On the Security of Cognitive Radio Networks

Maged Elkashlan, *Member, IEEE*,
Lifeng Wang, *Student Member, IEEE*,
Trung Q. Duong, *Senior Member, IEEE*,
George K. Karagiannidis, *Fellow, IEEE*, and
Arumugam Nallanathan, *Senior Member, IEEE*

***Abstract*—Cognitive radio has emerged as an essential recipe for future high-capacity, high-coverage multitier hierarchical networks. Securing data transmission in these networks is of the utmost importance. In this paper, we consider the cognitive wiretap channel and propose multiple antennas to secure the transmission at the physical layer, where the eavesdropper overhears the transmission from the secondary transmitter to the secondary receiver. The secondary receiver and the eavesdropper are equipped with multiple antennas, and passive eavesdropping is considered where the channel state information (CSI) of the eavesdropper's channel is not available at the secondary transmitter. We present new closed-form expressions for the exact and asymptotic secrecy outage probability. Our results reveal the impact of the primary network on the secondary network in the presence of a multiantenna wiretap channel.**

***Index Terms*—Cognitive radio, multiple antennas, physical-layer security, wiretap channel.**

I. Introduction

Future multitier heterogeneous networks have become more and more vulnerable to serious security attacks and security threats of eavesdropping. Due to the distributed nature of the broadcasting channel, security concerns are further escalated to the forefront and have taken on an increasingly important role in spectrum sharing networks. In underlay cognitive spectrum sharing networks, the primary network and the secondary network are allowed to transmit concurrently in the same spectrum [1], [2]. In such complex environments, securing and protecting the broadcast channel against eavesdropping is arguably a more challenging task. In addition, due to the dynamic nature of these environments, higher layer cryptographic authentication and identification have become expensive and vulnerable to attacks [3], [4].

In light of the aforementioned circumstances, there has been intense interest in physical-layer security to secure data transmission without the need for complex cryptographic operations. Physical-layer security is also a solution to support and supplement existing cryptographic protocols [5]. The fundamental principle is to strengthen the main channel of the legitimate receiver relative to the eavesdropper's channel for achieving perfect secrecy. Triggered by the rapid advances in multiantenna techniques for fourth generation and beyond, security enhancement in wiretap channels with multiple antennas has attracted widespread attention (e.g., [6]–[10] and the references therein), where the transmitter, the receiver, and/or the eavesdropper are equipped with multiple antennas. Previous work in [6] considered the single-input multiple-output wiretap channel and derived the secrecy outage probability with maximal ratio combining (MRC) at both the legitimate receiver and the eavesdropper. An extension of [6] to the practical scenario of multiple eavesdroppers was presented in [7]. Transmit antenna selection for security enhancement was introduced in [8] and [9] as a low-complexity cost-effective approach. More recently in [10], the secrecy outage probability was evaluated in the presence of an untrusted relay.

In particular, cognitive radio is envisioned as a promising technique to alleviate the scarcity of radio frequency spectrum, which is the most important radio resource of wireless networks. This can be done by allowing the unlicensed user to occupy the spectrum without causing harmful interference on the licensed user. Security is an important requirement for future fifth-generation systems, and cognitive radio is no exception. In particular, security of cognitive radio networks is critical as it is easily exposed to external threats [11]–[17]. The robust transmitter design via optimization for secure cognitive radio networks with and without perfect channel state information (CSI) was addressed in [11] and [12], respectively. In [13], security for the main channel was guaranteed by performing beamforming from a group of relays. In [14], relay selection was proposed for security constrained cognitive radio with a single eavesdropper. The proposed scheme selects a trusted relay to maximize the achievable secrecy rate subject to interference power constraints at the primary user (PU) under available channel knowledge. In [15], secure communications with untrusted secondary users in cognitive radio networks was proposed, and the achievable secrecy rate was derived. In [16] and [17], game theory was utilized to exploit the security aspect of cognitive radio networks. While the aforementioned laid a solid foundation to understand the role of physical-layer security in cognitive radio networks, the impact of multiantenna wiretap channels on cognitive spectrum sharing networks for passive eavesdropping is less well understood. In contrast to the aforementioned scenarios, we consider the passive eavesdropping scenario, where knowledge of the eavesdropper's channel is not known at the secondary transmitter. In such a scenario, perfect secrecy cannot be achieved, and as such, the secrecy outage probability is an important performance metric used for system evaluation.

In this paper, we take into account the cognitive wiretap channel and determine the necessary conditions to secure the confidential message against eavesdropping. Passive eavesdropping is considered, where the CSI of the eavesdropper's channel is not available at the secondary transmitter. In such a cognitive wiretap channel, the secondary transmitter sends confidential messages to the secondary receiver in the presence of a eavesdropper. With this in mind, the secondary receiver is equipped with multiple antennas to promote secure data transmission without the need for a secret key or code. The eavesdropper is equipped with multiple antennas to promote successful eavesdropping. In this network, the interference power at the PU from the secondary transmitter must not exceed a peak interference power threshold. Our aim is to address fundamental questions surrounding the joint impact of two power constraints on the cognitive wiretap channel: 1) the maximum transmit power at the secondary transmitter and 2) the peak interference power at PU. To address these constraints, we derive new closed-form expressions for the exact and asymptotic secrecy outage probability. Our expressions reveal important design insights into the impact of the primary network on the secondary network in cognitive wiretap radio networks.

Manuscript received August 11, 2013; revised January 5, 2014 and July 7, 2014; accepted September 1, 2014. Date of publication September 17, 2014; date of current version August 11, 2015. This work was supported in part by the Vietnam National Foundation for Science and Technology Development (NAFOSTED) under Grant 102.04-2013.13. The review of this paper was coordinated by Prof. M. C. Gursoy.

