Physical Layer Security in Two-Path Successive Relaying

Qian Yu Liau and Chee Yen Leow

Wireless Communication Centre, Faculty of Electrical Engineering, Universiti Teknologi Malaysia, 81310 Johor Bahru, Malaysia.

Email: qianyuliau@gmail.com, bruceleow@fke.utm.my

***Abstract*—This paper proposes a bandwidth-efficient transmission protocol with one source, one destination and two assisting half-duplex relays. The two relays operate alternately in a time-division-duplex mode to forward messages from source to destination in the presence of an eavesdropper. Therefore, the source transmits new information continuously and the bandwidth efficiency of ideal full-duplex relay network can be achieved. The two relays provide higher diversity gain compared to the existing schemes assisted by one relay. By considering the achievable secrecy rate as the minimum between the secrecy rate of the S-R and R-D links, the achievable secrecy capacity can be improved. We investigate the performance of the protocol in terms of ergodic secrecy capacity and secrecy outage probability and compared to the existing half-duplex relaying, full-duplex relaying and full-duplex jamming schemes. The proposed protocol achieves the highest ergodic secrecy capacity and the lowest probability of secrecy outage compared to the existing schemes.**

***Index Terms*—Physical layer secrecy, cooperative relay networks, two-path successive relaying, secrecy capacity, secrecy outage probability.**

I. Introduction

The fifth generation (5G) network will serve as a key enabler in meeting the continuously increasing demands for future wireless applications, including an ultra-high data rate, an ultra-wide radio coverage, an ultra-large number of devices, and an ultra-low latency [1]. Owing to the broadcast nature of wireless channels, the security of 5G wireless network from eavesdropping remains one of the core challenges. Traditionally, information security has been addressed in the upper layers based on cryptographic methods. Recently, physical layer security is identified as a promising strategy that provides secure wireless transmissions by exploring the characteristics of the wireless channel.

The cooperative relaying approach has great potential to provide substantial benefits not only in terms of reliability (diversity gain) and rate (bandwidth or spectral efficiency), also has the capability to enhance wireless security [2]–[4]. A conventional half-duplex relay cannot transmit and receive signal simultaneously in the same frequency channel. Therefore, the source has to keep silent and stop transmission of new message during the relay transmission phase. As a result, the spectral efficiency for conventional half-duplex relay is only half of the spectral efficiency of direct transmission. A full-duplex relay can receive and transmit signals at the same time in the same channel is proposed to improve the spectral efficiency of cooperative relaying transmission. However, the reception of the full-duplex relay is interfered with its own transmission, which is called self-interference. The self-interference can be minimised by sophisticated hardware and/or advanced signal processing which significantly increases the cost and complexity of relay nodes [5]–[7]. Compared to full-duplex relay, the implementation of a half-duplex relay is much easier and cheaper. Two-path successive relaying is proposed to achieve the full-duplex spectral efficiency by scheduling a pair of half-duplex relays to assist the source transmission alternately [8]. Existing literature mainly considers the TPSR in conventional scenarios without eavesdroppers [9]–[13]. The performance of TPSR in secrecy communication remains open.

In this paper, we propose a secrecy two-path successive relaying protocol. We evaluate the performance of the two-path successive relaying network in terms of secrecy capacity and secrecy outage probability and compared to half-duplex relaying, full-duplex relaying and full-duplex jamming schemes in [14].

II. System Model and Transmission Protocol

A. System Model

Consider a wireless network consisting of one source (S), one destination (D), and two half-duplex relays (R_1 and R_2) in the presence of an eavesdropper (E) as shown in Figure 1, where all nodes are equipped with a single antenna. The eavesdropper can intercept the transmission from source and one relay during each time-slot, simultaneously. The R_1 and R_2 apply the decode-and-forward protocol. We assume that direct S-to-D link is not available, so transmission from S to D requires the assisting of R_1 and R_2.

