Performance Evaluation of the Physical Layer Security Using Artificial Noise and Relay Station

Junichi Kabeya
and Osamu Takyu
Shinshu University
4-17-1 Wakasato
Nagano 380-8553
Email: 14tm209b@shinshu-u.ac.jp

Tomoaki Ohtsuki
Keio University
3-14-1 Hiyoshi
Kohoku
Yokohama
Kanagawa 223-8522

Fumihito Sasamori
and Shiro Handa
Shinshu University
4-17-1 Wakasato
Nagano 380-8553

***Abstract*—In the physical layer security (PLS), the beam forming with multiple antennas enhances the received signal power at the legitimate user but suppresses it at the other users. The other users hardly demodulate the information without the bit error. However, if the channel state between the legitimate user and the other one is highly correlated, it is possible for the other users to demodulate the information signal. This paper proposes the novel secure communication system with utilizing the artificial noise and the relay station. When the legitimate user emits the artificial noise, the relay station receives the information bearing signal and the artificial noise. The other users cannot demodulate the information due to the interference of artificial noise. After the relay forwards the combined signal between the information bearing signal and the artificial noise to the legitimate user, the artificial noise is removed from the forwarded signal by the legitimate user. As a result, the legitimate user can demodulate the information. Therefore, the secure wireless communication can be constructed. This paper evaluates the secure capacity for the various location of eavesdropper and clarifies the validity of proposed system.**

I. Introduction

Recently, the collaborations between various applications and wireless communication are attracting much attention, such as M2M(Machine to Machine Network) and D2D(Device to Device Network)[1]. In M2M and D2D, a lot of wireless systems construct communication link. Therefore, the exhausting of frequency spectrum is serious problem. In addition, the information with which M2M and D2D deal gives the huge impact to the life style, such as vital signs and control command to the machines. Therefore, the high efficiency of frequency spectrum usage and the high security of wireless communication are required for M2M and D2D.

The higher layer securities, such as cipher and authentication, are powerful security[2]. In addition, the physical layer security (PLS) is also powerful because of the enhancement of the higher layer securities. In the PLS, the information cannot be detected in the unspecified user except for the legitimate one[3][4].

One of PLS's techniques is the null stealing with the multiple antennas. The beam gain for the legitimate user is enhanced but that for the eavesdropper is suppressed. As a result, since the received signal power of legitimate user is much larger than that of eavesdropper, the eavesdropper cannot demodulate the received signal[5]. However, when the fading correlation between the legitimate user and the eavesdropper is high, the suitable beam pattern cannot be constructed. Therefore, there is a fear of information leak [6].

In Ref. [4], the information source and the destination transmits the information bearing signal and the artificial noise to the relay station, respectively. As a result, the relay station cannot demodulate the signal due to the disturbing from the artificial noise. The relay station relays the mixed signals between the information bearing signal and the artificial noise to the destination and then the destination successfully demodulates the relayed signal because the artificial noise can be removed from the relayed signal. Therefore, the secure communication link for the relay station can be constructed. The artificial noise and the relay station are powerful even under the high correlated fading environment. Therefore, these are expected for the secure communication but the effect of them has not been clarified, yet.

This paper proposes the novel PLS technique with using the relay station and the artificial noise. We analyze the secure capacity in the downlink (access from fusion center to sensor) and the uplink (access from sensor to fusion center). From the computer simulation, we clarify that the large secure capacity is achieved by the scheme of artificial noise and relay station.

A. System Model

Figure 1 shows the system model. There are one fusion center, S, one sensor, R, and one eavesdropper, E. S is equipped with the multiple antenna. If the channel transfer state information (CSI) between S and E is known, S can construct the beam pattern for nulling to E. If it is not, S uses the maximal ratio transmission (MRT) in down link and the maximal ratio combining (MRC) for enlarging the desired signal power from D. As a result, the E has the difficulty of data demodulation because it needs the more signal power to demodulation.