M. Elkashlan and L. Wang are with the School of Electronic Engineering and Computer Science, Queen Mary University of London, London E1 4NS, U.K. (e-mail: maged.elkashlan@qmul.ac.uk; lifeng.wang@qmul.ac.uk).

T. Q. Duong is with the Queen's University Belfast, Belfast BT7 1NN, U.K. (e-mail: trung.q.duong@qub.ac.uk).

G. K. Karagiannidis is with the Department of Electrical and Computer Engineering, Khalifa University, P.O. Box: 127788, Abu Dhabi, UAE, and also with the Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, 54 124 Thessaloniki, Greece (e-mail: geokarag@auth.gr).

A. Nallanathan is with the Department of Informatics, King's College London, London WC2R 2LS, U.K. (e-mail: arumugam.nallanathan@kcl.ac.uk).

Digital Object Identifier 10.1109/TVT.2014.2358624

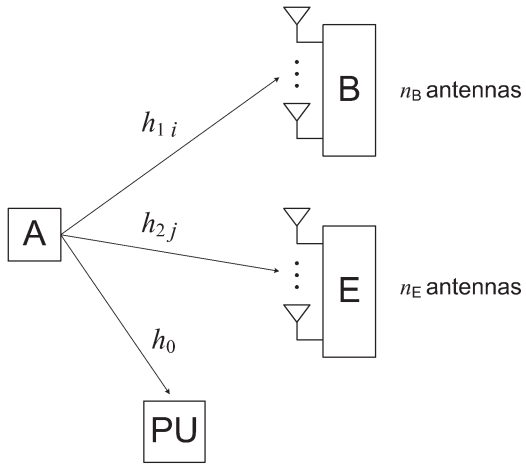

Fig. 1. Cognitive wiretap radio network.

II. System and Channel Models

Consider a cognitive wiretap radio network, where the secondary transmitter Alice (A) communicates with the secondary receiver Bob (B) under the malicious attempt of the eavesdropper Eve (E), as shown in Fig. 1. We assume a cognitive network with underlay spectrum sharing, which allows concurrent transmissions from PU and A in the same spectrum band. For this network, A transmits data to B, where B and E are equipped with multiple antennas n_B and n_E, respectively, whereas A and PU are equipped with a single antenna.

Both the primary channel and the secondary channel are assumed to undergo independent identically distributed (i.i.d.) Rayleigh fading, where the channel gains $\{h_{1i}\}_{i=1}^{n_B}$, $\{h_{2j}\}_{j=1}^{n_E}$, and h_0 are complex Gaussian random variables (RVs) with zero mean and variances Ω_1, Ω_2, and Ω_0, respectively. We also assume that the main channel from A to B and the eavesdropper's channel from A to E are independent of each other. We consider antenna selection[1] at B and E.[2] Here, B and E select their strongest receive antennas based on perfect CSI estimation via pilot signals transmitted by A. Based on this, the instantaneous SNR in the main and the eavesdropper's channel are given by

$$\gamma_M = \max_{i=1,\ldots,n_B} \frac{P_A}{N_0}|h_{1i}|^2, \quad \gamma_E = \max_{j=1,\ldots,n_E} \frac{P_A}{N_0}|h_{2j}|^2 \tag{1}$$

respectively, where P_A is the transmit power at A, and N_0 is the noise variance.

III. Secrecy Outage Probability

We focus on passive eavesdropping, where knowledge of the eavesdropper's channel is not known at A. In such a scenario, A has no choice but to encode the confidential data into codewords of a constant rate R_s [19]. Following the wiretap channel in [19] and [20], A encodes a message block W^k into a codeword X^n, and the eavesdropper receives Y_w^n from the output of its channel. The equivocation rate of Eve is $R_e = H(W^k|Y_w^n)/n$. We assume slow block fading for the main channel and the eavesdropper's channel, where the fading coefficients are constant during a codeword transmission.Taking this into account, we define the secrecy rate as [19]

$$C_s = \begin{cases} C_M - C_E, & \text{if } \gamma_M > \gamma_E \\ 0, & \text{if } \gamma_M \leq \gamma_E \end{cases} \tag{2}$$

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. The secrecy rate C_s in (2) is the maximum achievable perfect secrecy rate R such that $R_e = R$ [19], [20]. In passive eavesdropping, if $R_s \leq C_s$, perfect secrecy is guaranteed. Otherwise, if $R_s > C_s$, information-theoretic security is compromised. As such, the secrecy outage probability is the probability that C_s falls below R_s, i.e.,

$$P_{\text{out}} = \Pr(C_s < R_s) = \Pr(\gamma_M \leq \gamma_E) + \underbrace{\Pr(\gamma_M > \gamma_E)}_{\mathcal{A}} \underbrace{\Pr(C_s < R_s | \gamma_M > \gamma_E)}_{\mathcal{I}}. \tag{3}$$

