Spring 3-5-2010

Study of Physical Layer Security in Wireless Communications

Mustafa Duruturk
University of Nebraska at Lincoln, duruturk52@hotmail.com

STUDY OF PHYSICAL LAYER SECURITY IN WIRELESS COMMUNICATION

by

Mustafa Duruturk

A THESIS

Presented to the Faculty of

the Graduate College at the University of Nebraska

in Partial Fulfillment of Requirements

for the Degree of Master of Science

Major: Telecommunication Engineering

Under the Supervision of Professor Hamid Sharif and Michael Hempel

Lincoln, Nebraska

March, 2010

STUDY OF PHYSICAL LAYER SECURITY IN WIRELESS COMMUNICATION

Mustafa Duruturk, M.S.

University of Nebraska, 2010

Adviser: Hamid Sharif and Michael Hempel

This thesis has investigated security in wireless communications at physical layer. Security is an important issue for wireless communications and poses many challenges. Most security schemes have been applied to the upper layers of communications networks. Since in a typical wireless communication, transmission of data is over the air, third party receiver(s) may have easy access to the transmitted data. This work discusses a new security technique at the physical layer for the MIMO (802.11n) transmitters.

For this project, the wireless medium is secured by transmitting a noise signal that is only recoverable by the receiver. This report includes an analysis of a wireless system that shows the bit error rate (BER) of the data signal in a two dimensional map. The map is a view of the free space, which has a receiver and transmitter at the ends. This work demonstrates that the proposed security technique can significantly complement other security approaches implemented in the upper layers of the communication network.

Acknowledgments

I would like to thank Dr. Hamid Sharif for his help in performing the task described in this thesis and for the valuable discussions during the execution of this project. Professor Sharif had many good questions for improving the final result of my report. For his support in the completion of this thesis, I also thank Michael Hempel.

Table of Contents

Table of Figures

Statement of Purpose

The aim of this work is to simulate a channel model of a wireless network with a network security system that protects the wireless signal at the medium.

Chapter 1. Introduction

Computer technologies have become a very important part of people's lives for the past couple of decades. A big part of the computer market today is wireless networking. Wireless networks have many advantages over wired networks.

As technology develops further, computer hardware is getting smaller. At the same time, wireless technology gives people mobility, comfort and other conveniences.

Early wireless networking devices used infrared wavelengths to transmit data over the medium. Later models of the wireless devices have used radio waves because radio waves have better penetration behavior. Currently, radio waves provide better coverage, which is very important for a user.

New research is being made to enhance the coverage of wireless networks by using modulation and digital signal processing techniques.

In search of a better quality of service, diversity systems were used up until 2004. In diversity configurations there are multiple transmitters that have been used to decide which transmitter is more efficient for the specific time and location. In this configuration, only one transmitter and receiver have been used at a time.

A more sophisticated system of diversity is a system that can use multiple antennas at a time or at the same time. Using multiple antennas simultaneously is the first step of the MIMO, Multiple Input Multiple Output systems. With MIMO antennas (when they start transmitting in multiple antennas) the throughput has improved multiple times more than the single antenna configuration. MIMO also helped resolve multipath interference problems. Different digital signal processing techniques are improved for simultaneous transmitting. The quality of the data has improved also.

Multiple antenna systems allow for the use of beamforming. Beamforming is a digital signal processing technique that allows the pointing of the RF Signal to the specific direction. This requires that all the antennas use the same coding. In beamforming mode antennas tune phases in a different way and change amplitude to form a beam in a specific direction. In some cases, the importance of the digital signal processing is understood, such as when the number of spatial streams is greater than the number of receiving antennas. Data is recovered using advanced digital signal processing if the number of spatial streams are assigned to the antennas according to a set of rules.

MIMO is also called a smart antenna because of its ability to adapt a signal for different situations and requirements. In the field, people are trying to take advantage of smart antennas for higher speeds, longer ranges and security purposes. Smart antennas raise a very broad list of research topics.

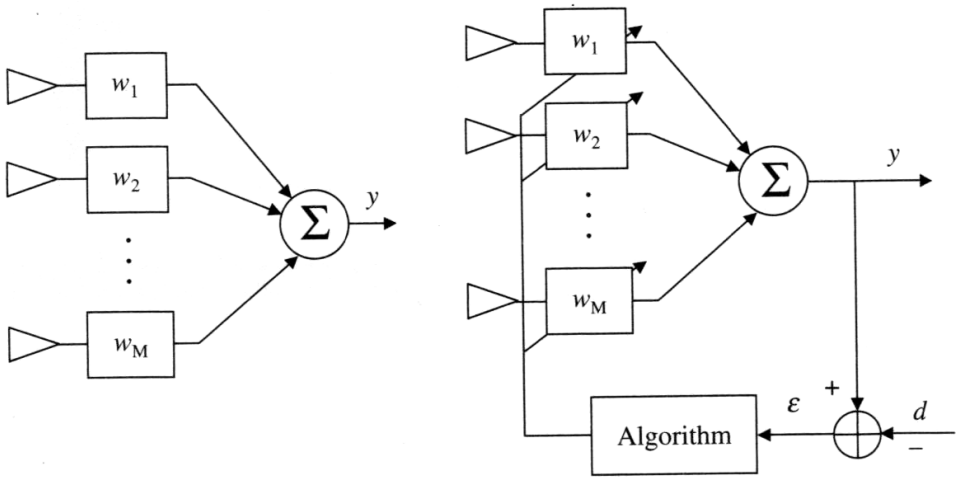
This report includes a summary of the background of wireless security systems. Before going into the implementation of this research project's security system, the report will cover wireless security systems, smart antennas and channel models.

Then this report describes the implementation of the newly proposed wireless security system, and the report demonstrates how to take advantage of wireless antennas and the beamsteering mode of smart antennas.

The term smart antenna is used for a multiple antenna system with a sophisticated algorithm that can adapt the environment and know the interfering signals. Adaptive arrays can be switched to beam arrays or adaptive beam arrays. Switched beam arrays have several fixed beams that the receiver can select in order to get the best performance and know the interfering noise. Adaptive arrays can steer a beam at a point of interest,

while knowing the interfering signals. Smart antenna systems are now mostly adaptive arrays.

Fixed beam systems are not considered smart antennas anymore because adaptive arrays are getting much more sophisticated than just a simple switched beam array. Figure 1.1 shows the difference between adaptive and switched beam antenna arrays.



(a) (b)

Figure 1.1: (a) Traditional array, (b) Smart array [2].

Chapter 2. Wireless Security Systems

In this chapter, current wireless security systems and system challenges are discussed. Wireless security is very important, especially for some critical data types. The important issues to cover for the purpose of this report are wired equivalent privacy, WEP, improvements on WEP and weaknesses of WEP.

2.1 Traditional Wireless Security Systems

Traditional wireless security can be discussed in two parts: authentication and encryption. Encryption is controlled by WEP and is responsible for encoding the data, so it is not decodable by someone else who is not authorized. Authentication is a policy between the receiver and the transmitter, so the two know each other and are not allowing other people or parties to enter into the network. Authentication is handled by medium access control, MAC layer.

2.1.1 Authentication

Most access points provide the feature of authentication on the hardware. MAC layers authenticate the connection, so only registered MAC addresses are allowed to connect to a network. Authentication is a procedure that is done by checking the MAC layer address of the attempted connection. This mechanism is vulnerable for two reasons. First, MAC addresses can be changed in some hardware, so a MAC layer of the authenticated user can be duplicated and used to provide access to a network. Second, hardware controls the authentication. A danger is that hardware can be stolen, and unapproved access can be given to a network.

In some cases, authentication can be one way the access point can verify a user, but a user does not authenticate an access point. This kind of authentication is dangerous because a user can access information about other users in the network.

2.1.2 Encryption

In wireless communication, an early encryption policy is WEP. Today, WEP encryption networks are not considered secure networks, but WEP is still the most common encryption people are using. The second generation encryption system is called Virtual Private Networking, VPN, mechanism.

WEP encryption is proven to have some weaknesses. Some cracks show WEP encryption can be decodable because of a weak initialization vector. Since security experts know that WEP is not secure, they have tried to fix the problem with improved WEP encryption in 802.11B products. In WEP encryption a transmitter transmits the initialization vector and a user follows the instructions.

For an alternative to WEP encryption, people use VPN software to encrypt their data because it is believed to be much more secure than WEP encryption. VPN offers much better encryption that is harder to decode by cracks.

Today, there are other encryption policies that are used in the market for the purpose of a more secure data transmission. Figure 2.1 shows the encryption systems that are used in the market.

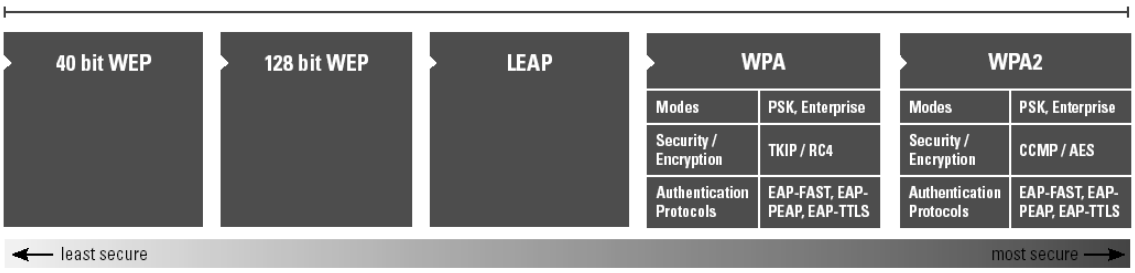


Figure 2.1: Encryption systems [8].

2.2 Problems with Wireless Security

In conventional data communication, data is transmitted through cable. However, it is become much preferable to set up an access point and start the network without the wiring hassle. With wireless, a user can also roam and still use the network under the coverage of the access point. With these advantages, wireless communication comes with security problems.

