Study of Physical Layer Security in Wireless Communications

Mandeep Sarangal

251000108

University of Western Ontario

**1. Introduction**

For past couple of decades, Computer technologies have become a very integral part of people’s lives. Wireless networking is a big part of computer market today. This is understandable as wireless technology has very many advantages over traditional wired systems.

Computer hardware is getting smaller day by day as the technology is getting better. Wireless technology also gives comfort, mobility and all other kinds of conveniences.

In the early stages of wireless networking devices, extensive use of infrared wavelengths was made for transmission over a medium. As the technology advanced, use of radio waves became more popular. Radio waves have better penetration behavior. Also, an important parameter for user satisfaction is coverage and radio waves provide a better coverage.

Using modulation and digital signal processing techniques, new research is being done to improve the coverage of wireless networks

Quality of service was also an important parameter. Diversity systems were used up until 2004 in order to provide better quality of service. Diversity Systems consist of several number of transmitters and depending on the specific time and location, the most efficient transmitter is chosen.

A more sophisticated diversity system is the one that can make use of multiple antennas at the same time. This is also called MIMO, Multiple Input Multiple Output systems. Using MIMO, the throughput increases drastically as compared to the systems that use only a single antenna. MIMO also helps resolve multipath interference issues. In order to transmit data simultaneously, several digital signal processing techniques are being made better to improve performance. Data quality is also being improved for the same reason.

Using multiple antenna systems, a new digital signal processing technique can be introduced which is called beamforming. In order to point the Radio Frequency signal in a specific direction, Beamforming can be used. In this kind of setting, it is required that all the antennas should use the same coding. Beamforming mode allows the antennas to tune the phase in a way that results in changing the 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 much larger than the number of receiving antennas. If the number of spatial streams are assigned to the antennas according to a set of rules, data is recovered using advanced digital signal processing.

Another name of MIMO is Smart Antenna system. This is because of MIMO system’s 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.

The following paragraphs will include a summary of the background of wireless security systems. Before going into the implementation part of the security system, the report will cover wireless security systems, smart antennas and channel models.

A sophisticated algorithm is used inside multiple antenna systems, also called smart antenna systems, in order to adapt to the environment and signal interference. Simple adaptive arrays can be converted to adaptive beam arrays. These switched or converted beam arrays provides a choice to the receiver to select the signal from depending upon which signal provides best performance and minimum interfering noise. Adaptive arrays are well aware of the interfering signals and regardless of that they can steer a beam towards the target point. All smart antenna systems used today are mostly adaptive arrays.

Since adaptive arrays are getting much more advanced and sophisticated when compared to simple switched beam array, as a result, fixed beam systems are not recognized as smart antennas anymore. Figure 1.1 shows the difference between adaptive and switched beam antenna arrays.

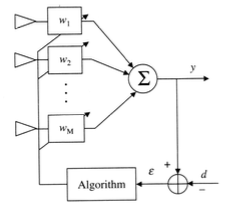


Figure 1.1 (a) Traditional Array

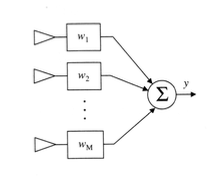


Figure 1.1 (a) Smart Array

**2. Wireless Security Systems**

In following paragraphs, the discussion focuses on current wireless security systems and the challenges of security. Sometimes the data being transmitted is very sensitive and private and hence the wireless security becomes vital for those critical data types. We will cover topics like 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**

Authentication is a feature provided by most access points on the hardware. The connection is authenticated by MAC layers, in a way that only the registered MAC addresses can connect to a network. The process of authentication is done by checking the MAC layer address of the connection attempted. This process is liable to an attack for two reasons.

Firstly, MAC addresses can be edited in some hardware, so duplication of a MAC layer of an authenticated user is possible and can be used to provide access to a network.

Secondly, authentication is controlled by hardware. So the danger is held by the fact that hardware can always be stolen, and an illegal access can be provided to a network.

Access points can verify a user through authentication, but an access point can’t be authenticated by a user. Authentication of this kind is dangerous as information about all the users in a network can be accessed by a user.

**Encryption**

WEP is one of the early encryption policies in wireless communication. WEP as an encryption policy is still used most commonly despite the fact that WEP encryption networks aren’t counted as safe networks nowadays. VPN mechanism or Virtual Private Networking is a second gen encryption system.

