A MIMO Based Cross-layer Approach to Augment the Security of Wireless Networks

Hong Wen and Guang Gong
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1, CANADA
Emails. h5wen@engmail.uwaterloo.ca; ggong@calliope.uwaterloo.ca

Abstract

In this work, we propose a novel MIMO-aided security scheme. By exploiting an extra dimension provided by MIMO systems for adding artificial noise to the transmission process, the physical-layer security is enhanced as a result. In the proposed scheme the physical-layer may rely on upper-layer encryption techniques for security, which results in a cross-layer security scheme.

1 Introduction

As wireless devices become increasingly pervasive and essential, they are becoming both targets of attacks and the very weapons with which such attacks can be carried out. Compared with wireline networks, wireless networks are open to intrusion from the outside without the need of a physical connection. The lack of security in these techniques may potentially result in a weak physical-layer security. The wireless security has become a critical concern in the physical layer. Cryptographic techniques can be used to provide security in a mobile environment, however these techniques do not directly leverage the unique property of the wireless domain to address security threats.

Physical-layer security techniques, which are based on the shannon secrecy model [1] are effective in resolving the boundary, efficiency and link reliability issues. Wyner [2] and Csiszar and Korner [3] developed the concept of the wire-tap channel for wired links. Based on these concepts, Hero [4] and koorapaty *et al.* [5] presented an information security approach which used channel state information (CSI) as the secret key in multiple-input multiple-output (MIMO) links. Unfortunately, attackers still can use the blind deconvolution algorithm [6, 7, 8] to estimate channels, which makes these approaches to lose security. Li *et al.* [9] and Kim *et al.* [10] developed MIMO security schemes which used the attacker's blind identification capacity loss. Their schemes assumed that the channels of intended receivers and attackers are neither identical, nor highly correlated. Under some special scenario where the attackers is very close to intended receivers, this method can't provide positive secrecy capacity.

The built-in security of the physical-layer is defined as the physical-layer transmissions guarantee low-probability-of-interception (LPI) based on transmission properties such as modulations, signals and channels, without resorting to source data encryption. No secret keys are required before transmissions.

Physical-layer built-in security is in fact equivalent to perfect secrecy [1]. Almost all existing results on physical-layer security are based on some kinds of assumptions that appear impractical [4, 5, 9, 10, 15].

Innovative cross-layer security designs with both physical-layer security and upper-layer traditional security techniques are desirable for wireless networks. In this paper, we propose a cross-layer approach to enhance the security of wireless networks for wireless environments. We combine cryptographic techniques implemented in the higher layer with the physical layer security scheme using MIMO systems to provide stronger security for wireless networks. Unlike the method in [4] and [5] we use multiple antennas to add artificial noise to the information signal such that only the intended receiver can eliminate the noise and recover the information. Therefore the transmitter can communicate with the intended receiver and prevent the attacker from decoding the message at the same time. The process of adding artificial noise is controlled by upper-layer cryptographic techniques. In our approach the physical-layer can utilize upper-layer encryption techniques for security, while physical-layer security techniques can also assist the security design in the upper-layer. Our new method also can be combined with the methods in [6, 9] to farther enhance secrecy.

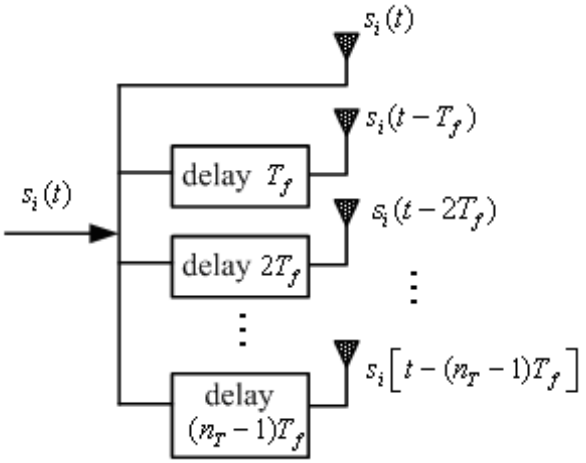

Figure 1: Delay transmit diversity scheme

2 A Novel MIMO Cross-Layer Secure Communication Model

Let us consider a single point-to-point MIMO system with arrays of n_T transmit and n_R receive antennas. The transmitted data is denoted as a vector $(s_1(t), \quad s_2(t), \quad \cdots, \quad s_T(t))$. Typically, an array with n_T transmit antennas sends a $n_T \times T$ signal matrix $\boldsymbol{S}$ over T time samples to n_R receive antennas. The transmission signal matrix can be formed as

$$\boldsymbol{S}_{inf} = \begin{bmatrix} s_1(t) & s_2 & \cdots & s_T(t) \\ s_1(t-T_f) & s_2(t-T_f) & \cdots & s_T(t-T_f) \\ \vdots & \vdots & \cdots & \vdots \\ s_1(t-jT_f) & s_2(t-jT_f) & \cdots & s_T(t-jT_f) \\ \vdots & \vdots & \cdots & \vdots \end{bmatrix} \tag{1}$$

