Evaluation of performance improvement of space selective modulation by increasing number of transmitting antennas

Daiki Fukushima(a), Hideichi Sasaoka, Hisato Iwai, and Shinsuke Ibi

1Graduate School of Science and Engineering, Doshisha University, 1-3 Tatara Miyakodani, Kyotanabe-shi, Kyoto, 610-0321 Japan
a) ctwc0310@mail4.doshisha.ac.jp

Abstract: As a physical layer security technique, directional modulation (DM) using an array antenna was proposed. By the method, modulated signal can be correctly reconstructed in only the pre-specified direction from the array. On the other hand, Space Selective Modulation (SSM) was proposed. SSM shares the similar principle to DM. Using the technique, modulated signal is correctly reconstructed in only the specified space, not the specified direction by utilizing fading characteristics. The originally proposed SSM uses three or four transmitting antennas. However, the transmissible probability is not 100%. Because a modulated signal is formed by summing up phase-controlled channel coefficients in SSM, symbols of the all constellation points may not be formed depending on the channel conditions. It brings about a decrease in the secrecy capacity of the secure information transmission. In this paper, we consider solving the problem by increasing the number of antennas. We quantitatively evaluated the secrecy capacity by computer simulations. The results confirm the improvement of the total performance in the secrecy capacity of SSM.

Keywords: physical layer security, Space Selective Modulation, Directional modulation, radio propagation characteristics

Classification: Wireless communication technologies

References

[1] H. Sasaoka, “[Tutorial lecture] Information security at physical layer based on radio propagation characteristics,” IEICE Technical Report, vol. 115, no. 40, pp. 13–18, May 2015. (in Japanese)

[2] M. P. Daly, J. T. Bernhard, “Directional modulation technique for phased arrays,” IEEE Trans. Antennas Propag., vol. 57, no. 9, pp. 2633–2640, Sep. 2009. DOI:10.1109/TAP.2009.2027047
1 Introduction

Recently, physical layer security techniques based on information theoretic safety are attracting attention [1]. An example of the technique is Directional Modulation (DM) [2, 3, 4]. DM forms a desired modulated signal only in pre-specified direction using an array antenna. In the preceding studies of DM [2], the environment is assumed to be a line-of-sight propagation. So the DM scheme cannot be applied to non-line-of-sight propagation. On the other hand, a secure information transmission suitable for non-line-of-sight propagation has been proposed [5]. The scheme shares similar principle to DM. By using the unique channel coefficients the scheme can form the modulated signal only at legitimate receiver in non-line-of-sight fading environments. For this reason, it is called Space Selective Modulation (SSM). SSM decomposes a desired modulated signal into multiple phase modulated signals having constant amplitude based on the channel coefficient so that a desired signal is reconstructed at the legitimate receiver. Reference [5] showed a method of decomposing a desired modulated signal assuming three and four transmitting antennas. However, in some cases, the modulated signal cannot be successfully reconstructed. In SSM, a modulated signal is formed by the sum of phase-controlled channel coefficients. Therefore, the desired modulated signal may not be reconstructed depending on the fading characteristics. We call the unsuccessful probability as untransmissible probability. One of the challenges about the technique is to improve the probability.

We consider increasing the number of transmitting antennas to solve the problem. In this paper, we focus on the performance evaluation particularly when multilevel modulation method is adopted because increasing the number of antennas is especially effective for higher multilevel modulation. We quantitatively evaluate the improvement of the untransmissible probability and the secrecy capacity. The results show the improvement of the untransmissible probability and the secrecy capacity.

2 Principle of SSM

2.1 Signal decomposition method of SSM

In this section, we show the signal decomposition method of SSM shown in [5]. The configuration of the transmission system is shown in Fig. 1(a). The scheme
consists of $N$ antennas at the transmitter and a single antenna at the receiver. The scheme decomposes a desired modulated signal into $N$ phase modulated signals so that the desired signal is properly reconstructed by summing up the received signals at the legitimate receiver as shown in Eq. (1).

$$s(t) = \sum_{i=1}^{N} h_i e^{j\theta_i(t)}$$  \hspace{1cm} (1)

$s(t)$ represents the desired modulated signal. $h_i$ is the channel coefficient between the $i$-th transmitting antenna and the receiving antenna. $e^{j\theta_i(t)}$ signifies phase modulated signal where $\theta_i(t)$ is the phase shift of the modulated signal. Eq. (1) indicates the desired modulated signal $s(t)$ is formed at the legitimate receiver as a result of summing up the phase modulated signals that had been affected by the change of the amplitude and phase of the channel coefficient $h_i$. In the DM scheme, a plane wave is assumed so the phases of the received signals transmitted from the different transmitting antennas are simply rotated without amplitude variation. On the other hand, the amplitude also fluctuates in non-line-of-sight fading environments for which SSM is expected to work. Therefore, it is necessary to consider the change of the amplitude and phase by the channel coefficients. The following briefly shows the signal decomposing method of SSM studied in [5]. We show the method for a case with four transmitting antennas ($N=4$). The channel coefficients are assumed to be ordered from largest to smallest. We assume the channel coefficients are obtained by some means before decomposing the signal.

$$|h_1| \geq |h_2| \geq |h_3| \geq |h_4|$$  \hspace{1cm} (2)

The absolute value of the channel coefficient is also expressed as $l_i (i = 1, 2, 3, 4)$.

