1-1-2003

Wireless security for secure facilities

DeAntrious Mitchell
Iowa State University

Wireless security for secure facilities

by

DeAntrious Mitchell

A thesis submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Co-majors: Computer Engineering; Information Assurance

Program of Study Committee:
Steve Russell, Co-major Professor
Doug Jacobson, Co-major Professor
Cliff Bergman

Iowa State University

Ames, Iowa

2003

Graduate College

Iowa State University

This is to certify that the master's thesis of

DeAntrious Mitchell

has met the thesis requirements of Iowa State University

Signatures have been redacted for privacy

Dedication

This thesis is dedicated to Sadhana Jackson. Thanks for being a good friend over the past years. Thank you for making me believe I can achieve even higher success. Thank you for all the late night conversations, telling me I can do it. The nights I could not figure out my homework, you were always giving me encouragement to keep going. I know there were many times I got on your nerves. But you were still there for me. There were many times you gave me strength when I felt I had none. The time when I should have been giving you support when you were tired and stressed. You found the strength to give to me, the will to make it through. I am so sorry that I was unable to return the love you have shown me. What you mean to me you will never know. You have truly been an angel in my life, thank you for being you. I will always be thankful for you. God has truly blessed me, by letting you in my life. I hope and pray with this dedication, you will start to understand.

Table of Contents

List of Tables

List of figures

Acknowledgements

First I had to thank GOD for giving me the strength and energy to complete this research. Then I had to say thank you to Dr. Steve Russell for his guidance and friendship he gave as a major professor. Next I had to thank my other major professor Dr. Doug Jacobson. Thank you for putting up with me all of these years. To, Richard Freeman, thanks for all your help with classes and getting me involved in Information Assurance.

I have to say a special thank you to Nikki Taylor. Not only have you done a lot of work for my thesis, in terms of most of my diagrams and tables, but you provided company for many of the nights while I was in this process. I'm really blessed that you came into my life and we have been able to become close friends. Greg Stamp is a fellow grad student, who helped me develop the jamming process. I wanted to say thank you for the long hours helping me. I want to thank Sadhana Jackson for her help with the formatting of the thesis.

Brylan Alexander not only read through and checked my work for content, but was in the lab many nights when I was in the process. We had many nights filled with laughs while on the caffeine highs.

I wanted to thank my good friend and fellow grad student in the department Josh Graves. During the long hours of researching an idea that many did not take serious, you were there to help motivate me. Then the many laughs and jokes was a great help.

Next I had to thank the people who edited my thesis for me. First I had to thank Chaka Allen (Modulo) for editing my thesis. Stephanie Holeman even though I still think Tae Kwon Doe sucks;☺ thanks for your support and help with this thesis. Eric Junker thanks for your help with editing. Then it has been fun playing with computers over the past few years with you.

Next I wanted to thank the people who did not directly help with my thesis. First I wanted to say thank you to my loving mom. Even though many days I know you did not understand what I was going through, you still gave me the love that I needed to get through. I am for ever grateful. I wanted to think my Aunt Jeannette and my adopted mom Naomi Porter, who still gives me the encouraging words that were really needed. Next I also had to say thanks to Mrs. Jackson, for the encouragement through e-mails and whenever I spoke to her on the phone. Then I had to say thanks to Louis Hill (Modulo). Then I had to send a special thanks to one of my best friends Dani Hite. I can not forget the boss lady Amy. I really enjoyed working with and thank you for looking out for me. I wanted to say thank you to Tom another guy who really took me under his wings during my time at PAX. Then Marcia Hare (You kept me laughing through this rough time). There were many other family and friends I just wanted to say thank you.

Dr Russell has come up with the idea of a wireless Honeynet system. I had suggested getting a patent on the idea. So I wanted acknowledge the honeynet system is Dr Russell's.

1. Introduction

1.1 Problem Statement

This thesis presents methods for securing a facility that has wireless connectivity. When using a hardwired network, an intruder needs physical access to the wire. The problem with wireless networks is that the physical layer is a very large area. The RF signals travel through the air. This makes it easier for an attacker to intercept packets being sent to wireless stations. With RF signals bouncing off of solid objects and traveling through the air, it makes eavesdropping easier. Another issue with wireless technology is spoofing. Within a given distance an attacker can spoof wireless signals and possibly jam the legitimate signals.

An example of this deals with the IEEE 802.11 wireless standard. The RF signals are sent over the 2.4 GHz frequency range. This means the signals can travel a few hundred feet within buildings from its source. The 802.11 standard does use spread spectrum technology, because the FCC specified the use of this technology to minimize mutual interference for all the services that will use the band. Spread spectrum is designed to make it harder to detect and intercept the signals and less susceptible to interference. Since IEEE 802.11 is able to travel a distance from the base, it makes the physical limits hard to secure. This helps an attacker if they wanted to intercept signals. The IEEE 802.11 standard does not provide adequate defense against jamming attacks from an outside source.

The goal is to prevent position location of cellular phones and other wireless devices within the secure facility. When going to a secure facility, devices like cell phones are usually restricted, for fear of cell phone tracking by unfriendly sources. Even if a cell phone is not in use it will still send out signals through attempts to connect to a base station. With

this knowledge, a person would have the ability to track a cell phone inside of a secure area. However, not all cell phones have to connect to a base station in order to connect. Direct connect, a technology that negates the need for a base station by allowing cellular phones to connect directly with one another, is offered by many cellular services.

This thesis will focus on securing a facility that uses wireless devices. The systems of focus are the IEEE 802.11, Code Division Multiple Access (CDMA) and Global system for mobile communication (GSM). The forms of spread spectrum technology are direct sequence and frequency hopping spread spectrum.

1.2 Research Overview

The goal of this research is to develop a solution to securing a facility that utilizes wireless communications. The research will introduce methods to track and locate the position of attackers. This research also introduces the idea of using a Honeynet system for added security. The idea of a Honeynet is not new. Honeynet is being adapted to this research as a potential defense solution. This research uses what is called **Defense-In-Depth.**

Defense- in-depth is when multiple layers of security are used. A more complete description of defense-in-depth is in the section **Defense-In-Depth**. The first of the layers is the Zone of Interference. This Zone is an area where jammer transmitters and directive antennas are set up to take advantage of the ***near-far-effect***. The near-far-effect will be explained in a later technical section (section 4.3). The idea is to use the near-far-effect to give a stronger signal on the perimeter of the secure area, to mask any signals escaping from the secure area.

This Zone uses directive Yagi antenna arrays to direct the radiation. There are multiple jamming methods that are utilized within this Zone. The transmitters are designed to flood the specified frequency range. The jammer design is then set to do what is called a smart jammer. This is done for frequency hopping spread spectrum. A more complete description is given in the section on jamming process.

The next layer of security is the Honeynet Zone. The idea behind a Honeynet is nothing new, but the idea is being adapted to fit this wireless communication security research. The idea is to make an attacker believe that they are seeing real network traffic. This is done at the Honeynet Zone once a device has been determined to be unfriendly.

Decoy mobile devices are first placed within the Honeynet Zone. Spoofed traffic is then created between the Honeynet base stations and the decoy mobile devices Zone, using adaptive antennas incorporated within the design to face the signals away from the inside secure area. Because an attacker could come from many directions, the adaptive antennas are used to provide a stronger signal in the direction of any attacking device.

The third defense is position location and tracking. This is done in the Honeynet Zone and inside of the secure area. The idea is to have constant tracking of all devices in the area. There are several methods available to locate and track a device that is giving off an RF signal. This thesis looks at combining all these methods into an integrated, and more robust, facility security system. Below in figure 1 is the block diagram of the integrated defense system.

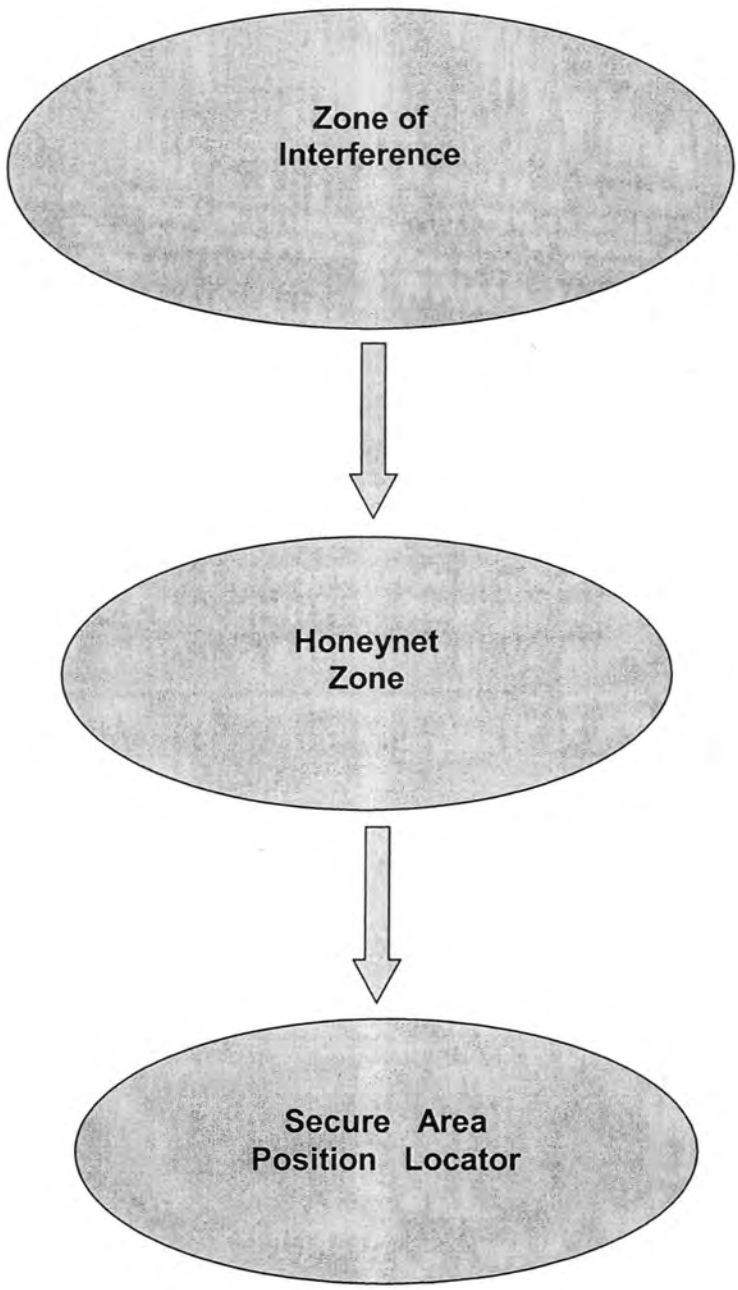


Figure 1.1 Block diagram of the integrated defense system

Defense-in-Depth

Defense-in-depth involves protecting a computer network with a series of defensive mechanisms such that if one mechanism fails, another will already be in place to thwart an attack. Because there are so many potential attackers with such a wide variety of attack methods available, there is no single method for successfully protecting a computer network. Utilizing the strategy of defense-in-depth will reduce the risk of having a successful and likely very costly attack on a network.

The object of this thesis is to explore the ideas of defense-in-depth and propose techniques to implement these ideas. The thesis looks at security with multiple layers. It shows that no security is full proof, so the best thing to do is to give the attacker many roadblocks. The purpose of this is to get the attacker to give up the attack or else be spoofed for some intelligence advantage, frustrating the attacker at one of the layers, or causing the attacker to spend too much time at one of the layers. Doing this will give security personnel more time to locate the attacker. In this thesis three different security approaches are utilized to represent the depth in the security scheme. This thesis uses many security design methods to detour attacks. [31]

1.3 Research Contributions

The key contributions of this research are the novel adaptations of existing ideas and technologies to the problem of providing comprehensive wireless network security

to a building, compound, or other such facility. Although the ideas and technologies are not completely new, they are being utilized in new and innovative ways.

One of these ideas, directive radio frequency interference, is a new result of this work. Exhaustive searching of current literature did not produce a single instance of anyone proposing to use classic military electronic counter measures to secure a wireless network environment. This research looks at ways of directing the jamming signals in the direction of attackers without interfering with the secure area. This also utilizes the near-far-effect to the advantage of the secure area.

Another contribution of this thesis is the utilization of stand-alone Honeynets. This thesis uses Honeynets in the wireless world to deceive the attacker. The Honeynet systems will give the attacker real packets to try and intercept and decrypt, utilizing decoy mobile devices on the wireless side, and servers and wireless base stations setup on the hardwired side. This is to give a complete network environment.

The unique contributions to Honeynet research presented by this thesis are position location and tracking using RF signature. This thesis utilizes not only a spoofed network, but provides the addition of decoy mobiles with spoofed traffic coming from these networks. The Honeynet layer is a complete stand-alone. The same protocols that are in a real network are in this network.

The last contribution of this thesis deals with position location technology. The inside area of the secure facility is the area that will have trusted wireless networking. The issue for the inside deals with an attacker gaining access to this trusted area. The position location system will keep constant tracking of all mobile devices, once they access the trusted area.

1.4 Literature Review

Lathi B P, Modern Digital and Analog Communication Systems

- The key methods for defeating spread spectrum systems were taken from this source. Both direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) are covered. Chapter nine discusses DSSS and how to attack it using the near-far effect [p 410]. Chapter nine discusses FHSS issues such as collisions and multi-path.

Ståhlberg Mika, Radio Jamming Attacks against Two Popular Mobile Networks

- This paper discusses methods of jamming cellular phone systems. It goes into great detail of jamming the call setup and traffic channels.

Poisel, Richard, Introduction to communication electronic warfare systems

- This text gives a great overview of many ideas of electronic warfare. It discusses position location methods and how jamming is done. It goes into great detail on the many different types of jamming, within communication systems.

Internet Security Systems Wireless LAN Security *802.11b and Corporate Networks*

- This text gave a detailed description of attacks against 802.11 networks. The attacks that are discussed in this thesis are against the physical layer.

Hromatka, Thomas, Frequency Hopping Spread Spectrum (FH-SS), EE 521, Dept. Of Electrical and Computer Engineering, Iowa State University: Ames, Iowa

- This paper gave a great detailed description about frequency hopping spread spectrum.

Eekhoff, Eric, An Overview of Smart Antenna Technology, EE 521, Dept. Of Electrical and Computer Engineering, Iowa State University: Ames, Iowa

- The text and the papers listed above were used in developing an idea of how to utilize smart antennas within this thesis.

Ganugapati , Vijay, CDMA IS-95, EE 521, Dept. Of Electrical and Computer Engineering, Iowa State University: Ames, Iowa

- This document gave a good overview of how CDMA setup and call channels operate.

Simon, Omura, Scholtz, Levitt, Spread Spectrum Communications Handbook

- This text gave a thorough detailed look at spread spectrum methods. This text was also a guide to methods of jamming.

Walter GOJ, Synthetic-Aperture Radar and Electronic Warfare

- This text went into great detail about many of the methods of jamming.

Tom Karygiannis Les Owens National Institute of Standards and Technology Wireless Network Security 802.11, Bluetooth and Handheld Devices

- This document went into great detail about how the 802.11 standard operates, giving a good picture of how the 802.11 works and how to attack it.

Nikita Borisov, Ian Goldberg, David Wagener **Intercepting Mobile Communications: The Insecurity of 802.11**

- This paper discussed the ways to intercept 802.11 transmissions. This paper also talks about the shortcoming of WEP and other security methods deployed by the 802.11.

1.5 Thesis organization

This thesis is organized to first give a look at a wireless communication overview. Next, it moves into spread spectrum methods. A look at Multiple Access Methods follows, along with a look at current Methods of Security and Electronic Warfare techniques. The next sections will go into the Research Contributions for this thesis. Last will be the conclusion and a discussion of future work.

2. Wireless Communication Overview

Table 2.1 Key Characteristics of 802.11

Physical Layer Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS)
Frequency Bands 2.4GHz (ISM band) and 5GHz
Hop rate 1Mbps, 2Mbps, 5.5Mbps, 11Mbps (11b), 54Mbps (11a), 54Mbps (11g)
Wired Equivalent Privacy (WEP) RC4-based stream encryption algorithm for confidentiality, authentication and integrity. Limited key management
Operating Range About 100 feet indoors to over 1500 feet outdoors
Positive Aspects Ethernet speeds without wires; many different products from many different companies. Wireless client cards and access point costs are decreasing
Negative Aspects Poor security in native mode; throughput decrease with distance and load.

[39]

Table 2.2 IEEE 802.11 channels with frequencies

Channel	Frequency (GHz)
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462

[39]

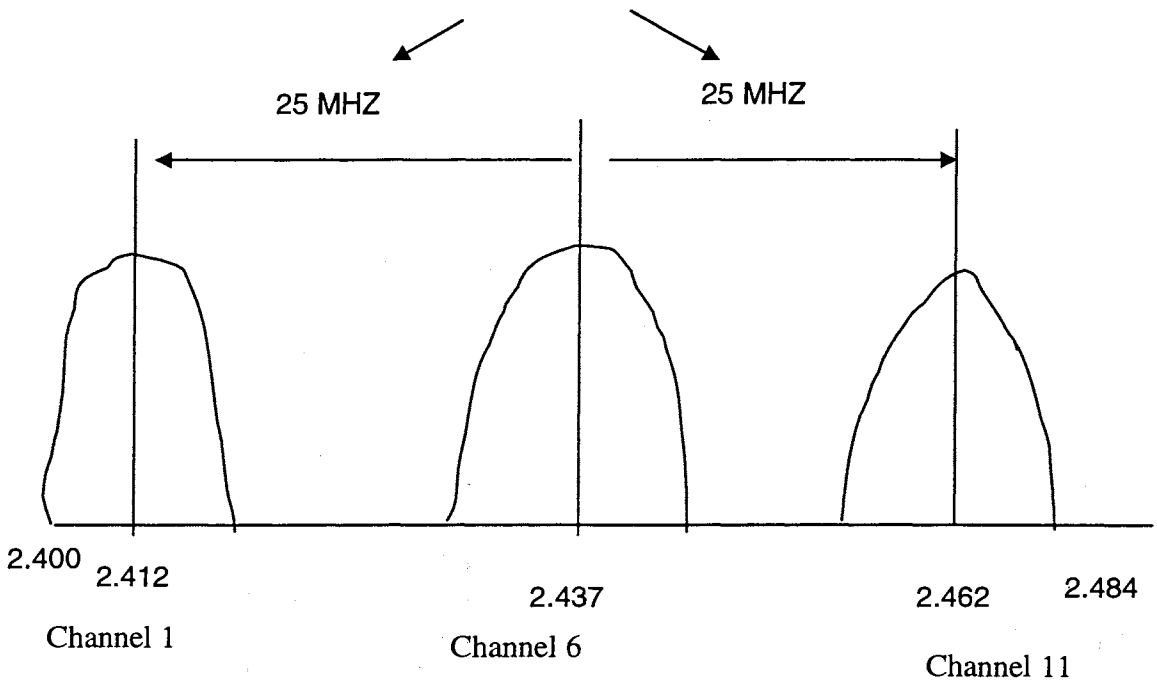


Figure 2.2 Minimum Channel Spacing between center frequencies 802.11 [39]

2.1 Introduction

2.2 Spread Spectrum Methods

Spread Spectrum techniques involve the use of a variety of radio-frequency modulation techniques to provide a measure of security. Two reasons to use spread spectrum are to minimize the effects of jamming and to hide or conceal data by spreading the bandwidth that is needed to transmit a signal. Spread spectrum was developed by the United States Military to transmit codes that were hard to detect and hard to jam. The signal gets spread across a frequency spectrum. It makes the signal resistant to noise, eavesdropping and interference.

There are two main Spread Spectrum techniques in use today. The most common techniques are called **direct sequence and frequency hopping**. Direct sequence is a method that spreads the signal out over a great distance, hiding the signal within what most systems consider noise, and thereby creating resistance to signal Interference and jamming. Frequency hopping thwarts resistance through use of its hopping sequence. In some frequency hopping systems, the signal hops 1600 times a second. This makes it hard for an attacker to find the correct frequency for interception and jamming. More complete descriptions of frequency hopping and direct sequence can be found within the appendix sections **Direct Sequence** and **Frequency Hopping**.

2.2.1 Direct Sequence

Direct Sequence Spread Spectrum (DSSS) is a transmission technology used in local-area wireless network (LAWN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. This increases the signal's resistance to interference. The original data can be recovered due to the redundancy of the transmission, if one or more bits in the pattern are damaged during transmission. This is true in a manner of speaking but only occurs when very short bursts of noise happen. Otherwise, it is the correlation process that gives it the best properties. **[52]**

2.2.2 Frequency hopping source

Frequency Hopping Spread spectrum (FHSS) is a transmission technology used in local-area wireless network (LAWN) transmissions where the data signal is modulated with a

narrowband carrier signal that "hops" in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. The signal energy is spread in the time domain rather than chopping each bit into small pieces in the frequency domain. This technique reduces interference because a signal from a narrowband system will only affect the spread spectrum signal if both are transmitting at the same frequency at the same time. If synchronized properly, a single logical channel is maintained.