where $s_i(t-jT_f)$, $(0 \leq j < n_T - 1)$, is the fundamental transmission information signal, and T_f represents the time delay. This is a typical delay diversity scheme in which multiple copies of the same symbol are transmitted through multiple antennas in different time slots as shown in Figure 1. However we do not directly transmit the signal given by Eq. (1). Let $\boldsymbol{S}_{noise}$ be a $T \times n_N$ noise matrix defined as:

$$\boldsymbol{S}_{noise} = \begin{bmatrix} w_{1,1} & w_{1,2} & \cdots & w_{1,T} \\ w_{2,1} & w_{2,2} & \cdots & w_{2,T} \\ \vdots & \vdots & \ddots & \vdots \\ w_{n_N,1} & w_{n_N,2} & \cdots & w_{n_N,T} \end{bmatrix} \tag{2}$$

where $n_N \leq n_T$ and each row in $\boldsymbol{S}_{noise}$ is a set of pseudorandom sequences with the length T. We also define the following binary control pseudorandom sequence matrix $\boldsymbol{S}_{control}$:

$$\boldsymbol{S}_{control} = \begin{bmatrix} v_{1,1} & v_{1,2} & \cdots & v_{1,T} \\ v_{2,1} & v_{2,2} & \cdots & v_{2,T} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n_N,1} & v_{n_N,2} & \cdots & v_{n_N,T} \end{bmatrix} \tag{3}$$

Each row in $\boldsymbol{S}_{control}$ is a set of pseudorandom sequences with the length T, and the elements in $\boldsymbol{S}_{control}$ are denoted by binary bits with above notations. We can represent the transmission signals with the following matrix $\boldsymbol{X}$:

$$\boldsymbol{X} = \begin{bmatrix} x_1^1 & x_1^2 & \cdots & x_1^T \\ x_2^1 & x_2^2 & \cdots & x_2^T \\ \vdots & \vdots & \ddots & \vdots \\ x_{n_N}^1 & x_{n_N}^2 & \cdots & x_{n_N}^T \\ x_{n_N+1}^1 & x_{n_N+1}^2 & \cdots & x_{n_N+1}^T \\ \vdots & \vdots & \ddots & \vdots \\ x_{n_T}^1 & x_{n_T}^2 & \cdots & x_{n_T}^T \end{bmatrix} \tag{4}$$

where the element x_i^j is determined by:

$$\begin{cases} x_j^i = s_i[t-(j-1)T_f], & j \le n_N, v_{j,i} = 0 \\ x_j^i = w_{j,i}, & j \le n_N, v_{j,i} = 1 \\ x_j^i = s_i[t-(j-1)T_f], & j > n_N. \end{cases} \tag{5}$$

In other words, if the control element $v_{j,i}$ is zero, the corresponding antenna will transmit the information signal. Otherwise, it will transmit the noise signal. The system block diagram is shown in Figure. 2. Both the noise sequences $\boldsymbol{S}_{noise}$ and the control sequences $\boldsymbol{S}_{control}$ are the stream ciphers generated by a set of keys. Both of them or one of them will be the secret keys between the transmitter and the intended receiver.