WEP encryption does have its weaknesses. Because of an inadequate initialization vector, WEP encryption has the probability of being decodable. Because security experts have realized that WEP is not the strongest of networks in terms of safety and security, an attempt to rectify the problem has been made by adopting an improved WEP encryption in 802.11B products. The process of WEP encryption involves a transmitter transmitting the initialization vector and the instructions are simply followed by the user.

Since VPN is considered to be safer than WEP encryptions, People are increasingly using VPN software as an alternative to WEP encryption. VPN promises a better encryption which is much tougher to decode by cracks.

Now days, the market is full of a variety of many more encryption policies which are used for safer data transmissions. Figure 2.1 lists out all the encryption systems being used in the market.

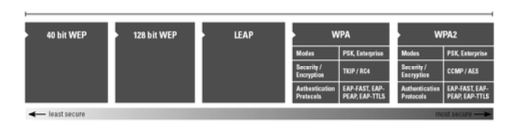
****

Figure 2.1: Encryption Systems

**2.2 Problems with Wireless Security**

The conventional data communication process entails data being transmitted through a cable. But, to avoid the wiring hassle, people are setting up access points and starting the network. This wireless system allows its users to use the network while roaming around, under the coverage of the network’s access point. However, the advantages of a wireless communication also come with security issues.

The ability to travel long distances is a radio wave’s main characteristic. It is very difficult to foresee how far it travels and in what particular direction. In case the wireless network is not secure, hackers can still record data through transmitters to process the code or collect it to analyze it in the future, despite being far away with their receivers. By doing so, it enables hackers to retrieve personal information like emails, banking information and password from their targets. Identity theft can be caused by using an unsecured internet connection.

Another security problem is that the unsecured wireless network can be accessed by any computer with similar equipment. One security problem is that any computer with the same equipment can access the unsecure wireless network. If the signal is weak for other equipment, a computer can use receivers which are more powerful to detect signals and to get into the network.

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 communication has developed more techniques to protect data. But network designers are apprehensive to use wireless networks in their designs because of their well known issues. This part of the report lists out some of the commonly faced and potential problems.

**2.2.1 Easy Access**

The network should allow any user to have access to the Wireless access points. The user can see the network before he connects to the network. For visibility, signals are broadcasted as frames called beacons by the access points. The user signal which is generated whenever a user tries to connect to a network is not encrypted. And since the signal isn’t encrypted, a third person could use the user signal to gain access to the network.

One solution can be shielding the signals by a strong wall for their protection, but it isn’t the most practical one. Also, as an authentication technique, VPN can be used.

**2.2.2 Rogue Access Points**

In many user networks, it is hard to monitor all users’ access. A similar challenge is educating the user about the security of the network. Users lack knowledge and concern about how to properly secure a wireless network. Also, despite the efforts in investing in a secure network, the network is open to easy attacks if a user who connects the wireless access point to a network.

Unfortunately, there is no easy solution to this. There are a number of techniques to identify all of the wireless signals connected to the network. One way is for the administrator to physically check the rooms to find the wireless access points. As neighboring networks may also be detected, this makes it difficult to gauge the access points connected to the owner’s network. Carrying out frequent checks in a solution to detect rogue access points, but the network administrators may not have time to carry out the checks.

**2.2.3 Unauthorized Use of Service**

It’s common for Offices and houses to have their own wireless access points now. People looking to surf the internet at their homes usually use the default settings on the wireless devices they buy. The default setting has very few restrictions, and users usually don’t even set up a key to secure their network because of convenience. Hence, there is no encryption or security whatsoever.

This can lead to two risks: unauthorized access and bandwidth issues and also challenges like legal problems.

Unauthenticated access may cause large amounts of data traffic since there are multiple computers’ data combing, despite a limited bandwidth being available. This makes the internet slow and may not work at all for applications needing a lot of bandwidth. Crowded areas, like apartment complexes see multiple unauthorized connections accessing unsecured wireless networks. 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.

Security isn’t required for all wireless networks. Many providers provide unsecured Internet access, i.e. without passwords. That means that the network is accessible to any customer in the compound, without it being a burden to the provider. In public places like these, users surf the internet at their own risk.

But for corporations and companies need to secure their wireless network with the highest level security, as the data traffic usually contains valuable or private information.

VPN provides the strongest authentication amongst the current technology. Depending on the capabilities of transport layer security, TLS, a choice of authentication methods is available to the user because of VPN. Only authenticated users can have authority to these access points. 802.1x can add security using transport layer.

