

Enhancing Secrecy by Full-Duplex Antenna Selection in Cognitive Networks

Gaojie Chen and Justin Coon
Department of Engineering Science,
University of Oxford, OX1 3PJ, United Kingdom.
Email: {gaojie.chen and justin.coon}@eng.ox.ac.uk

Abstract—We consider an underlay cognitive network with secondary users that support full-duplex communication. In this context, we propose the application of antenna selection at the secondary destination node to improve the secondary user secrecy performance. Antenna selection rules for cases where exact and average knowledge of the eavesdropping channels are investigated. The secrecy outage probabilities for the secondary eavesdropping network are analyzed, and it is shown that the secrecy performance improvement due to antenna selection is due to coding gain rather than diversity gain. This is very different from classical antenna selection for data transmission, which usually leads to a higher diversity gain. Numerical simulations are included to verify the performance of the proposed scheme.

Index Terms—Physical layer security, cognitive radio, antenna selection, full-duplex.

I. INTRODUCTION

The cognitive radio (CR) paradigm improves spectrum utilization by sharing resources between primary and cognitive (secondary) users. Among various spectrum sharing schemes including underlay, overlay and interweave [1], the underlay scheme is often of interest in practical implementations. In the underlay approach, the secondary user is allowed to access the spectrum of the primary user if its interference to the primary user is below a certain level.

An important issue that has attracted much attention recently is physical layer network security in the CR system. Unlike a traditional cryptographic security system [2], the physical network security is based on Shannon theory using channel coding to achieve secure transmission [3]. In a wireless network, both the intended receiver and an eavesdropper may receive the data from the source. But if the capacity of the intended channel is higher than that of the eavesdropping channel, the data can be transmitted at a rate close to the intended channel capacity so that only the intended receiver (not the eavesdropper) can successfully decode the data. The level of security is quantified by the capacity difference between the intended and eavesdropping channels, or the so called *secrecy capacity* [4].

Physical layer security has been investigated in various contexts, including direct point-to-point transmission, distributed beamforming in cooperative networks, cooperative jamming, relay and jammer selection [5], and buffer aided relay networks [6]. Many of these systems have also been considered in CR

networks. For instance, in [7], the secondary source is used as a jammer to improve the secrecy performance of the primary network. This is not a typical CR network as the secondary user does not transmit its own data. In [8], a CR network with multiple secondary users is considered, where the secondary user that maximizes the secrecy performance of the secondary network is selected for data transmission. In [9], transmission powers are carefully allocated between the primary and secondary users to balance the primary and secondary secrecy rates. Similarly, in [10], powers are optimally allocated to maximize the secrecy rate in a MIMO cognitive network, which is achieved with distributed beamforming at the source or the relay. In [11], the secrecy performance of primary user has been studied by using the dual antenna selection scheme.

Current wireless networks usually apply half-duplex relays (HDRs) which are easy to realize in practice but suffer from a comparatively poor spectral efficiency relative to devices that exploit full-duplex communication. Full-duplex systems were previously considered to be difficult to implement due to the associated self-interference, but these systems now pose an attractive alternative to HDRs in many applications because of the recent advances in the fields of antenna technology and signal processing [12], [13].

In this paper, we show that the full-duplex technique can also be used to improve the secrecy performance in CR networks. More specifically, if the secondary destination node exploits full-duplex communication, it can receive data from the source and transmit jamming signals to the eavesdropper simultaneously. As a result, the secrecy performance for both the primary and secondary networks can be improved. We additionally propose to use antenna selection at the full-duplex secondary node, where only antennas with the best data receiving performance and strongest jamming effect are selected for receiving and transmitting, respectively. Compared with transmitting jamming signals at the secondary source (e.g. [7]), the proposed scheme has the advantage that information can also be transmitted in the secondary network. Of particular interest is the secrecy outage probability of the proposed approach, which is analyzed in this work for the cases where exact and average eavesdropping channel information are available at the secondary receiver. The main contributions of this paper are summarized as follows:

- we propose the application of full-duplex communication at the secondary destination node, using antenna selection to improve secrecy performance in the cognitive network;
- we derive closed-form expressions for the secrecy outage probabilities for the secondary link for the cases where exact and average eavesdropping channel information is known at the secondary receiver;
- we analyze the secrecy diversity order and coding gain of the proposed antenna selection scheme, and conclude that the secrecy performance improvement resulting from antenna selection comes in the form of coding gain rather than diversity gain.

