IEICE TRANS. INF. & SYST., VOL.E99–D, NO.4 APRIL 2016

PAPER Special Section on Information and Communication System Security

A Security Enhancement Technique for Wireless Communications Using Secret Sharing and Physical Layer Secrecy Transmission

Shoichiro YAMASAKI[†a)], ***Senior Member and*** **Tomoko K. MATSUSHIMA**[†], ***Member***

SUMMARY Secret sharing is a method of information protection for security. The information is divided into n shares and reconstructed from any k shares, but no knowledge of the information is revealed from $k-1$ shares. Physical layer security is a method of achieving favorable reception conditions at the destination terminal in wireless communications. In this study, we propose a security enhancement technique for wireless packet communications. The technique uses secret sharing and physical layer security to exchange a secret encryption key. The encryption key for packet information is set as the secret information in secret sharing, and the secret information is divided into n shares. Each share is located in the packet header. The base station transmits the packets to the destination terminal by using physical layer security based on precoded multi-antenna transmission. With this transmission scheme, the destination terminal can receive more than k shares without error and perfectly recover the secret information. In addition, an eavesdropper terminal can receive less than $k-1$ shares without error and recover no secret information. In this paper, we propose a protection technique using secret sharing based on systematic Reed-Solomon codes. The technique establishes an advantageous condition for the destination terminal to recover the secret information. The evaluation results by numerical analysis and computer simulation show the validity of the proposed technique.

key words: *secret sharing, physical layer security, multi-antenna transmission, Reed-Solomon codes*

1. Introduction

To achieve secure wireless communications, physical layer security has received much attention [1]. In wireless data transmission from a base station to a terminal, a multi-antenna system yields more favorable channel conditions for the destination than for an eavesdropper, and so the security in wireless systems is enhanced [2]–[4].

Secret sharing of (k,n) threshold scheme is a method in which the information is divided into n pieces, called shares. The information is reconstructed from any k shares, but no knowledge of the information is revealed from $k-1$ shares [5], [6]. Various implementation methods exist and the non-systematic Reed-Solomon (RS) coding scheme is one of them [7].

In this study, a security enhancing method for wireless packet communication is proposed. This study was in part presented at [8], [9].

Secret sharing based on the (k,n) threshold scheme and physical layer security based on precoded multi-antenna transmission are used to exchange the secret encryption key. Secret sharing scheme based on RS codes is used, since the RS encoder and decoder, which are implemented for error correction encoding and decoding at the transmitter and the receiver in the packet communication system, can also be used to implement the processing for secret sharing. In the proposed method, the secret information is the key used to encrypt the payload data of the packets. The secret information is divided into n shares based on secret sharing using the (k,n) threshold scheme, and the n shares are located in the n packet headers. The secret information is exchanged periodically. Each packet is transmitted toward the terminal from the base station under protection by the physical layer security scheme based on precoded transmission. To recover the secret information, at least k shares must be known. The physical layer security scheme yields favorable channel conditions at the destination so that more than k shares are received without error at the destination and less than $k-1$ shares are received without error at the eavesdropper.

Furthermore, a method to yield a more favorable condition for recovering the secret information at the destination is proposed by using secret sharing with the (k,n) threshold scheme based on systematic RS codes, in which $k-1$ shares are arbitrarily decided and are independent of the secret information [10], [11]. Their $k-1$ shares are set to the destination terminal as the identification information to identify the destination terminal and they are fixed and not transmitted, since they are previously determined. The remaining $n-k+1$ shares are located at the $n-k+1$ packet headers and they are exchanged periodically. For the destination terminal to recover the secret information, at least 1 share among the $n-k+1$ transmitted shares must be received without error. On the other hand, for an eavesdropper terminal to recover the secret information, at least k shares among the $n-k+1$ transmitted shares must be received without error. The proposed method, which uses secret sharing of the (k,n) threshold scheme based on systematic RS codes as well as the physical layer security scheme based on precoding, favors the destination terminal over the eavesdropper terminal for recovery of the secret information.

This study considers the system performance in detail by adding the following considerations to our studies presented at [8], [9]. The computer simulation includes the evaluation on the condition that the channel matrix for the destination terminal and that for the eavesdropper terminal, which depend on a correlation coefficient, are correlated. And the effect of increasing the number of antennas

Manuscript received May 21, 2015.
Manuscript revised October 8, 2015.
Manuscript publicized January 13, 2016.

[†]The authors are with Polytechnic University of Japan, Kodaira-shi, 187–0035 Japan.
a) E-mail: syamasa@uitec.ac.jp

DOI: 10.1587/transinf.2015ICP0010

are considered by evaluating the system performance for a two-antenna model and for a three-antenna model.

Physical layer security using multi-antenna transmission based on precoding is described in Sect. 2, (k, n) threshold secret sharing is described in Sect. 3, and secret sharing based on systematic RS codes is described in Sect. 4. The proposed security method for wireless packet communication is described in Sect. 5, and evaluation results are given in Sect. 6.

2. Physical Layer Security

Wireless communications are vulnerable to eavesdropping from unauthorized terminals. Physical layer methods to secure the wireless systems support the security protocols in the upper layers in the network protocol stack [3], [4]. Figure 1 illustrates a wireless system which consists of the base station and the terminals. An information message is transmitted from the base station to the destination terminal. Physical layer security methods yield more favorable channel conditions for the destination than the eavesdropper.