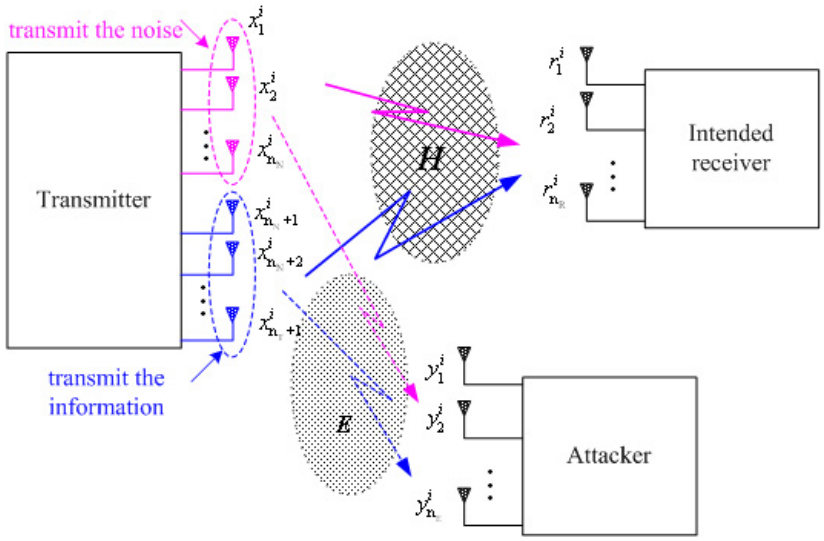

Figure 2: Antenna array redundancy model

The generators of secret keystream $\boldsymbol{S}_{noise}$ and $\boldsymbol{S}_{control}$ are shown in Figure 3. For secret keystream $\boldsymbol{S}_{noise}$ and $\boldsymbol{S}_{control}$ the principle of generation is same. Here we suggest two scheme, in which the stream ciphers will be the optimal selection for its fast implement speed. We also hope that the stream ciphers have ideal two-level autocorrelation and randomness properties such as balance distribution, long period, ideal tuple, whose autocorrelation function is a delta function. This function is very similar with those of gaussian white noise. A typical example is m-sequence. But the linear complexity of m-sequence is very low. Another good candidate is the WG stream ciphers [16] which generate pseudorandom sequence with high complexity and the same autocorrelation functions as m-sequences.

In Figure 3 (a) we generate the secret key $\boldsymbol{K}_0$ firstly, then the other keys is the shift of $\boldsymbol{K}_0$, which let the output keystream be different when the keystream generators have the same structure . In this scheme, $\boldsymbol{K}_0$ is the key that legitimate communication partners will share together. Therefore, the size of secret key is same as those of traditional cryptographic systems even if the secret keystream is a matrix. The disadvantage of this scheme is that the whole system will be destroyed when the attacker get the secret key. In Figure 3 (b) every row of the keystream matrix has its own secret key. There

are n different secret keys which are independent each other. The size of the secret key is bigger than the usual situation. The advantage of this scheme is that the leak of one or several secret keys only let the secret level of the system become lower and can not let the whole system be destroyed. For the structure of two stream cipher schemes we suggested in Figure 3., we can find a similar design in the literature, such as w7 [17].

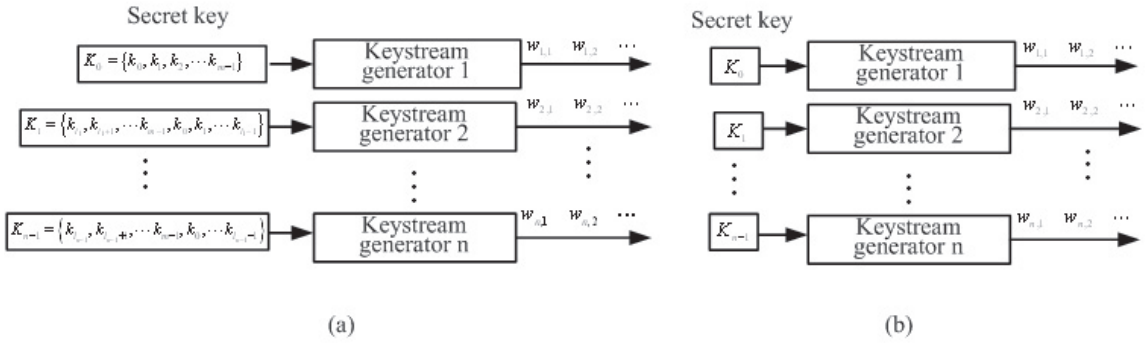

Figure 3: Keystream matrix generator

3 The Receiver for the Proposed Model

It is assumed that there are n_T transmit antennas, n_R receive antennas for the intended receiver, and n_A receive antennas for the attacker. We use a $n_R \times n_T$ matrix $\boldsymbol{H}^{(i)}$ to describe the channel from the transmitter to the intended receiver in the ith time slot and a $n_A \times n_T$ matrix $\boldsymbol{E}^{(i)}$ to denote the channel from the transmitter to the attacker in the ith time slot. $\boldsymbol{H}^{(i)}$ and $\boldsymbol{E}^{(i)}$ are defined as follows:

$$\boldsymbol{H}^{(i)} = \begin{bmatrix} h^i_{1,1} & h^i_{1,2} & \cdots & h^i_{1,n_T} \\ h^i_{2,1} & h^i_{2,2} & \cdots & h^i_{2,n_T} \\ \vdots & \vdots & \cdots & \vdots \\ h^i_{n_R,1} & h^i_{n_R,2} & \cdots & h^i_{n_R,n_T} \end{bmatrix} \tag{6}$$

and

$$\boldsymbol{E}^{(i)} = \begin{bmatrix} E^i_{1,1} & E^i_{1,2} & \cdots & E^i_{1,n_T} \\ E^i_{2,1} & E^i_{2,2} & \cdots & E^i_{2,n_T} \\ \vdots & \vdots & \cdots & \vdots \\ E^i_{n_A,1} & E^i_{n_A,2} & \cdots & E^i_{n_A,n_T} \end{bmatrix} \tag{7}$$