A behavior of a radio wave is the ability to penetrate long distances. It is very hard to predict how far it penetrates and in which direction. If wireless is unsecure, hackers can be far with their receivers and still record data with the transmitters to analyze the code or collect and analyze it at later times. Through this method, hackers can get all information from the targeted computer like passwords, e-mails and even more personal information, like banking information. Unsecured Internet use causes long-term problems like identity theft.

One security problem is that any computer with the same equipment can access the unsecure wireless network. Using more powerful receivers, a computer can detect the signals and try to get into the network, where the signal is very weak for other equipment.

Today, physical security is more confidential than wireless security, since the data is not broadcasted from a router. Hackers would have to cut the cables to reach the information.

Wireless has come with techniques to protect the data. However, with the known problems of wireless networks, network designers are hesitating to use wireless in their designs. In this part of the report is an overview of the most common problems and other potential problems, such as unauthorized access to the wireless networks.

2.2.1 Easy Access

Wireless access points should be accessible to any user in the network. Before a user connects to the network, the user is able to see the network. To be visible, access points broadcast signals as a frame called beacons. When a user attempts to connect to a network the user signal is not encrypted. Because there is no encryption, someone else could detect that user signal and use it to access the network.

Protecting the signal in a shield of walls is one solution, but it is not very practical. A network should have strong authentication and encryption controls. Also, VPN should be used as an authentication method.

2.2.2 Rogue Access Points

In a high number of user networks, it would be difficult to keep track of all users' access. A related challenge is user education about network security. Users are usually not every day very concerned about the network security, and they might not know how to properly secure a wireless network. Most unfortunately, the big investment to secure a

network can be ruined by a user who connects a wireless access point to a network and opens the network up to easy attacks.

There is no easy solution for this type of problem related to users who do rogue access points. There are ways to detect wireless signals that are connected to the network. For example, an administrator can go into the rooms of a building to find wireless access points. Nearby wireless networks from other offices may be detected, and that makes it hard to understand which access point is connected to the owner's network. Periodic checks are a solution for the rogue access point problem, but that is dependent on network administrators who may not have time to do the checks. This is not a sure solution to a constant risk of possible rogue access points.

2.2.3 Unauthorized Use of Service

Offices and houses with wireless access points are more common now. When people buy wireless devices to go onto the Internet in their homes, the setup includes default settings on the device. The wireless devices are manufactured that way to give some convenience. In the default setting, a wireless device has no security restrictions, and it is common that people are not setting up a key for a secure wireless network because that takes time. These people begin using a wireless router with no authentication or encryption.

This is a mistake that causes two main problems: unauthenticated access and bandwidth problems. Unsecured wireless networks can lead to challenges for the user, including legal problems.

Unauthorized connections can produce enormous amounts of data traffic because there is more than one computer's data combining, even though there is a limited total amount of bandwidth available. Combined data traffic makes the Internet use slow or even useless for some applications that need lots of bandwidth. Especially in crowded areas, like apartment complexes, there could be several unauthorized connections accessing the unsecured wireless network.

Unauthorized users that are connected to a network can be a legal problem by using Internet for illegal purposes like sharing copyrighted music or movies. An Internet Service Provider can decide to end Internet service if a customer breaks the terms of use with unauthorized users.

However, multiple users may not be a problem in some cases. It depends on the Internet activities of the unknown users. For example, a place like a public library can offer wireless Internet access without having to provide passwords to users. This is a convenience for the library, because it can still be in control of the network. Also this type of service would not cause harm to the provider, like a library, when valuable data is not stored in the same network.

All wireless networks do not have to be secured in the highest levels. There are some wireless Internet providers that have unsecured Internet access, meaning users do not give a password and can access the network with basic steps. That leaves the network open to any customers inside the area without adding unnecessary processes to the provider. In public places, users access and use the Internet at their own risk.

However for corporations, wireless networks have to be secured with the highest level security solutions, usually different than the public places. Valuable or private

information is part of data traffic in a corporation, so corporations need to have different security.

Among today's technology, VPN has one of the strongest authentication capabilities. VPN gives the network administrator a choice of authentication methods depending on the capabilities of transport layer security, TLS. Users can only connect to authorized access points. 802.1x has this capability to add security using transport layer.

2.2.4 Service and Performance Constraints

Wireless access points have less capacity than wired connections to transfer data. For example, 802.11b has a capacity of 11 Mbps and newer models of access points have 54 Mbps. Capacity is shared among all users that are connected to one wireless network. Due to the slower speed of wireless, router connections can be overwhelmed. MAC layer overhead and local area applications are factors of the access point reaching its capacity. This kind of situation is a good chance for denial of service attacks on the limited sources.

There are several ways to bring an access point to its capacity. One way is through massive amounts of data sent from a wired network to wireless devices. Because wired connections are much faster, it would easily bring the access point to capacity because the data would start piling up at the buffer of the access point.

Attackers can also produce heavy traffic on the wireless that would make the network adapt in a high traffic environment using a CSMA/CA mechanism to send the data, which causes the data to wait in the buffer of the access point.

In the heavy traffic of wireless networks, there will be lots of large traffic loads that can make security vulnerable.

2.2.5 MAC Spoofing and Hacking

Data transmission is made by frames. Each data frame has a header, and in the header there is a part of the source address. A frame is sent to the air by the source with the source address in the header. There is no authentication for the frames. There could be an attacker who can send the same frame with your source address. There is no protection against forgery.

Attackers can copy the source addresses and confuse and corrupt the data transmission. Authentication systems are developed to protect the network from this kind of attacks, but denial of service attacks cannot be stopped because there is nothing to keep attackers off of the medium in wireless networks. Authentication basics started in 2001 with 802.1x, but there were many improvements to handle the key management.

Attackers can also pretend to be the access point. An attacker can copy the beacon frames of the access point they want to imitate. When this happens and the users try to authenticate with the copy access point, they give away personal credentials to the attacker. After that, attackers can use the credential information to connect to secured wireless networks. The problem is that there is no way for a user to know the access point is the true access point, which is safe to connect to.

There are access points supporting two ways to solve this problem. One way is a wireless access point provides its identity before the connection can authenticate. The

problem will not be solved until access points authenticate each frame. Encryptions are also a good defense against this kind of attack.

2.2.6 Traffic Analysis and Eavesdropping

In wireless networks today there is no protection to keep the wireless signal away from an eavesdropper. Framed headers are always unencrypted, making it easy for an attacker to save all the traffic between a user and access point and analyze the data later.

Encrypting data is supposed to the best way to protect data against this type of attack. Early WEP encryption was vulnerable because it only protected the initial association with the access point and user. Only the data frames and encrypted remaining frames stayed the same way. There were attack tools developed to get into the networks.

The latest encryption products have much more complex systems changing the key in intervals of minutes. For the attacker it is very hard to find the right key but not impossible.

The latest wireless security products are supposed to protect against these vulnerabilities. The security solutions give network managers a comfort; on the other hand when the WEP was released, it was said that it had no vulnerabilities too.

2.2.7 Higher Level Attacks

In network systems there are several ways to attack if the connection is already established. Most security products are designed so there are no unauthorized connections from outside the network.

All networks can be vulnerable if a small part of the network is vulnerable. That is why networks where the highest level of security is assumed should be secured from the end to the backbone. It is easy to deploy a wireless network even if it is connected to vulnerabilities. Once the access is gained, depending on the network topology, it could be used to attack other networks. That would not be good for a network administrator's reputation, if a network is used to attack other networks. The preferred solution to the problem is to not give access to the attackers in the first place.

2.3 Security Requirements

Security policies must be developed for the ownership and the administration of wireless networks. Physical security must be established with the encryption. Physical network connections and rogue access point connections should be detected and handled.

Organizations have security solution options like limiting access of users and limiting wireless networks. Security solutions also use standard regulatory systems and rules from government and private organizations that have made publications as guides.

A common requirement for network security is that data should not be stored or transmitted through public networks. Data should be encrypted using certified encryption algorithms. These certified algorithms are regularly updated for secure communications because they are longer, improved algorithms.

Another way to secure connections to a network is authentication that has two levels. A requirement would be a security token, which is something that is physically carried away with a user like a card or flash drive. A second level in authentication could

be a password that a user has to provide at every new connection or biometrics, such as fingerprints.

Network security solutions are vulnerable against new tactics of attackers, and regulations tend to become more strict and complicated. Companies are looking to have different, stronger wireless security solutions.

Even as different wireless security mechanisms are implemented, most of them are proven to have vulnerabilities. These security mechanisms are user authentication, encryptions and firewalls.

Again, as a general definition, authentication is a requirement for the network to confirm legitimate devices accessing the network. Authentication policies are required to synchronize with other policies and devices.

All security systems are related to an organization's risk management processes. By using stronger algorithms and new security systems, risk is reduced by a fraction of the possibility of the network being attacked and accessed.

Companies should consider all the risk factors when connecting networks to wireless access points or other networks.

As mentioned earlier, authentication should not be with the hardware device. It should be between the user and the network. Credentials of the authentication can be stolen or removed with the hardware or wireless cards.

2.4 Security Layers

Networks have layers for management purposes. Layers help developers implement new security systems that fit into current and future systems. Layers are

required to make systems clear, distinct and manageable. Wireless networks also have three security layers that fit into and work with traditional networks. These security layers are wireless LAN layer, access control layer and authentication layer.

Wireless LAN layer is the lowest level that deals with data from the medium. This layer sends out the beacon packets and reviews the attempts into the network. This layer is also responsible for encrypting and decrypting the data after the connection is established.

The access control layer is responsible for the contents of the data traffic. This layer ensures that all the data is from the authenticated devices. This layer is getting new authenticated connection information to allow a device's data to go through.

The authentication layer authenticates connections. It validates identities of connections attempted. The authentication layer keeps the database to identify the users. In a small network, the authentication layer can be in the access point. In large-scale wireless networks, this data is stored in the server to have a more manageable and upgradable security system.

