SECURE PERFORMANCE ANALYSIS OF BUFFER-AIDED COGNITIVE RELAY NETWORKS UNDER DELAY UNCONSTRAINT CASE

Aiwei Sun[1] *Tao Liang*[2] *Yajun Zhang* [1]

[1] College of Communications Engineering, PLA University of Science and Technology
[2] Nanjing Telecommunication Technology Institute

ABSTRACT

This paper investigates the physical layer security for a buffer-aided cooperative cognitive radio network in the presence of an eavesdropper, wherein the relay is equipped with a buffer so that it can store packets received from secondary source. Multiple primary users (PUs) locate in the transmission range of the secondary users (SUs), and quality of service (QoS) requirement of them must be guaranteed. To improve the secure performance of cognitive radio networks, we propose a novel secure link selection scheme which incorporates the instantaneous strength of the wireless links and the status of buffer, the interference on PUs should be kept below a specific threshold simultaneously. Closed-form expressions of secrecy outage probability (SOP) for cognitive radio network is obtained based on the Markov chain. Numerical results demonstrate that the proposed scheme can significantly enhance the secure performance compared to the conventional relay selection scheme.

Index Terms— physical layer security, cognitive radio, buffer-aided relay, secrecy outage probability

1. INTRODUCTION

Cognitive radio (CR) is a promising technology which can alleviate the wireless spectrum under-utilization by allowing secondary users (SUs) to opportunistically access the licensed channels without degrading quality of service (QoS) of primary users (PUs), there are mainly three kinds of cognitive radio working modes: overlay, underlay and hybrid overlay/underlay [1]. Here we focus on the underlay working mode of CR, thus SUs can concurrently share the licensed spectrum with PUs if the interference on PUs is under a specific threshold. Similar to the general wireless networks, cognitive radio networks (CRNs) are vulnerable to malicious attacks due to the dynamic nature of wireless channel and the distributed nature of the CR architecture [2]. Traditional cryptographic techniques not only impose additional system complexity in terms of the secret key management, but also can be decrypted by exhaustive key search with the aid of brute-force attack. As an alternative, physical layer security is now emerging as a new secure communication method to defend against eavesdroppers by exploiting the physical characteristics of wireless channels [3], it has been investigated extensively in non-cognitive wireless transmission scene by exploiting the cooperative relays [4][5], however, all of them adopt conventional relay protocols, namely, the best "Source-to-Relay ($S-R$)" links and "Relay-to-Destination ($R-D$)" links for a packet transmission should be determined simultaneously.

Recently, buffer-aided cooperative transmission protocol has attracted increasing attention due to its significant performance advantage over the conventional cooperative protocols [6∼11]. By introducing data buffers at the relay, it is possible to relax the constraint in the conventional cooperative protocols. To improve the secure performance of the cooperative CRNs, we proposed a novel buffer-aided cognitive secure link selection scheme in this letter, which is different from existing works from the following two aspects: 1) since interference constraint problem must be taken into consideration, the link selection policy in [9] and [10] can not be applied to cognitive radio situation; 2) the link selection policy in [9] and [11] focused on general wireless communication without eavesdropping, which does not consider the security in cognitive radio situation. To the best of our knowledge, this is the first work that introduces the buffer at the relay for cooperative CRNs, and investigates the secure performance simultaneously. We have also derived the close-form expressions of secrecy outage probability (SOP) for cooperative CRNs to accurate assess the secrecy performance, which will be explained in details in the section 3.

2. SYSTEM MODEL AND PROTOCOL DESCRIPTION

The system model is shown in Fig. 1, we consider an cooperative CRN where a secondary source (S) communicate with a secondary destination (D) with the help of a relay node (R), R is equipped with a data buffer Q of finite size L (in the number of data packets) and operates on half-duplex decode and forward (DF) mode for easy implementation, no direct

This research was supported in part by the National Nature Science Foundation of China under grant 61471392 and grant 61501507, by Jiangsu Provincial National Science Foundation under grant BK20150719.