Two-antenna transmission is a basic technique to implement physical layer security. The transmitted signal symbols for antennas 0 and 1 are defined as u_0 and u_1, the received signal symbols for antennas 0 and 1 are defined as v_0 and v_1, and additive white Gaussian noise (AWGN) symbols are given by w_0 and w_1, respectively. We also define $U = (u_0\ u_1)^T$, $V = (v_0\ v_1)^T$ and $W = (w_0\ w_1)^T$. The channel inputs and the outputs are related as

$$V = HU + W, \tag{1}$$

$$H = \begin{pmatrix} h_{00} & h_{10} \\ h_{01} & h_{11} \end{pmatrix}, \tag{2}$$

where H is the channel matrix for flat fading. This relation is illustrated in Fig. 2.

The matrix P diagonalizing $H^H H$ yields the matrix decomposition of

$$\Lambda = \begin{pmatrix} \lambda_0 & 0 \\ 0 & \lambda_1 \end{pmatrix} = P^H H^H H P. \tag{3}$$

We define the transmission signal vector $X = (x_0\ x_1)^T$ and the receive signal vector $Y = (y_0\ y_1)^T$. We also define

$$U = PX, \tag{4}$$

$$Y = P^H H^H V. \tag{5}$$

The procedure is illustrated in Fig. 3. Then the following relation is obtained.

$$\begin{aligned} Y &= P^H H^H V \\ &= P^H H^H (HU + W) \\ &= P^H H^H HPX + P^H H^H W \\ &= \Lambda X + P^H H^H W \end{aligned} \tag{6}$$

If the AWGN terms are neglected, the following equation represents the parallel data transmission.

$$Y = \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} = \begin{pmatrix} \lambda_0 & 0 \\ 0 & \lambda_1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \Lambda X \tag{7}$$

This scheme is called eigen-mode transmission. It is assumed that both the transmitter and the receiver know the channel matrix H, and H is perfectly estimated. The information of the channel matrix H is shared with the base station and the destination terminal, and matrix P is also shared with them. This technique is implemented for time division duplex (TDD) transmission between the base station and the terminal as an example. The up-link transmission and the down-link transmission of the TDD use the same channel and the base station and the terminal can estimate the channel matrix from each received signal.

This transmission technique is used to implement physical layer security. The transmitter of the base station transmits $U = PX$, and receiver of the destination terminal receives $V = HU$ if the AWGN terms are neglected. The calculation of

$$Y = P^H H^H V = P^H H^H HPX = \Lambda X \tag{8}$$

outputs the signals without interference.

The channel matrix between the base station and the

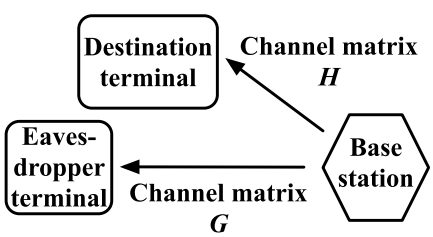

Fig. 1 Wireless system with destination and eavesdropper terminals.

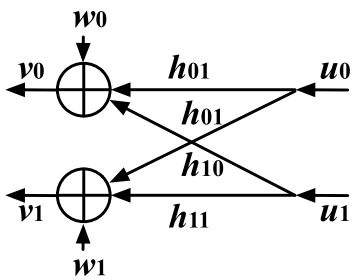

Fig. 2 Configuration of transmission with two transmitting antennas and two receiving antennas (two-antenna model).

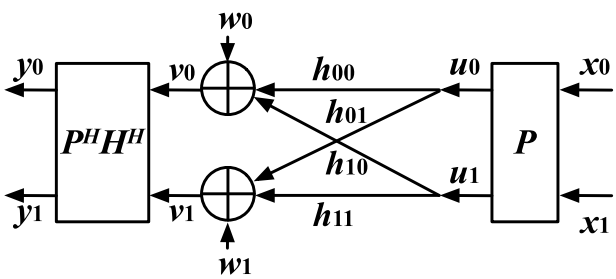

Fig. 3 Eigen-mode transmission using precoding for two-antenna model.

eavesdropper terminal is defined as G. Unless $G = H$, the eavesdropper terminal receives the signals from the base station with interference. The quality of these received signals is severely degraded, and eavesdropping is suppressed.

This scheme is expanded to three-antenna transmission which includes three transmit antennas and three receive antennas. The channel matrix is given by

$$H = \begin{pmatrix} h_{00} & h_{10} & h_{20} \\ h_{01} & h_{11} & h_{21} \\ h_{02} & h_{12} & h_{22} \end{pmatrix}. \tag{9}$$

3. Secret Sharing

Secret sharing using the (k, n) threshold scheme is a method in which secret information s is divided into n shares and is reconstructed from any k shares, but no knowledge of the secret information can be obtained from $k-1$ shares [5].

In the case of a $(3, 5)$ threshold scheme, s is divided into five shares $(a_0, a_1, a_2, a_3, a_4)$, and the shares are assigned to User 0, User 1, User 2, User 3 and User 4, respectively. The shares are set so that s can be reconstructed from any three shares of three users. The reconstruction is implemented by polynomial interpolation [6].

The (k, n) threshold scheme is also implemented by RS codes [7]. Nonzero elements of a finite field $GF(r)$ with r elements are defined as $(\alpha_0, \alpha_1, \cdots, \alpha_{r-2})$. In k words of $A = (a_0, a_1, \cdots, a_{k-1})$, $a_i \in GF(r)$, let a_0 be secret information and $a_1, a_2, \cdots, a_{k-1}$ be random information. The k words are encoded into a codeword $C = (c_0, c_1, \cdots, c_{r-2})$ by calculating

$$c_i = \sum_{j=0}^{k-1} a_j \alpha_i^j. \tag{10}$$

If $n = r - 1$, then c_i for $i = 0, 1, \cdots, n-1$ are the n shares. This calculation scheme is non-systematic (n, k) RS encoding, The $n-k$ erasure words are reconstructed by erasure decoding. If at least k shares exist, the n shares are reconstructed. The calculation of

$$s = a_0 = -\sum_{i=0}^{r-2} c_i \tag{11}$$

yields the secret information s.