In the ith time slot, the signal in the jth receiving antennas of the intended receiver and the attacker are respectively

$$r^i_j = \sum_{t=1}^{n_N} h^i_{j,t} x^i_t + n^i_j + \sum_{k=n_N+1}^{n_T} h^i_{j,k} x^i_k + n^i_j, \tag{8}$$

$$\text{and} \qquad y_j^i = \sum_{t=1}^{n_N} E_{j,t}^i x_t^i + \tilde{n}_j^i + \sum_{k=n_N+1}^{n_T} E_{j,k}^i x_k^i + \tilde{n}_j^i \tag{9}$$

where r_j^i and y_j^i denote the signals received by the legitimate user and the attacker in time slot i, respectively. n_j^i and $\tilde{n}_j^i$ are the channel noises for the legitimate receiver and the attacker respectively. In some time slot the first terms in Eqs. (8) and (9) will become noise. The legitimate receiver knows the noise, so this term can be removed. However, the attacker doesn't know the pseudo-sequence $\boldsymbol{S}_{control}$. Hence, this term provides another noise component and the total noise becomes high. As a result the attacker's signal is a degraded version of the legitimate receiver's signal. According to Wyner [2], it is possible to achieve a non-zero secrecy capacity.

3.1 The Intended Receiver

For the intended receiver, a maximum ratio combining diversity can be used. In the ith time slot, the output signal is a linear combination of a weighted replica of all of the received signals, which is given by

$$\hat{\mathbf{r}}^i = \sum_{j=1}^{n_R} \alpha_j r_j^i \tag{10}$$

where α_j is a weight factor for the receive antenna j. In the maximum ratio combining, the weight factor of each receive antenna is chosen to be in proportion to the ratio of its own signal voltage and the noise power. Let A_j and ϕ_j be the amplitude and the phase of the received signal r_j^i, respectively. Assuming that each receive antenna has the same average noise power, the weight factor α_j can be represented as:

$$\alpha_j = A_j e^{-i\phi_j} \tag{11}$$

The decision rule for the ML decoder can be stated as

$$\hat{s}_i(t) = \arg\min \|\hat{\mathbf{r}}^i - \sum_{k=1}^{n_R} \sum_{j=1}^{n_T} h_{k,j}^i x_j^i\|^2 \tag{12}$$

$\hat{s}_i(t)$ is the estimated transmission signal in the ith time slot. Because the intended receiver knows the Eq. (5), it can eliminate the noise by substituting the former slot estimation transmission signal and $w_{i,j}$ into x_t^i.

3.2 The Attacking Receiver

The attackers can use the same method that described from Eq.(9) to Eq.(12). Hence they don't know the $\boldsymbol{S}_{control}$. The noise can't be canceled. They can also use the original VLST receiver [11] based on a combination of interference suppression and cancellation, which separates the data streams and thereafter independently decodes each stream. The algorithm is described as following:

Let the order set

$$\boldsymbol{K}_{Opt} = \{k_1, k_2, \cdots, k_{n_T}\} \tag{13}$$

be a permutation of the integers $\{1, 2, \cdots, n_T\}$ specifying the order in which components of ith slot transmitted symbol vector $\boldsymbol{x}^{(i)} = \{x_1^i, x_2^i, \cdots, x_{n_T}^i\}^T$ are extracted. Later we show how to determine a particular ordering $\boldsymbol{K}_{Opt}$ which is optimal in a certain sense. The detection algorithm which operates on received signal $\boldsymbol{y}^{(i)} = \{y_1^i, y_2^i, \cdots, y_{n_A}^i\}^T$ can be described as following steps.

Step 1: Let $\boldsymbol{y}_{\_1}^i = \boldsymbol{y}^i$. Using nulling vector $\boldsymbol{m}_{k_1}$, form a linear combination of the components of $\boldsymbol{y}_{\_1}^i$ to yield $\boldsymbol{b}_{k_1}^i$:

$$\boldsymbol{b}_{k_1}^i = \boldsymbol{m}_{k_1}^T \boldsymbol{y}_{\_1}^i \tag{14}$$

Step 2: Slice $\boldsymbol{b}_{k_1}^i$ to obtain $\hat{\boldsymbol{x}}_{k_1}$

$$\hat{\boldsymbol{x}}_{k_1} = Q(\boldsymbol{b}_{k_1}^i) \tag{15}$$

where $Q(\cdot)$ denotes the quantization (slicing) operation appropriate to the constellation in use.

Step 3: Canceling $\hat{\boldsymbol{x}}_{k_1}$ from the received vector $\boldsymbol{y}^{(i)}$ results in modified received vector $\boldsymbol{y}_{\_2}^i$

$$\boldsymbol{y}_{\_2}^i = \boldsymbol{y}_{\_1}^i - \hat{\boldsymbol{x}}_{k_1} (\boldsymbol{E}^{(i)})_{k_1} \tag{16}$$

where $(\boldsymbol{E}^{(i)})_{k_1}$ denotes the k_1th column of $\boldsymbol{E}^{(i)}$. Step 3 are then performed for components $k_2, \cdots, k_{n_T}$ by operation in turn on the progression of modified received vectors $\boldsymbol{y}_{\_2}^i, \boldsymbol{y}_{\_3}^i, \cdots, \boldsymbol{y}_{\_n_T}^i$

