Physical Layer Security of Outdated CSI Based CRN

Sukannya Chetry
Department of Electronics & Communication Engineering,
M.B.M Engineering college, JNVU, Jodhpur,
Rajasthan, India.
Email: sukannya92@gmail.com

Ajay Singh
Department of Electrical Engineering,
Indian Institute of Technology Jammu,
Jammu & Kashmir, India.
Email: ajay.singh@iitjammu.ac.in

Abstract— **In this paper, an underlay spectrum sharing based cognitive wiretap channel with multiple primary users is considered. The secondary user transmitter communicates with a secondary user receiver in the presence of multiple eavesdroppers. The secondary transmitter is assumed to have multiple antennas and the secondary receiver and eavesdroppers are equipped with single antenna each. The eavesdroppers channel state information (CSI) is found to be outdated in our case. For the coordinated eavesdropping, we have derived the exact and asymptotic closed form expression for the secrecy outage probability.**

Keywords—Cognitive radio, secrecy capacity, primary user, wiretap channel

I. INTRODUCTION

Cognitive Radio (CR) is an emerging technology to eliminate the scarcity and underutilization of radio spectrum. Gastpar [1]states that the same frequency band is shared by multiple independent networks but are disjoint spatially. So coexistence is granted and capacity problem is partially solved by spatial spectrum sharing where unlicensed users are granted permission to access a licensed user's frequency band via spatial interference power restrictions implemented at network level.

Goldsmith *et al* [2] stated that CR has immense potential to enhance the spectral efficiency of wireless systems. In a CR Network (CRN), the spectrum sharing approaches are generally classified as underlay and overlay. Underlay CRN allows an unlicensed secondary user (SU) to occupy the same spectrum as the licensed primary user (PU) by keeping its induced interference under a certain threshold to avoid interrupting the primary transmission. In the overlay approach, the SU detects the PU's idle spectrum for its transmission and hence no interference is induced on the PU.

This work was supported in part by SERB, DST, Government of India, for the Project "Physical Layer Security of Cognitive Radio Networks." (Project Ref. no. : YSS/2015/001738)

Shiang *et al* [3] proposed a distributed resource management algorithm which allowed information exchange between network nodes in a multi-hop CRN. Based on the information exchanged, SU learns about the spectrum opportunities and dynamically exploits available frequency channels, thus improving the spectral efficiency.

According to recent research, the wireless networks have become more and more vulnerable to serious security attacks. Mukherjee *et al* [4] studied methods to reduce the likelihood of message interpretation by an undetected eavesdropper that is being transmitted between two multi-antenna nodes. Robust beam forming approach was proposed to enhance the secrecy in communication in this outdated channel state information (CSI) based wireless network. Huang *et al* [5] proposed cooperative jamming strategy with both perfect and imperfect (outdated) CSI of eavesdropper in a two-hop relay network, where eavesdropper tries to wiretap information in both the hops.

One of the most important requirements in wireless communication is the security, and this holds true for CRN as well. So, recently, the physical layer security of CRN has become a serious cause of concern. The security of cognitive radio networks in particular is critical because these networks are prone to security threats of eavesdropping, and are liable to external threats easily.

Pei *et al* [6] characterized the secrecy capacity by addressing the physical layer security issue of a SU from an information theoretic perspective in a spectrum sharing CRN. And in [7], they addressed the robust transmitter design with or without perfect CSI for secure CRN. Wu *et al* [8] modeled cooperative transmission paradigm in a CRN that helps PU to interact with trustworthy SUs in order to improve secrecy in the presence of a passive eavesdropper, which attempts to intercept and decode PU's messages. Jeon *et al* [9] applied information theoretic secrecy to CR scenario consisting of untrusted SU which tries to eavesdrop PU's messages, and proposed secure cooperative transmission scheme that allowed SU to sense and relay PU's spectrum but make them unaware of the PU's messages. Zhang *et al* [10] optimized the Cognitive relay beam-forming system's performance while keeping PU interference constraint and transmitted messages secret from the eavesdropper. Sakran *et al*[11] considered secrecy constrained CRN and proposed relay selection scheme to

maximize the achievable secrecy rate by enhancing the physical layer security of the network. Elkashan *et al* [12] worked on the physical layer security of multi antenna transmitter based cognitive wiretap channel with underlay spectrum sharing and passive eavesdropping under interference power constraint at PU.

