www.ietdl.org

Published in IET Communications
Received on 10th September 2011
Revised on 16th June 2012
doi: 10.1049/iet-com.2011.0638

ISSN 1751-8628

Proposed relay selection scheme for physical layer security in cognitive radio networks

H. Sakran[1] *M. Shokair*[1] *O. Nasr*[2] *S. El-Rabaie*[1] *A.A. El-Azm*[1]

[1]*Faculty of Electronic Engineering, El-Menoufia University, Menouf, Menufia, Egypt*
[2]*Faculty of Engineering, Cairo University, Giza, Egypt*
E-mail: hefdh_sakran@yahoo.com

Abstract: In this study, the physical layer security for cognitive radio network (CRN) will be investigated in which a secondary user transmitter (SU-Tx) sends confidential information to a SU receiver (SU-Rx) on the same frequency band of a primary user (PU) in the presence of an eavesdropper receiver. Moreover, relay selection scheme is proposed for the security constrained CRNs with single eavesdropper, multiple eavesdroppers and PUs. The proposed scheme selects a trusted decode and forward relay to assist the SU-Tx and maximise the achievable secrecy rate that is subjected to the interference power constraints at the PUs for the different number of eavesdroppers and PUs under available channel knowledge. The SU cooperates with relays only when a high secrecy rate is achieved. Secrecy rate and secrecy outage probability are the two performance metrics that are used to verify the effectiveness of the proposed scheme although asymptotic approximations of the secrecy outage probability are also derived. Simulation and analytical results demonstrate that the performance improvement of the proposed scheme reaches to the double relative to the conventional scheme for the secrecy capacity.

1 Introduction

There is an unparalleled increase in the usage of wireless devices in the last decade. However, most of the frequency spectrum has already been licensed exclusively to operators by government agencies, such as Federal Communications Commission (FCC). Therefore there exists an apparent spectrum scarcity for new wireless applications and services. In recent studies, especially by the FCC, it is reported that there are vast temporal and spatial variations in the allocated spectrum utilisation. The spectrum utilisation efficiency can be as low as 15% [1, 2]. Recently, CRN [3, 4] has attracted much attention, as it can solve the spectrum scarcity problem by allowing cognitive users (unlicensed users) to transmit concurrently on the same frequency bands with the licensed primary users (PUs) as long as the resulting interference power at the PU receivers is kept below the interference temperature limit [5].

Security is one of the most important aspects in this type of network, multimedia traffic and others [6]. Moreover, the security is one of the challenges to next generation services in IP multimedia subsystem [7] and in packet networks, especially on multimedia applications and real-time services [8]. The traditional security is issued based on cryptographic approaches, which can be broadly classified into public-key and private key protocols that are described in detail in [9]. In these approaches, the security is guaranteed by designing a protocol such that it is computationally prohibitive for the eavesdropper to decode the message. The main idea of these approaches is that security is ensured based on the limited computational power at the eavesdroppers. With the advent of the infrastructureless networks such as mobile *ad hoc* networks, further challenges have appeared which made the nodes more vulnerable to attack. Some of these challenges are memory and power-limited terminals, where the mobile nodes in *ad hoc* have limited storage devices and weak computational capabilities, and the absent of centralised hardware for security problems. Moreover, there are no fixed routers and the packets that are followed in multi-hop routers and pass through different nodes to arrive at their destination. Therefore to cope with these limitations, physical layer security has gained a considerable attention in the last few years. The theoretical foundation to study the physical layer security is the wiretap channel and the information-theoretic notion of secrecy that were introduced by Wyner [10]. He considered the wiretap channel model, in which the eavesdropper has degraded (high noisy) observations from the channel compared with legitimate receiver, that is, the eavesdropper is said to be degraded. Under this assumption, Wyner showed that the advantage of the main channel over that of the eavesdropper, in terms of the low noise level, can be exploited to transmit secrecy bits. In other words, it is possible to achieve a non-zero secret rate without sharing a key, where the eavesdropper is limited to learn almost nothing from the transmissions. An extension of this work to the case of broadcasting channel with confidential messages was proposed in [11].

The first attempt to deal with the secure transmission in a CRN in the context of information-theoretic point of view was considered in [12, 13, 14]. A secrecy multiple-input single-output (MISO) CR channel, in which a multi-antenna secondary user transmitter (SU-Tx) sends confidential information to a single-antenna SU receiver (SU-Rx) in the presence of a single-antenna PU-Rx and a single-antenna eavesdropper receiver (ED-Rx), was considered.

In contrast with [12] and [13] which assumed the availability of perfect channel state information (CSI) of all channels at the SU-TX, in [14], the issue of optimal transmitter design to achieve physical layer security for a cognitive radio network (CRN) was addressed. It is assumed that all the CSI of the secondary, primary and eavesdropper channels are not perfectly known at the SU-Tx. In previous papers of physical layer security in CRN, the authors took the advantage of multiple antenna systems to improve the secrecy rate. However, because of cost and size limitations, multiple antennas may not be available at network nodes.

In this paper, a scenario in which a SU-Tx communicates with a SU-Rx with assistance of multiple relays only when a high secrecy rate is achievable in the presence of different numbers of PUs and eavesdroppers will be considered. Optimal relay selection scheme is proposed in order to maximise the achievable secrecy rate. The decode and forward (DF) technique is considered with two stages. In *first stage*, an SU-Tx broadcasts its encoded signal to trusted relay nodes. In *second stage*, each relay first decodes the message and then re-encodes it. Then from these relays that decode the message correctly, we select the relay that gives us maximum secrecy rate that is subjected to the interference power constraints at the PUs to transmit a version of the re-encoded signal. The rest of this paper is organised as follows. In Section 2, the system model is introduced. The proposed relay selection scheme is explained in Section 3. In Section 4, the direct transmission (DT) secrecy rate and secrecy outage probability is done. In Section 5, the conventional selection scheme is investigated. The simulation results are interpreted in Section 6, followed by the conclusions, appendices and the relevant references.

Notation: Matrices and vectors are denoted using boldface upper and lower-case letters, respectively. $\boldsymbol{I}_m$ denotes an $m \times m$ identity matrix. The symbol $\triangleq$ denotes 'defined as'. $\mathcal{CN}(\mu, N_0)$ denotes circularly symmetric complex Gaussian random variable with mean μ and variance N_0. $\boldsymbol{E}\{.\}$ represents statistical expectation, $[x]^+ \triangleq \max\{0, x\}$.

2 System models

We consider a CR network model as shown in Fig. 1. It consists of one secondary user S (secrecy user), N relay nodes R, one destination node (SU-Rx), L PU ($L \geq 1$) and M eavesdroppers E ($M \geq 1$). The SU-Tx communicates with the SU-Rx under helping of relay nodes. There are some eavesdroppers that try to overhear the source information.

