Study of Physical Layer Security in Wireless Communications

Mandeep Sarangal

251000108

University of Western Ontario

**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.

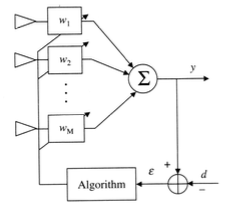


Figure 1.1 (a) Traditional Array

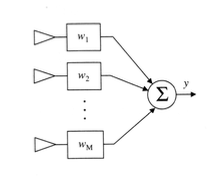


Figure 1.1 (a) Smart Array

**2. 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.

**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.

**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.

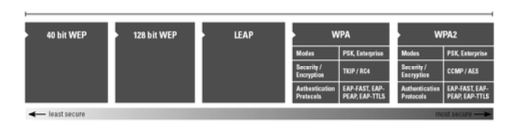
****

Figure 2.1: Encryption Systems

**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 stricter 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.

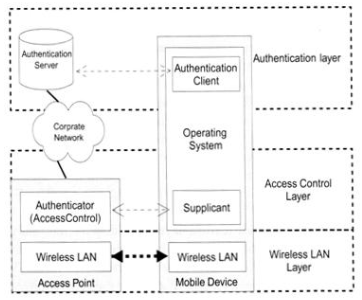


Figure 2.2: Relationship of layers

**3. 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.

This project focuses on Physical layer security of MIMO systems as a core architecture. MIMO system is one of the main LTE technologies. By using MIMO, rather than providing interference in previous telecommunications systems, multiple signals paths can be used to increase throughput. In 1995-1996, it was first proposed by Foschini [1] and Telatar [2] to improve the channel throughput effectively. The introduction of MIMO architecture has brought significant progress in the field of wireless communication systems since it improves the spectral efficiency significantly when compared to conventional systems [2]. MIMO architecture offers spectrum effectiveness in communications by utilizing the degrees of spatial freedom supplied by multiple transmit and receive antennas, such that the transmission rate and quality of communications can be improved. It has attracted worldwide attention in recent years since it improves systems throughput significantly without transmit power or bandwidth increase.

MIMO architecture offers spectrum effectiveness in communications by utilizing the degrees of spatial freedom supplied by multiple transmit and receive antennas, such that the transmission rate and quality of communications can be improved.

The information-theoretic physical-layer security in wireless communications has been exploited to face new challenges on conventional security measures such as cryptography and improve the overall security for wireless communications [3]. Unlike the conventional security techniques, the physical-layer security utilizes the physical-layer characteristics of wireless channel such as fading or noise for concealing legitimate communications without using the encryption key. Such characteristics provide structural randomness to prevent third parties from intercepting. The legitimate receiver can also benefit by exploiting the difference between the channels to legitimate receiver and eavesdropper [3].

The wiretap channel is a basic model representing the physical-layer security for communications [4]. As shown in Figure 3.1, a transmitter tries to transmit the confidential message M to a legitimate receiver meanwhile preventing the message to be obtained by the eavesdropper by stochastically encoding M into a code word Xk consisting of k symbols. Yk and Zk are output sequences for the legitimate receiver and the eavesdropper respectively, the legitimate receiver obtains estimated message M hat by decoding Yk.

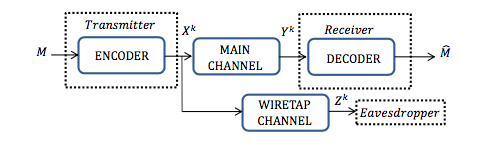


Figure 3.1: Wiretap Channel mode

Figure 3.2 shows the wiretap channel model with physically degraded assumption, where M hat can be obtained by the receiver by decoding Yk whereas Zk is a noisy version of Yk observed by the eavesdropper [3].