Yang *et al* [13]proposed a practical protocol of transmit antenna selection (TAS) to enhance the physical layer security in multiple-input-multiple-output (MIMO) wiretap channels. TAS is an essential part of future wireless systems to reduce the complexity of multiple antenna techniques and to satisfy the need of higher data rates. This antenna selection technique maximizes the signal-to-noise ratio (SNR) at the legitimate receiver, which helps to improve secrecy in communication.

Bloch *et al* [14] developed practical protocol to ensure wireless information theoretic security while transmitting confidential messages over wireless channels. Oggier *et al* [15] determined the perfect secrecy capacity of a multi-antenna MIMO wiretap channel considering perfect CSI of the eavesdropper, with arbitrary number of antennas at the transmitter, receiver and eavesdropper.

Lei *et al* [16] analyzed the physical layer security of MIMO cognitive wiretap channel over Nakagami-m fading and investigated the secrecy outage performance.

Pan *et al* [17] revealed the impact of imperfect CSI on the secrecy performance of MISO simultaneous wireless information and power transfer system consisting of a multi-antenna transmitter, single antenna receiver and multiple single antenna eavesdroppers, by adopting TAS at the transmitting end in the presence of multiple wiretap channels.

II. SYSTEM MODEL

The cognitive wiretap channel consists of Tx Alice equipped with N_A number of antennas, Rx Bob equipped with single antenna and N_E number of eavesdroppers, each equipped with a single antenna respectively. Underlay spectrum sharing with N PUs allow the PUs and SU to transmit in the same spectrum band concurrently. It is assumed that the main channel between Alice and Bob undergo independent and identically distributed Rayleigh fading, while the channels between Alice and Eves experience independent but not necessarily identical Rayleigh fading. Alice encodes her messages and communicates the code words to Bob at a constant code rate R_s [14], following the wiretap channel in [14] and [15]. Eavesdroppers try to overhear the communication between Alice and Bob either by uncoordinated approach or by coordinated approach. In this system model, the case of imperfect CSI is taken into consideration, where the SU Tx does not have information about any of the eavesdropper's channel. For secure transmission, the quality of the channel between Alice and Bob must be better than that of each channel between Alice and Eves. It is assumed that the main channel (between Alice and Bob) and the entire eavesdropper's channel (between Alice and each Eve) are independent of one another. Using TAS, Bob feeds back the CSI of the links between each antenna of Alice and Bob. Then by comparing the received signal strength over the channel between each transmitting antenna and itself, Bob feeds back the index of the strongest transmitting antenna to Alice. The selected antenna using TAS maximizes the instantaneous SNR between Alice and Bob. This protocol being independent of Eve's channel may not maximize their SNR. This boosts the achievable secrecy performance in the system. The channel gains of main channel, eavesdropper's channel and primary

channel are $\{h_{1i}\}$, $\{h_{2j}\}$ and $\{h_{0n}\}$, where $i = 1, 2,\ldots, N_A$, $j = 1, 2,\ldots, N_E$ and $n = 1, 2,\ldots,N$ respectively. The channel gains are complex Gaussian random variables (RVs) with zero mean and variances Ω_1, Ω_2, and Ω_0, respectively.

The channel gains of main channel, eavesdropper's channel and primary channel are $\{h_{1i}\}$, $\{h_{2j}\}$ and $\{h_{0n}\}$, where $i=1,2,\ldots,N_A$, $j = 1,2,\ldots,N_E$ and $n = 1, 2,\ldots,N$ respectively. The channel gains are complex Gaussian random variables (RVs) with zero mean and variances Ω_1, Ω_2, and Ω_0, respectively.

