Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 4143061, 7 pages
https://doi.org/10.1155/2018/4143061

Research Article

Threshold Secret Sharing Transmission against Passive Eavesdropping in MIMO Wireless Networks

Jungho Myung,[1] Keunyoung Kim,[1] and Taehong Kim [2]

[1]*Electronics and Telecommunications Research Institute (ETRI), Republic of Korea*
[2]*School of Information and Communication Engineering, Chungbuk National University, Republic of Korea*

Correspondence should be addressed to Taehong Kim; taehongkim@cbnu.ac.kr

Received 31 July 2018; Revised 19 September 2018; Accepted 2 October 2018; Published 22 October 2018

Guest Editor: Phuc V. Trinh

We propose a threshold secret sharing scheme for secure communications in multiple input and multiple output wireless networks. In the proposed scheme, the base station divides the secret data into N_{min} parts using a polynomial of degree $T-1$ ($T \leq N_{min}$) and transmits the divided data to the legitimate user by beamforming with multiple spatial dimensions. Then, at the user, the secret data can be reconstructed with a sufficient number ($\geq T$) of divided parts by using the Lagrange interpolating polynomial. However, it is difficult for the eavesdropper to correctly estimate the T parts due to the difference between the main channel with beamforming and the eavesdropping channel in the physical layer, which results in the failure of secret data reconstruction. The numerical results show that the eavesdropping probability of the proposed scheme is lower than those of conventional schemes. Moreover, we analyze the symbol-error-rate and show that the theoretical result is well aligned with simulation results.

1. Introduction

Recently, multiple input and multiple output (MIMO) wireless networks have attracted significant attention due to the potential performance improvements; they have been shown to lead to spatial multiplexing or diversity gain [1–5]. The spatial dimensions derived from multiple antennas have initiated many new transmission techniques utilizing space as a new resource other than frequency and time [3–5]. Among the conventional methods, maximum ratio transmission [3] is proposed, in which a single stream is sent for achieving full diversity gain from multiple spatial dimensions. In addition, for throughput enhancement, spatial multiplexing transmission has been proposed to transmit multiple streams simultaneously [4, 5]. However, most of existing works only focus on spatial dimensions by multiple antennas in order to maximize the spatial multiplexing gain or diversity gain without considering security.

Wireless transmission is inherently vulnerable to eavesdropping due to the broadcast nature of the wireless medium [6–12]. Although a large number of security measures—from wired equivalent privacy in the wireless link layer to transport layer security in the application layer—have already been developed and widely deployed throughout network layers, the fact remains that it is these very measures that must now confront substantial challenges by attackers or eavesdroppers with immense computing resources acquirable from a cloud or bounded error quantum polynomial time algorithms leveraging quantum computers, to list just a few. As one of new attempts to overcome this problem, physical layer security (PLS) has been introduced to achieve fundamental secrecy in the sense that it does not rely on any intractability assumptions unlike cryptographic algorithms implemented in higher network layers. With a single antenna configuration, Wyner first introduced a wiretap channel and the associated secrecy, the results of which show the feasibility of ultimately secure communication [6]. However, there is a problem in that secrecy cannot be guaranteed if the gain of the eavesdropping channels is higher than the gain of the main channel, that is, the channel of the target user. To overcome this problem, PLS with multiple antennas has been proposed [8–12]. In MIMO wireless networks, by beamforming and jamming techniques, the secrecy can be provided even though the quality of the main channel is

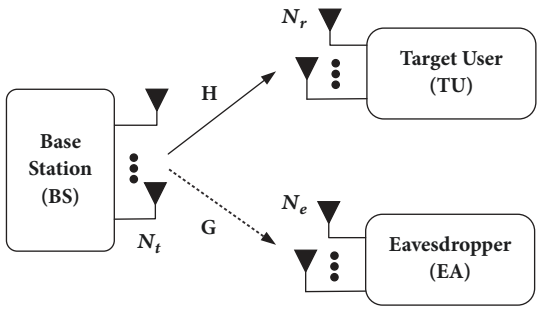

Figure 1: MIMO wireless networks with an eavesdropper.

worse than the quality of the eavesdropping channel. Most of existing works have only focused on increasing the secrecy rate by beamforming and jamming design, assuming that the 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, a new transmission technique with multiple spatial dimensions is needed on the condition that the transmitter cannot know the eavesdropping channels.