We define the following sets: S_{relays}, gives the set of all relay nodes and S_{evs}, denotes the set of the eavesdroppers. S_{PU}, gives the set of the PUs and C_{d} is considered as the decoding set which contains the relays that have decoded correctly the received messages from the SU-Tx in the first time slot.

In the following, benchmark scheme without cooperation DT and DF scheme as a cooperative scheme is described.

2.1 Direct transmission (DT)

For DT, the secrecy transmitter (SC-Tx) transmits its symbols directly to the SC-Rx. The received signal at the SU-Rx is given by

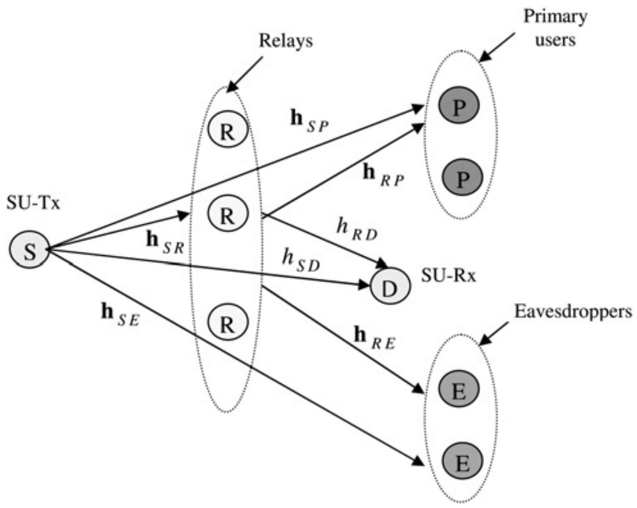

Fig. 1 *Illustration of system model*

$$y_{\text{d}} = \sqrt{P_{\text{s}}} h_{\text{SD}} x + z_{\text{d}} \tag{1}$$

where x is the transmitted symbol from the SU-Tx and P_{s} denotes the average transmitted power per symbol at the SU-Tx. $z_{\text{d}} \sim \mathcal{CN}(0, N_0)$ is the complex Gaussian noise at the SU-Rx and h_{SD} is the channel gains between SU-Tx and SU-Rx. All channels are assumed to undergo flat fading and quasi-static.

The received message at the eavesdroppers is given by

$$\boldsymbol{y}_{\text{e}} = \sqrt{P_{\text{s}}} \boldsymbol{h}_{\text{SE}} x + \boldsymbol{z}_{\text{e}} \tag{2}$$

where $\boldsymbol{y}_{\text{e}}$ is an $M \times 1$ vector, which represents the received signal at eavesdroppers, $\boldsymbol{h}_{\text{SE}}$ is $M \times 1$ vector, which denotes the channel gains between SU-Tx and eavesdroppers, $\boldsymbol{z}_e \sim \mathcal{CN}(0, N_0\boldsymbol{I}_M)$ is an $M \times 1$ vector, which represents complex Gaussian noise at the eavesdroppers, $\boldsymbol{I}_M$ is an $M \times M$ identity matrix.

The received message at the PUs is given by

$$\boldsymbol{y}_{\text{p}} = \sqrt{P_{\text{s}}} \boldsymbol{h}_{\text{SP}} x + \boldsymbol{z}_{\text{p}} \tag{3}$$

where $\boldsymbol{y}_{\text{p}}$ is an $L \times 1$ vector, which represents the received signal at PUs, $\boldsymbol{h}_{\text{SP}}$ is an $L \times 1$ vector, which denotes the channel gains between SU-Tx and PUs, $\boldsymbol{z}_{\text{p}} \sim \mathcal{CN}(0, N_0\boldsymbol{I}_L)$ is an $L \times 1$ vector, which represents complex Gaussian noise at the PUs, $\boldsymbol{I}_L$ is an $L \times L$ identity matrix.

2.2 Decode and forward (DF)

We describe the DF protocol based on our system model; there are two stages in DF. In the first stage, the SU-Tx broadcasts its message to trust relays in the first transmission slot.

The received messages at the N relays are given by

$$\boldsymbol{y}_{\text{r}} = \sqrt{P} \boldsymbol{h}_{\text{SR}} x + \boldsymbol{z}_{\text{r}} \tag{4}$$

where $\boldsymbol{y}_{\text{r}}$ is an $N \times 1$ vector, which represents the received signal at relays, $\boldsymbol{h}_{\text{SR}}$ is an $N \times 1$ vector, which denotes the channel gains between SU-Tx and relays, $\boldsymbol{z}_{\text{r}} \sim \mathcal{CN}(0, N_0\boldsymbol{I}_N)$ is an $M \times 1$ vector which represents complex Gaussian noise at the eavesdroppers, $\boldsymbol{I}_N$ is an $N \times N$ identity matrix.

In the second stage, one of the N trusted relays that decodes the message from SU-Tx to transmit successfully the re-encode message to the SU-Rx.

The received messages at the SU-Rx, the PU and the eavesdroppers are given as

$$y_{\mathrm{d}} = \sqrt{P_{\mathrm{R}}} h_{\mathrm{RD}} x + z_{\mathrm{d}} \tag{5}$$

$$\boldsymbol{y}_{\mathrm{p}} = \sqrt{P_{\mathrm{R}}} \boldsymbol{h}_{\mathrm{RP}} x + \boldsymbol{c}_{\mathrm{p}} \tag{6}$$

$$\boldsymbol{y}_{\mathrm{e}} = \sqrt{P_{\mathrm{R}}} \boldsymbol{h}_{\mathrm{RE}} x + \boldsymbol{z}_{\mathrm{e}} \tag{7}$$

where h_{RD} is the channel gains between the selected relay and SU-Rx, $\boldsymbol{h}_{\mathrm{RP}}$ and $\boldsymbol{h}_{\mathrm{RE}}$ are the channel vectors for selected relay-PUs and selected relay eavesdroppers, respectively. P_{R} denotes the transmitted power at the relay. Maximum ratio combining (MRC) is used to combine the two received signals that are represented in (1) and (5) at the destination.

3 Proposed relay selection scheme

In this section, the proposed relay selection scheme is provided. The object of this scheme is to select the node R that maximises the achieved secrecy rate. First, we will consider a CRN with one eavesdropper that can individually decipher the message from SU-Tx and single PU. Then, the effect of the multiple eavesdroppers will be studied. Finally, the effect of multiple of PUs will be considered.

3.1 Relay selection scheme with one eavesdropper

In this section, we consider one eavesdropper that tries to decode the source information. In this case, the instantaneous achievable secrecy rate for the network shown in Fig. 1 with decoding set C_{d}, is given by [15] (see (8)) where $R \in C_{\mathrm{d}}$.