To evaluate the term $\mathcal{I}$, we first rewrite C_s in (2) as

$$C_s = \log_2\left(\frac{1+\gamma_M}{1+\gamma_E}\right) < R_s \tag{4}$$

which is equivalent to

$$\gamma_M < 2^{R_s}(1+\gamma_E) - 1 = \epsilon(\gamma_E). \tag{5}$$

Then, $\mathcal{I}$ can be written as

$$\mathcal{I} = \frac{1}{\mathcal{A}} \int_0^\infty \int_{\gamma_E}^{\epsilon(\gamma_E)} f_{\gamma_M}(\gamma_M) f_{\gamma_E}(\gamma_E) d\gamma_M d\gamma_E \tag{6}$$

where $f_{\gamma_A}(\cdot)$ is the probability density function (pdf) of γ_A, $\gamma_A \in \{\gamma_M, \gamma_E\}$. By exchanging the variable in the limits of inner integral $\mathcal{I}$, we obtain

$$\mathcal{I} = \frac{\mathcal{I}_1 - \mathcal{I}_2}{\mathcal{A}} \tag{7}$$

where $\mathcal{I}_1$ and $\mathcal{I}_2$ are, respectively, given as

$$\mathcal{I}_1 = \int_0^\infty \int_0^{\epsilon(\gamma_E)} f_{\gamma_M}(\gamma_M) f_{\gamma_E}(\gamma_E) d\gamma_M d\gamma_E \tag{8}$$

$$\mathcal{I}_2 = 1 - \mathcal{A}. \tag{9}$$

Putting together (3) and (7)–(9), we get

$$P_{\text{out}} = \int_0^\infty \int_0^\infty F_{\gamma_{\mathsf{M}}|\{X=x\}}\left(\epsilon(\gamma_{\mathsf{E}})\right) f_{\gamma_{\mathsf{E}}|\{X=x\}}(\gamma_{\mathsf{E}}) f_X(x) d\gamma_{\mathsf{E}} dx \tag{10}$$

where $X = |h_0|^2$ is the channel power gain from A to PU and $F_{\gamma_M}(\cdot)$ is the cumulative distribution function (cdf) of γ_M.

According to underlay cognitive radio transmission, the transmit power at A must be managed under a peak interference power threshold to guarantee reliable communication at PU. With this in mind,

[1] It is well known that using antenna selection can achieve the full diversity gain with fewer RF electronics for each branch compared with MRC [18].

[2] In commercial wireless applications, the eavesdropper may be subject to the same resource constraints as the legitimate receiver. Specifically, it may be limited to a single radio-frequency (RF) chain due to size and complexity limitations, as was considered in [7] and [9].

A is power-limited such that the maximum transmit power is P_t. As such, the transmit power at A is strictly constrained by the maximum transmit power P_t at A and the peak interference power I_p at PU according to

$$P_A = \min\left(\frac{I_p}{|h_0|^2}, P_t\right) \tag{11}$$

from which the instantaneous SNR at Bob and Eve in (1) are reexpressed as

$$\gamma_M = \min\left(\frac{\overline{\gamma}_p}{X}, \overline{\gamma}_0\right) Y_M \quad \gamma_E = \min\left(\frac{\overline{\gamma}_p}{X}, \overline{\gamma}_0\right) Y_E \tag{12}$$

respectively, where $\overline{\gamma}_p = I_p/N_0$, $\overline{\gamma}_0 = P_t/N_0$, $X = |h_0|^2$, $Y_M = \max_{i=1,\ldots,n_B} |h_{1i}|^2$, and $Y_E = \max_{j=1,\ldots,n_E} |h_{2j}|^2$. In the following lemma, we present new exact closed-form statistics of γ_M and γ_E.

Lemma 1: If $Y = \max_{n=1,\ldots,N} Y_n$, where Y_n is i.i.d. exponential RV with parameter Ω_Y, then the cdf and pdf of $\gamma = \min((\overline{\gamma}_p/X), \overline{\gamma}_0)Y$ conditioned on X are

$$F_{\gamma|\{X\}}(\gamma) = \sum_{n=0}^{N} \binom{N}{n} (-1)^n e^{-\frac{n\gamma}{u(X)\Omega_Y}} \tag{13}$$

$$f_{\gamma|\{X\}}(\gamma) = \sum_{n=0}^{N-1} \binom{N-1}{n} \frac{N}{u(X)\Omega_Y} (-1)^n e^{-\frac{(n+1)\gamma}{u(X)\Omega_Y}} \tag{14}$$

where $\sigma = I_p/P_t$.

Proof: See Appendix A. ■

For ease of exposition and mathematical tractability, we denote $\overline{\gamma}_1 = \overline{\gamma}_0\Omega_1 = \overline{\gamma}_p\Omega_1/\sigma$ and $\overline{\gamma}_2 = \overline{\gamma}_0\Omega_2 = \overline{\gamma}_p\Omega_2/\sigma$. Here, $\overline{\gamma}_1$ represents the maximum possible average SNR of the channel between A and B, and $\overline{\gamma}_2$ represents the maximum possible average SNR of the channel between A and E.

A. Exact Secrecy Outage Probability

Based on Lemma 1, we present a novel closed-form expression for the exact secrecy outage probability, as given in the following theorem.

Theorem 1: The exact secrecy outage probability of the proposed cognitive multiantenna wiretap channel is given as follows: where $\mathrm{Ei}(\cdot)$ is the exponential integral function [21, Eq. (8.211.1)]. In (15), shown at the bottom of the page.

$$\mu = \frac{i2^{R_s}}{\overline{\gamma}_1} + \frac{j+1}{\overline{\gamma}_2}$$

$$\beta_1 = \frac{(2^{R_s}-1)}{2^{R_s}} + \frac{\sigma\overline{\gamma}_1}{i2^{R_s}\Omega_0}$$

$$\beta_2 = \frac{\sigma\overline{\gamma}_2}{\Omega_0(j+1)}.$$

Proof: See Appendix B. ■

It is worth noting that (15) involves only finite summations of exponentials, powers, and thus can be calculated in closed form. This expression serves as a prerequisite for other secrecy metrics such as the probability of nonzero secrecy capacity, calculated as $\Pr(C_s > 0) = \Pr(\gamma_M > \gamma_E) = 1 - P_{\mathrm{out}}(0)$. In addition, considering the special case of a single-antenna transmitter and a single-antenna receiver, our secrecy outage probability expression without interference power constraint reduces to [7, Eq. (11)]. Our secrecy outage probability expression without interference power constraint also reduces to [9, Eq. 34] with a single transit antenna in Rayleigh fading.

