Secure Switch-and-Stay Combining with Multiple Antennas in Cognitive Radio Relay Networks

Guilherme Oliveira, Samuel Mafra, Evelio Fernández

***Abstract*— Eavesdropping is a major concern in Cognitive Radio relay systems, due to the broadcast nature of these systems. Physical Layer Security (PLS) has been seen as a good alternative to enhance the secrecy performance of these networks. Based on the concept of perfect secrecy, PLS uses an information-theoretic approach to prevent secondary transmissions from malicious attacks. In this paper, the Secure Switch-and-Stay Combining (SSSC) protocol is extended to a multiple antenna scenario, namely Secure Switch-and-Stay Combining with Multiple Antennas (SSSC-MA) protocol. To choose the best out of two relays, the SSSC-MA is adopted, and the whole transmission process is subject to a multiple antenna eavesdropper attack. Using a Transmit Antenna Selection/Maximal Ratio Combining scheme within the SSSC-MA, the secrecy performance of the extended protocol is compared to three relaying protocols, the single relay Selective Decode-and Forward, the two relay Opportunistic Relaying and the original SSSC. Results show that the proposed SSSC-MA outperforms the other protocols, achieving satisfying secrecy performance even when the eavesdropper has more antennas than the relays.**

***Keywords*— Cognitive Relay Networks, Secure Switch-and-Stay Combining, Multiple Antennas, Physical Layer Security.**

I. Introduction

The usage of wireless communications systems is increasing significantly, which entails some concerns regarding spectrum sharing and transmission security, due to inherent issues as bandwidth limitation and the broadcast nature of wireless systems [1], [2]. To promote a more efficient spectrum usage, Cognitive Radio (CR) is considered to be a key-technology, since it is an intelligent system capable of learning its surroundings and adapting its parameters, allowing unlicensed users to share the same frequency band of licensed users [3].

In the last years, several works have evaluated the protection of information through the use of Physical Layer Security (PLS) techniques, which are based on the concept of information-theoretic perfect secrecy, not excluding high-layer traditional encryption and keying security techniques [1], [3], [4].

However, these advantages come with a drawback, since CR systems increased complexity is even more susceptible to eavesdropping and other malicious attacks. Another security issue regarding CR is that the transmit power of the Secondary Users (SUs) must not exceed a predefined threshold, in order to cause minimal interference at Primary Users (PUs) channels [3].

Guilherme Oliveira, Samuel Mafra and Evelio Fernández¸ Graduate Program in Electrical Engineering, Federal University of Paraná (UFPR), Curitiba-PR, Brazil, E-mails: gui.schunemann@gmail.com, mafrasamuel@gmail.com, evelio@eletrica.ufpr.br.

In this context, some techniques can be employed to enhance the security of wireless systems, for instance: cooperative diversity, antenna diversity, jamming and channel coding [4], [5], [6], [7]. In [4] transmissions in wireless systems subject to eavesdropping are aided by cooperative diversity. It is shown that the right placement of a single relay in the network can enhance significantly the system secrecy performance in cellular networks. A comparison between employing a node as a relay or as a jammer to aid in secure transmissions is made in [5], proving that both approaches are suitable to improve the secrecy performance of the system. Coding techniques to enhance PLS were studied in [6], such as error-control coding. Antenna diversity in a CR system without relays is studied in [7], where system nodes equipped with multiple antennas achieved a better secrecy performance, even when the eavesdropper also had multiple antennas.

In any cooperative system using multiple relays, switching from one relay to another eventually occurs, and choosing the best relay to assist in the secure transmission is a major concern [8], [9]. The SSSC [10] is a cooperative diversity protocol, which chooses one out of two relays to aid the transmission in CR underlay systems with single antenna nodes. There are others dual-hop relaying protocols that may be used to enhance security in CR wireless networks. The Selective Decode-and-Forward (SDF) [11], which uses only one Decode-and-Forward (DF) relay to aid in the secure transmission; and Opportunistic Relaying (OR) [12] protocols, where multiple relays are employed to aid in transmission, but only the selected subset of relays that correctly decoded the received message is activated to forward the message to the destination.

