Overloaded Wireless MIMO Switching for Secure Wireless Communication Exchanging to Untrusted Relay

Arata Takahashi, Osamu Takyu,
Fumihito Sasamori, and Shiro Handa
Shinshu University, Japan
Email: takyu@shinshu-u.ac.jp

Takeo Fujii
The University of Electro-Communications
Japan

Tomoaki Ohtsuki
Keio University
Japan

***Abstract*—Wireless MIMO Switch makes the information exchange among terminals by two time steps. As a result, the highly efficiency of information exchanging is achieved. If the relay is impersonated by eavesdropper, it can exploit the information during the relay process, where the relay exploiting the information is the untrusted relay. In the proposed wireless MIMO switch, the stations whose number is the number of antennas plus one access the relay. As a result, the relay station hardly decodes each information owing to the overloaded access. In each station, firstly, one information signal is decoded by the interference cancellation of its own signal and the zero forcing of relay filter. Since one information signal is shared to all the stations, each station can demodulate the information because the overloaded condition is mitigated by the shared information signal. We confirm the effect of proposed scheme by computer simulation.**

I. Introduction

Recently, wireless communications among automobile vehicles in a vehicular to everything (V2X) [1] and machines in factories are attracting much attentions [2] because these improve an efficiency of traffic and productivity. The difference between these and the Internet is the non-necessity to announce the information to the world wide but deal with it in the local area, in other words the local production for local consumption type communication. Therefore, the information passed through wireless communications are so private that these should be closed within the area.

For constructing wireless communication limited by the area, a deployment of isolated cell with using access point like wireless LAN is available. All the wireless terminals access to the access point and these can exchange the information relayed through the access point. The access point of wireless LAN has simple construction but low throughput and large latency of packet access based on carrier sense multiple access (CSMA) / collision avoidance (CA) [3]. In addition, any accessing terminal can access a system configuration of access point and thus it could reconstruct the access point for exploiting the information relayed through the access point.

Recently, a wireless mimo switching (MIMO Switch) has been proposed for exchanging the information among the wireless terminals with using multiple- antenna system [4]. MIMO Switch has two phases. In the first phase, all the terminals access a relay and it is upload. In the second phase, each information is delivered to the destination terminal and it is unicast. In the unicast, the precoder matrix based on permutation matrix (PM) is applied to the received signal of the relay. The switch of the received signal from the source to destination can be changed by PM.

However, accessing to the relay without authentication procedure for simplicity has a risk about exploiting the relaying information by relay, where the relay station without authentication is referred to as an untrusted relay [6]. The untrusted relay could exploit the information during the process of MIMO switch. The security based on abstract algebra for untrusted relay in MIMO switch has been considered [7]. In addition, a physical layer security (PLS) for untrusted relay with using artificial noise [6] and the PLS assisted by PLNC [5] have been considered. The PLS makes the security of wireless communication enhanced and the required redundancy for encryption reduced.

This paper proposes the overloaded MIMO switch for secure information exchanging through the untrusted relay. In the proposed MIMO switch, there are three phases. In first phase, all the terminals access the relay station like original MIMO switch but the number of terminals is larger than the number of antennas in the relay. Therefore, the received signal in relay is under the overload. In second and third phases, the terminals except one terminal construct MIMO switch where the terminal is referred to as the excepted terminal. In the second phase, identity matrix is used as PM and thus each terminal receives its own modulated signal with the modulated signal transmitted by the excepted terminal. In the similar to the PLNC, each terminal removes its own modulated signal from the received signal and thus it can demodulate the modulated signal from the excepted terminal. Since the excepted terminal can broadcast the information to all the other terminals, second phase is referred to as broadcasting. In the third phase, the PM in the relay is changed from identity matrix to the matrix specifying the destination and then the relay sent the pre-filtered signal to all the terminals. Each terminal receives the signal composed of the modulated

