Artificial Noise Based Secure Transmission Scheme in Multiple Antenna Systems

Bangwon Seo
Division of Electrical, Electronics and Control Engineering
Kongju National University, Cheonan, South Korea.

Abstract
We consider a secure transmission from a transmitter with multiple antenna to a desired receiver with a single antenna in the presence of an eavesdropper. In order to increase the secrecy rate performance, we propose an artificial noise (AR) based secure transmission scheme. Usually, in conventional schemes, transmission power reserved for the AR has been equally allocated to all orthonormal basis vectors composing of the null space of the desired channel vector between the transmitter and the desired receiver. However, in the proposed scheme, the whole AR transmission power is allocated to only one optimal vector among the basis vectors composing of the null space. The optimal vector is obtained by solving an optimization problem that maximizes the signal-to-interference plus noise ratio (SINR) at the desired receiver on the condition that the SINR at the eavesdropper should be lower than a given threshold. Through computer simulation, we show that higher secrecy rate performance can be obtained by allocating more power to the desired message transmission rather than the AR transmission. Also, the proposed scheme has higher secrecy rate performance than the conventional scheme for different number of transmit antennas and for various power allocation cases.

Keywords: Physical layer security, artificial noise, multiple antenna, precoding, secrecy rate.

INTRODUCTION
For the last several decades, it has been regarded that the security of data transmission can be ensured only by using the key-based cryptographic techniques at the network layer. Since the computational complexity for deciphering the enciphered data is excessively high without the knowledge of the secrecy key, it was considered to be infeasible to decipher the transmitted data. However, as the hardware technologies improve, the computational power of the hardware has been highly improved. Therefore, the deciphering for the enciphered data becomes feasible without the knowledge of the secrecy key. Recently, physical layer security has received considerable attention from the researchers. It achieves the security of the transmitted data without the aid of an encryption key by exploiting the randomness of wireless channel and the channel state information (CSI) among the transmitter, the desired receiver, and the eavesdropper [1]-[4]. Since the physical layer security requires the knowledge of some CSI among the channels instead of the encryption key, it is possible to implement the physical layer security schemes with very low computational complexity. Moreover, the physical layer security schemes can be employed independently of the network layer security schemes. Therefore, the two security schemes at the physical layer and the network layer can be jointly used to improve the security of the transmitted data.

For the last two decades, transmission schemes based on the multiple transmit antennas at the transmitter has received a lot of attention because it can reduce the interference in wireless channel and then, improve the signal-to-interference plus noise ratio (SINR) and the achievable rate at the desired receiver [5],[6]. Some researchers have shown that the multiple antenna techniques such as beamforming and precoding can also be used to improve the security at the physical layer. In conventional precoding schemes, precoding vectors are designed to maximize the SINR at the desired receiver by considering only the channel between the transmitter and the desired receiver. However, in order to improve the secrecy at the physical layer by using the multiple antennas, the channel between the transmitter and the eavesdropper should be also considered in the design of the precoding vector. An example of the physical layer security schemes using the multiple transmit antennas at the transmitter is artificial-noise (AN)-aided beamforming [7]-[10]. In AR transmission scheme, desired information is transmitted in the directions in which the desired receiver can obtain a channel gain and receive the information with a higher reliability. On the contrary, synthetic noise is generated at the transmitter and then, transmitted along the directions in which the AR has the least effect on the reception performance of the desired information at the desired receiver. Also, the AR is designed to prevent the eavesdropper from receiving the desired information.

In the conventional AR transmission schemes [7],[8], the power assigned to the AR transmission are equally allocated to all orthonormal basis vectors constituting the null space of the desired channel vector between the transmitter and the desired receiver. However, we will show that the conventional power allocation schemes are not optimal in terms of maximizing the secrecy rate.

In this paper, we consider an AR based secure transmission in multiple antenna systems in the presence of an eavesdropper. For the AR power allocation, transmission power assigned to the AR is not equally allocated to all basis vectors orthogonal to the channel vector from the transmitter to the desired receiver. Instead, the power is assigned to only one vector among the basis vectors which minimizes the SINR of the eavesdropper and maximizes the SINR of the desired receiver. Then, the precoding vector for the information symbol is designed to maximize the SINR of the desired receiver.