As an example, the construction of shares for the $(3, 5)$ threshold scheme using non-systematic $(5, 3)$ RS encoding is illustrated in Fig. 4. Since the shares are constructed by non-systematic RS encoding, all the shares depend on the secret information s.

4. Secret Sharing Method Using Systematic RS Codes

One of the authors has proposed the (k, n) threshold scheme implemented by the systematic RS codes [10], [11].

Let k words be $(a_0, a_1, \cdots, a_{k-1})$, $a_i \in GF(r)$ for $i = 0, 1, \cdots, k-1$. Among them, $(a_0, a_1, \cdots, a_{k-2})$ are randomly set in $GF(r)$, and the secret information is $s \in GF(r)$. Then

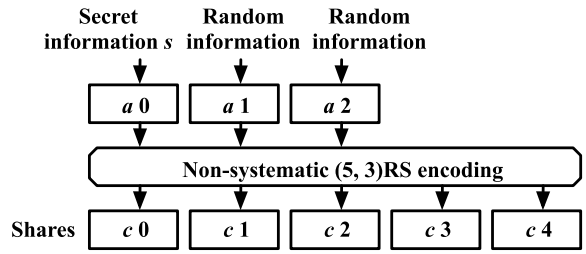

Fig. 4 (3, 5) threshold scheme using non-systematic (5, 3) RS codes.

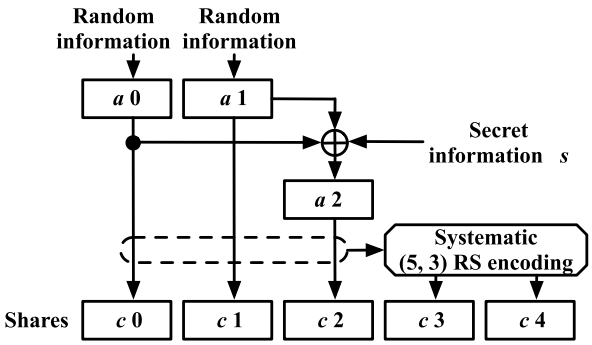

Fig. 5 (3, 5) threshold scheme using systematic (5, 3) RS codes.

a_{k-1} is calculated by

$$a_{k-1} = s + \sum_{i=0}^{k-2} a_i. \tag{12}$$

By using the k words of $(a_0, a_1, \cdots, a_{k-1})$ as the information words for the systematic (n, k) RS codes, the $n-k$ check words are calculated. Combining the k information words and the $n-k$ check words forms codeword $C = (c_0, c_1, \cdots, c_{n-1})$ of (n, k) RS codes, where $a_i = c_i$ for $i = 0, 1, \cdots k-1$. These words are the generated n shares.

If at least k shares are given, the n shares are reconstructed by (n, k) RS decoding, and s is calculated by

$$s = \sum_{i=0}^{k-1} a_i. \tag{13}$$

Since the shares are constructed by systematic RS encoding, the arbitrarily decided $k-1$ words of $(a_0, a_1, \cdots, a_{k-2})$ are equal to the $k-1$ shares. And the remaining $n-k+1$ shares depend on the secret information s.

As an example, the construction of the shares for the $(3, 5)$ threshold scheme using systematic $(5, 3)$ RS encoding is illustrated in Fig. 5. In the case of $(5, 3)$ RS codes over $GF(2^3)$ for $n = 5$ and $k = 3$, the polynomial

$$G(x) = (x - \alpha)(x - \alpha^2) \tag{14}$$

is used, where α is the root of $x^3 + x + 1 = 0$.

The secret information s is an element of $GF(2^3)$, and the two words of (a_0, a_1) is randomly determined in $GF(2^3)$. Then a_2 is calculated by

$$a_2 = s + a_0 + a_1. \tag{15}$$

By using the three words of (a_0, a_1, a_2) as the information words of systematic (5, 3) RS encoding, the two check words are calculated. Combining the three information words and the two check words forms the codeword $C = (c_0, c_1, \cdots, c_6)$, where each c_i corresponds to the share of (5, 3) threshold scheme for $i = 0, 1, \cdots, 6$.

Since the shares are constructed by systematic RS encoding, the arbitrarily decided $k-1$ words of $(a_0, a_1, \cdots, a_{k-2})$ are equal to the $k-1$ shares. And the remaining $n-k+1$ shares depend on the secret information s. Secret sharing based on systematic RS codes has a favorable property to implement the proposed method 2 for the packet communication shown in the next section.

5. Proposed Communication System

To enhance the security of the wireless packet communication system, methods combining the precoded multi-antenna transmission technique and the secret sharing (k, n) threshold technique are proposed. These techniques exchange the secret key for encryption. The information stored in the payload of the packet is encrypted, and its encryption key is the secret information s to be shared. Method 1 uses non-systematic RS codes and method 2 uses systematic RS codes.

5.1 Method 1

The secret information s is divided into n shares of $c_0, c_1. \cdots, c_{n-1}$ by the (k, n) threshold scheme using non-systematic RS encoding. Each share is stored in the header of the packet, and s is exchanged every n packets. Figure 6 illustrates an example using the (3, 5) threshold scheme. The first secret information s_0 is divided into five shares, which are Share 0, Share 1, $\cdots$, Share 4. In Fig. 6, Hd is the header of the packet, and each share is stored in each header. The second secret information s_1 is divided into five shares, which are Share 5, Share 6, $\cdots$, Share 9, and each share is stored in each header.