γ_{SD}: The instantaneous signal-to-noise ratios (SNRs) for the SU-Tx – SU-Rx link.
γ_{SE}: The instantaneous SNRs for the SU-Tx – eavesdropper link.
γ_{RD}: The instantaneous SNRs for the selected relay – SU-Rx link.
γ_{RE}: The instantaneous SNRs for the selected relay – eavesdropper link.

The distribution of the channel coefficient between the nodes i and j ($h_{\mathrm{i,j}}$) is modelled as a zero-mean, independent Gaussian random variable with variance $\sigma_{\mathrm{ij}}^2\, h_{\mathrm{i,j}} \sim \mathcal{CN}(0, \sigma_{\mathrm{i,j}}^2)$, where $\sigma_{\mathrm{ij}}^2 \triangleq \boldsymbol{E}\{|h_{\mathrm{ij}}|^2\} = d_{\mathrm{ij}}^{-\chi}$. d_{ij} is the Euclidean distance between node i and j, and χ is the path-loss exponent.

The secrecy outage probability in traditional wireless networks is defined as the probability that the secrecy rate is less than a given target secrecy rate $Rs > 0$ [16]. For CRN, we can define the secrecy outage probability as the probability that the secrecy rate is less than a given target that is subjected to the interference power constraints at the PUs (interference power at the PU is less than a certain limit) or the probability of the interference power at the PU is larger than a certain limit (interference temperature limit).

Based on (8), the secrecy outage probability for CRN is denoted as

$$P_{\mathrm{sop}} = \sum_{n=1}^{N} \Pr\{|C_{\mathrm{d}} = n|\}[\Pr\{C_{\mathrm{s}}^{\mathrm{n}}(R) < R_{\mathrm{s}}\} \\ \Pr(IN_{\mathrm{p}}^{\mathrm{R}} \leq \Gamma) + \Pr(IN_{\mathrm{p}}^{\mathrm{R}} > \Gamma)] \tag{9}$$

where $IN_{\mathrm{p}}^{\mathrm{R}}$: is the interference power at the PU from the SU-Tx, noise and the R relay.

Γ: gives the interference temperature limit.
$|C_{\mathrm{d}}|$: denotes the cardinality of a set C_{d}.

The object is to obtain the following constrained optimisation problem

$$\begin{aligned} &R^* = \arg \max_{R \in C_{\mathrm{d}}} \{C_{\mathrm{s}}^{|C_{\mathrm{d}}|}(R)\} \\ &S.T. IN_{\mathrm{p}}^{\mathrm{R}} \leq \Gamma \end{aligned} \tag{10}$$

The selection scheme in (10) that maximises the instantaneous secrecy rate and minimises the secrecy outage probability

$$R^* = \arg \min_{R \in C_{\mathrm{d}}} \{\Pr(C_{\mathrm{s}}^{|C_{\mathrm{d}}|} < R_{\mathrm{s}}) \Pr(IN_{\mathrm{p}}^{\mathrm{R}} \leq \Gamma) + \Pr(IN_{\mathrm{p}}^{\mathrm{R}} > \Gamma)\} \tag{11}$$

Assuming $|C_D| > 0$, the instantaneous secrecy rate is given by

$$C_{\mathrm{s}}(R) = \left[\frac{1}{2}\log_2\left(\frac{1+\gamma_{\mathrm{SD}}+\gamma_{\mathrm{RD}}}{1+\gamma_{\mathrm{SE}}+\gamma_{\mathrm{RE}}}\right)\right]^+ \tag{12}$$

Note from (12) that positive secrecy rate is achieved only in the case when the rate of the SU-Tx with respect to the SU-Rx is larger than the maximum rate over the eavesdroppers with respect to the SU-Tx.

The relay-selection process that will maximise the secrecy capacity given in (12) is denoted as

$$\begin{aligned} &R^* = \arg \max_{R \in C_{\mathrm{d}}} \left\{\frac{1+\gamma_{\mathrm{SD}}+\gamma_{\mathrm{RD}}}{1+\gamma_{\mathrm{SE}}+\gamma_{\mathrm{RE}}}\right\} \\ &S.T. IN_{\mathrm{p}}^{\mathrm{R}^*} \leq \Gamma \end{aligned} \tag{13}$$

3.1.1 Asymptotic secrecy outage probability: Here, an asymptotic approximation for the secrecy outage probability at high SNR is derived. In order to simplify the analysis, the symmetric case is considered where the

$$C_{\mathrm{s}}^{|C_{\mathrm{d}}|}(R) = \begin{cases} \left[\dfrac{1}{2}\log_2(1+\gamma_{\mathrm{SD}}) - \dfrac{1}{2}\log_2(1+\gamma_{\mathrm{SE}})\right]^+ & \text{if} \quad |C_{\mathrm{d}}| > 0 \\ \left[\dfrac{1}{2}\log_2(1+\gamma_{\mathrm{SD}}+\gamma_{\mathrm{RD}}) - \dfrac{1}{2}\log_2(1+\gamma_{\mathrm{SE}}+\gamma_{\mathrm{RE}})\right]^+ & \text{if} \quad |C_{\mathrm{d}}| = 0 \end{cases} \tag{8}$$

doi: 10.1049/iet-com.2011.0638

source–destination, source–eavesdropper, relay–destination and relay–eavesdropper distances are equal. This configuration simplifies the analysis and is a guideline for the general asymmetric case (a similar approach has been used in [17] for cooperative network).

Moreover, at high SNR values, all the relays are assumed to decode the signal that is transmitted from the SU-Tx correctly so that $|C_\mathrm{d}| = N$, where $(\Pr\{|C_\mathrm{d}| = |S_\mathrm{relay}| = N\} = 1)$.

Therefore the outage probability is simplified as

$$P_\mathrm{sop} = \Pr\{C_\mathrm{s}^N(R) < R_\mathrm{s}\}\Pr(IN_\mathrm{p}^\mathrm{R} \le \Gamma) + \Pr(IN_\mathrm{p}^\mathrm{R} > \Gamma) \quad (14)$$

According to this assumption, the secrecy outage probability for the case of one eavesdropper and one PU is given by

$$P_\mathrm{sop} = \left[1 - \frac{1}{(1+\beta)^2} - \frac{2\beta}{(1+\beta)^3}\right]^N \left[1 - \mathrm{e}^{(-\lambda/P)\Gamma}\left(\frac{\lambda}{P}\Gamma + 1\right)\right] + \left[\mathrm{e}^{(-\lambda/P)\Gamma}\left(\frac{\lambda}{P}\Gamma + 1\right)\right] \quad (15)$$

where $\beta = 2^{2R_\mathrm{s}}$. Details of the derivation of this equation are included in Appendix 1.