The rest of the paper is organized as follows. In Section II, system model is described. In Section III, a proposed multiple antenna transmission scheme for AR and optimal AR power allocation is presented. Simulation results are given in Section IV. Finally, the paper is concluded in Section V.
SYSTEM MODEL

Fig. 1 shows the system model for secure transmission that consists of a transmitter, a desired receiver, and an eavesdropper. The transmitter is equipped with $M > 1$ transmit antennas while the desired receiver and the eavesdropper have only a single antenna each. The channels from the transmitter to the desired receiver and to the eavesdropper are respectively denoted by $h_d$ and $h_s$ of size $M \times 1$.

If we denote the transmit signal vector by $x$ of length $M$, the received signal at the desired receiver and the eavesdropper can be respectively written as

$$r_d = h_d^H x + z_d,$$

$$r_s = h_s^H x + z_s,$$

where $z_d$ and $z_s$ are additive white Gaussian noises with mean 0 and variance $\sigma_s^2$ at the desired receiver and the eavesdropper, respectively.

Using the AR scheme, the transmitted signal vector $x$ at the transmitter is designed as a combination of the desired information component and the AR component and it is given by

$$x = \sqrt{\alpha} s + \sqrt{1-\alpha} Q v,$$

where $s$ is the information symbol with zero mean and unit variance and $v$ is an AN vector of size $(M-1) \times 1$ of which the elements are independent and identically distributed (i.i.d.) with mean 0 and variance 1. From the equation (1), the powers allocated to the desired information symbol and to the AR are $\alpha$ and $1-\alpha$, respectively. The vector $w$ normalized with $\|w\|=1$ is the beamforming vector for the desired information and $Q$ is a precoding matrix for the AN. Usually, in conventional AR transmission schemes, the power assigned to the AR transmission is equally allocated to all vectors composing of the matrix $Q$ and therefore, $Q$ is normalized with $Q^H Q = I_{M-1}$ where $I_{M-1}$ is an identity matrix of size $(M-1) \times (M-1)$.

\[\begin{array}{c}
\text{Transmitter} \\
\vdots \\
\text{Desired receiver} \\
\vdots \\
\text{Eavesdropper}
\end{array}\]

**Figure 1:** System model for secure transmission

Using the AR scheme, the transmitted signal vector $x$ at the transmitter is designed as a combination of the desired information component and the AR component and it is given by

$$x = \sqrt{\alpha} s + \sqrt{1-\alpha} Q v,$$

where $s$ is the information symbol with zero mean and unit variance and $v$ is an AN vector of size $(M-1) \times 1$ of which the elements are independent and identically distributed (i.i.d.) with mean 0 and variance 1. From the equation (1), the powers allocated to the desired information symbol and to the AR are $\alpha$ and $1-\alpha$, respectively. The vector $w$ normalized with $\|w\|=1$ is the beamforming vector for the desired information and $Q$ is a precoding matrix for the AN. Usually, in conventional AR transmission schemes, the power assigned to the AR transmission is equally allocated to all vectors composing of the matrix $Q$ and therefore, $Q$ is normalized with $Q^H Q = I_{M-1}$ where $I_{M-1}$ is an identity matrix of size $(M-1) \times (M-1)$.

In conventional schemes, $Q$ is designed as basis vectors consisting of the null space of $h_d$ so that the AR does not interfere to the reception of the desired signal $s$ at the desired receiver.

PROPOSED AR DESIGN AND POWER ALLOCATION

In this section, we propose a design method for the AR matrix $Q$. From the equation (4), we can see that the matrix $Q$ should be orthogonal to the desired channel vector $h_d$, i.e., $Q^H h_d = 0$ such that the AR does not have an effect on the reception of the desired information $s$. Hence, we decompose $Q = UD$ where the matrix $U$ of size $(M-1) \times M$ is orthogonal to $h_d$, i.e., $U^H h_d = 0$ and $D = \text{diag}(d_1, d_2, ..., d_M)$ where $\sum_{m=1}^{M} |d_m|^2 = 1$. Each element of the matrix $D$ represents the power allocated to the AR vector of the matrix $U$. In conventional schemes, $D$ is an identity matrix of size $M \times M$. Also, the column vectors of $[h_d \ U]$ constitute of an orthogonal basis.