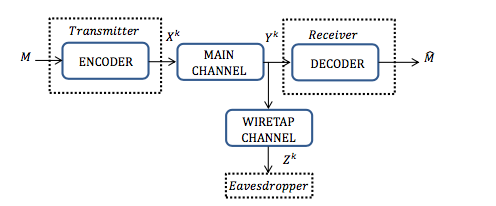


Figure 3.1: Wiretap Channel mode (degraded assumption)

The equivocation rate [3] is an important concept which quantifies how unlikely the eavesdropper to intercept valuable information in information-theoretic physical-layer security. This concept is defined as

../../Screen%20Shot%202018-03-28%20at%206.34.29%20PM.png

where ../../Screen%20Shot%202018-03-28%20at%206.36.40%20PM.png denotes the conditional entropy of random variable 𝐴 given random variable 𝐵; 𝑅𝑒 represents the normalized uncertainty of message for a given . The secrecy capacity 𝐶𝑠 is the maximum transmission rate achievable when the equivocation rate equals to the transmission rate as 𝑘 goes to infinity [3].

We focus on the secrecy issue for MIMO system. A Gaussian MIMO wiretap channel is considered where the transmitter, the legitimate receiver and the eavesdropper have multiple antennas; the signals received by the legitimate receiver and the eavesdropper are corrupted by additive white Gaussian noise (AWGN). The secrecy capacity of the Gaussian wiretap channel is lower-bounded by the difference between the capacity of the channel to the legitimate receiver and the capacity of the channel to the eavesdropper [3].

**3.1 MIMO Channel Capacity**

MIMO system provides a powerful paradigm in wireless communications. It has been observed that the channel capacity in rich scattering environments can be improved by employing the MIMO systems.

The relationship of MIMO system and practical wireless communications standards is addressed in [3]. It emphasizes some techniques and algorithms such as spatial multiplexing and space-time coding schemes for realizing the benefits of MIMO systems

The capacity formula of single user MIMO channel with and without fading is derived in [4] and later proves that the potential gains of such a MIMO system is much greater than SISO system when the noise and fades are assumed to be independent at different receiving antennas. A derivation of the capacity is given by maximizing the mutual information between input and output of the channel. The ergodic capacity of a Gaussian channel with Rayleigh fading is introduced. Each entry of this channel matrix has uniformly distributed phase and Rayleigh distributed magnitude, the capacity of such channel is achieved when the input signal is a circularly symmetric complex Gaussian variable.

Since it is difficult to evaluate the exact ergodic capacity of MIMO correlated fading channel, reference [5] focuses on evaluating the bounding techniques of MIMO capacity. The upper and lower bounds on the ergodic capacity of spatially correlated Rician MIMO channels are considered in [6], the outage capacity of such channels at high signal-to-noise ratio (SNR) is also discussed. It has been found that the upper bounds of ergodic capacity are tight at high SNR. Both ergodic and outage capacities can be affected by the antenna configuration. For the single-user system, the predicted capacity gain obtained from MIMO is based on sometimes unpractical assumptions such as the channel state information (CSI) is both known at transmitter and receiver.

**3.2 Information Theoretic Security**

Security, including confidentiality, integrity, authentication and nonrepudiation, is becoming an extremely important issue in the communication systems [3]. The confidentially, to guarantee that the legitimate receiver is able to obtain the intended information while preventing the eavesdropper accessing that information, is achieved via cryptographic encryption. The original source information is encrypted and converted by a key, including secret-key encryption algorithm and public-key encryption algorithm, from plaintext to ciphertext. The eavesdropper is able to access the ciphertext while being unable to get the decryption key to recover the original information. Using cryptography to provide the security over wireless communication networks meets several significant challenges because of the characteristics of the wireless network. Therefore, a new research direction based on information theory has been proposed to solve the security issues in wireless network

**3.3 Convex Optimization**

The optimization of transmitter in this thesis is based on convex optimization theory, which is introduced in [8] to [10]. It shows that the numerical results of a special class of mathematical optimization problems such as linear and least-squares problems can be solved efficiently since a reasonably complete theory for this class of problems has been found. In the last decades, new methods for solving new classes of optimization problems including semi definite problems were developed. Within a few years, numerous applications of convex optimization have been discovered. Formulating a problem as a convex optimization problem brings a lot of advantages. It allows us to efficiently and reliably solve the original problem. Reference [11] studied the robust convex optimization and [12] introduced four kinds of convexity which are weaker than strict convexity but stronger than quasiconvexity. Reference [13] discussed quasiconvex programmings. References [14, 15] investigated the central cutting plane algorithm for the convex problems. This algorithm approaches the optimum by building up a cutting plane through the center of a polyhedral approximation to the optimum to generate a series of points satisfying the KKT conditions of the problems.

