Access Decision based on Secure Capacity for prevention to CSI Impersonation of Untrusted Relay

Ryota Sugimoto* and Osamu Takyu †
* Shinshu University, Nagano, Japan
E-mail: 19W2059B@shinshu-u.ac.jp
† Shinshu University, Nagano, Japan
E-mail: takyu@shinshu-u.ac.jp

***Abstract*—A physical layer network coding is a highly efficient data exchanging scheme between two nodes through a relay. However, if the untrusted relay is assumed, it impersonates the channel state information (CSI) for exploiting the data through relay. This paper pays attention to the protocol of CSI impersonation and proposes the wireless access decision based on secure capacity. The computer simulation shows the proposed access decision suppresses the exploitation of data through relay as well as increases the secure capacity against the untrusted relay.**

I. Introduction

Wilress networks assisted relay function of wireless stations are attracting much attention [1].Physical Layer Network Coding (PLNC) achieves the high efficiency of data exchanging between two nodes through a relay [1].In PLNC, since two stations simultaneously access the relay, the signal transmitted by one station is interfered to that transmitted by the other station, the received signal to noise plus interference power ratio (SINR) in the relay is so small that the relay cannot demodulate the two transmitted signals. If no authentication to the relay is considered, the relay may steal the information through the relay process, where the relay is referred to as the untrusted relay [2]. However, in the PLNC, the untrusted relay hardly steals the information owing to the mutual interference between the two transmitted signals. The received power of signal transmitted by the station is larger than that by the other station due to the fading effect. As the SINR in relay becomes larger, the untrusted relay has opportunity to demodulate the transmitted signal. It is capture effect [4]. A transmit power control assisted by the channel state information (CSI) is effective to suppressing capture effect. Since the untrusted relay informs the CSI to the stations, it may impersonate the CSI for enlarging the SINR and exploiting the information. In [4], the impersonation model of CSI under maintaining the fidelity of fading model is constructed. The countermeasure to the impersonation of informing the CSI has not been considered, yet.

This paper proposes an access control for suppressing the secure capacity and the exploited capacity to the untrusted relay, where the exploited capacity is defined as the amount of information leaked to the untrusted relay. In the proposed access control, there are two criterions for deciding the access to the untrusted relay or not. First criterion is composed of the informing rate of each CSI and second one is composed of the assumed secure capacity and exploited capacity. From the computer simulation, the proposed access control achieves the suppression of information leak to the untrusted relay and thus it can improve the security to the exploitation of information by the untrusted relay. When the criterion of access control includes the assumed secure capacity and the assumed exploited capacity, it achieves the good tradeoff between the achieved secure capacity and the achieved exploited capacity.

II. System overview

A. System model

Figure 1 shows the overview of assumed wireless system. There are two stations, A and B, and there is a relay, R. A and B stations exchange the information data through the R. In the first phase, the A and B stations send each information bearing signal to the R. In the second phase, the R broadcasts the received combined signals to both A and B stations like the amplifying and forwarding scheme. In the R, the received signal from both A and B stations is shown as

$$y_R = w_A h_{AR} x_A \sqrt{P_A} + w_A h_{AR} x_A \sqrt{P_A} + n_R \tag{1}$$

where P_o and n_R are a transmit power of each station and noise component in relay, respectively, x_A, x_B are the information bearing signal transmitted by A and B stations, respectively, h_AR, h_BR are the channel state information (CSI)

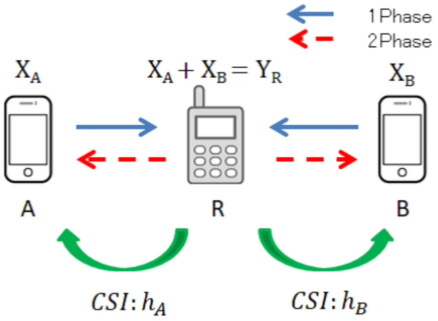

Fig. 1. System model

between A station and R and B station and R, respectively, w_A, w_B are the weight for a transmit power control (TPC) in A and B stations, respectively.

B. Transmission power control

The purpose of TPC is the suppression of capture effect in the relay station. In [3], the TPC based on zero forcing (ZF) criterions is optimal for maximizing the secure capacity. The w_A and w_B based on ZF criterion are given as

$$w_A = \frac{\frac{1}{h_{AR}}}{\sqrt{\frac{1}{h^2_{AR}} + \frac{1}{h^2_{BR}}}} \tag{2}$$

$$w_B = \frac{\frac{1}{h_{BR}}}{\sqrt{\frac{1}{h^2_{AR}} + \frac{1}{h^2_{BR}}}} \tag{3}$$

For constructing the weights, the A and B stations require the two CSIs, h_AR and h_BR. Since only the untrusted relay estimates both two CSIs, it informs two stations about the CSIs.