In underlay Cognitive radio network model, one of the most important performance metric is the instantaneous SNR of the main channel and the eavesdropper's channel. For both perfect and imperfect CSI case of eavesdroppers, the instantaneous SNR of main channel is given as,

$$\gamma_M = \max_{i=1,\ldots,N_B} \frac{P_A}{N_0} |h_{1i}|^2 \tag{1}$$

The instantaneous SNR of Eavesdropper's channel incase perfect CSI is known is given as,

$$\gamma_E = \max_{j=1,\ldots,N_E} \frac{P_A}{N_0} |h_{2j}|^2 \tag{2}$$

where, P_A = Transmit power at Alice
N_o = Noise variance

In the underlay CR transmission, the transmit power of Alice is managed under a peak interference power threshold of PU so that the communication at the PUs is not interfered. So, the transmit power of Alice is given by,

$$P_A = \min\left(\frac{Ip}{\max_{n=1,2,\ldots,N} |h_{0n}|^2}, P_t \right) \tag{3}$$

where, P_t represents the maximum transmission power at Alice, Ip represents the peak interference power at the PUs, and h_{0n} is the complex fading coefficient of the primary channel from the nth PU to Alice.

Taking this power constraint into consideration, the instantaneous SNR at Bob and Eve in (1) and (2) can be rewritten as,

$$\gamma_M = \min\left(\frac{\gamma_p}{X}, \gamma_0\right) \gamma_M \tag{4}$$

$$\gamma_E = \min\left(\frac{\gamma_p}{X}, \gamma_0\right) Y_E \tag{5}$$

where, $\gamma_p = I_p/N_0$, $\gamma_0 = P_t/N_0$, $X = \max_{n=1,2,\ldots N} |h_{0n}|^2$, $Y_M = \max_{i=1,\ldots,NA} |h_{1i}|^2$ and $Y_E = \max_{j=1,\ldots,NE} |h_{2j}|^2$.

In this system model, it is considered that the CSI of eavesdropper is not known, i. e., it is a case of imperfect or outdated CSI. For this case, the largest channel gain of the main channel between the selected transmitting antenna at Alice and Bob during selection is taken into consideration which can be expressed from [17] as,

$$h_1^{'} = \max_{i\in\{1,\ldots,N_A\}} \{h_{1i}^{'}\} \tag{6}$$

where h_{1i}' is the delayed channel coefficient between Alice's i^{th} antenna and Bob, which is different from the actual channel coefficient between Alice's i^{th} antenna and Bob denoted as h_{1i}. The correlation relationship between h_{1i}' and h_{1i} can be modelled as,

$$h_{1i}^{'} = \sqrt{\eta} h_{1i} + \sqrt{(1-\eta)} w_i \tag{7}$$

where, w_i represents a complex Gaussian variable with zero mean and variance Ω_w same as h_{1i} ,i.e., Ω_1 and η is the parameter which gives an estimation about the CSI of the eavesdropper. When η =1, then it is the case of perfect CSI as considered in the previous chapter.

After selecting antenna, Alice transmits information to Bob and the Eavesdroppers. Being malicious and in the coverage range, Eves try to get the information intended for Bob.

Taking the power constraint of underlay CRN as in equation (3) into consideration, the instantaneous SNR at Bob in this scenario remains the same as (4), whereas based on the type of eavesdropping, the instantaneous SNR at Eve varies.

III. SECRECY OUTAGE FOR COORDINATED EAVESDROPPING

For coordinated eavesdropping in outdated or imperfect CSI case, the SNR of all the channels of eavesdroppers sum up and this results in an increase in Eve's SNR.

In a CR network, the secrecy capacity can be defined as,

$$C_S = \begin{cases} C_M - C_E & \text{if } \gamma_M > \gamma_E \\ 0 & \text{if } \gamma_M \le \gamma_E \end{cases} \tag{8}$$

where, $C_M = \log_2(1+\gamma_M)$ is the capacity of the main channel and, $C_E = \log_2(1+\gamma_E)$ is the capacity of the eavesdropper's channel. If $R_s < C_s$, perfect secrecy is achieved or else, information theoretic security is jeopardized.