B. Asymptotic Secrecy Outage Probability

We derive a new asymptotic expression for the secrecy outage probability at high SNR operating regions. The main driver is to identify the key players that control network behavior. The aim is to determine the impact of PU on A in the presence of a multiantenna wiretap channel. In particular, we are interested in the joint impact of the maximum transmit power P_t at A and the peak interference power I_p at PU on the secrecy outage probability. Other key network players of interest are the number of antennas n_B at B and the number of antennas n_E at E. With this in mind, we address the interference power constraint of I_p proportional to P_t according to $I_p = \sigma P_t$, where σ is a positive constant. Based on Appendix A, we first obtain the first-order expansion of $F_{\gamma_M}(\gamma)$ as

$$F_{\gamma_M|\{X\}}(\gamma) = \begin{cases} \left(\frac{\gamma}{\overline{\gamma}_1}\right)^{n_B}, & X \le \frac{\overline{\gamma}_p}{\overline{\gamma}_0} \\ \left(\frac{X}{\overline{\gamma}_1\sigma}\gamma\right)^{n_B}, & X > \frac{\overline{\gamma}_p}{\overline{\gamma}_0} \end{cases} \tag{16}$$

where $\Gamma(\cdot,\cdot)$ is the incomplete gamma function [21, Eq. (8.350.2)].

Substituting (16) and $f_{\gamma_E}(\gamma_E)$ into (10), and using the binomial expansion, the asymptotic secrecy outage probability is calculated as

$$\begin{aligned} P_{\mathrm{out}}^{\infty} = & \left(1 - e^{-\frac{\overline{\gamma}_p}{\overline{\gamma}_0\Omega_0}}\right) \sum_{i=0}^{n_B} \binom{n_B}{i} \left(\frac{2^{R_s}-1}{\overline{\gamma}_1}\right)^{n_B-i} \left(\frac{2^{R_s}}{\overline{\gamma}_1}\right)^{i} \\ & \times \sum_{j=0}^{n_E-1} \binom{n_E-1}{j} \frac{n_E}{\overline{\gamma}_2} (-1)^j \int_0^{\infty} (\gamma_E)^i e^{-\frac{(j+1)\gamma_E}{\overline{\gamma}_2}} d\gamma_E \\ & + \sum_{i=0}^{n_B} \binom{n_B}{i} \left(\frac{2^{R_s}-1}{\overline{\gamma}_1\sigma}\right)^{n_B-i} \left(\frac{2^{R_s}}{\overline{\gamma}_1\sigma}\right)^{i} \sum_{j=0}^{n_E-1} \binom{n_E-1}{j} \\ & \times \frac{n_E}{\overline{\gamma}_2\sigma} (-1)^j \frac{1}{\Omega_0} \int_{\frac{\overline{\gamma}_p}{\overline{\gamma}_0}}^{\infty} e^{-\frac{x}{\Omega_0}} \int_0^{\infty} x^{n_B+1} (\gamma_E)^i e^{-\frac{(j+1)\gamma_E}{\overline{\gamma}_2\sigma}x} d\gamma_E dx. \end{aligned} \tag{17}$$

$$\begin{aligned} P_{\mathrm{out}} = & \left(1 - e^{-\frac{\sigma}{\Omega_0}}\right) \sum_{i=0}^{n_B} \binom{n_B}{i} \sum_{j=0}^{n_E-1} \binom{n_E-1}{j} \frac{n_E}{\overline{\gamma}_2} (-1)^{i+j} e^{-\frac{i\left(2^{R_s}-1\right)}{\overline{\gamma}_1}} \mu^{-1} \\ & + \sum_{i=0}^{n_B} \binom{n_B}{i} \sum_{j=0}^{n_E-1} \binom{n_E-1}{j} \frac{n_E}{\overline{\gamma}_2\sigma} (-1)^{i+j} \left(\frac{1}{\beta_1 - 1 + 2^{-R_s}} + \frac{1}{\beta_2}\right)^{-1} \frac{e^{-\frac{\sigma}{\Omega_0} - \frac{i\left(2^{R_s}-1\right)}{\overline{\gamma}_1}}}{\frac{1}{\Omega_0} + \frac{i\left(2^{R_s}-1\right)}{\overline{\gamma}_1\sigma}} \end{aligned} \tag{15}$$

Employing [21, Eq. (3.351.3)] given by $\int_0^\infty x^n e^{-\mu x} dx = \Gamma(n+1)/\mu^{n+1}$, we can evaluate the integrals in (17) and derive the secrecy outage probability as

$$P_{\text{out}}^{\infty} = (G_a \overline{\gamma}_1)^{-G_d} + O\left(\overline{\gamma}_1^{-G_d}\right) \tag{18}$$