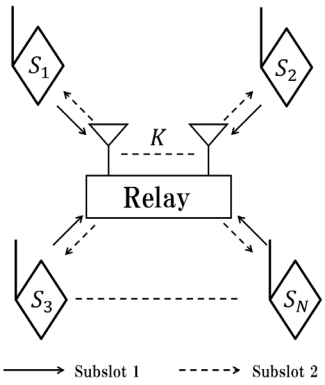

Fig. 1. System Model.

signal from the source as well as that from the excepted terminal. It can remove the modulated signal from the excepted terminal because it is obtained in second phase. Therefore, each terminal can demodulate the signal from the source. As a result, an information exchange is completed. The number of accessing signals to the relay is larger than the number of antennas in relay. Owing to the overloading, the relay has difficulty to separate the individual modulated signal and thus the secure wireless communication to the untrusted relay is constructed. From the computer simulation, the proposed MIMO Switch achieves the larger secure capacity than the original one [4].

II. System Model

Figure 1 shows an image of the considered wireless systems. There are N wireless terminals having the labels, $S_1, S_2, \ldots, S_N$. An untrusted relay, R, becomes a role of relay for exchanging the information among terminals. Each terminal has the information to the other terminals. The numbers of antennas in station and relay are 1 and K, respectively.

III. Proposed MIMO Switch: Overloaded MIMO Switch

For simple explanation, we assume the numbers of terminals, N, and antennas, K, are 3 and 2, respectively. Note that our proposed MIMO switch can be applied to the arbitral number of terminals as far as $N = K + 1$ is satisfied. In the proposed MIMO switch, there are three phases. First phase, second phase, and third phase are upload, broadcasting, and unicasting, respectively. For information exchanging, we consider the three information transfers from S_1 to S_3, S_2 to S_3, and S_3 to S_2. The proposed MIMO switch can be applied to the other pattern of information transfers by the same manner.

A. Phase1: Upload

We consider that x_{ij} is the modulated signal for informing the information of the S_ith ($i \in 1, 2, \ldots, N$) terminal to S_jth ($j \in 1, 2, \ldots, N$) terminal. In phase 1, all the terminals, S_1, S_2, and S_3, simultaneously access the relay station. We assume that h_{ik} is a channel transfer function from ith terminal to kth ($k \in a, b, \ldots,$) antenna in relay. The channel transfer function, h_{ik} is a random variable with an independent identical distribution for each terminal and each antenna. The signal recieved by kth antenna of relay, y_k, is derived as

$$\begin{bmatrix} y_a \\ y_b \end{bmatrix} = \boldsymbol{H}_{2,3} \begin{bmatrix} x_{23} \\ x_{32} \end{bmatrix} + \begin{bmatrix} h_{1a}x_{13} + v_a \\ h_{1b}x_{13} + v_b \end{bmatrix}, \tag{1}$$

where $\boldsymbol{H}_{2,3}$ is the channel transfer matrix between the stations, S_2 and S_3, and the antennas of relay and it is defined as follows.

$$\boldsymbol{H}_{2,3} = \begin{bmatrix} h_{2a} & h_{3a} \\ h_{2b} & h_{3b} \end{bmatrix}, \tag{2}$$

where v_a and v_b are the noise components in ath and bth antenna receiver, respectively.

After phase 1, the relay has the difficulty to demodulate the individual modulated signal because of overloading.

B. Phase2:Broadcasting

All the terminals except for one station construct wireless MIMO switch [4], where the latter station is referred to as the excepted station. We consider the stations, S_2 and S_3, constructed wireless MIMO switch and the excepted terminal is S_1. In wireless MIMO switching, for deciding the derivering destination terminal, the permutation matrix (PM) is used [4]. The PM is the indicator matrix and the indicator "1" means connection and "0" means disconnection. In relay, the weights of prefiltering composed of the inverse channel transfer matrix ($\boldsymbol{H}_{2,3}$) and PM are constructed. As a result, the relayed signal is given as follows.

$$\begin{bmatrix} \hat{y}_a \\ \hat{y}_b \end{bmatrix} = \boldsymbol{H}_{2,3}^{-1} \boldsymbol{A}_{a,b} \boldsymbol{P} \boldsymbol{H}_{2,3}^{-1} \begin{bmatrix} y_a \\ y_b \end{bmatrix}, \tag{3}$$

where $\boldsymbol{A}_{a,b} = \mathrm{diag}\{\alpha_a, \alpha_b\}$ and it is the factor of amplification in relay. $\boldsymbol{P} \in \mathcal{B}^{K \times K}$ is the PM[4].