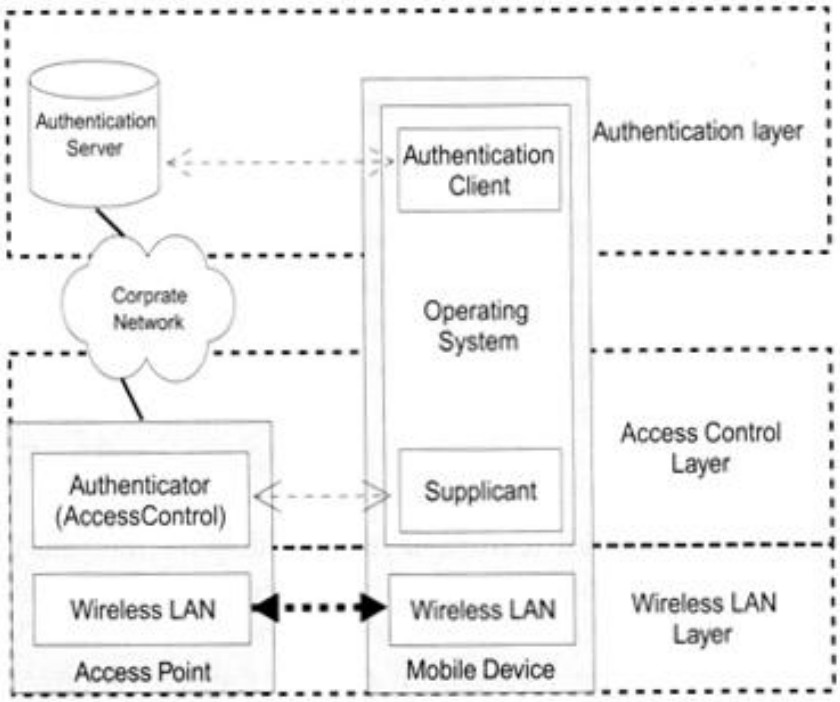


Figure 2.2: Relationship of layers [14].

2.5 Literature Review

The conventional network securities are relying on passwords or keys. The disadvantages of conventional network wireless securities are challenging. The biggest handicap of wireless security is being open to eavesdroppers seeing the signal in the medium.

Key-based security systems use big overhead over the network. As good as security gets, overhead increases. It may also cause key management problems in high number node networks.

All these vulnerabilities already covered lead to a need for investigating security solutions that do not depend on secrets. This project investigates the possibility of using

noisy feedback to achieve security without secrets by exploiting the structure of the wiretap channel and using a private key known only to the destination.

While designers tend to have explored the problem from an information theory perspective, this project focused on designing a system with a different channel model and receiver model. In order to achieve secure communications without shared secrets, the designated receiver intentionally injects noisy feedback during the sender's transmission, such that any message received at the eavesdropper (if any) has no clue about the source message from the sender.

Chapter 3. Background - Smart Antennas

In traditional array antennas, phase shifters steer the beams to the direction of interest. Phases of signals are changed directly in each antenna element. This is called electronic phase shifting because phases directly shift at the current of the signal.

The modern systems of beam steering are made by smart antennas because smart antennas are capable of steering the beam with certain criteria with a specific pattern. This is called digital beam forming or smart antenna arrays. The term “smart” is usually used for computer controlled systems. In smart antennas, a beam is steered using advanced digital signal processing techniques. Smart antennas are improved in many aspects of traditional antennas. Smart antennas are used in radar systems, mobile wireless devices and improved wireless communications of space time multiple access.

Algorithms control smart antennas to match to the certain criteria. These algorithms are controlled by analog circuits. These algorithms are designed to maximize the signal-noise ratio and minimize the probability of signal-to-error rate. Algorithms are also designed to know interfering signals. The implementation of these algorithms are required for a signal to be converted to a digital signal, using an analog-to-digital converter.

Digital signal processing is usually applied to baseband frequencies. The antenna pattern is formed using digital signal processing. Since it is done digitally, it is also called digital beamforming.

Figure 3.1 shows the electronically generated digital beam steering mechanism.

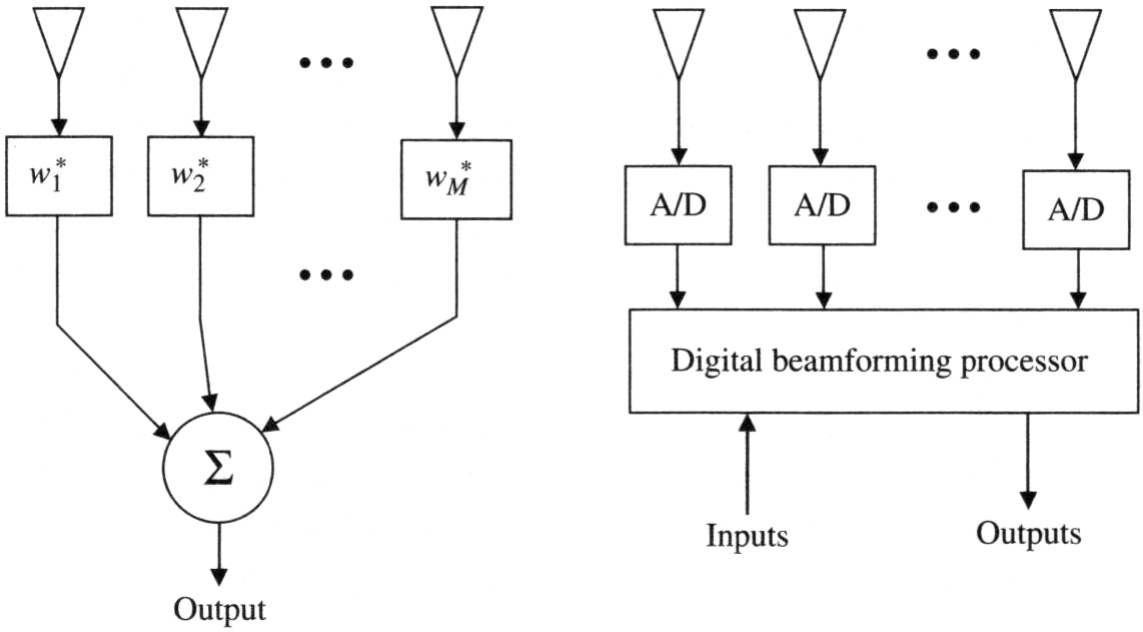


Figure 3.1: (a) Analog Beamforming. (b) Digital Beamforming [2].

In addition to digital beam forming algorithms these algorithms can also be designed to have adaptive beam forming capabilities. Digital beam forming has been applied to many different applications like radars. A main advantage of digital beam forming is being performed by software. It can be improved and modified because it is not performed with hardware. In a very similar way in the receiver side, hardware is not modified somehow to adapt to the environment. Beam forming is done digitally by the algorithms. A signal is processed computationally to get the part of the signal that a receiver is interested in when the circumstances change. In case the algorithms are not good enough to meet the requirements, algorithms can be replaced.

In an unpredictable electromagnetic environment, adaptive beam forming is the dominant choice for getting a better performance from a smart antenna. Adaptive algorithms improve the quality of signal.

The biggest difference between conventional arrays and adaptive arrays is the capability of overcoming difficult environments like interfering electromagnetic signals, clutter returns or multipath interference.

3.1 Historical Development

Smart antennas started developing the late 1950s. The word adaptive array was first used by Von Alta in 1954 to describe a self phased array.

In the first adaptive arrays there was only one capability of modern antenna arrays. The first antenna arrays could only transmit a signal at the incident of incoming signal to the antenna. Those antenna arrays used self phased antenna algorithms.

According to Frank Gross, author of Smart Antennas for Wireless Communications, phase locked (PLL) systems were incorporated into arrays in the 1960s in an effort to construct better retrodirective arrays. This approach was considered to be the best at that time.

In later years, adaptive sidelobe cancellation was proposed. That was the first initiation of the sidelobe cancelling technique that is used today. Sidelobe cancelling allowed cancelling of interfering signals to have a better signal quality. Then, Howells Applebaum improved this idea. He proposed an algorithm to have adaptive interference cancellation. According to Gross, these algorithms depend on eigenvalue spread such that larger spreads require longer convergence times.

3.2 Fundamentals of Beamforming

Smart antennas are a combination of nondirectional antennas. These nondirectional antennas work at the same time to form a beam by changing the phase of signals. This could be done by hardware, electronically or a combination of the two. In this chapter, the simplest smart antenna array is exhibited, which is very similar to one used in this project's simulations.

3.2.1 Uniform Four Element Linear Array

A very basic antenna array is the linear antenna array. Linear antenna arrays are the easiest to implement and give a very good understanding of smart antenna systems. In this section is the implementation of a linear antenna element.

In general, the linear antenna array has N element. Figure 3.2 shows an element linear antenna array. The first calculation is the signal strength at the far field from the origin with the phase difference of sigma at each element starting with the first one.

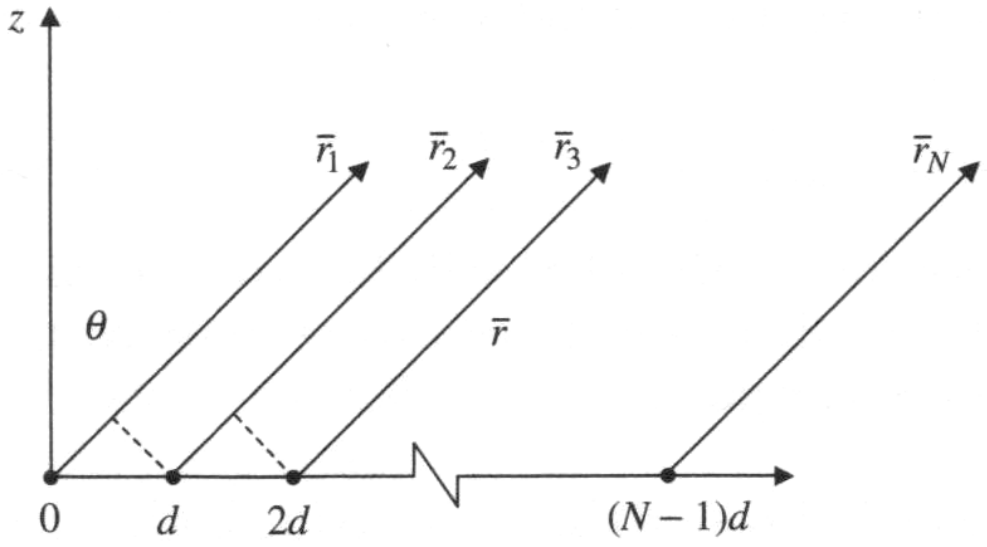


Figure 3.2: N-element linear array [2].