Fig. 1(b) and (c) are diagrams on the complex plane. $s$ represents a desired modulated signal. A complex vector from the origin to $s$ is decomposed into four complex vectors $r_i (i = 1, 2, 3, 4)$ by the signal decomposition method described below. Note that the length of $r_i$ is $l_i$. From the region surrounded by the bold line shown in Fig. 1(b), a point is randomly selected and defined as a point $c$. The area surrounded by the bold line is the possible range of the point $c$. Next, the vector from the origin to the point $c$ is represented by combination of two vectors $r_1$ and $r_2$, and the vector from the point $c$ to the modulated signal vector $s$ is by two vectors $r_3$ and $r_4$ as in Fig. 1(c). The vectors $r_i$, their arguments $\varphi_i$ and the angles $\alpha$ and $\beta$ are calculated by the following equation.

$$\alpha = \cos^{-1}\left(\frac{|c|^2 + l_1^2 - l_2^2}{2l_1 |c|}\right).$$  \hspace{1cm} (3)

$$\varphi_1 = \arg(c) \pm \alpha, \varphi_2 = \arg(c - r_1)$$  \hspace{1cm} (4)

$$\beta = \cos^{-1}\left(\frac{|s-c|^2 + l_3^2 - l_4^2}{2l_3 |s-c|}\right).$$  \hspace{1cm} (5)

$$\varphi_3 = \arg(s-c) \pm \beta, \varphi_4 = \arg(s-c - r_3)$$  \hspace{1cm} (6)

$$r_i = l_i e^{j\varphi_i}$$  \hspace{1cm} (7)

The phase $\theta_i$ of the transmitted signal from the $i$-th antenna is calculated by subtracting the phase of the channel coefficient from $\varphi_i$. 
2.2 Required condition for signal decomposition in SSM

In SSM, the signal decomposition shown in Eq. (1) may not be feasible depending on channel conditions. This section describes the required condition to decompose a desired modulated signal in SSM. The following shows the conditions. Eqs. (8) and (9) must be satisfied in order to decompose both of the maximum amplitude of the modulated signal $|s_{\text{max}}|$ and the minimum amplitude of the modulated signal $|s_{\text{min}}|$. Note that $s_{\text{max}}$ and $s_{\text{min}}$ are complex signals of the constellation of a modulation system on the complex plane.

\[
\sum_{i=1}^{N} |h_i| \geq |s_{\text{max}}| \tag{8}
\]

\[
|h_1| - \sum_{i=1}^{N} |h_i| \leq |s_{\text{min}}| \tag{9}
\]

The left terms of Eqs. (8) and (9) indicate the possible values as the minimum and the maximum, respectively, as the reconstructed signals after summing up the all received signals at the receiver. Therefore, if the amplitude of the desired modulated signal does not satisfy Eqs. (8) and (9), the signal could not be formed. If $|s_{\text{max}}|$ was set smaller than $\sum_{i=1}^{N} |h_i|$, the combination to reconstruct desired signal would not be unique. In other words, $\theta_i(t)$ can be variable. By changing the phase $\theta_i(t)$ while satisfying the above all conditions from Eqs. (1) to (9) for reconstructing the desired signal at the legitimate receiver, different signals are received at the eavesdropper due to different fading characteristics. As a result, demodulation at the eavesdropper becomes difficult. As described above, by intentionally suppressing the signal intensity from the maximum possible level, the degree of freedom of the signal decomposition can be improved, and it can be used for a countermeasure against eavesdropping. The parameter indicating the amount of the suppression is defined by the following equation.

\[
A_h = 20 \log_{10} \left( \sum_{i=1}^{N} |h_i|/s_{\text{max}} \right) \tag{10}
\]

We define $A_h$ to be greater than or equal to 0. So Eq. (8) is always satisfied. However, if $|s_{\text{max}}|$ were equal to $\sum_{i=1}^{N} |h_i|$, the phases of all $h_i e^{j\theta_i(t)}$ ($i = 1, 2, \cdots, N$) would be the same. In other words, $\theta_i(t)$ are uniquely determined. Therefore, the corresponding received signal at the eavesdropper is also uniquely determined. On the other hand, increasing $A_h$ extends the degree of freedom of $\theta_i(t)$. However, as $A_h$ increases, the amplitude of the modulated signal decreases and SNR (Signal to Noise power Ratio) also decreases. It brings about the deterioration of the BER performance at the legitimate receiver. Therefore, $A_h$ must be set appropriately because the sharing characteristic between legitimate users and eavesdropping resistance have such trade-off relationship.