3.2 Relay selection scheme with multiple eavesdroppers

Here, M eavesdroppers are considered that try to decode the signal transmitted from the SU-Tx. In this case, the instantaneous achievable secrecy rate for the CR network shown in Fig. 1, with a decoding set C_d is given as follows (see (16))

Assuming that $|C_D| > 0$, the instantaneous secrecy rate is given by

$$C_\mathrm{s}(R) = \left[\frac{1}{2}\log_2\left(\frac{1 + \gamma_\mathrm{SD} + \gamma_\mathrm{RD}}{\max\limits_{E_\mathrm{m} \in S_\mathrm{evs} \forall \mathrm{m}} (1 + \gamma_{\mathrm{SE}_\mathrm{m}} + \gamma_{\mathrm{RE}_\mathrm{m}})}\right)\right]^+ \quad (17)$$

The relay selection process that will maximise the secrecy capacity given in (17) is denoted by

$$R^* = \arg \max_{R \in C_\mathrm{d}} \left\{\frac{1 + \gamma_\mathrm{SD} + \gamma_\mathrm{RD}}{\max\limits_{E_\mathrm{m} \in S_\mathrm{evs} \forall \mathrm{m}} (1 + \gamma_{\mathrm{SE}_\mathrm{m}} + \gamma_{\mathrm{RE}_\mathrm{m}})}\right\}$$
$$\text{S.T. } IN_p^{R^*} \le \Gamma \quad (18)$$

As the previous case of one eavesdropper, we try to find the asymptotic secrecy outage probability for the symmetric case for simplicity, which is described as follows: (see (19))

Details of the derivation of this equation are included in Appendix 2.

For the special case of $M = 2$, the outage probability in (19) can be solved in closed form to yield

$$P_\mathrm{sop} = \left[1 - \frac{2 + 6\beta}{(1+\beta)^3} + \frac{6\beta^2 + 32\beta + 16}{(2+\beta)^4}\right]^N \times \left[1 - \mathrm{e}^{(-\lambda/P)\Gamma}\left(\frac{-\lambda}{P}\Gamma + 1\right)\right] + \left[\mathrm{e}^{(-\lambda/P)\Gamma}\left(\frac{-\lambda}{P}\Gamma + 1\right)\right] \quad (20)$$

3.3 Relay selection scheme with multiple PUs

In this section, M eavesdroppers and L PUs are considered. In this case, the instantaneous achievable secrecy rate for the CR network is given as follows: (see (21))

The relay selection process that will maximise the secrecy capacity given in (21) is described as follows

$$R^* = \arg \max_{R \in C_\mathrm{d}} \{C_\mathrm{s}^{|C_\mathrm{d}|}(R)\}$$
$$\text{S.T. } l = 1, 2, \ldots, L \quad \max_{p_l \in S_\mathrm{PU}} \{IN_{p_l}^{R^*}\} \le \Gamma \quad (22)$$

The secrecy outage probability is given by

$$P_\mathrm{sop} = \sum_{n=1}^{N} \Pr\{|C_\mathrm{d} = n|\}[\Pr\{C_\mathrm{s}^\mathrm{n}(R) < R_s\}\Pr(\max_{p_l \in S_\mathrm{PU}} \{IN_{p_l}^R\} \le \Gamma) + \Pr(\max_{p_l \in S_\mathrm{PU}} \{IN_{p_l}^R\} > \Gamma)] \quad (23)$$

$$C_\mathrm{s}^{|C_\mathrm{d}|}(R) = \begin{cases} \left[\frac{1}{2}\log_2(1 + \gamma_\mathrm{SD}) - \frac{1}{2}\log_2\left(\max\limits_{E_\mathrm{m} \in S_\mathrm{evs}} (1 + \gamma_{\mathrm{SE}_\mathrm{m}})\right)\right]^+ & \text{if} \quad |C_\mathrm{d}| = 0 \\ \left[\frac{1}{2}\log_2(1 + \gamma_\mathrm{SD} + \gamma_\mathrm{RD}) - \frac{1}{2}\log_2\left(\max\limits_{E_\mathrm{m} \in S_\mathrm{evs}} (1 + \gamma_{\mathrm{SE}_\mathrm{m}} + \gamma_{\mathrm{RE}_\mathrm{m}})\right)\right]^+ & \text{if} \quad |C_\mathrm{d}| > 0 \end{cases} \quad (16)$$

$$P_\mathrm{sop} \simeq \left[M\int_0^\infty [1 - \mathrm{e}^{-\lambda\beta y}(1 + \lambda\beta y)](\lambda^2 y \mathrm{e}^{-\lambda y})[1 - \mathrm{e}^{-\lambda y}(1 + \lambda y)]^{M-1}\,\mathrm{d}y\right]^N \times \left[1 - \mathrm{e}^{(-\lambda/P)\Gamma}\left(\frac{\lambda}{P}\Gamma + 1\right)\right] + \left[\mathrm{e}^{(-\lambda/P)\Gamma}\left(\frac{\lambda}{P}\Gamma + 1\right)\right] \quad (19)$$

$$C_\mathrm{s}^{|C_\mathrm{d}|}(R) = \begin{cases} \left[\frac{1}{2}\log_2(1 + \gamma_\mathrm{SD}) - \frac{1}{2}\log_2\left(\max\limits_{E_\mathrm{m} \in S_\mathrm{evs}} (1 + \gamma_{\mathrm{SE}_\mathrm{m}})\right)\right]^+ & \text{if} \quad |C_\mathrm{d}| = 0 \\ \left[\frac{1}{2}\log_2(1 + \gamma_\mathrm{SD} + \gamma_\mathrm{RD}) - \frac{1}{2}\log_2\left(\max\limits_{E_\mathrm{m} \in S_\mathrm{evs}} (1 + \gamma_{\mathrm{SE}_\mathrm{m}} + \gamma_{\mathrm{RE}_\mathrm{m}})\right)\right]^+ & \text{if} \quad |C_\mathrm{d}| > 0 \end{cases} \quad (21)$$

According to Appendix 3, the asymptotic secrecy outage probability for the symmetric case for simplicity is given by (see (24))

For the special case of $M = 1$ and $L = 2$, the outage probability in (24) yields the following closed form

$$P_{\text{sop}} = \left[1 - \frac{1}{(1+\beta)^2} - \frac{2\beta}{(1+\beta)^3}\right]^N \left[1 - \mathrm{e}^{(-\lambda/P)\Gamma}\left(\frac{\lambda}{P}\Gamma + 1\right)\right]^2 + \left[2\mathrm{e}^{(-\lambda/P)\Gamma}\left(\frac{\lambda}{P}\Gamma + 1\right) - \mathrm{e}^{(-2\lambda/P)\Gamma}\left(\frac{\lambda}{P}\Gamma + 1\right)^2\right] \tag{25}$$

4 DT secrecy rate and outage probability

In this section, we will consider the secrecy rate and outage probability of DT for different cases.