The distance between the antenna elements are much smaller than the distance between the receiver and the transmitter. A generalized array factor is calculated by Gross in Smart Antennas for Wireless Communications as follows:

$$AF_n = \frac{1}{N} \frac{\sin\left(\frac{Nkd}{2}(\sin\theta - \sin\theta_0)\right)}{\sin\left(\frac{kd}{2}(\sin\theta - \sin\theta_0)\right)} \quad [2]$$

3.2.2 Beamsteered and Weighted Arrays

Already the report has outlined a simple implementation of a uniformly weighted and same amplitude linear arrays. In this kind of system, the sidelobes are still very large in comparison to the mainlobes. In Figure 3.3, it is seen that the mainlobe can be steered in any direction, even without changing the amplitude of any array element.

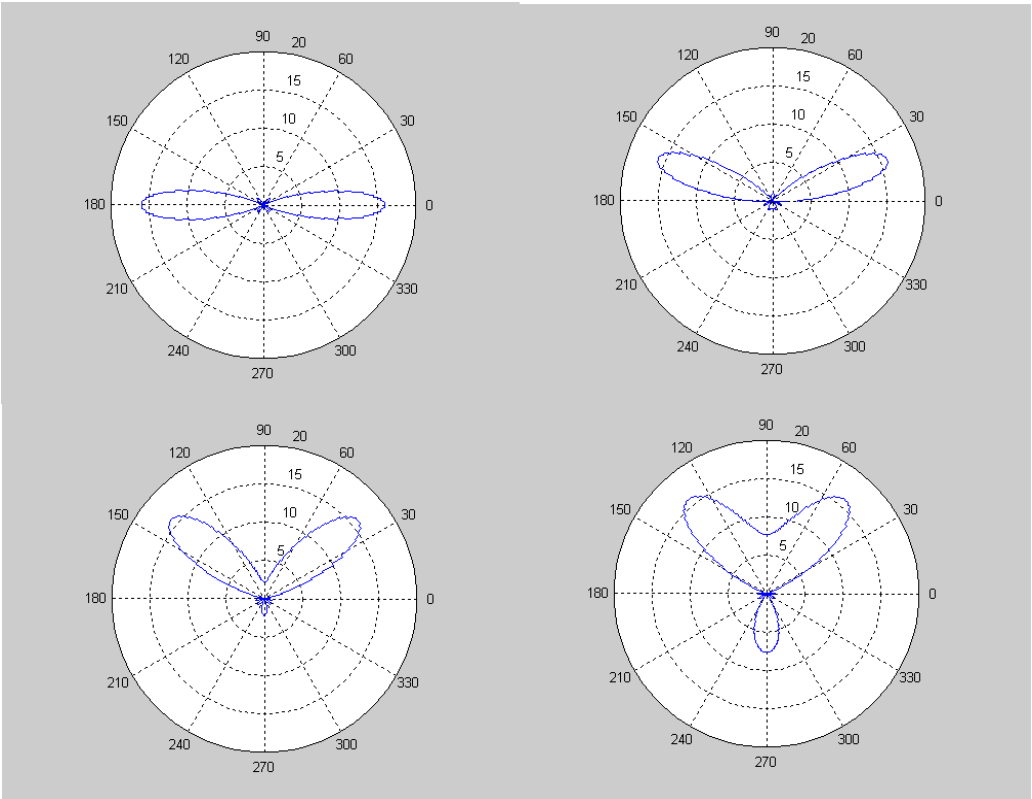


Figure 3.3: Footstep prints from the simulations.

In this setup, the sidelobes of the beam are seen clearly. Any sidelobe means an undesired signal is generated in the undesired direction. An undesired generated signal will consume some power, and that is why algorithms are designed to minimize the sidelobes or sidelobes can be used to surpass the unwanted signals. A mainlobe is always steered to the direction of interest, while a sidelobe is used to fade the unwanted signals from other directions.

Hardware or algorithms can also control array weighting, very similar to the phase shifting. To have more efficiency out of less array elements, both phase shifting and array weighting is used.

Chapter 4. Problem Statement

Wireless communication is becoming a replacement for the conventional wired connection. Today, there are security improvements necessary to have a wireless network that is as secure as the wired connection. This project's research is looking for any security improvement that can be done to bring the wireless connection to be as secure as the wired connection.

A problem with today's wireless security solutions is the fact that data is still available to a third party in the medium. Today's wireless security systems will require an upgrade. This will affect millions of people who will have to upgrade their systems and access points in order to have a secure connection. In this project is a search for a better security solution that provides an invisible connection to the third party.

Chapter 5. System Model

The system in this project's theory uses wireless technology with a new approach to securing the data. In this project's approach, the intention is to secure the wireless signal over the medium to prevent an eavesdropper from accessing the data. The data becomes invisible to the third party. However, the intended receiver will have no complication and no reduction of quality to the received signal.

The project requires an overlay signal transmitted by the receiver, so the receiver will be the only party to recover the desired signal from the overlay signal. This can be achieved because the eavesdropper has no way to predict the noise signal. There are no tools for an eavesdropper to separate the overlay signal from the data signal.

An advantage of this project's system over existing security systems for data transmission is avoiding secrets that can be stolen or misused. This project is intended to remove the security risk that comes with wireless data transmission.

Another advantage is it could be used with any security schemes already in place. This project's system is not interfering with the requirements or execution of security like encryption or authentication.

A possible disadvantage is detected by understanding the two signals are not overlapping in all places. Even so, the project shows the theory reduces risk to data security because the simulations in the project have a goal of securing a majority of the signal.

The system consists of a transmitter and a receiver. The transmitter and the receiver are placed at each side of a map, which is generated in different sizes up to a 100-meter length. Each transmitter and receiver is a directional antenna consisting of four

non-directional antennas. The directional antenna can steer a beam in any direction of interest. In this model beams are pointed toward each other. This model is designed and simulated using the Matlab programming language. Both the transmitter and receiver generates 2.4Ghz signals. The transmitter and receiver uses 16-Qam, Quadrature amplitude modulation. When the transmitter sends the message, the receiver intentionally transmits randomly generated feedback, such that the receiver is able to recover the data, while the eavesdropper cannot understand anything from the data. This model is prepared to see the two-dimensional maps of the BER of the signal. The map will show the areas that are not recoverable by an eavesdropper and areas that are not protected with the project's system.

5.1 Methodology

This method is usually used in radio signals to disturb communication by decreasing the signal-to-noise ratio. In this project the signal protects the data in the medium. Intentional communications jamming is usually aimed at radio signals to disrupt control of a battle situation. One side's transmitter will have the same frequency as the opponents' receiver equipment, and with the same modulation and enough power, overrides the receiver side signal.

The most common of these signal jams are random noise, random pulse, stepped tones, warbler, random keyed modulated CW, tone, rotary, pulse, spark, recorded sounds, gulls, and sweep-through. This project's system is randomly generated 16-Qam signals.

The main purpose of this project is to have as little signal available as possible in the medium to improve the security. The aim is to take the advantage of beamforming

and smart antennas. Smart antennas have a feature of beamforming and beamsteering, directing the signal to the point of interest. Therefore the signal is only available on the path from the transmitter to the receiver.

The contrast is that in traditional antennas a signal is broadcasted, and that would be very hard and costly to hide the signal of the non-directional antennas. In this project, the method uses two smart antennas working on beamforming mode, and the receiving side will direct the noise signal toward to the transmitter. In this way the receiver would be able to recover the data from the noise that is generated by itself, and the data signal would not be available on the path to the receiver.

5.2 Generating Signals

In beamforming there are many antennas working at the same time to form a beam that is directed to the point of interest. This project generated the beams with the same technique. Matlab generated four signals in polar coordinates and added them up to form a beam. In Figure 5.1 the single non-directional signal is propagating in all directions.

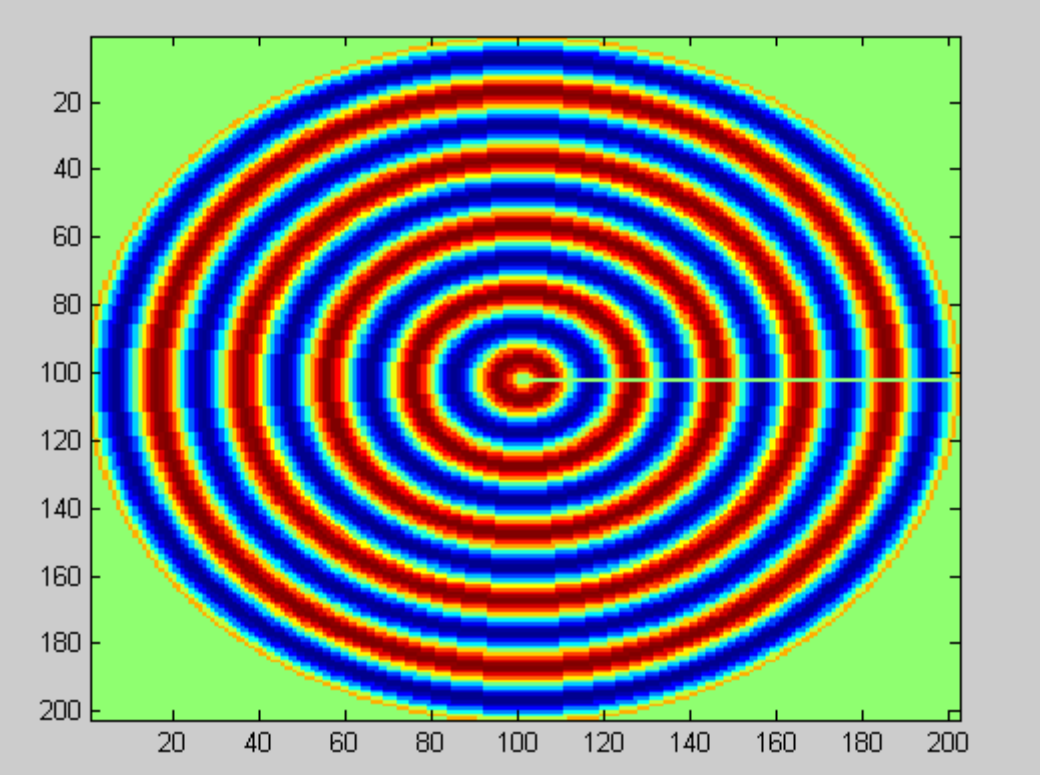


Figure 5.1: Single element antenna broadcasting in all directions.