where the secrecy diversity order is

$$G_d = n_B \tag{19}$$

and the secrecy array gain is

$$G_a = \Bigg[\left(1 - e^{-\frac{\sigma}{\Omega_0}}\right) \sum_{i=0}^{n_{\mathsf{B}}} \binom{n_{\mathsf{B}}}{i} (2^{-R_s} - 1)^{n_{\mathsf{B}}-i} 2^{R_s i} \times \sum_{j=0}^{n_{\mathsf{E}}-1} \binom{n_{\mathsf{E}}-1}{j} n_{\mathsf{E}} \overline{\gamma}_2^i (-1)^j \frac{\Gamma(i+1)}{(j+1)^{i+1}} + \sum_{i=0}^{n_{\mathsf{B}}} \binom{n_{\mathsf{B}}}{i} \times (2^{R_s} - 1)^{n_{\mathsf{B}}-i} \sigma^{-n_{\mathsf{B}}} 2^{R_s i} \sum_{j=0}^{n_{\mathsf{E}}-1} \binom{n_{\mathsf{E}}-1}{j} n_{\mathsf{E}} (\overline{\gamma}_2 \sigma)^i \times (-1)^j (\Omega_0)^{n_{\mathsf{B}}-i} \frac{\Gamma(i+1)}{(j+1)^{i+1}} \Gamma\left(n_{\mathsf{B}} - i + 1, \frac{\sigma}{\Omega_0}\right) \Bigg]^{-\frac{1}{n_{\mathsf{B}}}}. \tag{20}$$

IV. Numerical Results

Numerical examples are provided to highlight the impact of the primary network on the secondary network in the presence of a multiantenna wiretap channel. The exact and asymptotic curves are obtained from (15) and (18), respectively. The exact curves are in precise agreement with the Monte Carlo simulations. We also see that the asymptotic curves well approximate the exact curves at high SNR. The asymptotic curves accurately predict the secrecy diversity order and the secrecy array gain. Throughout this section, we assume unity variance $\Omega_0 = 1$ and expected secrecy rate $R_s = 0.1$ bit/s/Hz.

Fig. 2 plots the secrecy outage probability versus $\overline{\gamma}_1$ for different σ and different n_B. According to (19), we see that the secrecy diversity order increases with n_B, which in turn decreases the secrecy outage probability. We also see that the secrecy outage probability decreases with σ. This is due to relaxing the peak interference power constraint $I_p = \sigma P_t$, which in turn increases transmit power P_A, as indicated by (11). This can also be explained by the fact that the secrecy array gain in (20) increases with increasing σ.

Fig. 3 plots the secrecy outage probability versus $\overline{\gamma}_1$ for different $\overline{\gamma}_2$ and different n_E. The parallel slopes of the asymptotes confirm that the secrecy diversity order is independent of $\overline{\gamma}_2$ and n_E, as indicated in (19). Note the secrecy outage probability increases with increasing $\overline{\gamma}_2$ and n_E. This confirms that the secrecy array gain in (20) is a decreasing function of $\overline{\gamma}_2$ and n_E.

V. Conclusion

We proposed physical-layer security enhancement in cognitive multiantenna wiretap channels. In an effort to assess the secrecy performance in passive eavesdropping, we adopt the secrecy outage probability as a useful performance measure. We derived new closed-form expressions for the exact and asymptotic secrecy outage probability. Based on these, we revealed important design insight into the interplay between two power constraints, namely, the maximum transmit power at the secondary network and the peak interference power at the primary network. The impact of these constraints on the cognitive wiretap channel was showcased.

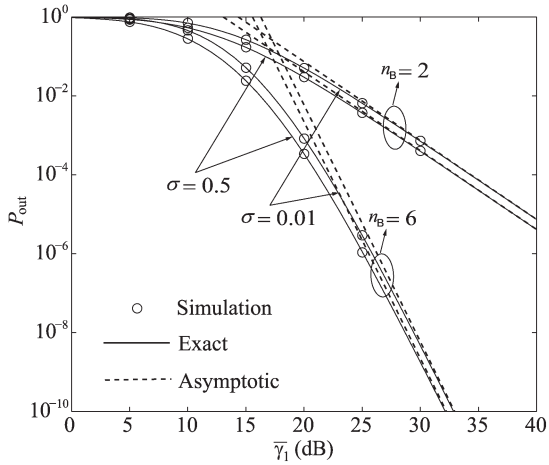

Fig. 2. Secrecy outage probability with $\overline{\gamma}_2 = 10$ dB and $n_E = 2$.

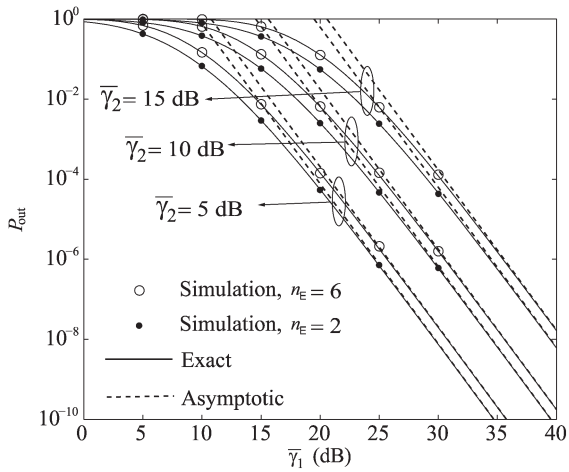

Fig. 3. Secrecy outage probability with $\sigma = 2$ and $n_B = 4$.

Appendix A
Proof of Lemma 1

The CDF and PDF of Y is written as

$$F_Y(y) = \sum_{n=0}^{N} \binom{N}{n} (-1)^n e^{-\frac{ny}{\Omega_Y}} \tag{21}$$

$$f_Y(y) = \sum_{n=0}^{N-1} \binom{N-1}{n} \frac{N}{\Omega_Y} (-1)^n e^{-\frac{(n+1)y}{\Omega_Y}}. \tag{22}$$

Let $u(X) = \min((\overline{\gamma}_p/X), \overline{\gamma}_0)$. Using the probability theory, for RV $\gamma = u(X)Y$, the conditional CDF and PDF of γ can be obtained as (13) and (14), respectively.