4.1 DT with one eavesdropper

Here, we consider one eavesdropper that tries to decode the source information. In this case, the instantaneous achievable secrecy rate for the network is given as follows

$$C_s = [\log_2(1 + \gamma_{\text{SD}}) - \log_2(1 + \gamma_{\text{SE}})]^+ \tag{26}$$

Based on (26), the secrecy outage probability for CRN is given as

$$P_{\text{sop}} = \Pr\{C_{\text{s}} < R_{\text{s}}\}\Pr(IN_{\text{p}} \le \Gamma) + \Pr(IN_{\text{p}} > \Gamma) \tag{27}$$

where IN_{p}: is the interference power at the PU from the SU-Tx and noise.

As the previous section, we try to find the asymptotic secrecy outage probability for the symmetric case for simplicity.

$$P_{\text{sop}} \simeq \frac{\alpha}{1+\alpha}[1 - \mathrm{e}^{(-\lambda/P_{\text{s}})\Gamma}] + [\mathrm{e}^{(-\lambda/P_{\text{s}})\Gamma}] \tag{28}$$

where $\alpha = 2^{R_{\text{s}}}$. Details of the derivation of this equation are included in Appendix 4.

4.2 DT with multiple eavesdroppers

Here, we consider M eavesdroppers that try to decode the source information. In this case, the instantaneous achievable secrecy rate is given as follows

$$C_{\text{s}} = [\log_2(1 + \gamma_{\text{SD}}) - \log_2(\max_{E_m \in S_{\text{evs}}}(1 + \gamma_{\text{SE}_{\text{m}}}))]^+ \tag{29}$$

As the previous case of one eavesdropper, the asymptotic secrecy outage probability is denoted by

$$P_{\text{sop}} \simeq \left[M\int_0^\infty [1 - \mathrm{e}^{-\lambda\alpha y}](\lambda \mathrm{e}^{-\lambda y})[1 - \mathrm{e}^{-\lambda y}]^{M-1}\,\mathrm{d}y\right] [1 - \mathrm{e}^{(-\lambda/P_{\text{s}})\Gamma}] + [\mathrm{e}^{(-\lambda/P_{\text{s}})\Gamma}] \tag{30}$$

Details of the derivation of this equation are included in Appendix 5.

For the special case of $M = 2$, the outage probability in (30) yields the following closed form

$$P_{\text{sop}} \simeq \left[1 - \frac{2}{1+\alpha} + \frac{2}{2+\alpha}\right][1 - \mathrm{e}^{(-\lambda/P_{\text{s}})\Gamma}] + [\mathrm{e}^{(-\lambda/P_{\text{s}})\Gamma}] \tag{31}$$

4.3 DT with multiple PUs

In this section, we consider M eavesdroppers and L PUs. The secrecy outage probability is given by

$$P_{\text{sop}} = \Pr\{C_s < R_s\}\Pr(\max_{p_l \in S_{\text{PU}}}\{IN_{p_l}\} \le \Gamma) + \Pr(\max_{p_l \in S_{\text{PU}}}\{IN_{p_l}\} > \Gamma) \tag{32}$$

According to Appendix 6, the asymptotic secrecy outage probability is denoted by

$$P_{\text{sop}} \simeq \left[M\int_0^\infty [1 - \mathrm{e}^{-\lambda\alpha y}](\lambda e^{-\lambda y})[1 - \mathrm{e}^{-\lambda y}]^{M-1}\,\mathrm{d}y\right] [1 - \mathrm{e}^{(-\lambda/P_{\text{s}})\Gamma}]^L + [1 - (1 - \mathrm{e}^{(-\lambda/P_{\text{s}})\Gamma})^L] \tag{33}$$

For the special case of $M = 1$ and $L = 2$, the outage probability in (33) yields the following closed form

$$P_{\text{sop}} \simeq \frac{\alpha}{1+\alpha}[1 - \mathrm{e}^{(-\lambda/P_{\text{s}})\Gamma}]^2 + \mathrm{e}^{(-\lambda/P_{\text{s}})\Gamma}[2 - \mathrm{e}^{(-\lambda/P_{\text{s}})\Gamma}] \tag{34}$$

5 Conventional relay selection scheme

In the conventional scheme, the link between the relay and eavesdropper is not taken into account. The conventional selection selects the relay that gives the best instantaneous link between the relay and SU-Rx which is subjected to the power interference at the PUs not exceeding the given interference temperature limit for PUs, which is described as

$$\begin{aligned} R^* &= \arg \max_{R \in C_{\text{d}}}\{\gamma_{R,D}\} \\ \text{s.t.} \quad & IN_{\text{p}}^R \le \Gamma \end{aligned} \tag{35}$$

For N relay nodes $R = \{R_1, R_2, \ldots, R_N\}$

$$P_{\text{sop}} \simeq \left[M\int_0^\infty [1 - \mathrm{e}^{-\lambda\beta y}(1 + \lambda\beta y)](\lambda^2 y \mathrm{e}^{-\lambda y})[1 - \mathrm{e}^{-\lambda y}(1 + \lambda y)]^{M-1}\,\mathrm{d}y\right]^N \times \left[1 - \mathrm{e}^{(-\lambda/P)\Gamma}\left(\frac{\lambda}{P}\Gamma + 1\right)\right]^L + \left[1 - \left(1 - \mathrm{e}^{(-\lambda/P)\Gamma}\left(\frac{\lambda}{P}\Gamma + 1\right)\right)^L\right] \tag{24}$$

To find maximum among N independent and identically distributed (i.i.d.) random variables

$$\Pr(R_i = \max_{R \in C_\mathrm{d}} \{\gamma_{R,D}\}) = \prod_{\substack{n=1\\ n\neq i}}^{N} \Pr(\gamma_{R_i} > \gamma_{R_n})$$

$$= \prod_{\substack{n=1\\ n\neq i}}^{N} [1 - \Pr(\gamma_{R_i} < \gamma_{R_n})]$$