In this paper, we propose a threshold secret sharing transmission for secure communications in the absence of an eavesdropping channel information. In the proposed scheme, the secret data is divided into N_{min} parts using a polynomial of degree $T-1$ and then transmitted to the target 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 the divided parts are combined together. We also propose the majority rule for secret reconstruction to overcome fading and noise impairments in wireless channels. At the point of the eavesdropper, it is difficult to correctly estimate the T parts due to the difference between main channel and eavesdropping channel in the physical layer. Therefore, attempt to reconstruct the secret data is unsuccessful. The numerical results show that the eavesdropping probability of the proposed approach is better than those of the conventional approaches. Also, we provide an analysis of SER for the proposed secret sharing scheme and verify that the proposed theoretically derived results well agree with the Monte-Carlo simulation results.

Notations. $\mathbf{X}^T$, $\mathbf{X}^*$, $\mathbf{X}^\dagger$, $\|\mathbf{X}\|$, and $\mathbf{E}[\cdot]$ denote the transpose, the conjugate transpose, the pseudo inverse, the Euclidean norm of matrix $\mathbf{X}$, and the expectation function, respectively.

2. System Model

As shown in Figure 1, we consider MIMO wireless networks with a base station (BS) with N_t transmit antennas, a target user (TU) with N_r receiving 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 $\mathbf{G}$. The channel coefficients are assumed to be mutually independent Rayleigh flat fading with additive white Gaussian noise (AWGN) having zero mean and unit variance.

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 $\mathbf{n}$ denote the received signal vector, the transmitted signal vector, and the 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 $\mathbf{w}$ denote the received signal vector and the AWGN vector at the EA, respectively.

3. Threshold Secret Sharing Transmission in MIMO Wireless Networks

3.1. Threshold Secret Sharing Generator. Threshold secret sharing is a well-known scheme in cryptography introduced by Adi Sharmir [13]. In the scheme, a secret data is divided into N parts by a polynomial of degree $T-1$. To reconstruct the secret data, a minimum number of parts (T) is required for solving the polynomial problem correctly. In the threshold scheme, this number is less than the total number of parts ($T \leq N$). Therefore, this is called the (T, N)-threshold secret sharing scheme [14–16].

For spectral efficiency and throughput enhancement in MIMO networks, a BS transmits independent and separately encoded signals, so-called streams, from each of the multiple transmit antennas. Considering our system model, the number of streams (that is, the spatial multiplexing order) can be obtained as

$$N_{min} = \min\left(N_t, N_r\right). \tag{3}$$

It means that there are N_{min} independent wireless paths between the BS and the TU by beamforming.

With multiple paths and the threshold scheme, the BS divides the secret data into N_{min} parts using a polynomial of degree $T-1$ ($T \leq N_{min}$). Then, the ith part with a polynomial can be calculated as

$$S_i = f(i) = \left(a_0 + a_1 i + \cdots + a_{T-1} i^{T-1}\right) \bmod p, \tag{4}$$

where coefficient a_0 is the original secret data while the other coefficients $a_1, a_2, \ldots, a_{T-1}$ are all randomly chosen at the BS. In addition, p, T, and mod denote a large prime number greater than any of the coefficients, a parameter controlling the balance between the symbol-error-rate (SER) and eavesdropping probability (EP), and the p-modulo operation, respectively. We assume that the value p and T are preshared with BS and TU.

For example, let us examine how the proposed scheme works in MIMO wireless networks with $N_t = N_r = 5$. In the given antenna configuration, the value of N_{min} is determined to be 5 by (3). Also, with preshared parameter (ex. $p = 17$ and $T = 3$), BS randomly chooses the remaining coefficients as a number smaller than p (ex. $a_1 = 4, a_2 = 2$). Then, S_i for secret data can be obtained as

$$S_i = f(i) = \underbrace{4}_{\text{secret data}} + 4i + 2i^2 \bmod 17, \tag{5}$$

and $S_1 = 10$, $S_2 = 3$, $S_3 = 0$, $S_4 = 1$, and $S_5 = 6$.

