facilities, processing plants, shops and so on. Some of these systems are alluded to as perimeter or "border frameworks" in light of the fact that they focus or locate whether the item being followed has left a certain limit or edge. The other classification of tracking frameworks is location based frameworks which are utilized to track the location of a device more closely and to a greater precision than border frameworks (Kluth 2003).

A tag can physically be attached to a gadget being tracked and the location communicated to by a network which might be a node of may be a cellphone, PDA, or that is capable of accessing network services using a wireless link. In a few frameworks, correspondence between a hub and an access point is given by a pulse based radio frequency (RF) wireless link connection. The data got from the asset tag label may show the serial number, type, unique ID no, or some other description of the device. The nature of location and tracking was analyzed by Clarke (2001a) whose findings noted an increasing concentration in the collection of transaction data, link of personal identifiers to with the transactional data, retention and main of that data. This brought about the idea of spying people's pockets, purses and wallets by cell phones and smart cards. Tagging by car hire companies investigators and customers, tagging of books in a library and asset tagging for inventory control (Clarke &

Wigan, 2011)

2.2.1 TRACKING OF NEW BORN BABIES AND EQUIPMENT IN HOSPITALS

In health institutions, RFID is also used to track patients, sample of blood after donation, drop administration, etc. Ohashi developed a shrewd therapeutic environment with RFID innovation. His investigation used two types of frequency for clinical intervention purposes such as drug administrations and blood tests at the patient bedside (Ohashi et al. 2010)

Collins examines how RFID is utilized to track newborn infants, nursing staff and hospital facility assets at Lucile Packard kids' hospital (Collins, 2005). Both mother and child are labelled with reusable battery powered RFID tags with the infant having an extra active RFID tag wristband at the ankle. This wristband contains a unique number that is associated with the mother's record captured at the point of registration through a software and stored in the monitoring computer and the security department. The baby's ankle trinket continuously transmits an RF flag and if the signal is not established an alarm is raised. This guarantees that the tag is not shielded from the reader. The wrist trinket tag is warily designed and gives an alert on the off chance if somebody tries to uproot it. RFID readers are installed at all lifts and corridors from the maternity to all different parts of the hospital. In the event that somebody tries to take out the child from the maternity, the readers pick the security tag on new born child giving a caution that sends a control sign to lock all the entryways. In this system, a mother can additionally also wear a watch like tag, and use the contiguity reader in the tag to recognize or verify her own baby to attend to it.(Collins, 2005)

Haskell notes that King Hamad University Hospital (KHUH) applies an integrated health care framework that combines passive RFID and Real Time Locating System (RTLS) technologies to track hospital assets, staff and patients. In this scheme, items to be traced are tagged with passive UHF RFID tags and are read by a system of readers mounted throughout the hospital

above elevators and doorways to monitor the assets. The information received by the readers is transmitted to a software which process the signal, track and give alerts when certain set rules are broken.(Haskell-Thomas, 2013)

Medications and supplies are additionally followed from the warehouse to the hospital by labeling pallets with passive UHF RFID chips and mounting readers at both the dock entries of both the hospital facility and distribution center. In the event that a tag enlisted at the distribution center does not reach the healing hospital at a foreordained time, the administration is alerted(Haskell-Thomas, 2013)

2.2.2 TRACKING OF ASSETS

In Warehouse management, organisations have used RFID technology to replace Bar Code or QR Code (Tu 2009). In 2006, Grandeur a German based organization that produces jeans and pants for men and ladies began utilizing RFID for tracking. Before stacking them onto trucks, workers read the labels with a RFID reader or investigator as the trolley passes through an entryway. The labels are then read when the garments arrive at the central warehouse and circulation centers. After tagging the clothes with the workers use available PDAs to record the barcode and write the information onto the memory chip. The PDAs transfer also transfers the data to a custom-designed information system via wireless LAN, after which bar-code numbers and ID numbers are linked to a stores management scheme. When the goods are delivered at the warehouse and distribution center, the tags are scanned again as they pass through an RFID porch which is used to compare with the earlier recorded at the initiating stage (Wessel, 2006)

O’Connor observes that a UK based container rental company pH Europe, employs real-time locating system (RTLS) that streams its operations by giving visibility and accessibility of its holders and guaranteeing that once the compartments are returned, they are readied for administration and redeployed as fast as could be allowed.. The service combine GPS, RFID

and bar code data into a real-time location system for tracking assets across a supply chain giving pH Europe improved customer retention and new sources of revenue. Although the global positioning system (GPS) met pH Europe's needs for real time visibility, a cost benefit analysis found that GPS technology was found to be expensive by Ivelina Ivanova, a research associate at the university Glasgow Caledonian University's School of the Built and Natural Environment.(O'Connor, 2005a)

Gambon looks at how RFID contains solutions to shipping challenges in China International Marine Containers by tracking containers from its factory to the storage yard.(Gambon, 2006). Passive tags that have the containers unique identification such as identification number, time and date of production and weight are appended at the assembly line using magnetic strips. Investigative specialists at the compartment yard examine both the container tags and the trailer and the information confirmed for distinguishing proof and charging purposes.

2.2.3 TRACKING OF ANIMALS

RFID has been used to track animals in ranches, to count herd and track cattle in rough terrain as well as in national parks to study migration of wild animals. RFID tags have commonly been installed on holes drilled on the ears of the animals but in recent times injectable RFID tagging are in use. The tags are injected under the skin of the animal concealing them from being easily identified by cattle rustlers of other vindictive people.(Taimoor, 2011)

Figure 4. A sheep with an ear RFID tag

A specimen RFID tag used for identification of cattle is as shown in figure 5

Figure 5 DARD tag

2.2.4 TRACKING BOOKS IN LIBRARIES

RFID has been used in libraries to replace bar code to tag library items and for security instead of tradition electromagnet security chips. When used for library applications, and since RFID can read multiple items through objects, there is then no need of opening the book cover to scan the tag since RFID reads through the cover. The advantage of this is that books can be read while in motion or in a heap at the same time which reduces handling time allowing user to borrow and return books without assistance. It is also possible to take inventory of books on a whole shelf within a short time using portable readers making detection of missing or misfiled books possible. The type of tags used are frequency only readable from a distance of 3m and do not contain any personal information and this addresses privacy concerns.(Agarwal & Mitra, n.d.) (Yu, 2007)

Figure 6 RFID tags used in libraries

2.2.5 TRACKING OF LAPTOPS

Johnson et al. discloses a structure and technique of tracking laptop computers that utilizes miniaturized deployment of GPS engineering which connect with the worldwide orbital positioned 24 GPS satellites. The framework comprises of an inherent interlocking device that lock the hard drive to counteract theft of data or the removal of the hard drive, a software that distinguishes the state of the laptop whether on or off, and a scaled down GPS transmitter that transmits radio frequency signals to a 24-hour care station. The station is then able to track a stolen laptop using the worldwide installed GPS framework.

There exists a system for deactivating the framework when the hard drive is deliberately removed for support or maintenance purposes. However, if the hard drive is removed by an approved individual, the tracking system is initiated. The stalking devices preserve battery power because they have an internal transmitter that remains in a deactivated off stage until the device is turned on. The system ceaselessly transmits a indication that is used to screen and track a device anywhere in the world regardless of the possibility that the device is powered off.(Johnson & Kudek, 2003)

The framework has a method for secret key authorisation that check whether the right passwords have been entered within a predetermined period to indicate whether utilization is approved or not. If the wrong passwords are entered, the tracking system that is integrated with the GPS transmitter is activated to lock the hard disk and also send RF signals to the nearest monitoring station. (Johnson & Kudek 2003)

Foster notes that the University of Kansas Medical Center has a tracking software installed on all its laptops used by faculty and staff members.(Foster, 2008) The software called Computrace, is made by Absolute Software Corporation. Whenever these laptops are

connected to the Internet, they send out signal that can be traced back to the Internet service provider enabling the connection. Once a device is reported stolen, Absolute unobtrusively begins calling the machine every 15 minutes to track its whereabouts (Foster 2008).

Byron discloses a location reliant watching system that comprises of a monitoring center consisting of a server, with a processor and suitable memory and basic interface between the server and the internet. After a device is stolen, the owner is first required to report to the police and then use internet access to log into a set server and reports the stolen device and the details of the police report filed. The server then sets a flag designating the reported device as stolen. The device which could now be anywhere in the world communicates with the monitoring center through a pre-installed device which then initiates a communication with the server or accepts a communication call from the server. The monitoring center then defines the location and identity of the stolen device and checks the status of the ID of the corresponding flag to decide whether the device is stolen. The server the send that ID and location of the stolen device to a remote station only operated by accredited investigators. After enough surveillance evidence is acquired and collated, the data is then conveyed to the police department for recovery of the lost device.(Byron Jung, Burnaby (CA); Damien Loveland, 2013)

2.2.6 RFID KIDS TRACKING SYSTEM

Aloul discusses an RFID based framework that permits security personnel to screen the position of a lost child who has been at one time tagged and locate the child's position at any point within the coverage area. Parents are obliged to enlist their kid's details like name, age and parents telephone number. The child is then given a RFID tag to be worn at the whole span of the recreation center. The framework has the capacity to distinguish and demonstrate whether a kid is in the scope zone and to locate the children area by utilization of an

arrangement of readers picking the children RFID tag signals. At the point when a child is reported lost, his/her label number is recovered from the database and contrasted with the readers introduced around the recreation park and ceaselessly transmitting areas of children inside the recreation center (Aloul et al. n.d.)

Wexler observes that a children's park in Denmark uses a combination of Wi-Fi and RFID to track kids in an amusement park. The parent's mobile phones are used to interface to this system. Once enrolled, the kids are given a Wi-Fi enhanced RFID wristband. Parents locate lost children by sending an instant message to the system which thus reacts by giving the area directions of where the child is (Wexler, 2004)

2.3 TECHNOLOGICAL ADVANCES IN RFID

RFID technology is a wireless Automatic Identification and Data Capture (AIDC) that uses radio-frequency waves to exchange information between a reader and a movable item. It permits the precise and programmed recognizable proof,, tracking and tracing location of objects without human involvement. . It is fast and does not require physical sight or contact between reader/scanner and the tagged item.