γ_{R_i} are exponential random variables with parameter λ_ι

$$f_X(x) = \lambda \mathrm{e}^{-\lambda x} \quad \text{PDF of the } \gamma_{R_i}$$

$$F_X(x) = 1 - \mathrm{e}^{-\lambda x} \quad \text{CDF of the } \gamma_{R_i}$$

$$\Pr(\gamma_{R_i} < \gamma_{R_n}) = \int_0^\infty \int_0^{\gamma_{R_n}} f(\gamma_{R_n}) f(\gamma_{R_i})\, \mathrm{d}f_{\gamma_{R_i}}\, \mathrm{d}f_{\gamma_{R_n}}$$

$$= \frac{\sigma^2_{R_i,D}}{\sigma^2_{R_i,D} + \sigma^2_{R_n,D}}$$

So,

$$\Pr(R_i = \max_{R \in C_\mathrm{d}} \{\gamma_{R,D}\}) = \prod_{\substack{n=1\\ n\neq i}}^{N} \frac{\sigma^2_{R_i,D}}{\sigma^2_{R_i,D} + \sigma^2_{R_n,D}} \tag{36}$$

The secrecy outage probability is given by

$$P_\mathrm{sop} = \sum_{n=1}^{N} \Pr\{|C_\mathrm{d}| = n\}[\Pr\{C_\mathrm{s}^n(R) < R_\mathrm{s}\} \Pr(IN_\mathrm{p}^R \le \Gamma) + \Pr(IN_\mathrm{p}^R > \Gamma)] \tag{37a}$$

The asymptotic secrecy outage probability is denoted by (see (37b))

$$P_\mathrm{sop} \simeq \left[N \sum_{k=0}^{N-1} \binom{N-1}{k} (-1)^k \left(\frac{1}{k(k+1)(1+\beta+k\beta)^2} - \frac{1}{k(1+\beta)^2} + \frac{1}{k+1} \right) \right] \times \left[1 - \mathrm{e}^{(-\lambda/P)\Gamma} \left(\frac{\lambda}{P}\Gamma + 1 \right) \right] + \left[\mathrm{e}^{(-\lambda/P)\Gamma} \left(\frac{\lambda}{P}\Gamma + 1 \right) \right] \tag{37b}$$

Details of the derivation of this equation are included in Appendix 7.

For the special case of $N = 4$, the outage probability in (37b) yields the following closed form

$$P_\mathrm{sop} \simeq \left[\frac{22}{3(1+\beta)^2} - \frac{6}{(1+2\beta)^2} + \frac{2}{(1+3\beta)^2} - \frac{1}{3(1+4\beta)^2} - 3 \right] \times \left[1 - \mathrm{e}^{(-\lambda/P)\Gamma} \left(\frac{\lambda}{P}\Gamma + 1 \right) \right] + \left[\mathrm{e}^{(-\lambda/P)\Gamma} \left(\frac{\lambda}{P}\Gamma + 1 \right) \right]$$

6 Simulation results

We perform Monte Carlo simulation consisting of 10 000 independent trials to obtain the average results. The system parameters are outlined as follows:

- $N = 4$ relays and $M = 1$, 2 eavesdroppers and $L = 1$, 2 PUs are deployed in one-dimensional area.
- The eavesdropper is located at (60,0) in the case of one eavesdropper and the eavesdroppers are located at (60,0) and (62,0) in the case of two eavesdroppers.
- The SU-Rx (destination) is located at (50,0).
- The PU is located at (100,0).
- The location of the four relays are located randomly as example (15,0), (10,0), (17,0) and (30,0).
- The relay power, $P_R = 10$ W.
- The interference temperature limit $\Gamma = -4$ dB.
- The path loss exponent is taken to be $\chi = 3$.
- The transmission rate is equal to $R_0 = 2$ bits/s/Hz.
- The target secrecy rate is equal to 0.1 bits/s/Hz.

Note that for the relay that belongs to the decoding set, the transmission rate R_0 must be less than the capacity of the SU-Tx-relay channel. The power of relays is fixed at 10 W.

Fig. 2 shows the secrecy rate of the DT, optimal selection (OS) and conventional selection (CS) against the power at SU-Tx. In this figure, two cases are considered, the first case of one eavesdropper and the other case of two eavesdroppers. For the OS, R is selected using (10) and (18) for the cases of one eavesdropper and two eavesdroppers, respectively. For the CS, R is selected using (35). It can be seen from Fig. 2 that the OS scheme significantly improves the secrecy rate for both one eavesdropper and two eavesdroppers. Moreover, the secrecy rate first increases to the power value equal to 12 dB, and then it decreases. This is because the power interference constraints at the PUs. We also note that the performance of CS is degraded compared with DT because the relay which is selected, based on (35), gives more benefit secrecy rate for the eavesdropper, better than for SU-Rx, where the link between the relay and eavesdropper does not take into account when R is selected.

The effect of the location of the relays is shown in Fig. 3. In this figure, the location of the relays varies from (5,0) to

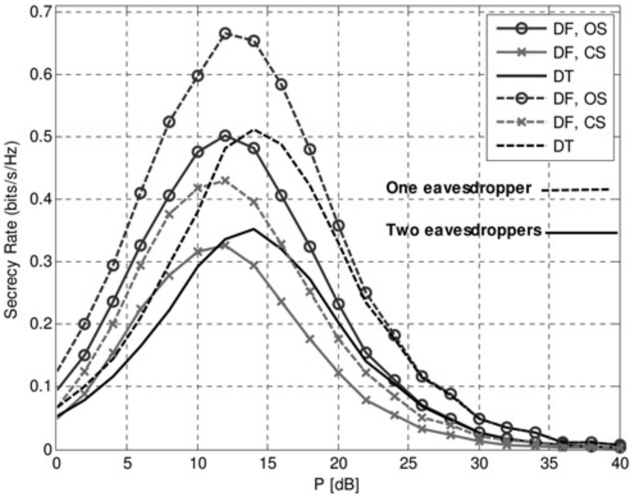

Fig. 2 *Secrecy rate against power at SU-Tx*

(45,0), where all N relays are located at the same position. The power of SU-Tx is fixed at 10 dB. From this figure, it can be seen that for the DT, the secrecy rate is independent of the relay location, as expected, although the secrecy rate of the OS and CS first increases and then decreases when the relays locations move away from the SU-Tx. Moreover, comparisons between the effect of one eavesdropper and two eavesdroppers will be considered for DT, CS and OS.

Figure 4 shows the secrecy rate for different values of IT limit Γ. In this figure, the location of the $N = 4$ relays at (15,0), (10,0), (17,0) and (30,0), $P_R = P_s = 10$ dB, eavesdroppers' location at (60,0) for the case of one eavesdropper and at (60,0), (62,0) for the case of two eavesdroppers. We note from Fig. 4 that when the IT limit increases, the secrecy rate increases and then becomes stable at IT limit value that is larger than 0 dB for both the cases of one eavesdropper and two eavesdroppers.