Since the security scheme in [11] operates with the SDF with only one relay, switchings do not occur. However, the security gain is typically lower than protocols which use multiple relays. Likewise, one could employ OR schemes for relay selection in cooperative communications networks [8], nonetheless, OR schemes may have higher complexity and switching rates due to continuous channel estimation [13]. In this context, the SSSC-MA can be a positive alternative to these issues, as the protocol introduces a more complex switching mechanism compared to other techniques, in order to address these aforementioned issues while improving the secrecy performance, since it applies spatial diversity to enhance the system performance.

Among those aforementioned techniques to enhance transmission security in CR networks, spatial diversity is relatively simple to implement when relay selection protocols are being employed in multiple relay systems. Hence, the main objective of this paper is to extend the SSSC protocol to

the multiple antenna case SSSC-MA, achieving lower switching rates and simultaneously improving the system secrecy performance due to cooperative and spatial diversity. The extension was achieved by including multiple antennas on some network nodes and by adopting a Transmit Antenna Selection (TAS)/Maximal Ratio Combining (MRC) scheme in these multiple antennas nodes.

Specifically, a two-phase CR system with two DF relays in the presence of an eavesdropper is examined. Except for the primary user and the secondary source, all system nodes are equipped with multiple antennas, in order to assess the improvement in secrecy performance of a relay switching protocol when relays are equipped with multiple antennas and adopt the TAS/MRC technique.

In addition, the secrecy performances of the SSSC-MA and three other relaying protocols are compared: the security SDF scheme proposed in [12], the OR with two relays and the original single antenna SSSC, which may be considered as a particular case of the proposed SSSC-MA. The latter obtains higher performance than the other protocols, depicted by its lower Secrecy Outage Probabilities. Finally, the performance of the extended protocol was analyzed in several different scenarios, i.e., with nodes equipped with different number of antennas.

The remainder of this paper is organized as follows. Sections II and III describes the system model and its secrecy performance, respectively. Section IV presents numerical results and discussions, and Section V concludes the paper.

II. System Model and Relay Selection Scheme

A. System Model

A cognitive radio system in which secondary transmissions are subject to eavesdropping is considered. Figure 1 shows the system model, consisting of two-single antenna nodes: the primary user P and the secondary source S; and four multiple-antenna nodes: relays $\mathrm{R_i}$, $i \in \{1, 2\}$, with N_{R_1} and N_{R_2} antennas, respectively, the secondary destination D with N_D antennas and an eavesdropper E with N_E antennas. Channel coefficients of single-antenna links are denoted by $h_{m,n}^{\varrho\rho}$ while channel vectors of multiple-antenna links are denoted by $\boldsymbol{h}_{m,n}^{\varrho\rho}$. Moreover, $m \in \{S, R_1, R_2\}$ denotes the transmitter node, $n \in \{R_1, R_2, D, E\}$ denotes the receiver node, ρ is a specific antenna at node *n* and ϱ is a specific antenna at node *m*. When a node has only one antenna, superscripts ρ and ϱ are not used.

All system nodes operate in half-duplex time-division mode and both relays use the DF protocol. In addition, it is assumed that when one relay is activated, the other is off. Direct links S-D and S-E do not exist, since a severe shadowing environment is considered as in [10]. Besides, it is considered that channels undergo independent Rayleigh flat fading, with average channel gain given by

$$\lambda_{m,n} = d_{m,n}^{-\alpha}, \tag{1}$$

where $d_{m,n}$ is the distance between nodes *m* and *n* and α is the channel path loss exponent. In addition, all links are subject to Additive White Gaussian Noise (AWGN) with variance N_0.