In Phase 2, the proposed MIMO switch uses identity matrix as PM. As a result, S_2 and S_3 receive their own transmitted modulated signal. We assume the channel symmetry of the channel transfer function between each terminal and each antenna of relay. As a result, the channel transfer matrix in the access from each terminal to relay is the same as that from relay to each terminal. As a result, the received signals in S_2 and S_3 terminals are given as follows.

$$\begin{aligned} \begin{bmatrix} r_2 \\ r_3 \end{bmatrix} &= \boldsymbol{H}_{2,3} \begin{bmatrix} \hat{y}_a \\ \hat{y}_b \end{bmatrix} \\ &= \boldsymbol{A}_{a,b} \begin{bmatrix} x_{23} \\ x_{32} \end{bmatrix} \\ &\quad + \boldsymbol{A}_{a,b} \boldsymbol{H}_{2,3}^{-1} \begin{bmatrix} h_{1a}x_{13} + v_a \\ h_{1b}x_{13} + v_b \end{bmatrix} + \begin{bmatrix} w_2 \\ w_3 \end{bmatrix}, \end{aligned} \tag{4}$$

where w_2 and w_3 are the noise components in the receivers of S_2 and S_3, respectively. The terminals S_2 and S_3 remove each own transmitted signal from the received signal. As a result, the co-channel interference (CCI) is mitigated and then S_2 and S_3 terminals can demodulate the modulated signal

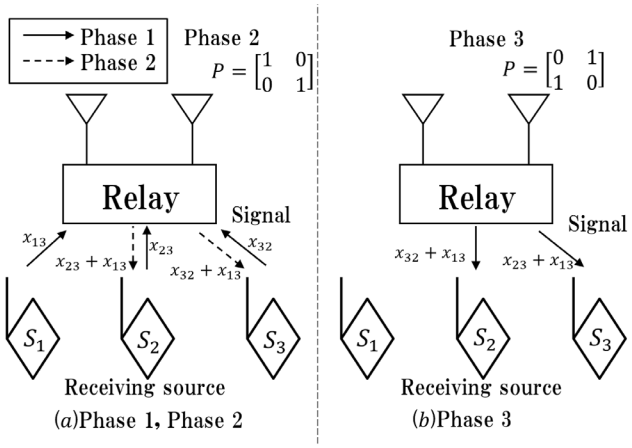

Fig. 2. Information exchange method at N = 3.

transferred from terminal S_1, x_{13}. Therefore, the excepted terminal can broadcast the signal to all the other terminals. Although terminal S_2 does not need x_{13}, it records the signal for Phase 3.

C. Phase3:Switching

After Phase 2, the relay resend the signal one more time. In this time, the PM is changed as follow.

$$P = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{5}$$

The changed PM means the modulated signals from the terminals S_2 and S_3 are transfered to the terminals S_3 and S_2, respectively. As a result, the received signal of S_2 and S_3, r_2 and r_3, are given as follow.

$$\begin{aligned} \begin{bmatrix} r_2 \\ r_3 \end{bmatrix} = & \boldsymbol{A}_{a,b} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_{23} \\ x_{32} \end{bmatrix} \\ & + \boldsymbol{A}_{a,b} \boldsymbol{H}_{2,3}^{-1} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} h_{1a} x_{13} + v_1 \\ h_{1b} x_{13} + v_2 \end{bmatrix} \\ & + \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} \\ = & \boldsymbol{A}_{a,b} \begin{bmatrix} x_{32} \\ x_{23} \end{bmatrix} \\ & + \boldsymbol{A}_{a,b} \boldsymbol{H}_{2,3}^{-1} \begin{bmatrix} h_{1b} x_{13} + v_2 \\ h_{1a} x_{13} + v_1 \end{bmatrix} + \begin{bmatrix} w_1 \\ w_2 \end{bmatrix}. \end{aligned} \tag{6}$$