The transmission frequencies are determined by a spreading, or hopping, code. The receiver must be set to the same hopping code and must listen to the incoming signal at the right time and correct frequency in order to properly receive the signal. The FCC requires manufacturers to use 75 or more frequencies per transmission channel with a maximum dwell time (the time spent at a particular frequency during any single hop) of 400 ms. **[51]**

2.3 Multiple Access Methods

2.3.1 Time Domain

Time domain is a representation of signal as a function of time.

$\Delta t = A(t)\cos[2\pi fc\tau + \phi c + \phi(x)]$ **Equation 2.1**

Δ = Envelope function (carries information)

f c= carrier frequency

t = Independent variable of time

ϕ = Carrier Phase

$\phi_{(\tau)}$ = Phase Function (this carriers the information)

[33]

2.3.2 Frequency Domain

Frequency domain is a representation of a signal as a function of spectrum.

$s_n(t) = c(t)A(t)\cos[2\pi f_c t + \phi_c + \phi_n]$ **Equation 2.2**

$A+\phi$ = constant over time interval

[33]

2.3.3 Code Division

Code Division Multiple Access (**CDMA**) is a military technology first used during World War II by the English allies to foil German attempts at jamming transmissions. The allies decided to transmit over several frequencies, instead of one, making it difficult for the Germans to pick up the complete signal. **[53]**

CDMA works by converting speech into digital information, which is then transmitted as a radio signal over a wireless network. CDMA is a form of multiplexing. This allows numerous signals to occupy a single transmission channel, optimizing the use of available bandwidth without static, cross-talk or interference. CDMA is used in ultra-high-frequency (UHF) cellular telephone systems in the 800-MHz and 1.9-GHz bands. **[53]**

CDMA employs analog-to-digital conversion (ADC) in combination with spread spectrum technology. Audio input is first digitized into binary elements. The frequency of the transmitted signal is then made to vary according to a defined pattern (code). A receiver, whose frequency response is programmed with the same code, is the only device that can intercept the signal. There are trillions of possible frequency-sequencing codes; this enhances privacy and makes cloning difficult. **[53]**

2.4 Wireless Networking Systems

2.4.1 IEEE 802.11b

This standard is also referred to as *802.11 High Rate* or *Wi-Fi.* 802.11b is an extension to 802.11 that applies to wireless LAN networks and provides 11 Mbps transmission. It has a fallback to 5.5, 2 and 1 Mbps in the 2.4 GHz band. 802.11b uses DSSS. 802.11b is a modification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet. **[55]**

2.4.2 GSM

Global System for Mobile communications (GSM) is a sophisticated cellular system used worldwide which was designed in Europe. A more complete description is in the Appendix section **GSM. [55]**

2.4.3 IS-95 CDMA

This is a standard which describes a cell system which uses a CDMA link and operates at 800 MHz. Sometimes the term is also used to describe 1900 MHz CDMA. A more complete description of IS-95 can be found in the appendix section **IS-95. [55]**

3. Electronic Warfare and Electronic Security

3.1 Methods of Electronic Warfare

3.1.1 Electronic Warfare (EW)

Electronic Warfare involves electromagnetism and directed energy to control the electromagnetic spectrum of transmitted data. There are three major subdivisions within electronic warfare: electronic attack, electronic protection, and electronic warfare support. **[29]**

3.2 Denial of Service

3.2.1 Jamming

Denial of Service (electronic attack)

Jamming is a form of ECM in which noise or noise like signals are transmitted at frequencies in the receiver bandpass to obscure the signal. This is the deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of disrupting enemy use of electronic devices, equipment, or systems. Jamming prevents a victim's receiver from demodulating the correct signal.

This process can also be used to defend, rather than attack, a wireless network work environment. This research uses the ECM signals to prevent the receiver used by an attacker from demodulating the signals from the inside secure area. **[29]**

Anti-jam

The jammer-to-signal (J/S) ratio, also known as the anti-jam (AJ) margin, provides a measure of how vulnerable a system is to interference. A larger jammer-to-signal ratio represents a greater system capability for noise rejection. The equation for (J/S) is given in Eq. 3.3. G_p is the processing gain of the system and is equal to the spreading bandwidth (W_{ss}) divided by the data rate, R, in bits per second. E_b is the bit energy. J_o is the equivalent noise power spectral density (PSD) due to the jammer. The ratio (E_b/J_o) is the SNR required to maintain the connection at a specified error probability. **[48]**

$$J/S = \frac{G_p}{E_b/J_o} \qquad \textbf{Equation 3.3 [48]}$$

There is an actual J/S and a minimum required J/S at the receiver input.

The AJ margin (M_{AJ}) is equal to the processing gain times the difference between the reciprocals of the signal-to-jammer ratios received and required. A larger M_{AJ} signifies a system with greater noise rejection capability. **[48]**

$$M_{AJ} = G_p\left[\frac{1}{(J/S)_{recv}} - \frac{1}{(J/S)_{recdv}}\right] \qquad \textbf{Equation 3.4 [48]}$$

Directive radio frequency Interference

By directing the radiation pattern in a given area, directive radio frequency interference allows the jamming signals to act has an invisible barrier. This is the key to this portion of the research. In the section below about the Yagi antenna, Yagi antenna array setup is discussed.

The Yagi antenna array will face in a given direction away from the secure area. The goal of this is to jam the call setup and traffic channels in the physical layer by pointing the interference signals around the base in a geometric configuration that will give total coverage of the target area. This will keep hostile mobiles from sending signals from a hostile call setup, and from using a hostile mobile unit to receive signals. The process of directing RF signals will allow a geographic zone to protect the facility. This will create a large jamming signal that prevents the unfriendly receiver from acquiring and demodulating the friendly transmitter signals.

3.2.2 Network Flooding

This is a form of denial of service. Network flooding is when a network gets congested from too much traffic. This is done in more then one way. Getting too many requests to connect is one way to flood a network. This is known as a syn flood attack. In terms of a wireless network, this is done when the wireless channel is filled to capacity or the base station can no longer expect connections. A good example of this is the Sprint PCS network. When Sprint PCS base stations become flooded, the system will not allow a user to place a call.

3.3 Eavesdropping

Eavesdropping is when a system is setup to intercept a signal between two parties. Placing the interceptor within reception range of two communicating stations is one eavesdropping technique used in wireless communication, and is a technique of choice for government agencies like the National Security Agency (NSA). NSA has towers and other

devices setup around the world to eavesdrop on countries. Blind Man's Bluff is an example of a site used by the National Security Agency and Naval Intelligence to eavesdrop on others through the use of inductance given off from devices such as network cords and monitors. The Navy was able to eavesdrop on the Soviet Union by putting a device on a Russian cable located under water. The device was able to record all traffic going along the cable using measurements based on radiation leaks and cable inductance. **[62]** Another example of this can be found through examination of U.S. Navy ships and airplanes designed to intercept communications. Requiring close proximity to the signals being produced, these ships have been utilized on many Navy eavesdropping missions. **[68]** Figure 3.3 demonstrates an example of placing a device in between two communication towers.

This research gives a method to stop this from happening. Eavesdropping is a unique challenge, and is a particularly serious problem for wireless security.

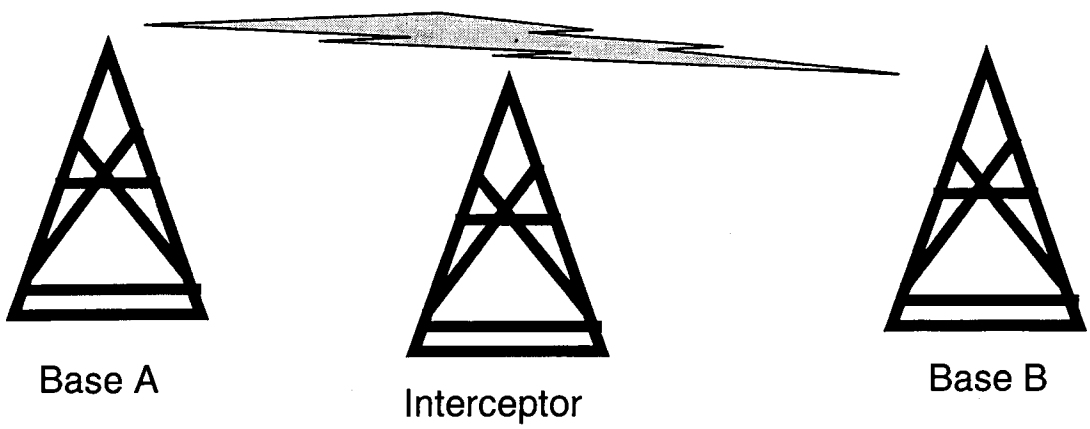


Figure 3.3 Signal Intercept/ Eaves dropping redone by Sadhana Jackson

3.4 Spoofing and Cloning

Spoofing is the process of faking a signal or a system that will fool users. Spoofing is done in many different ways. IP address spoofing is when an attacker fakes an IP address and pretends to be someone else. In the wireless world an attacker could pretend to be a base station and route traffic through it. Another example of spoofing in the wireless world deals with an attacker on the same channel transmitting false data. This is what the scenario shows below.

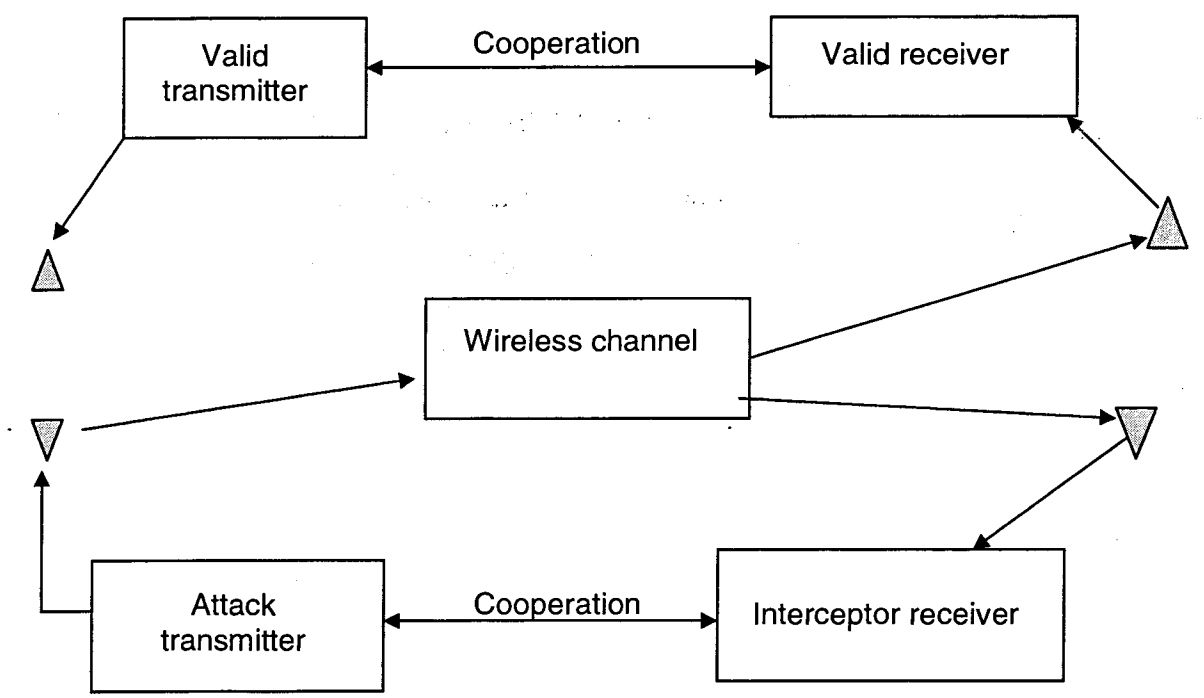


Figure 3.4 Counterfeit Base Scenario [33] redone by Nichole Taylor and Sadhana Jackson

3.5 Position-Location of hostile Portables

Time of Arrival (TOA)

The wireless device's signal is received at various antenna sites. Since each antenna is usually different distances from the device, the signal arrives at different times for each antenna. This technique requires signal timing information from at least three different antenna sites. [33]

Direction of Arrival (DOA)

This is also known as angle of arrival. The wireless device's signal is received at various antenna sites. Each antenna site is also equipped with additional gear to detect the compass direction from which the device's signal is arriving. [33]

Ranging

Ranging is a technique that is an active system, which sends out a signal to or from a mobile and reflects the signal back to the ranging station. The system then uses the round trip time delay to calculate the distance. The long integration time allows good performance in a signal to noise environment. [33]

Position location by strength of signal

This method is an idea from electromagnetic theory that uses the transmitted power of a mobile to locate the mobile. This is a method works with at least two base stations. For better results more base stations are needed. The base stations that are nearest to the source of the RF signal will receive the signal from the mobile station. [33]

3.6 Antennas

Adaptive Antenna arrays

Adaptive antenna arrays, or smart antennas, use a combination of an array of multiple antennas and appropriate signal processing to produce desirable antenna patterns. Such patterns have high gain in the direction of desired signals and null gain in the direction of undesired signals. Antenna arrays allow for multiple accesses. Adaptive arrays are used extensively in third generation cellular. Adaptive arrays can be used to maintain a beam of desired shape. **[49]**

Adaptive antenna arrays are used by this thesis for a few reasons. The first use of adaptive antenna arrays is at the Zone of Interference. The idea is to have an array of jamming stations set up around the perimeter of a facility. The jamming stations will use Yagi antennas. This is explained with greater detail in the section **Zone Of Interference**. The array will give maximum coverage around the given area. When a hostile mobile device comes into the area of the jamming stations the signal will concentrate on the device.

4. Wireless Facility Defense-in-Depth

4.1 Integrated Facility Security – Threat Assessment

There are many security concerns that come when dealing with wireless connectivity for a high security facility. They are as follows.

1. Signal intercept
2. Radiation leaks
3. Jamming
4. Locating rogue wireless devices (one in the area)
5. Position location of facility personal by un-friendlies

These issues have been thought during the research process for this thesis. The next section, **Integrated Facility Security**, discusses how an attacker will approach the secure facility, and the processes that will occur at each level. The security for the thesis research is as follows.

1. Zone of Interference
2. Honeynet layer
3. Position Location and Tracking

Integrated Facility Security

In order to explore the ways of implementing security to deal the issues just presented, the concepts and theories must be discussed first. There are three approaches that will be discussed in following sections:

1. The use of electronic countermeasures against an attacker.
2. Position-Location of an attack transmitter.
3. Spoofing of an attacker using a Honeynet.

The next section will show the concepts and theories of locating the RF signal. Once the RF signal has been located, various techniques will be used to track and locate the signal from the base station. The last technique that will be discussed deals with setting up a wireless communication system that attracts the attacker rather than sacrificing the real network. This is a theoretical but practical approach that will keep attackers busy so the security personnel can track and intercept the attacker.

The Zone of Interference is the first layer an attacker would come to. The idea of this Zone of Interference is to direct jamming signals in a direction that faces away from the secure area, creating a zone of protection around the secured area and convincing the attacker that wireless connectivity has been achieved.

Step 1

Attacker approaches the area with their mobile station. Some attackers will try to passively attack the area. This is done with signal interception. The attacker has their mobile station in what is called promiscuous mode. This is when the wireless network interface card sees all packets. The goal of the wireless network interface card is to demodulate the signals coming from a base station. When the attacker is within the Zone of Interference they will not be able to see the signals from the base stations. As stated earlier, the jamming stations will take advantage of the **near-far-effect**. The jamming stations will be closer and sending out a stronger signal then the base stations. This means that the signal the attacker will be forced to receive will be the signal coming from the jamming station.

The Zone of Interference will not only stop passive attacks, but active attacks too. For these attacks to work the attacker will have to receive a signal. The next form of an attack that can be tried is the rogue base station. If an attacker were attempting to setup a

rogue base station on the perimeter of the area, they would try to get friendly mobile stations to connect to it. This would cause passwords, usernames and other vital data to be compromised. The Zone of Interference would once again be able to stop this form of attack. The jamming stations would radiate a signal out in the direction of rogue station and mobiles that it might be able to contact.

Step 2

The first layer of security is good but not fool proof. With enough time an attacker will be able to figure out that within certain locations, their network interface cards are not responding the way they want them to. So an attacker might try to move closer within the area. This is to get more effective access to the signals they wish to intercept. Once the attacker gets beyond the Zone of Interference, they will come to the Honeynet system. Once coming to this layer of defense the attacker will pick up a signal. The signal they will pick up, however, will be from the Honeynet system. The Honeynet system has two purposes. The first is to distract the attacker. When the attacker comes to this location they will see spoofed signals. Not only will they see spoofed signals, but also the packets they see will be encrypted. The attacker will then see fake mobile stations as well. These stations are set up to give the attacker real data in transmission. If data were only being sent between stations an attacker would be able to realize the network is a decoy through simple network analysis. The attacker will see traffic between decoy mobile stations that are placed around the Honeynet area.

A savvy attacker, however, will do research into their target before attacking. To foil such research, the attacker is provided with an area that has all of the same things a real

network has. There are mobile units talking between the base stations, as well as mobile stations beaconing for a signal from a base station. These are just a few things an attacker will see within this area.

Once mobile stations are picked up by the Honeynet system, the system will determine whether the station is friend or foe using the MAC Address and the spectral characteristics of the network interface card. Then the position locator at the Honeynet Zone will perform position location and tracking to confirm the identity of the mobile unit.

Step 3

The next layer of security that an attacker will come to is the position locator within the secured area. Any mobile station entering the secured area is tracked, and its location is monitored, keeping the station space under constant observation. As soon as an attacker decides to either launch an attack or tries to exploit the system; the security system will know where the hostile mobile station is located.

4.2 Overall Geographic Design

The above geography represents an example of the area that is being secured. The outer rings represent the Zone of Interference. This is only a rough drawing of an example area. In the following sections the identical drawing is given for the next layer of security.

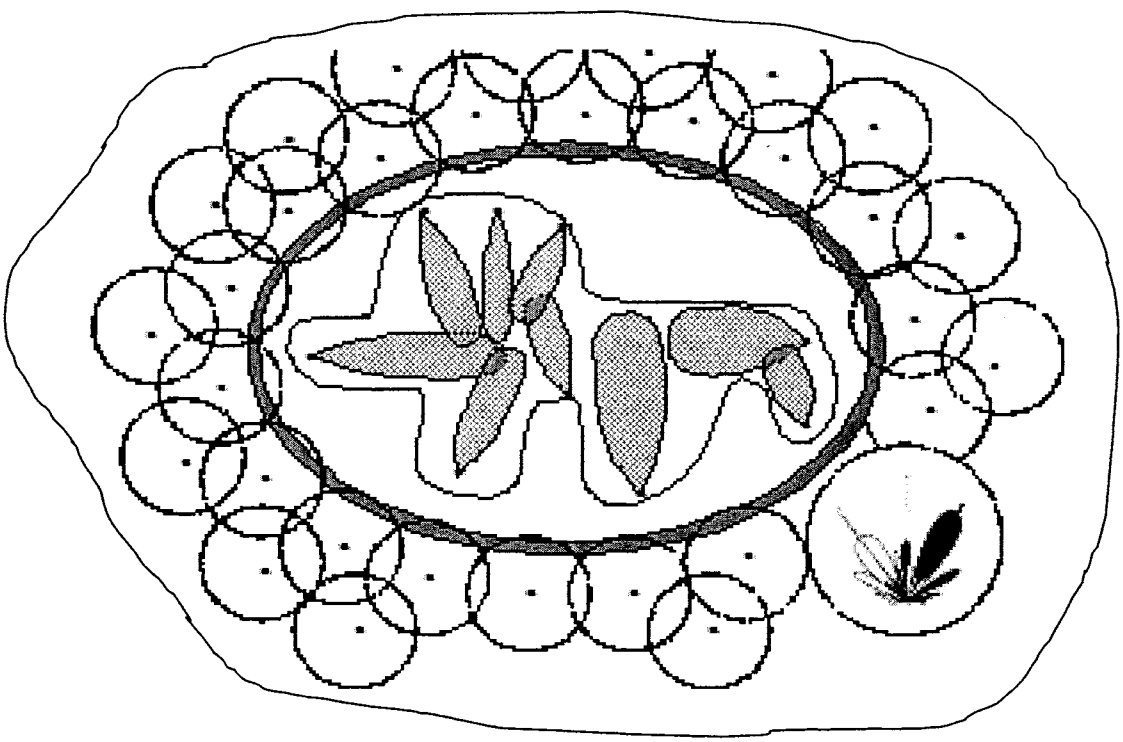


Figure 4.4 Overall Geographic Design

4.3 Electronic Countermeasures – Zone of Interference

The design process of this part of the defense-in-depth concept is very important. The Zone of Interference (dubbed the "cone of silence") is the first line of defense. The jamming concept discussed previously will be the key to these countermeasures. The ideas or theories behind this research are to use jamming as a defense instead of its usual role as an offense. No record of a technique like this exists in print, and discussions with members of the National Security Agency reflected interest in this technique as a novel approach to wireless security concerns. The reason jamming would work is simple. The advantage of the near-far effect and the low jamming margins of commercial designs such as 802.11b (direct sequence spread spectrum) make it easy to jam attacker receivers. For example, the jamming margin of 802.11b is only around 10. The designers of IEEE 802.11b only used the bare minimum to satisfy the FCC requirement. In contrast, the GPS military system has a jamming margin of 200,000. **[32]**

When a Zone of Interference is set up, it would, in theory, block the unfriendly receiver from correctly receiving any signals from inside the facility, including the base station it is trying to attack. **[32]** The goal is to direct the jamming energy in the direction of the insecure area while reducing it to acceptable levels inside the facility. The goal is to create a Zone of Interference that surrounds the area.