**4. System Model**

**4.1 Regular MIMO Channel’s capacity**

The standard discrete-time MIMO system model is given by

../../Screen%20Shot%202018-03-28%20at%208.23.15%20PM.png

where 𝐇**=**[𝐡 ,𝐡2, ... , 𝐡𝑚] is the 𝑛 × 𝑚 matrix consisting of channel gains between each transmit (Tx) antenna and each receive (Rx) antenna; 𝐡𝑖 denotes the *i*th column of 𝐇; 𝑛 and *m* are the number of Rx and Tx antennas; **y** = [𝑦 ,𝑦2,...,𝑦𝑛]T and 𝐱 = [𝑥 , 𝑥2, ... , 𝑥𝑚]T are the vectors representing the received symbols and transmitted symbols; **n** is the vector of circularly-symmetric additive white Gaussian noise (AWGN) assumed to be 𝒞𝒩(0, 𝜎02𝐈) , i.e. independent and identically distributed in each receiver. The channel matrix 𝐇 is assumed to be known by both the transmitter and receiver.

The channel capacity of such channel is given by

../../Screen%20Shot%202018-03-28%20at%208.26.40%20PM.png

**4.2 Secrecy Capacity of Wiretap MIMO channel**

The wiretap channel is a broadcast channel where one of the receivers, the eavesdropper, tries to access information illegally. In this thesis, we are focused on passive eavesdroppers that listen to source information without modifying or injecting information [3]. Figure 4.1 shows the Wiretap channel model.

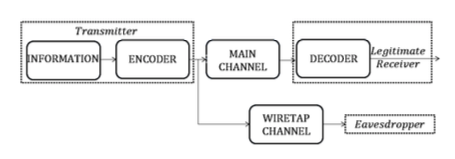


Figure 4.1: Wiretap channel model

In the Gaussian wiretap channel, the additive white Gaussian noise (AWGN) corrupts the outputs at both legitimate receiver and eavesdropper. The secrecy capacity of the Gaussian wiretap channel is given by

**../../Screen%20Shot%202018-03-28%20at%208.35.48%20PM.png**

where 𝜎2 and 𝜐2 are noise powers of the legitimate channel and eavesdropper’s channel respectively

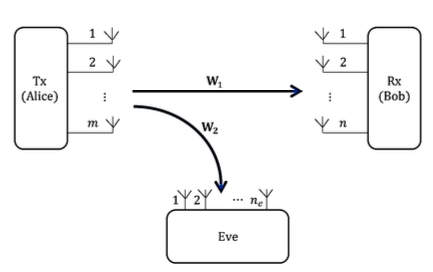
For the MIMO Gaussian wiretap channel, *ne* is the number of antennas employed by the eavesdropper. The secrecy capacity of the MIMO wiretap channel is defined as the maximized secrecy rate 𝐶𝑠(𝐑) of information can be reliably and securely transmitted subject to total transmit power.****

Figure 4.2 System model of MIMO wiretap channel.

**4.3 Summary**

With the extensive application of MIMO technology in wireless communications in this decade, the security issues of MIMO systems became a new challenge for the industry. Based on information-theoretic secrecy, the general expression of secrecy capacity of Gaussian MIMO wiretap channels has been obtained while an explicit, closed-form optimal solution is still problematic, except for some special cases. The purpose of this thesis is to discuss numerical methods for achieving the secrecy capacity of general Gaussian MIMO wiretap channels and their corresponding transmit covariance matrices.