**2.2.4 Service and Performance Constraints**

Wireless access points can transfer less data than wired connections. For example, 802.11b has a capacity of 11 Mbps and even the newer models have a capacity of 54 Mbps. The speed or capacity is distributed within all of the networks connected users. It is possible that router connections can be overwhelmed because of wireless’ slower speed. Some factors of an access point crossing its capacity are MAC layer overhead and local area applications. This property can often deny service attacks on limited sources.

The access point can reach its capacity in many ways. For e.g., large amounts of data can be sent from a wired network to wireless devices. Since wired connections are faster, as the data would start accumulating at the buffer of the access point, it will easily bring it to its capacity.

As the attackers may cause heavy traffic on the wireless, the network would adapt in the high traffic environment, to send the data it would use a CSMA/CA mechanism, because of which the data will wait in the buffer of the access point.

Also, because of the heavy traffic seen in wireless networks, there are huge traffic loads that leave the network 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.

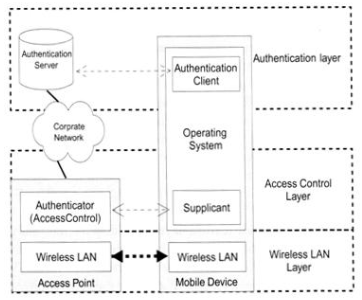


Figure 2.2: Relationship of layers

**3. Literature Review**

The traditional network securities rely on passwords or keys. There are very challenging disadvantages of conventional network wireless securities. The biggest vulnerability of wireless security is that eavesdroppers can easily see the signal in the medium.

Security systems based on secret key sharing are a big overhead over the whole network because key management becomes an issue. So with better conventional security, the overhead increases. In high number node networks, this would lead to management problems.

Given that we have so many vulnerabilities in key based security systems, we need to investigate other security solutions which do not depend on secret keys. In this project, we investigate the possibility of using noisy feedback to achieve security which does not have secrets by exploiting the wiretap channel structure and making use of a private key known exclusively to the destination or the receiver side.

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, instead of providing interference in earlier telecommunications systems, throughput is increased by using multiple signals paths. 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]. 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, MIMO architecture offers spectrum effectiveness in communications. It has attracted attention and became very popular all over the world in recent years since it improves systems throughput significantly without having to increase transmit power or bandwidth.

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 for physical layer security has been tapped into to face the challenges of traditional security involving cryptography and overall improvement of wireless security [3]. The main characteristic that differentiate this new security approach from traditional ones is the ability to use intrinsic features of the wireless transmission channel like noise or fading in order to prevent eavesdroppers from getting access to legit communications. The best part of this approach is not having to use any encryption key. The structural randomness provided by such methods prevents the illegitimate attackers from getting hold of the signal. Also, the difference between the channels of intended receiver and the eavesdropper can be used to fortify the security of the wireless transmission [3].

The wiretap channel is a model at a very basic level, representing the physical-layer security for wireless transmissions [4]. As shown in Figure 3.1, a transmitter tries to transmit the confidential message M to a legitimate receiver and at the same time preventing the message to be accessed by the eavesdropper by encoding M stochastically 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.

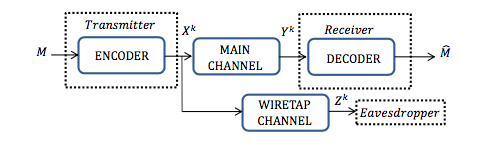


Figure 3.1: Wiretap Channel mode

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].

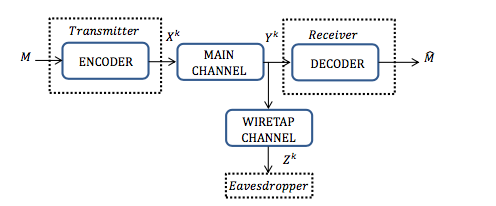


Figure 3.1: Wiretap Channel mode (degraded assumption)

The equivocation rate [3] is an important concept which quantifies how unlikely the eavesdropper can intercept valuable information in information-theoretic physical-layer security. This concept is defined by a formula 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 cipher text. The eavesdropper is able to access the cipher text 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.