The specifics of the detection process depend on the criterion chosen to compute the nulling vectors $\boldsymbol{m}_{k_1}$. One of common choice is zero-forcing (ZF) method. The full ZF detection algorithm can be described completely as a recursive procedure, including determination of the optimal ordering, as follows:

Initialization:

$$l \leftarrow 1 \tag{17a}$$

$$\boldsymbol{y}_{\_1}^i = \boldsymbol{y}^i \tag{17b}$$

$$\boldsymbol{G}_1 = (\boldsymbol{E}^{(i)})^\dagger \tag{17c}$$

$$k_1 = \underset{j}{\operatorname{argmin}} \|(\boldsymbol{G}_1)_j\|^2 \tag{17d}$$

Recursion

$$\boldsymbol{m}_{k_l} = (\boldsymbol{G}_i)_{k_l} \tag{17e}$$

$$\boldsymbol{b}_{k_l} = \boldsymbol{m}_{k_l} \boldsymbol{y}_{\_l}^i \tag{17f}$$

$$\hat{\boldsymbol{x}}_{k_l} = Q(\boldsymbol{b}_{k_l}) \tag{17g}$$

$$\boldsymbol{y}_{\_l+1}^i = \boldsymbol{y}_{\_l}^i - \hat{\boldsymbol{x}}_{k_l} (\boldsymbol{E}^{(i)})_{k_l} \tag{17h}$$

$$\boldsymbol{G}_{l+1} = (\boldsymbol{E}_l^{(i)})^\dagger \tag{17i}$$

$$k_{l+1} = \underset{j \notin \{k_1, \cdots, k_l\}}{\operatorname{argmin}} \|(\boldsymbol{G}_{l+1})_j\|^2 \tag{17j}$$

$$l = l + 1 \tag{17k}$$

where $(\boldsymbol{E}^{(i)})^{\dagger}$ in Eq. (17c) denotes the moore-Penrose pseudoinverse [11] of matrix $\boldsymbol{E}^{(i)}$. $(\boldsymbol{G}_i)_j$ in Eq. (17d) and Eq. (17e) denotes the jth row of $\boldsymbol{G}_i$. $\boldsymbol{E}_l^{(i)}$ in Eq. (17i) can be obtained by zeroing column $k_1, k_2, \cdots, k_l$ of $\boldsymbol{E}^{(i)}$.

4 Comparison the Proposed New Model with the Traditional Stream Cipher Encryption System

In a synchronous stream cipher encryption system, let $\boldsymbol{m} = m_1, m_2, \cdots$ be a plaintext sequence which will be encrypted. The stream cipher contains a keystream generator that produced a pseudorandom sequence, called the keystream, $\boldsymbol{z} = z_1, z_2, \cdots$. In general, the ith symbol in the keystream, z_i, is a function of the key K and the previous plaintext symbols $m_1, m_2, \cdots, m_i$, which can be represented by

$$z_i = f_i[K, (m_1, m_2, \cdots, m_i)] \tag{18}$$

The keystream together with an encryption function, g_i, are used to encrypt the message $\boldsymbol{m}$ symbol by symbol, as

$$c_i = g_i(z_i, m_i) \tag{19}$$

where c_i is the ith symbol in the ciphertext.

The simplest case is that

$$\begin{aligned} z_i &= f_i[K] \\ \textit{and} \quad c_i &= z_i \oplus m_i \end{aligned}$$

Ususlly, hope the functions f_i and g_i are nonlinear function. In practical application of stream cipher encryption system, we use different kind of nonlinear functions to imitate the random properties. In our new model, let $\boldsymbol{s} = s_1, s_2, \cdots$ be the information sequence which will be transmitted. We also have the noise controlled by a pseudorandom sequence as key $\boldsymbol{S}_{control}$ transmitted by n_N transmit antennas. Let N_j^i denote the first two terms in Eq. (8) and (9). Then we have

$$N_j^i = fc_j^i[\boldsymbol{S}_{control}, (s_1, s_2, \cdots, s_i)] \tag{20}$$

The received signal can model as:

$$r_j^i = gc_j^i[N_j^i, (x_{n_N+1}^i, x_{n_N+2}^i, \cdots)] \tag{21}$$

where $x_k^i, (k = n_N + 1, n_N + 2, \cdots)$ is the element of $\boldsymbol{X}$ in Eq.(4). In Eq. (15) and (16), the function fc_j^i and gc_j^i are determined by fading channel coefficients and noises which are random functions with high nonlinear properties. These random and nonlinear properties can be broken by channel estimation or searching the controlling sequence $\boldsymbol{S}_{control}$. But the performance properties BER have to be paid for the attacker. The secret capacity can be obtained.