An RFID framework is made out of three primary segments:

(i) tags, (ii) a reader and its antennas and (iii) a middleware application that is integrated into a host system. The components of an RFID framework are shown in fig. 7

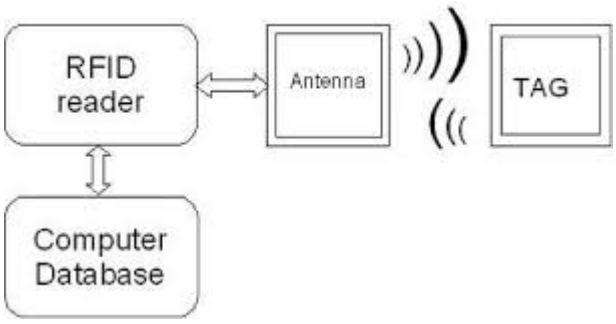


Figure 7. Components of an RFID system

2.3.1 RFID Operating frequencies

The application of RFID depends on the frequency. There are several frequencies used for RFID and with typical values show on table 1

Frequency Ranges	LF 125KHz	HF 13.56MHz	UHF 868 – 915 MHz	Microwave 2.45GHz & 5.8 GHZ
Typical max read Range(passive tags)	Shortest 1'' – 12''	Short 2'' – 24''	Medium 1' – 10'	Longest 1' – 15'
Tag power source	Generally passive tags only, using inductive coupling	Generally passive tags only, using inductive or capacitive coupling	Active tags with integral battery or passive tags using capacitive storage E-field coupling	Active tags with integral battery or passive tags using capacitive storage E-field coupling
Data rate	Slower	Moderate	Fast	Faster
Ability to read near metal or wet surfaces	Better	Moderate	Poor	Worse
Applications	Access control & security. Identifying widgets through	Library books. Laundry identification. Access control.	Supply chain tracking. Highway toll tags	Highway toll tags. Identification of private vehicle

	manufacturing process or in harsh environments. Ranch animal identification. Employee IDs	Employee IDs		fleet in/out of a yard or facility. Access tracking

Table 1 RFID Operation frequency ranges

2.3.2 RFID tags

RFID tags, otherwise called transponders labels contain a chip that store item unique data, for example, maker, item parcel, size and class, creation date, expiry date, final destination, and so forth. RFID labels have different qualities, for example, carrier frequency, power source, , communication technique, read range, information capacity, memory type, size, operational life, and cost. Case in point, is that the tags could be (i) read only, read once/read many or read/compose capable, and (ii) dynamic, inactive or semi-dynamic depending upon how the operating power is determined.

Figure 8 Sample of RFID Tags

(Source: Asif and Mandviwalla, 2005)

2.3.3 RFID reader and antennas

RFID readers, otherwise called examiners or interrogators, are electronic gadgets that emanate and get radio signals through the reception apparatuses/antennae coupled to them. They capture information stored in RFID labels and, contingent upon the innovation utilized, they might likewise overwrite information on the labels. Readers are in charge of the data stream between the labels and the host framework through the RFID middleware. Moreover, they are able to distinguish and read a substantial number of labels for every second without any issue. As demonstrated in figure 9, RFID readers come in various shapes and sizes and might be arranged into the accompanying three principle sorts: fixed reader; hand-held reader; and mobile reader

Fixed reader Hand-held reader Mobile reader

Figure 9 Types of RFID reader (Source: www.symbol.com)

There are two general classes of RFID frameworks, passive and active frameworks. Passive RFID labels don't have a transmitter; they just reflect back energy (radio waves) originating from the reader antennae. Active labels have their transmitter and a source of power, generally yet not generally a battery (could draw energy from the sun or different sources). They broadcast a signal to transmit the information stored on the microchip.

2.3.4 Active RFID Systems

In active RFID frameworks, tags have their own power source and transmitter. Ordinarily, the power source is a battery. Active tags air their own signal to transmit the data stored on their microchips.

Active RFID frameworks normally work in the ultra-high frequency (UHF) band and offer a scope of up to 100 m. As a rule, dynamic labels are utilized on huge articles, for example, rail cars, enormous reusable containers, and different items that need to be followed over long distances.

2.3.5 Passive RFID Systems

In passive RFID structures, the reader and reader antenna send a radio signal to the tag. The RFID tag then uses the transmitted signal to power on, and reflect energy back to the reader. Passive RFID frameworks can work in the low frequency (LF), high frequency (HF) or ultra-high frequency (UHF) radio bands. The ranges of passive frameworks are constrained by the power of the label's backscatter (the radio signal reflected from the tag again to the reader), they are commonly short of what 10 m. Since passive tags do not require a power source or transmitter, and only require a tag chip and antenna, they are less expensive, more modest, and simpler to manufacture than active tags. Passive tags can be packaged in numerous ways, contingent upon the particular RFID application prerequisites. Case in point, they may be mounted on a substrate, or sandwiched between a glue layer and a paper mark to make keen RFID marks. Passive tags might likewise be inserted in an assortment of gadgets or bundles to make the label impervious to amazing temperatures or cruel chemicals.

Inactive RFID results are helpful for some applications, and are generally conveyed to track merchandise in the supply chain, to stock holdings in the retail business, to authenticate items,

for example, pharmaceuticals, and to implant RFID capacity in a mixture of gadgets. Inactive RFID tags can even be utilized in distinction centers and in storerooms or warehouses, regardless of their shorter range, by locating readers at choke focuses to screen their movement

2.3.6 Battery-Assisted Passive (BAP) Systems

A Battery-Assisted Passive RFID tag is a kind of inactive tag which consolidates a significant active tag characteristic. While most inactive RFID labels utilize the energy from the RFID reader's sign to power on the label's chip and backscatter to the reader, BAP labels utilize a coordinated source of power (typically a battery) to power on the chip, so the greater part of the captured energy from the reader could be utilized for backscatter. Unlike transponders, BAP tags do not have their own transmitters.

2.3.7 Passive vs. Active RFID Comparison

The key dissimilarity amongst passive and active RFID tags is that latter tags are governed and powered by a battery and transmit their signal spontaneously, whereas inactive or passive tags do not possess a power source and only convey a signal upon getting Radio Frequency energy radiated by a reader in vicinity.

	Passive	**Active**
Read Range	Up to 40 feet (fixed readers) Up to 20 feet (handheld readers)	Up to 300 feet or more
Power	No power source	Battery powered
Tag Life	Up to 10 years depending upon the environment the tag is in	3-8 years depending upon the tag

		broadcast rate
Ideal Use	For inventorying assets using handheld RFID readers (daily, weekly, monthly quarterly, annually). Can also be used with fixed RFID readers to track the association of assets as long as security is not a requirement.	For use with fixed RFID readers to accomplish real-time asset monitoring at choke-points or within zones. Can afford a better layer of security than passive RFID.
Readers	Typically higher cost	Typically lower cost

Table 2 **Comparison of RFID systems**

2.3.8 Reader Control and Application Software

The reader control and application programming also known as middleware is at the basic of any RFID system. It screens readers, processes, monitors and groups all the information gathered from devices by readers and then transmits the data to the fervent database. In addition, the RFID middleware is also utilized in governing and overseeing the arrangement RFID readers'. It is considered as the core of RFID technology since it provides key functionalities, such as the proficient administration of the data created by the RFID system (Castro & Wamba 2015).

While RFID framework arrives in a variety of plans, the choice of the suitable labels, readers, antennae and middleware will rely on upon the prerequisites of every specific application. Case in point, passive tags are every now and again utilized for high-volume, low cost items

in the retail business; semi-active tags are commonly utilized for retail stalking; finally, dynamic labels are utilized to track high-value items, for example, auto engines in the car business.

Regardless of the enthusiastic enthusiasm toward RFID reception, there are a few impediments regarding absence of standards or technical ability and the high cost of the equipment and frameworks required to deploy RFID (e.g. tags, middleware). To overcome institutionalization issues, some generally acknowledged principles, for example, the EPC system are developing.

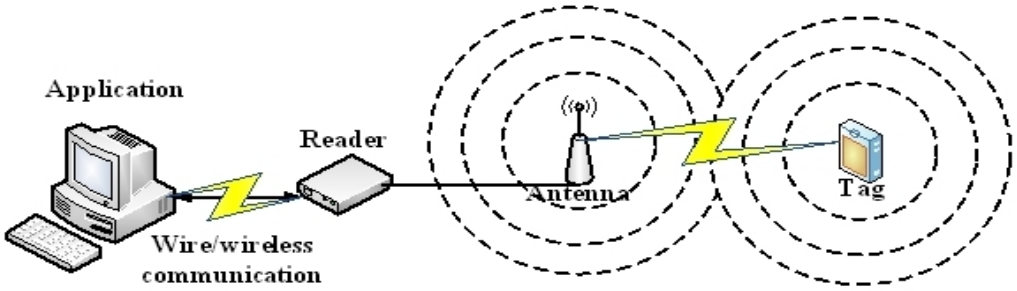


Figure 10 Operation concept of RFID system

2.3.9 Wi-Fi RFID Tags

These tags are Wi-Fi based Radio Frequency Identification Tags (RFID Tags) conforming to 802.11 WLAN standard commonly utilized for Real Time Location Systems. They communicate and connect to existing Wi-Fi access points and therefore when used there is no need of having separate RFID readers. The Tags are designed not to send data to the Access Points when the articles to which they are joined to are stationary, to spare battery power. They have a locating tracking accuracy of 3-5meters and since they continuously communicate with the Wi-Fi access point, they give real time location

2.4 Technological development in tracing and recovery of hand held devices

With the coming of bar code engineering, tracking of hand held devices assets grew exponentially. A scanner tag or bar code, was particularly made for basic supply and other

food stores. This scanner tag engineering later found application in other retail and business outlets. Today, even libraries have gotten into the demonstration by placing standardized identification marks inside their books which brings about a noticeable improvement during check out. Also for those organizations which have various areas or substantial distribution centers, this checking innovation for bar codes goes significantly further. Presently, representatives can scan different assets through a Palm Pilot and other portable scanning gadgets which are then connected to a computer or node to download the data it checked.