The remainder of the paper is organized as follows. Section II gives details of the system model and the proposed antenna selection scheme used at the full-duplex secondary destination node. Section III provides an analysis of the secrecy outage performance for the secondary eavesdropping network. Section IV gives simulation results to verify the analysis presented in the preceding section and to validate the efficacy of the proposed antenna selection scheme. Finally, section V concludes the paper.

II. SYSTEM MODEL WITH FULL-DUPLEX SECONDARY RECEIVER EMPLOYING ANTENNA SELECTION

The system model of the cognitive network with an eavesdropper is shown in Fig. 1, which consists of the primary network (including one primary source node PS and one primary destination PD), the secondary network (including one secondary source node SS and one secondary destination node SD), and one eavesdropper E . We assume the secondary destination performs in the full-duplex mode and is equipped with multiple antennas, where there are K_1 antennas for receiving data from the secondary source and K_2 antennas are for transmitting jamming signals to the eavesdropper. All other nodes are equipped with a single antenna and perform in the half-duplex mode.

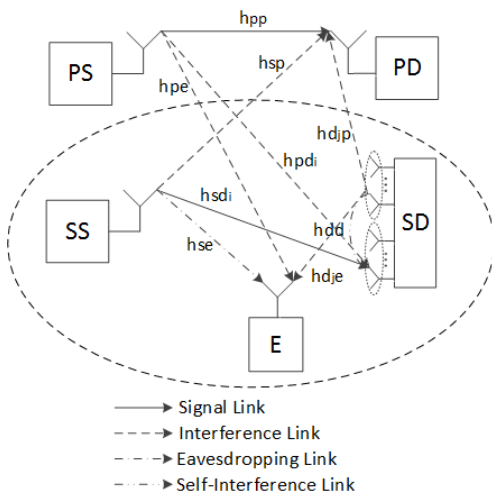


Fig. 1. Antenna selection in the CR eavesdropping system.

As is illustrated in Fig. 1, the channel coefficients for $SS \rightarrow SD_i$, $SS \rightarrow E$, $SS \rightarrow PD$, $SD_j \rightarrow PD$, $SD_j \rightarrow E$, $PS \rightarrow SD_i$, $PS \rightarrow PD$, $PS \rightarrow E$ and $SD_j \rightarrow SD_i$ are denoted as h_{sd_i} , h_{se} , h_{sp} , h_{d_jp} , h_{d_je} , h_{pd_i} , h_{pp} , h_{pe} and $h_{d_jd_i}$, respectively. The channel gains are labelled as $\gamma_{ab} = |h_{ab}|^2$ correspondingly, which are independently exponentially distributed with mean of λ_{ab} , where $ab \in \{sd_i, se, sp, d_jp, d_je, pd_i, pp, pe, d_jd_i\}$. We also assume the channels are quasi-static so that the channel coefficients remain unchanged during one packet duration, but independently vary from one packet time to another. All noises are additive white Gaussian noise. Without losing generality, the noise variances and transmission power for the primary source P_{ps} are all normalized to unity.

In the underlay cognitive system, the secondary nodes are only allowed to transmit if their interference to the primary destination is below a threshold I_{th} . We assume the secondary destination exploits full-duplex transmission. Thus the secondary source and destination nodes transmit data and jamming signals respectively at the same time, both of which impose interference to the primary destination. Similar to [8], [14], we may constrain the transmission powers of the secondary source and destination nodes by $P_{ss}\gamma_{sp} \leq 0.5I_{th}$ and $P_{sd}\gamma_{d_jp} \leq 0.5I_{th}$ respectively. We also assume that the eavesdropper can receive signals from the primary and secondary sources, but it only has the code book of the secondary source.