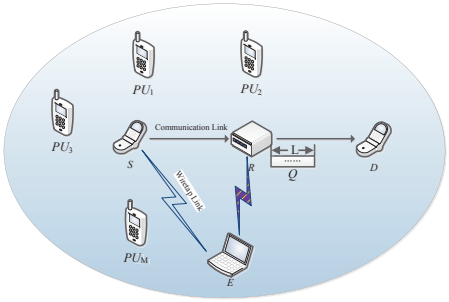

Fig. 1. System Model: A secondary source (S) communicates with its corresponding receiver secondary destination (D) via a buffer-aided relay (R), the transmission information can be intercepted by the eavesdropper (E).

link exist between S and D due to severe path loss or shadowing effects, the data packets in the buffer obey the "first-in-first-out" (FIFO) rule. There are M primary users and an active eavesdropper locate in the transmission range of both S and R, eavesdropper aims to wiretap the confidential messages of the secondary users. All nodes have a single antenna and operate in time slot mode. All channels suffer from additive white Gaussian noise (AWGN), they are assumed to be independent and quasi-static Rayleigh fading so that the channel coefficients remain unchanged during one packet duration but independently vary from one packet time to another, we denote h_{ab} as the channel power gains of the link $a \to b$, here $a \in (S, R)$ and $b \in (R, E, PU_k, D)$, and h_{ab} being exponential random variables (RVs) with parameter λ_{ab}, and $\lambda_{ab} = 1/\Omega_{ab}$, $\Omega_{SR} = \Omega_{RD}$, $\Omega_{SP_k} = \Omega_{RP_k}$ $(1 \le k \le M)$, $\Omega_{SE} = \Omega_{RE}$. We have assumed eavesdropper is the active node, such that exact knowledge of all channels including the eavesdropping channels are available. Each time slot can be dynamically allocated to either relay reception if $S - R$ link is selected, or destination reception if $R - D$ link is selected. It is easy to follow that if buffer is not full, the $S - R$ link is available, and if the buffer is not empty, the $R - D$ link is available. At the beginning of transmission process, the buffer is empty, the states transition can be categorized as follows: 1) the number of packets in the buffer can increase by one if $S - R$ link is the selected link meanwhile the instantaneous secrecy capacity is higher than R_s; 2) the number of packets in the buffer will decrease by one if $R - D$ link is the selected link and the instantaneous secrecy capacity is higher than R_s; 3) The number of packets in the buffer remains unchanged if the instantaneous secrecy capacity is higher than R_s, in respect that an outage event has occurred in the selected link.

For description convenience, in the sequel of this section, we denote $X - Y$ link as the selected link, with $X \in \{S, R\}$, $Y \in \{R, D\}$, which includes two cases: 1) if $S - R$ link is selected, X and Y represent S and R, respectively, and R is selected to receive data; 2) if $R - D$ link is selected, X and Y represent R and D, respectively, and R is selected to transmit data.

Considering the underlay working mode of CRNs, the transmit power of the S and R must be adjusted to satisfy the QoS requirement of PUs, moreover, the transmit power of S and R must be kept below their allowable maximum power $P_{\max}$. such that they can be expressed as

$$P_{X_T} = \min(P_{\max}, {}^{P_{th}}/_{\gamma_{XP}}) = P_{\max} \min(1, {}^{\mu}/_{\gamma_{XP}}) \quad (1)$$

where $P_{\max}$ is the allowable power of X, with $X \in \{S, R\}$, and P_{th} is the predefined interference power threshold at the PU_k, $\gamma_{XP} = \max(h_{XP_k})$, $1 \le k \le M$, h_{XP_k} is channel gain between X and PU_k, $\mu = P_{th}/P_{\max}$ is a positive constant.