C. Impersonation Scheme of CSI

Figure 2 shows the quantization of CSI for informing CSI. In this paper, the amplitude distribution of CSI is considered and the untrusted relay informs the two stations about the phase component of CSI without impersonation. In figure 2, the quantization levels of CSI is 5 and the CSI is modeled by a Rayleigh probability density function. We assume the uniform quantization. The dynamic range of CSI is decided by the total range within 99% existing probability. The value of amplitude takes zero to the maximal value decided by 99% existing probability. The median of a quantized duration is considered as the informing CSI. Therefore, the occurrence probability of each quantized CSI is given by the integral of probability density function of amplitude for the quantized duration.

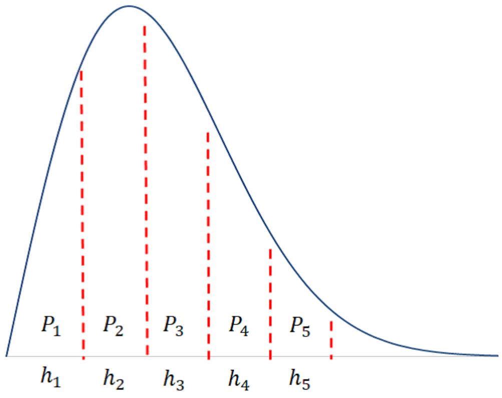

Fig. 2. Inform CSI method

III. CSI Impersonation method

For modeling the impersonation of CSI by the untrusted relay, the most powerful detection for recognizing the impersonation of CSI by the legitimated stations, stations A and B, is assumed. It is assumed that the station A and B analyzes the histogram of informed CSI during the certain long duration. If the stochastic distribution of informed CSI is not matched to that of the original CSI, the station A and B can recognize the impersonation of CSI. As a result, the untrusted relay constructs the ratio of informed CSI for maximizing the exploited capacity in the subject to the stochastic distribution of informed CSI matched to that of the original one. In Ref [4], constructing the ratio of informed CSI is linear optimization problem. The detail of the construction is given as follows.

A. Matching the informed CSI

The condition for matching the informed CSI to the original one is given as follows.

$$P_i = \sum_{j=1}^{N} \alpha(i,j) P_j \tag{4}$$

where P_i is the probability of CSI with ith quantization level,N is quantization number, $\alpha(i,j)$ is the ratio in which the original CSI is the CSI with ith quantization level but the informed CSI is that with jth quantization level.$0 \geq \alpha(i,j) \geq 1$.

$$\sum_{i=1}^{N} \alpha(i,j) = 1 \tag{5}$$

As a result, the exploited capacity is defined as

B. Secure capacity and exploited capacity

$$C_e = \sum_{j=1}^{N} \sum_{j=1}^{N} \{C_e(h_i, h_j)\} \alpha(i,j) P_j \tag{6}$$

Where $C_e(h_i, h_j)$ is the capacity of exploiting the information by the untrusted relay under the informed CSI, h_j and the original CSI, h_i.

The exploited capacity means the ability for exploiting the information through the relay process by the untrusted relay. If the untrusted relay tries to exploit the more information, the larger exploited capacity is better. Therefore, the untrusted relay can construct the impersonation ratio, $\alpha(i,j)$, for maximizing the exploited capacity. The construction problem is considered as the linear programing problem and given as follow.

$$\max C_e s$$

$$\text{Subject to } P_i = \sum_{j=1}^{N} \alpha(i,j) P_j$$

$$\sum_{j=1}^{N} \alpha(i,j) = 1, \forall i$$

$$0 \geq \alpha(i,j) \geq 1 \tag{7}$$

$$C_s = \sum_{i=1}^{N} \sum_{j=1}^{N} \{C_s(h_i, h_j)\} \alpha(i,j) P_j \tag{8}$$

The legitimated stations, A and B, also know the impersonation ratio, $\alpha(i,j)$. Therefore, these can assume not only the exploited capacity but also the secure capacity, where the secure capacity is defined as follows,

$$C_s = \sum_{i=1}^{N} \sum_{j=1}^{N} \{C_s(h_i, h_j)\} \alpha(i,j) P_j \tag{9}$$

where $C_s(h_i, h_j)$ is the secure capacity for the untrusted relay under the informed CSI, h_j, and the original CSI, h_i.

When the legitimated stations are informed by the untrusted relay about the CSI, these decide the access to the untrusted relay in accordance with the impersonation ratio, the secure capacity, and the exploited capacity. We consider the two criterions of access controls.

C. Criterion1: Impersonation Ratio

We assume the informed CSI by the untrusted relay is jth quantization level. The $\alpha(j,j)$ indicates the ratio of no difference between the informed CSI and the original CSI. The value of $\alpha(j,j)$ indicates the power of impersonation by the untrusted relay. We defines the following access criterion based on $\alpha(i,i)$ as

$$\alpha(j,j) > \eta_A \tag{10}$$

Where η_A is the certain value for deciding access ($0 \geq \eta_A \geq 1$). If this condition is true, the legitimated stations decide the access to the untrusted relay. Otherwise these stop it.

In this criterion, the larger impersonation of CSI is avoided and thus the exploited capacity can be reduced. However, the secure capacity is also reduced because the access opportunities to the untrusted relay are reduced.

