IEICE Communications Express, Vol.13, No.3, 72–75

ComEX

LETTER

A study of secure communication with secret sharing method in MIMO eigen stream parallel channels

Masaaki Yamanaka[1, a)], **Shigenori Kinjo**[1], **and Shinichi Miyamoto**[2]

Abstract This letter proposes a secure transmission method using spatially parallel channels formed in a multi-input multi-output (MIMO) communication scenario. In the proposed method, the transmitted information is divided into pieces using a secret-sharing method. These generated pieces are then transmitted separately to the destination through the parallel sub-channels of the MIMO communication link. The secret-sharing method ensures that the transmitted information remains unrevealed unless all the divided pieces are obtained, thus achieving secure communication by establishing an advantageous situation for the legitimate receiver to gather the divided pieces against wiretappers in the surrounding area. Computer simulations demonstrate that allocating transmission power inverse-proportionally to the channel gains among the MIMO sub-channels creates a secure link to the receiver from the channel capacity perspective. The secret capacity of the link increases with the number of antenna elements in the MIMO configuration at the expense of power gain.

Keywords: distributed transmission, MIMO parallel channels, secret-sharing method, physical layer security

Classification: Wireless communication technologies

1. Introduction

Distributed transmissions have received attention owing to their ability to establish secure connections between terminals [1]. The main concept of this method is to pre-divide the transmitted information into several pieces and send each piece separately through different routes to the destination. Previous research [2] has shown that combining directive transmission with a secret-sharing method (SSM) [3] effectively exploits the multi-path property of wireless link to establish a secure connection based on this concept. In this method, at the transmitter, multiple routes to the destination are provided by adjusting the antenna's directivity to align with the dominant propagation paths. The transmitted information is then divided into pieces, which are called "shares", using the SSM and sent separately to the destination. As the SSM ensures that the original information remains undisclosed unless all the divided shares are obtained, the secrecy of the transmitted information can be achieved by distributing each share spatially to the destination. Although the transmission rate decreases with the number of shares, the method aligns well with the concept of distributed transmission to establish secure connections in wireless link.

This study explores the concept of the distributed transmission in a multi-input multi-output (MIMO) communication scenario. In MIMO transmission, a transmission link can generate multiple sub-channels, serving as parallel routes for distributed transmission. We have pointed out in [4] that, by employing the SSM, optimum transmission can be achieved by allocating the transmission power inversely proportional to the channel gains among these sub-channels. This implies that the received signal power is evenly distributed among the parallel routes. The SSM's characteristic of requiring all shares to recover the original information determines the link's capacity, which is governed by the most erroneous sub-channel with the lowest received signal power.

This letter aims to elucidate the efficacy of inverse-proportional power allocation for secure transmission in a MIMO parallel link against potential wiretappers. Adjusting the power allocation for the legitimate receiver, making it suboptimal for unintended receivers in different locations, provides an advantage in countering wiretappers within the communication range. This power allocation strategy enables secure communication by exploiting the difference in achievable channel capacity between the links formed between the legitimate receiver and potential wiretappers.

One disadvantage of the proposed method is the degradation of power gain of the transmission link. Compared to the well-known water-filling based power allocation, the proposed method's performance diminishes due to its inverse-proportional power allocation policy. However, we believe this trade-off is necessary in certain applications or fields where the secrecy of transmitted information is highly prioritized. In the following sections, we demonstrate the effectiveness of the proposed method in enhancing secrecy through distributed transmission, including its impact on link's power gain through computer simulations.

2. Distributed transmission

2.1 Transmission signal flow

Figure 1 illustrates the signal flow of the distributed transmission method applied to the MIMO communication scenario. In this approach, we employ singular value decomposition (SVD)-MIMO transmission to create multiple eigen-streams, which serve as sub-channels for the separate transmission of divided shares. Equation (1) shows the operation of SVD on the channel matrix ($\mathbf{H}$), where $\mathbf{U}$ and $\mathbf{V}$ represent

[1] Faculty of Maritime Science & Technology, Japan Coast Guard Academy, Kure-shi, Hiroshima 737-8512, Japan.
[2] Faculty of Systems Engineering, Wakayama University, Wakayama-shi, Wakayama 640-8510, Japan.
[a)] yamanaka@jcga.ac.jp