The packets are transmitted from the base station to the destination terminal based on the precoded multi-antenna technique. The transmission technique is required to yield channel conditions so that the secret information is completely recovered by the destination terminal and is not recovered by the eavesdropper at all. The required channel conditions are as follows:

Condition 1 The destination terminal has favorable channel conditions such that more than k shares among the n shares are received without error.

Condition 2 The eavesdropper terminal has poor channel conditions such that less than $k-1$ shares among the n shares are received without error.

Figure 7 illustrates an example of using the (3, 5) threshold scheme based on non-systematic (5, 3) RS codes for $k = 3$ and $n = 5$.

For the destination terminal to recover the secret information, at least 3 $(= k)$ shares among the 5 $(= n)$ shares are required to be received without error. For the eavesdropper terminal to recover the secret information, the same requirement applies. So, the destination and the eavesdropper have the same recovery performance for $H = G$.

5.2 Method 2

The secret information s is divided into n shares of $c_0, c_1. \cdots, c_{n-1}$ by the (k, n) threshold scheme using systematic RS encoding [10], [11].

This scheme has the advantage that $k-1$ shares $c_0, c_1. \cdots, c_{k-2}$ are arbitrarily determined to be independent of secret information s. Among these $k-1$ shares, m shares $(m \leq k-1)$ of $c_0, c_1. \cdots, c_{m-1}$ are used as fixed identification information and have been previously shared with the base station and the destination terminal so that the destination is identified as the authorized terminal. Therefore the base station transmits $n-m$ shares of $c_{m-2}, c_k, \cdots, c_{n-1}$ and each share is stored in the header of each packet, and s is exchanged every $n-m$ packets. The packets are transmitted from the base station to the destination terminal based on the precoded multi-antenna technique. The transmission technique is required to yield channel conditions so that the secret information is completely recovered by the destination terminal and is not recovered by the eavesdropper at all. The required channel conditions are as follows:

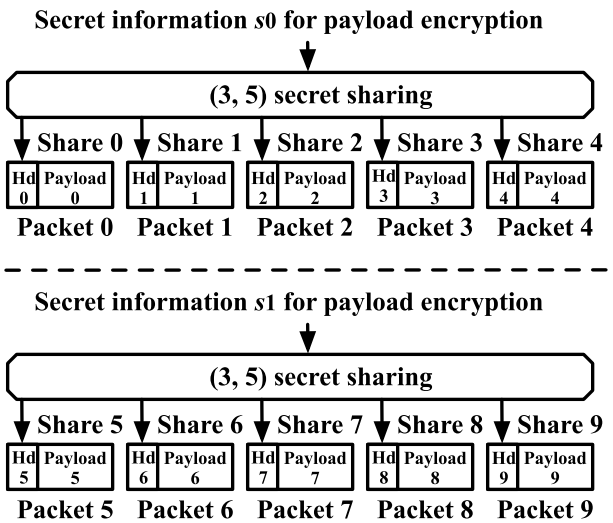

Fig. 6 Packet construction in the proposed method.

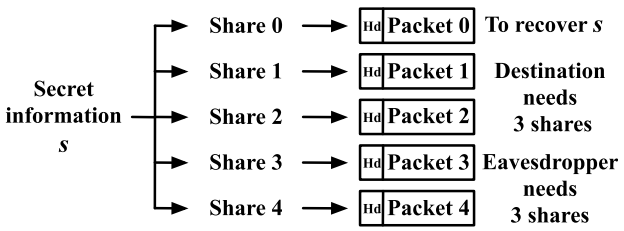

Fig. 7 Method 1 using non-systematic (5, 3) RS codes.

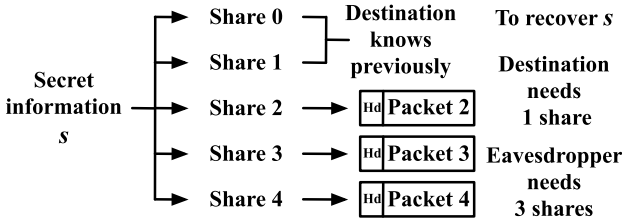

Fig. 8 Method 2 using systematic (5, 3) RS codes.

Condition 1 The destination terminal has favorable channel conditions such that more than $k - m$ shares among the $n - m$ shares are received without error.

Condition 2 The eavesdropper terminal has poor channel conditions such that less than $k - 1$ shares among the $n - m$ shares are received without error.

Figure 8 illustrates an example of using the $(3, 5)$ threshold scheme based on systematic $(5, 3)$ RS codes for $k = 3, n = 5$ and $m = 2$.

For the destination terminal to recover the secret information, at least 1 $(= k - m)$ share among the 3 $(= n - m)$ shares must be received without error, since the 2 $(= m)$ shares are previously known.

On the other hand, for the eavesdropper terminal to recover the secret information, 3 $(= k)$ shares among the 3 $(= n - m)$ shares must be received without error.

For $H \neq G$ and $H = G$, method 2 yields more favorable channel conditions for the destination than for the eavesdropper. Then the requirements of precoded multi-antenna transmission can be reduced.

6. Evaluations

6.1 Numerical Analysis

The proposed system consists of a combination of secret sharing and physical layer security. However, in this numerical analysis, only secret sharing is considered. The results show the security performance required for physical layer secrecy.

Let e be the random bit error rate (BER) of the received share and l be number of bits containing in one share. Then the share error rate ε, by which the share is erroneously received, is given by $\varepsilon = 1 - (1 - e)^l$.

Method 1

In the case of the (k, n) threshold scheme based on non-systematic RS codes, each P_{d1}, which is the secret information recovery rate for the destination and P_{e1}, which is the secret information recovery rate for the eavesdropper, are given by

$$P_{d1} = P_{e1} = \sum_{i=k}^{n} {}_nC_i(1 - \varepsilon)^i \varepsilon^{n-i}. \tag{16}$$

This equation shows the rate at which more than k shares among the n shares are received without error.