1) Proposed System Model: In proposed system, the relay station is between S and D. The accesses from S to D and D to S are downlink and uplink, respectively. The proposed wireless communication takes two time steps. In the first step of downlink, S transmits the information bearing signal, X_0 as well as D transmits the artificial noise, X_1. Therefore, R and E receive the mixed signal, Y_{01}, between X_0 and X_1. Y_{01} is

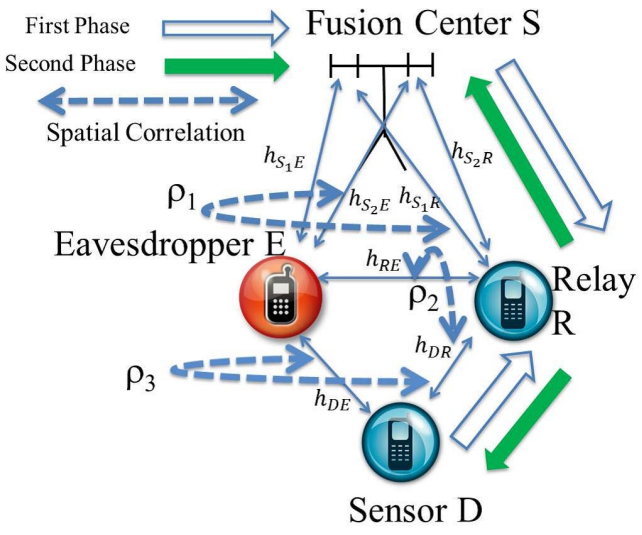

Fig. 1. System Model

derived as follows.

$$Y_{01} = X_0 + X_1 \tag{1}$$

In the second step of downlink, R relays the received signal to D by the amplifying and the forwarding (AF). As a result, D can detect the information by removing the artificial noise from the received mixed signal. In the first step of uplink, the D transmits the information bearing signal, X_0 to R as well as the S transmits the artificial noise, X_1. The R receives the mixed signal Y_{01}. In second step, the R relays the mixed signal by AF to the D. Since D knows X_1, it can detects information X_0 by removing X_1 from Y_{01}.

2) Space Correlation of Fading: This paper assumes the space correlation of fading as Fig. 1 shows. The fading correlations between the S-R channel and the S-E one the R-D channel and the R-E one, and the R-D channel and the D-E one are ρ_1, ρ_2, and ρ_3, respectively. Each fading correlation is derived by the following equation [7].

$$\rho(\Delta x) = exp(-4(\frac{\pi \Delta x \sigma_\phi \sin\phi_0}{\lambda})^2) \tag{2}$$

In this paper, the arrival angle is modeled as the Gaussian distribution with the average $\phi_0 = 90^\circ$ and the standard deviation $\sigma_\phi = 1$, where Δx is the distance between two received points.

B. Analysis of Secure Capacity

From the Shannon's information theory, the channel capacity from S to D though R, C_{SRD}, is derived as

$$C_{SRD} = \frac{1}{2}\log_2(1 + SNR_{SRD}), \tag{3}$$

where SNR_{SRD} is the end-to-end SNR from S to D. The channel capacity from S to E, C_{SE}, is also derived as

$$C_{SE} = \frac{1}{2}\log_2(1 + SINR_{SE}) \tag{4}$$

where $SINR_{SE}$ is the received signal to artificial interference plus noise power ratio in E. From the above, the secure capacity from S to D through R, C_S is derived as follow [4].

$$C_S = \left[\frac{1}{2}C_{SRD} - \frac{1}{2}C_{SE}\right]^+ \quad , \quad [x]^+ = \begin{cases} x & x \geq 0 \\ 0 & \text{otherwise} \end{cases} \tag{5}$$

C. Analysis of Secure Capacity in Down Link

1) Received $SINR$ in Relay: In proposed system, when S uses the MRT with two antenna, the received signal in relay, y_R, is derived as follows.

$$\begin{aligned} y_R &= \frac{h_{S_1R}}{L_{SR}} w_{S_1} \frac{1}{\sqrt{2}} x_0 \sqrt{P_0} + \frac{h_{S_2R}}{L_{SR}} w_{S_2} \frac{1}{\sqrt{2}} x_0 \sqrt{P_0} \\ &+ \frac{h_{DR}}{L_{DR}} w_D x_1 \sqrt{P_1} + n_R \end{aligned} \tag{6}$$

where h_{SR}, and h_{DR} are the channel state information between S and R and D and R, respectively. L_{SR} and L_{DR} are the propagation loss between them, respectively. P_0 is the power of the information bearing signal and P_1 is that of the artificial noise. n_R is the noise component in relay. $E[|x_0|^2] = E[|x_1|^2] = 1$ In addition, w_{S_1} and w_{S_2} are the coefficients of 1st and 2nd antenna in base station, respectively, and these are derived as follows. However,$\overline{X}$ is X of complex conjugate.