Since $h_d^H Q = (h_d^H U) D = \mathbf{0}^T$, the received signals $r_d$ and $r_s$ in the equations (4) and (5) can be rewritten as

$$r_d = \sqrt{\alpha} h_d^H w s + z_d,$$

$$r_s = \sqrt{\alpha} h_d^H w s + \sqrt{1-\alpha} h_d^H Q v + z_s.$$

From the equation (6), we can see that the AR does not interfere to the reception of the desired signal $s$ at the desired receiver because the AR component disappears in the desired received signal $r_d$.

The SINRs at the desired receiver and the eavesdropper are respectively given by

$$\text{SINR}_d = \text{SNR}_d = \frac{\alpha w^H (h_d h_d^H) w}{\sigma_s^2},$$

$$\text{SINR}_s = \frac{\alpha w^H (h_s h_s^H) w}{(1-\alpha) h_d^H Q U D^H U^H h_s + \sigma_s^2}.$$

If we define $g = [g_1, g_2, ..., g_M]^T = U^H h_s$, we can rewrite the component of the denominator of the equation (9) by $h_s^H U D U^H h_s = \sum_{m=1}^{M} |g_m^T d_m|^2$. We define the index $m_0$ as

$$m_0 = \arg \max |g_m^T|^2.$$ Then, the denominator of the equation (9) is maximized when $d_{m_0} = 1$ and $d_m = 0$ for $m \neq m_0$. In this case, we obtain $Q v = u_{m_0} v_{m_0}$ and then, the transmitted signal vector can be rewritten as
From the equation (10), we can see that the whole power assigned to the AR transmission is allocated only to the vector $u_{m_0}$ among the basis vectors consisting of $U$. Also, since $d_{m_0} = 1$ and $d_m = 0$ for $m \neq m_0$, the SINR$_c$ can be rewritten as

$$\text{SINR}_c = \frac{\alpha w^H (h_c h_c^H) w}{(1 - \alpha) |g_{m_0}|^2 + \sigma_z^2}.$$  \hspace{1cm} (11)

We assume that for the secure transmission, SINR$_c$ should satisfy the condition $\text{SINR}_c \leq \gamma_{TH}$ for a given threshold $\gamma_{TH}$. Hence, the proposed precoding vector for the desired information symbol is designed by solving the following optimization problem:

$$\max_w \frac{\alpha w^H h_c h_c^H w}{\sigma_z^2} \quad \text{subject to} \quad \frac{\alpha w^H h_c h_c^H w}{(1 - \alpha) |g_{m_0}|^2 + \sigma_z^2} \leq \gamma_{TH}. \hspace{1cm} (12)$$

If $w = h_c / \| h_c \|$ satisfies the condition of $\text{SINR}_c \leq \gamma_{TH}$, we can easily prove that the optimal solution for (12) is $w_{opt} = h_c / \| h_c \|$. On the other hand, if $w = h_c / \| h_c \|$ does not satisfy the condition of $\text{SINR}_c \leq \gamma_{TH}$, the optimal solution for $w$ should satisfy the following condition:

$$\frac{\alpha w^H h_c h_c^H w}{(1 - \alpha) |g_{m_0}|^2 + \sigma_z^2} = \gamma_{TH}. \hspace{1cm} (13)$$

This equation can be rewritten as

$$w^H h_c h_c^H w = \gamma_{TH} \frac{(1 - \alpha) |g_{m_0}|^2 + \sigma_z^2}{\alpha}.$$  \hspace{1cm} (14)

If $w_1$ and $w_2$ are the solutions of the equation (14), the region satisfying the condition of $\text{SINR}_c \leq \gamma_{TH}$ is given in Fig.2. From the figure, we can see that the optimal vector $w$ needs to exist on the subspace spanned by $h_c$ and $h_v$. Therefore, we rewrite $w$ as

$$w = c_1 h_c + c_2 h_v = [h_c, h_v] \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = Hc,$$  \hspace{1cm} (15)

where $c = [c_1, c_2]^T$ is a weighting vector.

Since the desired precoding vector $w$ is normalized with $\| w \| = 1$, we can write the multiple linear equations for finding the optimal vector $w$ as follows:

$$w^H w = c^H H^H Hc = 1 \quad \text{and} \quad c^H H^H h_c h_v Hc = 0.$$  \hspace{1cm} (16)

These two equations can be easily solved by using the MATLAB program.