The divided parts in (4) are modulated (ex. QPSK, QAM) and then the modulated signals are transmitted to the target user through spatial dimensions with the transmit beamforming matrix $\mathbf{V}$ as

$$\mathbf{y} = \mathbf{HVx} + \mathbf{n}, \tag{6}$$

where $\mathbf{x} = [\widetilde{S_1}, \widetilde{S_2}, \ldots, \widetilde{S}_{N_{min}}]^T$ and $\widetilde{S_i}$ denotes the i-th modulated signal. Also, the eavesdropping signal with transmit beamforming is rewritten as

$$\mathbf{z} = \mathbf{GVx} + \mathbf{w}. \tag{7}$$

3.2. Spatial Dimension with Beamforming. For the design of an efficient transmit beamforming and receive combining efficiently, we assume that the perfect CSI of $\mathbf{H}$ is available at the BS by channel reciprocity or feedback. If the BS also has the perfect CSI of the eavesdropping channel $\mathbf{G}$, a secure signal transmission can be possible using transmit beamforming (e.g., Zero-Forcing Beamforming) to nullify the eavesdropping channel. However, due to the passive characteristic of the EA, it is hard to obtain the eavesdropping CSI at the BS. Therefore, without any information about the eavesdropping channel, transmit beamforming is generally designed for maximizing the spectral efficiency or improving the reliability of the target user.

With the perfect CSI of $\mathbf{H}$, the spatial dimensions in the MIMO networks are obtained by singular value decomposition (SVD). The channel $\mathbf{H}$ can be decomposed to $\mathbf{UDV}^*$ by using SVD, 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 nonzero entries $\sqrt{\lambda_i}$ are the square roots of the eigenvalues of $\mathbf{H}^*\mathbf{H}$. With the transmit beamforming matrix $\mathbf{V}$ and the receive combining matrix $\mathbf{U}^*$, the combined signal at the target user can be rewritten as

$$\begin{aligned} \mathbf{U}^* \cdot \mathbf{y} &= \underbrace{\mathbf{U}^* \cdot \mathbf{U}}_{\mathbf{I}} \mathbf{D} \underbrace{\mathbf{V}^* \cdot \mathbf{V}}_{\mathbf{I}} \mathbf{x} + \mathbf{U}^* \cdot \mathbf{n}, \\ \widetilde{\mathbf{y}} &= \mathbf{Dx} + \widetilde{\mathbf{n}}. \end{aligned} \tag{8}$$

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

$$\widetilde{y_i} = \sqrt{\lambda_i} x_i + \widetilde{n_i}, \quad i = 1, \ldots, N_{min}. \tag{9}$$

3.3. Reconstruction of the Secret. With the receive combining matrix $\mathbf{U}^*$ and the channel compensation of the received signals, the demodulated data $[\widehat{S_1}, \widehat{S_2}, \ldots, \widehat{S}_{N_{min}}]$ can be obtained at the target user. Then, the target user with N_{min} demodulated data randomly chooses a subset composed of T data (ex. $[\widehat{S_1}, \widehat{S_2}, \ldots, \widehat{S}_T]$) and estimates the Lagrange interpolating polynomial as

$$\widehat{f}(i) = \sum_{j=1}^{T} \widehat{S_j} \cdot \left[\prod_{k=1, k \neq j}^{T} \frac{i - i_k}{i_j - i_k} \right] \bmod p, \tag{10}$$

where i_j, i_k means the index parameter of a subset. Then, the secret data can be obtained by $\widehat{f}(0) = \widehat{K}$. For example, with $N_{min} = 5$, $T = 3$, $p = 17$, and the demodulated data $\widehat{S}_1 = 10$, $\widehat{S}_2 = 3$, $\widehat{S}_4 = 1$, and the secret data and a polynomial of degree $T - 1$ can be reconstructed by (10) as