$$w_{S_1} = \overline{h_{S_1R}} \tag{7}$$

$$w_{S_2} = \overline{h_{S_2R}} \tag{8}$$

From eq. (7) and eq. (8), the eq. (6 is reformed as

$$\begin{aligned} y_R &= \frac{|h_{S_1R}|^2}{L_{SR}} \frac{1}{\sqrt{2}} x_0 \sqrt{P_0} + \frac{|h_{S_2R}|^2}{L_{SR}} \frac{1}{\sqrt{2}} x_0 \sqrt{P_0} \\ &+ \frac{h_{DR}}{L_{DR}} w_D x_1 \sqrt{P_1} + n_R \end{aligned} \tag{9}$$

From eq. (9), the power of received signal in R is

$$\begin{aligned} E\left[y_R \overline{y_R}\right] &= \frac{|h_{S_1R}|^4}{(L_{SR})^2} \frac{1}{2} P_0 E\left[|x_0|^2\right] \\ &+ \frac{|h_{S_2R}|^4}{(L_{SR})^2} \frac{1}{2} P_0 E\left[|x_0|^2\right] \\ &+ 2\frac{|h_{S_1R}|^2 |h_{S_2R}|^2}{(L_{SR})^2} \frac{1}{2} P_0 E\left[|x_0|^2\right] \\ &+ \frac{|h_{DR}|^2}{(L_{DR})^2} |w_D|^2 P_1 E\left[|x_1|^2\right] + E\left[|n_D|^2\right] \end{aligned} \tag{10}$$

From eq. (10), in first step, the signal to interference plus noise power in relay, $SINR_{SR}$, is

$$\begin{aligned} SINR_{SR} &= \frac{\frac{1}{2(L_{SR})^2}(|h_{S_1R}|^2 + |h_{S_2R}|^2)^2 P_0 E\left[|x_0|^2\right]}{\frac{|h_{DR}|^2}{(L_{DR})^2} w_1 P_D E\left[|x_1|^2\right] + E\left[|n_R|^2\right]} \\ &= \frac{\frac{1}{2(L_{SR})^2}(|h_{S_1R}|^2 + |h_{S_2R}|^2)^2 P_0}{\frac{|h_{DR}|^2}{(L_{DR})^2} w_D P_1 + \sigma_R^2} \end{aligned} \tag{11}$$

where σ_R^2 is the variance of noise in R.

2) Received SNR in D: In second step, R relays the mixed signal between the information bearing signal and the artificial noise to D The received signal in D, y_D, is

$$y_D = y_R \alpha \frac{h_{DR}}{L_{DR}} + n_D \tag{12}$$

where α is the factor of amplifying in relay station and it is derived as [8]

$$\alpha = \sqrt{\frac{P_R E\left[|x_R|^2\right]}{E\left[|y_R|^2\right]}} \tag{13}$$

Therefore, the received signal power in D is derived as

$$E\left[y_D \overline{y_D}\right] = \alpha^2 \frac{|h_{DR}|^2}{(L_{DR})^2} E\left[y_R \overline{y_R}\right] + E\left[|n_D|^2\right] \tag{14}$$

Since D knows the artificial noise, it can detect the signal by removing the artificial noise from the mixed signal. As a result, the received SNR in D, SNR_D, is

$$SNR_D = \frac{\frac{\alpha^2}{2(L_{SR})^2}\frac{|h_{DR}|^2}{(L_{DR})^2}\left(|h_{S_1R}|^2 + |h_{S_2R}|^2\right)^2 P_0}{\alpha^2 \frac{|h_{DR}|^2}{(L_{DR})^2}\sigma_R^2 + \sigma_D^2} \tag{15}$$