We denote $x(t)$ as the data packet transmitted to Y at time t, the received signal at the Y and E are given as

$$y_{xy}(t) = \sqrt{P_{X_T}} h_{xy}(t) \cdot x(t) + n_y(t) \quad (2)$$

$$y_{xe}(t) = \sqrt{P_{X_T}} h_{xe}(t) \cdot x(t) + n_e(t) \quad (3)$$

where, $n_y(t)$ and $n_e(t)$ are the noise at corresponding receiver and eavesdropper, respectively. For notational convenience, the time index t is ignored below unless necessary. If $S - R$ link is selected to receive the data, $y_{sr}(t)$ is the received signal of the relay, which will be decoded firstly and then stored into relay's buffer and wait for its turn to be transmitted.

Based on the above analysis, the signal-to-noise ratio of $X - Y$ link can be expressed as

$$\Psi_{XY} = \frac{P_{X_T} h_{XY}}{N_0} = Q_T \min(1, {}^{\mu}/_{\gamma_{XP}}) h_{XY} \quad (4)$$

where N_0 is power of the additive noise at node Y, $Q_T = P_{max}/N_0$, and the instantaneous secrecy rate of the $X - Y$ link can be given as

$$C_{X,Y}^{\text{secrecy}} = [C_M - C_E]^+ \quad (5)$$

where $(x)^+ = \max(x, 0)$, C_M and C_E are the achievable instantaneous rate for $X \to Y$ link and $X \to E$ link, they can expressed as

$$C_M = \frac{1}{2} \log_2(1 + Q_T \min(1, \frac{\mu}{\gamma_{xp}}) h_{xy}) \quad (6)$$

$$C_E = \frac{1}{2} \log_2(1 + Q_T \min(1, \frac{\mu}{\gamma_{xp}}) h_{xe}) \quad (7)$$

Similar to the existing works[3∼5], the SOP expressions can be formulated as

$$P_{\text{out}}(Rs) = Pr\left(C_{X,Y}^{\text{secrecy}} \le Rs\right) \quad (8)$$

Remark. Here, instantaneous channel capacity of the selected link is used as a measurement for investigating the channel quality and deriving the secrecy outage probabilities, which has been widely used in previous works [9],[11].

3. COGNITIVE SECURE LINK SELECTION SCHEME

Cognitive secure link selection scheme is proposed by selecting the link that can maximize the signal to eavesdropper channel secrecy rate among available $S \rightarrow R$ and $R \rightarrow D$ links, meanwhile satisfying the QoS requirement of PU, the proposed link selection scheme can be expressed as

$$\mathcal{L} = \arg\max \left\{ \begin{array}{c} \bigcup\limits_{\Psi(Q)\neq L} \frac{1+Q_T \min(1,{}^{\mu}/_{\gamma_{SP}})h_{SR}}{1+Q_T \min(1,{}^{\mu}/_{\gamma_{SP}})h_{SE}}, \\ \bigcup\limits_{\Psi(Q)\neq 0} \frac{1+Q_T \min(1,{}^{\mu}/_{\gamma_{RP}})h_{RD}}{1+Q_T \min(1,{}^{\mu}/_{\gamma_{RP}})h_{RE}} \end{array} \right\} \quad (9)$$

$\mathcal{L}$ denotes the selected link among the available links, $\Psi(Q)$ denotes the number of packets in the relay's buffer. According to (9), $S-R$ link is available only if $\Psi(Q) \neq L$; $R-D$ link is available only if $\Psi(Q) \neq 0$. where, ρ is a predefined value related with the target secrecy rate R_s, $\rho = 2^{2R_s}$.

Buffer state shows the number of the packets in the buffer, it can be modeled as a Markov chain according to its evolution [12]. We will study the state transition probabilities between different states of buffer in the next subsection, which is also a key point in deriving the closed-form expressions of SOP.