DOI: 10.23919/comex.2023XBL0144
Received November 1, 2023
Accepted November 22, 2023
Publicized January 15, 2024
Copyedited March 1, 2024

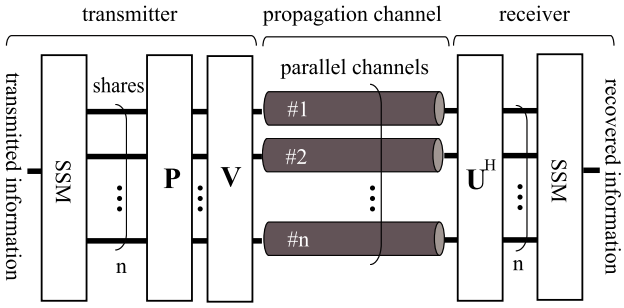

Fig. 1 Signal flow of the distributed transmission method.

unitary matrices, Λ is a diagonal matrix containing the singular values of $\mathbf{H}$, and $(\cdot)^H$ denotes the conjugate transpose. By employing SVD-MIMO transmission, the MIMO channel can be decomposed into multiple single-input single-output (SISO) channels, which is achieved using $\mathbf{V}$ as a pre-steering matrix at the transmitter, and $\mathbf{U}^H$ as a post-steering matrix at the receiver [5].

$$\mathbf{H} = \mathbf{U}\Lambda\mathbf{V}^H \tag{1}$$

In our proposed method, we utilize SSM to pre-divide the transmitted information prior to MIMO transmission. Here, we assume the number of sub-channels in the MIMO transmission as n, and the transmitted information is divided into n shares using SSM. The distributed transmission is then performed by transmitting each share through the parallel sub-channel by controlling its transmission power. Figure 1, block P denotes the transmission power allocation block to the parallel sub-channels. Within this block, the transmission power of the i-th sub-channel (P_i) is controlled by dividing the total transmission power (P_T) using Equation (2), which varies inversely with the channel gains among sub-channels. The channel gain of the i-th sub-channel, denoted as g_i, is determined by the second power of the i-th singular value of $\mathbf{H}$.

$$P_i = P_T \cdot \frac{(1/g_i)}{\sum_{j=1}^{n}(1/g_j)} \tag{2}$$

2.2 Secret-sharing method (SSM)

The SSM divides information into shares and manages information transmission based on the number of shares divided. The method is known as a (k, n)-threshold scheme, where information is divided into n shares and can only be reconstructed when k shares are obtained. When k is equal to n, it is referred to as an all-or-nothing scheme. In this case, all shares are required to reconstruct the original information, and no information is revealed unless all shares are collected.

The SSM can be implemented using a Reed-Solomon (RS) code. Leveraging its errors-and-erasures decoding algorithm, an (n, k)-RS code enables the formation of a (k, n)-threshold scheme, where a single message symbol is hidden among n code symbols of the RS code [6]. Consequently, the (k, n)-threshold scheme can be easily transformed into an all-or-nothing scheme by selecting k code symbols for transmission. We assume that an all-or-nothing scheme is applied at the transmitter to divide the transmitted information for distributed transmission [2].

Figure 2 illustrates the transmission error performance of the message symbol encoded in the RS code and its divided

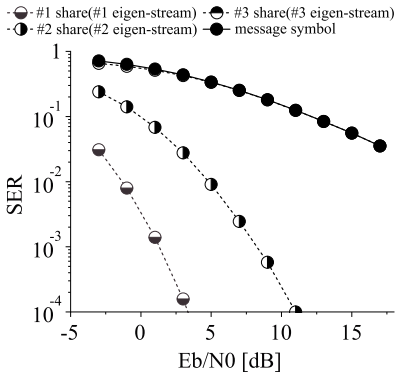

Fig. 2 Symbol error performances of the message symbol encoded in the RS code and its generated shares.

Table I Simulation parameters.

channel model	i.i.d Rayleigh fading channel
number of antenna elements	3
signal modulation	QPSK

shares for transmission. We employed a (7, 3)-RS code to implement a (3, 3)-threshold scheme, generating three all-or-nothing shares for the distributed transmission of the message symbol through parallel routes formed by SVD-MIMO transmission. Table I lists the parameter settings used for the simulation. We assumed a MIMO configuration with three antenna elements to form three parallel routes for distributed transmission. Through the SVD operation, multiple eigen-streams were generated in the MIMO channel as multiple sub-channels with varying power gains.