5 The Performance Properties of the Proposed Method

In this section, we use simulations to study the effectiveness of the proposed transmission scheme by evaluating the bit error rate (BER) of the intended receiver and the attacker. The channel is assumed to be able to block Rayleigh fading, i.e., it is constant during the transmission of one packet, but randomly changes between packets. Each packet contains 31 BPSK symbols. Here let the number of receiver antennas n_R and transmit antenna n_T be 2 and 8, respectively. The attacker and the intended receiver have the same receiver antennas. There are n_N antennas to transmit the noise signal among the n_T transmitter antennas. The parameter n_N is chosen to be 2, 4 and 6. We use 6 different m-sequences as the control pseudorandom sequences. In this work, we assume that an equal amount of power is allocated to all the sub-channels. The methods described here can be applied to a system using waterfilling-based allocations as well.

We do the simulations under two different conditions. firstly, we let the noise sequences $\boldsymbol{S}_{noise}$ be public. The control sequences $\boldsymbol{S}_{control}$ acts as a secret key between the transmitter and the intended receiver. Secondly, Both the noise sequences $\boldsymbol{S}_{noise}$ and the control sequences $\boldsymbol{S}_{control}$ are secret between the transmitter and the intended receiver. Figure.4 and Figure.5 show the BER for the proposed novel MIMO secure communication system under the fading channel in the two simulation conditions. From the simulation, we note that the more antennas transmit the noise the higher the security level is. In the meanwhile, less antennas can be used to transmit the information. Thus the penalty paid for the secure transmission of the information therefore is mostly in the rate of information that can be transmitted. Hence, there is a tradeoff between the of security level achieved and the transmission rate. When the noise sequences $\boldsymbol{S}_{noise}$ is public, the performances of this scheme are worst than those of the scheme that the noise sequences $\boldsymbol{S}_{noise}$ is kept as secret.

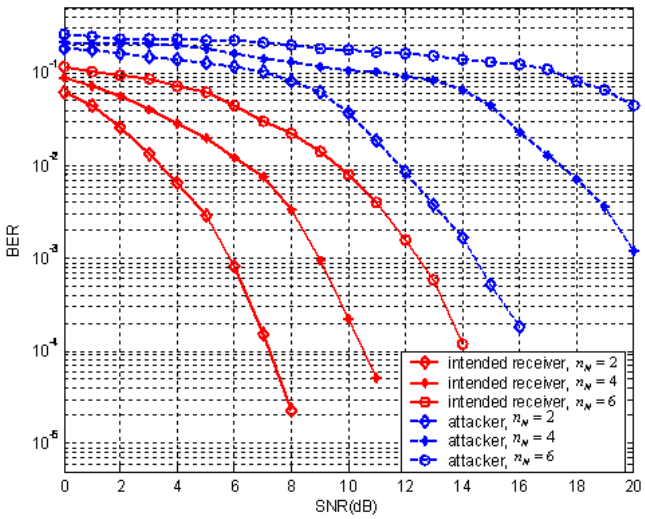

Figure 4: BER performance of novel MIMO secure communication system under fading channel,the noise sequences $\boldsymbol{S}_{noise}$ is public

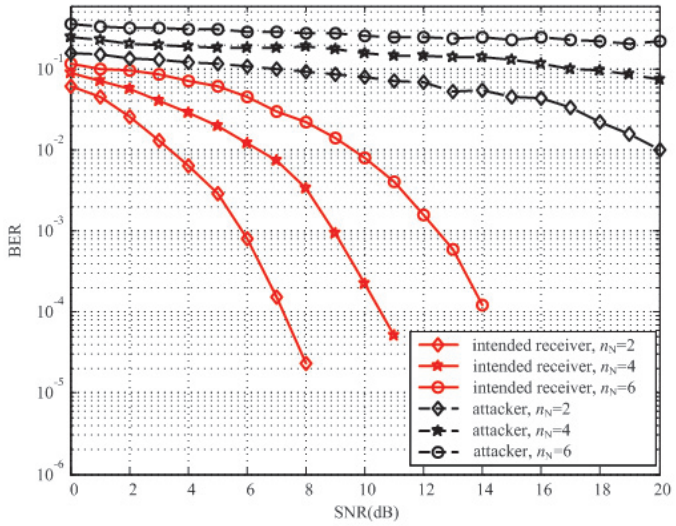

Figure 5: BER performance of novel MIMO secure communication system under fading channel,the noise sequences $\boldsymbol{S}_{noise}$ is secret