The next step generated similar signals with the phase and the amplitude difference. Signals are at a different location than the first signal generated. This way forms the linear array with four element.

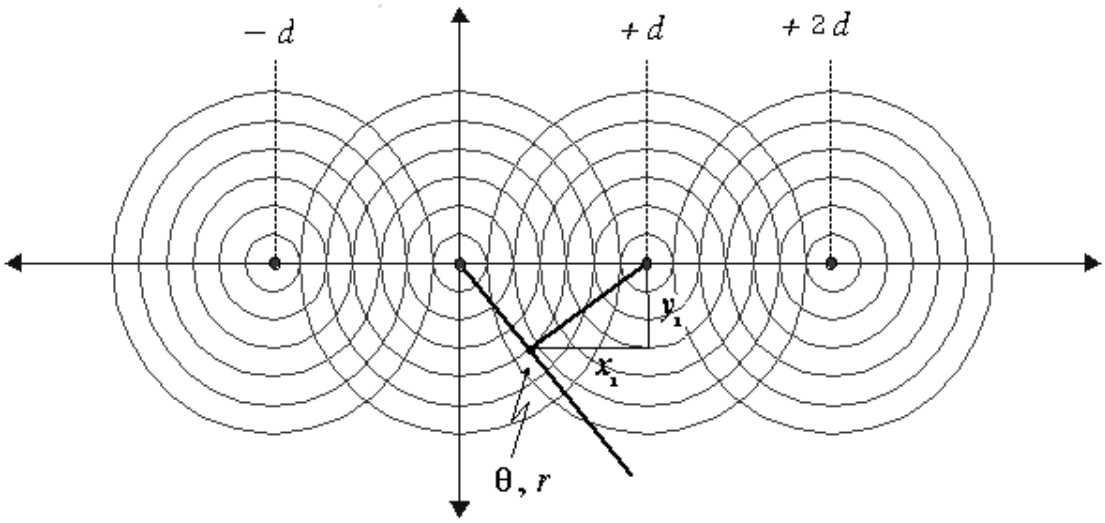


Figure 5.2: Theoretical addition of the signals.

From Figure 5.2 we will come up with the mathematical expression that will make it easier to generate the next beams.

$$x_1 = r \cos \theta$$

$$y_1 = r \sin \theta$$

$$r = \sqrt{x_1^2 + y_1^2}$$

$$\theta = \tan^{-1}\left(\frac{y_1}{x_1}\right)$$

After determining r and θ in terms of x and y,

$$S(\theta, r) = \sin(r) + \sin\left(\sqrt{x_1^2 + y_1^2} + \phi\right) + \ldots.$$

Then we put x and y in the place,

$$S(\theta, r) = \sin\left(\sqrt{(r\cos\theta - d)^2 + (r\sin\theta)^2} + \phi_1\right) +$$
$$\sin\left(\sqrt{(r\cos\theta)^2 + (r\sin\theta)^2} + \phi_2\right) +$$
$$\sin\left(\sqrt{(r\cos\theta + d)^2 + (r\sin\theta)^2} + \phi_3\right) +$$
$$\sin\left(\sqrt{(r\cos\theta + 2d)^2 + (r\sin\theta)^2} + \phi_4\right)$$

Using the formulas we generated the beams in the same way that we generated the single element antenna signal. We took advantage of Matlab commands to generate images from the matrix. Figure 5.3 shows the beams that we generated.

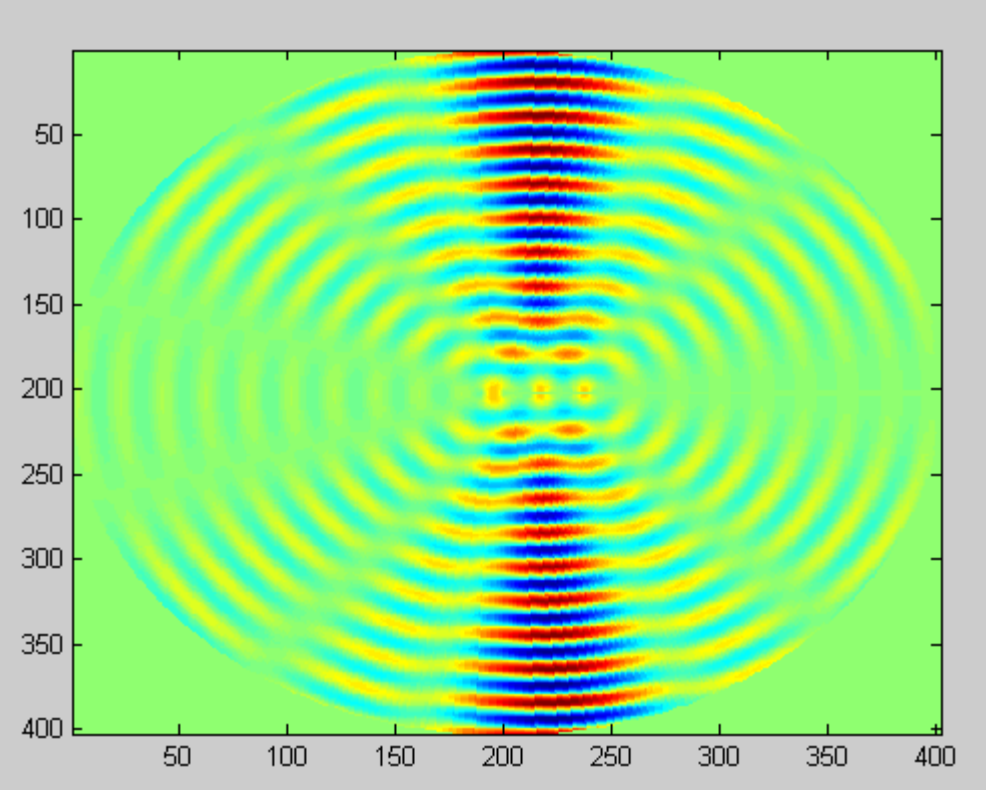


Figure 5.3: Four-element antenna array.

In Figure 5.3 we can see the beamforming. In this Matlab code I used a generic beamforming technique. In this setup there are four antenna elements that are placed 7.25 cm apart from each other and lined up on the horizontal axis. The frequency is 2.4 Ghz and the phase difference is zero. This is a sin wave to see the beamforming. At this point we generate single bits to get the image. In actual simulations we used 16-Qam signals carrying four bits in a signal. The 16-Qam signal would be impossible to put in an image because of its imaginary part.

The next step is to generate the actual beamforming, which is used in the smart antennas using the array weighting and different phase differences, as it is required to steer the beam.

5.3 Beam Steering

In the previous section is a presentation of the generic beamforming of the simple sinus waves. We used uniformly weighed array. We could steer the mainlobe to any desired direction of interest, but we still experience the problem of relatively large side lobes. That is why we are going to use weighted arrays to minimize the undesired side lobes and maximize the efficiency of the antenna by using more power for the mainlobe.

In general, any array can be steered to any direction by using phase shifters in the hardware or by digitally phase shifting the data at the back end of the receiver. In this case, we could easily give phase shift to the signals to direct the data to point the beam to a specific direction. The most general case for the array directivity is defined by Gross in Smart Antennas for Wireless Communications, the element-to-element phase shift δ in terms of the steering angle θ0 [2].

$$D(\theta, \theta_0) = \frac{4\pi \left(\frac{\sin\left(\frac{N}{2}(kd(\cos\theta - \cos\theta_0))\right)}{\frac{N}{2}(kd(\cos\theta - \cos\theta_0))} \right)^2}{\int_0^{2\pi} \int_0^{\pi} \left(\frac{\sin\left(\frac{N}{2}(kd(\cos\theta - \cos\theta_0))\right)}{\frac{N}{2}(kd(\cos\theta - \cos\theta_0))} \right)^2 \sin\theta \, d\theta \, d\phi} \quad \textbf{[2]}$$

We used the equation above to find the directivity of the antenna in our simulation. We direct both beams to each other, so the point of interest is constant for this simulation.