3) Received SINR in Eavesdropper: In the first step, the received signal in E, y_{E_1}, is

$$\begin{aligned} y_{E_1} &= \frac{h_{S_1E}}{L_{SE}} w_{S_1} \frac{1}{\sqrt{2}} x_0 \sqrt{P_0} + \frac{h_{S_2E}}{L_{SE}} w_{S_2} \frac{1}{\sqrt{2}} x_0 \sqrt{P_0} \\ &+ \frac{h_{DE}}{L_{DE}} x_1 \sqrt{P_1} + n_E \\ &= \frac{h_{S_1E}}{L_{SE}} \overline{h_{S_1R}} \frac{1}{\sqrt{2}} x_0 \sqrt{P_0} + \frac{h_{S_2E}}{L_{SE}} \overline{h_{S_2R}} \frac{1}{\sqrt{2}} x_0 \sqrt{P_0} \\ &+ \frac{h_{DE}}{L_{DE}} x_1 \sqrt{P_1} + n_E \end{aligned} \tag{16}$$

Therefore, the received signal power in E is

$$\begin{aligned} &E\left[y_{E_1} \overline{y_{E_1}}\right] \\ &= \frac{(|h_{S_1R}|^2 |h_{S_1E}|^2 + |h_{S_2R}|^2 |h_{S_2E}|^2) P_0}{2(L_{SE})^2} \\ &+ \frac{Re(\overline{h_{S_1R}} h_{S_1E} h_{S_2R} \overline{h_{S_2E}} + h_{S_1R} \overline{h_{S_1E} h_{S_2R}} h_{S_2E}) P_0}{2(L_{SE})^2} \\ &+ \frac{|h_{DE}|^2}{(L_{DE})^2} P_1 + \sigma_E^2 \end{aligned} \tag{17}$$

In second step, the received signal in E is derived as

$$y_{E_2} = y_R \alpha \frac{h_{RE}}{L_R E} + n_E \tag{18}$$

Therefore, the power of received signal is

$$\begin{aligned} &E\left[y_{E_2} \overline{y_{E_2}}\right] \\ &= \alpha^2 \frac{h_{RE}^2}{L_{RE}^2} E\left[y_R \overline{y_R}\right] + \sigma_E^2 \\ &= \frac{\alpha^2 |h_{RE}|^2 P_0}{2(L_{RE})^2 (L_{SR})^2} \left(|h_{S_1R}|^2 + |h_{S_2R}|^2\right)^2 \\ &+ \frac{\alpha^2 |h_{RE}|^2 |h_{DR}|^2 P_1}{(L_{RE})^2 (L_{DR})^2} + \frac{\alpha^2 |h_{RE}|^2 \sigma_R^2}{(L_{RE})^2} + \sigma_E^2 \end{aligned} \tag{19}$$

Therefore, the received SINR in E, is derived as follows.

$$\begin{aligned} SINR_E &= \frac{S}{I+N} \\ S &= \frac{(|h_{S_1R}|^2 |h_{S_1E}|^2 + |h_{S_2R}|^2 |h_{S_2E}|^2) P_0}{2(L_{SE})^2} \\ &+ \frac{Re(\overline{h_{S_1R}} h_{S_1E} h_{S_2R} \overline{h_{S_2E}} + h_{S_1R} \overline{h_{S_1E} h_{S_2R}} h_{S_2E}) P_0}{2(L_{SE})^2} \\ &+ \frac{\alpha^2 |h_{RE}|^2 P_S}{2(L_{RE})^2 (L_{SR})^2} \left(|h_{S_1R}|^2 + |h_{S_2R}|^2\right)^2 \\ I+N &= \frac{|h_{DE}|^2}{(L_{DE})^2} P_1 + 2\sigma_E^2 \\ &+ \frac{\alpha^2 |h_{RE}|^2 |h_{DR}|^2 P_1}{(L_{RE})^2 (L_{DR})^2} + \frac{\alpha^2 |h_{RE}|^2 \sigma_R^2}{(L_{RE})^2} \end{aligned} \tag{20}$$

When the received SNR in D and the received SINR in E are put into eq. (3) and eq. (4), we obtain the secure capacity.