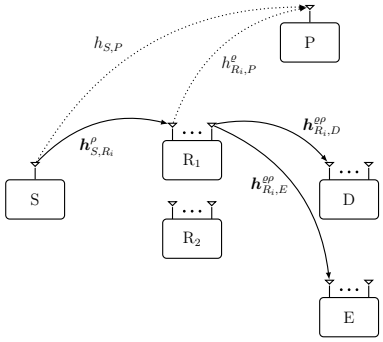

Fig. 1. System Model

It is also assumed that the relays have knowledge about the Channel State Information (CSI) of other channels, including the eavesdropper. CSI estimation is made through pilot signals and dedicated feedback channels for the interference and secondary channels. If the eavesdropper is another active user, the CSI may be estimated through some feedback from its activity. For a scenario with passive eavesdroppers, the CSI is obtained estimating the location of the eavesdropper in the network [14], [15].

Diversity techniques employed by the system are TAS, to select the best antenna at the transmitting relay, and MRC, since it is known that the system security is greater when receivers use MRC rather than other spatial diversity techniques, such as Selection Combining (SC) [16]. Hence, transmissions from S to D are always performed in two-phases. First, single-antenna node S transmits the encoded message to one of the relays, which combines each copy of the received signal using MRC. In case of successful decoding at the relay, the second transmission phase starts with $\mathrm{R_i}$ re-encoding the message and forwarding it (using TAS) to the secondary destination D, which also combines the received signal using MRC. Combining each copy of the received signal using MRC is performed at the receivers as follows

$$\|\boldsymbol{h}_{m,n}^{\varrho\rho}\|^2 = \sum_{\rho=1}^{N_n} |h_{m,n}^{\varrho\rho}|^2, \tag{2}$$

where $\|\boldsymbol{h}_{m,n}^{\varrho\rho}\|^2$ is the sum of the channel powers across all receiving antennas, $N_n \in \{N_{R_1}, N_{R_2}, N_D, N_E\}$ is the number of antennas at the receiver node and $h_{m,n}^{\varrho\rho}$ is the channel coefficient between the ϱ_{th} transmitting antenna of node *m* and the ρ_{th} receiving antenna of node *n*. In order to perform TAS in the second transmission phase, $\mathrm{R_i}$ selects one antenna to maximize the SNR at D. The index of the transmitting antenna in the $\mathrm{R_i}$-D link can be chosen as [17]

$$\varrho^* = \arg \max_{1 \le \varrho \le N_{R_i}} \|\boldsymbol{h}_{R_i,D}^{\varrho\rho}\|, \tag{3}$$

where $\boldsymbol{h}_{R_i,D}^{\varrho\rho}$ is the channel vector between the ϱ_{th} transmitting antenna at relay $\mathrm{R_i}$ and the N_D antennas at D.

Since secondary nodes operate in the underlay cognitive spectrum-sharing mode, the transmission power of SUs is constrained in order to ensure that the interference caused at

P is below an acceptable threshold

$$P_m \leq \frac{Q}{|h^{\varrho}_{m,P}|^2}, \tag{4}$$

where P_m is the transmission power of secondary node *m*, Q is the maximum allowable interference level at P and $h^{\varrho}_{m,P}$ is the instantaneous channel coefficient between secondary transmitter *m* and P.

Therefore, the received signal at R_i can be expressed as

$$\boldsymbol{y}_{R_i}(t) = \sqrt{P_S}\boldsymbol{h}^{\rho}_{S,R_i}x(t) + \boldsymbol{g}_{R_i}, \tag{5}$$

where $\boldsymbol{h}^{\rho}_{S,R_i}$ is the channel vector between S and the N_{R_i} antennas at R_i, $x(t)$ is the transmitted signal at time t and $\boldsymbol{g}_{R_i}$ is the AWGN vector at R_i. After combining the received signals using MRC, the single scalar symbol at R_i is given by

$$y_{R_i}(t) = \sqrt{P_S}\|\boldsymbol{h}^{\rho}_{S,R_i}\|^2 x(t) + \boldsymbol{h}^{\dagger}_{S,R_i}\boldsymbol{g}_{R_i}, \tag{6}$$

where $\boldsymbol{h}^{\dagger}_{S,R_i}$ is the conjugate transpose of the S-R_i channel vector. In addition, the received signal at secondary receiver node D, after performing TAS, is expressed as