The secrecy outage probability is the probability that the secrecy rate, C_s falls below R_s, and is expressed as,

$$P_{out} = \Pr(C_s < R_s) = \Pr(\gamma_M \le \gamma_E) + \Pr(\gamma_M > \gamma_E)\Pr(C_s < R_s | \gamma_M > \gamma_E) \tag{9}$$

Using [12], (9) can be simplified to,

$$P_{out} = \int_0^{\infty}\int_0^{\infty} F_{\gamma_M|\{X=x\}}(\epsilon(\gamma_E)) f_{\gamma_E|\{X=x\}}(\gamma_E) f_X(x) d\gamma_E dx \tag{10}$$

where, $\gamma_M < 2^{R_S}(1+\gamma_E) - 1 = \epsilon(\gamma_E)$.

$F_{\gamma M}(.)$ is the CDF of γ_M conditioned on X i.e. PU channel gain.
$f_{\gamma E}(.)$ is the PDF of γ_E conditioned on X.
$f_X(x)$ is the PDF of X.

Let $\gamma_1 = \gamma_0\Omega_1 = \gamma_p\Omega_{1/\sigma}$ and $\gamma_2 = \gamma_0\Omega_2 = \gamma_p\Omega_{2/\sigma}$ where, $\sigma = \gamma_p/\gamma_0$. Here, γ_1 denotes the maximum possible average SNR of the main channel and γ_2 denotes the maximum possible average SNR of the eavesdropper's channel.

The secrecy outage probability in (10) can be calculated as,

$$P_{out} = \int_0^{\frac{\gamma_p}{\gamma_0}}\int_0^{\infty} F_{\gamma_M|\{X=x\}}(\epsilon(\gamma_E)) f_{\gamma_E|\{X=x\}}(\gamma_E) f_X(x) d\gamma_E dx + \int_{\frac{\gamma_p}{\gamma_0}}^{\infty}\int_0^{\infty} F_{\gamma_M|\{X=x\}}(\epsilon(\gamma_E)) f_{\gamma_E|\{X=x\}}(\gamma_E) f_X(x) d\gamma_E dx$$

$$P_{out} = J1 + J2 \tag{11}$$

where,

$$J_1 = \int_0^{\frac{\gamma_p}{\gamma_0}}\int_0^{\infty} F_{\gamma_M|\{X=x\}}(\epsilon(\gamma_E)) f_{\gamma_E|\{X=x\}}(\gamma_E) f_X(x) d\gamma_E dx \tag{12}$$

$$J_2 = \int_{\frac{\gamma_p}{\gamma_0}}^{\infty}\int_0^{\infty} F_{\gamma_M|\{X=x\}}(\epsilon(\gamma_E)) f_{\gamma_E|\{X=x\}}(\gamma_E) f_X(x) d\gamma_E dx \tag{13}$$

The PDF of X can be written from [12] as,

$$f_X(x) = \sum_{k=0}^{N-1} \binom{N-1}{k} (-1)^k \frac{N}{\Omega_0} e^{-\frac{(k+1)x}{\Omega_0}} \tag{14}$$

The instantaneous SNR of eavesdropper's channel for coordinated eavesdropping in case of imperfect CSI can be expressed as,

$$\gamma_E = n(X) \sum_{j=1}^{N_E} |h_{2j}|^2 \tag{15}$$

where, $n(X) = \min((\gamma_p/X), \gamma_0)$.

Exact Secrecy Outage Probability

According to TAS criterion from [16], only the best transmit antenna out of N_A will be selected for transmission to the destination.