3.1. State Transition Probabilities

We have assumed that R is equipped with a buffer of size L in the system model, hence there are L+1 states in total, s_l is denoted as the buffer state when the number of packets in the buffer is equal to l-1, namely $s_l = l-1$, $(1 \leq l \leq L+1)$. According to property of Markov chain [12], all transition probability values can form a state transition matrix $\mathbf{A}$, which is a square matrix of size $(L+1)*(L+1)$, in which

$$\mathbf{A}_{i,j} = p(s_i \rightarrow s_j) = p(X_{t+1} = s_j \,|X_t = s_i) \quad (10)$$

$$\sum_{i=1}^{L+1} \mathbf{A}_{i,j} = 1 \quad (11)$$

We can find that if the relay's buffer is full or empty, there is only one link can be selected. Consequently, the total number of available links D_l in the proposed scheme is

$$D_l = \left\{ \begin{array}{ll} 2 & if\ 0 < \Psi(Q) < L \\ 1 & otherwise \end{array} \right. \quad (12)$$

In order to construct the state transition probability matrix, we should first identify the connectivity between the different states of the buffers.Due to the transmission link is symmetrical, to compute the probability that an outage event occurs if the $S \rightarrow R$ link is selected,let $x = h_{sp}$ and $y = h_{se}$, according to (5), the CDF $F_Z(z\,|x,y)$ conditioned on x and y is obtained as

$$F_Z(z\,|x,y) = 1 - \exp(-\frac{\lambda(z-1)}{Q_T \min(1,{}^{\mu}/_{x})} - \lambda z y) \quad (13)$$

Then the CDF $F_Z(z)$ can be computed as

$$F_Z(z) = \int_0^{+\infty} \int_0^{+\infty} F_Z(z\,|x,y) f_{\mathrm{x}}(x) f_y(y) dx dy \quad (14)$$

Where $f_{\mathrm{x}}(x)$ and $f_y(y)$ represent the probability density function (PDF) of the h_{sp} and h_{se}, they can expressed as

$$f_{\mathrm{x}}(x) = \sum_{m=1}^{M} (-1)^{m+1} C_M^m m \lambda_{SP} \exp(-m\lambda_{SP} x) \quad (15)$$

$$f_{\mathrm{y}}(y) = \lambda_{SE} \exp(-\lambda_{SE} y). \quad (16)$$

the probability to have an event and therefore no change in the buffer status can be computed as (17).

Thus, the probability that state of buffer leaves from s_l, p_{D_l} is derived as [13]

$$p_{D_l} \triangleq \frac{1}{D_l}[1 - P_{out}(\rho)^{D_l}] \quad (18)$$

$$\overline{p_{D_l}} \triangleq 1 - \sum_{i=1}^{D_l} p_{D_l} \quad (19)$$

where, $\overline{p_{D_l}}$ represent the probability that the buffer state remains unchanged, correspondingly.

3.2. Secrecy Outage Probability Analysis

Based on the fact that the state transition of the buffer can be modeled as a Markov chain, theoretical framework we adopt here is similar to [9]. We denote U_j as the set of states that connect to state s_j but except for s_j. According to the transmission protocol we have described in the section 2 and the state transition rules we have defined, there are three cases in total for the evolution of the s_j: 1) if an outage event occurs in the selected link, s_j can move to itself, which is also included in the set U_j, in which, the transition probability can be given as $\overline{p_{D_j}}$; 2) if s_j can move to another different state in the U_j in one step, the transition probability can be given as p_{D_j}; 3) the state transition probability equals to zero if another state that s_j can move to in two or more steps. In summary, the transition probability can also be expressed as

$$\mathbf{A}_{i,j} = \left\{ \begin{array}{ll} \overline{p_{D_l}} & if\ s_j \notin U_j \\ p_{D_l} & if\ s_j \in U_j \\ 0 & otherwise \end{array} \right. \quad for\ i,j \in \{1,\cdots,L+1\} \quad (20)$$