We assume that all channels experience block Rayleigh fading and that the channels remain constant over one block but vary independently from one block to another. The channel coefficient from node i to node j is denoted as h_{ij} and reciprocal ($h_{ij} = h_{ji}$). The noise at relays (R_1 and R_2), D and E are denoted as $n_r(t)$, $n_d(t)$ and $n_e(t)$ with variances of σ_r^2, σ_d^2 and σ_e^2 respectively. The transmit power, P of source and relays are subject to unit power constraint.

978-1-4673-8186-4/15/$31.00 ©2015 IEEE

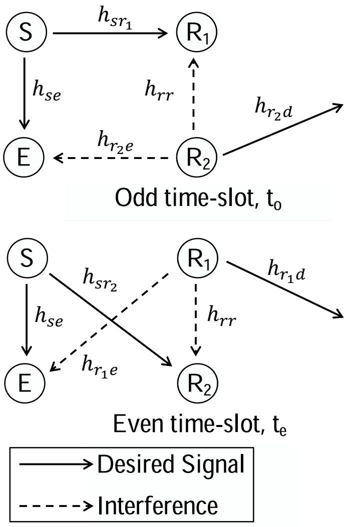

Figure 1: The secrecy two-path successive relaying (TPSR) network with an eavesdropper.

B. Transmission Protocol

The transmission protocol of two-path successive relaying (TPSR) is divided into $T+1$ consecutive equal-duration time-slots and S transmits independent codeword $x_s(t),\ t = 1,\ 2,\ \ldots,\ T$ continuously. The protocol is alternated by odd time-slot stage and even time-slot stage.

- In odd time-slot ($t_o = 1,\ 3,\ \ldots,\ T+1$), S transmits $x_s(t_o)$ and R_2 forwards $x_s(t_o-1)$. R_1 receives $x_s(t_o)$ from S while being interfered with by R_2 and D receives $x_s(t_o-1)$ from R_2. E receives $x_s(t_o)$ from S while being interfered with by R_2.
- In even time-slot ($t_e = 2,\ 4,\ \ldots,\ T$), S transmits $x_s(t_e)$ and R_1 forwards $x_s(t_e-1)$. R_2 receives $x_s(t_e)$ from S while being interfered with by R_1 and D receives $x_s(t_e-1)$ from R_1. E receives $x_s(t_e)$ from S while being interfered with by R_1.

In the first time-slot ($t=1$) and the last time slot ($t=T+1$), R_2 and S transmit artificial noise respectively to deteriorate the receiving signal of E from S. The protocol using $T+1$ time-slots to deliver T codewords from S to D, resulting in a bandwidth utilization efficiency equal to $T/(T+1)$, which approaches to one as $T\to\infty$.

The received signal at R_1, D and E in t_o are respectively given by

$$y_{r_1}(t_o) = \sqrt{P}\,h_{sr_1}x_s(t_o) + \sqrt{P}\,h_{rr}x_s(t_o-1) + n_r(t_o), \quad (1)$$

$$y_d(t_o) = \sqrt{P}\,h_{r_2d}\,x_s(t_o-1) + n_d(t_o), \quad (2)$$

$$y_e(t_o) = \sqrt{P}\,h_{se}\,x_s(t_o) + \sqrt{P}\,h_{r_2e}\,x_s(t_o-1) + n_e(t_o). \quad (3)$$

The received signal at R_2, D and E in t_e are similar to (1), (2) and (3) respectively by simply exchanging subscript R_1 and R_2. The the inter-relay interference can be mitigated effectively by spacing the two distributed relays sufficiently apart.