$$\boldsymbol{y}_D(t) = \sqrt{P_{R_i}}\boldsymbol{h}^{\varrho^*\rho}_{R_i,D}x(t) + \boldsymbol{g}_D, \tag{7}$$

where $\boldsymbol{h}^{\varrho^*\rho}_{R_i,D}$, $1 \leq \rho \leq N_D$, is the channel vector between R_i and D, and $\boldsymbol{g}_D$ is the AWGN vector at D. Once combined employing MRC, the received signals yield a single scalar symbol at D, written as

$$y_D(t) = \sqrt{P_{R_i}}\|\boldsymbol{h}^{\varrho^*\rho}_{R_i,D}\|^2 x(t) + \boldsymbol{h}^{\dagger}_{R_i,D}\boldsymbol{g}_D. \tag{8}$$

To consider a fair comparison between the legitimate users and the eavesdropper, as in [18], it is considered that E always performs MRC when trying to intercept a message. Thus, the received signal at E is similar to (7) and (8), after substituting the corresponding indexes for the links from D to E. The ϱ^*_{th} antenna, which is chosen by TAS to maximize the SNR at D, is seen by the eavesdropper as a random choice, therefore not interfering in the system security [19], [18]. Manipulating Equations (1) to (8), the received SNR at any receiver node *n* in the system can be written as

$$\gamma_n = \tilde{Q}\frac{\|\boldsymbol{h}^{\varrho\rho}_{m,n}\|^2}{|h^{\rho}_{m,P}|^2}, \tag{9}$$

where $\tilde{Q} = Q/N_0$.

An outage event occurs when the mutual information in the link between *m* and *n* is lower than the attempted data rate. Therefore, the correct decoding at R_i, which is subject to the data rate r_d, occurs when the S-R_i channel capacity is greater or equal to the data rate:

$$\frac{1}{2}\log_2(1+\gamma_{R_i}) \geq r_d, \tag{10}$$

which is equivalent to $\gamma_{R_i} \geq D_{th}$, if a correct decoding threshold is defined as $D_{th} = 2^{2r_d} - 1$.

Finally, a secure data rate r_s, which is the rate at which the secondary source S can reliably and securely transmit its message to the secondary destination D, is predefined. Hence, the Secrecy Outage Probability (SOP) of the system can be written as

$$Pr\left[\frac{1}{2}\log_2(1+\gamma_D) - \frac{1}{2}\log_2(1+\gamma_E) < r_s\right]. \tag{11}$$

Equation (11) can also be expressed in terms of a secrecy threshold $R_{th} = 2^{2r_s}$, and after some manipulation as

$$Pr\left[\frac{1+\tilde{Q}\frac{\|\boldsymbol{h}^{\varrho^*\rho}_{R_i,D}\|^2}{|h^{\varrho^*}_{R_i,P}|^2}}{1+\tilde{Q}\frac{\|\boldsymbol{h}^{\varrho^*\rho}_{R_i,E}\|^2}{|h^{\varrho^*}_{R_i,P}|^2}} < R_{th}\right] \tag{12}$$

B. Relay Selection Scheme

In the proposed SSSC-MA protocol, before starting any transmission, a randomly selected relay R_i first estimates all channel parameters. After that, to decide whether the same relay continues to be used for transmission or a relay switch must occur, the system needs to make sure that R_i can correctly decode the message and assure a secure transmission, using the switching threshold S_{th}

$$\frac{1+\tilde{Q}\frac{\|\boldsymbol{h}^{\varrho^*\rho}_{R_i,D}\|^2}{|h^{\varrho^*}_{R_i,P}|^2}}{1+\tilde{Q}\frac{\|\boldsymbol{h}^{\varrho^*\rho}_{R_i,E}\|^2}{|h^{\varrho^*}_{R_i,P}|^2}} \geq S_{th}. \tag{13}$$

If the relay in use fails to decode the message or the switching threshold S_{th} condition is not satisfied, a relay switch is made from R_1 to R_2 or vice-versa, starting a new transmission attempt. In this scheme, relay switching depends not only on the quality of the main channels, but also on the secure transmission threshold S_{th}, which makes switching from one to another relay less frequent.