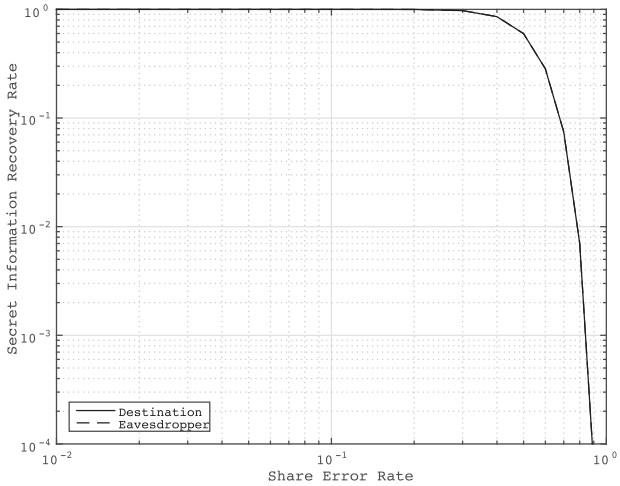

Fig. 9 Relation between the share error rate and the secret information recovery rate for method 1 based on non-systematic RS codes ($k = 8$, $n = 16$).

Method 2

In the case of the (k, n) threshold scheme based on systematic RS codes, $k - m$ shares contain the identification information for the destination terminal and are shared with the base station and the destination terminal, and $n - m$ shares are transmitted.

P_{d2}, which is the recovery rate of s for the destination, is given by

$$P_{d2} = \sum_{i=k-m}^{n-m} {}_{n-m}C_i(1 - \varepsilon)^i \varepsilon^{n-m-i} \tag{17}$$

This equation shows the rate at which more than $k-m$ shares among the $n - m$ shares are received without error.

P_{e2}, which is the recovery rate of s for the eavesdropper, is given by

$$P_{e2} = \sum_{i=k}^{n-m} {}_{n-m}C_i(1 - \varepsilon)^i \varepsilon^{n-m-i} \tag{18}$$

This equation shows the rate at which more than k shares among the $n - m$ shares are received without error.

The numerical analysis results are shown for $k = 8$ and $n = 16$ under the assumption that the $(8, 16)$ threshold scheme is based on shortened $(16, 8)$ RS codes over $GF(2^8)$.

Figure 9 illustrates the relation between the share error rate and the secret information recovery rate in the case of method 1 based on non-systematic RS codes. The destination and the eavesdropper have the same characteristics. Therefore, physical layer security is essential to suppress the eavesdropping.

Figure 10 illustrates the relation between the share error rate and the secret information recovery rate in the case of method 2 based on systematic RS codes for $m = 4$. Figure 11 illustrates the relation in the case of method 2 based on systematic RS codes for $m = 7$.

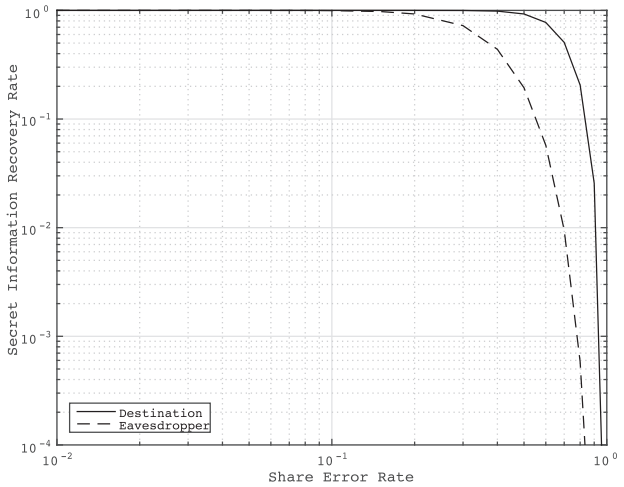

Fig. 10 Relation between the share error rate of the received share and the secret information recovery rate for method 2 based on systematic RS codes ($k = 8$, $n = 16$, $m = 4$).

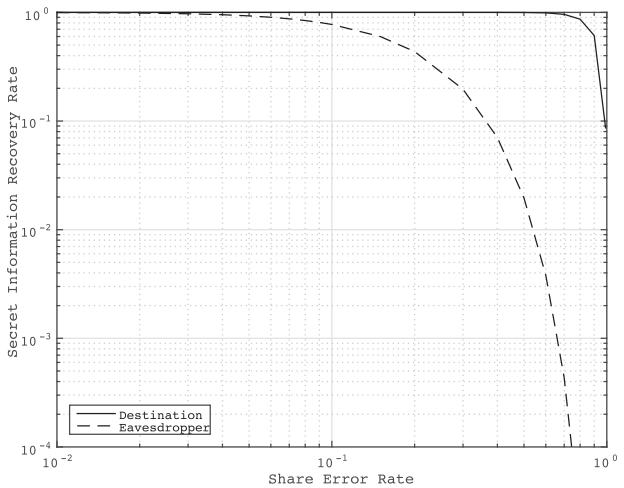

Fig. 11 Relation between the share error rate of the received share and the secret information recovery rate for method 2 based on systematic RS codes ($k = 8$, $n = 16$, $m = 7$).

The destination must receive at least 4 ($= k - m$) shares without error to recover the secret information among the received 12 ($= n - m$) shares for $m = 4$, and must also receive at least 1 ($= k - m$) shares without error to recover the secret information among the received 9 ($= n - m$) shares for $m = 7$. On the other hand, the eavesdropper must receive at least 8 ($= k$) shares without error among the received 12 shares for $m = 4$ and among the received 9 shares for $m = 7$.