III. Secrecy Capacity

In [14], the secrecy capacity is defined as (see [15]),

$$C_s = [C_t - C_e]^+, \quad (4)$$

where $[x]^+ = \max(x,\,0)$, C_t and C_e are the capacities for data transmission and eavesdropping respectively. Since, the relay apply decode-and-forward relaying, the capacity for data transmission is given by

$$C_t = \min\left(C_{sr},\, C_{rd}\right), \quad (5)$$

where C_{sr} and C_{rd} are the capacities for S-to-R and R-to-D channels. For the eavesdropping capacity, C_e, the eavesdropper can decode the data from either S or R. Secrecy capacity can be defined as

$$C_s = \min\left(S_{sr},\, S_{rd}\right), \quad (6)$$

where S_{sr} and S_{rd} are the secrecy rates for S-to-R and R-to-D channels.

A. Independent Secrecy Transmission Rate

The secrecy rates for S-to-R_1 and R_1-to-D channels are given by

$$\begin{aligned} S_{sr_1} = \frac{T}{2(T+1)}\,[\log_2(1+\frac{P\left|h_{sr_1}\right|^2}{P\left|h_{rr}\right|^2+\sigma_r^2}) \\ -\log_2(1+\frac{P\left|h_{se}\right|^2}{P\left|h_{r_2e}\right|^2+\sigma_e^2})]^+, \quad (7)\end{aligned}$$

$$\begin{aligned} S_{r_1d} = \frac{T}{2(T+1)}\,[\log_2(1+\frac{P\left|h_{r_1d}\right|^2}{\sigma_d^2}) \\ -\log_2(1+\frac{P\left|h_{r_1e}\right|^2}{P\left|h_{se}\right|^2+\sigma_e^2})]^+, \quad (8)\end{aligned}$$

respectively, where $\frac{T}{2(T+1)}$ is the pre-log secrecy capacity of R_1. Then, secrecy capacity of R_1 is given as

$$C_{R_1} = \min\left(S_{sr_1},\, S_{r_1d}\right). \quad (9)$$

Similarly, secrecy capacity of R_2 can be defined by simply exchanging subscript R_1 and R_2 in (7), (8) and (9) respectively. Finally, the secrecy capacity for two-path successive relaying (TPSR) is the sum of C_{R_1} and C_{R_2} as follows

$$C_{TPSR} = C_{R_1} + C_{R_2}. \quad (10)$$

B. Secrecy Outage Probability

From (10), the secrecy outage probability for the TPSR is given by

$$\begin{aligned} P_{TPSR} &= P\left(C_{TPSR} < r_s\right) \\ &= P\left(C_{R_1} + C_{R_2} < r_s\right), \quad (11)\end{aligned}$$

where r_s is the target secrecy rate.

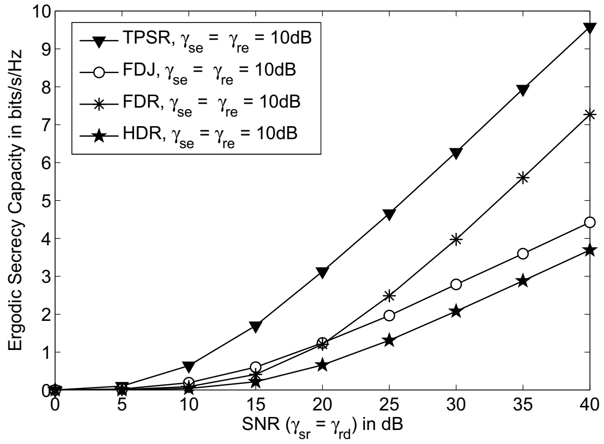

Figure 2: Ergodic secrecy capacity versus SNR where $\gamma_{sr} = \gamma_{rd}$, $\gamma_{se} = \gamma_{re} = 10\,\mathrm{dB}$ and the inter-relay interference and self-interference, $\gamma_{rr} = 0\,\mathrm{dB}$.