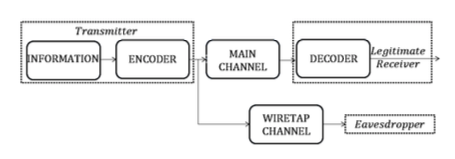


Figure 4.1: Wiretap channel model

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

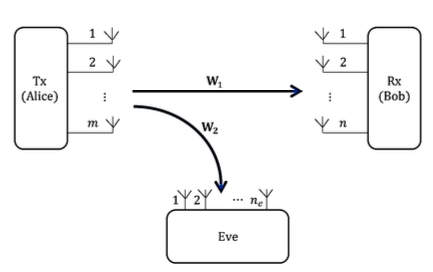
For the MIMO Gaussian wiretap channel, *ne* is the number of antennas employed by the eavesdropper. The secrecy capacity of the MIMO wiretap channel is defined as the maximized secrecy rate 𝐶𝑠(𝐑) of information can be reliably and securely transmitted subject to total transmit power.****

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**

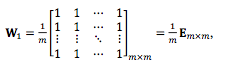
it uses statistical methods to estimate the numerical characteristics of the probability model thereby obtaining a numerical solution of practical problems. In this section, MC will be used to compute the secrecy capacity of Gaussian MIMO wiretap channel. In some cases, where *m* is large, the convergence 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

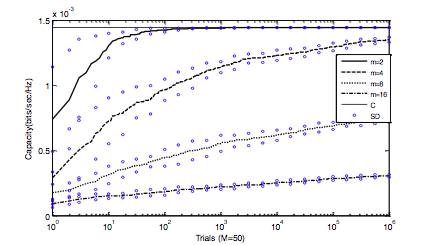


Figure 6.1, The capacity of Case 6.1 obtained by MC vs Trials (SNR = −30 dB).

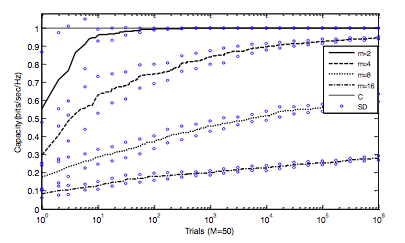


Figure 6.2, The capacity of Case 6.1 obtained by MC vs Trials (SNR = 0 dB).

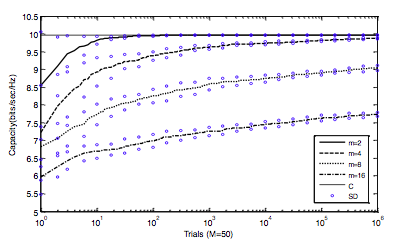


Figure 6.3, The capacity of Case 6.1 obtained by MC vs Trials (SNR = 30 dB).

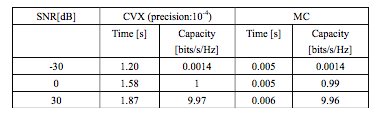


Table 6.1 The results of Case 6.1 returned by CVX and MC (𝑁 = 500, 𝑚 = 2).

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.

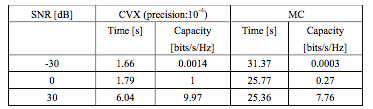


Table 6.2 The results of Case 6.1 resulted by CVX and MC (𝑁 = 106, 𝑚 = 16).

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.

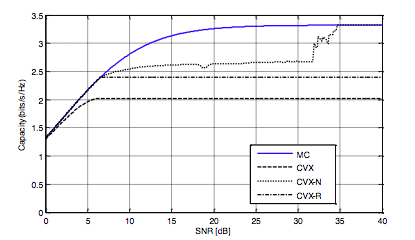
In such scenario, which is:

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

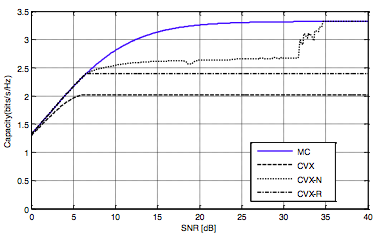
can be approximated by 𝐶𝑎 as

**../../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.

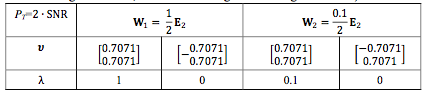


Table 7.1 The channel model of Case 6-1 (*m* = 2) (𝝊 denotes the eigenvectors of given matrix; λ denotes the eigenvalues of given matrix).

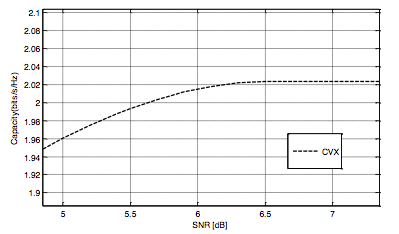


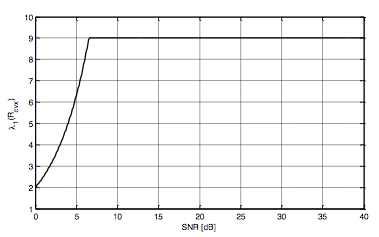
Figure 7.3 Saturation point and upper bound of approximated secrecy capacity of Case 7.1.