Method 2 yields better conditions at the destination terminal than at the eavesdropper terminal, Therefore, the requirements of physical layer security can be reduced for the destination terminal.

6.2 Simulation

In the simulation, $(8, 16)$ threshold scheme $(k = 8, n = 16)$ based on the shortened $(16, 8)$ RS codes over $GF(2^8)$ is assumed. The transmitted bits are mapped to the transmit symbols of 16-QAM (Quadrature Amplitude Modulation).

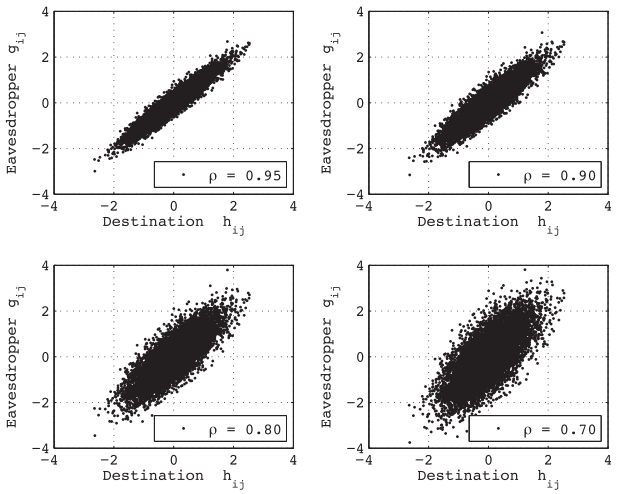

Fig. 12 Relation between the channel coefficient for the destination and the eavesdropper.

The two-antenna model and the three-antenna model are evaluated under the AWGN environments. For the L-antenna model ($L = 2$ and 3), the signals transmitted from the L transmitting antennas of the base station are received by the L receiving antennas of the destination terminal based on the precoded L-antenna system. The signals are assumed to be received by the L receiving antennas of the eavesdropper terminal. Average power of the signal that is output on the channel is 1, by setting the average output power of each transmitting antenna to $1/L$.

The channel coefficients between the base station and the destination terminal are defined as h_{ij} $(i, j = 0, \cdots, L-1)$. Each coefficient is ideally estimated and shared between the base station and the destination terminal. By assuming a block fading model, each coefficient is constant during one packet transmission. Its real and imaginary parts are given by zero mean Gaussian random variables with a variance of 0.5 [12], [13].

The channel coefficients between the base station and the eavesdropper terminal are defined as g_{ij} $(i, j = 0, \cdots, L-1)$. In the case of g_{ij} and h_{ij} $(i, j = 0, \cdots, L-1)$ having no correlation, the eavesdropper terminal recovered no secret information in the simulation.

Then we show the simulation results in the case of g_{ij} and h_{ij} $(i, j = 0, \cdots, L-1)$ having a correlation. The difference between g_{ij} and h_{ij} $(i, j = 0, \cdots, L-1)$ depends on their correlation, which is given by the Gaussian complex random variables in the simulations.

The correlation coefficient between variables $(x_1, x_2, \cdots, x_n)$ and $(y_1, y_2, \cdots, y_n)$ is given by

$$\rho = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{(\sum_{i=1}^{n}(x_i - \bar{x})^2)(\sum_{i=1}^{n}(y_i - \bar{y})^2)}}, \tag{19}$$

where $\bar{x}$ and $\bar{y}$ are the mean values of the variables. In general, the system has a strong correlation for $\rho > 0.7$. Figure 12 illustrates the relation between h_{ij} and g_{ij}.

The simulation results for the two-antenna model are illustrated in Figs. 13, 14 and 15. Figure 13 illustrates the relation between the secret information recovery rate and the signal to noise ratio (SNR) for method 1 ($k = 8$ and $n = 16$). For smaller ρ, the recovery rate for the eavesdropper terminal is inferior to that for the destination terminal. Figure 14 illustrates the secret information recovery rate for method 2 ($k = 8$, $n = 16$ and $m = 4$). The eavesdropper terminal recovers no secret information for $\rho = 0.8$. Figure 15 illustrates the secret information recovery rate for method 2 ($k = 8$, $n = 16$ and $m = 7$). The eavesdropper terminal also recovers no secret information for $\rho = 0.85$.

The simulation results for the three-antenna model are illustrated in Figs. 16, 17 and 18. Figure 16 illustrates the secret information recovery rate for method 1 ($k = 8$ and $n = 16$). Figure 17 illustrates the secret information recovery rate for method 2 ($k = 8$, $n = 16$ and $m = 4$), and Fig. 18 illustrates that for method 2 ($k = 8$, $n = 16$ and $m = 7$). Comparing the characteristics of the three-antenna model with those of the two-antenna model, the eavesdropper terminal for the three-antenna model has the poor secret information recovery rate, since the coefficient g_{ij}, which deviates from h_{ij}, tends to occur as the number of antennas increases.

By selecting smaller k or larger n, the destination terminal and the eavesdropper terminal tend to recover the secret information owing to the property of secret sharing. To avoid eavesdropping, the physical layer security performance is required to be improved by increasing the number of antennas (L) at the expense of implementation complexity. For method 2, the requirement of the physical layer security for the destination terminal is reduced by selecting larger m.