6 The Secret Capacity

In [3], the secrecy capacity C_s is defined as the maximum rate at which a transmitter can reliably send information to an intended receiver such that the rate at which the attacker obtains this information is arbitrarily small. In other words, the secrecy capacity is the maximal number of bits that a transmitter can send to an intended receiver in secrecy for each use of the channel. If the channel from the transmitter to the intended receiver and the channel from the transmitter to the attacker have different bit error probabilities (BER) ε and δ, respectively, i.e., the common input to channel is the binary random variable X, and the binary random variables received by the legitimate and the attacker are Y and Z where $P_{Y|X(y|x)} = 1-\varepsilon$ if $x = y$, $P_{Y|X(y|x)} = \varepsilon$ if $x \neq z$, $P_{Z|X(z|x)} = 1-\delta$ if $x = z$, $P_{Z|X(z|x)} = \delta$ if $x \neq z$. Without loss of generality, we may assume that $\varepsilon \leq 0.5$ and $\delta \leq 0.5$. The secret capacity C_s is [12]

$$C_s = \begin{cases} h(\delta) - h(\varepsilon), & \text{if } \delta > \varepsilon \\ 0, & \text{otherwise.} \end{cases} \tag{22}$$

where h denotes the binary entropy function defined by

$$h(p) = -plog_2p - (1-p)log_2(1-p) \tag{23}$$

Based on the BER results in Figure.4 and Figure.5 for the intended receiver and attacker, respectively, the secret capacity is calculated by Eq.(17) and shown in Figure.6 and Figure.7. It is assumed that the transmitter and the intender receiver can achieve the normal communication when the BRE

performance of the intended receiver is less than 10^{-2}. Therefore, our new method can achieve sufficiently good secret capacity within the corresponding SNR ranges.

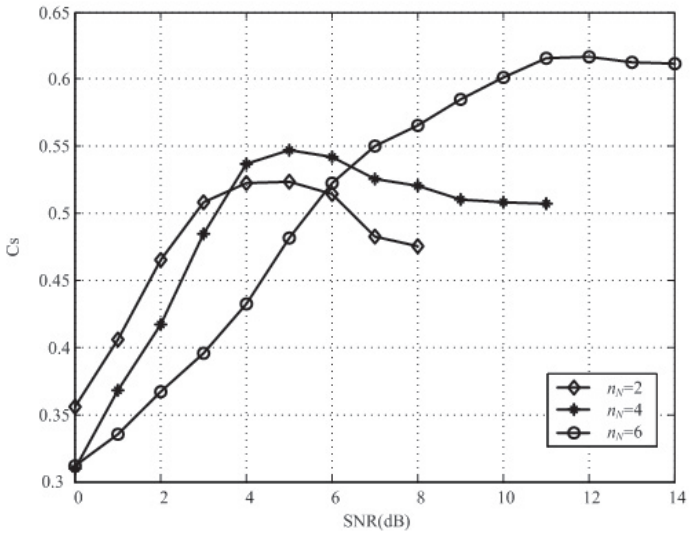

Figure 6: The secret channel capacity from the BER performance results,the noise sequences $\boldsymbol{S}_{noise}$ is public

7 Comparison the Proposed New Model with the Other Physical Layer Security Models

The existing physical-layer security techniques [4, 5, 9, 10, 15] are to guarantee wireless transmissions with low-probability-of-interception (LPI) which do not directly rely on upper-layer data encryption or secret keys. All methods can be realized based on channel diversity by using multiple antennas transmissions and receiving. The method presented in [4] used the channel state information (CSI) as the secret key. The drawback is that the eavesdroppers can get the CSI and the CSI changes frequently because of communication condition changing. So the CSI secret key will be very weak sometimes. The new proposed cross-layer model leverages the upper-layer secret key combining with multiple antenna diversity. This method can provide solid and stronger secret than method in [4]. The performances of our approaches do not depend on the number of the receivers, which are different from the methods in [4,10] whose performances depend on the number of the receivers. So the new method will be a good candidate for downlink transmission. Even if the receivers only have one antenna, this scheme also can work well. The method introduced in [10] which can be described as a randomized MIMO transmission scheme also focused on the downlink transmission. In this case the channel is known to the transmitter. Then the transmit antenna weights are designed by a special deliberate randomization method for LPI transmission. We compare the secret capacity of the method and our approach in Figure 8. They have close property. But the method in [10] assumed that the channels of intended receivers and attackers are highly correlated, which made this method become impractical.

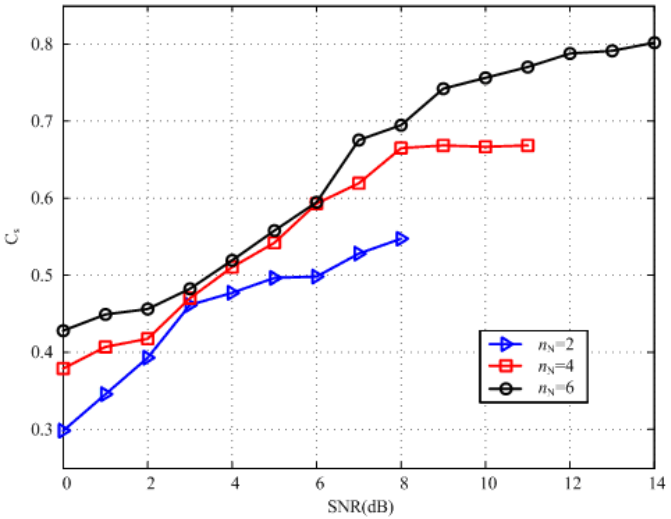

Figure 7: The secret channel capacity from the BER performance results,the noise sequences $\boldsymbol{S}_{noise}$ is secret