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

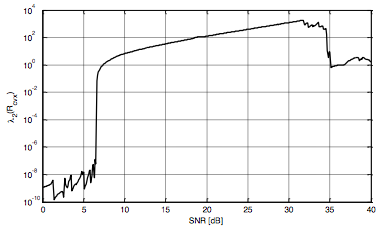
../../Screen%20Shot%202018-03-29%20at%203.58.31%20PM.png

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

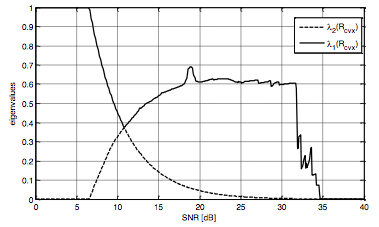
We can then observe that the power transmitted to 𝝊 (𝐑cvx) is fixed at 9 while the power transmitted to 𝝊2(𝐑cvx) jumps between [0,𝑃𝑇 −9] with the variety of SNR. The relationships of SNR with λ (𝐑cvx) and λ2(𝐑cvx) are indicated in Figures 7.4 − 7.6, thus proving our conclusion above.



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



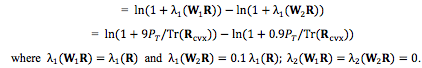
**Figure 7.5.** λ 2(𝐑cvx) vs SNR of Case 7.1 (Tr(𝐑) ≤ 2 SNR)



**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

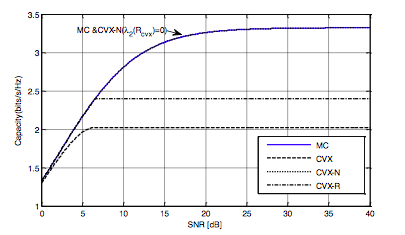
../../Screen%20Shot%202018-03-29%20at%204.04.24%20PM.png



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.

**8. Linear Approximation**

In this section we will provide a new method for the optimization problem for the secrecy capacity of Gaussian MIMO wiretap channel. As we have observed in the previous section, CVX is unable to accept the ‘ln(|𝐀|) − ln(|𝐁|)’ function and has a difficulty with the ‘ln(|𝐀|) − Trace(𝐁)’ function in term of returning optimal eigenvectors of the transmit covariance matrix, where ln(|𝐀|) and ln(|𝐁|) denote the logarithm function of the determinant of a matrices 𝐀 and 𝐁. Hence it is important to reformulate the original objective function 𝐶𝑠(𝐑) into a pattern that can be accepted by CVX directly.

The linear approximation reformulates the secrecy capacity optimization problem to allow the latter to be handled by CVX (since CVX has no difficulty for solving the optimization problem whose objective function is linear). The optimal solution can be obtained by solving this reformulation. Backtracking line search is used to improve the convergence. This method might return a local optimal solution when 𝐖 ≱ 𝐖2 i.e. the objective is not concave. To resolve this difficulty, the Min-Max Algorithm is introduced to make the objective concave or convex with respects to the variables (**R** or **K** respectively) such that the obtained solution is globally optimal. Oscillation may appear during the convergence in some cases since CVX is not able to handle the optimization over two variables jointly.

**9. Summary of the report**

As popularity of MIMO systems is growing at a rapid pace, the scale at which they are being used is considerably large. With their increased adoption, MIMO security issue is of utmost importance for a successful transition to this new technology. According to information theoretic secrecy, Gaussian MIMO wiretap channel’s secrecy capacity has been identified as an optimization problem with regard to transmit covariance matrix. Barring a few special cases, a closed form or explicit optimized solution has not been reached. This report focuses on numerical methods to obtain optimal transmit co-variance matrix of general Gaussian MIMO wiretap channel by utilizing CVX, Differential Evolution algorithm and Monte Carlo Optimization.

In order to calculate the capacity of MIMO channel and corresponding optimal covariance matrix for a given channel matrix, CVX offers a great simulation modelling toolbox. Despite the fact that CVX is a very popular methodology, it does not help in solving the convex/concave problems of optimization in correct manner for some cases.

For the cases in which the number of transmit antennas *m* is not too large, we found that Monte Carlo optimization is a good algorithm to calculate the secrecy capacity approximately. On the other hand, for the cases where *m* is large, it gets difficult for Monte Carlo to calculate accurate results especially for cases where the 𝐑 has been ranked low.