**5. What is CVX and why it matters**

CVX is a popular modeling system for solving convex optimization problems. This modeling system is implemented in MATLAB which allows convex programs to be constructed by common MATLAB functions and operators. It is convenient to use CVX to formulate and solve convex problems such as constrained entropy maximization and determinant maximization. CVX is an important toolbox for solving the problem of optimization the secrecy capacity of Gaussian MIMO wiretap channel

**5.1 Precision of CVX**

The numerical results of convex optimization problems obtained by CVX are not exact; they are computed within a predefined numerical precision or tolerance [63]. We will not interpret this variable thoroughly since it might be different in different applications and heavily depends on how does the CVX transform problems into its solvers. While the setting of CVX precision affects the accuracy of results and processing time, we will try to find the proper CVX precision so that the accuracy and processing time are both acceptable.

The optimization problem to be processed and solved by CVX is given as:

../../Screen%20Shot%202018-03-28%20at%208.50.46%20PM.png

Covariance matrix 𝐑 is the variable of this problem and has to be positive semi-definite. Based on the total power constraint, Tr(𝐑) representing the total input power cannot be greater than 𝑃𝑇 . Note that as mentioned in the last chapter, the noise power 𝜎2 is set to be 1 so that SNR is equivalent to 𝑃𝑇*.* For the given 𝐖, the capacity and corresponding optimal covariance matrix 𝐑 can be obtained by CVX. The accuracy of the result is controlled by the CVX precision variable. We chose some channel matrixes which have different characteristics to verify the impact of CVX precision variable.

The MATLAB code of this problem is given as follows,

rho=10^(SNRdB/10); % SNR in linear domain

cvx\_begin; % CVX begins

cvx\_precision( ); % set CVX precision, can be 10-1, 10-4, 1016

variable R(m,m) symmetric; % define variable (covariance matrix)

R == semidefinite(m); % R has to be positive semidefinite

C= log\_det(eye(m)+W\*R);

maximize C;

0<=trace(R)<= m\*rho; % Tr(R) is less than total transmit power

cvx\_end; % CVX ends

**5.2 Summary**

CVX is a good numerical toolbox to compute the MIMO channel capacity and corresponding optimal transmit covariance matrix for a given channel matrix. Since the optimization problem for secrecy capacity of the Gaussian MIMO wiretap channel is not concave unless 𝐖 − 𝐖2 ≥ 𝟎, (i.e. degraded channel). Even if 𝐖 − 𝐖2, CVX cannot process such objective directly neither. Other numerical methods for handling this non-convex optimization problem will be discussed in next section.

**6. Random Optimization Methods**

Barring some specific channels, the analytical solution for the optimal transmit covariance matrix of the Gaussian MIMO wiretap channel is unknown. In further sections, in order to find a numerical solution for this optimization problem, we will discuss about Monte Carlo optimization and Differential Evaluation Algorithm.

**6.1 Monte Carlo Optimization**

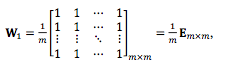
it uses statistical methods to estimate the numerical characteristics of the probability model thereby obtaining a numerical solution of practical problems. In this section, MC will be used to compute the secrecy capacity of Gaussian MIMO wiretap channel. In some cases, where *m* is large, the convergence time will be long as shown in Figures 6.1 and 6.3. In this section, we will investigate the impacts introduced by different types of channels and *m* on the speed of convergence and accuracy of results.

The optimization problem for the channel capacity for a given Gaussian MIMO channel with covariance matrix 𝐑 is formulated as

../../Screen%20Shot%202018-03-28%20at%209.49.08%20PM.png

where 𝐶(𝐑) denotes the channel transmit rate which is a function of 𝐑

We will begin with the case where the optimal transmitting is beamforming (rank(𝐑 ) = 1).



Case 6.1

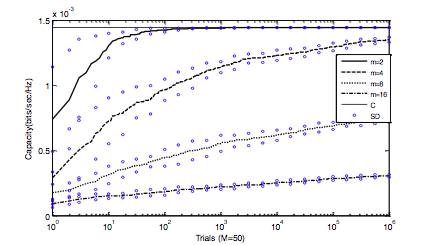


Figure 6.1, The capacity of Case 6.1 obtained by MC vs Trials (SNR = −30 dB).