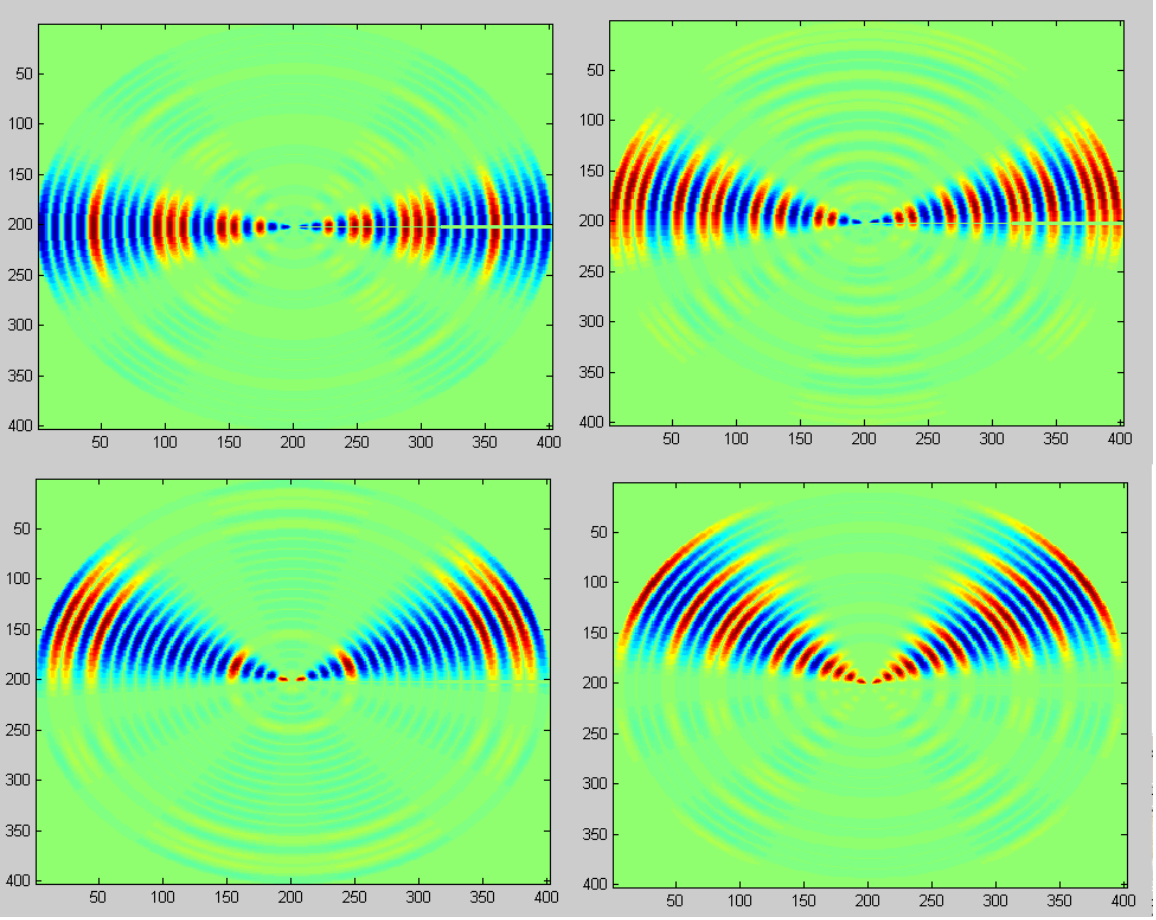


Figure 5.4: Beam directivity θ = 0, 10, 20, 30 respectively.

Figure 5.4 shows the randomly generated signals that are pointed in different angles. In this figure we did not include the fading parameter. The next step would be to add the fading to get a realistic channel model in the computer environment. When we add the realistic fading parameters to the signal it is not visible on the computer image, so that visual is not included. The path loss of the signal is calculated by Hans Steyskal in Digital Beamforming Antennas-An Introduction, with the following free space path loss equation.

$$\mathrm{FSPL(dB)} = 10\log_{10}\left(\left(\frac{4\pi}{c}df\right)^2\right)$$

5.4 Mapping Signals in Two-dimension

According to the theoretical model, we have the transmitter and the receiver 100 meter apart from each other. Therefore we generated two signals for each transmitter and receiver. Each signals is generated in a single matrix, which are placed 100 meters apart and added together. We generated the signals, which are added to each other, to have a 100-meter range. Figure 5.5 shows the visual illustration of the signals.

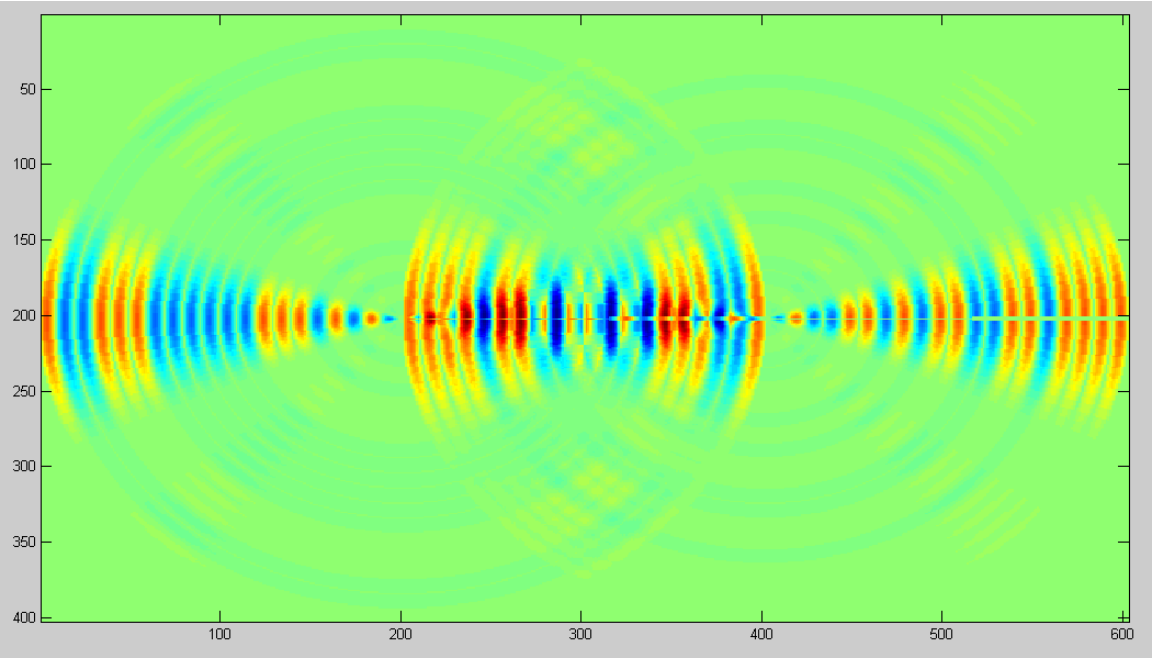


Figure 5.5: Snapshot of two signals on the map.

From Figure 5.5 we can see some cancelling of two signals that would not be recovered by the eavesdropper. In this image we still use no modulation, but we used 16-Qam signals for the actual results with attenuation included. This is only a snapshot of the signals at a moment. We need to find out if the BER, bit error rate, of the signal is under the acceptable level of recoverable signal.

At this simulation we see the amplitudes of the signals but we needed to find a measure of recoverability. We can obviously see that noise signal would make an efficient security tool, but we needed to find solid proof.

For the BER calculation the signal pattern that you can see from Figure 5.5 would not work. It is not impossible to calculate the BER map from the amplitude pattern, but it would require very high processing speed and memory. To ease our calculation I switched my map to the SNR map.

The SNR map is calculated in a similar way that we calculated the amplitude pattern map. The fist step is to generate a power pattern map of the transmitter. I started with the transmitter power, which is 23dbm, and antenna gain is 6dbi. I have another 6dbi gain that comes from the 16-Qam. The white gaussian noise is added to every pixel on the map which has an average power of –95dbm. Therefore three equal size maps are generated to calculate Eb/No value. First is the signal map, which is propagating from the right side of the map. Second is the noise signal from the receiver, which is very similar to the first except this one is on the left side of the map. The last is the noise map that is everywhere on the map. We generated three maps so that two of them will be considered as noise in a similar way. Two noise maps are added to each other and divide the signal map to calculate the Eb/No map. We used the Eb/No map to calculate the BER for the 16Qam.

5.5 16-Qam BER Calculation

The Qam scenario is the modulation technique where a signal carries multiple bits. In this case we will look at the 16-Qam modulation that carries 4 bits for each signal. Each level of the constellation point can represent Log2(16) = 4 bits. In this simulation two bits will be represented by a real number and the other two will be represented by imaginary numbers.

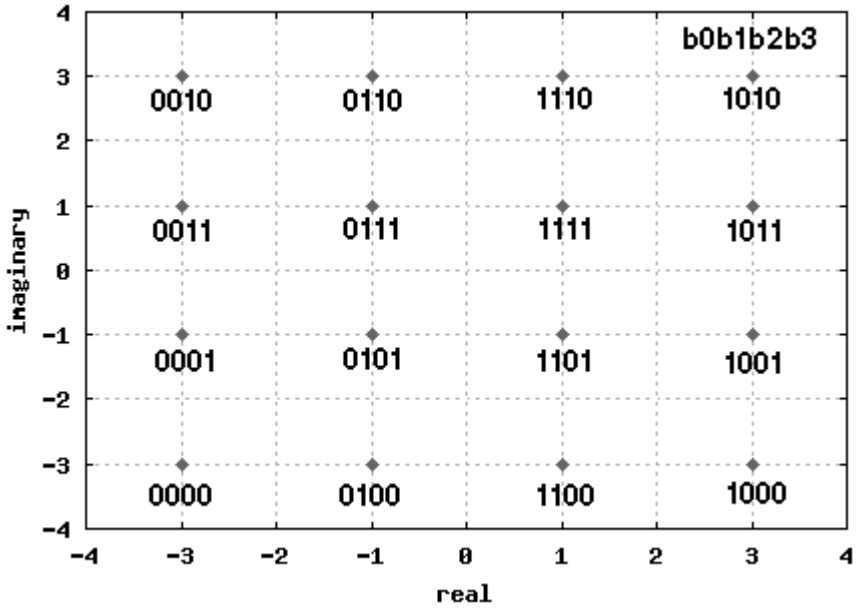


Figure 5.6: Gray code mapping for 16-Qam [15].

It is shown in Figure 5.6 there are four levels of amplitude for each real and imaginary part of the signal. When we randomly generated the bits we gave the proper amplitude for the signal for every four bits. Then we add the proper level of noise that we calculated from the SNR map and recovered the data and calculated the BER.

Chapter 6. Results

The improvement of the security level is observed from the results. The method provides the ability to hide the wireless signal in some part of the signal.