For the coordinated eavesdropping scenario, variation is in the SNR of eavesdropper's channel. While the PDF of γ_E conditioned on X can be expressed as,

$$f_{\gamma_E|\{X=x\}}(\gamma_E) = \left(\frac{1}{n(X)\Omega_2}\right)^{N_E} \frac{{\gamma_E}^{N_E-1}}{(N_E-1)!} e^{-\frac{\gamma_E}{n(X)\Omega_2}} \tag{16}$$

Hence, the closed form expression for the exact SOP can be expressed as,

$$P_{out} = N_A \sum_{i=0}^{N_A-1} \sum_{k=0}^{N-1} \binom{N_A-1}{i} \binom{N-1}{k} \frac{(-1)^{i+k} N}{(i+1)(k+1)} \left(1 - \frac{e^{-L(2^{R_s}-1)}}{(L2^{R_s}\gamma_2+1)^{N_E}}\right)$$
$$\times \left\{1 - e^{-\frac{(k+1)\sigma}{\Omega_0}} \left(1 - \left(\frac{M(2^{R_s}-1)\Omega_0}{k+1} + 1\right)^{-1}\right)\right\} \tag{17}$$

Where,

$$M = \frac{(i+1)}{[\eta\gamma_1\sigma + (1-\eta)\gamma_p\Omega_w](1+(1-\eta)i)}$$
$$L = \sigma M$$

Asymptotic Secrecy Outage Probability

The closed form expression for the asymptotic SOP can be expressed as,

$$P_{out} = N_A \sum_{i=0}^{N_A-1} \sum_{k=0}^{N-1} \binom{N_A-1}{i} \binom{N-1}{k} (-1)^{i+k} NQ$$
$$\times \left\{\frac{\sigma}{(k+1)} \left(1 - e^{-\frac{(k+1)\sigma}{\Omega_0}}\right) (2^{R_s}(1+\gamma_2 N_E) - 1)\right.$$
$$\left. + \left[\frac{(2^{R_s}-1)e^{-\frac{(k+1)\sigma}{\Omega_0}}}{(k+1)} + \frac{2^{R_s}\sigma\gamma_2 N_E}{\Omega_0} \Gamma\left(0, \frac{(k+1)\sigma}{\Omega_0}\right)\right]\right\} \tag{18}$$

where,

$$Q = \frac{1}{[\eta\gamma_1\sigma + (1-\eta)\gamma_p\Omega_w](1+(1-\eta)i)} \tag{19}$$

IV. NUMERICAL RESULTS

In this section, the numerical results are given for the verification of the proposed analytical model for imperfect CSI scenario. The exact curves are shown for the given model. The parameters used for analysis are assumed to be unity variance $\Omega_0 = \Omega_1 = \Omega_w = 1$, expected secrecy rate $R_s = 0.1$ bits/s/Hz, $\sigma = 0.5$, number of antennas at Alice $N_A = 4$, number of eavesdroppers $N_E = 4$, number of PUs $N = 4$and $\gamma_2 = 10$ dB.

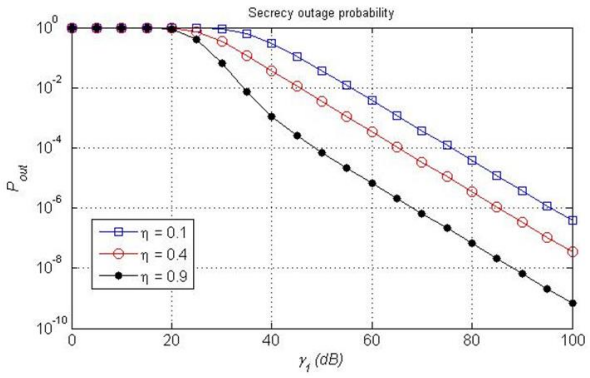

Figure 1

Figure 1 shows the exact SOP plot for coordinated eavesdropping with outdated or imperfect CSI scenario, with γ_1 on the abscissa and SOP on the ordinate for different values of η. It is observed that as η increases, the exact SOP of the system decreases which means that as the CSI of the eavesdroppers tend to be perfect the system's performance improves.

Figure 2 shows the asymptotic SOP plot for coordinated eavesdropping with imperfect CSI scenario, with γ1 on the abscissa and SOP on the ordinate for different values of η. It is observed that as η increases, the asymptotic SOP of the system decreases which means that secrecy performance of the system improves as the CSI of the eavesdroppers tend to be perfect. Hence the closed form expressions deduced accurately analyses the security of the system. Also, for increasing value of η, there is improvement in the secrecy performance of the system model considered which means the system performs better as the CSI of the eavesdroppers at the Tx tends to be perfect.