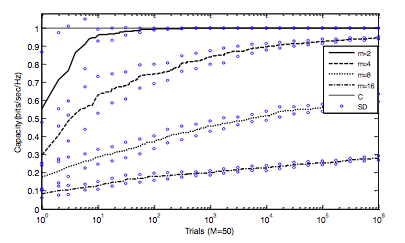


Figure 6.2, The capacity of Case 6.1 obtained by MC vs Trials (SNR = 0 dB).

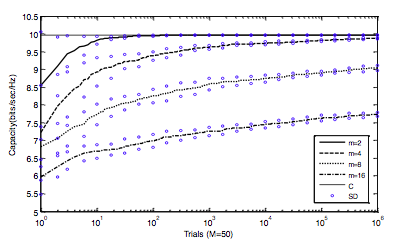


Figure 6.3, The capacity of Case 6.1 obtained by MC vs Trials (SNR = 30 dB).

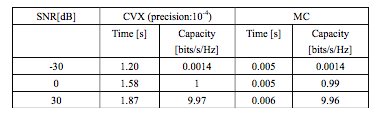


Table 6.1 The results of Case 6.1 returned by CVX and MC (𝑁 = 500, 𝑚 = 2).

As shown in Table 6.1, when *m =* 2, the capacity obtained by MC is much close to the capacity obtained by CVX, and the processing time of MC is much shorter than the processing time of CVX. Therefore, it can be concluded that MC optimization is the better method for computing the capacity of a MIMO channel when the number of antennas is small.

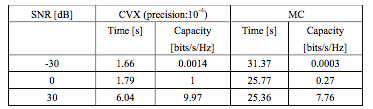


Table 6.2 The results of Case 6.1 resulted by CVX and MC (𝑁 = 106, 𝑚 = 16).

However, in Table 6.2 where *m* is large, even if we increase 𝑁 to106, the performance of MC is noticeably worse than that of CVX. A possible explanation of this phenomenon is that when 𝑚 = 16, the randomly generated transmit covariance matrix 𝐑 is a 16×16 matrix whose rank has 16 possibilities; hence the probability of rank(𝐑) = 1 is much lower than that in the case where 𝑚 = 2. In other word, it is difficult for MC to find the optimal eigen direction and allocate all of the power to the optimal direction when the size of the channel matrix is large.

**Monte Carlo versus CVX (Weak Eavesdropper):**

Since CVX is not able to solve for secrecy capacity:

../../Screen%20Shot%202018-03-28%20at%2010.33.08%20PM.png

even if 𝐖 ≥ 𝐖2, we consider the scenario where the eavesdropper is weak, i.e. 𝐖2𝐑 << 𝐈. Based on the following formula,

ln|𝐈+𝐀|≈Tr(𝐀) for 𝐀 << 𝐈

the secrecy capacity 𝐶𝑠 can be approximated as

𝐶𝑠 ≈𝐶𝑎 =max{ln|𝐈+𝐖 𝐑|−Tr(𝐖2𝐑)}; s.t.𝐑≥𝟎,Tr(𝐑)≤𝑃𝑇

when 𝐖2𝐑 𝐈, i.e. λ𝑖(𝐖2𝐑) 1; 𝐶𝑎 denotes the approximated secrecy capacity and is an affine function which is both concave and convex.

In general, when the number of transmit antennas is small (*m* = 2), the secrecy capacity can be approximately obtained faster and more accurately using MC. We can conclude that Monte Carlo optimization is a good algorithm to approximately compute the secrecy capacity when *m* is small and that MC is more efficient than CVX. However, MC performs worse as *m* increases, and increasing the number of trials does not improve the results significant but instead takes enormous amount of processing time. Compared to MC, CVX is able to solve the optimizations approximately in low SNR regime regardless of *m.* While the results obtained by CVX in high SNR regime can only be considered as the lower bound of the secrecy capacity of a given channel. Neither Monte Carlo nor CVX can handle the optimization problems for secrecy capacity of a Gaussian MIMO wiretap channel properly when *m* and SNR are both large. We will discuss other methods for obtaining the numerical results in the following sections.