The way to achieve this is to use directive antennas and antenna arrays. This will allow the electronic countermeasure signals to be directed outward. Figure 4.5 is an example of the jamming situation for the secure area.

The goal of this system is to jam multiple types of wireless connections. The next sections will discuss multiple techniques of jamming wireless system frequency bands such

as 802.11 and the cellular ranges. This thesis will show two jammer designs. The first is for direct sequence and the other is for frequency hopping. The use of the near-far-effect as a key element in securing wireless systems is central to this thesis. By jamming the geographic area outside of the secure zone, the signal strength of the jamming signal will be greater than the signal that the attacker is attempting to compromise. **[33]** This thesis shows how the **near-far-effect** will be able to play a major role in the wireless network connectivity security of a facility. The transmitter's stations are placed in a ring like pattern around the area. Each station is set an array to give a stronger signal. **[33]**

Effectiveness of Jamming Zone

The jammer sphere of influence will allow the signals from the jammer to overpower any signals coming from the secure area. The power of the jammer will cause the mobile to demodulate the jammers signal. The Zone of Interference takes advantage of the near-far effect. This states that power varies by $\frac{1}{d^2}$ in respect to distance (d) between the base and the mobile device. This says that the signal will deplete has the signal travels further from the source transmitter. The incoming mobile receiver will acquire the signal that is nearest and most powerful. **[33]**

There are disadvantages to the jamming system in terms of friendly communications. There is no way of the jamming system to tell friend from foe. Friendly communication would be disabled within the jammer's sphere of influence. A visual example is shown in figure 4.4

The Near-Far Effect

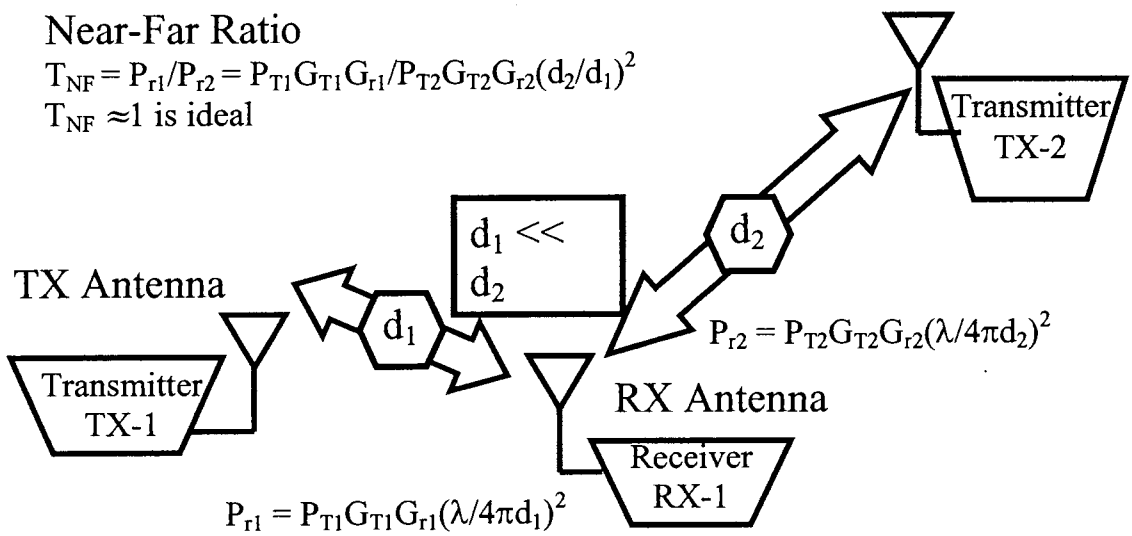


Figure 4.4 [33] redone by Nichole Taylor and Sadhana Jackson

Jammer Types

Barrage jamming

Jamming is accomplished by transmitting a band of frequencies that is large with respect to the bandwidth of a single emitter. Barrage jamming may be accomplished by presetting multiple jammers on adjacent frequencies or by using a single wideband transmitter. Barrage jamming makes it possible to jam emitters and receivers on different frequencies simultaneously and reduces the need for operator assistance or complex control equipment. These advantages are gained at the expense of reduced jamming power at any given frequency. [33]

Barrage jamming is ideal for the jamming process proposed here. The jamming zone has to jam direct sequence and frequency hopping spread spectrum. Direct sequence is a narrow band system. This is not the case for frequency hopping, which uses a wide band system. Knowing this makes barrage jamming one of the best methods to utilize. Since the goal is to deal with both spread spectrum systems, this thesis will use wide barrage jamming, thus covering both spread spectrum systems. The research shows two jammer designs are needed, to cover both FHSS and DSSS. The following section gives an example of how the jammers will work. The example used is GSM cellular. The methods used for jamming CDMA and 802.11b DSSS are similar. [33]

Smart Jamming

There are many ways to turn a jammer into a smart jammer. Within this thesis a design is presented to perform smart jamming for direct sequence and frequency hopping spread spectrum systems. In the sections for jamming a greater explanation is given of smart jamming.

4.3.1 Geographic

Design

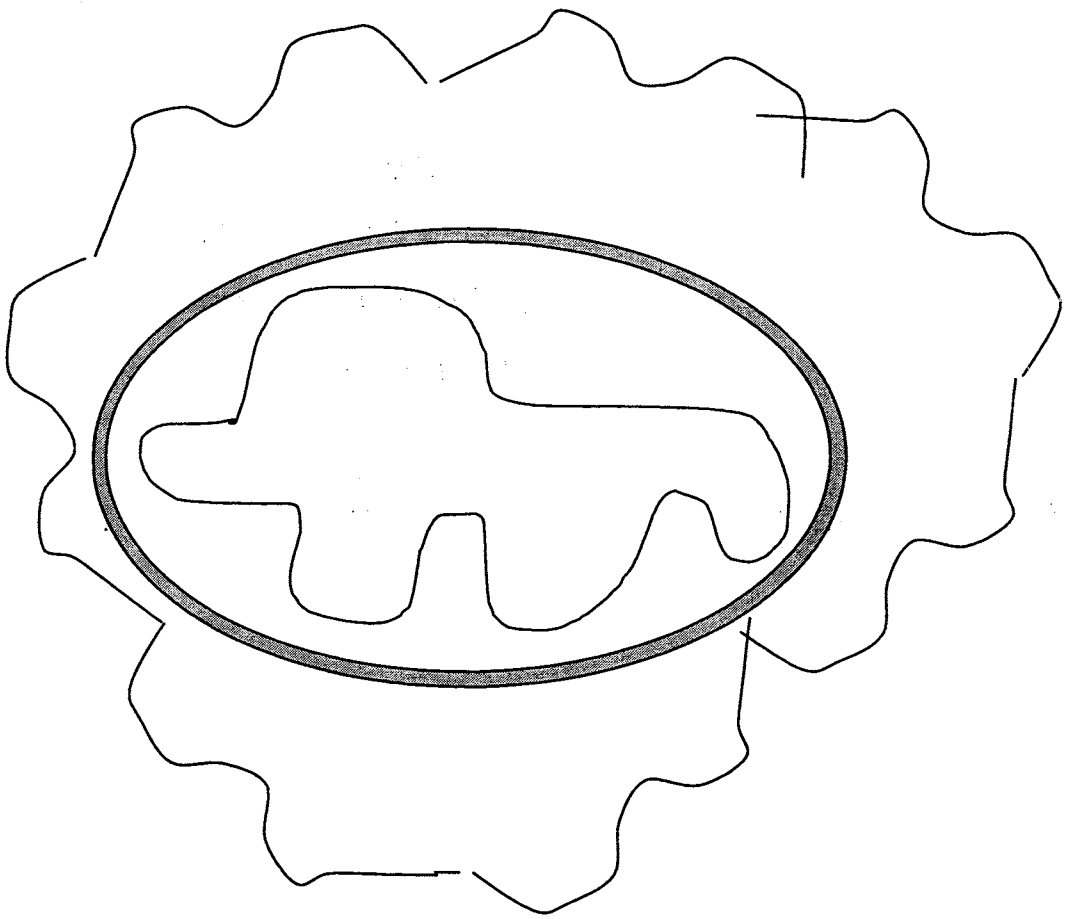


Figure 4.5 Geographic Design for Zone of Interference

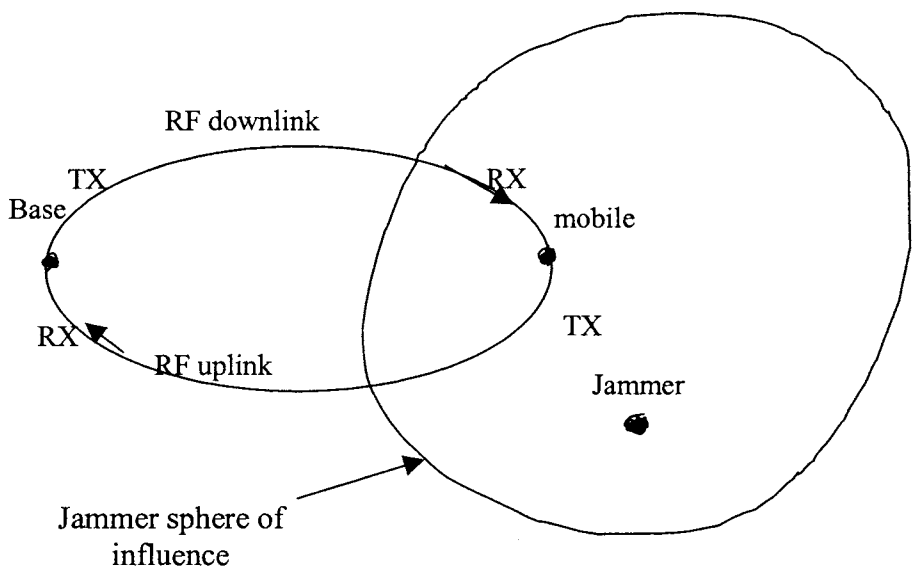
The outer ring of the diagram represents the Zone of Interference.

4.3.2 Antenna Design - Directive RF Interference

This is a process utilized with the system. By directing the radiation pattern in a given area, allows jamming signals act as an invisible barrier. This is the key to this portion of the research. In the section below about the Yagi antenna, will describe how the Yagi antennas are set up in an array. The Yagi antenna array will face in a given direction away from the secure communications and Honeynet areas. The goal of this is to jam the call setup and traffic channels in the physical layer, by pointing the interference signals in particular directions around the base, giving total coverage. This will keep hostile mobiles from receiving the signal, and will jam the call setup on the attacker's mobile device. The process of directing RF signals will allow a geographic zone to protect the facility. This will create a large jamming signal that prevents the unfriendly receiver from acquiring and demodulating the friendly transmitter signals. **[33]**

Figure 4.6 Jammer sphere of influence example

This diagram shows how the jamming systems sphere influence works against the attacking mobile. This shows how the jammer is not allowing the mobile to receive and transmit correctly.



[41] Figure 4.6 redone by **Nichole Taylor and Sadhana Jackson**

4.3.3 Jammer Design for DSSS and FHSS

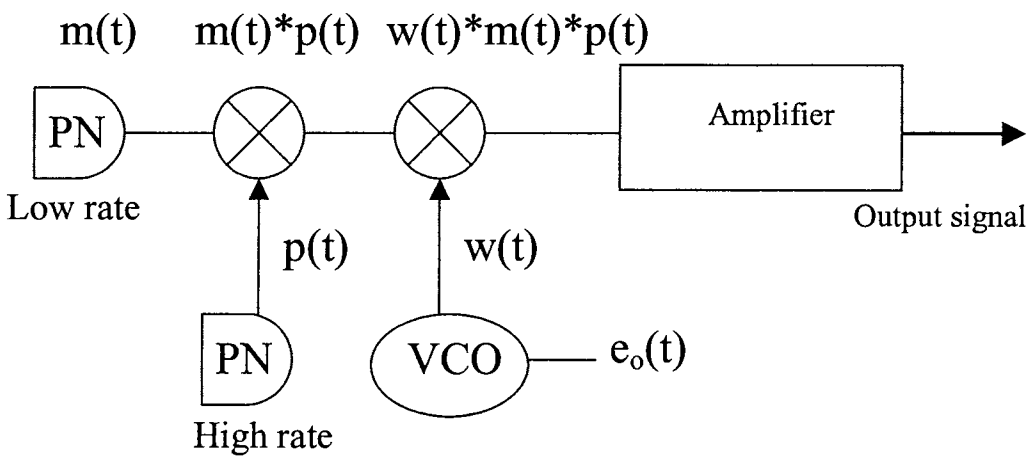


Figure 4.7a DSSS jamming block diagram [47] and author redone by Nichole Taylor

4.3.3.3.1 Direct sequence jammer components

m(t)= message signal

c(t)= polar signal (pseudo random carrier)

VCO= voltage control oscillator

Amplifier= this is used to make the signal stronger

w (t)= output signal

eo(t)= external voltage

[32][33][35]

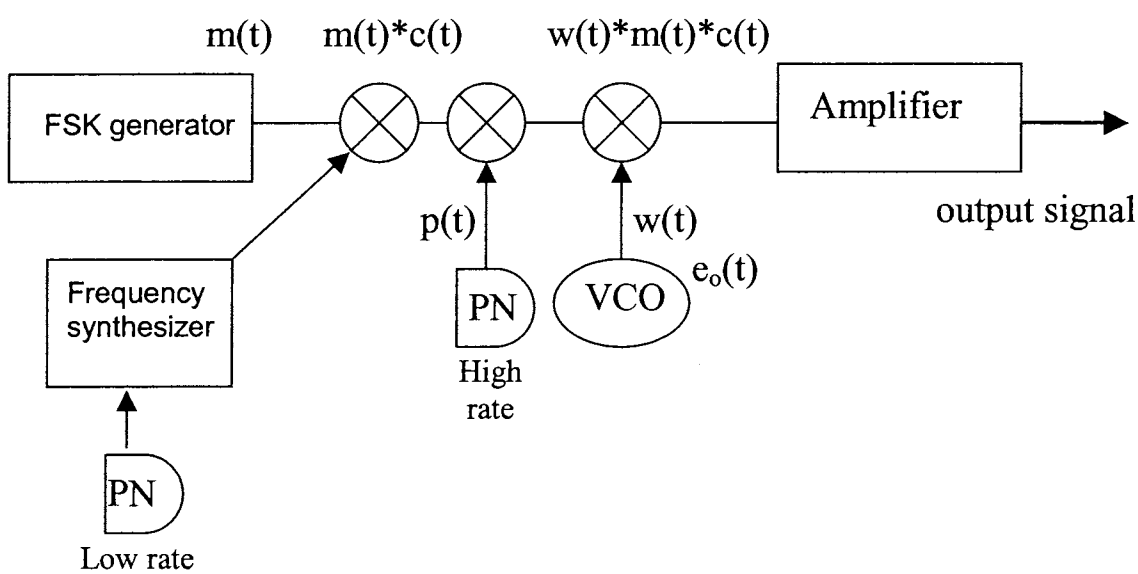


Figure 4.7b jamming block diagram for FHSS [32] and author redone by Nichole Taylor

4.3.3.3.2 FHSS jammer components

FSK generator= frequency scheduling key generator

Frequency synthesizer= helps determine the frequency to hop

m(t)= message signal

c(t)= polar signal (pseudo random carrier)

VCO= voltage control oscillator

Amplifier= this is used to make the signal stronger

w (t)= output signal

eo(t)= external voltage

[32][33][35]

4.3.3.3.3 Jamming process and design

The jammer for direct sequence spread spectrum is able to work for a few reasons. Primarily, this technique generates a signal across the frequency range of the target signal that looks like noise to receivers. This means direct sequence receivers will be not able to demodulate the signals correctly. This jammer design sends out two polar signals, a high rate and a low rate. The amplifier in the design serves to over power other signals. This is another concept drawing on the principle of near-far-effect. **[35]**

As explained in the section for DSSS, the polar signal is used to put the message back together, confusing the attacking receiver through the use of multiple polar signals. This is the method the jammer will use to do what is known has smart jamming. The section of DSSS weakness that the jammer exploits within the Zone of Interference explains in greater detail the process that is used. **[35]**

The same concepts are used for frequency hopping spread spectrum. The jammer for frequency hopping has both a frequency synthesizer and frequency scheduling key generator. The pseudo random number generator is connected to the frequency synthesizer. Recall that

in frequency hopping the generated frequency shift key is shifted by an amount determined by the pseudo random number generated code. The frequency shift keying is added with the synthesizer frequency and the frequency shift keying. This design will send signals out for a wide band system. The band pass filter selects the sum frequencies and suppresses the difference frequencies. The data then gets transmitted. The data then hopes over a range of frequencies that is determined according to the pseudo random number generated code. **[35]**

This will cover the whole frequency band. It is known that frequency hopping is able to avoid interception and jamming because of the hopping sequence. In military system the hopping sequence is around 1600 hops per second. The design also will try to confuse the receiver of an attacker. A greater description of both systems and the jammer design is include within the following sections. First will be shown a brief description of how frequency hopping and direct sequence works. Then the process for beating both spread spectrum systems will be presented. **[35]**

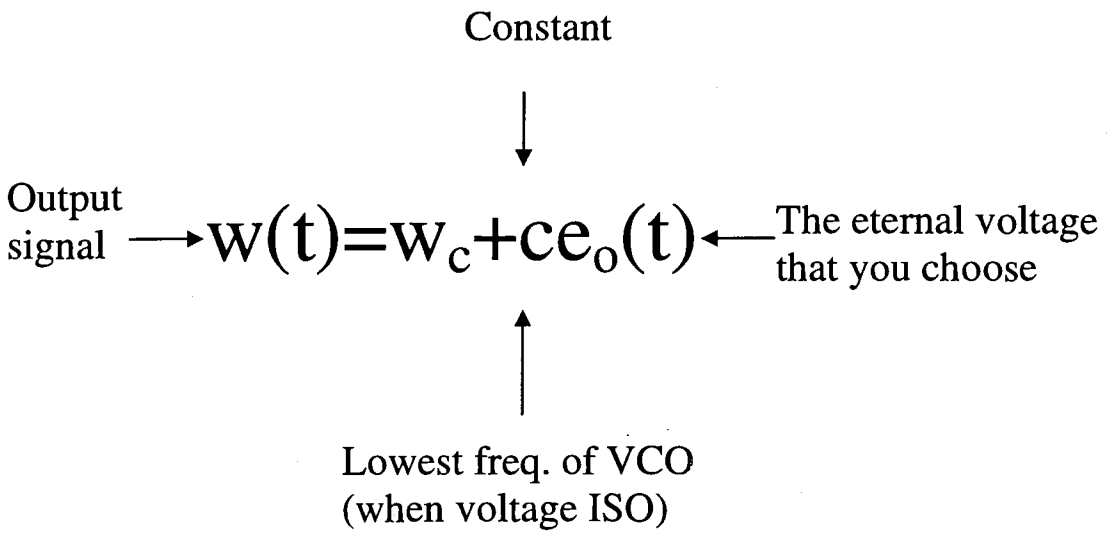
The jamming transmitter designs contain a voltage control oscillator (VCO). This is to determine the frequency to jam. A more complete description of VCO is in the section methods of jamming. Each jamming station has the circuits that were just described.

4.3.3.3.4 Methods of jammer operation

These are just two methods proposed by this thesis to jam within the Zone of Interference. The next is a method that the transmitter in the jamming design will use to fool the receiver of the attacking mobile device. This process is explained in the section below.