Differential Evolution algorithm was adopted to achieve numerical results for the optimization problem without making any approximation. We saw an improvement in the convergence such that the approximate calculation of secrecy capacity and the optimal covariance matrix is possible. It can be used to solve the optimization problem properly, considering the processing time and complexity of the algorithm. Also, CVX cannot return the correct optimal eigenvectors of the covariance matrix, so it is conclusive that the CVX is not able to solve the approximated problem in a proper manner. The optimization problem is approximately reformulated as an optimization problem for linear function with several constraints that can be solved by CVX properly. Since the CVX is not able to deal with the optimizations collectively, oscillations may appear during the iterations in a few cases. It was found that step size on the ascent direction affects the oscillations. Therefore, a method for making CVX to deal with the optimizations jointly will be important and necessary in the future. Furthermore, if the algorithm chooses the step size in an adaptive way, the convergence might be improved.

**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

MATLAB Codes

**CVX**

% SNRdB - SNR in dB, scalar integer from -30 to 30

% m - the number of transmit antennas

% W1 – for the main channel matrix

% W2 – for the eavesdropper’s channel matrix

C\_CVX = zeros(1,length(SNRdB)); % Channel Capacity returned by CVX

C\_PT = zeros(1,length(SNRdB)); % Channel Capacity returned after substituting R/Tr(T)

into (3.9)

for j=1:length(SNRdB);

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

% cvx part

cvx\_begin; % CVX begins

cvx\_precision(10^-4); % set CVX precision

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

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

C= log\_det(eye(m)+W1\*R)-trace(W2\*R);

maximize C;

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

C\_CVX(j)=cvx\_optval; % save the capacity

% scaled R part

Rcvx = m\*rho\*R/trace(R); % scaling normalized R (covariance matrix returned by CVX

C\_PT(j) = log(det(eye(m)+W1\*Rcvx))-log(det(eye(m)+W2\*Rcvx));

end

**Regular Monte Carlo**

% SNRdB ̈C SNR in dB

% M ̈C scalar integer from 1 to 50, the number of iterations % N=10^5 - the number of trials of Monte Carlo

% W1 - C main channel matrix

% W2 - C eavesdropper’ s channel matrix

% a - W2 = aW1

% m - the number of transmit antennas

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

[m,m] = size(W41);

trials = 1:1:N;

C = zeros(1,length(trials)); % vector for saving the final capacity vs

trials

SD = zeros(1,length(trials)); %standard deviation

CS = zeros(length(M),length(trials));% save randomly generated cpacity for computing standard deviation

R = zeros(m); % optimal covariance matrix

for i=1:length(M);

A = randn(m,m);

Rt = (A'\*A)/trace(A'\*A);

CM = zeros(1,length(trials1)); % vector for saving the capacity in each iteration

R1M = zeros(m); % for saving optimal covariance matrix in each iteration

R1M = Rt;

CM(1) = log2(det(eye(m)+rho\*W1\*Rt))-log2(det(eye(m)+rho\*W2\*Rt));

CS(i,1) = CM(1);

for j = 1:length(trials)-1

A = randn(m,m);

Rt = (A'\*A)/trace(A'\*A);

Ct = log2(det(eye(m)+rho\*W1\*Rt))-log2(det(eye(m)+rho\*W2\*Rt));

if Ct > CM(j);%

CM(j+1) = Ct;

R1M = Rt;

else

CM(j+1) = CM(j);

R1M = R1M;

end

CS(i,j+1) = CM(j+1);

end

C = C+CM;

R = R+R1M;

end

C = C/length(M); % do the average

R = R/length(M);

%computation of Standard deviation

for k=1:length(trials)

sum=0;

for n=1:length(M)

sum=sum+(C(k)-CS(n,k))^2;

end

SD(k)=sqrt(sum/length(M));

end

**Differential Evoluiton**

CR=0.9;%crosssover constant

F=1.5;

SNRdB=-20:20:20;

M=1:1:25;

a=0.1;

rho=10^(SNRdB(3)/10);

num\_NP = 1:1:200; % number of population

num\_Gen = 1:1:1000; % total number of generations

CE = zeros(1,length(num\_Gen));% optimal capacities vs number of generations

RE(:,:,length(num\_Gen)) = zeros(m);

for p = 1:length(M);

HE(:,:,length(num\_NP)) = zeros(nt1);%target H

CEM = zeros(1,length(num\_Gen));% Best Capacity of each generation in

each iteration

REM(:,:,length(num\_Gen)) = zeros(nt1);% Best R of each generation in

each iteration

CE = zeros(1,length(num\_NP));% all Capacities of each generation

HEbest(:,:,length(num\_Gen)) = zeros(nt1);% Best H of each generation

VE(:,:,length(num\_NP)) = zeros(nt1);%Mutant H UE(:,:,length(num\_NP)) = zeros(nt1);%Trial H