Without losing generality, we assume at one time, the i th receiving antenna and j th jamming antenna of the secondary destination are selected by the proposed antenna selection rules¹ for receiving and transmitting. Then the received signals at the PD , SD_i and E can be written as

$$y_{pd} = h_{pp}s_p + \sqrt{P_{ss}}h_{sp}s_s + \sqrt{P_{sd_j}}h_{d_jp}s_t + n_{pd}, \quad (1)$$

$$y_{sd_i} = \sqrt{P_{ps}}h_{pd_i}s_p + \sqrt{P_{ss}}h_{sd_i}s_s + \sqrt{P_{sd_j}}h_{d_jd_i}s_t + n_{sd_i}, \quad (2)$$

$$y_e = \sqrt{P_{ps}}h_{pe}s_p + \sqrt{P_{ss}}h_{se}s_s + \sqrt{P_{sd_j}}h_{d_je}s_t + n_e, \quad (3)$$

respectively, where s_p , s_s and s_t are the transmitted signals from the PS , SS and the j th antenna of secondary destination SD_j respectively; n_{pd} , n_{sd_i} and n_e are the noise samples at PD , SD_i and E respectively. We note that $h_{d_jd_i}$ is the self-interference channel coefficient from the transmitting to receiving antenna at the secondary destination node. The secrecy capacity is defined as [15]

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

where $[a]^+ = \max(a, 0)$, and C_d and C_e are the capacities for data channel and the eavesdrop channel, respectively. In order to maximize the secrecy capacity C_s , the selected antennas at the secondary destination need to maximize C_d and minimize C_e . To be specific, in the secondary eavesdropping

¹We come to these rules later; see (5) and (6).

network, the eavesdropper intercepts data from the secondary source. Because the reception by the secondary destination is affected by interference from the primary transmission, the receiving antenna should be selected to maximize the ratio $|h_{sd_{k_{1,i}}}|^2/|h_{pd_{k_{1,i}}}|^2$ in order to maximize the data capacity C_d . At the same time, the transmitting antenna not only jams the eavesdropper but also interferes with the reception of the primary destination. Thus, the jamming antenna should be selected to maximize $|h_{d_{k_{2,i}}e}|^2/|h_{d_{k_{2,i}}p}|^2$ in order to minimize C_e . Depending on the knowledge of the eavesdropper channel, we have two antenna selection rules:

Case 1: If the exact knowledge of all channels is available, the receiving and jamming antennas at the secondary destination are selected to satisfy

$$\begin{aligned} i_{\text{case 1}} &= \arg \max_{k_{1,i}} \left\{ \frac{|h_{sd_{k_{1,i}}}|^2}{|h_{pd_{k_{1,i}}}|^2} \right\} \\ j_{\text{case 1}} &= \arg \max_{k_{2,i}} \left\{ \frac{|h_{d_{k_{2,i}}e}|^2}{|h_{d_{k_{2,i}}p}|^2} \right\}, \end{aligned} \quad (5)$$

respectively; where $k_{1,i}, i \in (1, 2, \dots, K_1)$ and $k_{2,i}, i \in (1, 2, \dots, K_2)$ denote the i th receiving and jamming antenna at the SD, respectively.

Case 2: Only the average channel gains of the eavesdropping channels, i.e. λ_{pe} , λ_{se} and λ_{de} , are available. The exact knowledge for all other channels is known. Then the receiving and jamming antennas at the secondary destination are selected to satisfy

$$\begin{aligned} i_{\text{case 2}} &= \arg \max_{k_{1,i}} \left\{ \frac{|h_{sd_{k_{1,i}}}|^2}{|h_{pd_{k_{1,i}}}|^2} \right\} \\ j_{\text{case 2}} &= \arg \max_{k_{2,i}} \left\{ \frac{1}{|h_{d_{k_{2,i}}p}|^2} \right\}, \end{aligned} \quad (6)$$

respectively.

III. SECRECY OUTAGE PROBABILITY ANALYSIS

In the secondary eavesdropping network, the eavesdropper only has the code book of the secondary source² [8]. Receiving and jamming antenna selection at the secondary destination are applied to maximize the data transmission capacity at the secondary destination and to minimize the eavesdropping capacity at the eavesdropper respectively, leading to the best secrecy capacity in the secondary network. On the other hand, antenna selection at the secondary destination has no effect on the data transmission in the primary network since primary and secondary channels are assumed to be statistically independent. In this section, we analyze the secrecy outage probability of the secondary network for the cases where exact and average knowledge of the eavesdropping channels are available at the secondary receiver.