D. Analysis of Secure Capacity in Up link

1) Received SINR in Relay: In the first step of uplink, D and S transmit the information bearing signal and the artificial noise to R, respectively. The received signal in R, y_R, is derived as

$$y_R = \frac{h_{DR}}{L_{DR}} x_0 \sqrt{P_0} + \frac{h_{SR}}{L_{SR}} x_1 \sqrt{P_1} + n_R \tag{21}$$

Therefore, the power of received signal in R is derived as

$$\begin{aligned} E\left[y_R \overline{y_R}\right] &= \frac{|h_{DR}|^2}{(L_{DR})^2} P_0 E\left[|x_0|^2\right] \\ &+ \frac{|h_{SR}|^2}{(L_{SR})^2} P_1 E\left[|x_1|^2\right] + E\left[|n_R|^2\right] \end{aligned} \tag{22}$$

Therefore the received SINR in R is

$$SINR_{DR} = \frac{\frac{|h_{DR}|^2}{(L_{DR})^2} P_0 E\left[|x_0|^2\right]}{\frac{|h_{SR}|^2}{(L_{SR})^2} P_1 E\left[|x_1|^2\right] + \sigma_R^2} \tag{23}$$

2) Received SNR in S: In the second step of uplink, the relay transmits the mixed signal between the information bearing signal and the artificial noise to S. The received signal in R is

$$y_S = y_R \alpha \frac{1}{\sqrt{2}} w_{S_1R} \frac{h_{S_1R}}{L_{SR}} + y_R \alpha \frac{1}{\sqrt{2}} w_{S_2R} \frac{h_{S_2R}}{L_{SR}} + n_S \tag{24}$$

Since S is equipped with two antennas, each antenna receives the relayed signal. After that, the two relayed signals are combined in accordance with maximum ratio combining (MRC). For combining, the weights of 1st and 2nd antennas are derived as eq.(7) and eq.(8), respectively. Since the S can remove the artificial noise from the received signal, the received SNR in S is derived as

$$SNR_S = \frac{\frac{\alpha^2}{2(L_{SR})^2}\frac{|h_{DR}|^2}{(L_{DR})^2}\left(|h_{S_1R}|^2 + |h_{S_2R}|^2\right)^2 P_0}{\alpha^2 \frac{(|h_{S_1R}|^2 + |h_{S_2R}|^2)^2}{2(L_{SR})^2}\sigma_R^2 + \sigma_S^2} \tag{25}$$

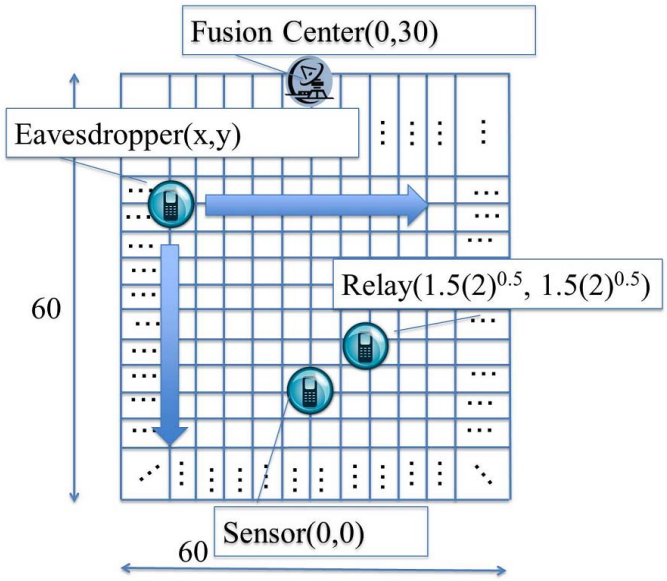

Fig. 2. Location of Eavesdropper

TABLE I. SIMULATION PARAMETERS

Transmission Power	5dBm
Noise Power	-90dBm
Relay's Noise Power	-100dBm
Artificial Noise Power	-15dBm
Center Frequency	2.4GHz
Path Loss Model	Simple Propagation Loss
Distance Attenuation Coefficient	3
Fading	Rayleigh
Number of Trials	10000