Notwithstanding standardized tags, there is electronic observation utilizing attractive innovations and in addition radio frequencies. Gadgets could be covered up inside an item's bundling obscure to shoppers and would-be shoplifters.

Tracking technologies are utilized by organizations to screen assets and avoid loss of stock. Tracking with the end goal of finding a gadget is not one, single innovation but a blending of a few advances that might be consolidated to create systems that track vehicle fleets, stock, animals etc. Current technologies being used to create location-tracking and location-based systems include:

2.4.1 Geographic Information Systems (GIS)

For large-scale location-tracking frameworks, it is important to capture and store geographic data. Geographic information systems can capture, store, analyze and report geographic information.(Jian & Wu, n.d.)

2.4.2 Global Positioning System (GPS)

A group of 27 Earth-circling satellites (24 in operation and three additional ones the event that one fails). Worldwide Positioning System tracking is a technique for finding out precisely where something is. A GPS tracking framework, for instance, may be set in a vehicle, on a

mobile phone, or on unique GPS gadgets, which can either be a fixed or portable unit. GPS lives up to expectations by giving data on accurate location. It can similarly track the movement of a vehicle or individual. In this way, for instance, a GPS tracking framework might be utilized by an organization to screen the route and advancement of a conveyance truck, or by parents to monitor the whereabouts of their youngster, or even to screen high-value transit goods. (Kim, 2007)

2.4.3 Radio Frequency Identification (RFID)

Radio frequency identification (RFID) is a technology used to track and trace and identify a person/object using radio frequency transmission. An RFID system includes tags, readers, and an application system. Information is exchanged wirelessly between a tagged object and a reader when they are tuned to the same radio frequency.

2.4.5 Wireless Local Area Network (WLAN)

These are system of gadgets that associate by means of radio frequency, for example, 802.11b. These gadgets transmit information through radio waves within a range of between 70 to 300 feet. (Bonsor n.d.)

Any location-based service or tracking framework makes use of the fact that framework entails that a node or tag placed on the object, animal or person can be used to find the exact location at any one time.. For example, the GPS receiver in a mobile phone or an RFID tag on a asset can be used to track those devices with a detection system such as GPS satellites or RFID receivers.

2.4.6 Mobile Phone Tracking

Gadgets using mobile communication have been developed using advanced technology and offer more than the capacity to just make a conversation. All cell phones unceasingly conveys a wireless signal even when not on a call. Mobile phones have been tracked over the years

using triangulation information from the base stations that receives the signal. However, the introduction of GPS technology into cell phones has meant that can now be tracked and located to a more precise location and in real time

2.5 CRITIQUE OF THE LITERATURE

Grandeur's method of using RFID tags on clothing to track them between point of manufacture and the warehouse does not however give details of what happens in between. The method only check to verify whether all goods sent from the warehouse are received but if any is lost on the way there is no indication of knowing where.

While Aloul's system of tracking kids was tested as accurate over a small area by overlapping method, the following could affect the accuracy of the results:

- The tag visibly worn around the wrist can easily be removed either by the child or interested child traffickers

- The tracking is only initiated after a kid is reported stolen and by this time, the kid could have left the park with or without the wrist worn tag..

- Due to the high number of kids, readers and the overlapping method used to locate the kids, there is a possibility

- The method discussed by Johnson requires that a when a device is reported stolen, the tracking software enables wiping of the hard disc to prevent confidential data getting into the wrong hands. This however does not help the owner in either recovery of the data or the device.

- The software methods discussed for the recovery of stolen devices requires that the

device has to be connected to the internet for it to be tracked. However not all devices are either immediately or at all connected to the internet to necessitate this.

The methods reviewed have provided similar and innovative concepts of applying RFID technology but fail to explain the big picture of how the readers communicate with the backend database and how a lost device is actually located.

The researcher will explore the various protocols used by RFID readers and the middleware in order to realize the objectives of this research of tracing and recovering a hand held device.

CHAPTER THREE

3.0 Methodological approach

This thesis will result in the development of an artifact to trace and recover hand held devices. In order to do that, a robust underlying methodology is required in order to realize the specific objectives of this research.

Information will be obtained from an assortment of sources, including whitepapers, books, diaries, web sites, daily papers and press discharges.

3.1 Current methods applied in tracking hand held devices

There are several systems that are being used today to track and locate mobile assets some claiming to be more superior to others. Most of the software methods only state what they are capable of doing and not the procedure of how they arrive at the results or how the software runs. A few of the methods are outlined below.

3.1.1 Tracking by IP address

IP address (short for Internet Protocol Address) is a code comprising of numbers and dots distinguishing a specific gadget (machine, Web server, printer, cell phone, tablet, and so forth), and attached to an IP (TCP/IP) system. Reliant upon the administration utilized, or the agreement, the ISP (Internet Service Provider) allocates the IP address. When a device is connected to the web, and through the service provide and the IP allocated, then the location of the device can be found.(Bahade, 2014a)

3.1.2 Tracking by Gmail and Dropbox

A gadget could be followed through its IP address by utilizing G-mail or Dropbox accounts. At the point when one logs into Gmail or Dropbox from any computer, the logs of the IP address utilized and can be fetched which shows the last utilized IP. At the point when Dropbox is installed on a gadget, it turns on automatically on startup and keeps on running

naturally in the background. When the owner of a stolen gadget logs on to his/her Dropbox account from some other gadget, all gadgets ever joined to his record are shown. In the event that the stolen gadget is among the recorded, then the IP address might be discovered and tracked. This is however troublesome if the thief spoofs and shrouds his/her IP address. However, a criminal could conceivably transfer their own particular data to the administration coincidentally that could uncover some data that could help you discover them. (Obaiza, 2013)

3.1.3 Tracking Softwares

3.1.3.1 Laptop cop

This product utilizes skyhook Wi-Fi situating which is a worldwide situating system utilized on numerous platforms, for example, Mac, Windows operating systems, Linux, Symbian, and Android. Through this engineering, one can track a portable computer to within 60 feet anywhere on the planet It was the primary spotting engine for iPhone application, for example Google maps. Most tracking programs will send an email to you after locating your device and that's it, but laptop cop works with local law enforcement agencies to recover it.. This is important because information to law enforcement officers that a laptop is stolen without means of recovering it is not useful information and many a times they may not bother pursuing it

Laptop cop permits one to tenuously link to a stolen computer by simply logging in to his/her account, to copy personal documents and thereafter erase them from the hard drive. However this is only possible when the device is connect to the Internet. Laptop cop is only available for the later windows operating systems and works on both 32-bit and 64-bit frameworks, It has the ability to monitor what an authorized person does on the laptop without them knowing and this sometimes provides useful additional informational that helps accelerate the recovery process (Ropelato, n.d.)

3.1.3.2 Plan B

This locates a lost or stolen android phone regardless of whether it had installed before hard. It permits remote installation and once this is done, the device immediately sends its coordinates. There is no setup obliged and no creation of user accounts. The location of the device will simply appear on your Gmail and tracks a device for 10 minutes messaging you updates in the event of change of location. At any one time simply text "locate" from a mobile phone and the coordinates of the device you are tracking will be sent.

3.1.2.3 Lojack

Lojack is install in stealth mode deliberately hiding their vicinity thus gathers data about the thief without letting him know he's being watched. Once a device has been reported stolen, the Lojack companies' team place forensic tools on the laptop to gather information which goes to absolute software of the user Most modern laptops comes with a module programming preinstalled in the Bios that enacts when you introduce Lojack and checks for fitting operation. Lojack can survive a hard disk wipe or swap. Lojack resists any factory reset, installation of a new or even a complete hard drive replacement. It provide a link between owner and the device being tracked enabling the investigation team to gather data to help police recover it. (Carroll, 2010)

3.1.2.4 Wi-Fi lookup

Most anti-theft producers use Wi-Fi look up to determining the geo-location of the stolen laptop This is carried out by checking the adjacent Wi-Fi hotspots against a database regularly Google's or sky snares' to discover where the portable computer is.

3.1.2.6 Laptop superhero

Incorporates an offline lock option in case a thief keeps a stolen device disconnected. After

10min. 8hrs, or 24 hrs. offline, the system locks down the device requiring a password or pin to startup. This means that tracking is the made difficult however the unauthorized user cannot also use the device.

The chart below shows a summary of important features for some software products(Neil J Rubenking, 2011)

	GadgetTrak Laptop Security	Laptop Cop	Laptop Superhero	LaptopSentry 3.1	**LoJack for Laptops by Absolute Software**	Snuko Anti-Theft & Data Recovery Premium
Price per year	$34.95	$65.00	$29.99	$99.99	**$39.99**	$29.95
Star rating	3.0	4.0	3.0	2.5	**4.5**	2.5
Geolocation						
WiFi lookup	Y	Y	Y	Y	**n***	Y
IP-based location	n	n	n	n	**Y**	Y
Forensics						
Webcam image capture	Y	n	Y	Y	**Y****	Y
Screen capture	n	Y	n	n	**Y****	Y
Log keystrokes	n	Y	n	n	**Y****	n
Monitor email	n	Y	n	n	**Y****	n
Monitor IM	n	Y	n	n	**Y****	n
Monitor Web activity	n	Y	n	n	**Y****	n
Tamper-resistance						
Not easily disabled	n	Y	n	n	**Y**	Y
Survives reformat	n	n	n	n	**Y**	n
Survives hard drive swap	n	n	n	n	**Y**	n
Offline lock	n	n	Y	n	**n**	n
Recovery Style						
Stealth installation	n	Y	n	n	**Y**	n
Audible alarm	n	n	Y	Y	**n**	n
Police report required	n	Y	n	n	**Y**	n
Communicate with finder	n	n	Y	Y	**Y**	Y
Remote lockdown	n	n	Y	Y	**Y**	Y
Vendor handles recovery	n	n	n	n	**Y**	n
File Protection						
Online backup	n	n	n	Y	**n**	Y
Remote retrieval	n	Y	n	n	**n**	n
Remote encryption	n	n	n	Y	**n**	Y
Remote deletion	n	Y	Y	Y	**Y**	n

* WiFi geolocation in LoJack for Laptops premium edition only
** Absolute Software does not expose forensic details to the user

Table 3. Summary of software features

Source: Absolute Software Corporation

3.2 Evaluation of current methods

3.2.1 Research methodology is a way of systematically solving a research problem. In other words, it is the science of learning how research is conducted scientifically. It refers to the way in which research studies are designed and the procedures by which data is analysed (Prof. Williams 2012), Research can be done using either quantitative or qualitative methods.

