Threshold Secret Sharing Transmission Against Passive Eavesdropping in MIMO Wireless Network

Jungho Myung and †Taehong Kim
Electronics and Telecommunications Research Institute (ETRI)
†School of Information and Communication Engineering, Chungbuk National University
Email: jhmyung@etri.re.kr and †taehongkim@cbnu.ac.kr

***Abstract*—In this paper, we propose a threshold secret sharing scheme for secure communications even in the absence of eavesdropper channel state information. In the proposed scheme, the secret data is divided into N_{min} parts by polynomial of degree $T-1$ and transmits to the target user through multiple spatial dimensions by beamforming. The divided secret data at the user can be reconstructed with a sufficient number ($\geq T$) of parts by using the Lagrange interpolating polynomial. The numerical results show that eavesdropping probability of the proposed scheme is better than those of the considered conventional schemes.**

***Index Terms*—Data Transmission, Secret Sharing, Threshold Secret Sharing.**

I. Introduction

Recently, wireless transmission is inherently vulnerable to eavesdropping due to the broadcast nature of a radio propagation [1]-[5]. Even though a large number of security measures – from wired equivalent privacy (WEP) to transport layer security (TLS) – throughout the network layers are developed and already widely deployed, they now face considerable challenges by attackers with immense computing powers acquirable from the cloud and quantum computer.

As one of the new attempt to overcome this problem, physical layer security (PLS) has been introduced as an alternative security method to achieve fundamental secrecy in physical layer. With a single antenna configuration, Wyner first introduced a wiretap channel and the secrecy, the results of which show the feasibility of secure communication [1]. Also, PLS with multiple antennas has been studied [3]-[5]. In MIMO network, by beamforming and jamming techniques, the secrecy can be provided even though the quality of the main channel is worse than the quality of the eavesdropping channel. Most of existing works have focused only on increasing the secrecy rate by beamforming and jamming design, assuming that transmitter knows the channel state information (CSI) of the eavesdropper. However, it is impossible to obtain the CSI of the eavesdropper due to the passive posture. Therefore, to ensure secrecy against passive eavesdropper, new transmission technique with multiple spatial dimensions is needed in the absence of an eavesdropping channel.

In this paper, we propose a threshold secret sharing transmission for secure communications. In the proposed scheme, the secret data is divided into N_{min} parts using polynomial of degree $T-1$ and transmits to the user through multiple spatial dimensions by a transmit beamforming. At the user, based on the Lagrange interpolating polynomial, the secret data can be recovered when a sufficient number ($\geq T$) of parts are combined together. Also, we propose the majority rule for secret reconstruction to overcome the channel fading and noise in wireless network. At the eavesdropper, it is difficult to estimate the T parts correctly due to the difference between main channel and eavesdropping channel in physical layer. Therefore, attempt to reconstruct the secret data is generally unsuccessful. The numerical results show that the eavesdropping probability of the proposed approach is better than those of the considered conventional approaches.

Notations: $\mathbf{X}^{\dagger}$, $\mathbf{X}^{-1}$, and $||\mathbf{X}||$ denote the conjugate transpose, inverse, and the Euclidean norm of matrix $\mathbf{X}$, respectively.

II. Threshold Secret Sharing Transmission

A. System Model

As shown in Fig. 1, we considers MIMO wireless network with a base station (BS) with N_t transmit antennas, a target user (TU) with N_r receive antennas, and an eavesdropper (EA) with N_e receive antennas. When BS transmits a secret data over the channel matrix $\mathbf{H}$ to the TU, the radio signal is exposed to the EA over the cross channel $\mathbf{G}$. Then, the received signal at the target user can be written as

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}, \tag{1}$$

where $\mathbf{y}, \mathbf{x}$, and $\mathbf{n}$ denotes a received signal vector, a transmitted signal vector, and AWGN vector, respectively. Also, the eavesdropping signal can be written as

$$\mathbf{z} = \mathbf{G}\mathbf{x} + \mathbf{w}, \tag{2}$$

where $\mathbf{z}$ and $\mathbf{w}$ denotes a received signal vector and AWGN vector at the EA, respectively.