**6.2 Differential Evaluation**

For the cases where the number of transmit antennas is large, the efficiency and the accuracy of the Monte Carlo optimization is extremely low. Hence, we will apply the differential evolution (DE) algorithm to see if it is able to improve the efficiency and the accuracy of the results.

There are three main steps which are *Mutation*, *Crossover* and *Selection*. More specifically, mutation is for generating new parameter matrices, called mutant matrices, by adding the scaled difference between two population matrices to a third population matrix, called target matrix. In the step of crossover, the trial matrix is generated by mixing the parameters of mutant matrix and the parameters of the predetermined target matrix in order to increase diversity. The trial matrix is compared with the target matrix by estimating the values of objective function yielded by them respectively. If the trial matrix yields a better objective function value than target matrix, then the trial matrix is decided to be a member of the following generation, otherwise, the target matrix is retained.

**6.3 Summary**

We discussed the Monte Carlo optimization for achieving the numerical results of the optimization problem for the secrecy capacity of a given Gaussian MIMO wiretap channel. We found that Monte Carlo is able to approximately obtain the secrecy capacity for the cases where *m* is small. When *m* is large, it is difficult for Monte Carlo to converge to the accurate results especially when 𝐑 has a low rank. The value of SNR does not affect the convergence. We also discussed the approximation of the optimization problem for the MIMO wiretap channel with weak eavesdropper which can be processed by CVX. By comparing the results obtained by Monte Carlo with results obtained by CVX, we found that CVX is able to return relatively accurate results when SNR is low.

**7 Case of Weak Eavesdropper**

**7.1 Weak Eavesdropper Approximation**

As shown before, the disciplined CVX does not process secrecy rate function 𝐶𝑠(𝐑) of the Gaussian MIMO wiretap channel as objective since it is not always concave. In Chapter 5, we considered the scenario where 𝐖2𝐑 𝐈 such that an approximation for weak eavesdropper can be implemented.

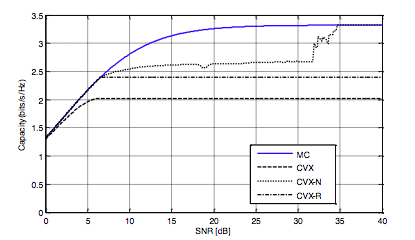
In such scenario, which is:

../../Screen%20Shot%202018-03-29%20at%203.40.45%20PM.png

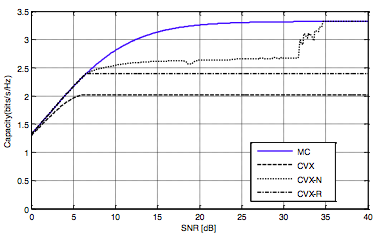
can be approximated by 𝐶𝑎 as

**../../Screen%20Shot%202018-03-29%20at%203.41.27%20PM.png**

**../../Screen%20Shot%202018-03-29%20at%203.43.45%20PM.png** Case 7.1



**Figure 7.1** Secrecy capacity of Case 6-1 obtained by different methods vs SNR, CVX precision = 10−4.



**Figure 7.2.** Secrecy capacity of Case 6-1 obtained by different methods, CVX precision=10− 16.

Observing Figures 7.1 and 7.2, even if the CVX-N curve is oscillating, it still has a better performance than using 𝐑cvx (CVX-R) directly. In Figure 7.2, the CVX precision variable is set as 10-16, which means that the solver of CVX continues as long as it reaches a lower tolerance level. Comparing Figures 7.1 and 7.2, enhancement of CVX precision variable cannot eliminate the oscillation.

***Adjustment of Approximation for Weak Eavesdropper:***

We will use the channel matrices of Case 7.1. For the purpose of convenience, we set 𝑚 = 2. The properties of this channel model are given in Table 7.1. Since 𝐖 and 𝐖2 both have the same eigenvectors, based on the previous discussion, 𝑟+(𝐖 −𝐖2)=1→𝑟+(𝐑 )=1, 𝐑 =𝑃𝑇 ∙𝐄/2, where 𝑟+(𝐀) is the number of positive eigenvalues of 𝐀.