% generate NP target matrices

for i = 1:length(num\_NP);

HE(:,:,i) = randn(m);

end

RE = (HE(:,:,1)'\*HE(:,:,1))/trace(HE(:,:,1)'\*HE(:,:,1));

% Capacity of first Generation

Cs = log2(det(eye(m)+rho\*W1\*RE))-log2(det(eye(m)+rho\*W2\*RE)); HEbest(:,:,1) = HE(:,:,1);

Score = Cs;

for i = 2:length(num\_NP); % selecting the best target of first generation RE = (HE(:,:,i)'\*HE(:,:,i))/trace(HE(:,:,i)'\*HE(:,:,i));

Cs = log2(det(eye(m)+rho\*W1\*RE))-log2(det(eye(m)+rho\*W2\*RE));

if Cs > Score

Score = Cs;

HEbest(:,:,1) = HE(:,:,i);

else

end

end

CEM(1) = Score;

REM(:,:,1) = (HEbest(:,:,1)'\*HEbest(:,:,1))/trace(HEbest(:,:,1)'\*HEbest(:,:,1));

for i = 1:length(num\_NP); % computing all capacities yielded by target matrices of first generation

RE = (HE(:,:,i)'\*HE(:,:,i))/trace(HE(:,:,i)'\*HE(:,:,i));

CE(i) = log2(det(eye(m)+rho\*W1\*RE))-log2(det(eye(m)+rho\*W2\*RE));

end

for i = 2:length(num\_Gen)

%Generate NP mutant matrixs

for j = 1:length(num\_NP)

i\_1 = randi(length(num\_NP));

j\_1 = randi(length(num\_NP));

k\_1 = randi(length(num\_NP));

while((i\_1 == j\_1) || (k\_1 == j\_1) || (k\_1 == i\_1))

i\_1 = randi(length(num\_NP));

j\_1 = randi(length(num\_NP));

k\_1 = randi(length(num\_NP));

end

VE(:,:,j) = HE(:,:,i\_1)+F\*(HE(:,:,j\_1)-HE(:,:,k\_1));

end

%Generate NP trial matrixs

for k = 1:length(num\_NP)

row = randi(m);

col = randi(m);

Ut = HE(:,:,k);%Ut and Vt are intermediate variables Vt = VE(:,:,k);

for r = 1:m

for c = 1:nt1

if rand(1) <= CR

Ut(r,c) = Vt(r,c);

else

Ut(r,c) = Ut(r,c);

end

end

end

Ut(row,col) = Vt(row,col);

UE(:,:,k) = Ut;

Ru = (UE(:,:,k)'\*UE(:,:,k))/trace(UE(:,:,k)'\*UE(:,:,k)); %trial

covariance

matrix

% comparaing trial matrix U with target matrix H, if U yields better

capacity than H, swap H by U

Cu =log2(det(eye(m)+rho\*W1\*Ru))-log2(det(eye(m)+rho\*W2\*Ru)); if Cu > CE(k)

CE(k) = Cu;

HE(:,:,k) = UE(:,:,k);

else

CE(k) = CE(k);

HE(:,:,k) = HE(:,:,k);

end end

% Finding the optimal Solution of current Generation

CEM(i) = Score;

REM(:,:,i) = REM(:,:,1);

for g = 1:length(num\_NP)

if CE(g)> = CEM(i)

CEM(i) = CE(g);

REM(:,:,i) = (HE(:,:,g)'\*HE(:,:,g))/trace(HE(:,:,g)'\*HE(:,:,g));

else

CEM(i) = CEM(i);

REM(:,:,i) = REM(:,:,i);

end

end

end

CE = CE+CEM;

RE = RE+REM;

end

CE = CE./length(M);

RE = RE./length(M);

**Weak Eavesdropper**

SNRdB=-20:1:40;

C=zeros(1,length(SNRdB));

% the threshold of transmit power - Pstar, there is no Pstar W2 is singular if det(W2) ~= 0

Pinner=(eye(m)-(W2^0.5)\*(W1^(-1))\*(W2^0.5)); [dp,vp]=eig(Pinner);

vp=vp.\*(vp>0);