D. Criterion2: Capacities

The criterion 2 takes the two capacities, secure and exploited capacities into consideration. Firstly, the following value is defined.

$$\beta(j) = \frac{C_s ji + C_e ji}{C_s ij} \tag{11}$$

and

TABLE I
SIMULATION PARAMETERS

Total Transmission Power	20dBm
Noise Power	-95dBm
Center Frequency	2400MHz
Path Loss Model	Simple propagation loss model
Fading	Rayleigh
Transmission Power Control	Zero-Forcing

$$C_s ji = \sum_{i=1}^{N} \{C_s(h_i, h_j)\} \alpha(i,j) P_j \tag{12}$$

$$C_e ji = \sum_{i=1}^{N} \{C_e(h_i, h_j)\} \alpha(i,j) P_j \tag{13}$$

If $\beta(j) = 1$, $C_e j = 0$. Therefore, the secure wireless communication is constructed. If $\beta(j) < 1$, the untrusted relay may exploit any information through the relay process. Therefore, if the untrusted relay informs the legitimated stations about jth CSI, the legitimated stations calculate $\beta(j)$ and then if the following condition is satisfied, the legitimated stations decide the access to the untrusted relay.

$$\beta > \eta_B \tag{14}$$

As η_B is larger, the exploited and secure capacities are reduced. However, $\beta(j)$ includes the secure capacities. As the large secure capacities are assumed, the legitimated stations are more willing to the access to the untrusted relay.

IV. Numerical Results

Table I shows the simulation parameters. Figure 3 shows the performance between secure capacity and exploited capacity, where the proposed access control 1 with $\eta_\alpha = 0.5$ and that 2 with $\eta_\beta = 0$ are used.

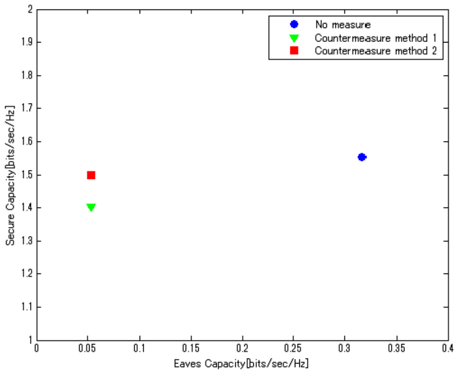

Fig. 3. α=0.5, B=0

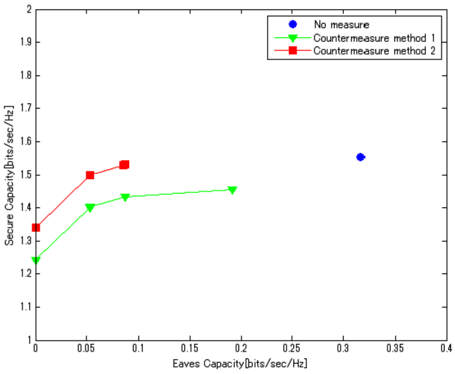

Fig. 4. α=0~ 0.9, B=-1~ 1

Tables II and III shows the secure capacity and the exploited capacity.

From the figure and tables, the secure capacity without access control achieves the largest secure capacity but the large exploited capacity. The exploited capacity with the access control with criterion 1 is as larger as that with the access control with criterion 2 but the secure capacity with the latter is 0.1 larger than that with the former. Therefore, the access control with criterion 2 can suppress the exploitation of information under the larger access opportunities for enlarging the secure capacity.

Figure 4 shows the performance between the secure capacity and the exploited capacity in the various thresholds for the proposed access control. From this figure, the access control with criterion 2 has better tradeoff between secure capacities and exploited one than that with criterion 1. Therefore, the access control with criterion 2 is available for exploiting the opportunity of access in the secure communication link and suppressing the exploitation of information by the untrusted relay.

V. Conclusion

This paper proposed the access control for suppressing the exploited capacity and enlarging the secure capacity even under the impersonation of the channel state information by the untrusted relay. The criterion of proposed access control is constructed by the informed channel state information and the assumed impersonated rate. As a result, it can exploit the opportunity of secure communication and suppress the exploitation of information by the untrusted relay. From the computer simulation, the proposed access control can construct the secure wireless communication.

TABLE II
Secure Capacity

	Average secure Capacity
No action	1.55bit/sec/Hz
Countermeasure method 1	1.40bit/sec/Hz
Countermeasure method 2	1.50bit/sec/Hz

TABLE III
Exploited Capacity

	Averge eaves Capacity
No action	0.316bit/sec/Hz
Countermeasure method 1	0.053bit/sec/Hz
Countermeasure method 2	0.053bit/sec/Hz

Acknowledgement

A part of this research project is sponsored by JSPS KAKENHI (17H03264).

References

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

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

[3] 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.

[4] K. Matsumoto, O. Takyu, T. Fujii, T. Ohtsuki, F. Sasamori and S. Handa, ”Evaluation of information leak by robustness evaluation of countermeasure to disguised CSI in PLNC considering physical layer security,” 2015 IEEE Radio and Wireless Symposium (RWS), San Diego, CA, 2015, pp. 123-125.