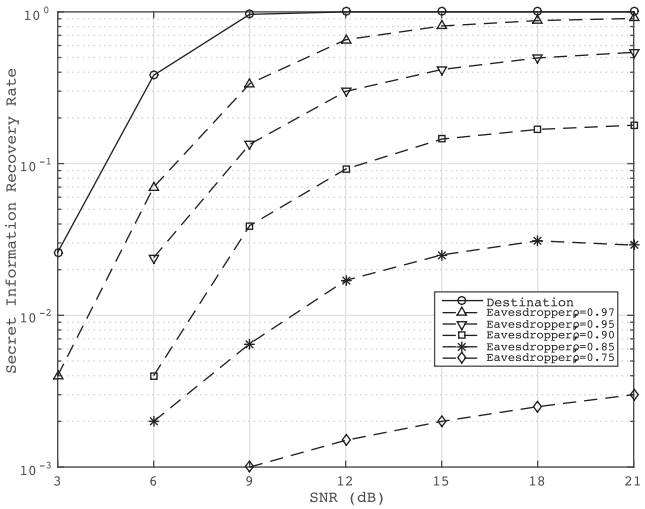

Fig. 13 Relation between the SNR and the secret information recovery rate for method 1 ($k = 8$, $n = 16$, two-antenna model).

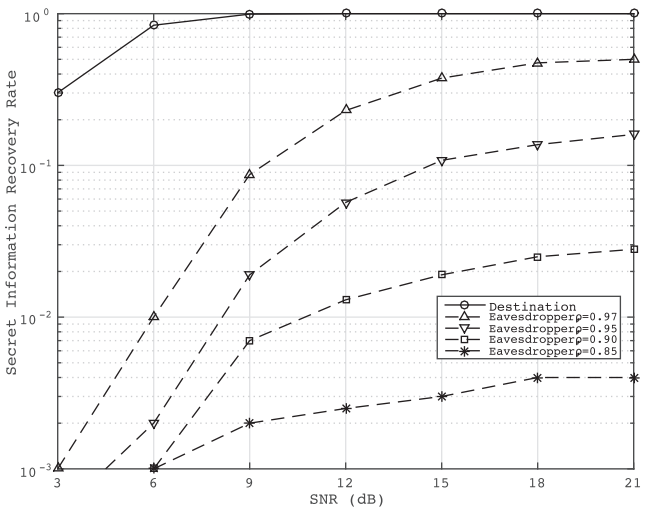

Fig. 14 Relation between the SNR and the secret information recovery rate for method 2 ($k = 8$, $n = 16$, $m = 4$, two-antenna model).

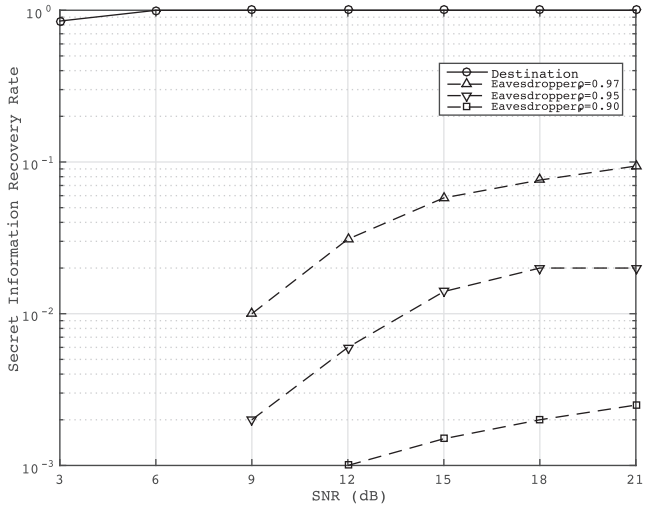

Fig. 15 Relation between the SNR and the secret information recovery rate for method 2 ($k = 8$, $n = 16$, $m = 7$, two-antenna model).

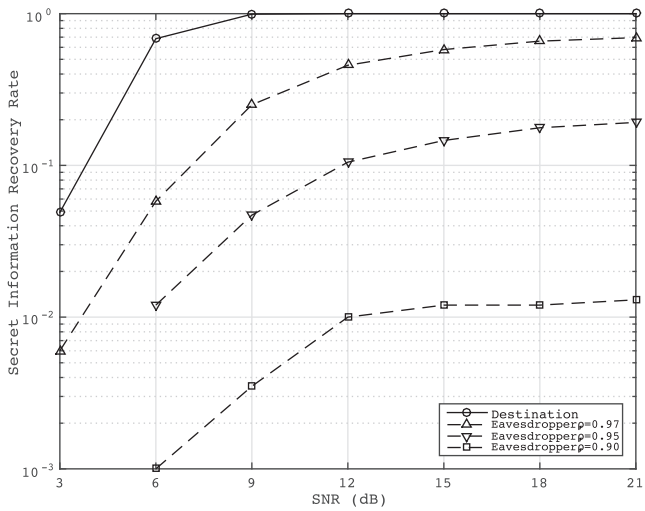

Fig. 16 Relation between the SNR and the secret information recovery rate for method 1 ($k = 8$, $n = 16$, three-antenna model).

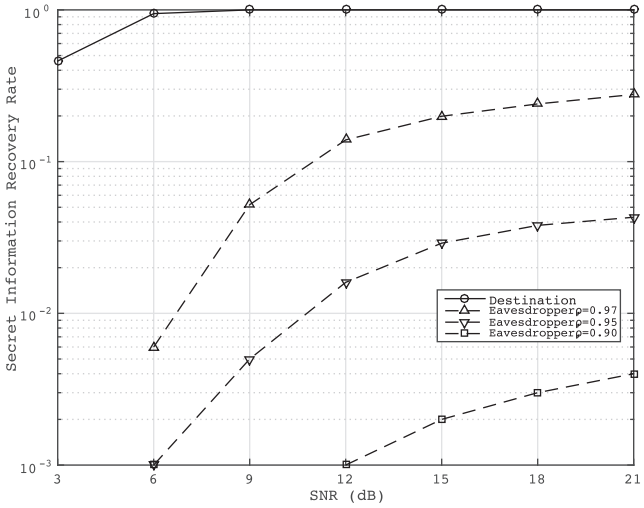

Fig. 17 Relation between the SNR and the secret information recovery rate for method 2 ($k = 8$, $n = 16$, $m = 4$, three-antenna model).