E. Received SINR in E

The received signal in E, y_{E_2}, is

$$y_{E_1} = x_0 \frac{h_{DE}}{L_{DE}} + x_1 \frac{h_{SE}}{L_{SE}} + n_E \tag{26}$$

$$y_{E_2} = y_R \alpha \frac{h_{RE}}{L_{RE}} + n_E \tag{27}$$

Therefore, the received $SINR$ in E is derived as

$$\begin{aligned} SINR_E &= \frac{S}{I+N} \\ S &= \frac{|h_{DE}|^2 P_0}{(L_{DE})^2} + \frac{\alpha^2 |h_{RE}|^2 |h_{DR}|^2 P_0}{(L_{RE})^2 (L_{DR})^2} \\ I+N &= \frac{|h_{SE}|^2}{(L_{SE})^2} P_1 + 2\sigma_E^2 \\ &+ \frac{\alpha^2 |h_{RE}|^2 |h_{SR}|^2 P_1}{(L_{RE})^2 (L_{SR})^2} + \frac{\alpha^2 |h_{RE}|^2 \sigma_R^2}{(L_{RE})^2} \end{aligned} \tag{28}$$

When the received SNR in S and the received SINR in E are put into eq. (3) and eq. (4), we obtain the secure capacity.

F. Numerical Results

Figure 2 shows the target area of wireless communication, where it is composed of 60m × 60m. The location of system

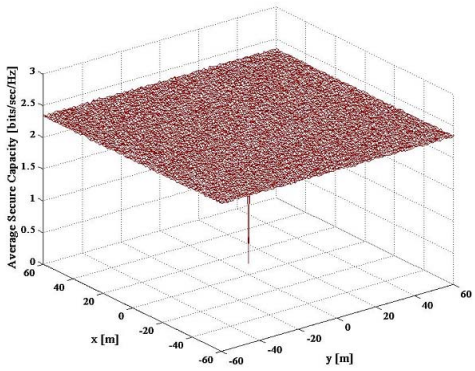

Fig. 3. Secure Capacity versus Location of Eavesdropper (Conventional 1)

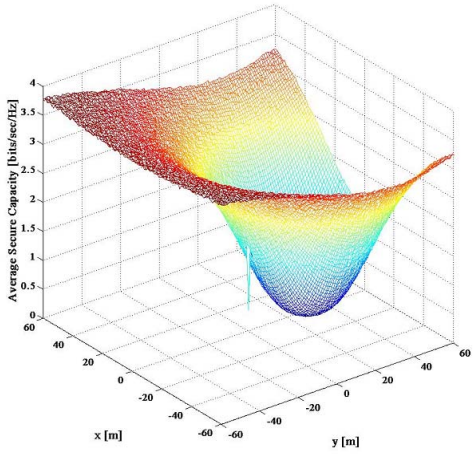

Fig. 4. Secure Capacity versus Location of Eavesdropper (Conventional 2)

is determined by x-y axes. In downlink, the S, D, and R are located at (x, y) = (0, 30), (0, 0), $(\frac{3}{\sqrt{2}}, \frac{3}{\sqrt{2}})$, respectively. In uplink, the S, D, and R are located at (x, y) = (0, 0), (0, 30), $(\frac{3}{\sqrt{2}}, \frac{3}{\sqrt{2}})$, respectively. The area is in the form of mesh, where the minimum mesh is 1m × 1m. When we assume E is located at the center of each minimum mesh, the secure capacity is evaluated.

We consider two conventional techniques. First one is null steering [9]. We assume the CSI between the source and the eavesdropper is ideally known. Therefore, the S can construct the null beam form to eavesdropper. In second conventional technique of down link, the S uses the maximal ratio transmission (MRT) to the D. Since the received signal to noise power ratio (SNR) in the D is enlarged by MRT, the E hardly obtains the required SNR for demodulation. In uplink, since the S can receive the relayed signal from the relay in two antennas, the S uses the maximal ratio combining (MRC) for obtaining the large power of relayed signal. Table I shows the simulation parameters.

1) Downlink: Figures 3, 4, and 5 show the relationship between the average secure capacity and the location of

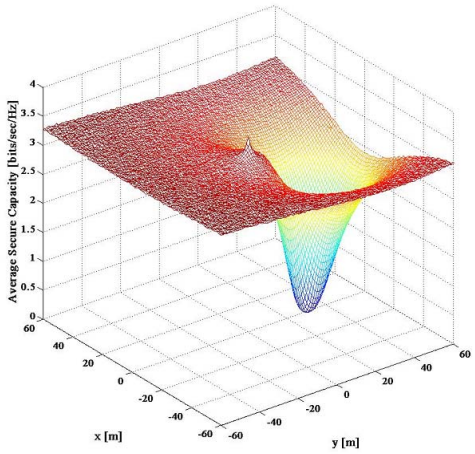

Fig. 5. Secure Capacity versus Location of Eavesdropper (Proposed)