The secrecy outage probability is the second performance metric that is used to verify the effectiveness of the proposed scheme. Fig. 5 shows the secrecy outage probability against transmitted power at SU-Tx. The target secrecy rate is equal to 0.1 bits/s/Hz. From this figure, we can see that the robustness of the proposed scheme and the improvement in the secrecy outage probability are achieved.

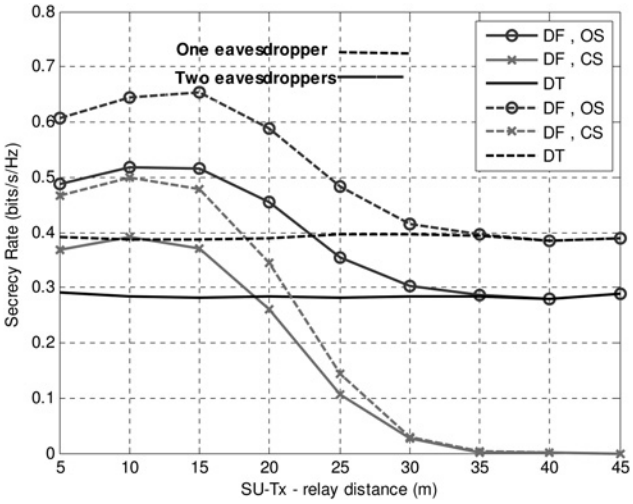

Fig. 3 *Secrecy rate against SU-Tx to relay distance*

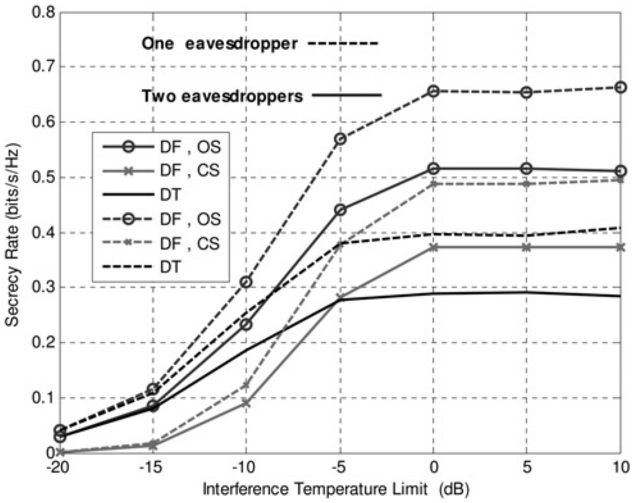

Fig. 4 *Secrecy rate against different values of IT limit*

In Fig. 6 we test the impact of the relays' location on the secrecy outage probability. It can be seen that for the CS and OS, as the relays are closer to the SU-Rx than the SU-Tx, the secrecy outage probability reaches one for CS and reaches the secrecy outage probability that is equal to that of DT for OS. The reason CS reaches one is that the relays become closer to both SU-Rx and eavesdroppers, where relay–eavesdroppers links are not taken into account when selecting the relay for CS. Therefore it may select that relay with relay–eavesdroppers link and relay-SU-Rx link have the same fading.

Finally, we test the impact of the number of PUs on the achieved secrecy rate and secrecy outage probability of the proposed scheme.

In Fig. 7, the PUs' location is fixed at (100,0) for the case of one PU and at (100,0), (90,0)) for the case of two PUs. This figure shows the secrecy rate of the DT, CS and OS against the power transmitted at SU-Tx. The location of the $N = 4$ relays at (15,0), (10,0), (17,0) and (30,0) and the eavesdropper's location at (60,0), The interference temperature limit $\Gamma = -4$ dB and the power at relay = 10 dB. We conclude from this figure that the secrecy rate degrades when the number of PUs increases. We note also that the difference on secrecy rate only starts at the transmitted power from SU-Tx at 7 dB. This is because the difference of the fading channels between