Pinner=dp\*vp\*dp'; Pstar=trace((W2^-1)\*Pinner); Pstar=10\*log10(Pstar);

end

for i=1:length(SNRdB)

rho=10^(SNRdB(i)/10);

lmax=m/rho;% the upper bound of Lagrangian multiplier lambda lmin=0;% the lower bound of Lagrangian multiplier lambda

for j=1:10^4 % large enough to ensure the accuracy is high

% bisection part, we deal with the case where m = 2

if det(W2) == 0 % there is no Pstar when W2 is singular lam=(lmax+lmin)/2;% Lagrangian multiplier lambda

else

if rho>=10^(Pstar/10)

lam=0;

else

lam=(lmax+lmin)/2;%lambda

end

end

A=lam\*eye(m)+W2;

W1t=A^(-0.5)\*W1\*A^(-0.5);% W1~

[d1,v1]=eig(W1t);

if v1(1,1)>1

ir1=1-1/v1(1,1);% first entry of diagonal matrix 'capital lambda' else

ir1=0;

end

if v1(2,2)>1

ir2=1-1/v1(2,2);% second entry of diagonal matrix 'capital

lambda'

else

ir2=0;

end

lamRt=[ir1,0;0,ir2];%lmabda of R~ Rt=d1\*lamRt\*d1';%R~

R=A^(-0.5)\*Rt\*A^(-0.5);% optimal covariance matrix

if abs((trace(R)-rho))/rho<=0.001; break

end

% bisection

if trace(R)>rho

lmin=lam;

else

lmax=lam;

end end

C(i)=[log(det(eye(m)+W1\*R))-trace(W2\*R)];% capacity yielded by final R returned by above discussion

end

**Linear Approximation**

SNRdB

N=1:10;% number of total trials

T=zeros(1,length(N)); % for saving the last t of each trial n=zeros(1,length(N)); % for saving the last n of each trial rho=10^(SNRdB/10);

C=zeros(1,length(N));% for saving the capacity of each trial R(:,:,length(N))=zeros(m); % for saving the optimal R of each trialn R0=(eye(m)/m)\*rho; % initialized covariance matrix

I = eye(m);

for i=1:length(N)

Z=((eye(m)+W1\*R0)^-1)\*W1-((eye(m)+W2\*R0)^-1)\*W2;

e = 1/max(norm(I/(I+W1\*R0)\*W1), norm(I/(I+W2\*R0)\*W2));% initialized

cvx\_begin quiet SDP;

cvx\_precision(10^-16);

variable dR(m,m) symmetric;% delta R

dC=trace(Z\*dR);% delta C

step size

maximize dC ;

trace(dR)==0;

dR+R0==semidefinite(m);

dR+e\*eye(m)==semidefinite(m);

cvx\_end;

% backtracking part

t=1;

n=0;

alpha=1/4; % alpha is from 0 to 1/2

C1=log2(det(eye(m)+W1\*(R0+t\*dR)))-log2(det(eye(m)+W2\*(R0+t\*dR))); % substituting R0+tdR into the true formula

C2=log2(det(eye(m)+W1\*(R0)))-log2(det(eye(m)+W2\*(R0)))+ alpha \*t\*trace((((eye(m)+W1\*R0)^-1)\*W1-((eye(m)+W2\*R0)^-1)\*W2)\*dR); % substituting t, dR and alfa into the linear approximation

[d,v]=eig(R0+t\*dR);%test if R0+tdR is PSD

psd=0; %if psd = 1 later, means that R0+dR is not PSD for l=1:m;

if v(l,l)<0;

psd=1;

end end

while (C1<C2)||(psd==1);

n=n+1;

t=t/2;

% to make sure that R0+tdR is positive definite

[d,v]=eig(R0+t\*dR);

psd=0; %if psd = 1 later, means that R0+tdR is not PSD for l=1:m; %test if R0+tdR is PSD

if v(l,l)<0;

psd=1;

end end

C1=[log2(det(eye(m)+W1\*(R0+t\*dR)))-log2(det(eye(m)+W2\*(R0+t\*dR))) ];% if R0+tdR is PSD, then renew C1 and C2 and continue the backtracking C2=[log2(det(eye(m)+W1\*(R0)))-log2(det(eye(m)+W2\*(R0)))+ alfa\*t\*trace((((eye(m)+W1\*R0)^-1)\*W1-((eye(m)+W2\*R0)^-1)\*W2)\*dR)] ;

end

T(i)=t;

n(i)=n; C(i)=log2(det(eye(m)+W1\*(R0+t\*dR)))-log2(det(eye(m)+W2\*(R0+t\*dR)));

R0=R0+t\*dR;% optimal R of current iteration

R(:,:,i)=R0;

end