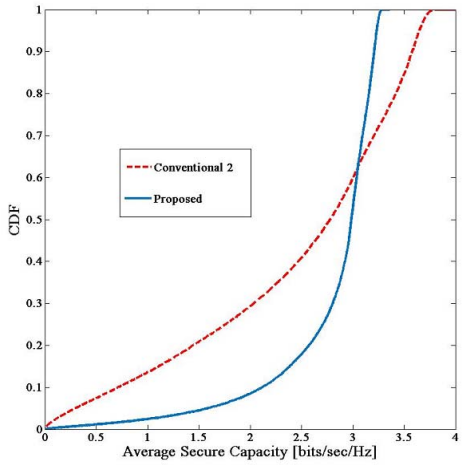

Fig. 6. CDF of Secure Capacity in Downlink

E, where the first, second, and third figures are the results with Conventional1: Null Steering, Conventional2: MRT, and Proposed: Artificial noise plus relay, respectively. In addition, Fig. 6 shows the cumulative distribution function (CDF) of average secure capacity, where Conventional 2 and Proposed technique are used.

In Figs. 3 and 4, when E is near the D, the average secure capacity significantly drops because the correlation of channel transfer function between S-E and S-D is so high that E can obtain the large received SNR. In Figs. 4 and 5, when E is near the S, the average secure capacity also drops. In proposed technique, since E is far from D and near to S, the power of artificial noise emitted by D becomes small and that of information bearing signal emitted by S becomes large. Therefore, E achieves the large received SNR enough to demodulate the signal.

In proposed technique, even when E is near to the D, the large secure capacity is achieved because the significant artificial noise makes the E difficult to demodulate the signal. In D's demodulation, since the artificial noise is perfectly removed, the large received SNR is maintained.

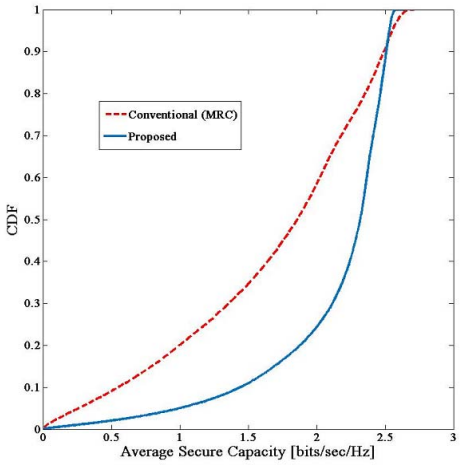

Fig. 7. CDF of Secure Capacity in Uplink

We also confirm the advantage of proposed technique from Fig. 6. In this figure, when CDF is 0.1, the secure capacity with proposed technique is 1.5 bits/sec/Hz larger than that with conventional 2. However, the maximal secure capacities with proposed technique and conventional 2 are 3.25 bits/sec/Hz and 3.75 bits/sec/Hz, respectively. This is because the relay process consume one time slot, so the secure capacity performance is degraded. Therefore, when the proposed technique sacrifices the location of large secure capacity, the area where the safe communication link can be constructed is enlarged.

2) Uplink: In uplink, S uses the MRC. Figure 7 shows the CDF performance of the average secure capacity. The proposed technique achieves 1 bits/sec/Hz large secure capacity than the conventional and thus the advantage of the proposed technique is confirmed. When we compare the uplink and the down link, the secure capacity of down link is larger than that of uplink. When we compare the received SNR in uplink, eq. (25) and that in down link, eq.(15), the noise components generated in relay is enlarged by MRC. Therefore, the average secure capacity in uplink is degraded.

G. Various Number of Relay Stations

We evaluate the secure capacity of proposed technique in multiple relay stations. Figure 8 shows the system model. There are some base stations near together. The each CSI is modeled by the independent identical distribution. We select one relay station among all the relay stations in accordance with the maximal end-to-end received SNR between S and D.