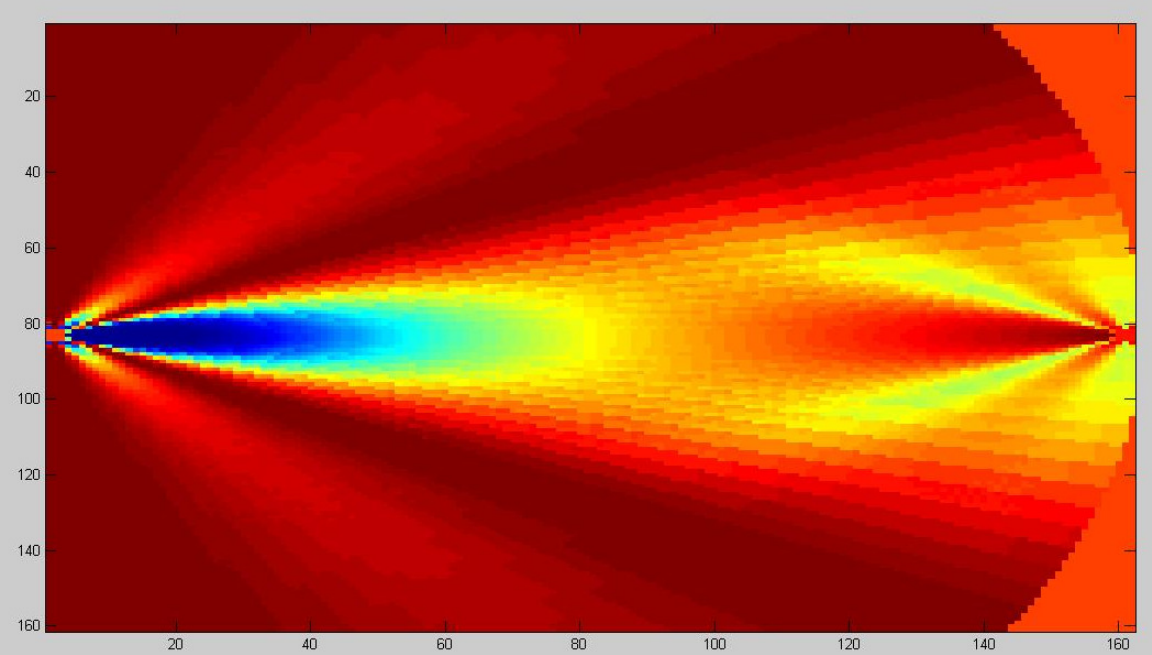


Figure 6.1: BER map of the medium.

Figure 6.1 illustrates the BER of the signal on the map. In Figure 6.1 we placed the figure about 20 meters apart. In the BER map the red color represents the areas that are safe and data is not available in those areas. The blue color is the areas which has a BER value of 0.14 or smaller. In our research we define the secure signal as the signal, which has Eb/No (db) value of 0, which means the energy per bit is equal to the noise power spectral density. Eb/No is the normalized SNR measure, which is also known SNR per bit. We used this measure for BER calculation, because the modulation technique that we used carries four bits per signal.

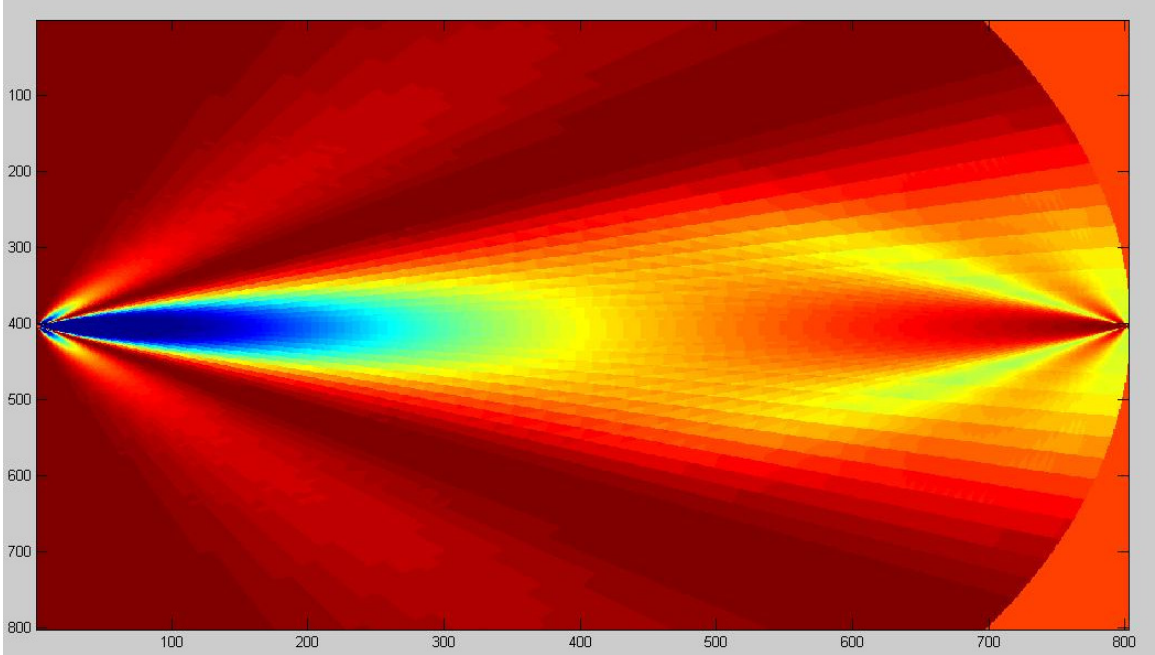


Figure 6.2: BER map of the signal at 100 meter.

Figure 6.2 is the illustration showing the behavior of the system in a long range application. In this case the insecure area is larger, but the fraction of the secure area to insecure area is very similar to the previous simulation. In this security model, the insecure area has a lower BER rate than the signal with no security.

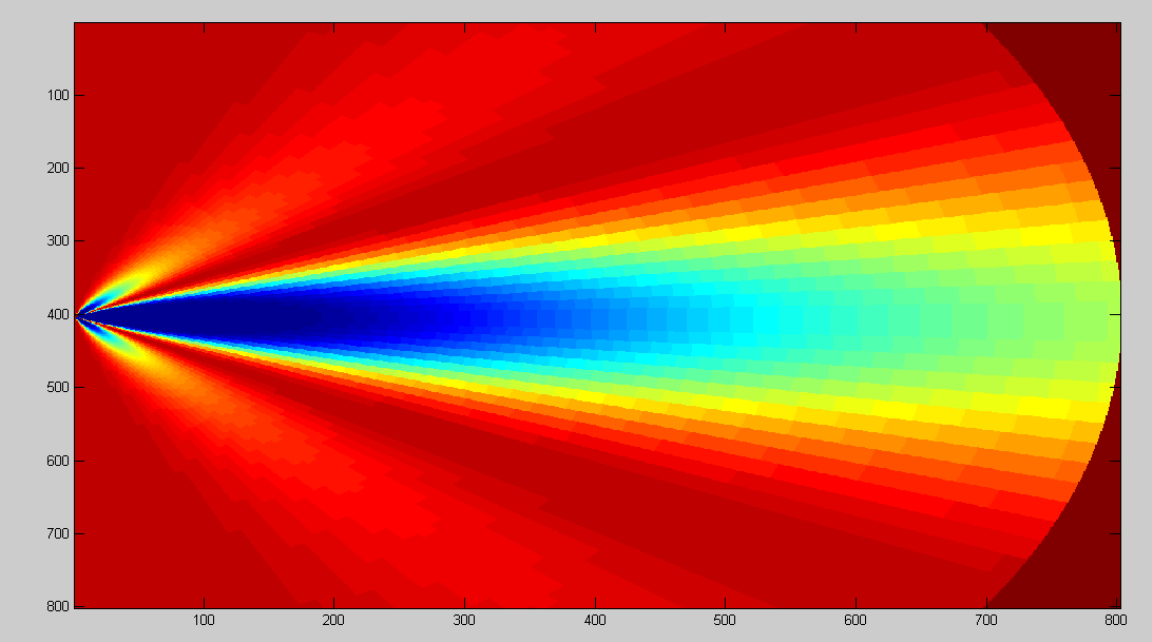


Figure 6.3: BER map of the signal without noise at 100 meter.

Figure 6.3 shows the BER map without the effect of a noise signal from the receiver. It can be clearly seen that signal quality is much better for the third party.

As a result, we see that we have improved the security level. Data is not as available as when using conventional security systems.

Chapter 7. Conclusion

In this report we have discussed the security systems and levels for the wireless systems 802.11 and introduced a new approach to improve an overall security level. The main concentration is securing the signal at the physical layer to eliminate the biggest disadvantage of the wireless communication over wired connections.

Before we explore the latest model of our system we have explained aspects of wireless security systems. First is an outline of current security systems, the weaknesses of these security systems and problems anticipated with these systems. Similar systems have been simulated like array canceling and beam overlapping, which will be discussed in the following related work section.

Although the project's model has potential for improvements, it can by itself increase security and makes data invisible throughout most of the medium. In the simulation, it is proven that the BER is very high for the eavesdroppers.

A challenge of this project was to integrate many different pieces together to get the result. We generated signals on the map; these maps are integrated to the 16-Qam signal generation technique and the beamforming is also applied to the same signal. Digital image processing is also used to picture the maps. Finally, we integrate the BER calculation for the generated map.

Another obstacle was the processing speeds of computers. This simulation requires very heavy calculations for each pixel on the map. We had more than four million pixels on the map, so we needed extra effort to get the results.

This project was very useful for learning about security systems and how each work. The project also provided firsthand experiences with wireless physical layer

simulations. By the end, I have improved programming skills and an ability to write more efficient codes. This research project improved my Matlab knowledge and experience in wireless communication.

7.1 Discussion

In this project we simulated our system in free space. In a real world environment, a variable like walls and objects could change our results. For the project, we assumed that a receiver sends the noise signal to the same direction where it receives the signals. This could leave more unsafe areas for the system.