$$\begin{aligned} \widehat{f}(i) &= \sum_{j=1}^{3} \widehat{S_j} \cdot \left[\prod_{k=1, k \neq j}^{3} \frac{i - i_k}{i_j - i_k} \right] \bmod 17, \\ &= \left(10 \cdot \frac{i-2}{1-2} \cdot \frac{i-4}{1-4} + 3 \cdot \frac{i-1}{2-1} \cdot \frac{i-4}{2-4} + 1 \cdot \frac{i-1}{4-1} \right. \\ &\quad \left. \cdot \frac{i-2}{4-2} \right) \bmod 17, \\ &= \left(21 - 13i + 2i^2\right) \bmod 17 = \underbrace{4}_{\text{secret data}} + 4i + 2i^2. \end{aligned} \tag{11}$$

However, since modulated signals are transmitted with fading channel and noise in MIMO wireless networks, the reconstruction of the secret must consider the demodulation error. In other words, the derived result in (10) can change depending on which subset a user chooses. Considering the proposed secret sharing scheme, the number of the subset (N_s) is

$$N_s = \mathbf{C} \binom{N_{min}}{T}, \tag{12}$$

where $\mathbf{C}\binom{a}{b}$ denotes the number of possible combinations of b objects from a set of a objects. Then, a set $(\mho)$ of the estimated secret data $\widehat{K}$ from (10) and (12) is obtained as

$$\mho = \left\{ \widehat{K}_1, \widehat{K}_2, \ldots, \widehat{K}_{N_s} \right\}, \tag{13}$$

and the secret data is finally determined by majority rule of $\mho$ to reduce the effect of the demodulation error. Figure 2 shows a simplified block diagram of the proposed threshold secret sharing system in MIMO wireless networks.

3.4. Performance Analysis. In this subsection, we provide an analysis of SER to show how SER is affected by T, N_{min}, and signal-to-noise ratio (SNR). In our MIMO networks, the i-th modulated signal $\widetilde{S_i}$ is transmitted to the user through the i-th spatial dimension in (9) by beamforming technique in Section 3.2. To find the distribution of the i-th eigenvalue, the joint probability density function (E_{JPDF}) of the N_{min}-eigenvalues of Wishart matrices, $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{N_{min}} \geq 0$, is defined [17] as

$$\begin{aligned} E_{JPDF} &= \frac{1}{K_{m,n}} e^{-(1/2)\sum_{i=1}^{N_{min}} \lambda_i} \prod_{i=1}^{N_{min}} \lambda_i^{(1/2)(N_{max} - N_{min} - 1)} \\ &\quad \cdot \prod_{i<j} \left(\lambda_i - \lambda_j\right) d\lambda_1 \cdots d\lambda_{N_{min}}, \end{aligned} \tag{14}$$

where

$$\begin{aligned} K_{m,n} &= \left(\frac{2^{N_{max}}}{\pi} \right)^{N_{min}/2} \\ &\quad \cdot \prod_{i=1}^{N_{min}} \Gamma\left(\frac{N_{max} - i + 1}{2} \right) \Gamma\left(\frac{N_{min} - i + 1}{2} \right), \\ N_{max} &= \max\left(N_t, N_r\right). \end{aligned} \tag{15}$$

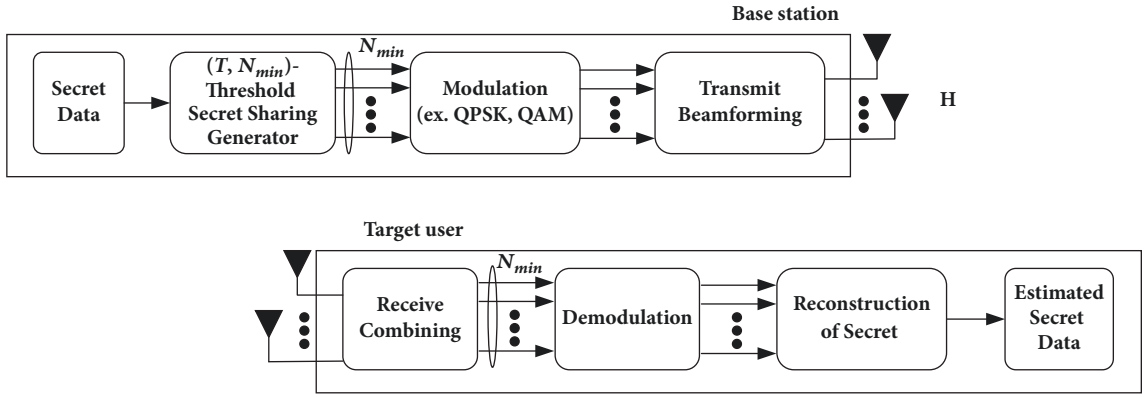

Figure 2: A simplified block diagram of the proposed threshold secret sharing system in MIMO wireless networks.