First is the equation for the voltage control oscillator (VCO). By using a VCO within the circuit, the jammer is allowed to sweep the whole frequency range forward and back. This is to prevent the need to guess where the signal is located in the range. For example, a

signal could be at 2.43 GHZ. A jammer would have to know this in order to jam the signal. By jamming the whole spectrum range, guessing is eliminated. The following equation shows how the output signal is determined. **[35]**



Equation 4.4 [38]

VCO generates a sine wave of the frequency you want to jam

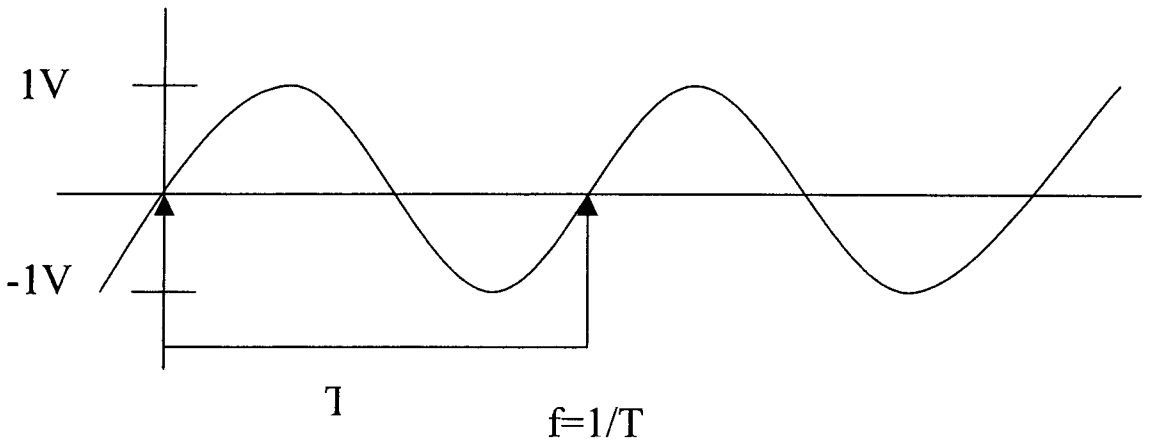


Figure 4.8 VCO [38]

If a frequency change were desired, the voltage would have to be changed. Frequency changes linearly with the voltage. This design is universal for the frequencies that this thesis proposes to jam within the Zone of Interference. The VCO would need to be changed to adjust to the 802.11 and cellular frequencies. **[35][38]**

The jammer has an amplifier connected to it. This is to make the signal stronger to cover the given area. By amplifying the signal, it will give noise to the frequency range it is trying to attack. This will drown out frequency hopping and the frequency shift key will not have anywhere to hop. The amplifier helps to take advantage of the near far problem within direct sequence. As stated earlier, power is the key to this design. It will have the power to generate the signals over the given area. **[35][38]**

4.3.3.5 Process for Direct Sequence Spread Spectrum [32][33]

$s(t) = c(t)A(t)\cos[2\pi f_{ct} + \phi_c + \phi_{(t)}]$ equation 4.5

$A(t)$ and $\phi_{(t)}$ = informative functions

f c = carrier frequency

ϕ_c = carrier phase

$c(t)$= the spreading code

$c(t) = \pm 1$ $+1 \Rightarrow \theta^0$ phase

$-1 \Rightarrow \pm 180^0$ phase

$c(t)$ is the spreading code. It is a pseudo random waveform used to show that the structure of the wave form. Using this shows that the structure of the waveform comes from algebraic coding theory. ± 1 represents a square or rectangle wave. It is basically an inverter.

$X_j(t) = \Gamma_{jk}A(t)\cos[2\pi f_{ct} + \phi_{cj} + \phi_c]$ **Equation 4.6**

The receiver of a direct sequence receiver has the same Tx code as the transmitter.

This yields the algebraic expressions $Ave\{\Gamma_{jk}(t)\} \leq 1$
$Ave\{\Gamma_{jk}(t)\} \cong 0$

equation 4.6, equation 4.7

$k \neq j$ This can not get any larger than one. It can yield a negative number.

$-1 \leq \Gamma_{jk} \leq +1$

This process restores the original equation with a multiplied factor.

Next is another example of the process that has just been explained. This process uses the equation

y (*t*) =m (*t*) * c (*t*) **Equation 4.8 [35]**

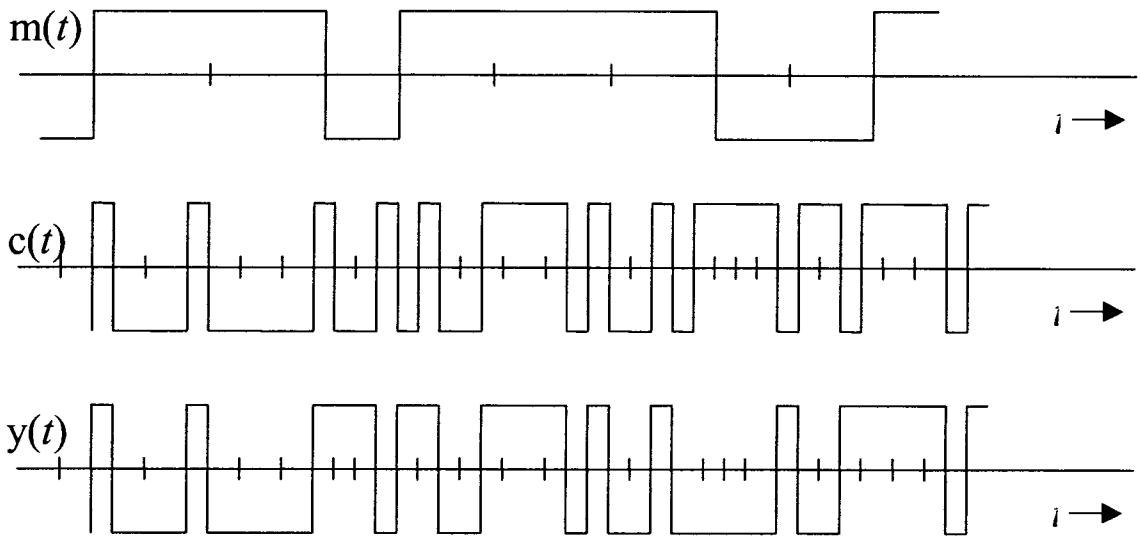


Figure 4.9 Wave forms direct sequence Spread Spectrum [35]

The diagram that shows the signals m(t), c(t), and y(t) states that c(t) is a factor between -1 and +1. The polar signal c(t) represents the binary sequence which is the pseudorandom carrier. This is multiplied by m(t). The equation representing this is below. The symbol m(t) represents the message signal. This is how the system is able to get the direct sequence signal, which is represented by y(t). The value of c(t) seems to be

unpredictable. But it can be generated by deterministic means. That is why it is called pseudorandom. **[35]**

The other part to this process is the receiver. At the receiver a synchronous version of the pseudorandom sequence c(t) used at the transmitter. The signal that is received y(t) is multiplied by c(t). After multiplying c(t) and y(t) they yield the desired m(t). This is how the message is recovered at the receiver. This is represented by the equation below.

$y(t)*c(t)=m(t)*c^{2}(t)=m(t)$ because $c^{2}(t)=1$ **equation 4.9, equation 4.10 [35]**

4.3.3.5.1 DSSS weaknesses that the jammer exploits within the zone

Direct sequence suffers from the near-far problem. It assumes that the signals from all users are received with the same signal power. This is far from true. The near-far-effect occurs during the dispreading process. The dispreading of a desired signal increases its strength N-fold compared to the residual noise level. This is because of unwanted signals. If unwanted signal strength is strong due to the proximity of its transmitter to the receiver, the strength of the desired signal is weak due to the remoteness of its transmitter from the receiver; the undesired signal will therefore drown out the desired signal. **[35]**

4.3.3.5.2 How the Jammer works against DSSS

In both direct sequence and frequency hopping, a pseudorandom number generator is used. In direct sequence the pseudorandom number generator is the value c(t). Recalling that c(t) is used to demodulate the signal. The design has two pseudorandom number generators. One is a high rate and one is a low rate. The process is rather simple. The two

pseudorandom number generators will have to produce different results. If the high rate pseudorandom number generator produces a 1, the low rate will produce a 0 or a -1. The goal is to produce conflicting results. By doing this the receiver of the attacker will try to de-modulate both signals and get confused by the jamming signal. This will cause the receiver within the zone to be unable to de-modulate a good signal. It is then being denied service, or jammed. With the algebraic theory representation this process will yield an answer larger then one. This causes the receiver of the attacking mobile device to be confused. This would deny it service within the Zone of Interference. **[38][32[33][35]**

4.3.3.6 Frequency Hopping Spread Spectrum

Frequency shift keying transmits either a 0 or a 1 by sending out sinusoid pulses. The frequency shift keying is used by frequency hopping. The frequency shift key is generated and is then shifted to another frequency. This is done by an amount determined by the pseudorandom number generator. At the receiver a frequency mixer with frequency controlled by an identical pseudorandom number generator code synchronized with the received signal shifts the frequencies back to the original frequency shift key frequency. The resulting frequency shift key is then demodulated. **[35]**

4.3.3.6.1 FHSS Weaknesses that the jammer exploits within the zone

Frequency hopping does not have the same resistance to jamming as direct sequence. Frequency hopping achieves jamming resistance by randomly hopping the frequency. This is how it avoids the jammer frequency. Because of this collisions do occur. Knowing this information, a jammer could simply jam the entire frequency range of a device. This would

give the device no frequency to hop to. For example, within 802.11, if an attacker jammed the 2.4 GHz frequency range, the frequency shift key would have nowhere to hop.

Knowing this, the jammer will send out identical waveforms to that of a frequency hopping spread spectrum system. The enemy's receiver will see two different signals within the Zone of Interference. This will cause the receiver to be confused and not work correctly. This is a backup method to cause denial of service within the Zone for frequency hopping spread spectrum. **[35]**

4.3.3.7 Jamming of rogue base stations

This thesis research on jamming concentrates on jamming of the mobile device. But it is known that an attacker could possibly try to set up a rogue base station to gather information. Even though this design discusses the use of directional antennas, signals can still bounce off of objects. Or persons could still try and access things too early. They might come in contact with the rogue base station that an attacker has set up. Laptop computers and other smaller device can be set up to act has a base station. This is not as much of a worry as an attacking mobile. But it is an issue that has been brought to light. Some methods are discussed within the appendix section for GSM for jamming base stations. The jamming techniques for jamming CDMA are quite similar to that of GSM. **[45]**

4.4 Position-location

4.4.1 Geographic Design

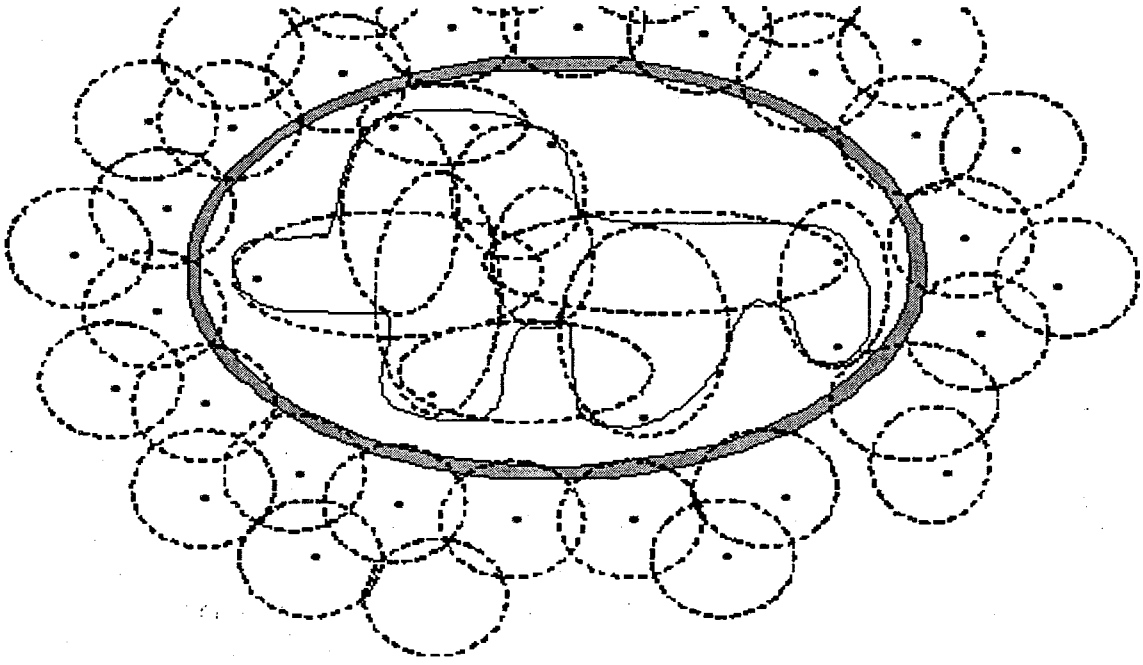


Figure 4.10 Geographic Design position location with Radiation Pattern inside secure zone figure done by Nichole Taylor and Sadhana Jackson

4.4.2 Antenna Design

The design of the antennas is very simple for this layer. The system uses directional antennas for this layer. This layer does not utilize adaptive antennas. The goal is to point the radiation towards the inside. Then the antennas will also point to each of the base stations on the inside. By doing this process should minimize bleeding of the radiation into the other layers of defense.

4.4.3 Information Processing

Design

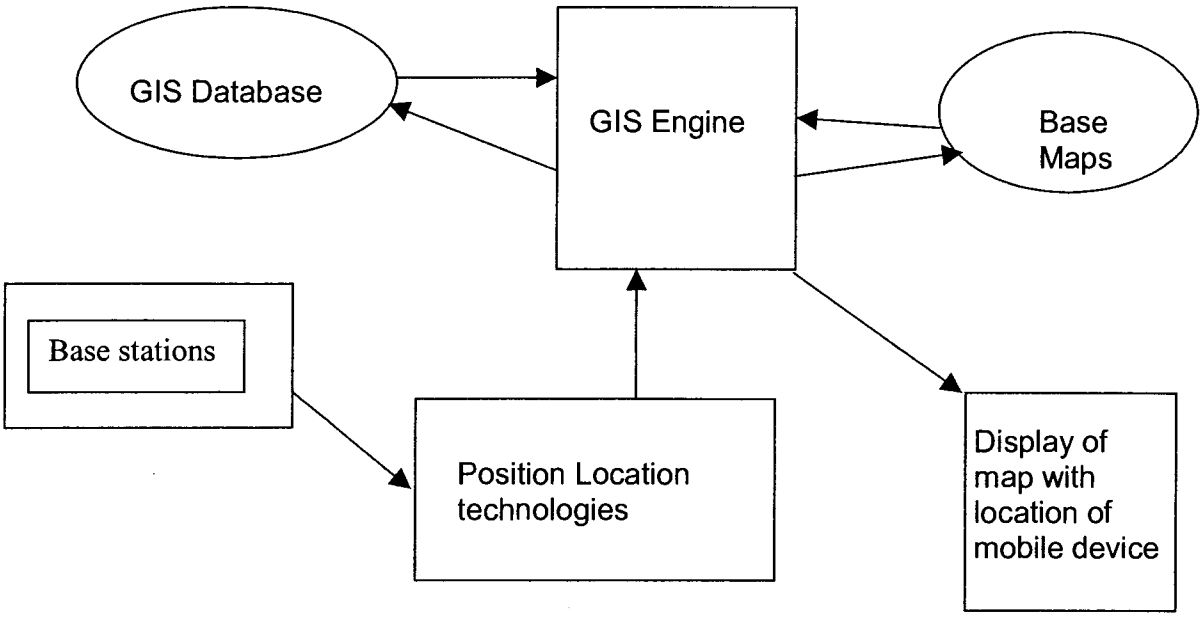


Figure 4.11 Information Processing Block Design inside position location System

The above diagram shows how the inside position locating and tracking will be done. First the base station or base stations will pick up the mobile device. Then the base station will send a signal to the position location. Then the position location will send a signal to the GIS engine, this in turns gathers information from the GIS database and the base maps. This information is then sent to the display of the map with the location of the device or devices.

4.4.4 Methods of the Position location system

involves the multi-path problem. Multi-path is described within appendix E, **Position location methods**. There will be many signals within the inside secure area. The problem of signal collision has therefore been addressed. [**32**]

4.5 Wireless Honeynet

4.5.1 Geographic Design

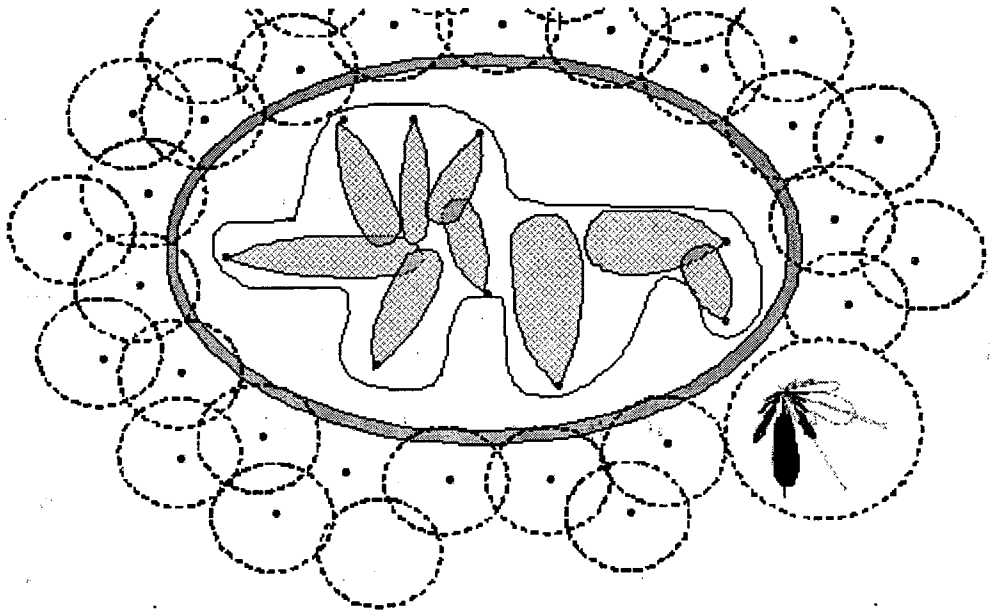
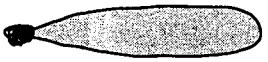


Figure 4.12 Geographic Design Honeynet Position location with radiation pattern. Done by Nichole Taylor and Sadhana Jackson

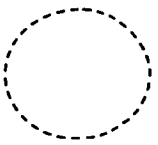
This is the radiation pattern of the Honeynet base stations. The dots surrounding the secure area represent the picture of the Honeynet base station.

Figure 4.13 radiation patterns of the Honeynet base stations



This pattern represents the radiation pattern for the directional antennas for communication in the secure area.

Figure 4.14 radiation pattern for directional antennas for secure area



The circles that surround the Honeynet stations represent the area that the position located will search in.

Figure 4.15 Honeynet stations

4.5.2 Design of the System

The systems design is performed in several stages. The reason for this is not only does the system need placement in a specific area, but the goal is to have it look just like a real wireless system. This is a key part. If the system does not look as if it is in use, this will let attackers know that it is only a decoy system. Once again the wireless Honeynet is the second line of defense for this defense-in-depth study. The following sections will go into further depth about design theories of the wireless Honeynet. A very important point to mention is this research does not go into new areas of designing a Honeynet. The point of this research is adapting the idea of Honeynet to the wireless world. **[32]**

The idea for this research is to have the Honeynet not connected to the real network. The Honeynet system will be total separated from the real wireless network. It is located at

the second layer of defense. This concept of Honeynet is not new, but the idea to have a total system independent of the real one is somewhat new. So this layer of defense it a total stand-alone system. **[32]**

This thesis will show methods of building a Honeynet system from the side of the hardware. The software is discussed, but great detail is not given. The detail given about the software is mentioned but no real detail. This thesis does talk about the integration of the two, yet concentrates on the hardware. **[32]**

4.5.3 Honeynet Deployment

Area of coverage and Placing of Honeynet Base stations

The diagram shows how to place the Honeynet stations. Depending on the geography the placement of the Honeynet stations might be slightly different. The reason for this is signals have a way of interacting with objects. So if the secure wireless facility is in a mountainous region, signals will bounce off the mountain ranges. This is an example of an area being covered. This thesis does not take into account the weather conditions and other environmental conditions that could change the RF signal propagation. The antenna type that will be used is an adaptive antenna, giving the signal more signal strength in the direction of the rogue mobile host. This thesis gives a general idea of signal propagation, when traveling through the air. **[33]**

The placing of the Honeynet stations will be very similar no matter what type arrangement the facility is. The diagram below shows how the stations are placed diagonal

from each other. This is done for a few reasons. Below is a list of goals that this setup will accomplish.

1. Allow position location to be done. Look at the section. Position location by Radiofrequency signal strength
2. Line of sight for RF signal to travel
3. Make this decoy network appear to be the real thing
4. Lure an attacker to the decoy network.

There is a buffer zone between the real network and the decoy network. There are a few reasons for this. Signals are able to bounce off objects. So even though the directional antennas are set up, the buffer zone is to minimize signal interference. The antennas that are in use will adapt to the mobile connecting to that base station. Knowing this the zone will make sure the Honeynet antennas will not have any attraction to the mobiles on the inside zone. This is the method this thesis proposes to keep the zones separate. The diagram below shows in detail the methods just described.