The transition matrix $\mathbf{A}$ is column stochastic, irreducible and aperiodic[11], therefore, the stationary state probability vector is obtained as

$$\pi = (\mathbf{A} - \mathbf{I} + \mathbf{B})^{-1}\mathbf{b} \quad (21)$$

here $\pi = [\pi_1, \cdots, \pi_{L+1}]$ is the stationary distribution.

$$\mathbf{b} = [1,1,\cdots,1]^T, \mathbf{B}_{i,j} = 1, \forall i,j \quad (22)$$

$$P_{out}(R_s)=F_Z(z)\,|_{z=2^{2R_s}} = 1-\sum_{m=1}^{M}(-1)^{m+1}\binom{M}{m}\frac{\lambda_{SE}}{\lambda_{SR}2^{2R_s}+\lambda_{SE}}\exp(-\frac{\lambda_{SR}(2^{2R_s}-1)}{Q_T})\left[1-\exp(-m\lambda_{SP}\mu)\right] - \sum_{m=1}^{M}(-1)^{m+1}\binom{M}{m} m\lambda_{SP}\frac{\lambda_{SE}}{\lambda_{SR}2^{2R_s}+\lambda_{SE}}\frac{Q_T\mu}{m\lambda_{SP}Q_T\mu+\lambda_{SR}(2^{2R_s}-1)}\exp\left[-\frac{m\lambda_{SP}Q_T\mu+\lambda_{SR}(2^{2R_s}-1)}{Q_T\mu}\mu\right] \quad (17)$$

Finally, according to (20), (21) and (22), we can easily reformat the secrecy outage probability as[12]

$$P_{out}(R_s)=\sum_{i=1}^{L+1}\pi_i\overline{p_{Dl}}=\mathrm{diag}(\mathbf{A})\pi \quad (23)$$

where $\mathrm{diag}(\mathbf{A})$ is a vector consisting of all diagonal elements of $\mathbf{A}$.

4. RESULTS AND ANALYSIS

We have given system and channel model in section 2, here we will simulate the secrecy outage performance of proposed scheme in DF buffer-aided cognitive relay network, the conventional cooperative selection scheme without buffer is used as reference scheme, channel parameter of wiretap channel are set as $\Omega_{SE}=\Omega_{RE}=5$, $\Omega_{SP_i}=\Omega_{RP_i}=5dB$, the target secrecy rate of the system is set as R_s bits per channel use (BPCU), the number of primary users, M=6, the theoretical results are all based on (17), and simulation results are obtained by averaging 10^7 independent runs, which verifies the close-form expression of SOP obtained in this paper.

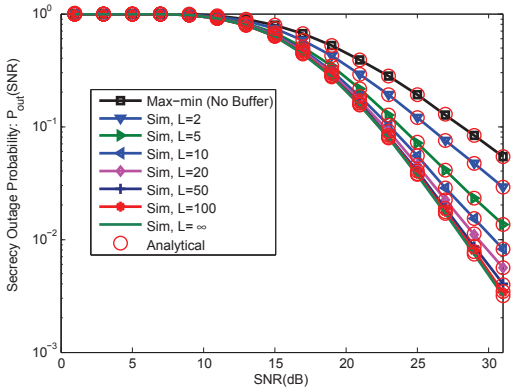

Fig. 2. P_{out} versus SNRs of communication link under different buffer length, L=[2,10,20,50,100,∞].P_{th}=5 dB

Fig. 2 compares the SOP of the proposed secure link selection scheme under different SNRs of signal link with the conventional max-min relay selection scheme has no buffer. We can find that the theoretical curves match precisely with the Monte Carlo simulation results, which validates the accuracy of our analysis. the results also show that the SOP can decrease apparently with the SNR of the signal link increase.