Then, the density of the i-th eigenvalue can be obtained by integrating (14) as

$$E_{PDF}^{i} = \int_{R_{+}^{N_{min}-1}} E_{JPDF} d\Omega, \tag{16}$$

where $d\Omega = d\lambda_1 \cdots d\lambda_{i+1} d\lambda_{i-1} \cdots d\lambda_{N_{min}}$ and the integration takes place over the positive orthant, $R_{+}^{N_{min}-1} = \{(\lambda_1, \ldots, \lambda_{i+1}, \lambda_{i-1}, \ldots, \lambda_{N_{min}}) : \lambda \geq 0\}$.

Also, if $\log_2 M$ is even integer, SER of M-QAM in AWGN channel can be defined [18] as $P_{SER} = 1 - (1-p)^2$ with

$$p = \left(1 - \frac{1}{\sqrt{M}}\right) erfc\left(\sqrt{\frac{3}{2(M-1)} \frac{E_s}{N_o}}\right), \tag{17}$$

where

$$erfc(x) = \frac{2}{\sqrt{\pi}} \int_{x}^{\infty} e^{-t^2} dt, \tag{18}$$

and E_s/N_o means the signal-to-noise ratio. Then, SER of M-QAM in fading channel can be obtained as

$$P_s = 2\mathbf{E}[p] - \mathbf{E}\left[p^2\right]. \tag{19}$$

Also, with N_{min} spatial dimensions in our MIMO network, SER of the i-th dimension is rewritten as

$$P_s^i = 2\mathbf{E}_i[p] - \mathbf{E}_i\left[p^2\right], \tag{20}$$

where

$$\begin{aligned} \mathbf{E}_i[p] &= \int_0^{\infty} \overline{p} \cdot E_{PDF}^{i} d\lambda_i, \\ \mathbf{E}_i\left[p^2\right] &= \int_0^{\infty} \overline{p}^2 \cdot E_{PDF}^{\mathrm{i}} d\lambda_i, \\ \overline{p} &= \left(1 - \frac{1}{\sqrt{M}}\right) erfc\left(\sqrt{\frac{3\lambda_i}{2(M-1)} \frac{E_s}{N_o}}\right). \end{aligned} \tag{21}$$

Since we cannot find any closed-form expression in our best knowledge, P_s^i needs to be calculated by numerically integrating (21). Then, based on the majority rule in Section 3.3, SER of the proposed threshold sharing scheme can be obtained by (10) and (20) as

$$P_s = 1 - \sum_{sum(\mathbf{k}) \leq N_{min} - T - 1} \prod_{i=1}^{N_{min}} \left(P_s^i\right)^{k_i} \cdot \left(1 - P_s^i\right)^{1-k_i}, \tag{22}$$

where

$$\begin{aligned} \mathbf{k} &= \left\{k_1, \ldots, k_i, \ldots, k_{N_{min}}\right\}, \\ sum(\mathbf{k}) &= \sum_{i=1}^{N_{min}} k_i, \quad k_i \in \{0, 1\}. \end{aligned} \tag{23}$$

4. Eavesdropper Behavior

In this section, we explain the eavesdropper's behavior against the threshold secret sharing system.