²For example, the primary system only transmits non-confidential message without secrecy constraint, e.g. a public video. To the contrary, the secondary system transmits confidential information which maybe intercepted by eavesdropper [16].

A. Case 1: Exact Knowledge of Eavesdropping Channels

From (2), and considering the secondary power constraints in the CR system, the capacity of secondary data transmission is given by

$$C_{sd} = \log_2 \left(1 + \frac{2\gamma_{sd_i}\gamma_{d_jp}}{\gamma_{sp}(2\gamma_{d_jp}\gamma_{pd_i} + I_{th}\gamma_{dd} + 2\gamma_{d_jp}\gamma_{sp})} \right). \quad (7)$$

Considering that current technology can significantly suppress the self-interference to the noise level (e.g [12], [17]), we assume that both the noise and self-interference γ_{dd} can be ignored when the transmission power is high enough. Further, from the receiving antenna selection rule at the secondary destination, at high SNR, we have

$$\begin{aligned} C_{sd} &\approx \log_2 \left(1 + \frac{I_{th}\gamma_{sd_i}}{2\gamma_{sp}\gamma_{pd_i}} \right) \\ &= \log_2 \left(1 + \frac{I_{th}}{2} \max_{k_{1,i}} \left(\frac{\gamma_{d_{k_{1,i}}e}}{\gamma_{d_{k_{1,i}}p}} \right) \right). \end{aligned} \quad (8)$$

Since the eavesdropper only has the codebook of the secondary source, from (3), the eavesdropping capacity is obtained as

$$\begin{aligned} C_{se} &= \log_2 \left(1 + \frac{P_{ss}\gamma_{se}}{P_{ps}\gamma_{pe} + P_{sd}\gamma_{d_{j,e}} + 1} \right) \\ &\approx \log_2 \left(\frac{P_{ss}\gamma_{se}}{P_{ps}\gamma_{pe} + P_{sd}\gamma_{d_{j,e}}} \right), \end{aligned} \quad (9)$$

where the approximation holds at high SNR. With the secondary transmission constraints in the CR system, (9) leads to

$$\begin{aligned} C_{se} &\approx \log_2 \left(\frac{I_{th}\gamma_{se}\gamma_{d_jp}}{2\gamma_{d_jp}\gamma_{sp} + I_{th}\gamma_{d_{j,e}}\gamma_{sp}} \right) \\ &\leq C_{se}^{up} = \log_2 \left(\frac{\gamma_{se}\gamma_{d_jp}}{\gamma_{sp}\gamma_{d_{j,e}}} \right). \end{aligned} \quad (10)$$

where C_{se}^{up} is the upper bound of C_{se} . When $\frac{\gamma_{d_{j,e}}}{\gamma_{d_jp}} \gg \gamma_{pe} \gg 1$, we have $C_{se} \approx C_{se}^{up}$. This occurs when the eavesdropper is closer to the secondary than to the primary source, which is often the case in the secondary eavesdropping network.

Now, from (8) and (10), and considering the antenna selection rule in Case 1, we can write the lower bound on the secrecy capacity of the secondary network as

$$\begin{aligned} C_{ss}^{low} &= C_{sd} - C_{se}^{up} \\ &\simeq \log_2 \left(\frac{I_{th}}{2\gamma_{se}} \max_{k_{1,i}} \left(\frac{\gamma_{sd_{k_{1,i}}}}{\gamma_{pd_{k_{1,i}}}} \right) \max_{k_{2,i}} \left(\frac{\gamma_{d_{k_{2,i}}e}}{\gamma_{d_{k_{2,i}}p}} \right) \right). \end{aligned} \quad (11)$$

Thus, the secrecy outage probability is given by

$$P_{ss}^{up} = P(C_{ss}^{low} < R_{ts}) = P \left(\frac{X_1 X}{W} < z_2 \right), \quad (12)$$

where

$$W = \gamma_{se}, \quad z_2 = \frac{2^{R_{ts}+1}}{I_{th}}, \quad (13)$$

$$X = \max_{k_{2,i}} \left(\frac{\gamma_{d_{k_{2,i}}e}}{\gamma_{d_{k_{2,i}}p}} \right) \quad X_1 = \max_{k_{1,i}} \left(\frac{\gamma_{sd_{k_{1,i}}}}{\gamma_{pd_{k_{1,i}}}} \right).$$