3.2.2 Quantitative research

Quantitative research seeks explanatory laws and is based on the measurement of quantity or amount. It is an exploration of what is assumed to be dynamic.

3.2.3 Qualitative research

Qualitative research involves collecting, analyzing, and interpreting data by observing what people do and say. It is open ended where participants are asked to respond to a set of questions and the researcher analyses these responses to identify and define people's opinions, discernments and approaches about the topic or idea being discussed and to determine the degree of agreement that exists in the group

Procedure		Quantitative	Qualitative
Preparation	Definition Hypothesis Operationalisation	Precise, accurate & specific Formulated before the study yes	General & loosely structured To be achieved through study no
Research design	Design Representativeness Method of collection Measurement scales	Accurately planned Yes Yes Yes	Well planned but not prescriptive No Yes Mostly nominal
Data collection	Methodology Working method	Quantitative method Employs assistants	Qualitative methods Usually solo
Execution		Quantitative statistical	Qualitative collection and analysis occur simultaneously
Processing		Indicative generalisation	Analytical generalisation

Table 4 Comparison between Quantitative and Qualitative methods

Qualitative examination which includes the era of information in quantitative structure which might be subjected to thorough quantitative investigation is further characterized into inferential, experimental and simulation approaches to research.

3.2.4 Inferential Method is where a database is generated from which to deduce characteristics or relationships of population. This normally means study research where a sample of populace is studied to determine its physiognomies, and it is then inferred that the population has the same characteristics.

3.2.5 Simulation Technique involves the development of an artificial environment inside which relevant information and data can be created. This allows a perception of the dynamic behaviour under controlled conditions.

3.2.6 Experimental method is a systematic and scientific approach to research in which the specialist controls one or more variables, and controls and measures any change in other variables.

3.3 Proposed method

- Since the goal of this research is to investigate how RFID technology can be used to enhance object tracking and develop an artifact for identification by radio frequency for tracking and recovering hand held devices, qualitative research was used to review various concepts and theories used in the area of tracking and in particular RFID tracking of mobile devices.
- Experimental research is applied to give a systematic approach in the design of an artifact for a RFID hand held devices tracking system, manipulate the distance and position of the RFID readers to implement test and evaluate the artifact
- Quantitative research is then used to seek explanation of the measurements taken on the artifact that will be developed

The design of an artifact for a RFID hand held devices tracking system will involve the following activities:

a) Identification of a suitable tag that can easily be concealed within the device and tagging of the hand held devices to be tracked
b) Programming of the reader using C# language to develop a source code and logic which will link with the database and process and display the tracking activity
c) Creating a master database of the devices and maintaining a unique database for every device e.g. serial number, name of owner, type/make or model. In the

data base the relationship between the owner and device tags will be linked

The readers placed at various points will be used to read the tags hidden within the devices and the data compared with that in the database to identify the rightful owner of the device

3.4 Artifact Design

Testing and evaluation is an important factor after an artifact is developed. In this research, there are no available methods of simulating the theory and the researched therefore decided to source real components for testing purposes.

There are no manufactures or resellers of RFID components within the county and the available components from other countries are very expensive especially for the readers that cost between $500 to $3,000 (Violino, 2005)

An important point to note is that the size of the device will highly influence the size of the RFID tag to be used. For the purpose of this research, laptops are chosen to represent any hand held device and to implement, evaluate and test this method.

CHAPTER FOUR

4.0 CONCEPTUAL MODEL, IMPLEMENTATION AND TESTING

4.1 Introduction

This chapter discusses the proposed model for the tracing and recovery of hand held devices using RFID

4.2 Model

A conceptual model is a framework arrived at after review of the literature. The framework shows the relationship between the variables and how they interact to give the final desired outcome.

The system will involve communication by radio waves from the tags to the reader and by an RS-232 adaptive Ethernet cable from the reader to the middleware at the host computer which will also store the data.

The researcher has chosen a system operating at a frequency of 2.45 Ghz which is in the microwave band which will be able to read both passive and active tags at distances of over 30m depending on environmental conditions. The choice of these tags is to enable the device to be read at a distance before the holder get near the monitoring point to enable the security personnel time to intervene in case of an unauthorized handler.

The conceptual model was developed after the literature review and therefore the ideas used in this model are not new and are likely to have been used before.

Figure 11 shows the conceptual model used for the purpose of this research.

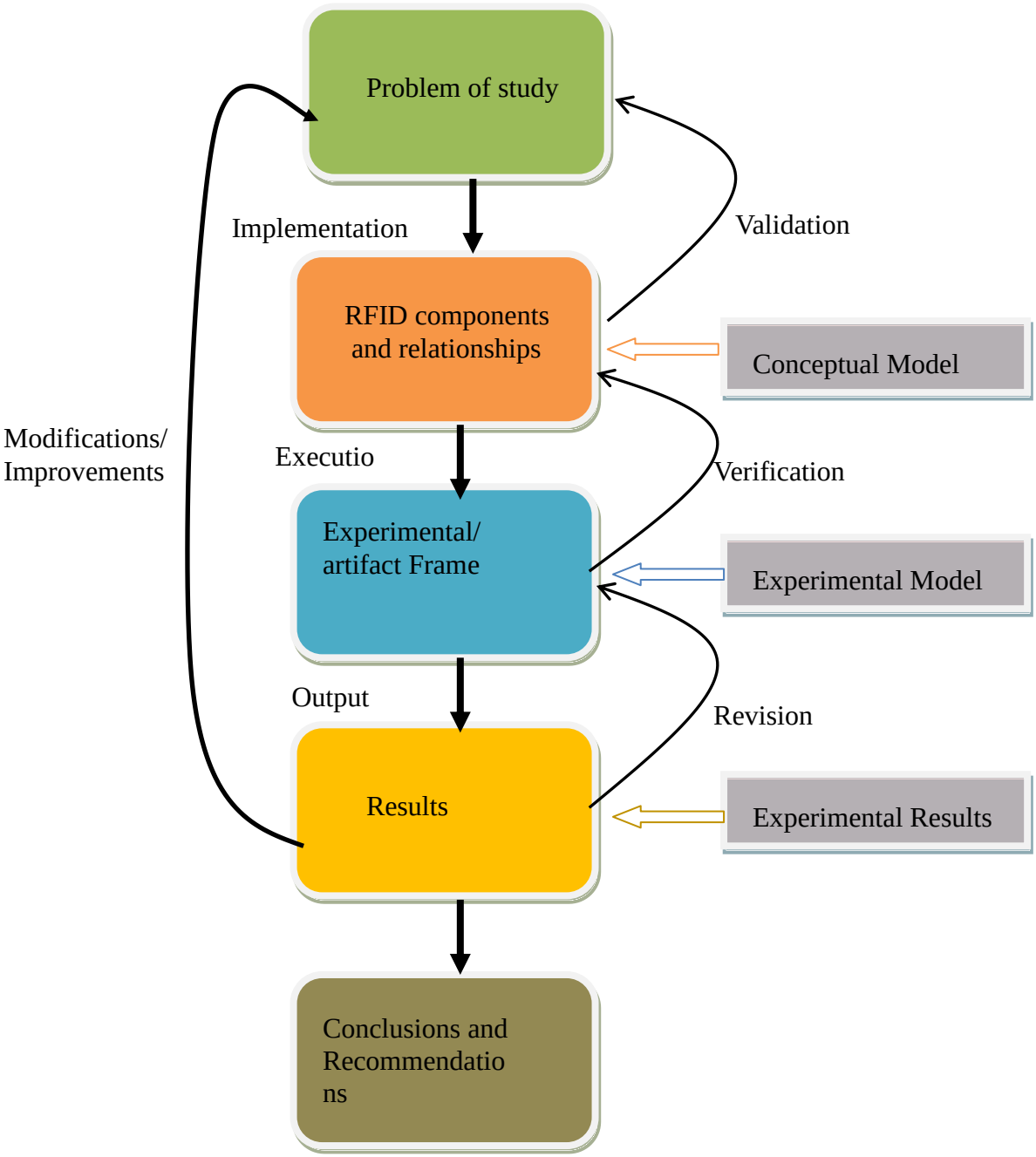


Figure 11: Conceptual Model

4.3 IMPLEMENTATION AND TESTING

The purpose of these research was to trace and recover hand held devices using RFID technology. The researcher has then chose to track a laptop to represent any other hand held device.

4.3.1 Choice of tags

Although the larger parts of laptops are plastic, some contain a large quantity of metal in the screen and other components like the outer shell. The choice of tags to be used for tracking a laptop is therefore of importance to avoid metal interference of the radio waves. For this research, and to locate the device over large distances. The researcher chose active tags operating at 2.45 GHz frequency. The reason for this choice is that a wireless connection will be set up without interfering or requiring access to any existing network.

4.3.2 Location of tags

In tracking, the location of RFID tags is a crucial aspect that determines the success of the results. Placing the tags on the lid gives the best results as this has minimum interference/blockage, however this makes it easy for the tag to be noticed by thief who can either remove or destroy it. It is therefore advisable to conceal the tags by embedding them inside the device.

4.3.3 Choice of Readers

The reader to be used to index and track the tags need to be carefully chosen since not any RFID reader can be used to read all tags. The reader chosen has to be compatible with the tags used to give best results. The cost of readers is prohibitive ranging from $ 200 for hand held to about $ 3000 for fixed readers depending on manufacturer and application (alibaba.com). Since the tags used in this research are active 2.45 GHz RFID tags, the researcher chose a reader capable of operating in the 2.4 – 2.48 GHz frequency range. The reader chosen is

compatible with passive and active operating tags and has an optional Ethernet connection.