4.1. With only **G**. If EA is a legitimate user and an internal eavesdropper in wireless network, EA can easily obtain the channel state information of **G** by channel estimation using pilot and preamble signals of BS [19]. With only information **G**, the eavesdropping signal in (7) is combined by the receive combining matrix $\mathbf{U}_{\mathbf{e}}^{\mathbf{G}}$ to eliminate interference caused by channel **G** as

$$\begin{aligned} \mathbf{U}_{\mathbf{e}}^{\mathbf{G}} \cdot \mathbf{z} &= \mathbf{U}_{\mathbf{e}}^{\mathbf{G}} \cdot \mathbf{GVx} + \mathbf{U}_{\mathbf{e}}^{\mathbf{G}} \cdot \mathbf{w} \\ &= \widetilde{\mathbf{V}}\mathbf{x} + \widetilde{\mathbf{w}}^{\mathbf{G}}, \end{aligned} \tag{24}$$

where

$$\mathbf{U}_{\mathbf{e}}^{\mathbf{G}} = \frac{\mathbf{G}^{\dagger}}{\|\mathbf{G}\|}. \tag{25}$$

In this case, since there is no information of the transmit beamforming matrix **V** and the eavesdropper fails to decode the received signal correctly, except for the transmit beamforming matrix $\mathbf{V} = \mathbf{I}$.

4.2. With **G** *and* **H**. For efficient eavesdropping, channel information about **H** and **G** is needed at the EA. First,

based on the channel estimation technique, EA knows **G**. We also assumed that smart EA can be obtained **H** and p by eavesdropping the TU's channel feedback and the exchanged information for secure data transmission.

Then, with the channel information of **H**, EA predicts **V** for the target user by SVD of **H**. Therefore, for efficient eavesdropping, the eavesdropping signal can be combined by the receive matrix $\mathbf{U}_e^{\mathbf{GH}}$ considering channel compensation as

$$\begin{aligned}\mathbf{U}_e^{\mathbf{GH}} \cdot \mathbf{z} &= \mathbf{U}_e^{\mathbf{GH}} \cdot \mathbf{GVx} + \mathbf{U}_e^{\mathbf{GH}} \cdot \mathbf{w} \\ &= \widetilde{\mathbf{D}}_e \mathbf{x} + \widetilde{\mathbf{w}},\end{aligned} \tag{26}$$

where

$$\mathbf{U}_e^{\mathbf{GH}} = \frac{(\mathbf{G} \cdot \mathbf{V})^{\dagger}}{\|\mathbf{G} \cdot \mathbf{V})\|}, \tag{27}$$

and $\widetilde{\mathbf{D}}_e$ denotes the diagonal matrix through the inverse matrix operation. Then, the transmitted data are estimated by the compensation of $\widetilde{\mathbf{D}}_e$. Finally, the secret data can be obtained through the same procedure as that of the secret reconstruction described in Section 3.3.

5. Numerical Results

In this section, we provide the simulation results of the symbol-error-rate (SER) and the eavesdropping probability of the proposed scheme. For simulation, MIMO wireless channels are considered as shown in Figure 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 (T, N_{min})-threshold secret sharing scheme (TS-(T, N_{min})) with spatial multiplexing transmission (SM) and diversity transmission (Div). In SM, for full multiplexing gain, we assumed that the BS transmits N_{min} independent data to the TU by beamforming. Therefore, an instantaneous EP at the EA is defined by N_{sm} over N_{min}, where N_{sm} is the number of successfully decoded data. Also, since a single data transmission is assumed for full diversity gain in Div, an instantaneous EP is defined by eavesdropping success (1) or failure (0). The specific parameters are indicated at each figure.

In Figure 3, SER versus SNR at the TU is evaluated for different approaches. With full diversity gain, Div shows the best SER performance. On the other hand, SM shows the worst SER performance, because N_{min} stream is simultaneously transmitted through spatial dimensions with an equal transmit power constraint. In general, we can see that TS achieves better performance than SM. In the high SNR region in particular, it achieves the diversity gain as 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 (9). On the contrary, in a low SNR region, due to the error propagation of majority rule, the TS shows the worst SER performance. In addition, through the slope of the graph, we can see that SER performance is determined by a gap between T and N_{min}. With the fixed N_{min}, the performance of the TS approaches that of the SM as T approaches to N_{min}, because the secret data can be reconstructed only when all parts are successfully decoded to solve the polynomial. In addition, if T approaches 1, the performance of the TS approaches that of Div, because the secret data can be easily obtained by solving the polynomial with a small number of parts. It is noticeable that the theoretically derived result in Section 3.4 is well matched with simulation results.