Figure 9 shows the performance of secure capacity for the various location of eavesdropper in downlink, where the number of relays is two. When we compare the performance between Figs. 9 and 5, the secure capacity in two relay station is larger than that in one relay station. For example, the maximal secure capacities are 3.9 bits/sec/Hz in Figure 9 but 3.4 bits/sec/Hz in Figure 5, respectively. The end-to-end

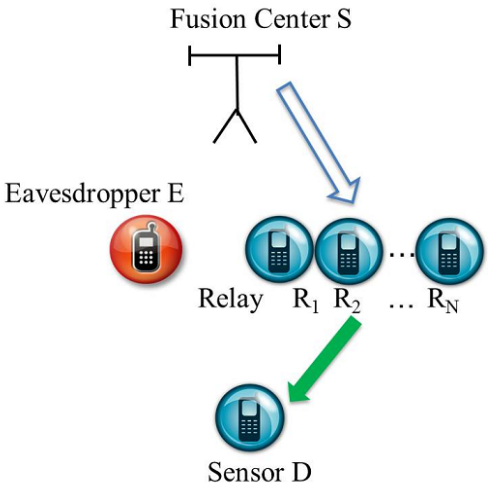

Fig. 8. System Model with Multiple Relay Stations

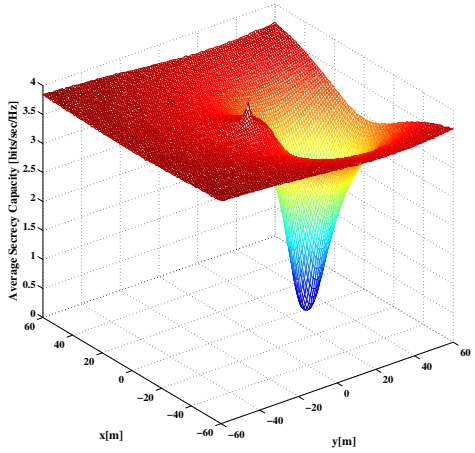

Fig. 9. System Model with Multiple Relay Stations

SNR between source and destination becomes large owing to the diversity gain of relay selection. Since the eavesdropper requires the larger SNR for demodulation, the secure capacity becomes large.

II. Conclusion

This paper proposed the secure wireless communication with using relay and artificial noise. For avoiding the leak of information to eavesdropper, the artificial noise is generated by the destination. The relay station can receive the mixed signal between the information bearing signal and the artificial noise and then it relays the mixed signal to destination. The destination removes the artificial components from the mixed signal, so the received SNR is large enough for the destination to demodulate the signal. However, the eavesdropper hardly obtains the required SNR to demodulation. From the computer simulation, we show that the proposed technique achieves the large secure capacity. The suitable position of relay station and the impact of shadowing and fading have not been considered yet, and thus these are important future work.

Acknowledgment

A part of this research project is sponsored by KAKENHI (15H04010).

References

[1] Geng Wu; S.Talwar, K.Johnsson, N.Himayat, K.D.Johnson, ”M2M: From mobile to embedded internet,” Communications Magazine, IEEE , vol.49, no.4, pp.36,43, April 2011

[2] A Tanenbum, Computer networks, Prentice Hall 4th edition, 2002.

[3] M. Bloch, J. Barros, Physical-Layer Security, Cambridge, 2011

[4] X.He and A. Yener, “Two-hop secure communication using an untrusted relay,” Eurasip J. Wireless Commun. Networks, 13pages, Nov. 2009

[5] F.Oggier, B.Hassibi, ”The Secrecy Capacity of the MIMO Wiretap Channel,” Information Theory, IEEE Transactions on , vol.57, no.8, pp.4961,4972, Aug. 2011

[6] S.Kawamura,et al.”Position Dependence of Key Capacity in Secret Key Agreement Scheme Using ESPAR Antenna” RCS2009, Sep.2009

[7] Y.Karasawa, et al.:Modeling of Signal Envelope Correlation of Line-of-Sight Fading with Applications to Frequency Correlation Analysis,IEEE Transactions on Communications,42,6,pp.2201-2203(1994)

[8] P.Popovski, H.Yomo, ”Wireless network coding by amplify-and-forward for bi-directional traffic flows,” Communications Letters, IEEE , vol.11, no.1, pp.16,18, Jan. 2007

[9] A.Goldsmith,”Wireless Communications”,Maruzen/Cambridge,2007