The terminals S_2 and S_3 can remove the components of x_{13} from the received signals r_2 and r_3, because these receive x_{13} in Phase 2. Owing to the suppression of CCI, the terminals S_2 and S_3 can demodulate the modulated signals from S_3 and S_2, these are x_{32} and x_{23}. As a result, the information transfer among terminals is completed.

D. Extension of Proposed MIMO Switch for arbitrary number of antennas and terminals

The relationship between the number of antennas, K, and the number of terminals, N, is $N = K + 1$. In the phase 2 of the proposed MIMO switching, the modulated signal transferred from the excepted terminal is broadcasted to all the other terminals. As a result, the information transfer from the excepted terminal and other terminal is completed. In the phase 3 of the proposed MIMO switching, the total K modulated signals are exchanged among all the terminals except for the excepted terminal. As a result, the efficiency of information exchanging in the proposed MIMO switching is given as follows.

$$\frac{K+1}{3}. \tag{7}$$

On the other hand, it in the original MIMO switch [4] is given as follows.

$$\frac{K}{2}. \tag{8}$$

In $K = 2$, the channel efficiencies of proposed MIMO switch and original one are the same. In $K > 2$, that of original MIMO switch is better than that of the proposed MIMO switch. However, the proposed MIMO switch has the following advantages. 1. The security for the untrusted relay is enhanced owing to the overloading condition of relay. 2. If the information exchange are repeatedly performed, the additional information can be exchanged in odd phase. 3. A secure common control channel can be constructed.

In the 3rd advantage, the modulated signal transferred from the excepted terminal can be demodulated by only the accessing terminals to relay because the accessing terminals only know the transmitted signal and can remove them from the received signal in phase 2.

TABLE I
SIMULATION PARAMETERS.

Signal Noise Ratio	40dB
Fading	Rayleigh
Number of Trials	10000

IV. SIMULATION RESULTS

An effect of proposed MIMO switch is evaluated by computer simulation. Table I shows the simulation parameters. The average SNR between each terminal and each relay is the same.

Figure 3 shows the cumulative distribution function (CDF) of secure capacity, where the secure capacity is defined as follows.

$$C_s = \left[C(\gamma_{e2e}) - C(\gamma_r) \right]^+, \tag{9}$$

where γ_{e2e} and γ_r are an end-to-end signal to noise power ratio (SNR) between two terminals and an signal to interference plus noise power ratio (SINR) between each terminal and relay, respectively. The capacities of end to end terminals and each terminal to relay are given as follows.

$$C(\gamma_{e2e}) = \frac{1}{Slots} \log_2(1 + SNR_{ij}), \tag{10}$$

$$C(\gamma_r) = \frac{1}{Slots}\log_2(1 + SINR_{iR}), \tag{11}$$

where $SNR_{ij}(\{i,j\} \in 1,2,\ldots,N)$ is the end to end SNR from terminal S_i to terminal S_j. $SINR_{iR}$ is the SINR from terminal S_i to relay.

In the number of terminals 3, $N = 3$, the end-to-end SNR in phase 2 is given as follows.

$$SNR_{ij2} = \frac{|h_{2k}^{-1}h_{1a}\alpha_k + h_{3k}^{-1}h_{1b}\alpha_k|^2|x_{13}|^2}{\left(|h_{2k}^{-1}\alpha_k|^2 + |h_{3k}^{-1}\alpha_k|^2 + 1\right)\sigma_n^2}. \tag{12}$$

It in phase 3 is also given as follows.