B. Spatial Dimensions with Beamforming

For designing a transmit beamforming and receive combining efficiently, we assumed that perfect CSI of $\mathbf{H}$ is available at the BS. If the BS also has the perfect CSI of the eavesdropping channel $\mathbf{G}$, a secure signal transmission can be possible with transmit beamforming (e.g. Zero-Forcing Beamforming) to nullify the eavesdropping channel. However, it is impossible to obtain the eavesdropping CSI due to the

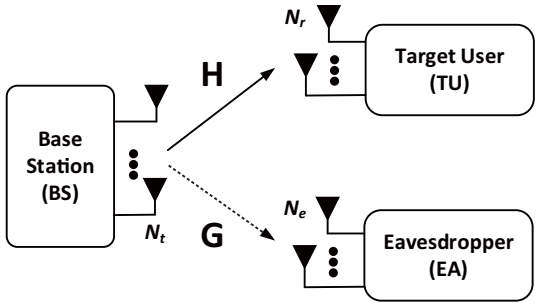

Fig. 1. MIMO wireless network with a eavesdropper

passive posture of the EA. Therefore, without any information about the eavesdropping channel, transmit beamforming is generally designed for maximizing the spectral efficiency or improving the reliability.

With CSI of $\mathbf{H}$, spatial dimensions are generally obtained by singular value decomposition (SVD). The SVD of channel $\mathbf{H} = \mathbf{U}\mathbf{D}\mathbf{V}^{\dagger}$ can be performed, where $\mathbf{U} \in \mathbb{C}^{N_r \times N_r}$, $\mathbf{V} \in \mathbb{C}^{N_t \times N_t}$ are unitary matrices, and $\mathbf{D} \in \mathbb{C}^{N_r \times N_t}$ is a diagonal matrix whose non-zero entries $\sqrt{\lambda_i}$ are the square roots of the eigenvalues of $\mathbf{H}^{\dagger}\mathbf{H}$. With the transmit beamforming matrix $\mathbf{V}$ and the receive combining matrix $\mathbf{U}^{\dagger}$, the combined signals can be rewritten as

$$\begin{aligned} \mathbf{U}^{\dagger}\mathbf{y} &= \underbrace{\mathbf{U}^{\dagger}\cdot\mathbf{U}}_{\mathbf{I}}\mathbf{D}\underbrace{\mathbf{V}^{\dagger}\cdot\mathbf{V}}_{\mathbf{I}}\mathbf{x} + \mathbf{U}^{\dagger}\mathbf{n}, \\ \tilde{\mathbf{y}} &= \mathbf{D}\mathbf{x} + \tilde{\mathbf{n}}. \end{aligned} \tag{3}$$

Since $\mathbf{U}$ is unitary matrix, noise vector $\tilde{\mathbf{n}}$ and $\mathbf{n}$ have the same distribution. Then, the i-th combined signal of $\tilde{\mathbf{y}}$ can be obtained as

$$\tilde{y_i} = \sqrt{\lambda_i}x_i + \tilde{n}_i, \quad i = 1, ..., N_{min}, \tag{4}$$

where $N_{min} = \min(N_t, N_r)$. From (4), it is apparent that the MIMO wireless channel has been transformed into independent N_{min} spatial dimensions by a transmit beamforming and a receive combining.

C. Threshold Secret Sharing Transmission

Threshold secret sharing is a conventional scheme in cryptography created by Adi Sharmir [6]. In the scheme, a secret data is divided into n parts by a polynomial of degree $t-1$. To reconstruct the secret data, t out of n parts must be needed for solving the polynomial problem correctly. Therefore, this is called the (t, n)-threshold secret sharing scheme [7]-[9].

With the conventional scheme in MIMO wireless network, the i-th part with a polynomial can be obtained as

$$S_i = f(i) = (a_0 + a_1 i + ... + a_{T-1} i^{T-1}) \bmod p, \tag{5}$$

where coefficient a_0 is the original secret data K while other coefficient $a_1, a_2, ..., a_{T-1}$ are all randomly chosen at the BS. And p and T are a large prime number greater than any of the coefficients and a system parameter to control the security strength, respectively. We assumed that the value of p is pre-shared with BS and TU for secure communications.

Divided parts are modulated with a modulation scheme (ex. QPSK, QAM) and then the modulated parts are transmitted through spatial dimensions with beamforming in (3) as

$$\mathbf{y} = \mathbf{H}\cdot\mathbf{V}\cdot\mathbf{x} + \mathbf{n}, \tag{6}$$

where $\mathbf{x} = [\tilde{S_1}, \tilde{S_2}, ..., \tilde{S}_{N_{min}}]^{\mathbf{T}}$ and $\tilde{S_i}$ denotes the i-th modulated secret part.