4.4 Implementation

A laptop to be tracked will covertly be tagged with an active SAAT-T510 RFID tag (Innotech, n.d.) that has a unique identity to that laptop and also the owner. Details about the laptop like the serial number, make, owners name/contacts will be indexed at registration and stored in the systems database.

A SAAT-F527 with omnidirectional antennae reader will be placed at an exit point say the gate or entrance to a building. Several readers and their location ID can also be used to identify the location at which the laptop will be identified. The information picked by the reader will then be sent to computer that will record, store, retrieve and compares information with that in the database. Configuration of the reader for wireless communication and user information was done as shown and a program developed in C# language as given in the following extract of the source code.

The SAAT-F527 reader is connected to the computer via an Ethernet cable. Both the IPs of the reader and computer were set to belong to the same network segment so as to enable communication. The readers IP address set at factory is 192.168.0.238 port number 7086. The computer was then set to an IP address of 192.168.0.100

Unique information relating to each tags was be recorded and stored in the database. These information include; make of the device, serial number, full names of the owner and telephone contact.

4.4.1 Source code

```
tagDBStruct tagDetails, parentDetails;
```

```
RevMsgStruct tempRevMsg = new RevMsgStruct();
int retryCounter = 0;
int messageType = 0;
string message;
RevMsgStruct revMsg = new RevMsgStruct();
int dwStart = System.Environment.TickCount;
bool bConnectIsOK = false;
while (bReadCodeState)
{
   messageType = 0;
   nRevMsgResult = CRevCodeMsg(ref revMsg);
   if (nRevMsgResult == 1)
   {
      bConnectIsOK = true;
      String temp;
      temp = revMsg.sCodeData;

      oldCount = currentCount;
      currentCount = revMsgLine.TagCount;

      tagDetails = dbConnection_query(temp);
      if (tagDetails.rfid == null)
      {
         message = "Tag unknown: " + revMsg.sCodeData + "\n" +
System.DateTime.Now;
```

```
    messageType=1;
    messageLabel.Text = message;
}
else
{
    parentDetails = dbConnection_query2(tagDetails.belongsTo);
    if (parentDetails.rfid == null && tagDetails.deviceType != 1)
    {
        message = "Tag has no parent: " + tagDetails.rfid +
                "\nOwner: " + tagDetails.owner +
                "\nDevice: " + tagDetails.deviceDesc +
                "\nPhoneNumber: " + tagDetails.phoneNo
                 + "\n" + System.DateTime.Now;
        messageLabel.Text = message;
        messageType=2;
    }
    else if (tagDetails.deviceType != 1)
    {
        int i = 0;
        for (i = 0; i < revMsgLine.TagCount; i++)
        {
            revMsgLine.RevMsgGet(ref tempRevMsg, i);
            if (parentDetails.rfid == tempRevMsg.sCodeData)
                break;
            else if (i == revMsgLine.TagCount - 1)
```

```
                {
                    if (retryCounter <= 5)
                        retryCounter++;
                    else
                    {
                        message = "Tag unauthorized!" +
                                "\nTag ID: " + revMsg.sCodeData +
                                "\nOwner: " + tagDetails.owner +
                                "\nParent: " + parentDetails.rfid +
                                "\nPhoneNumber: " + tagDetails.phoneNo
                                 + "\n" + System.DateTime.Now;
DataSet ds = new DataSet();
OleDbConnection conn =
    new OleDbConnection(connectionString);

tagDBStruct tagDetails;
tagDetails.id = 0;
tagDetails.rfid = null;
tagDetails.owner = null;
tagDetails.deviceDesc = null;
tagDetails.serialNo = null;
tagDetails.phoneNo = null;
tagDetails.belongsTo = 0;
tagDetails.deviceType = 0;
```

```
        try
        {
            //Open Database Connection
            conn.Open();

            OleDbDataAdapter da =
                new OleDbDataAdapter(query, conn);

            //Fill the DataSet
            da.Fill(ds, tableName);
            conn.Close();

            try
            {
                tagDetails.id = Convert.ToInt32(ds.Tables["Tags"].Rows[0]["ID"]);
                tagDetails.rfid = Convert.ToString(ds.Tables["Tags"].Rows[0]["RFID"]);
                tagDetails.owner = Convert.ToString(ds.Tables["Tags"].Rows[0]["Owner"]);
                tagDetails.deviceDesc =
Convert.ToString(ds.Tables["Tags"].Rows[0]["DeviceDescription"]);
                tagDetails.serialNo =
Convert.ToString(ds.Tables["Tags"].Rows[0]["SerialNumber"]);
                tagDetails.belongsTo =
Convert.ToInt32(ds.Tables["Tags"].Rows[0]["BelongsTo"]);
                tagDetails.deviceType =
Convert.ToInt32(ds.Tables["Tags"].Rows[0]["DeviceType"]);
```

```
                tagDetails.phoneNo                                                =
Convert.ToString(ds.Tables["Tags"].Rows[0]["PhoneNumber"]);
            }
            catch
            {
                tagDetails.id = 0;
                tagDetails.rfid = null;
                tagDetails.owner = null;
                tagDetails.deviceDesc = null;
                tagDetails.serialNo = null;
                tagDetails.phoneNo = null;
                tagDetails.belongsTo = 0;
                tagDetails.deviceType = 0;
            }

/*              MessageBox.Show(" Hello World "
                    + ds.Tables["Tags"].Rows.Count
                    + "  "
                    + ds.Tables["Tags"].Rows[0]["ID"]
                    + "  "

                tagDetails.owner = Convert.ToString(ds.Tables["Tags"].Rows[0]["Owner"]);
                tagDetails.deviceDesc                                             =
Convert.ToString(ds.Tables["Tags"].Rows[0]["DeviceDescription"]);
                tagDetails.serialNo                                               =
```

```
Convert.ToString(ds.Tables["Tags"].Rows[0]["SerialNumber"]);
                tagDetails.belongsTo                                    =
Convert.ToInt32(ds.Tables["Tags"].Rows[0]["BelongsTo"]);
                tagDetails.deviceType                                   =
Convert.ToInt32(ds.Tables["Tags"].Rows[0]["DeviceType"]);
                tagDetails.phoneNo                                      =
Convert.ToString(ds.Tables["Tags"].Rows[0]["PhoneNumber"]);
            }
            catch
            {
                MessageBox.Show("Not found");
                tagDetails.id = 0;
                tagDetails.rfid = null;
                tagDetails.owner = null;
                tagDetails.deviceDesc = null;
                tagDetails.serialNo = null;
                tagDetails.phoneNo = null;
                tagDetails.belongsTo = 0;
                tagDetails.deviceType = 0;
            }

            /*          MessageBox.Show(" Hello World "
                        + ds.Tables["Tags"].Rows.Count
                        + "  "
                        + ds.Tables["Tags"].Rows[0]["ID"]
```

```
                    + "  "
                    + ds.Tables["Tags"].Rows[0]["Owner"]
                    + "  "
                    + ds.Tables["Tags"].Rows[0]["Device"]);
        */
    }
    catch (OleDbException exp)
    {
        MessageBox.Show("Database Error:"
                + exp.Message.ToString());
    }
    finally
    {
        if (conn.State == ConnectionState.Open)
        {
            conn.Close();
        }
    }

    return tagDetails;
}
```

4.4.2 Database

At the point of entry or registration each device will be tagged and scanned and the unique information pertaining each device and the owner's details are entered. The relationship

between the device tag and the covert tag identifying the owner is also recorded on the database. Figure below shows a sample of the data entered in the database for testing purposes.