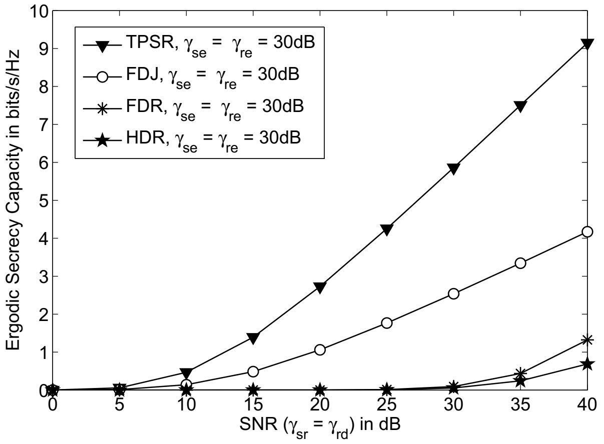

Figure 3: Ergodic secrecy capacity versus SNR where $\gamma_{sr} = \gamma_{rd}$, $\gamma_{se} = \gamma_{re} = 30\,\mathrm{dB}$ and the inter-relay interference and self-interference, $\gamma_{rr} = 0\,\mathrm{dB}$.

IV. Numerical Results

In this section, several Monte Carlo simulation results are provided to investigate the secrecy performance of the proposed two-path successive relaying (TPSR). The secrecy performance of TPSR is compared to the half-duplex relaying (HDR), full-duplex relaying (FDR) and full-duplex jamming (FDJ) schemes. In the FDR, the full-duplex relay can receive $x_s(t)$ from S and forward the previously decoded $x_s(t-1)$ to D simultaneously at time slot t. But, when the relay is receiving $x_s(t)$ from S, it is interfered by its own transmission which is called self-interference. In the FDJ, the full-duplex relay and S transmits jamming signal to E at time slot t and time slot $t+1$ respectively to deteriorate the eavesdropping capacity. This decreases the spectral efficiency of FDJ to 1/2. The details of the comparison schemes are presented in [14]. In the following simulations, the noise variances of all nodes and the transmit power of source and relay, P are normalized to unity. There are $T = 1000$ independent codewords have to be transmitted by S.

Figure 2 and Figure 3 show the ergodic secrecy capacity versus SNR of various schemes when $\gamma_{sr} = \gamma_{rd}$, inter-relay interference and residual self-interference, $\gamma_{rr} = P/\sigma_r^2 = 0\,\mathrm{dB}$ and $\gamma_{se} = \gamma_{re} = 10\,\mathrm{dB}$ (weak eavesdropping channels) and $\gamma_{se} = \gamma_{re} = 30\,\mathrm{dB}$ (strong eavesdropping channels) respectively. Regardless of weak or strong eavesdropping channels, the FDR and FDJ achieve higher ergodic secrecy capacity than the HDR. This is because the FDR has a higher spectral efficiency compared to HDR, whereas the FDJ employs jamming technique to interfere the eavesdropper. When the eavesdropping channels are strong, the jamming technique benefits the FDJ, whereas the secrecy capacity of the FDR is decreased by the increased eavesdropping capacity. On the other hand, the proposed TPSR shows its robustness by achieving the similar ergodic secrecy capacity in both cases and outperforms the other schemes significantly. The higher secrecy capacity of TPSR compared to the other schemes is contributed by the definition of the secrecy rate in (6) and the use of two relays.