4.5.4 Antenna and Access Point Design

Antenna type

To obtain the desired effect, adaptive antennas are used. An Adaptive antenna is an antenna that controls its own pattern, by means of feedback control, while the antenna operates. Some adaptive Antennas also control their own frequency. Adaptive Antennas are ideal for various reasons. An attacker could come from many angles. So the idea is to use the Adaptive array to cover all angles that an attacker may approach from. A more complete

description of Adaptive Antennas is in the section on Adaptive Antennas and the appendix section Antennas. **[40]**

4.5.5 Network Design

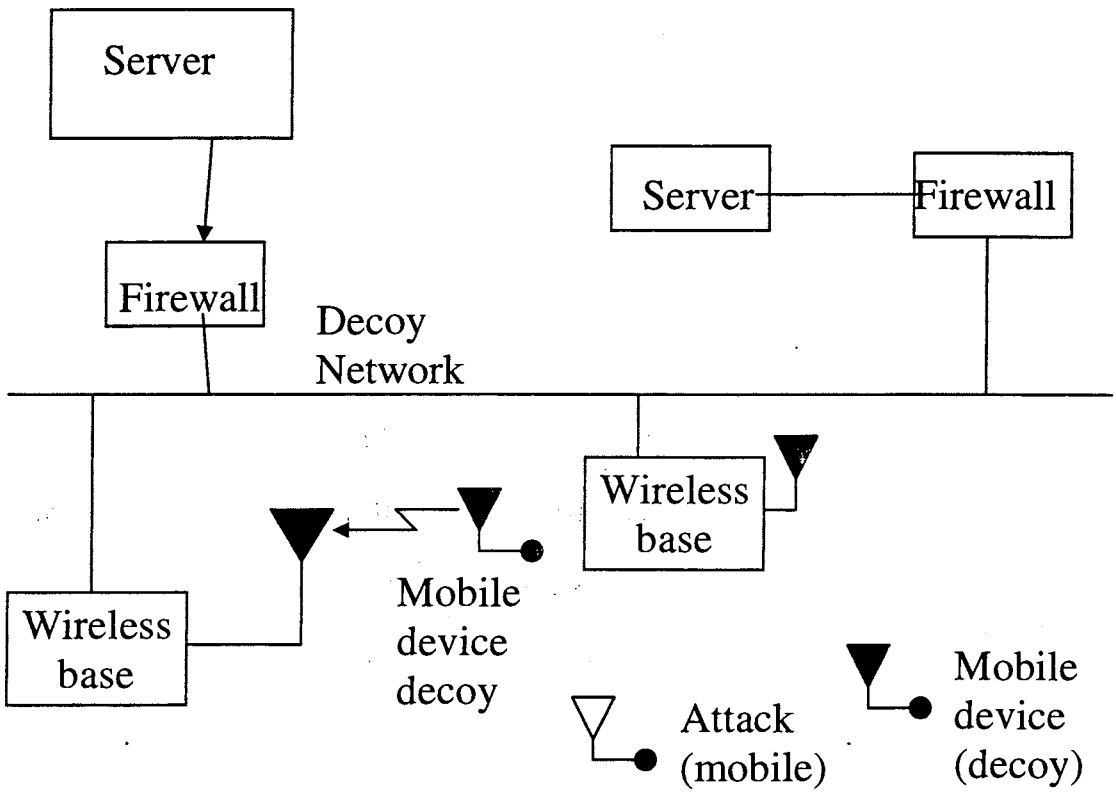


Figure 4.16 Honeynet Block Diagram [32] redone by Nichole Taylor and Sadhana Jackson

Figure 4.16 shows the network configuration design of the Honeynet layer. This zone is made up of stand-alone servers with wireless base stations and decoy mobile stations. The above block diagram shows the mobile decoys and the attacking mobile stations. The attacking mobile will see network traffic between mobiles and other parts of the wireless

system. In the following sections is the detail of the design of the protocols needed to make this decoy network spoof network traffic.

4.5.5.1 Server and the base station Design

The design of the servers and base stations are identical to real network servers. The base stations are connected to the firewalls and the firewalls are connected to the servers. This is the same type of set up real networks should have. This gives the attacker the idea of added protection to the wired network.

4.5.5.2 Spoofed Network Traffic

The network traffic will have to show the presence of a real network. The artificial intelligence to the design of the spoofed traffic will have real messages within the packets. The spoofed traffic will supply false and deceptive information. This process simulates a real network. This network is being designed for a Department of Defense system. So the traffic will to appear to give important information to an attacker. The only thing is the information is false. The data has a level of encryption. If the traffic did not have encryption an attacker would be able to realize that the network is a decoy. Then to decrypt the packets, the attacker will have to collect a given amount of packets being sent. **[32]**

4.5.5.3 Spoofed Mobiles devices

There are many things the decoy mobiles will do, in order to make an attacker believe that it is an authentic network. The mobile will have the same protocols as a real network. The mobiles will run the same protocols but not at the same time. For example while one

mobile is in beacon mode, another decoy mobile will be in transmit mode. The goal of this thesis is to start the process of designing the Honeynet system. This thesis lays out the groundwork that other students will use to design the software, which will drive the system.

The software design for the decoy mobiles will do many things. First the design will have an artificial intelligence to the design. The reason being is the mobile decoys will have to do protocols in a somewhat pseudo random order. Then the decoy mobiles will not keep the same order. This is to make sure an attacker will not see the same communications between the decoy mobiles and the base stations. Then while one decoy mobile is beaconing for a base station, another station will be in contention free mode. This is an example of what the software will do for the Honeynet system. As stated earlier this thesis only goes into the hardware design. **[32]**

4.5.4.4 Technical issues that have been fixed

This thesis is designed to fix the flaws that other wireless Honeynet systems have. A group in Texas has designed a wireless Honeynet system that utilizes **VMware**. They use **VMware** to try and produce the traffic. This is also used to make an attacker believe that there are multiple operating systems on their Honeynet system. Another research project that has been done is the Honeynet project. This is another group that has flaws within their system design. **[32]**

The way to break these systems is easy. An attacker who knows what they are doing follows steps when attacking a system. The biggest step that an attacker will perform is investigation of the target. After investigating either one of the mentioned systems, an attacker will be able to see that the network is a decoy. An attacker that knows what they are doing will monitor the traffic between the mobiles device and the base stations. The systems

mentioned above do not have spoofed traffic. So they do not portray the process of mobiles devices communicating with the base. Knowing this information, the design within this thesis uses the same protocols has real networks. The mobiles stations are stationary but they will still give the picture of a real network. **[32]**

One concern about Honeynet systems is attackers using the Honeynet to compromise other systems. Other systems are connected to real networks. This system is a complete stand-alone wireless network. The servers that are connected to the base stations are not connected to a network. Firewalls within the design are located between the base stations and the servers. This is to give the attacker the thought of a firewall in front of the wired network. The servers are completely stand-alone. This takes care of some issues. For example a network that this system is designed for would be a sensitive network. Knowing this, outbound traffic to base stations other then the Honeynet base stations will be disabled. This will make it more believable that the network is a real network for sensitive data. **[32]**

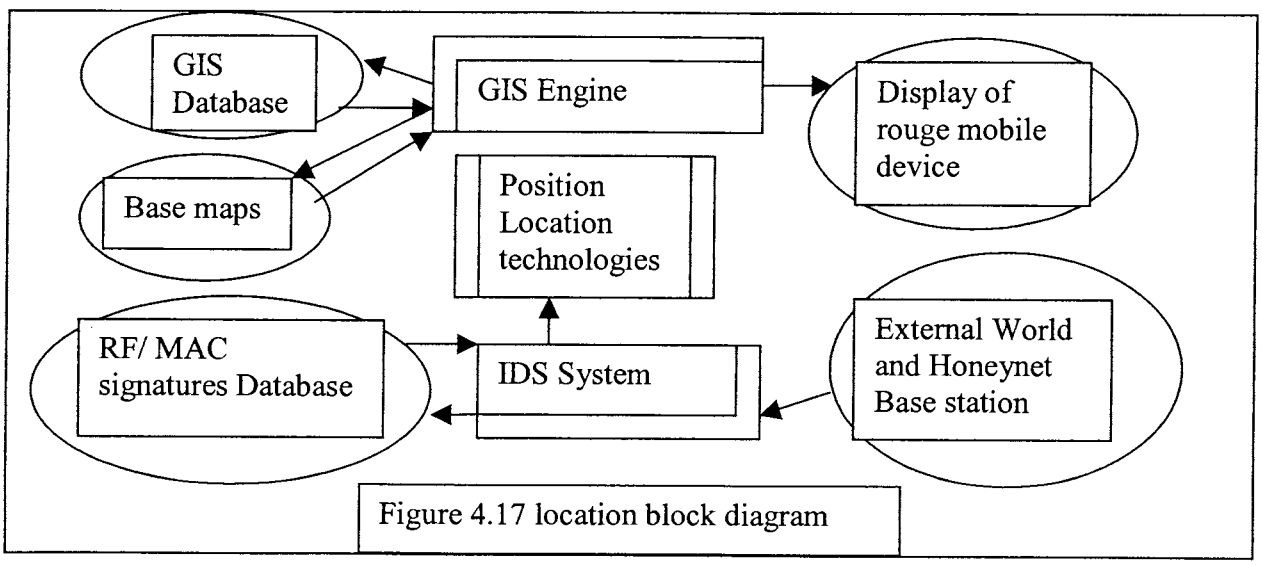


Figure 4.17 location block diagram

Figure 4.17 Honeynet position location block design redone by Sadhana Jackson

Figure 4.17 is the block diagram for the Honeynet system. The diagram shows how the Honeynet system is constructed. The Honeynet base station will get a signal from a mobile device. The Honeynet station triggers the intrusion detection system. The intrusion detection system checks the database of known RF signatures and MAC addresses. If a known RF signature and MAC Address can not be found in the database, it is then sent back to the intrusion detection system which red flags it for analysis. Then the intrusion detection system sends the signal to the position location. Then the position location will send the data to the GIS system. Then a known position will be determined. This is demonstrated in the diagram above. The next sections will discuss the designs of the separate parts of the above system.

4.5.4.5 Intrusion Detection System

This is the portion of the system that will monitor Probes, Association and Authentication request frames. The monitoring system will also detect network sniffing programs. These programs exist at the data link layer. The monitoring system will also record all incoming IP packets; it will produce alerts for well-known attacks. The monitoring system will be the part that performs data capture, data control and data collection.

Data Capture is the capturing of all of the attacker's activities. These activities are then analyzed to learn the tools and tactics used by attackers. The goal is to capture as much data as possible, without the attacker knowing their every action is captured. The goal is to capture data in layers. It cannot depend on a single layer for information.

The monitoring is connected to the Honeynet system. It is not part of the Honeynet system. The monitoring system will be the section that sets stations to track mode. This is how the position locating and tracking is done.

4.5.4.4 Identification- Friend or Foe

The system will have to tell friend from foe. This will be done in a couple of ways. The first is to use the Media Access Control (MAC) address. Each network interface card has its own MAC address. This is only one way of identifying friendly mobiles. The one problem with this method is MAC address cloning. This is the process of spoofing a known MAC address. The second method that the system will use to tell friend from foe is to look at the spectral characteristics of the network interface card. Each NIC gives off its own RF signature. The circuits within devices give off a different RF signal. Knowing this allows the system to keep a record of all signals from the authorized portable devices. This is the second method that will be used to tell who is an authorized user of the system and who is not. [32]

4.5.4.5 Position Location and Tracking Design

The wireless Honeynet is the second line of defense. This could also in some ways be considered the true first line of defense. The reason for this is it is not simply designed to keep an attacker busy by supplying false data. Once a host is picked up by the wireless Honeynet system, in most instances the system will identify them has an attacker. It is also known that a friendly might come in the zone. This is when the system will use one of the

two methods discussed earlier. As stated earlier, the monitoring system will trigger the position system to track the attacker. **[32][33]**

The above example shows the placement of the Honeynet base stations. The stations are placed in this manner, for two reasons. The system will use line of sight, to communicate between the base stations. By using this type of setup, an attacker will be fooled into believing that a real network is in use. The other reason is to enable use of the position location system. The position location works by reading the strength of the signal. This is then is relayed to the nearest Honeynet base stations. To get a more accurate position location, at least three base stations are needed. So by placing the Honeynet stations in this manner at least three stations will be able to get a reading of a signal. **[32][33]**

5. Conclusion

The defense that was discussed in this paper is not based on new concepts. The Honeynet is a well-known technique that has been in use by many security professionals for years. The idea of how the Honeynet system is used in this thesis is a new concept. The method involves using the concept of defense-in-depth.

The inner layer of security is also not a new concept. The way that it is being used is just has an added layer of security. The methods for the position tracing and location are methods that are currently used. This thesis utilizes multiple techniques to give a more robust system, allowing the system to overcome some of the issues that come with using a tracking and position location.

The Zone of Interference is set up to stop many problems that are associated with wireless networks. The first of these problems is intercepting wireless signals. Within the Zone the attackers will see what could be called radio blackness. The signals that they receive will be the jamming signals. The Zone will stop cell phones from be tracked, while powered on, in the area that is being secured. The cell phone will beacon while in the secure area. The signals from the base stations will not be able to be reached. This is another example of the near far problem that was discussed earlier. This is because the jamming signals are nearer to the attacking receivers.

This thesis has discussed these methods and putting them all to use should in theory give a secure area for wireless connectivity. Using the concept of defense-in-depth gives many ways to slow down an attacker. The idea is that nothing is fool proof. The goal is to slow the attacker down, or make the attacker frustrated enough because of the added security to just give up. The only fool proof method for securing a network is to not have one. This

is true for both wireless and wired, but that is not an option. So the best thing to do is to try and give the attacker many roadblocks to get them to not want to spend the time or money.

6. Future Work

The future work section includes a few details that would make a better system. Future work is needed, first of all, within the secure area. Currently the system tracks all mobile stations within the secure area. One upgrade of the system would be to put a wireless IDS system within the secure Zone. This IDS system would have attack patterns within a database. This would be a method to catch attackers right in the act. Then the system would track and perform a position locate on the attacker. The system would also know what type of an attack is happening. So follow up work on a design of the wireless IDS would be needed. This would allow the correct safety precautious to take place.

The next part for future work deals with the Honeynet system. This thesis describes how to design and setup the hardware. The software for the system needs to be designed. The current method of doing the software described by this thesis is very simple in design. The goal is to design software that would be considered complicated and robust. Then the Honeynet will be able to perform many of the ideas of fooling the attacker that is described in this thesis. One of the biggest parts of the future work of the software involves putting misleading data within the packets that are being sent between the fake mobiles and the base stations. The software would need to have many other features that a real network would have. For example, sometimes a network might have a lot of packets being sent. At other times, very little network traffic takes place. If there is constant traffic, an attacker might realize that they are receiving spoofed data. The system would then require one mobile device in beacon mode and another in CF poll, with another station sending data. Another mobile would then be necessary to receive information from a base station. These are future

things that need to be done with more advanced software. As stated earlier this thesis focuses on the hardware design.

The jammer design that is being utilized for the Zone of Interference wipes out the whole frequency range. Future work might involve using an intelligent jammer. The design of the jammer used by this thesis utilizes methods of fooling the incoming receivers but better methods are possible to create a more intelligent jammer. This would make it harder to determine if the signal is being jammed. This type of jamming would also help reduce the amount of power that is needed by the current design within this thesis.

Appendix-A IS-95 CDMA

Code Division Multiple Access Channel Structure

The channels in IS-95 are really channel pairs, the forward channel and the reverse channels. A channel pair constitutes a CDMA channel. The forward channels carry voice and signaling messages from the base to the mobiles. The reverse channels carry the voice traffic and signaling messages from mobile to the base. The coverage area, like in other cellular systems, is modeled by closely packed hexagonal cells. Each cell may have more than one CDMA channel separated by FDMA channels and each CDMA channel in IS-95 supports a maximum of 64 users [47]

Forward Channels

The Pilot Channel is broadcast by base station all the times. The synchronization channel is used to synchronize the clocks of the various mobiles with the base station. A mobile synchronizes to the synchronization channel every time it powers up because high-precision timing is needed. [47]

The base station uses paging channels to communicate with the mobile device when it is not making or receiving a call. The mobile gets informed of its incoming call through the paging channel. The base station sends the information about the channel assignment of the forward and reverse traffic channels to the mobile device through the paging channel. The Forward and Reverse traffic channels carry the actual voice during a call. The digital voice

data in the traffic channels is Time Division Multiplexed into signaling packets during the call. **[56]**

There are a total of 64 forward channels (base to mobile) that allow 64 users to share the same spectrum of 1.23 MHz. The good cross correlation properties of Orthogonal Walsh codes keep these channels from interfering. Traffic channel "1" functions as a pilot channel for all mobiles and the 32^{nd} channel functions as a synchronization source. The paging channel accounts for a third forward channel. The forward traffic channels use the remaining 61 channels to carry traffic. **[47]**

The pilot channel is an un-modulated carrier. It is spread by a factor of 64 using Walsh code 1 (of 64). In addition to this, each base station has a 15-bit PN code (PN short code) that is unique from its neighbors and keeps the pilot signals of neighboring base stations from interfering at the mobile. The synchronizing channel is a low bit rate channel carrying clock information. It is spread by a factor of 64 using the Walsh code 32 (of 64). It is also byte interleaved, symbol-repeated and scrambled using a 42-bit PN-long code. Paging channels are modulated in a similar way, except the bit rate of the paging channels are higher than the synchronization channel. **[47]**

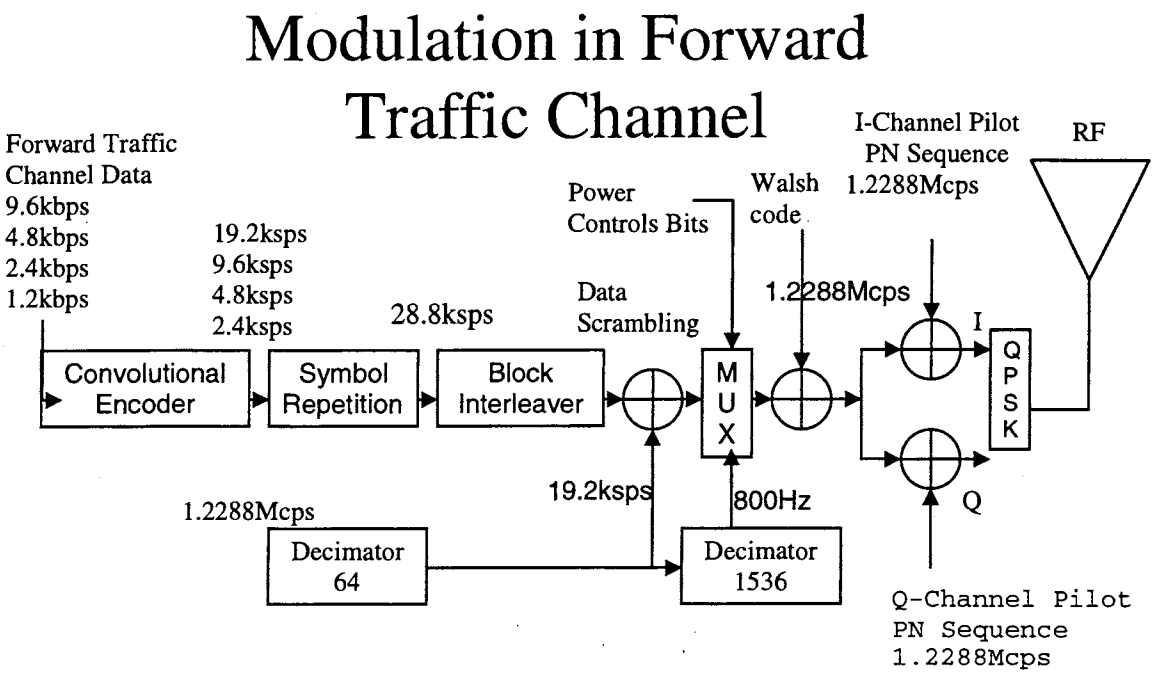


Figure A.18 Modulation in Forward Traffic Channel [47] redone by Nichole Taylor and Sadhana Jackson

The variable rate coded symbols are repeated to give a constant bit rate of 19.2Kbps. The symbols are block-interleaved to prevent burst errors due to fast fading. The PN long code is used to scramble the data to randomize replicas resulting from symbol repetition. The power control bits are multiplexed and the resulting low bit rate data is spread by a factor of 64 using the Walsh code. The spread spectrum signal has a chip rate of 1.288Mcps. In-phase (I) and Quadrature-phase (Q) PN short codes are used to separate this spread-spectrum signal from the traffic due to neighboring cells. **[47]**

The mobile uses access channels to communicate with the base station when not in a call. The signaling messages include registration at the power up, or idle handoffs. There are 32 access channels available for the mobile station in a cell. These channels share the

same spectral band; they are separated using the PN-long codes. The mobile knows the PN-long codes assigned to each of these channels. An access channel can be used by only one mobile at a time. **[47]**

The reverse traffic channels are used to carry voice and signaling messages traffic from mobile to base. Reverse channels use the same spectral frequency as the access channels. These channels are separated by PN long codes to keep the users within a cell from interfering. The PN long codes are randomly allocated at the beginning of the call unlike the pre-assigned PN codes for the access channels. There can be a maximum of 61 Forward channels and this limits the number of users in a CDMA channel. **[47]**

The modulation of access channels and reverse traffic channels is very similar. The only difference is that access channels carry slightly different bit rate. The figure below shows the modulation of reverse traffic channels.