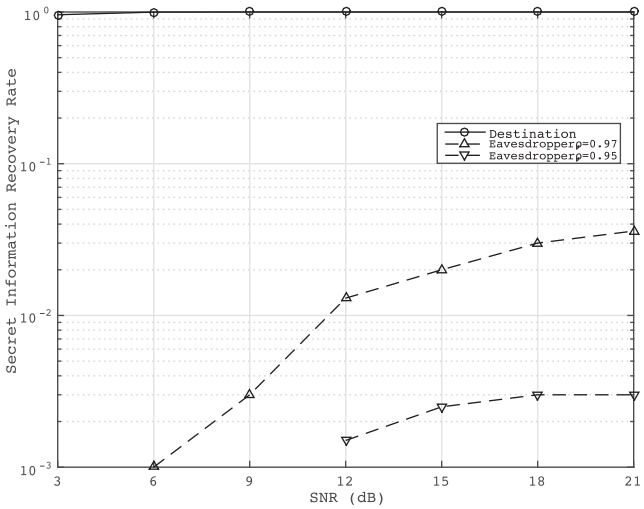

Fig. 18 Relation between the SNR and the secret information recovery rate for method 2 ($k = 8$, $n = 16$, $m = 7$, three-antenna model).

7. Conclusion

We proposed a security enhancing method for wireless communications. The method uses secret sharing and physical layer security to exchange the secret encryption key. The physical layer security method yields more favorable secret information recovery conditions for the destination terminal than for the eavesdropper terminal. Method 1 is implemented using a (k, n) threshold secret sharing scheme, such as a scheme with non-systematic RS codes. Method 2 is implemented using a (k, n) threshold scheme with systematic RS codes, and it attains a higher information recovery rate that reduces the requirements of physical layer security.

Acknowledgments

This work was supported by JSPS KAKENHI Grant Numbers 25420396 and 25420397.

References

[1] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M.D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," IEEE Commun, Mag., vol.53, no.4, pp.20–27, April 2015.
[2] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M.R. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer," IEEE Signal Process. Mag., vol.30, no.5, pp.16–28, Sept. 2013.
[3] Y.-W.P. Hong, P.-C. Lan, and C.-C.J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems," IEEE Signal Process. Mag., vol.30, no.5, pp.29–40, Sept. 2013.
[4] Y.-W.P. Hong, P.-C. Lan, and C.-C.J. Kuo, Signal processing approaches to secure physical layer communications in multi-antenna wireless systems, Springer briefs in electrical and computer eng., 2014.
[5] A. Shamir, "How to share a secret," Commun. ACM, vol.22, no.11, pp.612–613, 1979.
[6] K. Kurosawa and W. Ogata, Introduction to modern cryptography, Corona Publishing, 2004.
[7] R.J. McEliece and D.V. Sarwate, "On sharing secrets and Reed-Solomon codes," Commun. ACM, vol.24, no.9, pp.583–584, 1981.
[8] S. Yamasaki, T.K. Matsushima, and K. Ohno, "A security enhancement scheme for wireless packet communications using secret sharing and precoding," IEICE Technical Report, SIS2013-51, Dec. 2013.
[9] S. Yamasaki, T.K. Matsushima, and K. Ohno, "On a secret sharing scheme with systematic Reed-Solomon codes and its applications," IEICE Technical Report, IT2013-88, March 2014.
[10] C. Kawashima, T. Yoshida, and T.K. Matsushima, "Study on hierarchical secret sharing schemes using product and concatenated codes," IEICE Technical Report, ISEC2007-76, Sept. 2007.
[11] C. Kawashima, T. Yoshida, and T.K. Matsushima. "A study on hierarchical secret sharing schemes using product codes," 2008 Symposium on Cryptography and Information Security (SCIC2008), pp.22–25, Jan. 2008
[12] V. Tarokh, N. Seshadri, and A. Calderbank, "Space time codes for high data rate wireless communication: Performance criterion and code construction," IEEE Trans. Inf. Theory, vol.44, no.2, pp.744–765, March 1998.
[13] B. Vucetic and J. Yuan, Space-Time Coding, John Wiley & Sons Ltd., 2003.

Shoichiro Yamasaki received B.E., M.E., and Dr.Eng. Degrees in Electrical Engineering from Keio University, Yokohama, Japan, in 1980, 1982, and 1985, respectively. He was with Toshiba Corporation from 1985 to 2004. He has been a professor in the Polytechnic University, Japan, since 2004. His research interests include coding, signal processing, and security in wireless and multimedia communications. Dr. Yamasaki is a member of the Japan Society for Industrial and Applied Mathematics, the Institute of Image Information and Television Engineers and IEEE.

Tomoko K. Matsushima received B.E., M.E. and Dr.E. degrees from Waseda University, Tokyo, Japan, in 1985, 1987 and 1999, respectively. From 1987 to 1994, she was with the Toshiba Corporate Research & Development Center, Kanagawa, Japan. From 1994 to 2005 she was a lecturer, from 2005 to 2013 she was an associate professor, and from 2014 she has been a professor in the Polytechnic University, Japan. From 2001 to 2002, she was a Visiting Researcher at the University of Hawaii, U.S.A. Her research interests are coding theory and its applications. She received the 1991 Shinohara Memorial Young Engineer Award, and the 2008 Best Paper Award from IEICE. Dr. Matsushima is a member of the Information Processing Society of Japan and IEEE.