Appendix B
Proof of Theorem 1

Based on (12), we note that when $X \leq (\overline{\gamma}_p/\overline{\gamma}_0)$, $\gamma_{\mathsf{M}} = \overline{\gamma}_0 Y_M$, $\gamma_{\mathsf{E}} = \overline{\gamma}_0 Y_E$, and when $X > \overline{\gamma}_p/\overline{\gamma}_0$, $\gamma_{\mathsf{M}} = (\overline{\gamma}_p/X) Y_M$, $\gamma_{\mathsf{E}} =$

$(\overline{\gamma}_p/X)Y_E$. Hence, the secrecy outage probability in (10) can be calculated as

$$P_{\text{out}} = \underbrace{\int_0^{\frac{\overline{\gamma}_p}{\overline{\gamma}_0}} \int_{q_0}^{\infty} F_{\gamma_{\mathsf{M}}|\{X=x\}}\left(\epsilon(\gamma_E)\right) f_{\gamma_{\mathsf{E}}|\{X=x\}}(\gamma_{\mathsf{E}}) f_X(x) d\gamma_{\mathsf{E}} dx}_{\mathcal{J}_1} + \underbrace{\int_{\frac{\overline{\gamma}_p}{\overline{\gamma}_0}}^{\infty} \int_0^{\infty} F_{\gamma_{\mathsf{M}}|\{X=x\}}\left(\epsilon(\gamma_{\mathsf{E}})\right) f_{\gamma_{\mathsf{E}}|\{X=x\}}(\gamma_{\mathsf{E}}) f_X(x) d\gamma_{\mathsf{E}} dx}_{\mathcal{J}_2}. \quad (23)$$

Based on Lemma 1, for $X \le \overline{\gamma}_p/\overline{\gamma}_0$, we have

$$F_{\gamma_{\mathsf{M}}|\{X=x\}}\left(\epsilon(\gamma_{\mathsf{E}})\right) = \sum_{i=0}^{n_{\mathsf{B}}} \binom{n_{\mathsf{B}}}{i} (-1)^i e^{-\frac{i\epsilon(\gamma_{\mathsf{E}})}{\overline{\gamma}_0\Omega_1}}$$

$$f_{\gamma_{\mathsf{E}}|\{X=x\}}(\gamma_{\mathsf{E}}) = \sum_{j=0}^{n_{\mathsf{E}}-1} \binom{n_{\mathsf{E}}-1}{j} \frac{n_{\mathsf{E}}}{\overline{\gamma}_0\Omega_2} (-1)^j e^{-\frac{(j+1)\gamma_{\mathsf{E}}}{\overline{\gamma}_0\Omega_2}}. \quad (24)$$

By substituting (24) and $f_X(x) = (1/\Omega_0)e^{-(x/\Omega_0)}$ into $\mathcal{J}_1$ of (23), $\mathcal{J}_1$ can be derived as

$$\begin{aligned}\mathcal{J}_1 &= \int_0^{\frac{\overline{\gamma}_p}{\overline{\gamma}_0}} f_X(x)dx \sum_{i=0}^{n_{\mathsf{B}}} \binom{n_{\mathsf{B}}}{i} \sum_{j=0}^{n_{\mathsf{E}}-1} \binom{n_{\mathsf{E}}-1}{j} \frac{n_{\mathsf{E}}}{\overline{\gamma}_0\Omega_2} (-1)^{i+j} \\ &\quad \times \int_0^{\infty} e^{-\frac{i\epsilon(\gamma_{\mathsf{E}})}{\overline{\gamma}_0\Omega_1} - \frac{(j+1)\gamma_{\mathsf{E}}}{\overline{\gamma}_0\Omega_2}} d\gamma_{\mathsf{E}} \\ &= \left(1 - e^{-\frac{\overline{\gamma}_p}{\gamma_0\Omega_1}}\right) \sum_{i=0}^{n_{\mathsf{B}}} \binom{n_{\mathsf{B}}}{i} \sum_{j=0}^{n_{\mathsf{E}}-1} \binom{n_{\mathsf{E}}-1}{j} \frac{n_{\mathsf{E}}}{\overline{\gamma}_0\Omega_2} (-1)^{i+j} \\ &\quad \times e^{-\frac{i\left(2^{R_{\mathsf{s}}}-1\right)}{\overline{\gamma}_0\Omega_1}} \left(\frac{i2^{R_{\mathsf{s}}}}{\overline{\gamma}_0\Omega_1} + \frac{j+1}{\overline{\gamma}_0\Omega_2}\right)^{-1}. \end{aligned} \quad (25)$$

For $X > \overline{\gamma}_p/\overline{\gamma}_0$, we have

$$F_{\gamma_{\mathsf{M}}|\{X=x\}}\left(\epsilon(\gamma_{\mathsf{E}})\right) = \sum_{i=0}^{n_{\mathsf{B}}} \binom{n_{\mathsf{B}}}{i} (-1)^i e^{-\frac{i\epsilon(\gamma_{\mathsf{E}})}{\overline{\gamma}_p\Omega_1}x}$$

$$f_{\gamma_{\mathsf{E}}|\{X=x\}}(\gamma_{\mathsf{E}}) = \sum_{j=0}^{n_{\mathsf{E}}-1} \binom{n_{\mathsf{E}}-1}{j} \frac{n_{\mathsf{E}}}{\overline{\gamma}_p\Omega_2} (-1)^j x e^{-\frac{(j+1)\gamma_{\mathsf{E}}}{\overline{\gamma}_p\Omega_2}x}. \quad (26)$$