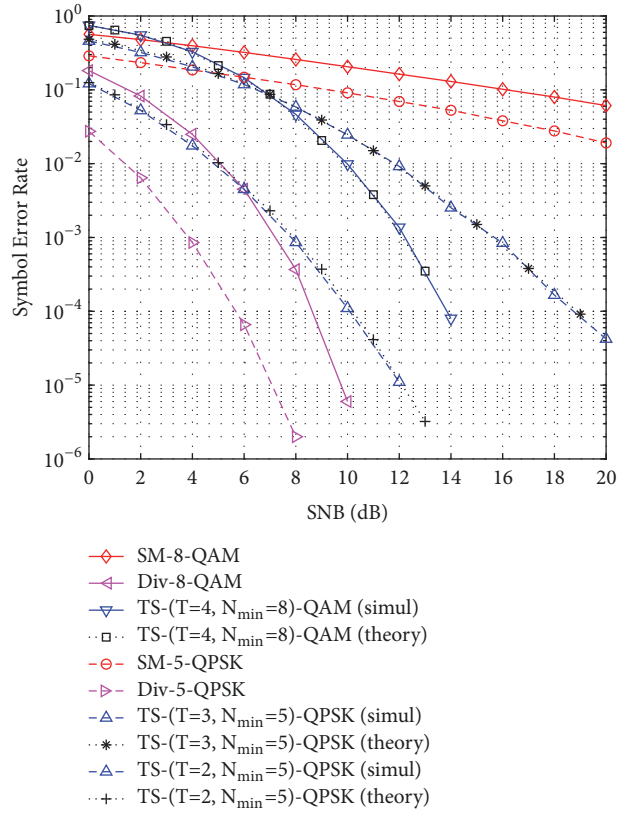

FIGURE 3: Symbol error rate vs. SNR (dB) at the target user, where $N_t = N_r = \{8, 5\}$ and $T = \{4, 3, 2\}$.

In Figure 4, we evaluate the performance of EP at the eavesdropper under different SNR. With full diversity gain, Div shows the most vulnerable performance to eavesdropping. On the other hand, the proposed TS shows good performance against eavesdropping compared to SM and Div, especially in the low SNR region. If only G is available, the eavesdropping fails due to the intersymbol interference caused by beamforming matrix **V**. Even though the smart EA has the perfect CSIs of both **G** and **H**, it is hard to estimate the sufficient number ($\geq T$) of parts correctly, and it fails to reconstruct the secret data because the gain of the effective eavesdropping channel **GV** is degraded compared to the gain of the effective main channel **HV** in physical layer. We can also see that EP is determined by the threshold value. When the threshold value is set to be N_{min}, the most secure communication against eavesdropping is possible. Therefore, an appropriate threshold value should be set according to the user's purpose because there is a performance trade-off between SER and DP depending on the threshold value.

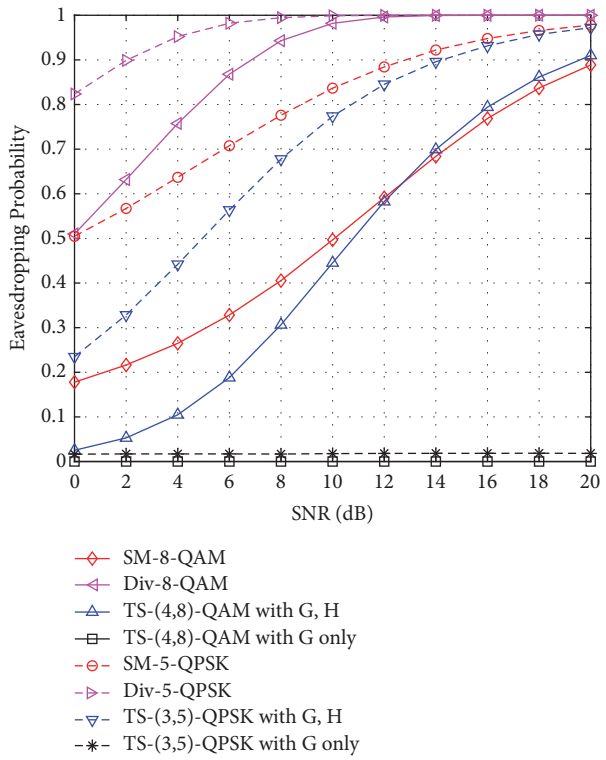

FIGURE 4: Eavesdropping probability vs. SNR(dB) at the eavesdropper, where $N_t = N_r = N_e = \{8, 5\}$ and $T = \{4, 3\}$.