$$SNR_{ij3} = \frac{|\alpha_k|^2|x_{ij}|^2}{\left\{A + |w|^2\left(|h_{2k}^{-1}\alpha_k|^2 + |h_{3k}^{-1}\alpha_k|^2 + 1\right)\right\}\sigma_n^2}, \tag{13}$$

$$A = |h_{2l}^{-1}\alpha_k|^2 + |h_{3l}^{-1}\alpha_k|^2 + 1 \quad (l \in a,b,\ldots,). \tag{14}$$

When the untrusted relay uses a zero forcing for exploiting the information, the SINR of relay station, $SINR_{iRj}$, is given as follows.

$$\begin{aligned} SINR_{2R1} &= \frac{|x_{23}|^2}{C}, \\ C &= \left\{\left|h_{23(1,1)}^{-1}h_{1a} + h_{23(1,2)}^{-1}h_{1b}\right|^2 \right. \\ &\left. + \left(\left|h_{23(1,1)}^{-1}\right|^2 + \left|h_{23(1,2)}^{-1}\right|^2\right)\right\}\sigma_n^2, \end{aligned} \tag{15}$$

$$\begin{aligned} SINR_{2R3} &= \frac{|x_{23}|^2}{D}, \\ D &= \left\{\left|h_{12(2,1)}^{-1}h_{3a} + h_{12(2,2)}^{-1}h_{3b}\right|^2 + \right. \\ &\left.\left(\left|h_{12(2,1)}^{-1}\right|^2 + \left|h_{12(2,2)}^{-1}\right|^2\right)\right\}\sigma_n^2, \end{aligned} \tag{16}$$

where σ_n^2 is noise components, $h_{ij(m,n)}^{-1}(\{m,n\} \in 1,2,\ldots,K)$ is the component of mth line and nth column in the channel transfer matrix $\boldsymbol{H}_{i,j}^{-1}$. We assume the untrusted relay tries to enhance $SINR_{2R}$ for exploiting the information. Therefore, the SINR of the untrusted relay is defined as the following equation.

$$SINR_{2R} = max\left(SINR_{2R1}, SINR_{2R3}\right). \tag{17}$$

"Conventional" indicates the original MIMO Switching [4]. As the number of terminals, N, are 3, 4, and 5, the number of antennas in relay, K are 2,3, and 4, respectively.

Figure 3 shows the secure capacity of conventional is zero secure capacity. Therefore, the secure communication cannot be constructed. The proposed MIMO switch achieve the larger secure capacity. Especially, as the number of terminals becomes larger, the secure capacity becomes larger because the channel capacity is defined as the total one among all the terminals. We evaluate the end-to-end SNR and the SINR from each terminal to relay. Figures 4 and 5 show the CDF

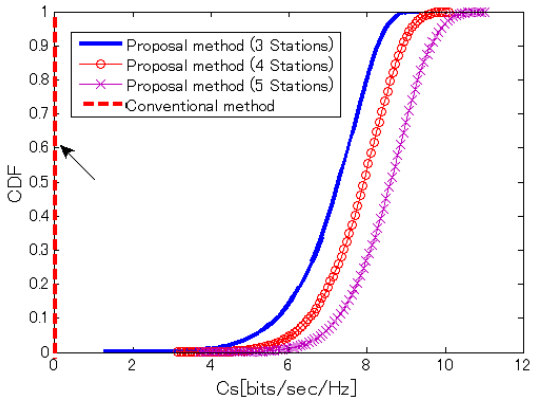

Fig. 3. CDF of Cs.