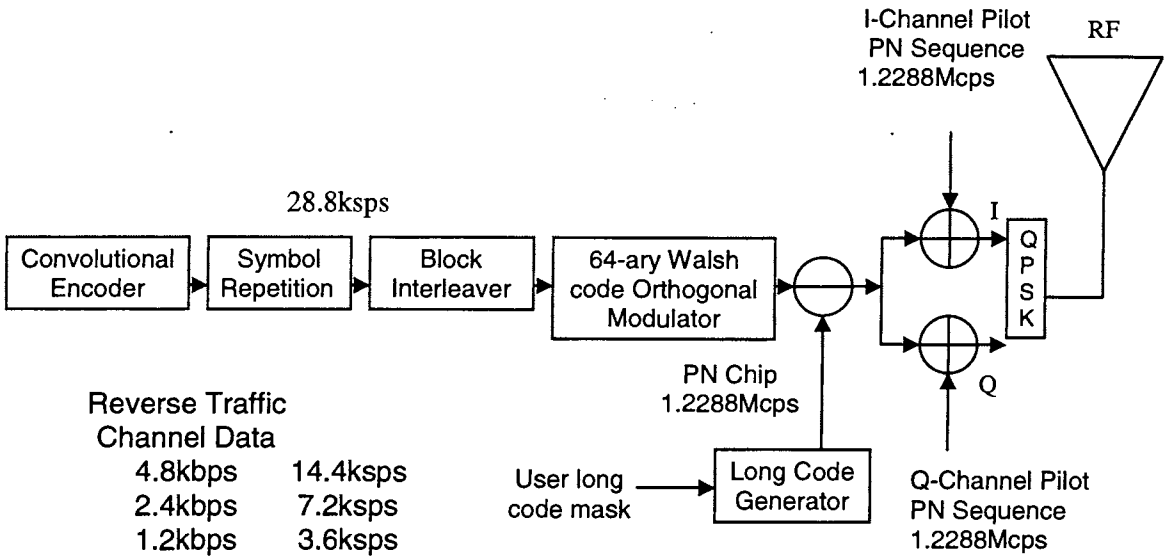


Figure A.19 Modulation in Reverse traffic Channel [47 redone by Nichole Taylor and Sadhana Jackson

Appendix-B GSM

In the GSM network, the base station subsystem (BSS) takes care of the radio resources. The BSS has the Base Transceiver Station (BTS), the actual RF transceiver, and the Base Station Controller (BSC), which is in charge of mobility management and signaling on the Air-interface between the mobile. The GSM air-interface uses a combination of two different multiplexing schemes: 1) TDMA (Time Division Multiple Access) and 2) FDMA (Frequency Division Multiple Access). The spectrum is divided into 200 kHz channels and each channel is divided into 8 timeslots. Each of the 8 timeslot frames has duration of 4, 6 ms. The GSM transmission frequencies are presented in the table B.3. **[45]**

Table B. 3 Downlink Uplink [45] redone by Sadhana Jackson

	Downlink Uplink
GSM analog **GSM digital**	**935-960 MHz 8900-915 MHz** **1710-1785MHz 1805-1880 MHz**

The timeslots are called physical channels. A physical channel is full duplex and several logical channels are able to share it. GSM has several different logical channel types. GSM system has control channels. When a mobile enters a network, it first looks for a beacon of the nearby Base station by scanning all channels. All base stations transmit their beacons at a fixed frequency and power level. The mobile finds the beacon by searching the frequency with the highest signal level for a timeslot with a sequence of "00000..." - a sine wave - which is transmitted on the Frequency Correction Channel (FCCH). FCCH is one logical channel in the physical channel called the Broadcast Control Channel (BCCH) and it is used for bit synchronization. BCCH is on the 0-timeslot of the beacon frequency. After the

mobile achieves bit synchronization, it finds the Synchronization Channel (SCH) from the BCCH physical channel. The mobile can then find the logical channel BCCH. The logical channel BCCH transmits important BTS information such as the frequency hopping sequences. [45]

There are three downlink control channels FCCH, SCH and BCCH, along with three call control logical channels located in the physical channel BCCH. The Paging Channel (PCH) is used when the network wants to contact a mobile. The mobile monitors all PCH channels on the BCCH-frequency. When the mobile is turned on, the network knows where the mobile is. The location may consist of several cells. Then the mobile is paged in all cells in the area. The mobile recognizes the page through the use of an identity number in the paging sequence. When the mobile wants to request service from the network or replying to a page, it sends a service request on the Random Access Channel (RACH). The network replies to a request from a mobile on the Access Grant Channel (AGCH). Table B.4 presents logical control channels that are located on the physical BCCH channel. **[45]**

Table B.4 GSM Control Channels [45] redone by Sadhana Jackson

Downlink	1. Frequency Correction Channel (FCCH)
	2. Synchronization Channel (SCH)
	3. Broadcast Control Channel (BCCH)
	4. Paging Channel (PCH)
	5. Access Grant Channel (AGCH)
Uplink	6. Random access channel (RACH)

The mobile measures the Signal-to-Noise ratio of cells from BCCH. The location updates are then performed according to these measurement results. The mobile keeps a list of the best BCCH frequencies according to the selection criteria used by the operator. In a multi-frequency cell, only one frequency is required to have the BCCH on its 0-timeslot. During a call, the mobile transmits and receives on its own Traffic Channel a burst in only one of the eight timeslots. During the other timeslots, the mobile monitors the BCCH levels and information on the neighboring cells. The GSM system uses slow Frequency Hopping (FH), meaning the frequency changes after each burst, or every 4.6 ms. **[45]**

All physical channels, except the 0-timeslot of BCCH-channel can hop. A 6-bit Hopping Sequence is transmitted on BCCH and both the mobile and BTS have a frequency list indicating to which frequencies and in which order to hop. The uplink hopping follows the downlink hopping with a fixed delay. Power control is optional for the BTS, and BCCH must use a constant power level due to the specific measurements carried out by the mobiles. Power control is triggered by the field strength and reception quality measurements. If the measurement average from a 480 ms period is not within the limits, the output power in the other end of the connection is altered accordingly. The base controls the power of the mobile. The GSM maximum transmitting powers are presented in table B.5. **[45]**

Table B.5 GSM dBm Max and Min [45] redone by Sadhana Jackson

	Max	Min
GSM 900		
Mobile	39 dBm	5 dBm
BTS	58 dBm	9 dBm
DCS 1800		
Mobile	30 dBm	0 dBm
BTS	46 dBm	17 dBm

Jamming of the GSM System

In GSM is frequency hopping is used for the reduction of fast fading caused by the movement of the mobile devices. The hopping sequence can use up to 64 different frequencies. Compared to military FH systems designed for avoiding eavesdropping and jamming GSM uses a very small number. The jammer is able listen to Broadcast Control Channel and derives the hopping sequence in advance. The speed of GSM hopping is just over 200 hops per second. This can be followed by a follow-on jammer. GSM frequency hopping provides no real protection against jamming attacks because its jamming margin is so low. **[45]**

The GSM system is designed to handle sudden drop-outs in Traffic Channel (TCH) connections. These drop-outs are normally caused by obstacles such as bridges, buildings, and tunnels. A connection can also be lost if the user detaches the mobile's power source while the mobile is connected to the base station. In jamming situations, call re-establishment is the method the network will use. This is to re-initiate the jammed Traffic Channel. When the connection is dropped, a timer initiates ticking in the Mobile service switching center (MSC). If a new connection has not been established when the timer has reached its maximum time (a system operator setting) the connection is completely lost. **[45]**

The GSM channel architecture shows that the downlink Control Channels (FCCH, SCH and BCCH) should be targeted. These channels are recognizable because they use a constant power output. By jamming the synchronization of the information, it is possible to prevent the mobile device from detecting a valid GSM network. The GSM system has a feature that makes jamming easier to an attacker. The system will give feedback to the jammer. The feedback is about the jamming efficiency. Increasing all of the power agile channels power levels. This is done when jamming is successful. **[45]**

Jamming efficiency for the GSM

In order to jam a GSM system, the needed jam to signal ratio is -5 dB. The jammer will concentrate on attacking the uplink. Because a majority of BTS units are located in places with higher elevation, uplink jamming is a very good jamming method against GSM. **[45]**

The connections that are in progress can be halted by jamming the Traffic Channel. They use the connection and the Random Access Channels of all other cells in the area. This will prevent the system from re-initiating the connection by going through another base station. This jamming must be sustained until the network ends, the attempt, by the mobile to re-establish the connection. This says that the channels have to be jammed for a few seconds. This guarantees that the connection should be lost. **[45]**

Appendix-C IEEE 802.11b

Table C.1 Key Characteristics of 802.11

Physical Layer Direct Sequence Spread Spectrum (DSSS), Frequency Hopping
Spread Spectrum (FHSS)
Frequency Bands 2.4GHz (ISM band) and 5GHz
Hop rate 1Mbps, 2Mbps, 5.5Mbps, 11Mbps (11b), 54Mbps (11a), 54Mbps (11g)
Wired Equivalent Privacy (WEP) RC4-based stream encryption algorithm for confidentiality, authentication and integrity. Limited key management
Operating Range About 100 feet indoors to over 1500 feet outdoors
Positive Aspects Ethernet speeds without wires; many different products from many different companies. Wireless client cards and access point costs are decreasing
Negative Aspects Poor security in native mode; throughput decrease with distance and load.

[39]

Table C.2 IEEE 802.11 channels with frequencies

Channel	Frequency (GHz)
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462

[39]

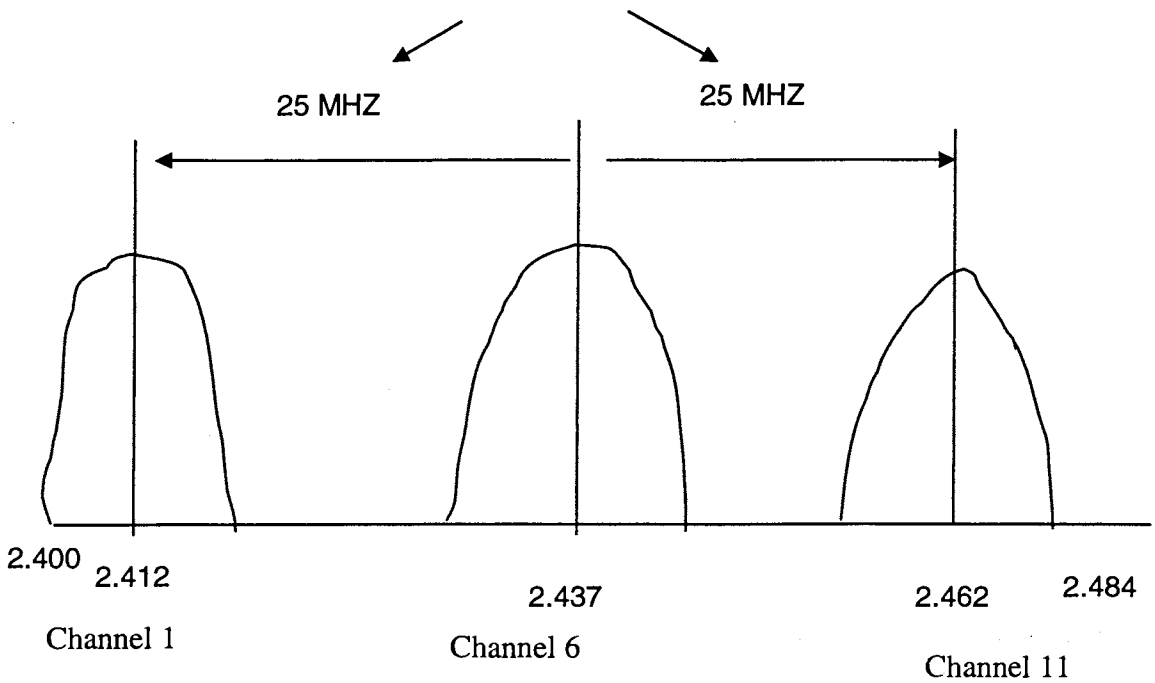


Figure C.2 Minimum Channel Spacing between center frequencies 802.11 [39]

Methods of Security for IEEE 802.11

Wired Equivalent Privacy Protocol (WEP)

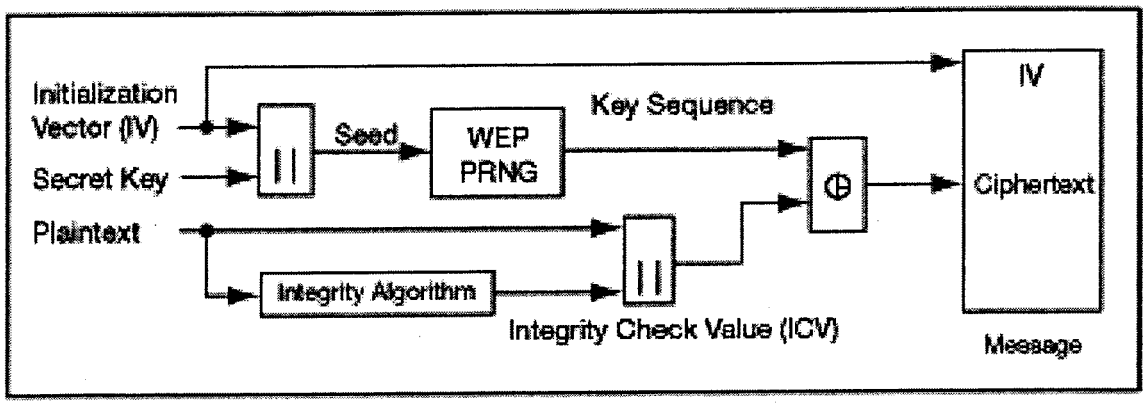
WEP is a security protocol used in wireless local area networks (WLANS) defined in the 802.11 standard. WEP was envisioned to give the same level of security as local area networks (LAN). LANs are inherently more secure than WLANS because LANs are protected by their physical structure, having some or all part of the network inside a building that can be protected from unauthorized access. WLANS are implemented over radio waves. They do not have the same physical structure and are more vulnerable to tampering. WEP provides security by encrypting data over radio waves, protecting the data during

transmission. The WEP protocol attempts to focus on three areas of security of WLANS. One of the biggest areas involves protection of the confidentiality of data. The physical layer of wireless networks is large; the possibility of an unauthorized person intercepting data is much greater. Access control is the second area. This is the process of protecting access to a wireless network. WEP includes a checksum field, to protect the data from being tampered with. **[64]**

Encryption methods used by Wired Equivalent Privacy (WEP)

WEP uses a secret key that is shared between the areas that are communicating, to protect the transmission of the frame of data being sent. This means that the same key is used to encrypt and decrypt the data. The plaintext goes through two processes, one process encrypts, and the other process attempts to protect against changes in the data from unauthorized persons. **[16][7][1][19]**

WEP will first compute the integrity check vector (ICV) by doing a redundancy of the frame, and then it appends the vector to the original frame. The result is in the original data. The RC4 algorithm is used is used to encrypt ICV and the message. The RC4 uses a 40-bit secret key and a 24-bit initialization vector. Then an exclusive XOR operation is done to make to produce the cipher text. Then the cipher text gets sent through the radio transmission link. The diagram below shows an example of how the WEP encryption algorithm works.



C.20 WEP encryption algorithm diagram [6]

WEP Decryption Methods

In the decryption process the initialization vector gets used to key the session used to generate the key sequence to decrypt the incoming message. When the proper key gets put together with the cipher text, the original data is back along with the integrity check vector. The decryption is verified doing the integrity check algorithm on the recovered data and comparing it the output integrity check vector to the integrity check vector transmitted data. If they are not equal it is an error. Then a message is sent saying that it could not be authenticated. **[16][7][1][19]**

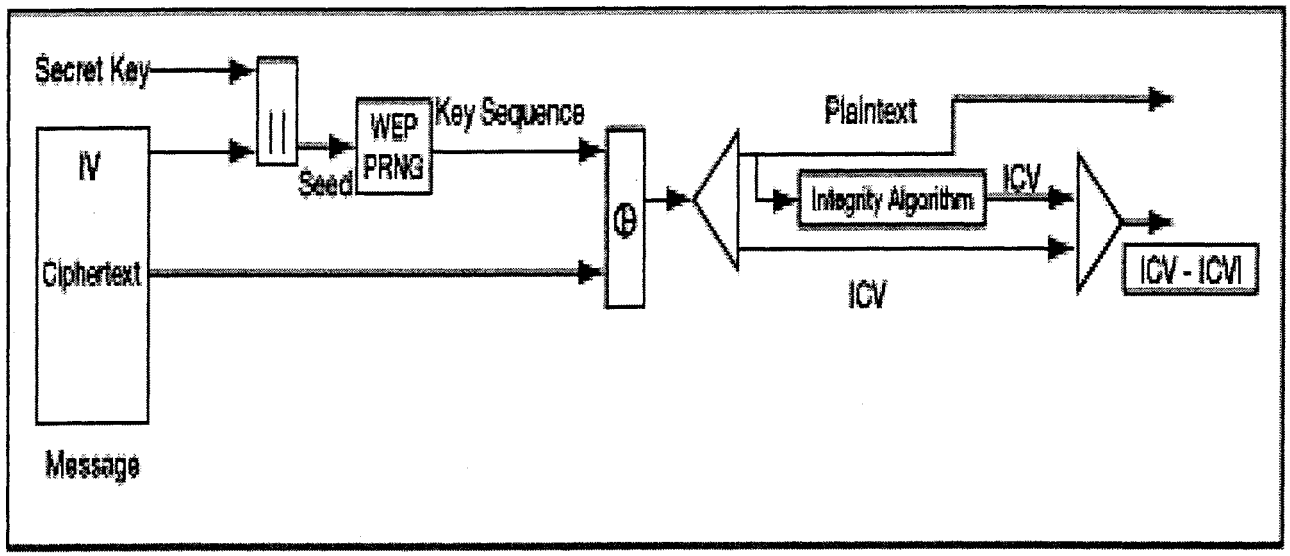


Figure C.21 WEP decryption algorithm diagram [6]

Methods of Authentication for WEP

The data gets encrypted and decrypted with the same key. Some access points do use WEP alone without using a shared key authentication. When WEP is utilized in this way it is used for an encryption engine only. The method just described is implemented utilizing a type of authentication. There are two types of authentication used in the IEEE 802.11b. There are the Open systems authentication and the Shared key authentication. **[16][7][19]**

Open Systems Authentication

[9][7][19]

Open systems authentication is the default authentication protocol authentication. Open systems authentication authenticates anyone who request authentication. It provides a NULL authentication process. This method of authentication is used when the administrator is not concerned with security. The method sends data in clear text.

Shared key Authentication

[16][7][1][19]

This method of authentication uses the response and challenge response with a shared secret key to give the authentication. To talk, the initiator sends an authentication request management frame. This says they wish to share to use the shared key. The receipt of the authentication request responds by sending an authentication management frame containing the challenge to the initiator. The challenge is made by using the pseudo- random number generator (PRNG) with the shared secret and the random initialized vector (IV)^2. When the initiator receives the management frame, they copy the contents of the challenge into a new management frame. Then it gets encrypted with the secret key with the new IV that is selected by the initiator. Then the encrypted frame is sent to the responder. The responder decrypts the frame and verifies the CRC integrity check value is correct. Then the challenge text is matched against the original data. If they do match authentication was successful. Below is a diagram of the action that takes place during this process.

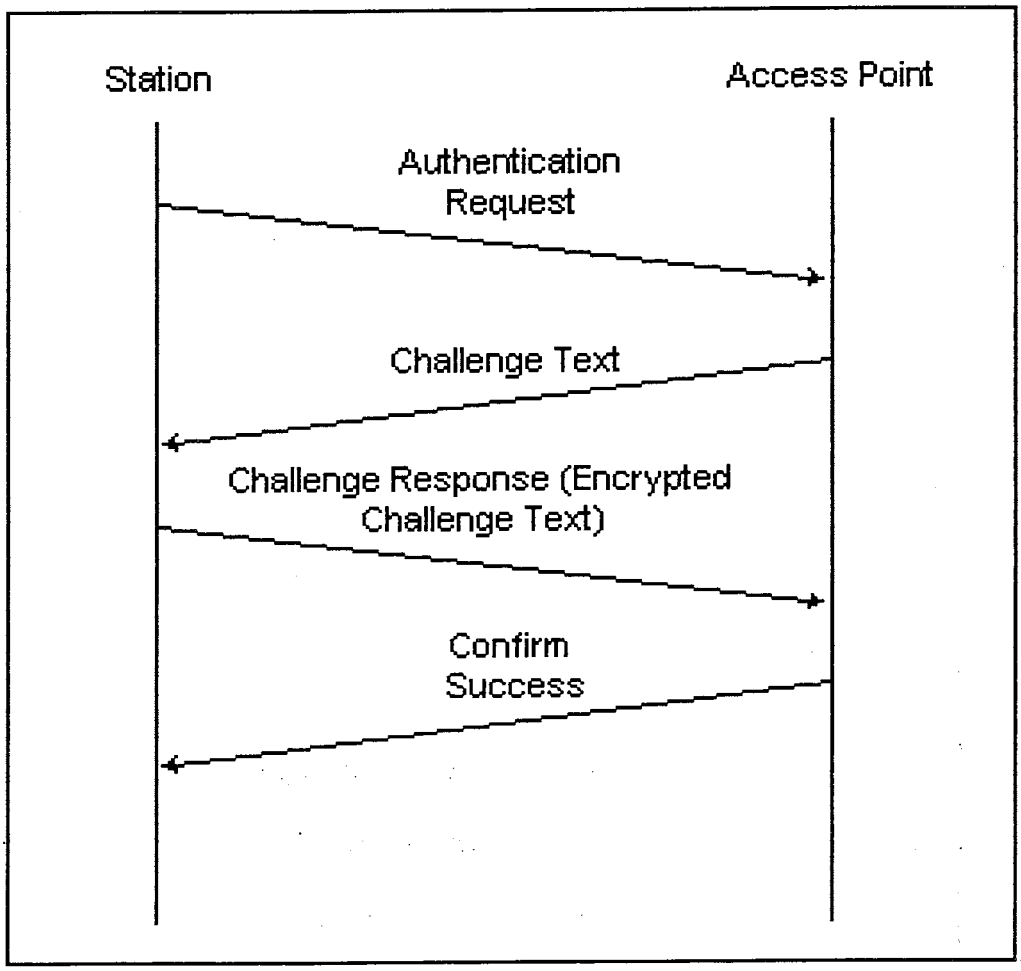


Figure C.22 WEP Authentication Diagram [6]

WEP can be used with 40-bit key and 24-bit IV. The shorter key length can be much easier to comprise, even if the attacker uses modest computing resources. A large key of 128-bit keys would make some attacks near impossible. This is even if the attacker uses sophisticated computers.