By substituting (26) into $\mathcal{J}_2$ of (23), $\mathcal{J}_2$ can be derived as

$$\begin{aligned}\mathcal{J}_2 &= \sum_{i=0}^{n_{\mathsf{B}}} \binom{n_{\mathsf{B}}}{i} \sum_{j=0}^{n_{\mathsf{E}}-1} \binom{n_{\mathsf{E}}-1}{j} \frac{n_{\mathsf{E}}}{\overline{\gamma}_p\Omega_2} (-1)^{i+j} \frac{1}{\Omega_0} \\ &\quad \times \int_{\frac{\overline{\gamma}_p}{\overline{\gamma}_0}}^{\infty} e^{-\frac{x}{\Omega_0}} \int_0^{\infty} x e^{-\frac{i\epsilon(\gamma_{\mathsf{E}})}{\overline{\gamma}_p\Omega_1}x - \frac{(j+1)\gamma_{\mathsf{E}}}{\overline{\gamma}_p\Omega_2}x} d\gamma_{\mathsf{E}} dx \\ &= \sum_{i=0}^{n_{\mathsf{B}}} \binom{n_{\mathsf{B}}}{i} \sum_{j=0}^{n_{\mathsf{E}}-1} \binom{n_{\mathsf{E}}-1}{j} \frac{n_{\mathsf{E}}}{\overline{\gamma}_p\Omega_2} (-1)^{i+j} \frac{1}{\Omega_0} \\ &\quad \times \int_{\frac{\overline{\gamma}_p}{\overline{\gamma}_0}}^{\infty} x e^{-\frac{x}{\Omega_0} - \frac{i\left(2^{R_{\mathsf{s}}}-1\right)}{\overline{\gamma}_0\Omega_1}x} \int_0^{\infty} e^{-\frac{i2^{R_{\mathsf{s}}}x\gamma_{\mathsf{E}}}{\overline{\gamma}_0\Omega_1} - \frac{(j+1)\gamma_{\mathsf{E}}}{\overline{\gamma}_p\Omega_2}x} d\gamma_{\mathsf{E}} dx \\ &= \sum_{i=0}^{n_{\mathsf{B}}} \binom{n_{\mathsf{B}}}{i} \sum_{j=0}^{n_{\mathsf{E}}-1} \binom{n_{\mathsf{E}}-1}{j} \frac{n_{\mathsf{E}}}{\overline{\gamma}_p\Omega_2} (-1)^{i+j} \frac{1}{\Omega_0} \\ &\quad \times \left(\frac{i2^{R_{\mathsf{s}}}}{\overline{\gamma}_p\Omega_1} + \frac{j+1}{\overline{\gamma}_p\Omega_2}\right)^{-1} \frac{e^{-\frac{\overline{\gamma}_p}{\overline{\gamma}_0\Omega_0} - \frac{i\left(2^{R_{\mathsf{s}}}-1\right)}{\overline{\gamma}_0\Omega_1}}}{\frac{1}{\Omega_0} + \frac{i\left(2^{R_{\mathsf{s}}}-1\right)}{\overline{\gamma}_p\Omega_1}}. \end{aligned} \quad (27)$$

Substituting (25) and (27) into (23), we get the desired result in (15).

REFERENCES

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

[2] A. Goldsmith, S. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proc. IEEE*, vol. 97, no. 5, pp. 894–914, May 2009.

[3] 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, Jan. 2011.

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

[5] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Wireless Commun.*, vol. 19, no. 1, pp. 40–47, Feb. 2012.

[6] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 509–511, May 2011.

[7] V. U. Prabhu and M. R. D. Rodrigues, "On wireless channels with M-antenna eavesdroppers: Characterization of the outage probability and ε-outage secrecy capacity," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 853–860, Sep. 2011.

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

[9] 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, Jan. 2013.

[10] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2536–2550, May 2013.

[11] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.

[12] 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, Apr. 2011.

[13] J. Zhang and M. C. Gursoy, "Secure relay beamforming over cognitive radio channels," in *Proc 45th Annu. CISS*, Baltimore, MD, USA, Mar. 2011, pp. 1–5.

[14] 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," *IET Commun.*, vol. 6, no. 16, pp. 2676–2687, Nov. 2012.

[15] H. Jeon, S. W. McLaughlin, and J. Ha, "Secure communications with untrusted secondary users in cognitive radio networks," in *Proc IEEE GLOBECOM*, Anaheim, CA, USA, Dec. 2012, pp. 1072–1078.

[16] Y. Wu and K. J. R. Liu, "An information secrecy game in cognitive radio networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 831–842, Sep. 2011.

[17] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 134–145, Jan. 2013.

[18] Z. Chen, J. Yuan, and B. Vucetic, "Analysis of transmit antenna selection/maximal-ratio combining in Rayleigh fading channels," *IEEE Trans. Veh. Technol.*, vol. 54, no. 4, pp. 1312–1321, Jul. 2005.

[19] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[20] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
[21] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 7th ed. San Diego, CA, USA: Academic, 2007.