D. Reconstruction of the Secret

With the receive combining matrix $\mathbf{U}^{\dagger}$ and the channel compensation of the received parts in (4), the demodulated secret parts $[\hat{S_1}, \hat{S_2}, ..., \hat{S}_{N_{min}}]$ can be obtained at the target user. With N_{min} demodulated parts, the target user randomly chooses a subset composed of T parts (ex. $[\tilde{S_1}, \tilde{S_2}, ..., \tilde{S_T}]$) and estimates the Lagrange interpolating polynomial in (5) as

$$\hat{f}(i) = \sum_{j=1}^{T} \hat{S_j} \cdot \left[\prod_{k=1, k\neq j}^{T} \frac{i - i_k}{i_j - i_k} \right] \bmod p, \tag{7}$$

where i_j, i_k means the index parameter of a subset. Then, ideally, the secret data can be obtained by $\hat{f}(0) = \hat{K}$.

However, since secret parts are transmitted with fading channel and noise in MIMO wireless network, the reconstruction of the secret must be considered with demodulation error. In other words, the derived result in (7) can be changed depends on how the user chooses a subset. In the proposed scheme, the number of subset (N_s) is

$$N_s = {}_{N_{min}}\mathbf{C}_T, \tag{8}$$

where $\mathbf{C}$ denotes combination function. Therefore, a set ($\mho$) of the estimated secret data $\hat{K}$ is also obtained as $\mho = \{\hat{K_1}, \hat{K_2}, ..., \hat{K}_{N_s}\}$ and the secret data is finally determined by majority rule of $\mho$.

III. Eavesdropper Behavior

For eavesdropping efficiently, channel information about $\mathbf{H}$ and $\mathbf{G}$ are needed at the EA. First, based on the channel estimation technique, EA knows $\mathbf{G}$ from pilot and preamble signals of BS. Also, we assumed that EA can be obtained $\mathbf{H}$ and p by eavesdropping the TU's channel feedback and the exchanged information for secure data transmission.

With channel information of $\mathbf{H}$, EA predicts $\mathbf{V}$ for target user by the SVD of $\mathbf{H}$. Therefore, for efficient eavesdropping, the eavesdropping signal in (2) can be combined using the receive matrix $\mathbf{U_e}$ considering channel compensation as

$$\mathbf{U_e}\cdot\mathbf{z} = \mathbf{U_e}\cdot\mathbf{G}\cdot\mathbf{V}\cdot\mathbf{x} + \mathbf{U_e}\cdot\mathbf{w} = \mathbf{D_e}\cdot\mathbf{x} + \tilde{\mathbf{w}}, \tag{9}$$

where $\mathbf{U_e} = \frac{(\mathbf{G}\cdot\mathbf{V})^{-1}}{||(\mathbf{G}\cdot\mathbf{V})||}$ and $\mathbf{D_e}$ denotes the diagonal matrix through the inverse matrix operation. Then, the transmitted secret parts are estimated by compensation of $\mathbf{D_e}$. Finally, the secret data can be obtained by the same procedure of the secret reconstruction in section II.D.

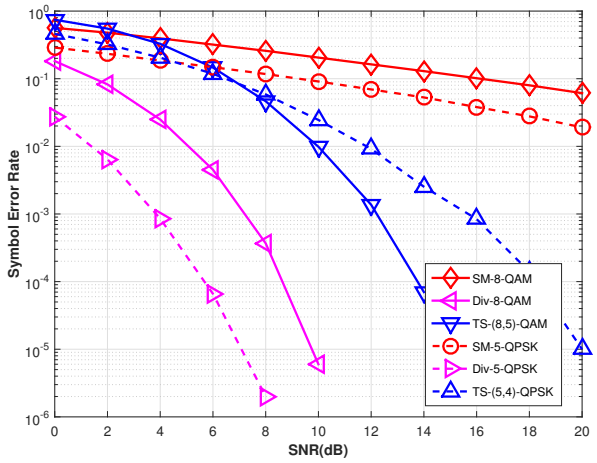

Fig. 2. Symbol error rate vs. SNR (dB) at the target user, where $N_t = N_r = N_e = \{5, 8\}$ and T ={4, 5}.

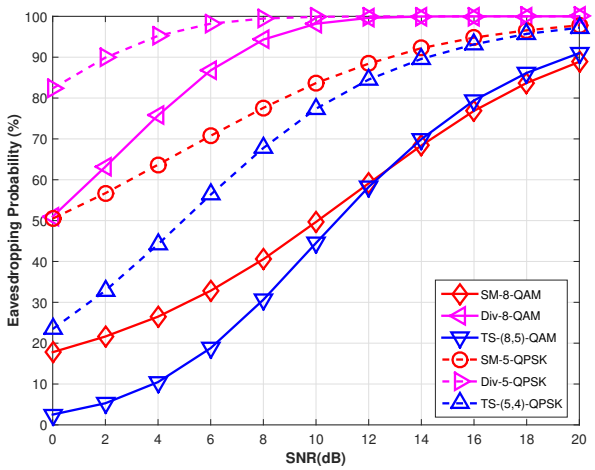

Fig. 3. Eavesdropping probability vs. SNR(dB) at the eavesdropper, where $N_t = N_r = N_e = \{5, 8\}$ and T ={4, 5}.