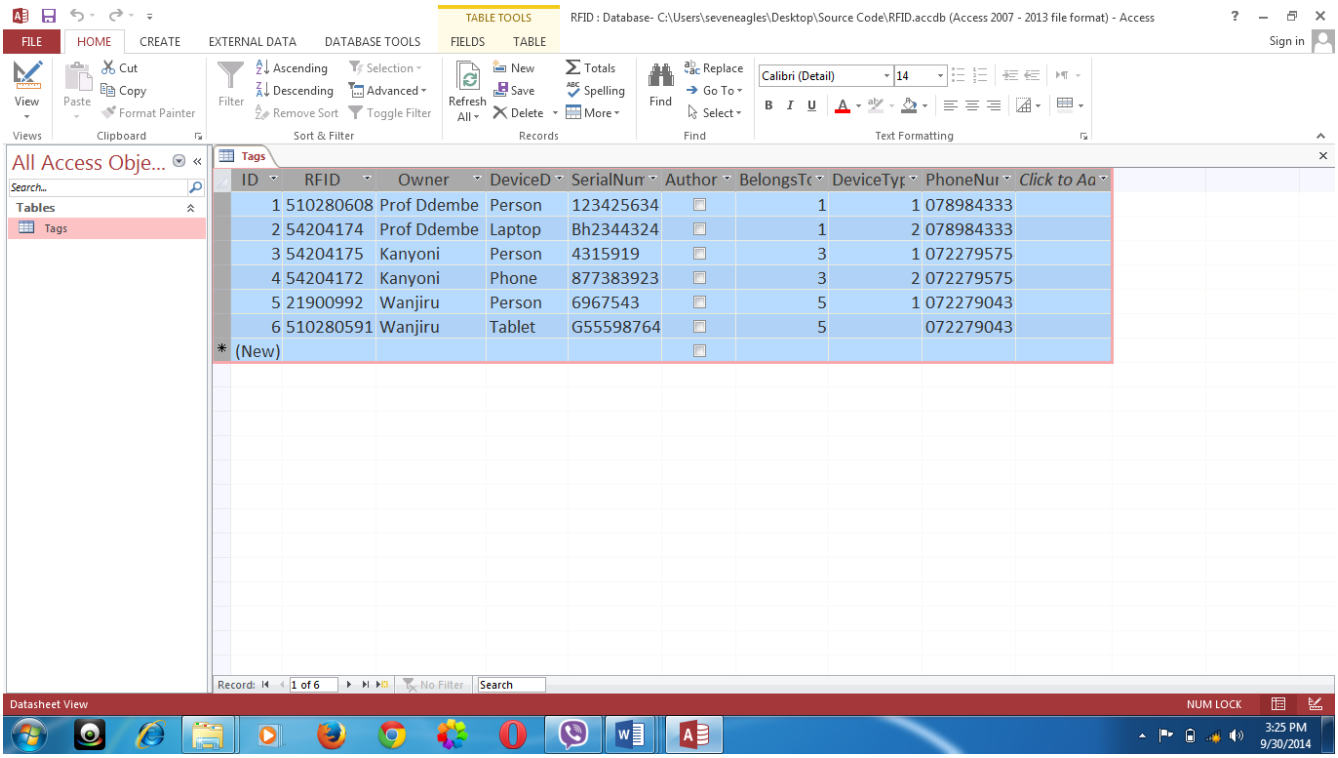


Figure 12: Test Database

4.5 Testing

As a device approaches the surveillance or access point, the tag is read a distance of about 20m. The information picked by the reader is then compared to that sensed at registration and recorded in the database. This will however indicate whether the particular device was registered or not and will not be able to authenticate the owner. Since a person needs to be identified as the lawful owner or legalized user some means of authentication need to be done. To achieve this another tag will be used as unique identity of the owner. When a person carries a device through a surveillance point, both the device tag and owner tags IDs are identified. The system then matches the device tag information with that of the person carrying the device. The results will show whether the person is authorized or not to carry the

laptop. In a case where the persons ID does not match that of the laptop as previously entered in the database or is missing, the system displays that a perquisite tag has not been identified and the owners details and tag ID are displayed. The occurrence time is also given and the surveillance location. Reports can be generated either on daily or monthly basis as required to show all passages of the tagged devices

4.6 Results

The test result were carried out recorded as shown in the following figures

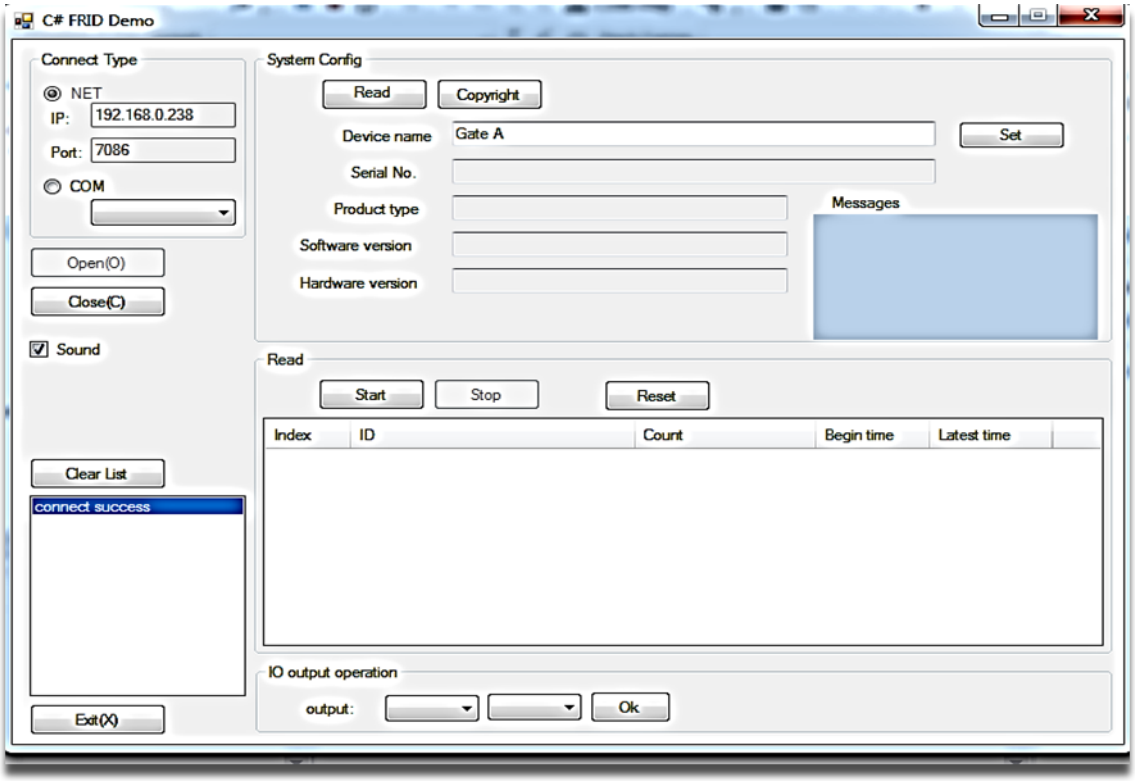


Figure 13: The reader after being set to communicate with the computer before any tag is read

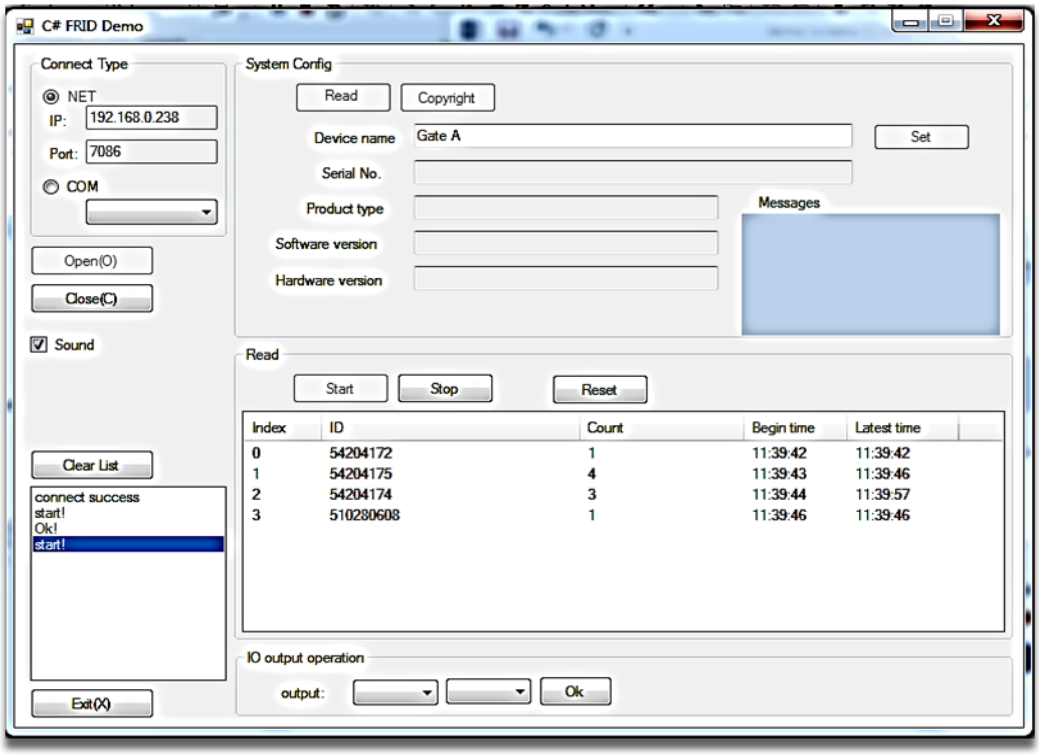


Figure 14: Reader showing the tags read, their Id and the time of reading

During this test a device assigned to Prof. Ddembe with ID no 54204174 was scanned. To clear or authenticate that this device belonged to Prof. Ddembe, The owner was had a covert tag no 510280608 registered at the entry. At exit, the owners tag was not read meaning that the person in possession of the device is not the authorized owner. The date and time of this event as well as the rightful owner's name, tag Id and his telephone contact are displayed. Fig 4.4 below shows this result and that the other devices that were scanned and authenticated.

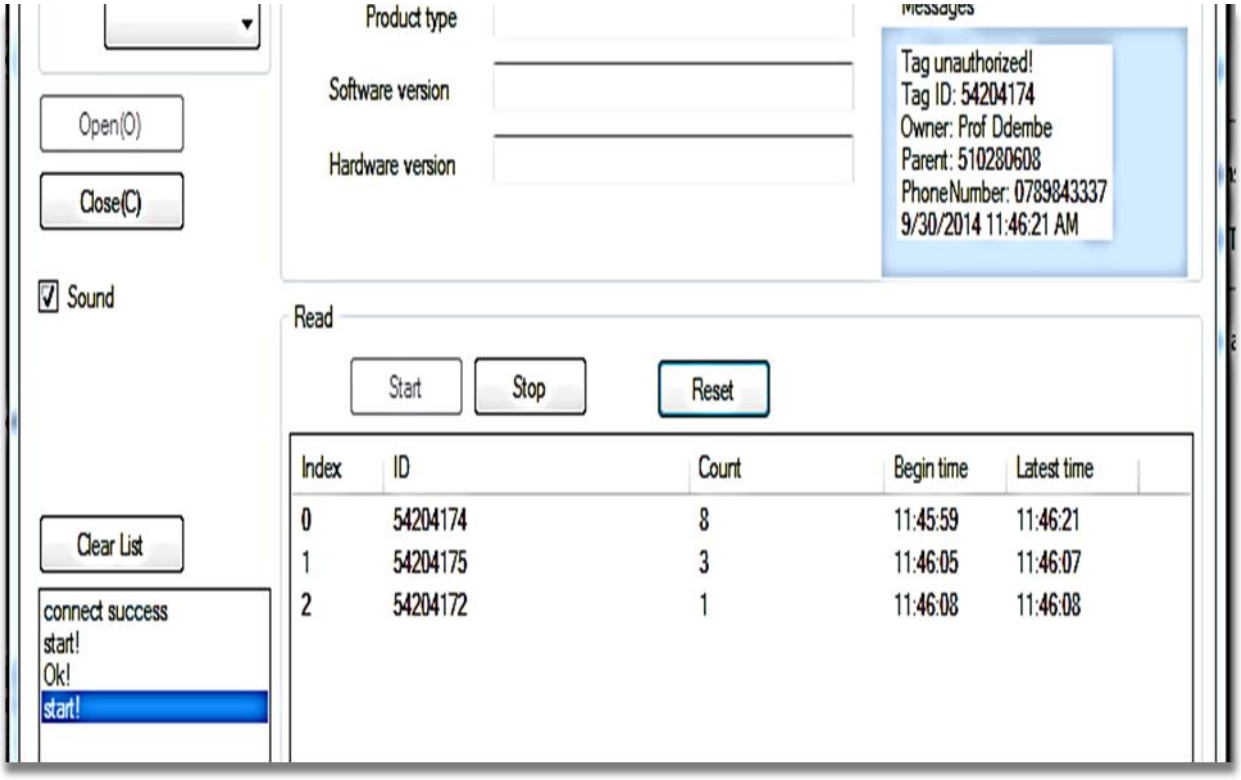


Figure 15: Reader display showing that an authorized tag/person

CHAPTER FIVE

5.0 CONCLUSIONS AND RECOMMENDATIONS

5.1 Overview

This chapter contains the conclusion and recommendations after the study on Radio Frequency Identification tracking and recovery of hand held devices. The researcher also gives possible areas of further study in this area.