MAC Address Filtering

The Media Access Control address is a hardware address that identifies each node of a network. It is a 12 digit hexadecimal In IEEE 802 networks, the Data Link Control (DLC) layer of the OSI Reference Model is divided into two sub-layers: the Logical Link Control (LLC) layer and the Media Access Control (MAC) layer. The MAC layer interfaces directly with the network media.

The idea behind MAC address filtering is to limit access to the AP. This is done by creating a list of the MAC address of the wireless network interfaces cards of the users on the network. Mobile users whose wireless network interface cards do not match one from the list associated with the access point, will not be allowed to associate with the AP. [66]

Internet Protocol Address Filtering

Access points allow a user to set up a form of security, which will reject IP address. This is done when a block of IP addresses are specified to work with the AP. If an IP address is not on the list of addresses associated with that AP, the access point will not let the mobile host associate to it. [66]

Direct Sequence Spread Spectrum

This is the most known method of spread spectrum technology, it is also know called Pseudo-noise Spread spectrum (PNSS). This method is when the signal gets spread out at the base band. The spread signal is modulated. The modulation is apart from the spreading

operation. Once the receiver gets the signal it performs operations on it. The operations are done to recover the data. **[3]** The process is shown in the diagram below.

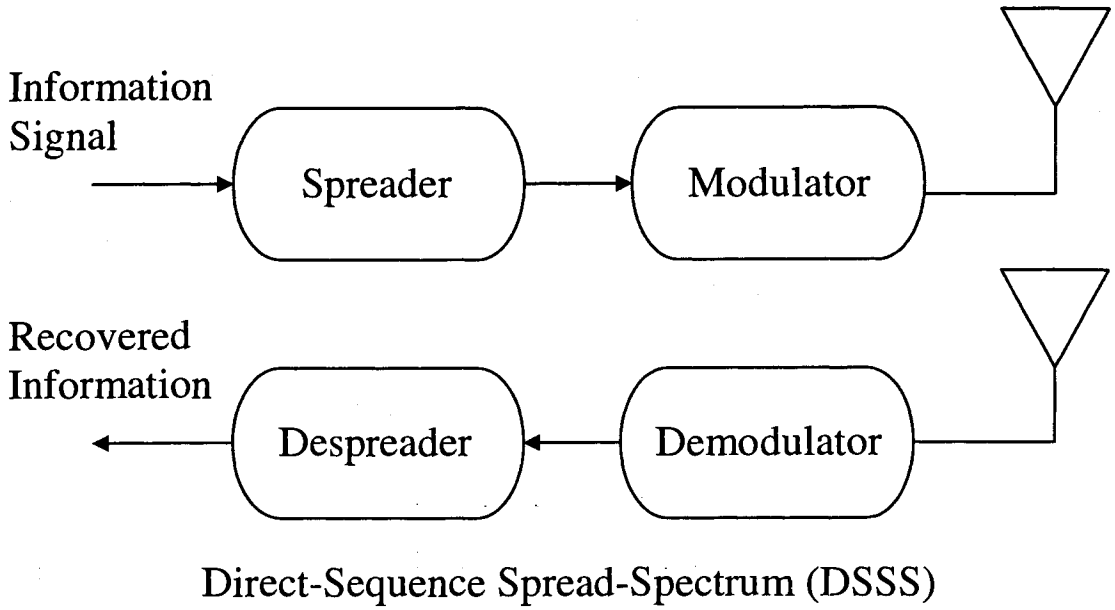


Figure C.23 Block Diagram of a simple DSSS system [3] redone by Nichole Taylor

Figure C.23 shows an arrow for the information going into the spreader. This is when the information is spread below the base line. Then the signal is modulated. Then the information is received and demodulated. From there the information is sent to the Despreader. Then the information is recovered. **[3]**

Direct sequence is able to resist jamming and Interference. The processing gain (PG) is the ratio of the signal bandwidth to the message bandwidth. The process gain is the presence of Interference.

In direct sequence systems the codes length is the same as the spreading factor giving the equation:

(G)p(DS)=(N)ds **Equation C.11 [3]**

The spreading codes are designed so the chip amplitudes are independent. The period of the PN sequence has N time chips. (N)ds=2^n-1 equation C.12 N is the number of stages in the code generator.[3]

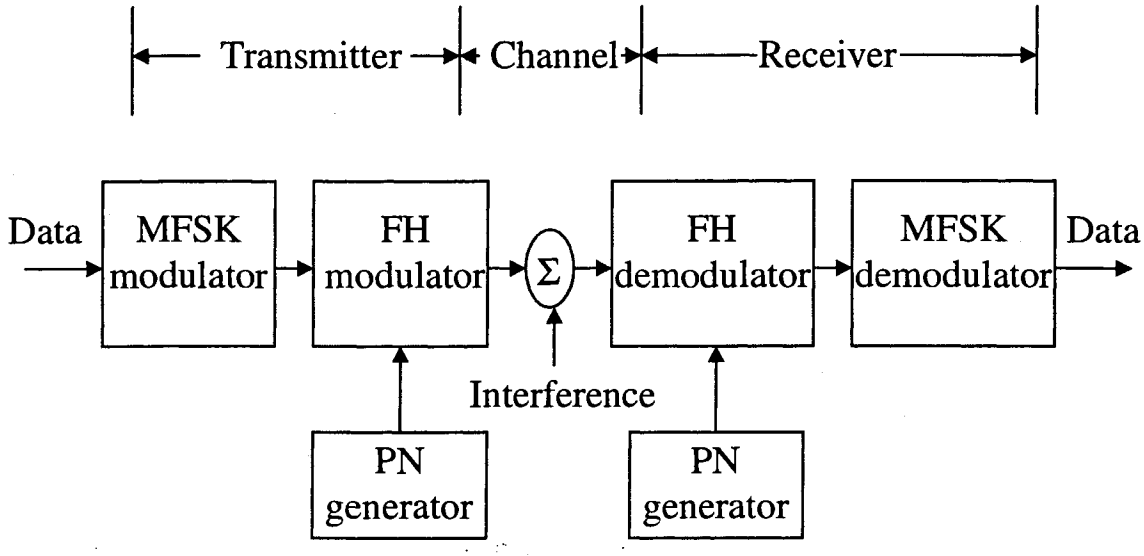
Pseudo-Random Noise (PN) Sequences

The PN sequence used for DS-spreading is N symbols long. These symbols are called chips in the time domain and have only two amplitude values: ± 1. The PN sequence is multiplied by the base band data sequence to produce the BPSK modulation function that will be used to modulate the transmitter. [3]

When properly chosen, the suite of PN sequences chosen for a given communication system design will have acceptably low cross-correlation values and thus allow the separation of all transmitted signals at the receiver correlator. The receiver correlator also spreads the jammer signal, thus turning it into equivalent noise and making it difficult to jam the intended signal. The spreading can also hide the signal in the ambient noise. [3]

Frequency Hopping spread spectrum

Frequency Hopping spread spectrum systems are usually used with M-ary Frequency Shift Keying (MFSK) [this is a common method but they can use any technique]. The digital binary data is input into an MFSK modulator. The output of the MFSK modulator is then put into an FH modulator. The FH modulator mixes the data signal with a carrier sinusoid, whose frequency is dependent upon the PN generator. The carrier frequency is hopped over the bandwidth. Then the signal is transmitted through a channel.



[48]

Figure C.24 Frequency Hopping spread spectrum Diagram [57] redone by Nichole Taylor and Sadhana Jackson

The bandwidth of a FH system, over a number of frequency hops or chips, is equal to the bandwidth of the frequency hopper. For example, the FH modulator has a bandwidth of 100 MHz, and then the bandwidth of the entire system is 100 MHz. The bandwidth of a single chip is equal to the bandwidth of the MFSK modulator.

Diversity

Frequency Hopping spread spectrum systems feature robustness. A signal has the ability to overcome channel shortcomings. One method of surmounting the inadequacies of a channel is by diversity transmission. In FH/MFSK systems, diversity means the transmission of a single tone several times over several different carrier frequencies. By sending the same piece of data multiple times at different frequencies, the probability of successful reception increases. **[48]**

Fast Hopping vs. Slow Hopping

An FH system is divided into one of two classes – fast-frequency hopping (FFH) or slow-frequency hopping (SFH). FFH is systems in which the carrier frequency is hopped several times per modulation symbol. The chip size in a FFH system is the time duration of the single frequency hop. SFH, are systems in which the carrier frequency remains unchanged for several of modulation symbols. The chip size of an SFH system is the time duration of a single modulation symbol. **[48]**

Known Security Risks for IEEE 802.11b

Denial of service (Jamming)

Jamming is simply providing RF energy to block reception of the signals. Jamming takes advantage of the near-far-effect. "The example is according to a CNN special report". An example of this is when Iraq set up GPS jammer during Gulf war two. The GPS satellites would beam the data down to the GPS receivers and this is how the personal on the ground would get the GPS data. Iraq set up jammers to block these signals from being received. This was done because the signals that the jammer was sending were near the devices that

were trying to receive the signals. To over come this, military beamed the signals from the GPS satellites to drone that were flying around the Iraq skies. This made the signals strong enough to overcome the signals that the jammers the Iraqis were sending out. **[32]**

Insertion Attacks

Insertion attacks occur when crackers deploy unauthorized devices in an effort to be recognized by an existing network. For instance, a cracker could set up shop outside an access point, armed with a notebook computer or PDA and Wireless Network cards. Because of the required devices' portability, it's simple enough to accomplish these attacks while parked in a car outside a business or home. The access point may or may not be configured for password authentication. **[28]**

Interception and Monitoring of Wireless Traffic

The attacker needs to be within range of an access point (approximately 300 feet for 802.11b) for this attack to work. All a wireless intruder needs is access to the network data stream. Second, access points transmit their signals in approximately a circular pattern, which means that the 802.11b signal almost always extends beyond the physical boundaries of the work area it is intended to cover. This signal can be intercepted outside buildings, or even through floors in buildings. **[28]**

Access Point Clone Traffic Interception

The attacker fools a legitimate wireless client into connecting to the attacker's spoofed access point. This is done by placing an unauthorized access point with a stronger signal in close proximity to wireless clients. **[28]**

3.6.5 Denial of Service (Flooding)

Flooding attacks can be easily done to wireless networks. This is when legitimate traffic cannot reach the clients or the access point because illegitimate traffic.
This creates a denial of service attack. The action that has just been described overwhelms the frequencies. An attacker with the proper equipment can easily flood the 2.4 GHz frequency band. It corrupts the signal until the wireless network ceases to function. Cordless phones, baby monitors and other devices that operate on the 2.4 GHz band can disrupt a wireless network because they use this same frequency band. **[32]**

Appendix-D Antenna Theory

Directional antennas, such as the Yagi, are good for directing the radiation pattern of a radio transmitter to a given direction and area. A Yagi Consist of one element that is driven. The remainder of the elements is passive and is driven parasitically. The spacing of the elements is such that the phases of the driven element and that of the reradiated waves add properly off the end of the array. **[61]**

Table D.6 Summary of typical characteristics of Yagi antennas	
Typical Half-Power Beamwidth:	**50degX 50 deg**
Typical gain:	**5 to 15 dB**
Bandwidth:	**5% cr 1.05:1**

[61]

Table D.7 Frequency limit:	
Lower:	**50 MHZ**
Upper:	**2 GHZ**

[61]

Characteristics of a Yagi Antenna

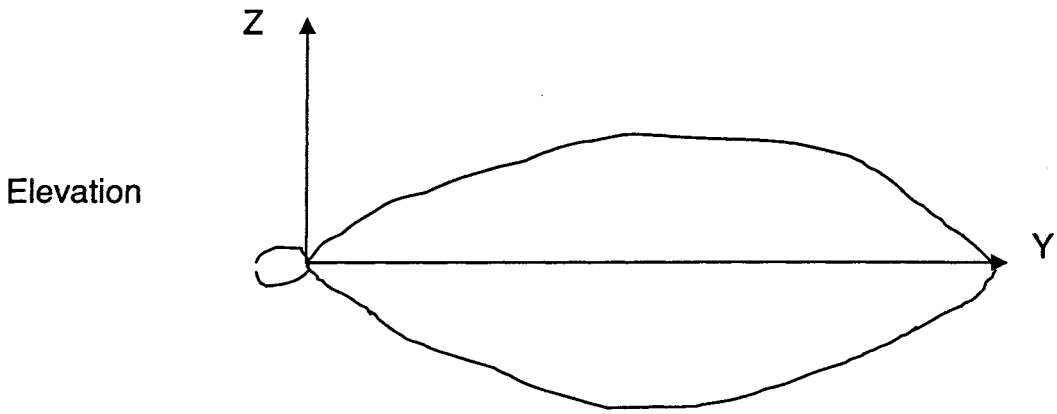
Figures D.25 2 dimensional Elevation radiation patterns of the YAGI Antenna

D.26 2 dimensional azimuth radiation patterns of the YAGI Antenna

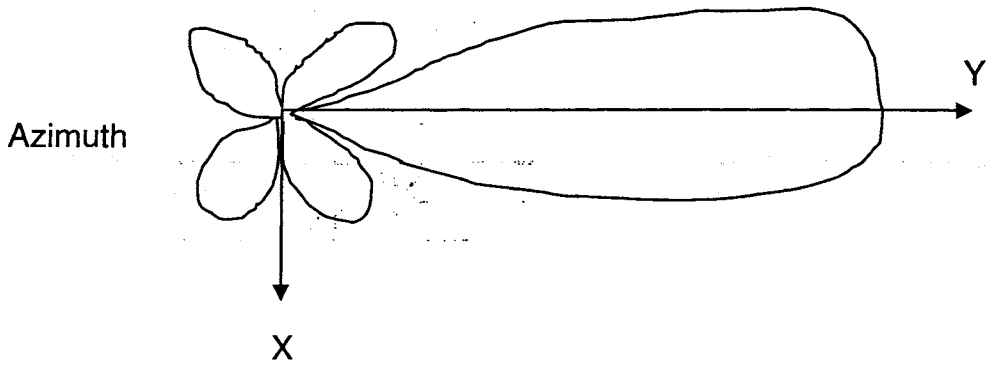
Figure D.27 Azimuth radiation pattern of a typical 3-element Yagi antenna

Figure D.28 Typical Yagi azimuth radiation patterns for different numbers of elements.

Figure D.29 describes constant equal receive signal. The diagram shows how the signal radiates from a signal point. The method in this thesis then shows how the arrays will then combine and form an array.



D.25 Yagi Elevation [61] redone by Sadhana Jackson



D.26 Yagi Azimuth [61] redone by Sadhana Jackson

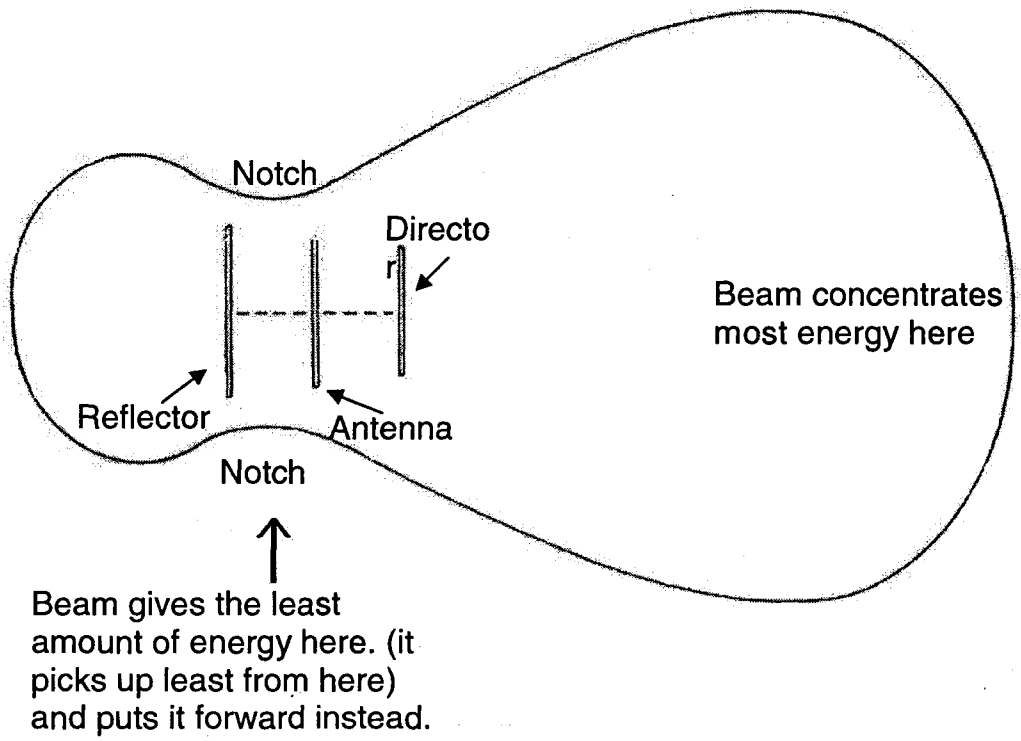


Figure D.27 Looking straight down on a 3 Beam Element [61] redone by Nichole Taylor

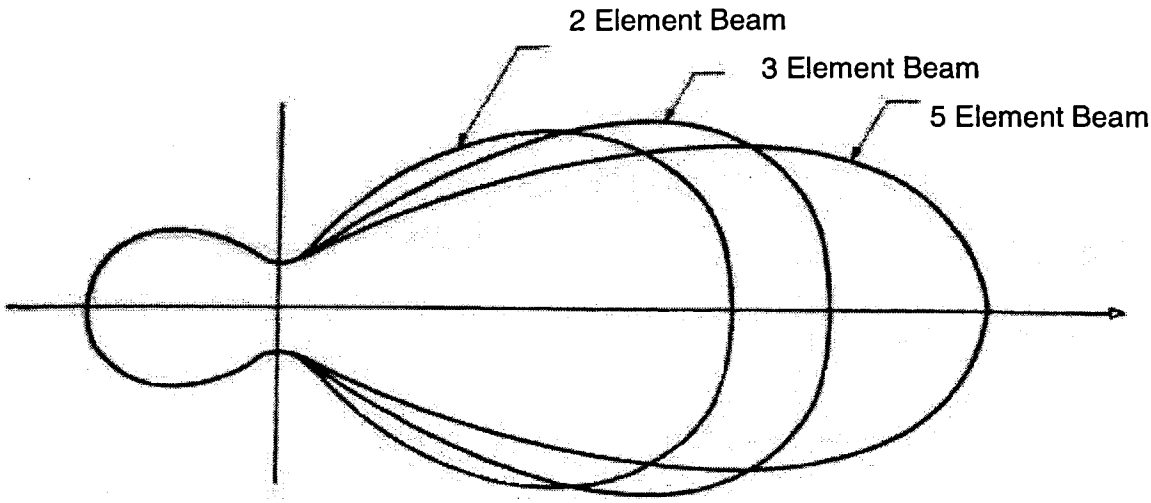


Figure D.28 Yagi Radiation Pattern [61] redone by Nichole Taylor

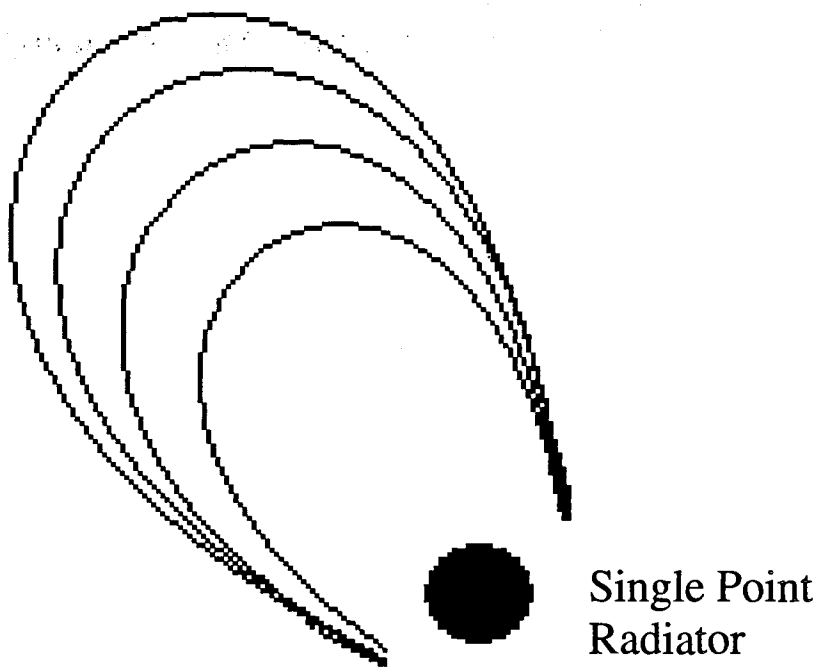


Figure D.29 Constant equal receive signal [32] redone by Nichole Taylor

Array Power Pattern equations

$P(r,\theta)$ $P(r,\theta)$ P=array times array power pattern

$P_A(r,\theta)$ = Array

Positioning the array in a curve shape helps to maintain the maximum power throughout through out the bandwidth. This is known has frequency shadowing. This is how to setup the Yagi antennas around the secure area. The radiation patterns, from the array's that surround the Zone, will over lap each other. This is to give maximum coverage, around the secure area **[32] [40]**

Beam Power Pattern equation

$P(x, y) = P_T P(r,\theta)$

Multiplying the beam power pattern by the array pattern determines the total of the combined pattern. **[32]**

Appendix-E Position-Location Theory

Theoretical approach to the Position location

Using the electromagnetic field strength received by one or more base stations (access points); allows the system to calculate an estimate of the position of the unfriendly. For example, one base station could estimate where the unfriendly is located on a circle. A second base station would add another circle and a third would add a third circle. This way, one could pinpoint the location within a certain accuracy that you would estimate.