$|s_{\text{max}}|$ is determined by the sum of the amplitude of all channel coefficients (left side of Eq. (8)) and the value of $A_h$. $|s_{\text{min}}|$ depends on $|s_{\text{max}}|$ and the modulation level. And when the modulation level is higher, $|s_{\text{min}}|$ becomes smaller assuming constant $|s_{\text{max}}|$ and, as the result, the probability of satisfying Eq. (9) decreases. As the countermeasure to the problem, we consider increasing the
number of transmitting antennas. The untransmissible probability is improved by increasing the number of transmitting antennas. And the improvement is particularly clear for higher multilevel modulation. For this reason, in this paper we focus on the performance evaluation of SSM when high multilevel modulation is adopted such as 256QAM and 1024QAM.

3 Extension of signal decomposition in SSM

In SSM, the untransmissible probability is expected to improve as the number of transmitting antennas increases. To realize the signal decomposition of SSM using more number of antennas, it is necessary to extend the conventional decomposition scheme. We describe the extended method in this section. The configuration of the method is fundamentally the same as the conventional method shown in Fig. 1(a). As in the existing SSM, we decompose a desired modulated signal into \( N \) phase modulated signals based on the channel coefficient and transmit them.

Here we show assume a case with eight transmitting antennas as an example to show how to determine the transmission phase. In the method, a waypoint is set between the origin and the desired modulated signal. The waypoint is equivalent to point \( c \) in Fig. 1(b). We select the top four antennas with the higher absolute value of the channel coefficient from the eight transmitting antennas. The vector from the origin to the waypoint is formed by summing up the received signals from the four transmitting antennas. And all other transmitting antennas form the vector from the waypoint to desired signal. The method shown in Section 2.1 is applied to determine the phase of the transmitted signal. The case of more transmitting antennas than eight can be realized by the same way.

4 Performance evaluation by computer simulation

4.1 Simulation system

In this section, we evaluate the performance of SSM using many transmitting antennas by computer simulation. Table I shows the specifications of the simulation system. The configuration of the legitimate users is the same as that of Fig. 1(a). The eavesdropper has the same configuration of the legitimate receiver.
The channel coefficient between the legitimate users is $h_i$. Similarly, the channel coefficient between the $i$-th transmitting antennas and the eavesdropper is expressed as $h_{ei}$. The correlation of the fading variation between $h_i$ and $h_{ei}$ is assumed $\rho$. In this paper, we assume a block Rayleigh fading channel where the amplitude and phase fluctuations are constant during a single block. And we assume 100 symbols are transmitted per block. As described in the above section, high-level modulation method (256QAM and 1024QAM) is assumed in this paper. Selection of the value of $A_t$ is important to realize the best performance of SSM. However, we emphasis the improvement by increasing antennas in this paper. So $A_t$ is simply fixed 1 dB.

4.2 Simulation result

In this section, we evaluate the untransmissible probability in SSM and the secrecy capacity. The secrecy capacity is calculated from BER of the legitimate receiver and the eavesdropper based on the conditional entropies $H(X|Y)$ and $H(X|Z)$. Note that the information transmitted by the legitimate transmitter, the information received by the legitimate receiver and the eavesdropper are expressed by $X$, $Y$ and $Z$, respectively. The secrecy capacity is found from the difference between $H(X|Y)$ and $H(X|Z)$.

Fig. 2(a) shows the untransmissible probability in SSM. In the case of original four transmitting antennas, the untransmissible probability is high for both 256QAM and 1024QAM. However, when the number of transmitting antennas is increased to 8, even if 1024QAM is used, the probability is greatly reduced.

Fig. 2(b) shows the secrecy capacity for 256QAM. It is confirmed by the figure, as the number of the transmitting antennas increases, the secrecy capacity improves.

| Number of transmitting antennas | Modulation scheme | Untransmissible probability |
|---------------------------------|-------------------|-----------------------------|
| 4                               | 256 QAM           | $5.14 \times 10^{-2}$       |
|                                 | 1024 QAM          | $6.91 \times 10^{-2}$       |
| 8                               | 256QAM            | $3.97 \times 10^{-6}$       |
|                                 | 1024 QAM          | $8.46 \times 10^{-6}$       |

(a) Untransmissible probability (b) Secrecy capacity (256QAM)

Fig. 2. Simulated result of SSM.

5 Conclusion

In this paper, we examined the performance of SSM using many transmitting antennas. Computer simulations show that the untransmissible probability and the overall secrecy capacity are improved by increasing the number of transmitting antennas.