8 Conclusion

In this paper, we proposed a novel MIMO-based secure communication scheme in which the extra demission provided by the MIMO system is leveraged to enhance the physical layer security in wireless networks. In our approach, the physical-layer can use the upper-layer encryption techniques to control transmission sequences. So the security of approach is based on the secret key. Because the eavesdroppers can only receive the noisy signals, they have to find the secret key in the noisy key stream. It is more difficult than traditional attacking to ciphers which assumed that the key stream is error free. Therefore, our scheme combines the higher layer cryptographic techniques with the physical layer security together. A more detailed study on the robustness of the scheme against attacking to find the secret key is left for future. From the simulation we also can know that the number of antennas which transmit noises provides the performance tradeoff between the security level and the MIMO performance gains.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 29, pp. 656–715, 1949.

[2] A. D. Wyner, "The Wire-tap Channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. on Inform. Theory*, vol. 24, pp. 339–348, May 1978.

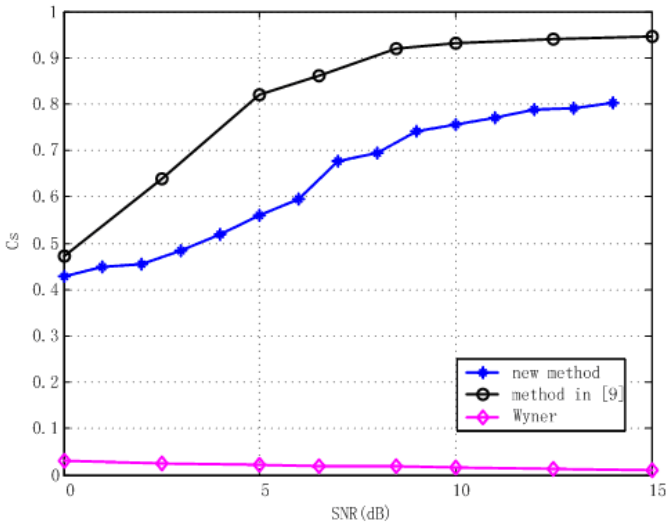

Figure 8: The secret channel capacity comparesion

[4] A.O. Hero, "Secure space-time communication," *IEEE Trans. Inform. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[5] H. Koorapaty, A.A. Hassan, S. Chennakeshu, "Secure Information Transmission for Mobile Radio," *IEEE Trans. Wireless Communications*, pp. 52–55, July 2003.

[6] S.Hayking, *Blind Deconvolution*, Prentice Hall, Englewood Cliffs, NJ, 1994.

[7] J. F. Cardoso, "Blind signal separation: statistical principles," *Proc. IEEE*, vol. 86, n. 10, pp. 2009-2025, Oct. 1998.

[8] Y. Hua, S. An and Y. Xiang, "Blind identification of FIR MIMO channels by decorrelation subchannels," *IEEE Trans. Signal Processing*, vol. 51, no. 5, pp. 1143-1155, May 2003.

[9] X. Li and J. Hwu, "Using antenna array redundancy and channel diversity for secure wireless transmissions," *Journal of Communications*, vol. 2, no. 3, pp. 24–32, May 2007.

[10] H. Kim and J. D. Villasenor, "Secure MIMO communcications in a system with equal numbers of transmit and receive antennas," *IEEE Communications Letters*, vol. 12, no. 5, pp. 386–388, May 2008.

[11] G. D. Golden, G. J. Foschini, R. A. Valenzuela and P. W. Wolniansky, "Detection algorithm and initial laboratory results using the V-BLAST space-time communication architecture," *Electronics Letters*, vol. 35, no. 1, pp. 14–15, January 1999.

[12] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, no. 3, pp. 733-742, Mar. 1993.

[13] G. H. Golub, and C. F. Van Loan, "Matrix computations," Johns Hopkind University Press, 1983.

[14] B. M. Hochwald and S. ten Brink, "Achieving near-capacity on a multiple-antenna channel," *IEEE Trans. Commun.*, vol. 51, no. 3, pp. 389-399, 2003.

[15] M. Nloch, J. Barros and M. R. D. Rodrigues, "Wireless information theoretic security," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2515-2534, June, 2008.

[16] Y. Nawaz and G. Gong, "WG: A family of stream ciphers with designed randomness properties," Information Sciences, Vol. 178, No. 7, April 1, 2008, pp. 1903-1916.

[17] Thomas S., Anthony D., Berson T., and Gong G., "The W7 Stream Cipher Algorithm," Internet Draft, April 2002.