Cross-Layer Network Lifetime Maximization in Interference-Limited WSNs

Halil Yetgin, *Student Member, IEEE*,
Kent Tsz Kan Cheung, *Student Member, IEEE*,
Mohammed El-Hajjar, *Member, IEEE*, and
Lajos Hanzo, *Fellow, IEEE*

***Abstract*—In wireless sensor networks (WSNs), the network lifetime (NL) is a crucial metric since the sensor nodes usually rely on limited energy supply. In this paper, we consider the joint optimal design of the physical, medium access control (MAC), and network layers to maximize the NL of the energy-constrained WSN. The problem of NL maximization can be formulated as a nonlinear optimization problem encompassing the routing flow, link scheduling, transmission rate, and power allocation operations for all active time slots (TSs). The resultant nonconvex rate constraint is relaxed by employing an approximation of the signal-to-interference-plus-noise ratio (SINR), which transforms the problem to a convex one. Hence, the resultant dual problem may be solved to obtain the optimal solution to the relaxed problem with a zero duality gap. Therefore, the problem is formulated in its Lagrangian form, and the Karush–Kuhn–Tucker (KKT) optimality conditions are employed for deriving analytical expressions of the globally optimal transmission rate and power allocation variables for the network topology considered. The nonlinear Gauss–Seidel algorithm is adopted for iteratively updating the rate and power allocation variables using these expressions until convergence is attained. Furthermore, the gradient method is applied for updating the dual variables in each iteration. Using this approach, the maximum NL, the energy dissipation per node, the average transmission power per link, and the lifetime of all nodes in the network are evaluated for a given source rate and fixed link schedule under different channel conditions.**

***Index Terms*—Cross layer design, energy efficiency, interference, network lifetime, wireless sensor networks.**

NOMENCLATURE

- Number of nodes: $V = 10$.
- Total number of TSs per link: $N = 18$.
- Path-loss exponent: $m = 4$.
- Euclidean distance between consecutive nodes: $d[\text{m}] = 1$.
- Maximum affordable transmit power per node: $(P_v)_{\max}[\text{W}] = 50$.
- Spatially periodic link scheduling parameter: $T = \{3, 4, 5, 6, 7, 8, 9\}$.
- Initial battery energy per node: $E_v[\text{J}] = 5000$.
- Spectral noise power density: $N0[\text{dBm/Hz}] = 1$.
- Power amplifier inefficiency: $\alpha = 0.01$ [26].
- Set of all directed links: $\mathcal{L}$.
- A directed link spanning from transmitter i to receiver j: $l_{i,j}$.
- Set of all sensor nodes: $\mathcal{V}$.
- Network topology incidence matrix: $\mathbf{A}$.
- Emerging link of node v: $l \in \mathcal{O}(v)$.
- Incoming link of node v: $l \in \mathcal{I}(v)$.
- Network-channel-gain matrix: $\mathbf{G}$.
- Fading gain of the link between transmitter i and receiver j: $H_{i,j} = |h_{i,j}|^2$.
- NL: T_{net}.
- Reciprocal of NL: z.
- Transmission rate of link l in TS n: $r_{l,n}$.
- Transmit power of link l in TS n: $P_{l,n}$.
- Logarithm of the transmit power of link l in TS n: $Q_{l,n} = \log(P_{l,n})$.
- A set of dual variables for energy conservation constraint in (5): $\mathbf{\Omega}$.
- A set of dual variables for transmission rate constraint in (4): $\mathbf{\Psi}$.
- A set of dual variables for transmit power constraint in (6): $\boldsymbol{\vartheta}$.
- A set of dual variables for flow constraint in (3): $\boldsymbol{\mu}$.
- Convergence tolerance of the iterative algorithm: $\epsilon = 10^{-5}$.

I. INTRODUCTION

A wireless sensor network (WSN) is composed of a large number of nodes that monitor physical and environmental conditions and pass their accumulated data through the network to a sink node. There are numerous attractive applications for WSNs, including, for example, designing intelligent highways, controlling air pollution, providing remote health assistance for disabled or elderly people, monitoring river level variations, etc. Each of these applications may be composed of many sensor nodes, each of which consumes considerable amount of energy with sensing, communication, and data processing activities. Since each sensor node drains its limited energy supply as time elapses, the network lifetime (NL) is a crucial metric for these applications and has a major impact on the achievable performance of WSNs. Hence, we aim for analyzing and optimizing the NL of the WSNs under different channel conditions.

The NL defines the total amount of time during which the network is capable of maintaining its full functionality and/or achieves particular objectives during its operation, as exemplified in [1] and [2]. Specifically, the authors of [3]–[5] defined the expiration of the NL as the time instant at which a certain number of nodes in the network depleted their batteries. As a further example, the NL was defined in [6] as the lifetime of the specific sensor node associated with the highest energy consumption rate, whereas the authors of [7]–[9] considered the lifetime of the network to be expired at the particular instant, when the first node's battery was depleted. The NL in [8] was also defined as the instant when the first data collection failure occurred. In this paper, the NL is deemed to be expired, when at least one of the nodes fails due to its discharged battery. Therefore, extending the lifetime of a single node becomes an important and challenging task due to the battery-dependent characteristics of the wireless sensor nodes.

Manuscript received November 29, 2013; revised August 1, 2014; accepted September 20, 2014. Date of publication September 25, 2014; date of current version August 11, 2015. This work was supported in part by the Republic of Turkey Ministry of National Education, by the Industrial Company Members of the Mobile VCE, by the U.K. Engineering and Physical Sciences Research Council, and by the Research Councils U.K. through the India–U.K. Advanced Technology Center of the European Union under the auspices of the Concerto Project and of the European Research Council's Senior Research Fellow Grant. The review of this paper was coordinated by Prof. S. Chen.

The authors are with the School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K. (e-mail: hy3g09@ecs.soton.ac.uk; ktkc106@ecs.soton.ac.uk; meh@ecs.soton.ac.uk; lh@ecs.soton.ac.uk).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.
Digital Object Identifier 10.1109/TVT.2014.2360361