The CDF of X and X_1 can be calculated to be

$$F_X(x) = \left(\frac{x}{M+x} \right)^{K_2} \quad \text{and} \quad F_{X_1}(x_1) = \left(\frac{x_1}{N+x_1} \right)^{K_1}, \quad (14)$$

respectively, where $M = \lambda_{de}/\lambda_{dp}$ and $N = \lambda_{sd}/\lambda_{pd}$. Then we let $T = X_1X$, the CDF of T can be obtained as (15) at the top of the next page, where $\mathcal{MG}(\cdot)$ denotes Meijer's G function. Then using the fact that the PDF of W is given by

$$f_W(w) = \frac{1}{\lambda_{se}} e^{-w/\lambda_{se}}, \quad (16)$$

finally the following upper bound on the secrecy outage probability in the secondary network can be obtained as (17) at the top of the next page. In the secondary eavesdropping network, the eavesdropper is normally closer to the secondary than to the primary source, thus (17) provides a close bound for the secrecy outage probability. This will be verified in the simulations later.

B. Case 2: Knowledge of the Average Eavesdropping Channel Gains

If only the average gains of the eavesdropping channels are known, the antenna selection rule is given by (6), and the lower bound on the secrecy capacity (11) can be expressed as

$$C_{ss}^{low} = \log_2 \left(\frac{I_{th} \gamma_{d_{k_{2,i}}e}}{2\gamma_{se}} \max_{k_{1,i}} \left(\frac{\gamma_{sd_{k_{1,i}}}}{\gamma_{pd_{k_{1,i}}}} \right) \max_{k_{2,i}} \left(\frac{1}{\gamma_{d_{k_{2,i}}p}} \right) \right). \quad (18)$$

Referring to (18), let $X_1 = \max_{k_{1,i}} \left(\frac{\gamma_{sd_{k_{1,i}}}}{\gamma_{pd_{k_{1,i}}}} \right)$, $X_2 = \max_{k_{2,i}} \left(\frac{1}{\gamma_{d_{k_{2,i}}p}} \right)$ and $W_2 = \frac{\gamma_{d_{k_{2,i}}e}}{\gamma_{se}}$. Then the CDF of X_1 and the PDFs of W_2 and X_2 are written as

$$F_{X_1}(x_1) = \left(\frac{x_1}{N+x_1} \right)^{K_1},$$

$$f_{X_2}(x_2) = \frac{K_2}{\lambda_{dp} x_2^2} e^{-\frac{K_2}{\lambda_{dp} x_2}}, \quad (19)$$

$$f_{W_2}(w_2) = \frac{w_2}{(V+w_2)^2},$$

respectively. Letting $T_2 = X_1X_2$, yields the CDF of T_2 :

$$F_{T_2}(t_2) = \int_0^\infty F_{X_1}(t_2/x_2) f_{X_2}(x_2) dx_2$$

$$= \frac{\lambda_{dp} t_2 \mathcal{MG} \left([[2-K_1], []], [[2,1], []], \frac{K_2 N}{\lambda_{dp} t_2} \right)}{K_2 N \Gamma(K_1)}. \quad (20)$$

Letting $Z_2 = T_2 W_2$, we can obtain the secrecy outage probability for Case 2:

$$P_{ss}^{low} = F_{Z_2}(z_2) = \int_0^\infty F_{T_2}(z_2/w_2) f_{W_2}(w_2) dw_2$$

$$= \frac{\lambda_{dp}^2 z_2^2 \mathcal{MG} \left([[2, 3-K_1], []], [[3, 3, 2], []], \frac{V K_2 N}{\lambda_{dp} z_2} \right)}{V^2 K_2^2 N^2 \Gamma(K_1)} \quad (21)$$

where $V = \lambda_{de}/\lambda_{se}$.