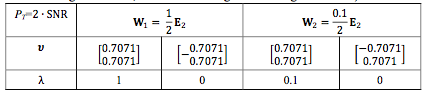


Table 7.1 The channel model of Case 6-1 (*m* = 2) (𝝊 denotes the eigenvectors of given matrix; λ denotes the eigenvalues of given matrix).

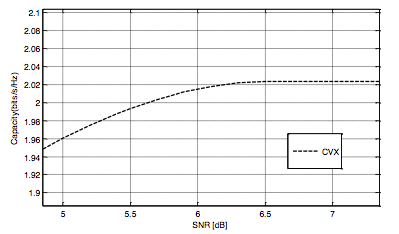


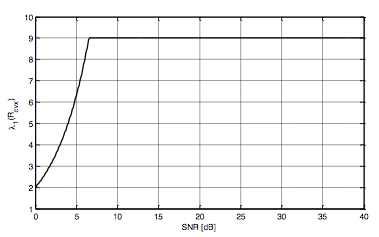
Figure 7.3 Saturation point and upper bound of approximated secrecy capacity of Case 7.1.

After SNR = 6.53 dB, the optimal covariance matrix 𝐑cvx returned by CVX has the following properties:

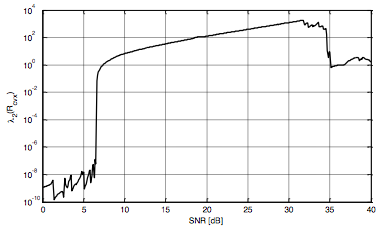
../../Screen%20Shot%202018-03-29%20at%203.58.31%20PM.png

Table 7.2 Eigenvectors and eigenvalues of 𝐑cvx (SNR ≥ 6.53 dB).

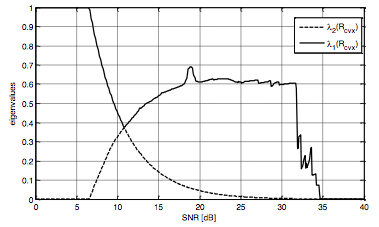
We can then observe that the power transmitted to 𝝊 (𝐑cvx) is fixed at 9 while the power transmitted to 𝝊2(𝐑cvx) jumps between [0,𝑃𝑇 −9] with the variety of SNR. The relationships of SNR with λ (𝐑cvx) and λ2(𝐑cvx) are indicated in Figures 7.4 − 7.6, thus proving our conclusion above.



**Figure 7.4.** λ (𝐑cvx) vs SNR of Case 7.1 (Tr(𝐑) ≤ 2 SNR).



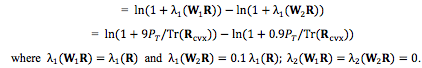
**Figure 7.5.** λ 2(𝐑cvx) vs SNR of Case 7.1 (Tr(𝐑) ≤ 2 SNR)



**Figure 7.6.** Eigenvalues of 𝐑cvx normalized by 𝑃𝑇 (𝑃𝑇 = 2 SNR).

Therefore, if we substitute modified 𝐑cvx as 𝐑 = 𝑃𝑇 ∙ 𝐑cvx/Tr(𝐑cvx) into 𝐶𝑠(𝐑) given in (7.1), the secrecy capacity is given as

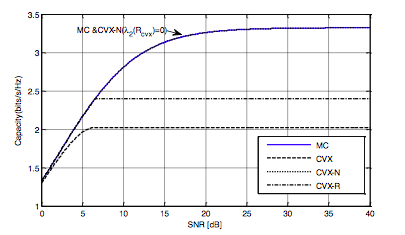
../../Screen%20Shot%202018-03-29%20at%204.04.24%20PM.png



Note that (7.5) is not a monotonically increasing function of 𝑃𝑇 (SNR) and PT/Tr(𝐑cvx) is not a constant. These two factors contribute to the oscillation of curve CVX-N shown in Figure 6.1. Figure 6.6 shows λ (𝐑cvx) /𝑃𝑇 and λ 2(𝐑cvx) /𝑃𝑇.