We also use a secrecy rate as a performance metric which is defined by

$$C_s = [C_d - C_e] = \left[ \log_2 (1 + \text{SINR}_d) - \log_2 (1 + \text{SINR}_e) \right],$$  \hspace{1cm} (17)

where $[x]^+ = \max\{x, 0\}$.

**SIMULATION RESULTS**

We have performed the computer simulation to evaluate the performance of the proposed secure transmission scheme based on the AR transmission in multiple antenna systems. The SINR performances at the desired receiver and the eavesdropper are compared between the proposed scheme and the conventional scheme. The performance is evaluated by averaging over 400 independent channel realizations. In all simulation, the channel vectors from the transmitter to the desired receiver and to the eavesdropper are assumed to be composed of independent and identically distributed Gaussian random variables with zero mean and unit variance. In the conventional scheme, the power

---

**Figure 2:** Region satisfying the SINR$_c$ condition

**Figure 3:** SINR at the desired receiver and the eavesdropper with $M = 6$, $\alpha = 0.5$ and $\gamma_{TH} = 0$ dB.
assigned to the AR is allocated to all vectors composing of the null space of the channel vector from the transmitter to the desired receiver. On the contrary, in the proposed scheme, AR power is allocated to only one vector among orthonormal vectors composing of the null space.

Fig. 3 shows the SINR performances of the proposed scheme and the conventional scheme at the desired receiver and the eavesdropper according to the received SNR at the desired receiver when \( M = 6, \alpha = 0.5, \) and \( \gamma_{th} = 0 \) dB. Since the power allocation parameter is \( \alpha = 0.5 \), half the total power is allocated to the transmission of the desired message symbol and the other half power is allocated to the AR. The received SNR at the desired receiver is calculated by assuming that the transmit power is not allocated to the AR, i.e., \( \alpha = 1 \). From the figure, we can observe that the SINR at the desired receiver is almost the same for the proposed scheme and the conventional scheme. However, the SINR of the proposed scheme at the eavesdropper is much lower than that of the conventional scheme and the difference between the two becomes larger as the SNR increases. Since the SINR at the eavesdropper in the figure is lower than the threshold \( \gamma_{th} = 0 \) dB, both the proposed scheme and the conventional scheme satisfy the SINR constraint.

Fig. 4 shows the secrecy rate for different number of transmit antennas according to the received SNR at the desired receiver when the power allocation parameter is \( \alpha = 0.5 \) and the SINR threshold of the eavesdropper is \( \gamma_{th} = 0 \) dB. The number of transmit antenna is \( M = 4, 8 \). From the figure, we can observe that the secrecy rate increases as the received SNR increases. The secrecy rate performance for \( M = 8 \) is higher than that for \( M = 4 \). Therefore, if more transmit antennas at the transmitter is employed, higher secrecy rate performance can be obtained. Also, the proposed scheme has better secrecy rate performance than the conventional scheme.

Fig. 5 compares the secrecy rate performance of the proposed scheme and the conventional scheme for various power allocation cases when \( M = 6 \) and \( \gamma_{th} = 0 \) dB. The power allocation parameter is \( \alpha = 0.25, 0.5, \) and 0.75. The case of \( \alpha = 0.25 \) represents the case when more transmission power is allocated to the AR transmission rather than the desired message transmission. The case of \( \alpha = 0.75 \) represents the case when more transmission power is allocated to the desired message transmission. From the figure, we can see that higher secrecy rate performance can be obtained by allocating more power to the desired message transmission rather than the AR transmission. Also, for all cases, the proposed scheme has better secrecy rate performance than the conventional scheme.

**CONCLUSION**

In this paper, we have considered secure transmission in multiple antenna systems in the presence of the eavesdropper. We proposed an AR based secure transmission scheme. In the proposed scheme, the AR transmission power is not allocated to all basis vectors orthogonal to the channel vector between the transmitter and the desired receiver. Instead, the power is allocated to only one vector among the basis vectors. The precoding vector for the information symbol is optimized to maximize the SINR of the desired receiver while maintaining the SINR of the eavesdropper to be lower than the given threshold. Through the simulation results, we showed that the secrecy rate performance of the proposed scheme is better than the conventional scheme.

**ACKNOWLEDGMENT**

This work was supported by the research grant of the Kongju National University in 2015.

**REFERENCES**