III. Secrecy Performance Analysis

The SOP of the system when using the SSSC-MA can be written as

$$P_{out_{SSSC\text{-}MA}} = \underbrace{q_1 O_{R_1}}_{1^{\text{st}}} + \underbrace{q_1 O_{R_{12}}}_{2^{\text{nd}}} + \underbrace{q_2 O_{R_2}}_{3^{\text{rd}}} + \underbrace{q_2 O_{R_{21}}}_{4^{\text{th}}}, \tag{14}$$

where q_1 and q_2 are the probabilities that relays R_1 and R_2 be activated, respectively. O_{R_1} and O_{R_2} are the SOPs when relays R_1 and R_2 continue to be used for transmission, respectively, and $O_{R_{12}}$ and $O_{R_{21}}$ are the SOPs when R_1 switches to R_2, and vice-versa, respectively. Therefore, the 1st and 3rd terms in (14) represent the outage probability when relay R_1 or R_2 are activated and able to decode the received message, but fail to achieve the secrecy threshold R_{th}, respectively.

The 2nd and 4th terms in (14) denote the outage probability when relay R_1 fails to decode the message or does not achieve the switching threshold S_{th}, and the relay R_2, after a relay switch, fails to achieve the secrecy threshold R_{th}, and vice-versa, respectively. For more detail on specific outage probabilities in Equations (14), please see the Appendix.

The SSSC-MA is compared with another two another dual-hop relaying protocols already established in the literature, the

OR with two relays and the SDF with a single relay. The SOP for these cases can be written as [12]

$$P_{out_{SDF,OR}} = 1 - [(1 - O_{SR_i}^{\Upsilon})(1 - O_{R_i D})], \quad (15)$$

where Υ is the number of relays in the system, the outage probability O_{SR_i} due to the S-R$_i$ link outage is given by

$$O_{SR_i} = \Pr\left[\left(\tilde{Q}\frac{\|\boldsymbol{h}_{S,R_i}^{\rho}\|^2}{|h_{S,P}|^2}\right) < D_{th}\right], \quad (16)$$

while the SOP of the R$_i$-D link can be written as

$$O_{R_i D} = \Pr\left[\left(\frac{1+\tilde{Q}\frac{\|\boldsymbol{h}_{R_i,D}^{\varrho^*\rho}\|^2}{|h_{R_i,P}^{\varrho^*}|^2}}{1+\tilde{Q}\frac{\|\boldsymbol{h}_{R_i,E}^{\varrho^*\rho}\|^2}{|h_{R_i,P}^{\varrho^*}|^2}}\right) < R_{th}\right]. \quad (17)$$

Hence, the end-to-end SOP is the probability that the first hop fails to achieve the decoding threshold D_{th} and the second hop fails to achieve the secrecy threshold R_{th}. Assuming equal average channel gains for every S-R$_i$ link, due to similar distances between S and every R$_i$, two situations are possible: if $\Upsilon = 1$, the protocol in use is the SDF; If $\Upsilon > 1$, the system is adopting OR. Here, this assumption was made, and when the OR protocol was analyzed Υ was set to 2.

IV. Simulation Results

In this section, numerical results are presented to evaluate the performance of the proposed SSSC-MA protocol in terms of its SOP as a function of the maximum allowable interference, Q. In the simulations, a data rate of $r_d = 1$ bits per channel use (bpcu) is considered, so that the associated SNR threshold $D_{th} = 3$ and the secure data rate was set $r_s = 0.5$ bpcu, yielding a secrecy data rate $R_{th} = 2$ bpcu. Additionally, the switching threshold S_{th} was set to 2, a unitary noise variance was considered ($N_0 = 1$) and the path loss exponent was set to $\alpha = 4$. In all simulation runs, the distance between nodes were normalized with respect to the distance between secondary source and the primary user, S and P, respectively, and d_{SP} is set to unity. Hence, the following values were used for the remaining nodes distances $d_{SR_i} = d_{R_1 D} = 0.5$, $d_{SR_2} = 0.3$, $d_{R_2 D} = 0.7$, in a scenario similar to [10].