6. Conclusion

In this paper, we considered a threshold secret sharing to enhance physical layer security against an eavesdropper. In the proposed scheme, with N_{min} spatial dimensions by beamforming, the secret data is divided into N_{min} parts using a unique polynomial of degree $T - 1$ and then transmitted to the user. Then, the user can reconstruct the secret data with a sufficient number ($\geq T$) of parts by using the Lagrange interpolating polynomial. However, at the eavesdropper, the reconstruction of secret data fails due to the difference between the main channel and the eavesdropping channel in the physical layer. The simulation shows that the eavesdropping probability of the proposed scheme is better than those of the conventional approaches. Moreover, we found that the threshold value plays an important role in our scheme. Therefore, in the future, we would like to extend our current scheme with a fixed threshold value to a dynamic scheme where the base station can determine their own threshold value to simultaneously maximize the user's symbol error rate and to minimize the eavesdropping probability with imperfect CSI.

Data Availability

The data used to support the findings of this study are included within the article.

Disclosure

A preliminary version of this paper was presented at International Conference on Ubiquitous and Future Networks (ICUFN), Czech Republic, July 2018 [20].

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

T. Kim is the corresponding author of this paper.

Acknowledgments

This research was partially supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2016R1D1A1B03933007) and Electronics and Telecommunications Research Institute (ETRI) grant funded by the Korean government (18ZF1100, Wireless Transmission Technology in Multi-point to Multipoint Communications).

References

[1] M. H. M. Costa, "Writing on dirty paper," *IEEE Transactions on Information Theory*, vol. 29, no. 3, pp. 439–441, 1983.

[2] G. J. Foschini and M. J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas," *Wireless Personal Communications*, vol. 6, no. 3, pp. 311–335, 1998.

[3] T. K. Y. Lo, "Maximum ratio transmission," *IEEE Transactions on Communications*, vol. 47, no. 10, pp. 1458–1461, 1999.

[4] P. W. Wolniansky, G. J. Foschini, G. D. Golden, and R. A. Valenzuela, "V-BLAST: an architecture for realizing very high data rates over the rich-scattering wireless channel," in *Proceedings of the URSI International Symposium on Signals, Systems, and Electronics (ISSSE '98)*, pp. 295–300, IEEE, Pisa, Italy, September-October 1998.

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

[6] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[7] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 54, no. 6, pp. 2453–2469, 2008.

[8] E. G. Larsson and E. A. Jorswieck, "Competition versus cooperation on the MISO interference channel," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 7, pp. 1059–1069, 2008.

[9] R. Liu and H. V. Poor, "Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 55, no. 3, pp. 1235–1249, 2009.

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

[11] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

[12] J. Myung, H. Heo, and J. Park, "Joint beamforming and jamming for physical layer security," *ETRI Journal*, vol. 37, no. 5, pp. 898–905, 2015.

[13] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[14] 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, 2004.

[15] 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, 2005.

[16] 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, 2005.

[17] R. J. Muirhead, *Aspects of Multivariate Statistical Theory*, John Wiley & Sons, New York, NY, USA, 1982.

[18] M. K. Simon and M. Alouini, *Digital Communication Over Fading Channels*, John Wiley & Sons, Inc., New York, USA, 2000.

[19] B. He and X. Zhou, "Secure On-Off transmission design with channel estimation errors," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1923–1936, 2013.

[20] J. Myung and T. Kim, "Threshold Secret Sharing Transmission Against Passive Eavesdropping in MIMO Wireless Network," in *Proceedings of the 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 634–636, Prague, Czech Republic, July 2018.