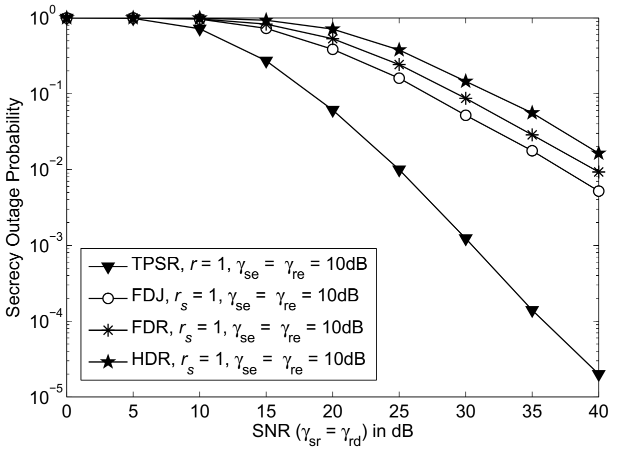

Figure 4: Secrecy outage probability versus SNR where $\gamma_{sr} = \gamma_{rd}$, $\gamma_{se} = \gamma_{re} = 10\,\mathrm{dB}$, $r_s = 1$ bits/s/Hz and the inter-relay interference and self-interference, $\gamma_{rr} = 0\,\mathrm{dB}$.

Figure 4 and Figure 5 show the secrecy outage probability versus SNR of various schemes when $\gamma_{sr} = \gamma_{rd}$, $\gamma_{rr} = 0\,\mathrm{dB}$, target secrecy rate, $r_s = 1\,\mathrm{bits/s/Hz}$ and $\gamma_{se} = \gamma_{re} = 10\,\mathrm{dB}$ and $\gamma_{se} = \gamma_{re} = 30\,\mathrm{dB}$ respectively. Same as the former simulation, the HDR has the worst performance compared to the other schemes in both cases by achieving the highest probability of secrecy outage. Based on Figure 4 and Figure 5, the HDR and FDR only able to deliver the target secrecy rate when the channel gain of the main channels is greater than the eavesdropping channels. On the other hand, the FDJ and TPSR are able deliver the target secrecy rate even the channel gain of the main channels is less than the eavesdropping channels.

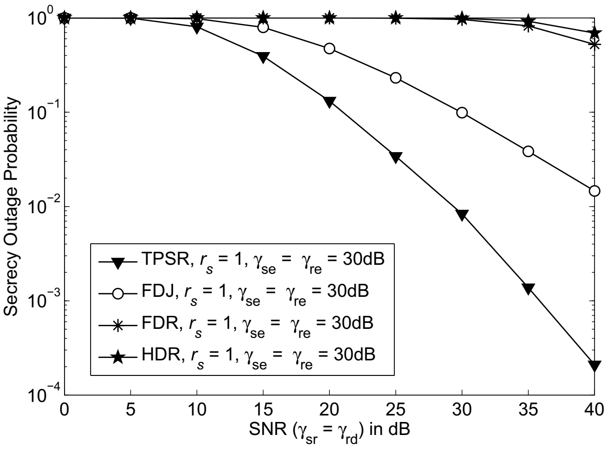

Figure 5: Secrecy outage probability versus SNR where $\gamma_{sr} = \gamma_{rd}$, $\gamma_{se} = \gamma_{re} = 30\,\mathrm{dB}$, $r_s = 1$ bits/s/Hz and the inter-relay interference and self-interference, $\gamma_{rr} = 0\,\mathrm{dB}$.

This shows the robustness of the FDJ and TPSR. In the FDJ, the eavesdropping capacity is decreased significantly when the eavesdropper has strong eavesdropping channels. This is because the eavesdropper is interfered by strong jamming signals when it has strong eavesdropping channels. For the TPSR, there are several factors that support the TPSR to achieve the lowest probability of secrecy outage compared to the other schemes in both cases. The first factor is the higher spectral efficiency of TPSR compared to the HDR and FDJ. The second factor is the higher diversity gain compared to the other schemes that provided by the two distributed half-duplex relays in TPSR.

V. Conclusion

In this paper, TPSR is proposed to improve the security for the transmission of the source and relays from interception. The numerical results reveal that the proposed TPSR has better secrecy performance compared to the other schemes in terms of ergodic secrecy capacity and secrecy outage probability. This is because the proposed TPSR achieves higher spectral efficiency compared to the HDR and FDJ. In additional, the two half-duplex relays provide higher diversity gain for the TPSR compared to the FDR. In short, with the TPSR protocol, the secured wireless transmission can be achieved by using conventional half-duplex relays without employing sophisticated jamming techniques.