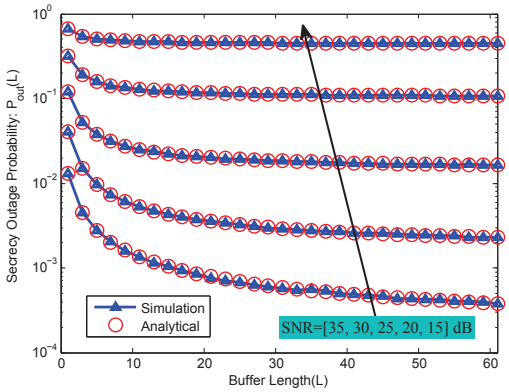

Fig. 3. P_{out} verus buffer size L under signal link SNR, SNR =[15,20,25,30,35]dB.

In Fig. 3, SOP of the proposed scheme versus the buffer size is provided. As can be seen, if the buffer size is increased, the SOP can be improved, and then converge to a relatively fixed value, and a small size of the buffer is sufficient (e.g.,L=10 for SNR=20 dB). We can also see from Fig. 3 that if we increase SNR of signal link, the required value of the buffer size is increased (e.g.,L=10 for SNR=20 dB and L=30 for SNR=25 dB).

5. CONCLUSIONS

In this paper, we investigated the secure performance of max-ratio secure link selection scheme for DF cooperative cognitive radio networks with finite buffers. Unlike conventional relay selection scheme, the proposed secure link selection scheme exploits the buffering capability of the relay, and schedules transmission only through the optimal available channel link. New closed-form expressions for secrecy outage probability was derived, and investigate the various parameters on the secure performance. Numerous results shown that the proposed scheme can significantly improve the secure performance and provide an attractive secrecy transmission method for cognitive radio networks.

6. REFERENCES

[1] J. Mitola and G. Q. Maguire, "Cognitive radio: making software radios more personal," *IEEE Personal Commun.*, vol. 6, pp. 13–18, 1999.

[2] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Communications Surveys & Tutorials*, vol.17, no.2, pp.1023-1043, 2015.

[3] M. Bloch and J. Barros, "Physical-Layer Security," *Cambridge University Press*, 2011.

[4] D Lun, H Zhu, A P Petropulu, and H V Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875-1888, 2010.

[5] J. Li, A. P. Petropulu, and S. Weber, "On Cooperative Relaying Schemes for Wireless Physical Layer Security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985-4997, 2011.

[6] N. Zlatanov, A. Ikhlef, T. Islam, and R. Schober, "Buffer-aided cooperative communications: opportunities and challenges," *IEEE Commun. Mag.*, vol. 52, no. 4, pp. 146-153, 2014.

[7] X. Bing, F. Yijia, J. Thompson, and H. V. Poor, "Buffering in a Three-Node Relay Network," *IEEE Trans. Wireless Commun.*, vol. 7, no. 11, pp. 4492-4496, 2008.

[8] A. Ikhlef, D. S. Michalopoulos, R. Schober, "Max-Max Relay Selection for Relays with Buffers," *IEEE Trans. Veh. Tech.*, vol. 11, no. 3, pp. 1124–1135, 2012.

[9] I. Krikidis, T. Charalambous, and J. S. Thompson, "Buffer-Aided Relay Selection for Cooperative Diversity Systems without Delay Constraints," *IEEE Trans. Wireless Commun.*, vol. 11, no. 5, pp. 1957-1967, 2012.

[10] G. Chen, Z. Tian, Y. Gong, J. Chambers, "Max-Ratio Relay Selection in Secure Buffer-Aided Cooperative Wireless Networks," *IEEE Trans. Inf. Forensics Security.*, vol. 9, no. 4, pp. 719–729, 2014.

[11] G. Chen, Z. Tian, Y. Gong, J. Chambers, "Decode-and-Forward Buffer-Aided Relay Selection in Cognitive Relay Networks," *IEEE Trans. Veh. Tech.*, vol. 63, no. 9, pp. 4723–4728, 2014.

[12] J. R. Norris, Markov Chains, *Cambridge University Press*, 1998.

[13] C. M. Grinstead and J. L. Snell, Introduction to Probability, 2ed. Providence, RI, USA: Amer. Math. Soc., 1991.