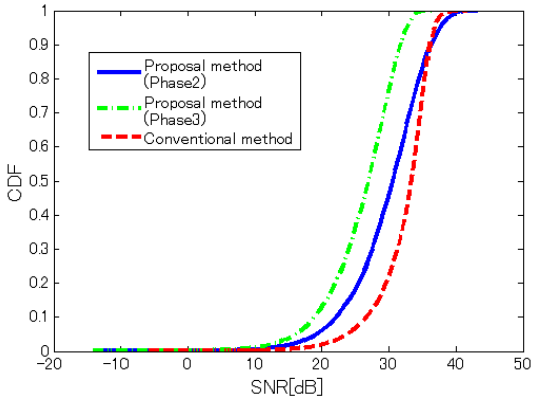

Fig. 4. CDF of SNR.

of end-to-end SNR and SINR. From Figure 4, the SNR of conventional is 8dB larger than that of Phase 3 in proposed MIMO switch. This reason is as follows. In proposed MIMO switch, the total accessing signals are larger than that in conventional by one signal. Therefore, the signal power per a signal becomes small. In addition, the soft decision signal of modulated signal transfer from the excepted terminal is used for cancellation. Therefore, the noise components are added to the received signal in phase 3. In Phase 2, the distribution of end to end SNR is more widely spread than the other performances. The prefiltering of relay station is not matched to the channel transfer function between the excepted terminal and the relay. It causes the fluctuation of received signal power. Figure 5 shows the SINR in the proposed MIMO switch is 30 dB larger than that in the conventional one owing to the overloading. Therefore, the proposed MIMO switching can construct the secure information exchange to the untrusted relay.

V. Conclusion

This paper proposed the overloaded wireless MIMO switch for secure information exchanging to the untrusted relay. In the proposed wireless MIMO switch, a terminal can securely broadcast the information signal to all the other terminals and then overloaded condition is mitigated by the interference

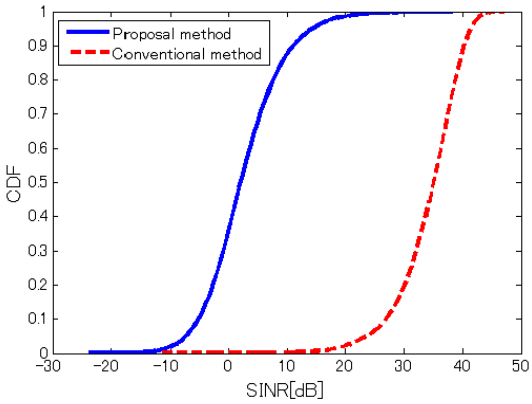

Fig. 5. CDF of SINR.

cancellation with the informed signal. From the computer simulation, the proposed wireless MIMO switch achieves larger secure capacity than the original one.

ACKNOWLEDGEMENT

A part of this research project is sponsored by MIC in Japan under SCOPE 175104004 and JSPS KAKENHI JP16K14265.

REFERENCES

[1] S. Chen et al., "Vehicle-to-Everything (v2x) Services Supported by LTE-Based Systems and 5G," in IEEE Communications Standards Magazine, vol. 1, no. 2, pp. 70-76, 2017.

[2] C. Garrido-Hidalgo, D. Hortelano, L. Roda-Sanchez, T. Olivares, M. C. Ruiz and V. Lopez, "IoT Heterogeneous Mesh Network Deployment for Human-in-the-Loop Challenges Towards a Social and Sustainable Industry 4.0," in IEEE Access, vol. 6, pp. 28417-28437, 2018.

[3] H. S. Chhaya and S. Gupta, "Performance of asynchronous data transfer methods of IEEE 802.11 MAC protocol," in IEEE Personal Communications, vol. 3, no. 5, pp. 8-15, Oct. 1996.

[4] F. Wang and S. C. Liew, "Wireless MIMO switching," 2012 IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, 2012, pp. 4374-4379.

[5] K. Yamaguchi, O. Takyu, T. Ohtsuki, F. Sasamori and S. Handa, "Physical layer network coding with multiple untrusted relays for physical layer security," Signal and Information Processing Association Annual Summit and Conference (APSIPA), 2014 Asia-Pacific, Siem Reap, 2014, pp. 1-5.

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

[7] F. Wang, X. Yuan, J. Lee and T. Q. S. Quek, "Wireless MIMO switching with trusted and untrusted relays: Degrees of freedom perspective," 2015 IEEE International Conference on Communications (ICC), London, 2015, pp. 4943-4948.