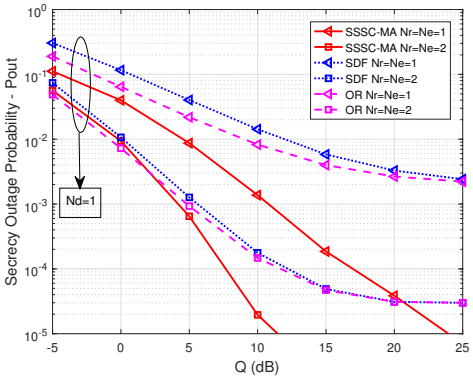

Fig. 2. System SOP using the SDF, the OR and the SSSC-MA protocols

Eavesdropper channels were considered always as a degraded version of the main channel, as in [10] using the concept of Main-to-Eavesdropper Ratio (MER), which is a ratio between the average channel gains of the main and the eavesdropper channels. Thus, the average channel gains adopted for the R$_1$-E and R$_2$-E links were $\lambda_{R_1,E} = \lambda_{R_1,D}/\text{MER}$ and $\lambda_{R_2,E} = \lambda_{R_2,D}/\text{MER}$, respectively. First, the SOP of the system using the SSSC-MA, the SDF and the OR was compared. In this comparison, the single antenna cases were assessed together with cases when $N_R = N_E = 2$ and $N_D = 1$. The results, shown on Figure 2, were achieved setting the MER to 30 dB.

For this specific scenario, it is not difficult to see that the SSSC-MA outperforms both the SDF and the OR in terms of secrecy performance. In addition, the SDF and the OR saturate faster than the SSSC-MA, due to the more complex switching mechanism of the SSSC-MA. Although the OR operates with two relays, its SOP does not change significantly compared to the single relay SDF. Examining Equation (15), one can see that the diversity gain of having more relays does not affect the outage event $O_{R_i D}$. Moreover, the more the relays, the faster O_{SR_i} tends to zero. Nonetheless, all three protocols benefit from having two antennas at the relays, even when $N_E = 2$ as well.

The SSSC-MA with only two antennas at the relays and at D achieves greater secrecy performance than the SDF, the OR and the original SSSC, even when the eavesdropper also has two antennas. Besides the better secrecy performance, the SSSC-MA operates with less relay switching during transmissions than other switching protocols, due to the switching threshold S_{th}.

Then, the SOP for the SSSC-MA employing TAS/MRC was analyzed in several multiple antenna cases. In the top part of Figure 3, the cases where the secondary destination D has only one antenna are presented. For this simulation, the MER was set to 10 dB, in order to test the SSSC-MA in a worst case compared to the original scenario in [10]. One can see that, when the eavesdropper channels are only 10 dB worse than the main channels, i.e. a low MER regime, it is difficult to achieve an acceptable SOP if D does not have multiple antennas.

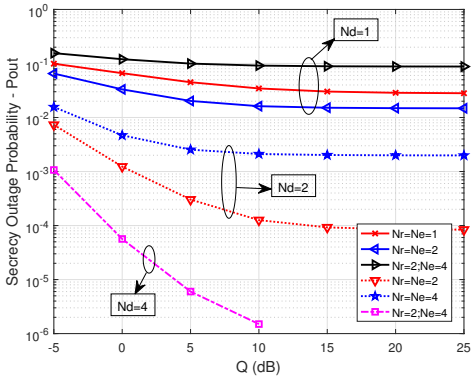

Fig. 3. SSSC-MA in different multiple antenna scenarios

In fact, when the R$_i$-D link is 10 dB better than the R$_i$-

E, satisfactory SOPs are achieved only when $N_D \geq 2$, cases seen on the bottom part of Figure 3. Increasing the number of antennas at the relays does not cause improvements in the system secrecy performance if N_E also increases. However, spatial diversity techniques prove their capability to improve the system SOP. It is straightforward to see that even when the number of antennas at the eavesdropper ($N_E = 4$) is greater than the number of antennas at the relays ($N_R = 2$), the best case is achieved when $N_D = 4$.