Acknowledgment

This research is supported by the Ministry of Science, Technology and Innovation Malaysia (MOSTI), the Ministry of Education Malaysia (MOE) and University Teknologi Malaysia under Project Vote No. 4S079, 4F261 and 05H39.

References

[1] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5g wireless communication networks using physical layer security," *Communications Magazine, IEEE*, vol. 53, no. 4, pp. 20–27, April 2015.

[2] P. Popovski and O. Simeone, "Wireless secrecy in cellular systems with infrastructure-aided cooperation," *Information Forensics and Security, IEEE Transactions on*, vol. 4, no. 2, pp. 242–256, June 2009.

[3] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *CoRR*, vol. abs/1311.0404, 2013. [Online]. Available: http://arxiv.org/abs/1311.0404

[4] Y. Zou, J. Zhu, X. Wang, and V. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *Network, IEEE*, vol. 29, no. 1, pp. 42–48, Jan 2015.

[5] D. Bliss, T. Hancock, and P. Schniter, "Hardware phenomenological effects on cochannel full-duplex mimo relay performance," in *Signals, Systems and Computers (ASILOMAR), 2012 Conference Record of the Forty Sixth Asilomar Conference on*, Nov 2012, pp. 34–39.

[6] T. Riihonen, S. Werner, and R. Wichman, "Mitigation of loopback self-interference in full-duplex mimo relays," *Signal Processing, IEEE Transactions on*, vol. 59, no. 12, pp. 5983–5993, Dec 2011.

[7] O. Taghizadeh and R. Mathar, "Full-duplex decode-and-forward relaying with limited self-interference cancellation," in *Smart Antennas (WSA), 2014 18th International ITG Workshop on*, March 2014, pp. 1–7.

[8] B. Rankov and A. Wittneben, "Spectral efficient protocols for half-duplex fading relay channels," *Selected Areas in Communications, IEEE Journal on*, vol. 25, no. 2, pp. 379–389, February 2007.

[9] N. Nomikos and D. Vouyioukas, "A successive opportunistic relaying protocol with inter-relay interference mitigation," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International*, Aug 2012, pp. 228–233.

[10] Y. Hu, K. H. Li, and K. C. Teh, "An efficient successive relaying protocol for multiple-relay cooperative networks," *Wireless Communications, IEEE Transactions on*, vol. 11, no. 5, pp. 1892–1899, May 2012.

[11] N. Nomikos, D. Vouyioukas, T. Charalambous, I. Krikidis, D. Skoutas, and M. Johansson, "Capacity improvement through buffer-aided successive opportunistic relaying," in *Wireless Communications, Vehicular Technology, Information Theory and Aerospace Electronic Systems (VITAE), 2013 3rd International Conference on*, June 2013, pp. 1–5.

[12] N. Nomikos, T. Charalambous, I. Krikidis, D. Skoutas, D. Vouyioukas, and M. Johansson, "Buffer-aided successive opportunistic relaying with inter-relay interference cancellation," in *Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on*, Sept 2013, pp. 1316–1320.

[13] N. Nomikos, D. Vouyioukas, T. Charalambous, I. Krikidis, P. Makris, D. N. Skoutas, M. Johansson, and C. Skianis, "Joint relay-pair selection for buffer-aided successive opportunistic relaying," *Transactions on Emerging Telecommunications Technologies*, vol. 25, no. 8, pp. 823–834, 2014. [Online]. Available: http://dx.doi.org/10.1002/ett.2718

[14] G. Chen, Y. Gong, P. Xiao, and J. Chambers, "Physical layer network security in the full-duplex relay system," *Information Forensics and Security, IEEE Transactions on*, vol. 10, no. 3, pp. 574–583, March 2015.

[15] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *Information Theory, IEEE Transactions on*, vol. 54, no. 10, pp. 4687–4698, Oct 2008.