IV. Numerical Results

In this section, we provide the symbol-error-rate (SER) and eavesdropping probability (EP) numerical results of the proposed secret sharing scheme. For simulation, MIMO wireless channels are considered as shown in Fig. 1, where the channel coefficients are assumed to be flat Rayleigh fading with mutually independent and additive white Gaussian noise terms having zero mean and equivalent variance $\mathbb{CN}(0, \sigma^2)$. We compare the threshold secret sharing scheme (TS) with spatial multiplexing transmission (SM) [10] and diversity transmission (Div) [11]. The specific parameters are indicated at each figure.

In Fig. 3, the SER versus signal-to-noise ratio (SNR) at the TU is evaluated for different approaches. We can see that TS achieves better performance compared with SM. Especially, in high SNR region, it achieves same diversity gain compared with Div because the TS can recover the secret data by majority rule even though there are some miss-decoded parts due to the low eigenvalues in (4). We can see that SER performance is determined by a gap between a threshold value and N_{min}. If a threshold value becomes closer to N_{min}, the performance of the TS becomes closer to that of SM because the secret data can be reconstructed only when all parts are successfully decoded to solve the polynomial. Also, if a threshold value becomes closer to 1, the performance of the TS becomes closer to that of Div because the secret data can be obtained easily by solving the polynomial with a small number of parts.

In Fig. 4, we evaluate the performance of EP at the eavesdropper under different SNR. The proposed TS shows good performance against eavesdropping compared with SM and Div, especially in low SNR region. Since the transmit beamforming $\mathbf{V}$ is designed considering $\mathbf{H}$ only, a gain of the effective eavesdropping channel $\mathbf{G} \cdot \mathbf{V}$ is generally degraded compared to a gain of the effective main channel $\mathbf{H} \cdot \mathbf{V}$ in physical layer. Therefore, in the proposed scheme, EA is difficult to estimate the sufficient number ($\geq T$) of parts correctly and fails to reconstruct the secret data.

V. Conclusion

In this paper, we consider a threshold secret sharing to enhance physical layer security against an eavesdropper. The simulation shows that the eavesdropping probability of the proposed scheme is better than those of the conventional approaches. Also, since there is an inverse proportion between SER and EP, it is necessary to set an appropriate threshold value according to the service type and purpose.

Acknowledgement

This work was supported by Electronics and Telecommunications Research Institute (ETRI) grant funded by the Korean government. [18ZF1100, Wireless Transmission Technolgy in Multi-point to Multi-point Communications]

References

[1] A. D. Wyner, "The wire-tap channel," *The Bell Sys. Tech. J.*, vol. 54, no. 8, pp. 1355?1387, Oct. 1975.

[2] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," *in ISIT*, pp. 356-360, 2006.

[3] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547-2553, June 2009.

[4] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*", vol. 57, no. 8, pp. 4961-4972, Aug. 201.

[5] J. Myung, H. Heo, and J. Park, "Joint Beamforming and Jamming for Physical Layer Security," *ETRI Journal*, vol. 37, no. 5, pp. 898-905, Oct. 2015.

[6] Adi Shamir, " How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612-613, Nov 1979.

[7] C. C. Yang, T. Y. Chang, and M. S. Hwang , "A (t, n) multi-secret sharing scheme," *Applied Mathematics and Computation*, vol. 151, no. 2, pp. 483-490, Apr 2004.

[8] C. W. Chan and C. C. Chang, "A scheme for threshold multi-secret sharing," *Applied Mathematics and Computation*, vol. 166, no. 1, pp. 1-14, Jul 2005.

[9] L. J. Pang and Y. M. Wang , "A new (t, n) multi-secret sharing scheme based on Sharmir's secret sharing," *Applied Mathematics and Computation*, vol. 167, no. 2, pp. 840-848, Aug 2005.

[10] Q. H. Spencer, A. L. Swindlehurst and M. Haardt, "Zero-forcing methods for downlink spatial multiplexing in multiuser MIMO channels," *IEEE Trans. Signal Process.*, vol. 52, no. 2, pp. 461-471, Feb. 2004.

[11] T. K. Y. Lo, "Maximum ratio transmission," *IEEE Int. Conf. Commun.*, pp.1310-1314, June 1999.