From Fig. 2, we can observe that the symbol error rate (SER) of the message symbol exhibits a similar performance to the share allocated in the third eigen-stream of the link, which has the lowest power gain among the three streams. This similarity can be attributed to the characteristics of the all-or-nothing scheme, in which all divided shares are necessary to recover the original information. The error performance of the message symbol is determined by the share with the highest error rate and lowest signal power. This result indicates that the inverse-proportional power allocation policy among streams is optimal in terms of transmission error performance. Furthermore, it enhances the channel capacity of the link when an all-or-nothing scheme is applied to the distributed transmission.

3. Computer simulation

3.1 Simulation setting

The security of the proposed method is evaluated through computer simulations, considering channel capacity and assuming a wiretap channel exploited by an eavesdropper. Figure 3 illustrates the channel scene used for the evaluation, which includes a legitimate link between a transmitter (Alice) and a receiver (Bob), with an eavesdropper (Eve) in close proximity. The legitimate link and wiretap link (between Alice and Eve) are assumed to be uncorrelated and realized as independent and identically distributed (i.i.d) Rayleigh fading channels. All three terminals have an equal number of antenna elements. Therefore, Alice transmits information

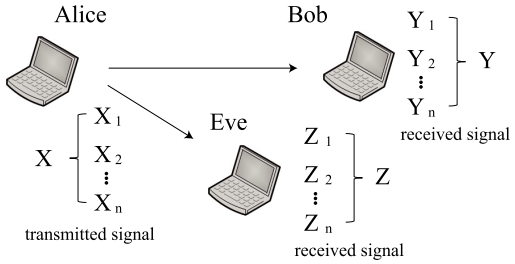

Fig. 3 Channel scene for computer simulation evaluation.

Table II Simulation parameters.

channel model	i.i.d Rayleigh fading channel
number of antenna elements	2, 4, 8
signal modulation	QPSK

(X) by dividing it into shares X_i $(i = 1, ..., n)$, which are received by Bob as Y_i $(i = 1, ..., n)$ to recover the transmitted information as Y. Simultaneously, Eve attempts to intercept the shares as Z_i $(i = 1, ..., n)$ to recover the transmitted information as Z, where n is the number of antenna elements. In this evaluation, Eve employs maximum likelihood detection (MLD) [7] to wiretap the transmitted information using knowledge of the channel matrix between Alice and Eve, including Alice's precoding matrix ($\mathbf{V}$). This assumption favors Eve by considering the possibility of blind estimation of the wiretap channel characteristics. By utilizing MLD, which is an optimum signal detection method that achieves the lowest transmission error rate for transmitted signals, Eve can evaluate the secrecy of the transmitted information under the worst-case scenario of interception.

Table II lists the simulation parameters used in the evaluation. We conducted Monte Carlo simulations to assess the transmission error performances of both links. The divided shares for transmission were generated bit by bit and transmitted separately across multiple sub-channels. Subsequently, we evaluated the mutual information of each link based on the derived error performance and examined the relative superiority of the legitimate link compared to the wiretap link in terms of channel capacity. Equations (3) and (4) are used to derive the mutual information [8] for the i-th sub-channel at both links, where $\mathrm{I}(\cdot)$ denotes the mutual information function, r represents the dimension of the transmitted shares, and p_i and q_i denote the transmission error rates of the share allocated to the i-th sub-channel in the legitimate link and the wiretap link, respectively. Based on the discussion presented in Sec. 2.2, the transmission error performance of X is determined by the most erroneous share using the all-or-nothing scheme. Additionally, the mutual information of the legitimate link and the wiretap link is determined by the lowest mutual information among all individual sub-channels, as shown in Equation (5) and Equation (6), respectively.