5.2 Conclusions

Radio Frequency identification is a technology that is finding its way in our everyday life especially in tracking of assets and equipment. A lot of resources are spent in tracking lost devices and recovery is a great challenge to the law enforcement officer. The Inconvenience of losing valuable data when we loose our hand held devices let alone the cost of replacement can now be reduced by utilization of RFID in tracking and recovery. The researcher achieved the objectives of the study and demonstrated that a hand held device can be tracked and recovered before it leaves the surveillance area thus eliminating the loss of data, application for search warrants and utilization of the available software and hardware methods of recovery.

The test results show how a stolen device can be monitored at the exit point. However when two or more individuals exit at the same time and carrying devices being tracked, once they reach the reader proximity area all the tags will be identified. If however one is an authorized the system will only be able to show that a device is leaving without the rightful owner but is not able to pick who among the individuals has the device. In this case, all the persons within the vicinity area will have to be scanned individually (physically if need be) and required to produce proof of the personal clearing tags. This however does not happen all the time but only where an authorized tag (stolen device) id identified

5,3 Limitations

In the carrying out this study, the researcher was encountered the following challenges

- Lack of simulation tool. The researcher had to source the reader and tags from China at a cost of $550, as such only one type of reader was used during this study.

- Limitation in programming. To develop the necessary source code and logic, for the reader to communicate with the database computer, a good knowledge of programming was required. The researcher had to study and use C# programming language.

5.4 Recommendations

RFID tracking should be utilized in tracking hand held devices especially in areas commonly used by the public or large number of people. These are the areas where devices are easily stolen since the large number of persons make surveillance almost an impossibility when person leaving the facility has to be searched individually

5.4 Further Work

The reader used for the test results has a capacity of reading 200 tags/per second and capable of identifying 300 tags at the same time without conflict and therefore suitable for use in large office buildings and institutions of higher learning.

The greatest challenge and therefore suggestions for further study is in the development of the necessary logic to differentiate and identify the an authorized tags/devices

References.

Agarwal, A., & Mitra, M. (n.d.). RFID : Promises and Problems, 1–12.

Ahsan, K., Shah, H., & Kingston, P. (2010). RFID Applications : An Introductory and Exploratory Study, *7*(1), 1–7.

Albrecht, K. (2003). RFID Position Statement of Consumer Privacy and Civil Liberties Organizations | Privacy Rights Clearinghouse. Retrieved July 29, 2014, from https://www.privacyrights.org/ar/RFIDposition.htm

Amer, N. (2011). A Real-Time Tracking System using RFID in Mecca Master of Engineering.

Bahade, S. S. (2014a). Detection of Stolen or Lost Laptop Using MAC and IP Address, *2*(4), 457–464.

Bahade, S. S. (2014b). Laptop Theft tracking : A Review, *4*(1), 900–902.

Bertagna, P. (2010). How does a GPS tracking system work? | EE Times. Retrieved June 28, 2014, from http://www.eetimes.com/document.asp?doc_id=1278363&page_number=2

Bruce Verduyn, et. a. (2005). 2005 FBI Computer Crime Survey. *Computer*. Retrieved from www.fbi.gov/publications/ccs2005.pdf

Byron Jung, Burnaby (CA); Damien Loveland, R. (CA). (2013). LOCATION DEPENDENT MONITORING FOR STOLEN DEVICES, *1*(19).

Carroll, J. (2010). Dude, where's my laptop? *CA Magazine*, *143*, 14. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=50404460&site=ehost-live

Clarke, R., & Wigan, M. (2011). Journal of Location Based Services You are where you ' ve been : the privacy implications of location and tracking technologies, (May 2014), 37–41. doi:10.1080/17489725.2011.637969

Collins, J. (2005). RFID Delivers Newborn Security - RFID Journal. Retrieved June 25, 2014, from http://www.rfidjournal.com/articles/view?1372/4

Davis, R., Geiger, B., Gutierrez, A., Heaser, J., & Veeramani, D. (2009). Tracking blood products in blood centres using radio frequency identification : a comprehensive assessment, 50–60. doi:10.1111/j.1423-0410.2009.001174.x

Dimkov, T., Pieters, W., & Hartel, P. (2010). Laptop theft: a case study on the effectiveness of security mechanisms in open organizations. ... *Computer and Communications Security*, 666–668. doi:10.1145/1866307.1866391

Foster, A. (2008). Increase in stolen laptops endangers data security. *The Chronicle of Higher Education*, 43–45. Retrieved from http://www.csun.edu/pubrels/clips/clips08-09/July08/07-01-08B.pdf

Gambon, J. (2006). RFID Contains Solution to Chinese Shipping Problems - RFID Journal. Retrieved June 25, 2014, from http://www.rfidjournal.com/articles/view?2707

Griebenow, A. (2005). RFID as Mandatory Protection for Laptops , Intellectual P r o p e r t y , a n d . . . . . E x e c u t i v e s White.

Haskell-Thomas, H. (2013). Tracking Assets with RFID : King Hamad University Hospital.

Hunt V. Daniel, Puglia Albert, P. M. (2007). Rfid-a guide to radio frequency identification.

Innotech, A. (n.d.). SAAT-T510.pdf.

Jian, M., & Wu, J. (n.d.). RFID Applications and Challenges, 1–26.

Johnson, R., & Kudek, S. (2003). System and method for tracking laptop computers. *US Patent App. 10/746,920*, *1*(19). Retrieved from www.google.com/patents/US20050149752

Kim, G. G. (2007). LOCATING AND TRACKING ASSETS USING RFID, (August).

McGrath, L. C. (2008). RFID – Tracks It , Tracks You RFID – Tracks It , Tracks You, (March 2014), 37–41. doi:10.1300/J179v04n04

Mishra, D., & Mishra, A. (2010). Improving Baggage Tracking , Security and Customer Services with RFID in the Airline Industry, *7*(2), 139–154.

Mohamed Mohandes, D. (2013). SYSTEM AND METHOD FOR TRACKING PEOPLE, *2*(12).

Neil J Rubenking. (2011). 6 Ways to Find Your Stolen Laptop.

O'Connor, M. C. (2005a). Container Company Puts Lid on Slip-Ups - RFID Journal. Retrieved July 16, 2014, from http://www.rfidjournal.com/articles/view?1445/4

O'Connor, M. C. (2005b). EPC Bag Tagging Takes Wing - RFID Journal. Retrieved July 16, 2014, from http://www.rfidjournal.com/articles/view?2024/5

Obaiza, O. (2013). How to Use Dropbox to Track and Locate Your Stolen Laptop « Digiwonk. Retrieved June 20, 2014, from http://digiwonk.wonderhowto.com/how-to/use-dropbox-track-and-locate-your-stolen-laptop-0146294/

Reuven R. Levary, David Thompson, K. K. (2005). RFID, Electronic Eavesdropping and the Law - RFID Journal. Retrieved July 29, 2014, from http://www.rfidjournal.com/articles/view?1401

Roberti, M. (2012). About That Problem With Metal and Water - RFID Journal. Retrieved July 29, 2014, from http://www.rfidjournal.com/articles/view?9841

Ropelato, J. (n.d.). Laptop Cop Review - TopTenREVIEWS. Retrieved June 20, 2014, from http://laptop-tracking-review.toptenreviews.com/laptop-cop-review.html

Swedberg, C. (2014). Qatar's Public Prosecution Office Cuts File Search Time by 60 Percent - RFID Journal. Retrieved July 16, 2014, from http://www.rfidjournal.com/articles/view?11935&utm_medium=email&utm_source=rfid+journal&utm_campaign=4412507_GeneralNewsletter071014&dm_i=1JOI,2MKPN,EUW2FR,9LHML,1

Taimoor, M. (2011). TARGET DETECTION USING RFID TECHNOLOGY.