There are several methods that can be used for this. In this system design, it calls for the use of various techniques. The reason for using various techniques is because of multi-path issues will arrive from the many signals that will be within the secured area. Multi-path is explained in greater detail in a section below. **[33]**

Multi-Path

Multi-path Interference causes of receive performance sue to phase difference between the direct signal and its reflection. The reflected signal can totally cancel the direct signal. The delay caused by multi-path shows up has ghost figures on a broadcast television image. The delay shows up as ghost on the screen, they will be somewhat physically offset from the intended picture. **[65]**

Graphical Information Systems database (GIS)

A GIS is a computer system capable of assembling, storing, manipulating, and displaying geographically referenced information, data identified according to their locations. The locations on a simple system are plotted on an X and Y coordinate system. This will allow the tracking system will be connected to the tracking system. This will allow the system to track the attacker and locate using the GIS database. The GIS system has these key components.

- A computer graphics program that is used to draw a map.
- One or more external databases that are linked to the objects shown on the map. This linkage permits changes entered into the database to be immediately displayed on the map and querying of the database directly from the map.
- A set of analysis tools that can be used to graphically interpret the externally stored data, for example, by showing objects or regions that meet certain criteria in different colors or shadings. [33][32]

Time of Arrival (TOA)

- A wireless transmits can use any handset (digital, analog, TDMA, CDMA)

The wireless device's signal is received at various antenna sites. Since each antenna is usually different distance from the device, the signal arrives at a slightly different time. This technique requires signal timing information from at least three different antenna sites.

- The receivers, synchronized by a clock, sends the signal timing data on to the mobile switch, where the times are compared and computed to generate a latitude and longitude for the device.
- The signals device and the latitude and longitude are then sent to the GIS system.
- Maps are drawn with specified latitudes and longitudes that can place the device on the map at a given location **[33][32]**

Key ideas of TOA

- Propagation time
- Delay between sender and receiver
- One-way time synchronization
- Accurate clocks
- Synchronization with 2 signals having different velocity
- Additional reference
- Round-trip time
- No synchronization

[33][32]

Figure E.30 is a diagram representing TOA

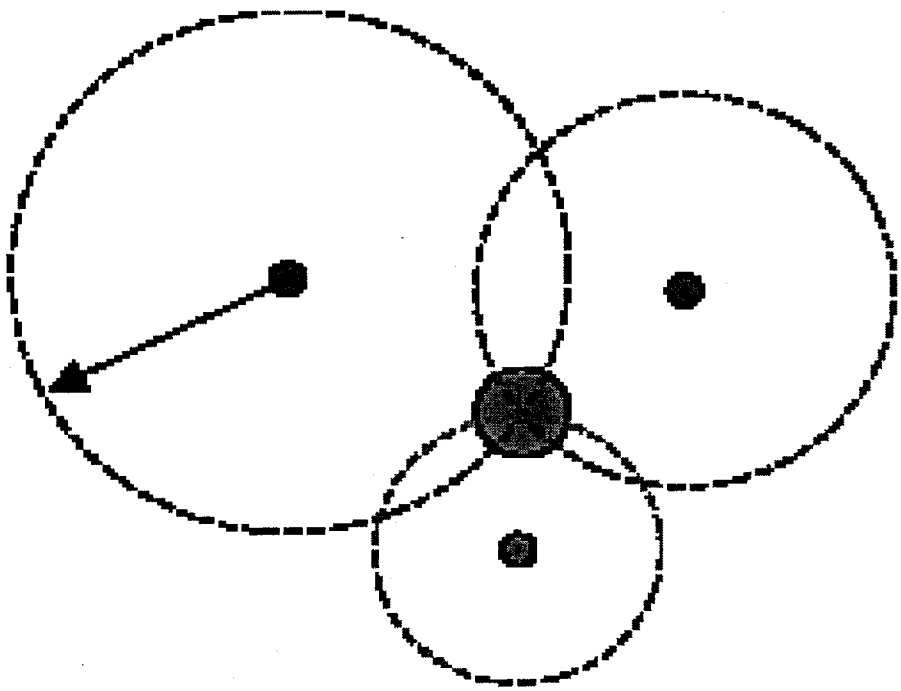


Figure E.30 Time of Arrival (TOA) Diagram
[33] redone by Nichole Taylor

Direction of Arrival (DOA)

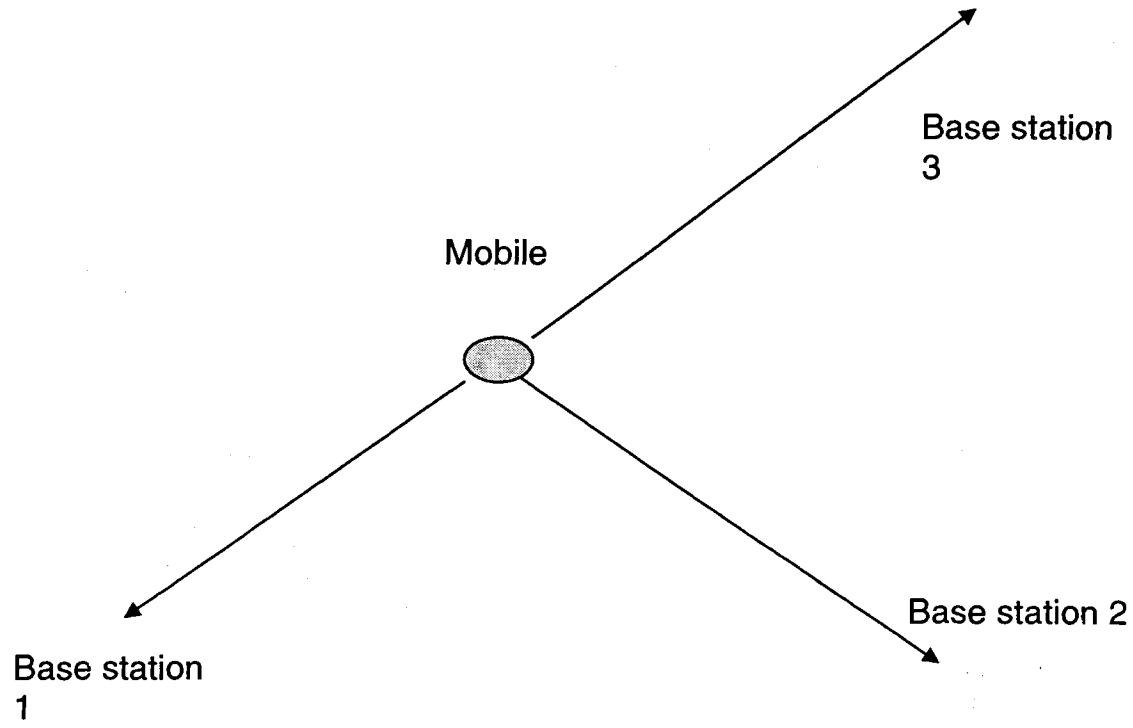


Figure E.31 Direction of Arrival Diagram [33] redone by Nichole Taylor

This is also known as angle of arrival. The mobile is somewhere on the line of direction, where the 2 or mobiles lines intersect. This is where the mobile is located.

- A wireless transmits can use any handset (digital, analog, TDMA, CDMA)
- The wireless device's signal is received at various antenna sites. Each antenna site is also equipped with additional gear to detect the compass direction from which the device's signal is arriving.
- The receivers send the signal and compass data on to the mobile switch, where the angles are compared and computed to generate a latitude and longitude for the signal.
- The devices signal and the latitude and longitude are then sent to the GIS system and mapped. **[33]**

Ranging

Ranging is an active system. Ranging sends out a signal to or from a mobile and reflects the signal back. Ranging then measures the round trip time delay. This equals the distance. The long integration time allows good performance in a signal to noise environment. The one drawback to ranging is multi-path. Below is a diagram of how ranging works. **[33]**

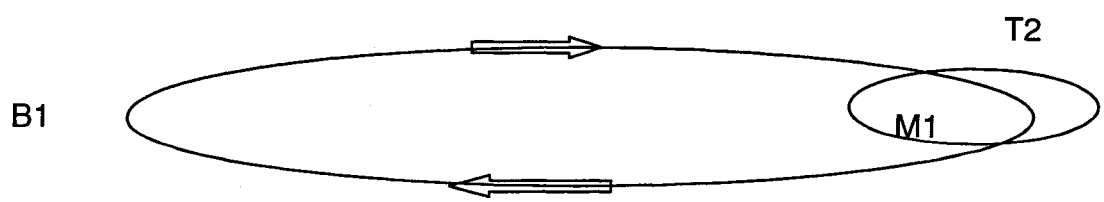


Figure E.32 ranging diagram [33] redone by Nichole Taylor

Equations for ranging [33]

Measured delay

Tm=T1+T2+T3 Equation 4.4

Assumption

T1=T3 Equation 4.5

Propagation

Tp= Tm-T2/2 = T1+T3/2 Equation 4.6

Distance base –mobile is d=TpC Equation 4.7

$c = 3 * 10^8 m/s$ **Speed of light Equation 4.8**

[33]

Position location by strength of signal

This method is an idea from electromagnetic theory. It says that the transmitted power is how the position is a system is able to locate the mobile. This is a method works with at least two base stations. For better results, more base stations are needed. The base stations that are nearest to the source of the RF signal will receive the signal from the mobile station. Then the received power is calculated. From this point the distance (d) is calculated. This gives the distance between the base station and the mobile. When using this with the GIS system, the position location method is a very powerful solution, to locating mobile stations. Below are the equations and the diagrams to further explain Position location from the RF signal. **[33]**

$$P_R = P_T G_T G_R \left(\frac{\lambda}{4\pi R} \right)^2$$ **Equation 4.9 [33]**

Receiving units' measure received power, PR

Estimate PT, GT, GR, Lambda

Calculation of D

D

M ←——————————————————— **B**

This makes it possible to develop a scheme to tell where a mobile is located.

Figure 28 [33]

Below is a diagram of how the system works

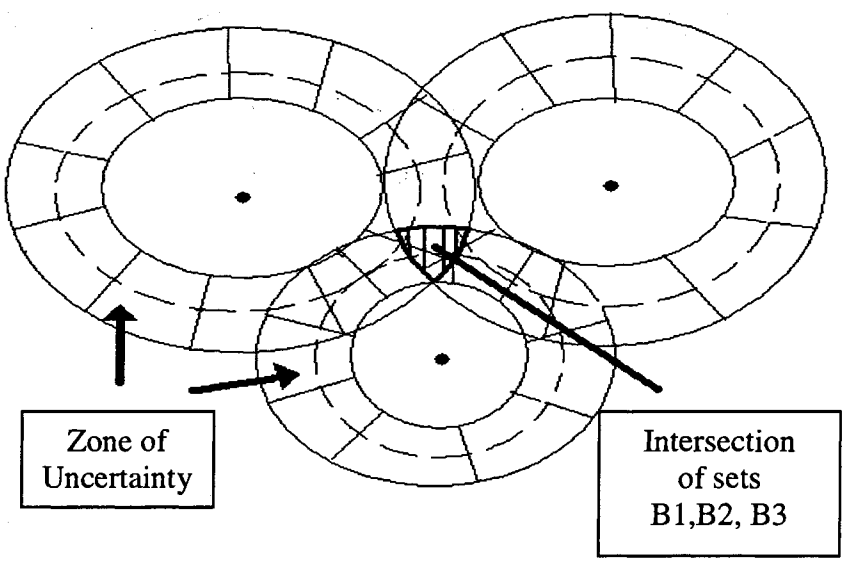


Figure E.33 strength of signal [33] redone by Nichole Taylor

- **Apply probabilities in the annular rings giving a 2-dimensional probability function.**
- **Use maximum likelihood estimate.**

References

[1] William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan **Your Wireless Network has No Clothes** Department of Computer Science University of Maryland

College Park, Maryland 20742

March 30, 2001

[2] Scott Fluhrer, Itsik Mantin, Adi Shamir **Weakness in the Key Scheduling Algorithm of RC4** Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134

sfluhrer@cisco.com

2 Computer Science department, The Weizmann Institute, Rehovot 76100, Israel.

fitsik,shamirg@wisdom.weizmann.ac.il

[3] Harold E. Price **Digital Communications date 7/20/03**

http://www.sss-mag.com/pdf/ssprice.pdf

[4] Jim Geier Spread **Spectrum: Frequency Hopping vs. Direct Sequence date 7/20/03**

http://www.wireless-nets.com/articles/whitepaper_spread.htm

[5] White Paper Spread **Spectrum Wireless Technology date 7/20/03**

http://www.wi-lan.com/library/whitepaper_mcdsss.pdf

[6] Sultan Weatherspoon **Overview of IEEE 802.11b Security date 7/20/03**

http://www.intel.com/technology/itj/q22000/pdf/art_5.pdf

[7] Brad Knowles **More Airport/IEEE 802.11b Security date 7/20/03**

http://www.powerbookcentral.com/columns/knowles/081501.shtml

[9] Nikita Borisov, Ian Goldberg, David Wagener **Intercepting Mobile Communications: The Insecurity of 802.11 http://www.cs.berkeley.edu/~daw/papers/wep-mob01.pdf** date 7/20/03

[10] Princy C. Mehta **Wired Equivalent Privacy Vulnerability April** 4, 2001 http://www.xsecurity.ws/documentacao/papers/geral/equiv.htm date 7/20/03

[11] Bernard Aboba **WEP2 Security Analysis date 7/20/03 http://www.drizzle.com/~aboba/IEEE/11-01-253r0-I-WEP2SecurityAnalysis.ppt**

[12] Lisa Phifer Improving **Wlan Security date 7/20/03 http://www.80211-planet.com/columns/article.php/928471**

[13] Wireless Ethernet Compatibility Alliance **802.11b Wired Equivalent Privacy (WEP) Security http://www.alvarionusa.com/RunTime/Materials/KnowledgePoolFiles/C3_80211b_Wired_Equivalent_Privacy_Security.pdf** February 19, 2001

[14] Angela Champness IEEE 802.11 DSSS: **The Path to High Speed Wireless Data Networking http://www.utdallas.edu/ir/wlans/whitepapers/weca80211.pdf date 7/20/03**

[15] **http://www.palowireless.com/i802_11/ date 7/15/03**

[16] Jim Geier **Overview of the IEEE 802.11 Standard date 7/22/03 http://www.wireless-nets.com/articles/whitepaper_overview_80211.htm**

[17] Christopher W. Klaus **Wireless 802.11b Security FAQ date 7/22/03 http://www.iss.net/wireless/WLAN_FAQ.php**

[18] William Jackson **Protocol used for 802.11b standard is not strong enough for information at 'official use only' security status, expert says 7/22/03**

http://www.gcn.com/20_24/mobile_wireless/16838-1.html

[19] Miika Komu **Known Vulnerabilities in Wireless LAN Security date 7/22/03**

http://www.niksula.cs.hut.fi/~mkomu/docs/wirelesslansec.html

[20] http://www.drizzle.com/~aboba/IEEE/ date 7/15/03

[21] Nicki Hayes **Wired Equivalent Privacy (WEP) date 7/22/03**

http://www.wirelessdevnet.com/channels/wireless/features/newsbyte31.html

[22] Jacobus Petrus Franciscus GLAS Non-Cellular Wireless Communication Systems date 7/22/03 http://cas.et.tudelft.nl/~glas/thesis/main-text.html

[23] http://www.wireless-nets.com/articles/whitepaper_spread.htm date 7/15/03

[24] http://www.ee.byu.edu/ee/class/ee444/ComBook/ComBook/node47.html date 7/15/03

[25] http://wcrg.engr.ucf.edu/VPI_frame/DSSS.html date 7/15/03

[26] Patuxent River Naval Air station. Naval Air Warfare Center. Interviews June 2002

[27] Tom Karygiannis Les Owens National Institute of Standards and Technology Wireless Network Security 802.11, Bluetooth and Handheld Devices

[28] Internet Security Systems Wireless LAN Security 802.11b and Corporate Networks 2001 Internet Security Systems,

29] http://www.its.bldrdoc.gov/fs-1037/ date 7/15/03

[30] http://www.sss-mag.com/ss.html date 7/15/03

[31] http://www.sans.org/rr/securitybasics/defense.php Todd McGuiness Defense in Depth 2001

[32] Steve Russell, Electrical Engineering Dept., Iowa State University, Interview 2002, 2003

[33]Russell, CprE 537: Wireless Network Security, Dept. of Electrical and Computer Engineering, Iowa state University: Ames, Iowa 2003

[34] Robert Taylor, Interview 2002, 2003

[35] Lathi B P, Modern Digital and Analog Communication Systems New York: Holt, Rinehart and Winston, c1983.

[36] Poisel, Richard, Introduction to communication electronic warfare systems Boston: Artech House, c2002.

[37] Maksimov, M.V., Radar Anti-jamming Techniques Dedham, MA: Artech House, 1979.

[38] Greg Stamp, interview 2003, Jamming process date March 2003

[39] Cheng, CprE 543: Wireless Network Architecture, Dept. Of Electrical and Computer Engineering, Iowa State University: Ames, Iowa fall 2002

[40] Compton R.T., Adaptive Antennas concepts and performance Englewood Cliffs, N.J.: Prentice-Hall, c1988

[41] Halm, M.A., Adaptive Array measurements in Communications Boston: Artech House, 2001. date 7/22/03 http://shop.ieee.org/store/product.asp?prodno=PC4519

[42] Blogh J.S., Hanzo L., Third Generation systems and Intelligent Wireless Networks. Smart Antennas and the adaptive modulation

[43] Walter GOJ, Synthetic-Aperture Radar and Electronic WarFare Boston: Artech House, c1993.

[44] Simon, Omura, Scholtz, Levitt, Spread Spectrum Communications Handbook New York: McGraw-Hill, c1994.

[45] Ståhlberg Mika, Radio Jamming Attacks against Two Popular Mobile Networks date 7/22/03 http://www.hut.fi/~mstahlbe/papers/jamming_paper.pdf

[46] Smith, Brian, Smart Antennas for Wireless Communications, EE 521, Dept. Of Electrical and Computer Engineering, Iowa State University: Ames, Iowa date spring 2003

[47] Ganugapati , Vijay , CDMA IS-95, EE 521, Dept. Of Electrical and Computer Engineering, Iowa State University: Ames, Iowa date spring 2003

[48] Hromatka, Thomas, Frequency Hopping Spread Spectrum (FH-SS), EE 521, Dept. Of Electrical and Computer Engineering, Iowa State University: Ames, Iowa date spring 2003

[49] Eekhoff, Eric, An Overview of Smart Antenna Technology, EE 521, Dept. Of Electrical and Computer Engineering, Iowa State University: Ames, Iowa date spring 2003

[50] http://www.governmentsecurity.org/articles/WirelessTaping.php date 7/15/2003

[51] **http://www.webopedia.com/TERM/F/FHSS.html** date 7/15/2003

[52] **http://www.webopedia.com/TERM/D/DSSS.html** date 7/15/2003

[53] http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213842,00.html date 7/15/2003

[54] http://www.cs.ucl.ac.uk/staff/S.Bhatti/D51-notes/node11.html date 7/15/2003

[55] http://home.san.rr.com/denbeste/glossary.html#J-STD-008 date 7/15/2003

[56] http://www.cdmaonline.com/members/workshops/terms1/1008.htm date 7/15/2003

[57] http://www.uksecurityonline.com//threat/insertion.php date 7/15/2003

[58] http://www.shoshin.uwaterloo.ca/~jscouria/GSM/index.html date 7/15/2003

[59] http://ccnga.uwaterloo.ca/~jscouria/trio.html date 7/15/2003

[60] http://seclab.cs.ucdavis.edu/projects/history/ date 7/15/2003

[61] https://ewhdbks.mugu.navy.mil/antena11.gif date 7/15/2003

[62] Sontag, Drew, Blind Man's Bluff: The Untold Story of Cold War Submarine Espionage, Arrow; ISBN: 0099409984 19 January, 2001

[63] Douglas Jacobson, Electrical Engineering Dept., Iowa State University, Interview 2002, 2003

[64] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci549087,00.html date 7-15-03

[65] Wiley, Blogh, L. Hanzo, Third generation systems and intelligent wireless networking: IEEE Press; Chichester, West Sussex; New York: Wiley, c2002.

[66] http://arstechnica.com/paedia/w/wireless/security-3.html date. 7/15/2003

[67] http://www.uksecurityonline.com/threat/dos.php 7/15/2003

[68] http://www.logogo.net/liberty.htm 7/16/2003