Study of Physical Layer Security in Wireless Communications

Mandeep Sarangal

251000108

University of Western Ontario

**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.

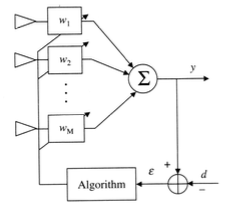


Figure 1.1 (a) Traditional Array

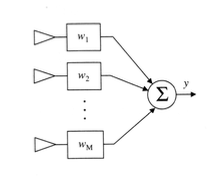


Figure 1.1 (a) Smart Array

**Wireless Security Systems**

In following paragraphs, 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.

**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.

**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.

**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.