Traub, K. (2014). Gen2v2 Ensures Tags Are Authentic - RFID Journal. Retrieved July 29, 2014, from http://www.rfidjournal.com/articles/view?11469

Violino, B. (2005). Plateau | Your premier telecomm provider for Eastern New Mexico and West Texas. Retrieved May 08, 2014, from http://www.plateautel.com/wireless_stolen_phones.asp

Violino, B. (2011). Watchmaker Tracks Assets in Real Time. Retrieved July 16, 2014, from https://www.rfidjournal.com/purchase-access?type=Article&id=8353&r=/articles/view?8353

Want, R. (2004). Enabling ubiquitous sensing with RFID. *Computer*, *37*(4). doi:10.1109/MC.2004.1297315

Wessel, R. (2006). Clothing Manufacturer Invests Its ROI in RFID - RFID Journal. Retrieved July 16, 2014, from http://www.rfidjournal.com/articles/view?2547/3

Wexler, J. (2004). Case Study: Legoland tracks children with Wi-Fi based RFID - How-to - Techworld.com. Retrieved August 15, 2014, from http://howto.techworld.com/mobile-wireless/532/case-study-legoland-tracks-children-with-wi-fi-based-rfid/

Wood, S. R. (2003, December 25). Asset tracking methods and apparatus. Retrieved from http://www.google.com/patents/US20030235172

Yu, S.-C. (2007). RFID implementation and benefits in libraries. *The Electronic Library*. doi:10.1108/02640470710729119

Zaino, J. (2008). The Queens Library System Grows With RFID. Retrieved July 16, 2014, from https://www.rfidjournal.com/purchase-access?type=Article&id=4237&r=/articles/view?4237

Appendices

Appendix A 2.45GHz RFID Reader

CASC

Product Overview

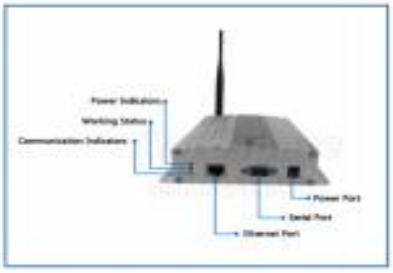
SAAT-F527

Omni-directional RFID Reader

2.45GHz Reader SAAT-F527 can connect to various omini-directional antennas, with high identification and reliability, strong expandability, etc. The read range is adjustable within 0~100 radius meter.

Applications

- Personal position Management in Hospital & Nursing Home, industrial mining and prison sector



Functions

- Support RS-232, 10/100M Adaptive Ethernet; customized RS-485, Wiegand 26/34 interface(optional).
- External interface and power supply configurable for users' need, enhancing flexibility of systematic integration
- Multi-group I/O ports: input interface can detect the TTL or pulse signals of connected devices', used to control the working status of the reader. Output interface can control other devices according to TTL or pulse signals through predetermined conditions
- Support active reading, passive identifying, command trigger, timing trigger, external trigger and other modes, to meet users' various integration needs
- Support multi-reading. Multi-reader operating under intensive environment
- Reading distance is auto-regulation or adjustable
- Strong API port
- All external interfaces under lightning circuit protection, in line with IEC61000-4-5 and ITU-K.21 specifications
- Aluminum shell, high-tension, waterproofing IP55
- Flash memory (optional)

SAAT-F527

2.45GHz Omni-directional Reader

Specifications

RF Parameters	
Operating Frequency	2.4~2.48GHz
Output Power	+15dBm (adjustable by software)
Sensitivity	-85dBm
Identification Angle	Omni-directional
Polarization	Vertical

Communication Interfaces	
Communication Interfaces	RS-232, 10/100M Adaptive Ethernet interfaces
Optional Interfaces	RS-485 interface, Wiegand 26/34 interfaces
I/O Port	2- channel relays output(optional), 2- channel trigger input(optional)
Firmware Upgrade	Support serial port
Application Software Platform	Provide development kit of API (C++ and C#)

Tag operation	
Tag Protocol	Private Protocol
Tag Operating Mode	Compatible with active and passive operating mode tags
Reading Range	0-100m (depend on the tag power output)
Identification Speed	200pcs/s (tag ID)
Anti-confliction	Identifying 300pcs tag at the same time

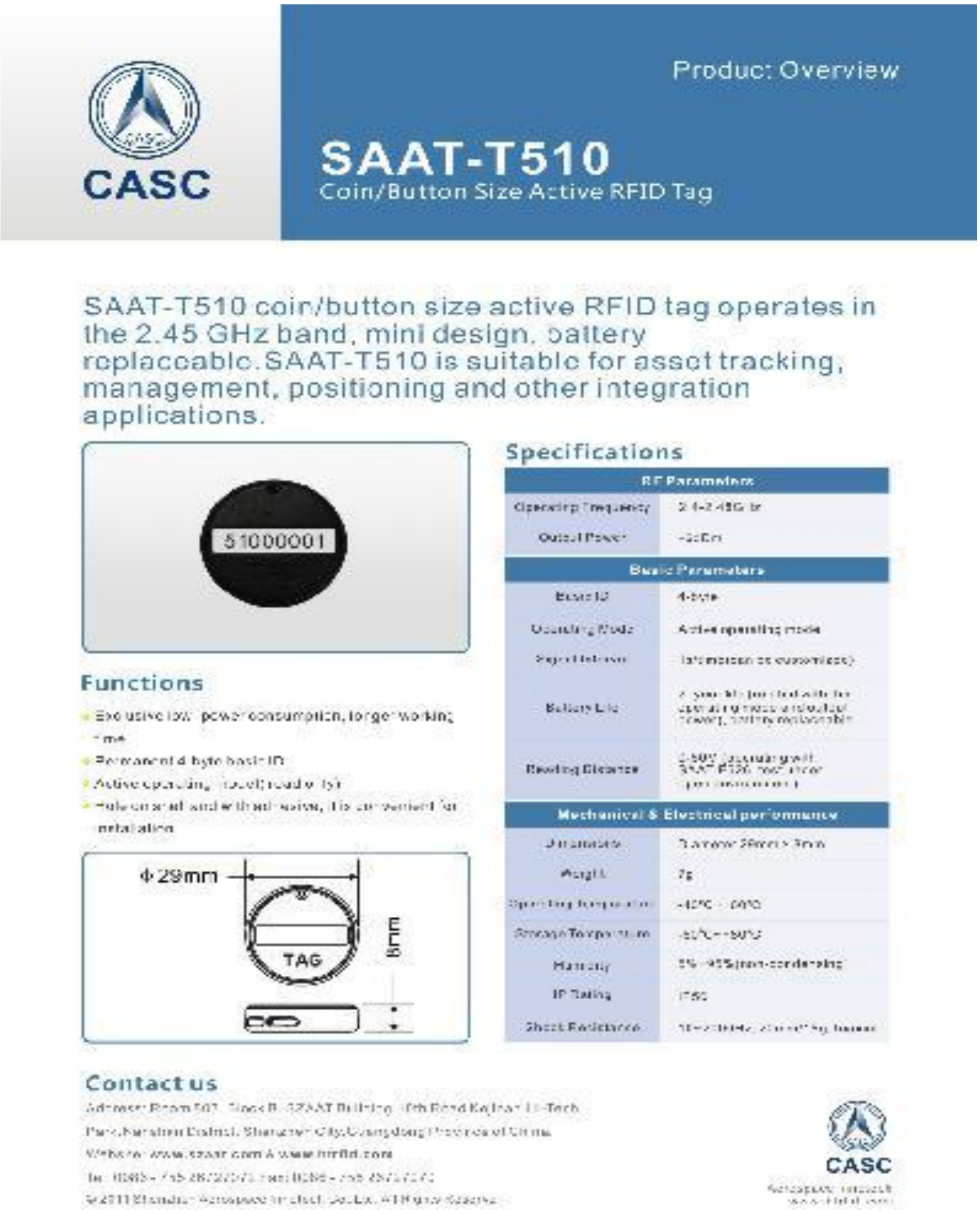
Mechanical & Electrical performance	
IP Rating	IP55
Indicator	Buzzer, LED
Product Dimension	190mm×120mm×40mm(excluding antenna)
Package Dimension	320mm×220mm×139mm
Net Weight	0.6kg
Gross Weight	2kg
Power Supply	DC5V input
Power Consumption	300mW
Operating Temperature	-40℃~+60℃
Storage Temperature	-60℃~+80℃
Humidity	5% ~ 95% (non-condensing)
Shock Resistance	10~500Hz, 100sec/15g, triaxial

Contact us

Address: Room 603, Block B, SZAAT Building,10th Road Keijinan,Hi-Tech Park,Nanshan District, Shenzhen City,Guangdong Province of China.
Website: www.szaat.com & www.hfrfid.com
Tel: 0086 - 755 26727572 Fax: 0086 - 755 26727070

CASC
Aerospace Innotech
www.hfrfid.com

Appendix B 2.45GHz RFID tag (Button/coin type)



CASC

Product Overview

SAAT-T510

Coin/Button Size Active RFID Tag

SAAT-T510 coin/button size active RFID tag operates in the 2.45 GHz band, mini design, battery replaceable. SAAT-T510 is suitable for asset tracking, management, positioning and other integration applications.

Functions

- Exclusive low power consumption, longer working time
- Permanent 4 byte basic ID
- Active operating [illegible]
- [illegible] it is convenient for installation

Specifications

RF Parameters	
Operating Frequency	[illegible]
Output Power	[illegible]
Basic Parameters	
Basic ID	4-byte
Operating Mode	Active operating mode
[illegible]	[illegible]
Battery Life	[illegible]
Reading Distance	[illegible]
Mechanical & Electrical performance	
Dimensions	[illegible]
Weight	7g
Operating Temperature	[illegible]
Storage Temperature	[illegible]
Humidity	5%~95%(non-condensing)
IP Rating	[illegible]
Shock Resistance	[illegible]

Contact us

Address: [illegible] Kejiao [illegible]-Tech Park, Nanshan District, Shenzhen City, Guangdong Province of China
Website: [illegible]
Tel: [illegible]

CASC

Appendix C 2.45GHz Card type RFID tag

Card Type Active RFID Tag

SAAT-T505

SAAT-T505 active RFID tag operates in the 2.45 GHz band, which can be worn or mounted on vehicle windshield. SAAT-T505 can be widely used in school & corporation personnel management & positioning, automatic vehicle identification, parking management, highway toll collection and so on.

RF Parameters

Operating Frequency	2.4-2.48GHz
Output Power	-6dBm

Basic Parameters

Basic ID	4-byte
Operating Mode	Active operating mode
Signal Interval	500ms/time(can be customized)

Battery Life	6–year life (related with the operating mode and output power)
Reading Distance	0-150m(operating with SAAT-F526, test under open environment)

Mechanical & Electrical Performance

Dimensions	3.3 in × 1.4 in × 0.2 in(L ×W × H)
Weight	22g
Operating Temperature	-40℃~+60℃
Storage Temperature	-60℃~+80℃
Humidity	5% ~ 95% (non-condensing)
IP Rating	IP67
Shock Resistance	10~2000Hz, 20mm/15g, Triaxial