V. Conclusions

This paper investigated the SSSC-MA protocol secrecy performance in a two-phase CR wireless network, which promises to have a lower switching rate compared to OR protocols. Simulations results showed that the SSSC-MA outperforms the SDF and the OR protocol regarding the SOP of the system, due to cooperative diversity. In addition, the SSSC-MA outperforms also the original SSSC, on account of spatial diversity techniques. Considering a system with multiple antennas in the low MER regime, the TAS/MRC scheme plays an important role to enhance the system secrecy performance; even when $N_E \geq N_R$, if $N_D = N_E$ it is possible to achieve a SOP in the order of 10^{-6}. Future works comprise deriving analytical expressions for the SSSC-MA and assessing the effect of relay placement in the proposed scheme.

Acknowledgements

We would like to thank CAPES-CNPq for the financial support without which this research could not be made.

References

[1] J. Barros and M. D. Rodrigues, "Secrecy Capacity of Wireless Channels," *2006 IEEE International Symposium on Information Theory*, vol. 1, pp. 356–360, 2006.

[2] S. Mafra, R. Souza, J. Rebelatto, E. M. Fernandez, and H. Alves, "Cooperative overlay secondary transmissions exploiting primary retransmissions," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, no. 1, p. 196, 2013.

[3] Y. Zou, J. Zhu, L. Yang, Y.-c. Liang, and Y.-d. Yao, "Securing Physical-Layer Communications for Cognitive Radio Networks," no. September, pp. 48–54, 2015.

[4] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Communications Letters*, vol. 16, no. 6, pp. 878–881, 2012.

[5] H. Deng, H. M. Wang, W. Guo, and W. Wang, "Secrecy transmission with a Helper: To relay or to Jam," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 293–307, 2015.

[6] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proc. IEEE*, vol. 103, no. 10, pp. 1725–1746, Oct 2015.

[7] T. Zhang, Y. Cai, Y. Huang, T. Q. Duong, and W. Yang, "Secure Transmission in Cognitive MIMO Relaying Networks With Outdated Channel State Information," *IEEE Access*, vol. 3536, no. c, pp. 1–1, 2016.

[8] T. Q. Duong, T. T. Duy, M. Elkashlan, N. H. Tran, and O. A. Dobre, "Secured cooperative cognitive radio networks with relay selection," *2014 IEEE Global Communications Conference, GLOBECOM 2014*, pp. 3074–3079, 2014.

[9] M. G. Khafagy, M. S. Alouini, and S. Aïssa, "Full-Duplex opportunistic relay selection in future spectrum-sharing networks," *2015 IEEE International Conference on Communication Workshop, ICCW 2015*, pp. 1196–1200, 2015.

[10] L. Fan, S. Zhang, T. Q. Duong, and G. K. Karagiannidis, "Secure switch-and-stay combining (SSSC) for cognitive relay networks," *IEEE Transactions on Communications*, vol. 64, no. 1, pp. 70–82, 2016.

[11] H. Alves, G. Brante, R. D. Souza, D. B. Da Costa, and M. Latva-Aho, "On the performance of full-duplex relaying under phy security constraints," *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, pp. 3978–3981, 2014.

[12] Y. Zou, B. Champagne, W. P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Transactions on Communications*, vol. 63, no. 1, pp. 215–228, Jan 2015.

[13] D. Michalopoulos and G. Karagiannidis, "Distributed Switch and Stay Combining (DSSC) with a Single Decode and Forward Relay," *IEEE Communications Letters*, vol. 11, no. 5, pp. 408–410, 2007.

[14] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4871–4884, 2011.

[15] "Acknowledgments," no. August, 2008.

[16] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in mimo wiretap channels," *IEEE Transactions on Communications*, vol. 61, no. 1, pp. 144–154, January 2013.

[17] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with Alamouti scheme in MIMO wiretap channels," *GLOBECOM - IEEE Global Telecommunications Conference*, vol. 61, no. 1, pp. 665–670, 2013.