C. Asymptotic Secrecy Performance for $N \rightarrow \infty$

Recall that $N = \lambda_{sd}/\lambda_{pd}$, i.e., the ratio of the average secondary data channel gain to the primary-to-secondary interference channel gain. Because the antenna selection rules for Cases 1 and 2 are similar, it is expected that the asymptotic secrecy performance for both cases are also similar. Therefore, we would like to analyze the asymptotic secrecy performance of Case 2. Firstly, it is clear from (22) that P_{ss} depends greatly on N . Similar to the secrecy performance, it is of interest to analyze the asymptotic outage performance that, when $N \rightarrow \infty$, how P_{ss} varies with the receiving antenna number K_1 . Specifically, the diversity order for the secondary data transmission can be defined as

$$d_o = - \lim_{N \rightarrow \infty} \frac{\log P_{ss}}{\log N}. \quad (22)$$

Unfortunately, because (21) contains the Meijer G function $\mathcal{MG}(\cdot)$, it is very hard to derive the diversity order. On the other hand, numerical results show that $\mathcal{MG}(\cdot)$ has little effect on the diversity order. We can then obtain from (21) and (22) that, the diversity order is approximately 2, regardless of the antenna numbers K_1 and K_2 . Therefore, there is no secrecy diversity gain from the antenna selection. Rather, the secrecy performance improvement is mainly from the coding gain, or a "shift" of the secrecy outage probability to a lower level with larger K_1 or K_2 . This will be well verified in later simulations for both Cases 1 and 2.

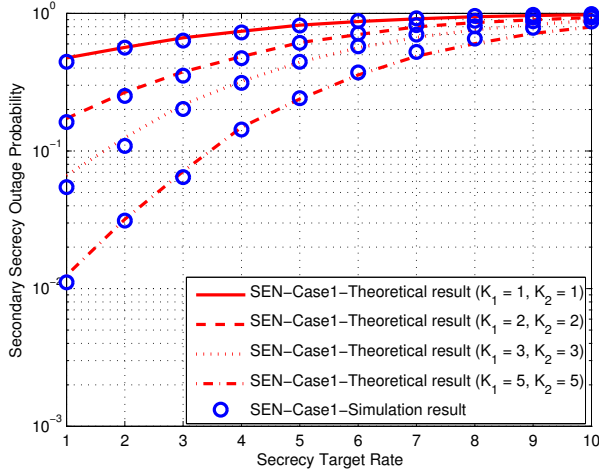
IV. NUMERICAL SIMULATIONS

In this section, simulation results are provided to verify the theoretical performance analysis detailed above and to validate the efficacy of the proposed antenna selection scheme. In the simulations, all noise variances and primary transmission powers are normalized to one. Both theoretical and simulation secrecy outage probabilities are shown in the figures on the next page, where the theoretical results are based on the outage upper bounds obtained in the previous section, and the simulation results are obtained by averaging over 10^6 independent Monte Carlo trials. In all simulations, the theoretical results are very close to the simulation results, and thus provide a good indication of the system performance, even in the case of the upper bound given for Case 1.

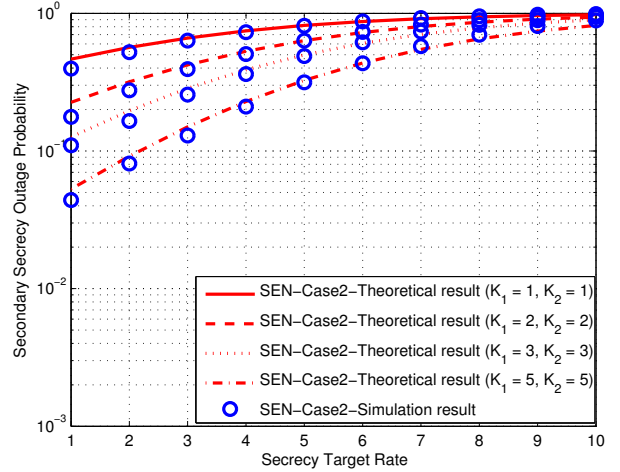
More specifically, in the simulations, we consider the secondary eavesdropping network (SEN), where we set $\gamma_{sd} = 60$