$$\mathrm{I}(X_i; Y_i) = \log r + (1 - p_i)\log(1 - p_i) + p_i \log \frac{p_i}{r - 1} \quad (3)$$

$$\mathrm{I}(X_i; Z_i) = \log r + (1 - q_i)\log(1 - q_i) + q_i \log \frac{q_i}{r - 1} \quad (4)$$

$$\mathrm{I}(X; Y) = \min_i I(X_i; Y_i) \quad (5)$$

$$\mathrm{I}(X; Z) = \min_i I(X_i; Z_i) \quad (6)$$

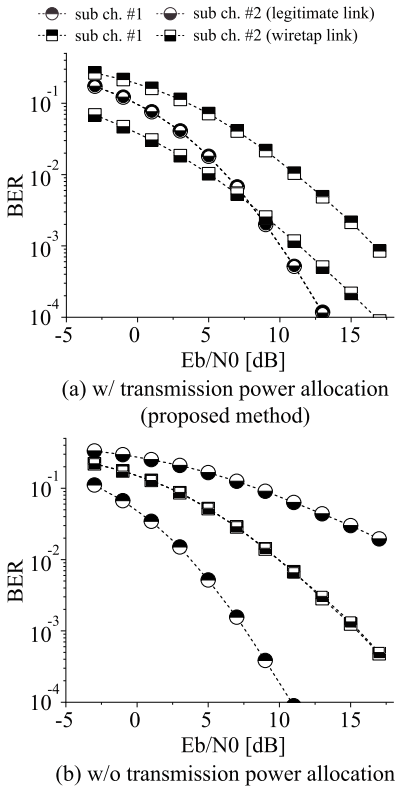

Fig. 4 Transmission error performances of the shares.

3.2 Simulation results

Figure 4(a) shows the error performance of the transmitted shares (X_i) using the proposed method across the sub-channels in both legitimate and wiretap links. The number of antenna elements in the simulation was set to two. For comparison, Fig. 4(b) shows the same performance without transmission power allocation. We assume that a situation which received Eb/N0 remains unchanged in the legitimate link with transmission power allocation. As the power gain decreases in the legitimate link owing to the power-allocation procedure, we compensate for the gain reduction by increasing the transmission power to attain the same Eb/N0 at the receiver. This assumption increases the received Eb/N0 ratio in the wiretap link. Figure 4(a) reflects the influence of the increase in the received Eb/N0 in the simulation; however, the x-axis in the figure indicates Eb/N0 before transmission power allocation to consistently evaluate the effect of power allocation, as shown in Fig. 4(b).

From Fig. 4(b), it can be observed that although the error performances originally vary among the sub-channels in the legitimate link, they exhibit identical performance by the proposed method, as shown in Fig. 4(a). Conversely, in the wiretap link, the error performances vary among the sub-channels by the proposed method, despite originally showing identical performance. This change in performance results in inferior transmission error performance for signal transmission in the wiretap link. Because the SSM determines the error performance of the transmitted information (X) based on the most erroneous divided share, the results in Fig. 4(a) indicate that the proposed method eventually achieves superior transmission error performance for X in the legitimate link compared with the wiretap link for signal transmission.

This discrepancy is due to the transmission power allocation of the proposed method. The optimal power allocation to the legitimate link no longer aligns with that of the wiretap link because the channel characteristics differ between the two. In addition, the application of SVD in the legitimate link significantly affects the error performance difference among the sub-channels in the wiretap link. Specifically, the channel power gain difference generated by SVD in the legitimate link leads to varying received signal powers across the sub-channels in the wiretap link by the inverse-proportional power allocation policy of the proposed method.

Figure 5 shows the mutual information performances of the legitimate link and the wiretap link for every 1-bit transmission of X, considering the simulation settings with 2, 4, and 8 antenna elements. We determined the transmission error performance of all the sub-channels and used Eqs. (3)–(6) to calculate the mutual information associated with X transmitted through both links. As shown in Fig. 5, mutual information demonstrates superior performance in the legitimate link compared to the wiretap link. Therefore, secure transmission can be achieved by utilizing the difference in the mutual information within the transmission bits, which increases with the number of antenna elements.