Another concern is the effect of the noise signal at the receiver. In the free space model we assumed that the data signal is recovered without a problem because the noise signal is generated by the receiver, which already knows what signal to subtract from the received signal. On the other hand in the real world, generated noise could bounce back to the receiver from obstacles and mess up the data signal. That is why we should consider possible time-delayed noise signals when we design the receiver.

7.2 Related Work

Before we came up with the last shape of the system, we investigated two different ideas. A first project was about electromagnetic cancelling at the point of interest. A second was beam overlapping, which has two beams at the transmitter side and a data beam is partially jammed by the noise beam.

7.2.1 Electromagnetic Cancelling

Electromagnetic cancelling is a theoretical idea, which has two noise generators on each side of the transmitter.

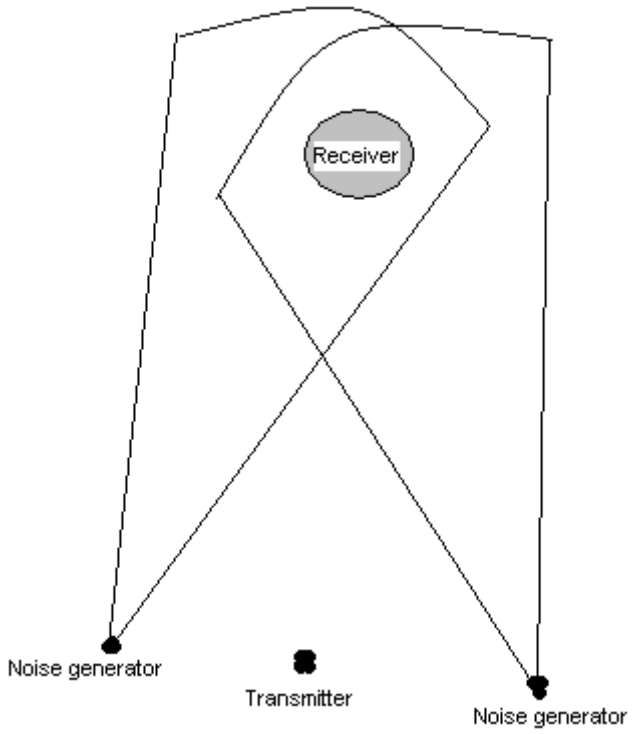


Figure 7.1: Noise cancelling.

In Figure 7.1 we can see the electromagnetic cancelling system. In this project we have two smart noise generators that can adapt their phase difference to cancel each other's signal at the point of interest. This system provides very unique security to the physical layer. It can cover the medium from the transmitter to the receiver.

What is bad about this system is the cancelling area is not as manageable as we would like it to be. In our simulation, I used same randomly generated signals with an opposite sign to each other. For example, I used signal X generated from the noise

generator 1 and signal –X generated at the noise generator 2 with the different phase differences.

As a result we saw that cancelling area is not moving most of the places as it should be. The only variable we have is the phase difference to change and we simulated the signal with all possible phase differences and saw that the cancelling area is moving in the very small portion of the range of the transmitter.

We could change the distance between the noise generators and the frequency of the signal to get the cancelling in more places, but it would not be practical and would cause different problems to change those variables.

7.2.2 Beam Overlapping

Beam overlapping is very similar idea to our main system, which is jamming part of the signal to make it invisible to the third party.

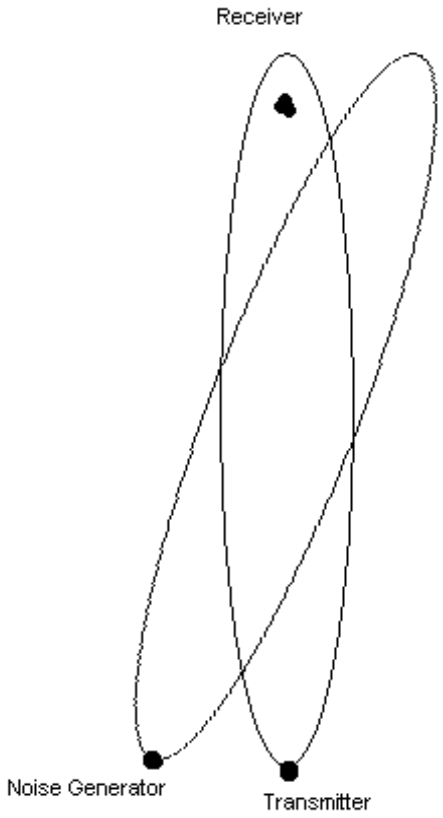


Figure 7.2: Beam overlapping system.

In Figure 7.2 we see another physical security system, which consist of two smart antennas. The first antenna is used to transmit the data, and the second one is used to generate a noise beam to jam part of the signal at the medium.

In this system the noise beam can be tuned to jam more signal at the medium. We also simulated this system for the signal quality at the receiver side. As the noise signal overlaps the data signal we could not see any significant difference with the data quality.

We put the noise beam slightly on the receiver to jam more signals and simulated for different angles of the noise beam.

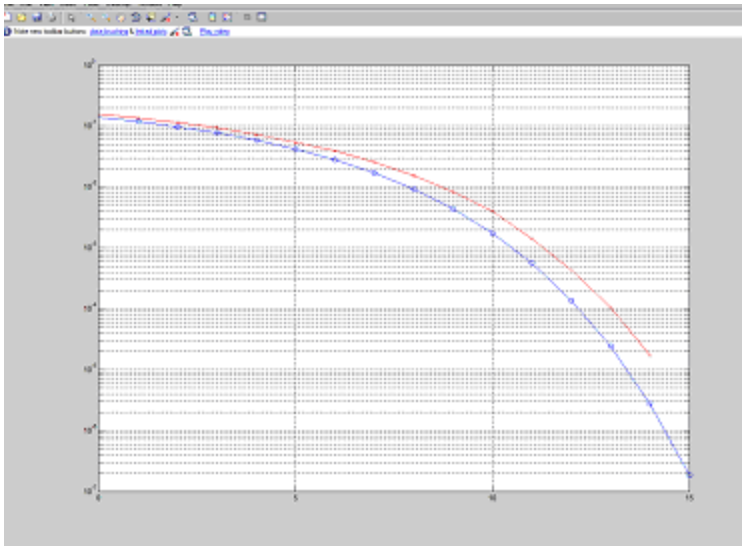


Figure 7.3: BER vs. Eb/No graph.

In Figure 7.3 the blue line shows the BER rate of the signal with no noise beam around the receiver. The red line shows the BER value of the signal with a noise beam that is partially on the receiver. In this graph the receiver is exposed to one-fourth of the peak amplitude of the noise beam. As two beams overlap more, the performance gets worse.

As a result we did not make any further research about this system and left it at this point. This system can also be used with the main system like a hybrid system to get closer to perfect security.

Chapter 8. Future Works

In this project we summarized the BER for the eavesdropper. After further investigation, we can also find out the effects of the noise to the signal quality at the receiver.

The 16-Qam signal is used for the noise signal. Using the same kind of signal does not necessarily mean that the signal will be jammed the best way it could. We could improve the jamming by working on coding techniques and different modulation schemes.

In our system we send the noise signal from the receiver. With the effect of the attenuation, the noise signal becomes weaker close to the transmitter. The data beam is not hidden at the places that are close to the transmitter. In future work, we could add another noise signal, which is generated by the transmitter, and investigate the effects on both the eavesdropper and the transmitter. This noise beam would be picked to have much less range and more power at close areas.

References

[1] Proxim Wireless. 2003. Wireless Network Security, ORiNOCO security white paper. http://www.sparcotech.com/Proxim%20Wireless%20Security.pdf.

[2] Gross, Frank. 2005. *Smart Antennas for Wireless Communications: With MATLAB*. New York: McGraw Hill.

[3] Steyskal, H. "Digital Beamforming Antennas - An Introduction" *Microwave journal*. Vol. 30. 1987.

[4] Howels, P., "Intermediate Sidelobe Canceller," U.S. Patent 3202990, Aug. 24, 1965.

[5] Applebaum, S., 1966. *Adaptive Arrays*. Syracuse University Research Corporation.

[6] Perrig, A and J.D. Tygar. 2003. *Secure Broadcast Communication in Wired and Wireless Networks*. Norwell, Massachusetts.: Kluwer Academic Publishers.

[7] Walker, Jesse, Intel Corp. whitepaper November 2000. "Unsafe at any Key Size: an analysis of the WEP encapsulation," http://md.hudora.de/archiv/wireless/unsafew.pdf.

[8] O'Neil Product Development Inc. January 2009. "The Importance of Enhanced Security and Encryption Protocols for Wireless Hardware," http://www.oneilprinters.com/Documents/RMS_%20Product_%20Announcement.pdf

[9] Gast, Matthew. 2002. *802.11 Wireless Networks: The Definitive Guide: Creating and Administering Wireless Networks*. Sebastopol, California.: O'Reilly Media.

[10] Skolnik, M., "System Aspects of Digital Beam Forming". Naval Research Lab report, June 28, 2002.

[11] Liberty, J., and T. Rappaport, 1999. *Smart Antennas for Wireless Communications*, New York: Prentice Hall.

[12] Hewlett-Packard Development Company. September 2003. "Executive Briefing: Wireless Network Security," http://docs.hp.com/en/T1428-90017/T1428-90017.pdf.

[13] Rysavy Research. December 2007. "Security Requirements for Wireless Networking," http://www.rysavy.com/Articles/2007_12_rysavy_research_security_white_paper.pdf.

[14] Edney, John and William A. Arbaugh. 2004. *Real 802.11 Security Wi-Fi Protected Access and 802.11i*. Boston: Addison Wesley Publishing.

[15] Sankar, Krishna. June 2008. "DspLog Signal Processing for Communication. Binary to gray code for 16-Qam," http://www.dsplog.com/2008/06/01/binary-to-gray-code-for-16Qam.