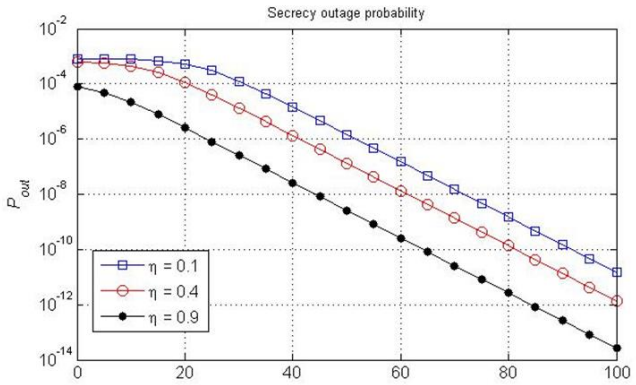

Figure 2

V. CONCLUSION

The secrecy performance of underlay wiretap CRN with multiple PUs and eavesdroppers implementing TAS on the transmitting end is analyzed for outdated CSI scenario of eavesdroppers. The performance metric used for this analysis is the SOP of the system models formulated. The closed form expressions for exact as well as asymptotic SOP are derived and the results are studied. It is observed that as the CSI of eavesdroppers approaches to be perfect, the system's secrecy performance gets better.

REFERENCES

[1] M. Gastpar, "On capacity under receive and spatial spectrum-sharing constraints," *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 471–487, 2007.

[2] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with Cognitive Radios : An Information Theoretic Perspective," vol. 97, no. 5, 2009.

[3] H. Shiang, M. Van Der Schaar, and S. Member, "Distributed Resource Management in Multihop Cognitive Radio Networks for Delay-Sensitive Transmission," vol. 58, no. 2, pp. 941–953, 2009.

[4] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, 2011.

[5] J. Huang and A. L. Swindlehurst, "Cooperative Jamming for Secure Communications in MIMO Relay Networks," vol. 59, no. 10, pp. 4871–4884, 2011.

[6] Y. Pei, Y. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure Communication over MISO Cognitive Radio Channels," vol. 9, no. 4, pp. 1494–1502, 2010.

[7] Y. Pei, Y. C. Liang, K. C. Teh, and K. H. Li, "Secure Communication in Multiantenna Cognitive Radio Networks With Imperfect Channel State Information," *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1683–1693, 2011.

[8] Y. Wu and K. J. R. Liu, "An Information Secrecy Game in Cognitive Radio Networks," vol. 6, no. 3, pp. 831–842, 2011.

[9] H. Jeon, S. W. Mclaughlin, and J. Ha, "Secure Communications with Untrusted Secondary Users in Cognitive Radio Networks," pp. 1072–1078, 2012.

[10] J. Zhang and M. C. Gursoy, "Secure relay beamforming over cognitive radio channels," *2011 45th Annu. Conf. Inf. Sci. Syst. CISS 2011*, no. 1, 2011.

[11] H. Sakran, M. Shokair, O. Nasr, S. El-rabaie, and A. A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," vol. 6, no. September 2011, pp. 2676–2687, 2012.

[12] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the Security of Cognitive Radio Networks," vol. 64, no. 8, pp. 1–15, 2015.

[13] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, 2013.

[14] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. Mclaughlin, "Wireless Information-Theoretic Security," vol. 54, no. 6, pp. 2515–2534, 2008.

[15] F. Oggier and B. Hassibi, "The Secrecy Capacity of The MIMO Wiretap Channel," *Arxiv*, vol. 57, no. 8, p. 24, 2009.

[16] H. Lei *et al.*, "Secrecy Outage Performance of Transmit Antenna Selection for MIMO Underlay Cognitive Radio Systems over Nakagami- m Channels," vol. 9545, no. c, pp. 1–13, 2016.

[17] G. Pan *et al.*, "On Secrecy Performance of MISO SWIPT Systems With TAS and Imperfect CSI," vol. 64, no. 9, pp. 3831–3843, 2016.