$$F_T(t) = \int_0^\infty F_X(t/x_1) f_{x_1}(x_1) dx_1 = \begin{cases} \frac{K_2 (\frac{t}{MN})^{K_2-1} \mathcal{M}\mathcal{G}([0, K_2-K_1], [], [[K_2-1, K_2], [], \frac{MN}{t}])}{\Gamma(K_1)\Gamma(K_2+1)}, & \text{if } K_1 \neq K_2, \\ \frac{K_1 t \mathcal{M}\mathcal{G}([[-1, 0], [], [[K_1-1, K_1-1], [], \frac{MN}{t}])}{MN\Gamma(K_1)\Gamma(K_1+1)}, & \text{if } K_1 = K_2, \end{cases} \quad (15)$$

$$P_{ss0}^{up} = F_{Z_2}(z_2) = \int_0^\infty F_T(z_2 w) f_W(w) dw = \begin{cases} \frac{(\frac{\lambda_{se} z_2}{MN})^{K_2-2} \mathcal{M}\mathcal{G}([[-1, K_2-K_1-1], [], [[K_2-2, K_2-1, K_2-1], [], \frac{MN}{\lambda_{se} z_2}])}{\Gamma(K_1)\Gamma(K_2)}, & \text{if } K_1 \neq K_2, \\ \frac{K_1 \mathcal{M}\mathcal{G}([[-1-K_1, 1-K_1], [], [[1, 1, 0], [], \frac{MN}{\lambda_{se} z_2}])}{\Gamma(K_1)\Gamma(K_1+1)}, & \text{if } K_1 = K_2. \end{cases} \quad (17)$$



(a) Case 1



(b) Case 2

Fig. 2. The secondary secrecy outage probabilities vs target secrecy rate.

dB, $\gamma_{sp} = \gamma_{dp} = 10$ dB, $\gamma_{se} = 40$ dB, $\gamma_{pe} = 5$ dB, $\gamma_{pd} = 30$ dB, $\gamma_{dd} = 1$ dB, $\gamma_{de} = 20$ dB, and $I_{th} = 3$. Fig. 2 (a) and (b) show the secrecy outage probability plotted against the secrecy target rate of the secondary network for Cases 1 and 2. It is observed that the secrecy performance improves significantly with more antennas for selection. It is also shown that the secrecy performance with exact eavesdropping channel information (Case 1) is better than the case when only average information is available (Case 2).

Fig. 3 shows the secrecy outage probability plotted against $N = \lambda_{sd}/\lambda_{pd}$, where the results for Cases 1 and 2 are shown. Here, we set $I_{th} = 1$, the average gain ratio $V = \lambda_{de}/\lambda_{se} = -20$ dB, $\lambda_{dp} = 10$ dB, and the secrecy target rate is $R_{st} = 3$ bits per channel use. It is clearly shown that, for both Case 1 and Case 2, the rate at which the secrecy outage probability decreases with respect to N does not change with different numbers of antennas. These results indicate that the diversity gain is fixed. However, with more antennas, the secrecy performance still improves, which is clearly due to a coding gain, or more accurately described, array gain. This result corroborates the analysis detailed above.

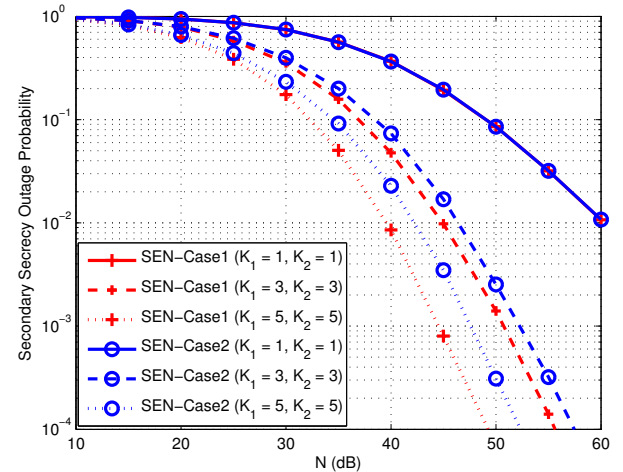


Fig. 3. The secondary secrecy outage probabilities vs $N = \lambda_{sd}/\lambda_{pd}$ (dB).