Although the proposed method can achieve secret transmission within the transmission bits determined by the amount of mutual information obtained against the wiretap link, its power allocation policy reduces the power gain of the legitimate link achieved by MIMO transmission. Figure 6 shows the power gain reduction from the other power allocation policies. We considered two other power allocation policies: equal power allocation and the well-known water-filling based power allocation. The presented power gain in Fig. 6 in the y-axis is the total average power gain of all sub-channels formed by the MIMO transmission in the legitimate link, which is normalized based on the propagation gain of a unit set of transmissions between antenna elements. From Fig. 6, we observe that our employed power allocation policy decreases the power gain of the legitimate link compared to the other two methods. In addition, it is evident that the reduction in the power gain increases as the number of antenna elements increases. One drawback of the proposed method is that secrecy in transmission comes at the expense of reduced power gain in the link.

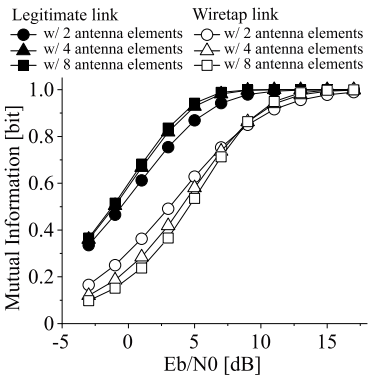

Fig. 5 Comparison of the mutual information attained in the legitimate link and the wiretap link.

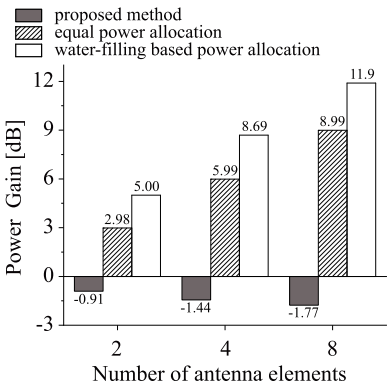

Fig. 6 Comparion of the total channel power gain attained in the legitimate link with different number of antenna elements.

4. Conclusion

In this letter, we have proposed a method for establishing a secure wireless link through distributed transmission combined with the SSM technique in the context of MIMO communication scenarios. SVD-MIMO transmissions were employed to create multiple sub-channels, serving as parallel routes for distributed transmissions. We emphasize that optimal transmission can be achieved by allocating transmission power that is inversely proportional to the channel gains among the sub-channels, assuming that the SSM is employed for distributed transmission. Furthermore, through computer simulation results, we demonstrate that the proposed method achieves higher mutual information in the legitimate link than in the surrounding wiretap links, thus enabling secret transmission from a channel capacity perspective. The secret capacity increases with the number of antenna elements in the MIMO configuration, although this comes at the expense of the power gain of the link.

Acknowledgments

The authors are deeply grateful to Dr. Seiichi Sampei for the kind advice and comments. This work was supported by JSPS KAKENHI Grant Number JP20K11782.

References

[1] M. Baldi, F. Chiaraluce, N. Laurenti, S. Tomasin, and F. Renna, "Secrecy transmission on parallel channels: Theoretical limits and performance of practical codes," *IEEE Trans. Inform. Forensics Security*, vol. 9, no. 11, pp. 1765–1779, Nov. 2014. DOI: 10.1109/TIF.2014.2348915

[2] M. Yamanaka, S.C. Wei, J. Zou, S. Ohno, S. Miyamoto, and S. Sampei, "Distributed transmission for secure wireless links based on a secret-sharing method," *IEICE Trans. Commun.*, vol. E102-B, no. 12, pp. 2286–2296, Dec. 2019. DOI: 10.1587/transcom.2018EBP3284

[3] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979. DOI: 10.1145/359168.359176

[4] M. Yamanaka, et al., "A study on transmission secrecy of MIMO eigenbeam communication with secret sharing method," 2023 IEICE Gen. Conf., B-5-131, March 2023 (in Japanese).

[5] B. Vucetic and J. Yuan, *Space-Time Coding*, John Willy & Sons, 2003. DOI: 10.1002/047001413x

[6] R.J. McEliece and D.V. Sarwate, "On sharing secrets and Reed-Solomon codes," *Communications of the ACM*, vol. 24, no. 9, pp. 583–584, Sept. 1981. DOI: 10.1145/358746.358762

[7] J.G. Proakis, *Digital Communications*, Mcgraw-Hill, 2001.

[8] N. Abramson, *Information Theory and Coding*, Mcgraw-Hill, 1963.