**A room for Improvement**

Observing (6.5), for a given SNR (𝑃𝑇), 𝐶𝑠 is affected by Tr(𝐑cvx) only which equals to λ (𝐑cvx) + λ2(𝐑cvx). In Case 6-1, λ (𝐑cvx) is fixed at 9 when SNR ≥ 6.53 dB while λ2(𝐑cvx) can float in an interval (shown in Figure 7.2), so that the solutions of this case are non-unique and CVX selects only one of them. This is a possible explination of the oscilations appearing in Figures 7.1 and 7.2. Hence if we manually enforce λ2(𝐑cvx) to zero, (7.5) tends to its maximum value, which coincides with the secrecy capacity obtained by Monte Carlo (Figure 7.7).

****

**Figure 7.7.** Improved result obtained by enforcing λ2(𝐑cvx) = 0.

**7.2 Summary**

We discussed the approximation formula for weak eavesdropper of Gaussian wiretap MIMO channel secrecy capacity that is accepted by CVX and we concluded that CVX is not able to solve it properly since it cannot return the correct optimal eigenvectors of the covariance matrix.

**References**

[1] G. J. Foschini, Layered Space-Time Architecture for Wireless Communication in a Fading Environment when using Multiple Antennas, *Bell Lab*, *Tech.* J., V. 1, N. 2, pp. 41-59, Oct. 1996.

[2] I. E. Telatar, Capacity of Multi-Antenna Gaussian Channels, *AT&T Bell Lab. Internal Tech. Memo*., Jun. 1995.

[3] Y. Liang, H. V. Poor, S. Shamai(Shitz), Information Theoretic Security, *Found. and Trends in Commun*. *and Info. Theory*, V. 5, N. 45, 2008, pp. 355-580.

[4] D. Hofheinz, E. Kiltz, Secure Hybrid Encryption from Weakened Key Encapsulation, *Crypto*’ *07*, *LNCS*, Santa Barbara, CA, USA, Aug 2007, pp. 553–571.

[5] Q. T. Zhang, X. W. Cui, X. M. Li, Very Tight Capacity Bounds for MIMO-Correlated Rayleigh-Fading Channels, *IEEE Trans. Wireless Commun*., V. 4, N.2, pp. 681-888, Mar. 2005.

[6] M. R. McKay, I. B. Collings, General Capacity Bounds for Spatially Correlated Rician MIMO Channels, *IEEE Trans. Info. Theory*, V. 51, N. 9, pp. 3121-3145, Sep. 2005.

[7] A. Goldsmith, S. A. Jafar, N. Jindal, S. Vishwanath, Capacity Limits of MIMO Channels, *IEEE J. Select. Areas Commun.*, V. 21, N. 5, pp. 684-702, Jun. 2003

[8] S. Boyd, L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.

[9] D. P. Bertsekas, A. Nedic, A. E. Ozdaglar, *Convex Analysis and Optimization*, Belmont, MA: Athena Scientific, 2003.

[10] J. B. Hiriart-Urruty, C. Lemarechal, *Fundamentals of Convex Analysis*, New York: Springer, 2001.

[11] A. Ben-Tal, A. Nemirovski, Robust Convex Optimization, *Math. Operat. Res*., V. 23, N.4, pp. 769–805, 1998.

[12] J. Ponstein, Seven Kinds of Convexity, *SIAM Rev*., V.9, N.1, pp.115–119, Jan. 1967.

[13] D. G. Luenberger, Quasi-Convex Programming, *SIAM J. Applied Mathematics*, V.16, N.5, pp. 1090-1095, Sep. 1968.

[14] J. E. Kelley, The Cutting-Plane Method for Solving Convex Programs, *J. Soc. Industrial and Applied Mathematics*, V.8, N.4, pp. 708–712, 1960.

[15] J. Elzinga, T. G. Moore, A Central Cutting Plane Algorithm for the Convex Programming Problem, *Math. Programming*, V.8, pp.134–145, 1975