[18] J. Xiong, Y. Tang, D. Ma, P. Xiao, and K.-K. Wong, "Secrecy Performance Analysis for TAS-MRC System With Imperfect Feedback," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1617–1629, 2015.

[19] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Processing Letters*, vol. 19, no. 6, pp. 372–375, 2012.

Appendix

The Secrecy Outage Probability terms for the SSSC-MA in Equation (14) are defined as follows. The probability that relay $\mathrm{R_i}$ activates is given by

$$q_i = Pr\left[\tilde{Q}\frac{\|\boldsymbol{h}^{\rho}_{S,R_i}\|^2}{|h_{S,P}|^2} \geq D_{th}, \frac{\|\boldsymbol{h}^{\varrho}_{R_i,P}\|^2 + \tilde{Q}\|\boldsymbol{h}^{\varrho\rho}_{R_i,D}\|^2}{\|\boldsymbol{h}^{\varrho}_{R_i,P}\|^2 + \tilde{Q}\|\boldsymbol{h}^{\varrho\rho}_{R_i,E}\|^2} \geq S_{th}\right], \tag{18}$$

where i is the index of the activated relay $\{R_i | i = 1, 2\}$. The SOP due to transmitting relay outage is

$$\begin{aligned} O_{R_i} = Pr\Bigg[&\left(\tilde{Q}\frac{\|\boldsymbol{h}^{\rho}_{S,R_i}\|^2}{|h_{S,P}|^2} \geq D_{th}\right), \\ &\left(\frac{\|\boldsymbol{h}^{\varrho}_{R_i,P}\|^2 + \tilde{Q}\|\boldsymbol{h}^{\varrho\rho}_{R_i,D}\|^2}{\|\boldsymbol{h}^{\varrho}_{R_i,P}\|^2 + \tilde{Q}\|\boldsymbol{h}^{\varrho\rho}_{R_i,E}\|^2} \geq S_{th}\right), \\ &\left(\frac{\|\boldsymbol{h}^{\varrho}_{R_i,P}\|^2 + \tilde{Q}\|\boldsymbol{h}^{\varrho\rho}_{R_i,D}\|^2}{\|\boldsymbol{h}^{\varrho}_{R_i,P}\|^2 + \tilde{Q}\|\boldsymbol{h}^{\varrho\rho}_{R_i,E}\|^2} < R_{th}\right)\Bigg], \end{aligned} \tag{19}$$

and the SOP due to a relay switching from $\mathrm{R_i}$ to $\mathrm{R_j}$ is expressed as

$$\begin{aligned} O_{R_{ij}} = Pr\Bigg[&\left(\tilde{Q}\frac{\|\boldsymbol{h}^{\rho}_{S,R_i}\|^2}{|h_{S,P}|^2} < D_{th}\right) \vee \\ &\left(\frac{\|\boldsymbol{h}^{\varrho}_{R_i,P}\|^2 + \tilde{Q}\|\boldsymbol{h}^{\varrho\rho}_{R_i,D}\|^2}{\|\boldsymbol{h}^{\varrho}_{R_i,P}\|^2 + \tilde{Q}\|\boldsymbol{h}^{\varrho\rho}_{R_i,E}\|^2} < S_{th}\right), \\ &\left(\tilde{Q}\frac{\|\boldsymbol{h}^{\rho}_{S,R_j}\|^2}{|h_{S,P}|^2} \geq D_{th}\right), \\ &\left(\frac{\|\boldsymbol{h}^{\varrho}_{R_j,P}\|^2 + \tilde{Q}\|\boldsymbol{h}^{\varrho\rho}_{R_j,D}\|^2}{\|\boldsymbol{h}^{\varrho}_{R_j,P}\|^2 + \tilde{Q}\|\boldsymbol{h}^{\varrho\rho}_{R_j,E}\|^2} < R_{th}\right)\Bigg], \end{aligned} \tag{20}$$

where $\vee$ refers to the logical "OR" operation.