V. CONCLUSIONS

In this paper, we proposed the application of full-duplex communication at the secondary destination along with an-

tenna selection to improve the physical layer secrecy performance for secondary eavesdropping networks. Antenna selection rules for the cases where exact knowledge and statistical knowledge of the eavesdropping channels were considered, and the secrecy outage performance was analyzed for each case. Additionally, the asymptotic secrecy performance showed that the secrecy performance improvement is a result of coding (array) gain rather than diversity gain. Numerical simulations were executed, the results of which validated the proposed scheme and pointed to significant gains that can be achieved in practice using the proposed approach. In the future, we will consider how the channels correlated affects the secrecy performance.

ACKNOWLEDGEMENTS

This work was supported by EPSRC grant number EP/N002350/1 (“Spatially Embedded Networks”).

REFERENCES

- [1] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, “Breaking spectrum gridlock with cognitive radios: an information theoretic perspective,” *Proceedings of the IEEE*, vol. 97, no. 5, pp. 894–914, May. 2009.
- [2] E. D. Silva, A. L. D. Santos, L. C. P. Albin, and M. Lima, “Identity-based key management in mobile ad hoc networks: Techniques and applications,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 5, pp. 46–52, Oct. 2008.
- [3] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.
- [4] A. Khisti, A. Tchamkerten, and G. W. Wornell, “Secure broadcasting over fading channels,” *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2453–2469, June 2008.
- [5] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, “Physical layer network security in the full-duplex relay system,” *IEEE Trans. Inf. Forensics and Security*, vol. 10, no. 3, pp. 574–583, March 2015.
- [6] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, “Max-ratio relay selection in secure buffer-aided cooperative wireless networks,” *IEEE Trans. Inform. Forensics and Security*, vol. 9, no. 4, pp. 719–729, Apr. 2014.
- [7] Z. Shu, Y. Yang, Y. Qian, and R. Hu, “Impact of interference on secrecy capacity in a cognitive radio network,” in *Proc. IEEE Globecom, Houston, USA*, Apr. 2011.
- [8] Y. Zou, X. Wang, and W. Shen, “Physical-layer security with multiuser scheduling in cognitive radio networks,” *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 5103–5113, Dec. 2013.
- [9] Y. Wu and K. Liu, “An information secrecy game in cognitive radio networks,” *IEEE Trans. Inform. Forensics and Security*, vol. 6, no. 3, pp. 831–842, Sep. 2011.
- [10] N. Mokari, S. Parsaeefard, H. Saeedi, and P. Azmi, “Cooperative secure resource allocation in cognitive radio networks with guaranteed secrecy rate for primary users,” *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 1058–1073, Feb. 2014.
- [11] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, “Dual antenna selection in secure cognitive radio networks,” *IEEE Tran. Veh. Tech.*, vol. 65, no. 10, pp. 7993–8002, Oct. 2016.
- [12] H. Ju, E. Oh, and D. Hong, “Improving efficiency of resource usage in two-hop full duplex relay systems based on resource sharing and interference cancellation,” *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 3933–3938, Aug. 2009.
- [13] T. Riihonen, S. Werner, and R. Wichman, “Optimized gain control for single-frequency relaying with loop interference,” *IEEE Trans. Wireless Commun.*, vol. 8, pp. 2801–2806, June 2009.
- [14] G. Chen, Y. Gong, and J. A. Chambers, “Study of relay selection in a multi-cell cognitive network,” *IEEE Wireless Commun. Lett.*, vol. 11, no. 6, pp. 2351–2354, June 2012.
- [15] P. K. Gopala, L. Lai, and H. E. Gamal, “On the secrecy capacity of fading channels,” *IEEE Trans. Inform. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
- [16] N. Yang, L. Wang, G. Geraci, M. ElKashlan, J. Yuan, and M. D. Renzo, “Safeguarding 5G wireless communication networks using physical layer security,” *IEEE Communications Magazine*, vol. 53, pp. 20–27, April 2015.
- [17] C. R. Anderson, S. Krishnamoorthy, C. G. Ranson, T. J. Lemon, W. G. Newhall, T. Kummetz, and J. H. Reed, “Antenna isolation, wideband multipath propagation measurements and interference mitigation for on-frequency repeaters,” in *Proc. IEEE SoutheastCon*, Mar. 2004.