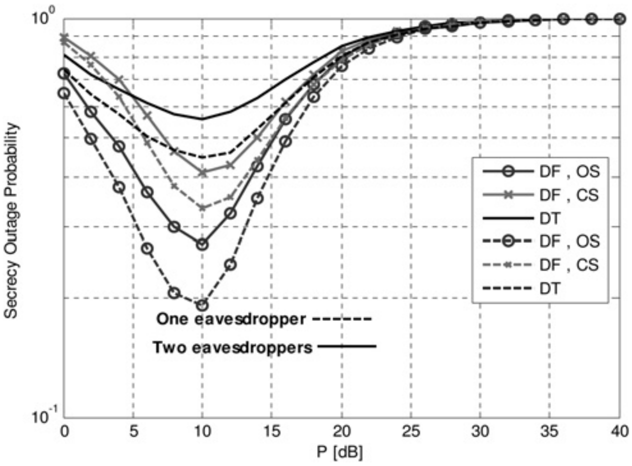

Fig. 5 *Secrecy outage probability against power at SU-Tx*

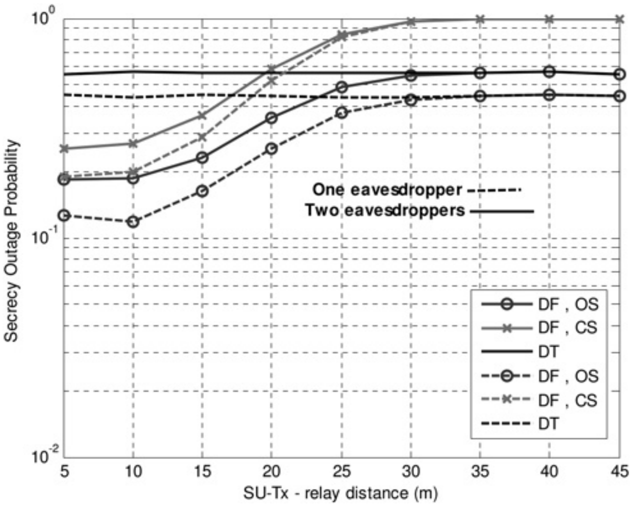

Fig. 6 *Secrecy outage probability against SU-Tx to relay distance*

doi: 10.1049/iet-com.2011.0638

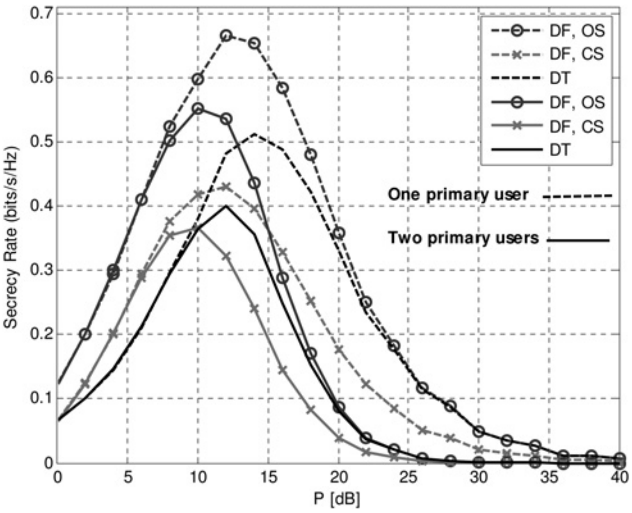

Fig. 7 *Secrecy rate against power at SU-Tx with different number of PUs*

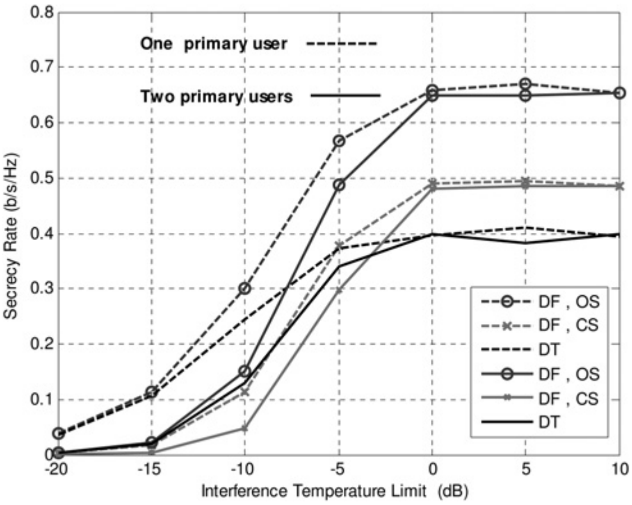

Fig. 8 *Secrecy rate against interference temperature limit with different number of PUs*

SU-Tx and two PUs appears when power transmitted from SU-Tx is larger than 7 dB.

Fig. 8 shows the secrecy rate for different values of IT limit Γ. In this figure, the power transmitted from SU-Tx is fixed at 10 dB and the IT limit is varied from −20 dB to 10 dB. It can be seen from this figure that the secrecy rate is equal for the two cases (for IT limit larger than 0 dB) because the interference power constraint relaxes.

7 Conclusions

In this paper, we have proposed relay selection scheme for secrecy-constrained CRN s which improves the secrecy rate and enhances the outage performance of such systems. We have tested the proposed scheme in CRNs at different number of eavesdroppers and PUs.

In the proposed OS, one relay is selected in the second phase to enhance the security against the eavesdroppers that are subjected to the power interference constraints at the PUs. From simulation results, we can conclude that the proposed selection scheme can significantly improve the system performance in terms of the achievable secrecy rate and the secrecy outage probability. Moreover, we have derived the asymptotic secrecy outage probability for the different number of eavesdroppers and PUs.

8 References

1 Federal Communications Commission: 'Spectrum policy task force report'. FCC Document ET Docket no. 02-155, November 2002

2 Federal Communications Commission (FCC): 'Notice of proposed rulemaking on cognitive radio'. Std.no. 03-322, December 2003

3 Mitola, J.: 'Cognitive radio: an integrated agent architecture for software defined radio'. PhD thesis, Stockholm, Sweden, 2000 KTH

4 Haykin, S.: 'Cognitive radio: brain-empowered wireless communications', *IEEE J. Sel. Areas Commun.*, 2005, **23**, (2), pp. 201–220

5 Kolodzy, P.J.: 'Interference temperature: a metric for dynamic spectrum utilization', *Int. J. Netw. Manage.*, 2006, **16**, (2), pp. 103–113

6 Zhou, L., Chao, H.C.: 'Multimedia traffic security architecture for internet of things', *IEEE Netw.*, 2011, **25**, (3), pp. 29–34

7 Chen, C.Y., Chang, K.D., Chao, H.C.: 'Transaction pattern based anomaly detection algorithm for IP multimedia subsystem', *IEEE Trans. Inf. Forensics Sec.*, 2011, **6**, (1), pp. 152–161

8 Xiong, K., Qiu, Z.D., Guo, Y.C., Zhang, H.K., Chao, H.C.: 'Two LIC-based fast forwarding schemes for explicit routing with scalability, flexibility and security', *J. Internet Technol.*, 2011, **12**, (3), pp. 407–416

9 Delfs, H., Knebl, H.: 'Introduction to cryptography: principles and applications' (Springer, 2007, 2nd edn.)

10 Wyner, A.: 'The wire-tap channel', *Bell Syst. Tech. J.*, 1975, **54**, (8), pp. 1355–1387

11 Csiszar, I., Korner, J.: 'Broadcast channels with confidential messages', *IEEE Trans. Inf. Theory*, 1978, **24**, (3), pp. 451–456

12 Pei, Y., Liang, Y.-C., Teh, K.C., Li, K.H.: 'Achieving cognitive and secure transmissions using multiple antennas'. IEEE 20th Int. Symp. on Personal, Indoor and Mobile Radio Communications, Singapore, Singapore, September 2009, pp. 1–5

13 Pei, Y., Liang, Y.-C., Teh, K.C., Li, K.H.: 'Secure communication over MISO cognitive radio channels', *IEEE Trans. Wirel. Commun.*, 2010, **9**, (4), pp. 1494–1502

14 Pei, Y., Liang, Y.-C., Teh, K.C., Li, K.H.: 'Secure communication in multiantenna cognitive radio networks with imperfect channel state information', *IEEE Trans. Signal Process.*, 2011, **59**, (4), pp. 1683–1693

15 Lai, L., El Gamal, H.: 'The relay-eavesdropper channel: cooperation for secrecy', *IEEE Trans. Inf. Theory*, 2008, **54**, (9), pp. 4005–4019

16 Barros, J., Rodrigues, M.D.: 'Secrecy capacity of wireless channels'. IEEE Int. Symp. on Information Theory, Seattle, USA, July 2006, pp. 356–360

17 Krikidis, I., Thompson, J.S., McLaughlin, S.: 'Relay selection for secure cooperative networks with jamming', *IEEE Trans. Wirel. Commun.*, 2009, **8**, (10), pp. 5003–5011

18 Gradshteyn, I.S., Ryzhik, I.M.: 'Table of integrals, series, and products' (Academic Press, 2000, 6th edn.)

19 Galambos, J.: 'The asymptotic theory of extreme order statistics' (Krieger Pub. Co., 1987, 2nd edn.)

20 Miller, S., Childers, D.: 'Probability and random processes: with applications to signal processing and communications' (Elsevier Academic Press, 2004)

9 Appendix 1

9.1 Asymptotic secrecy outage probability of OS (one eavesdropper)

We consider the high SNR values in which all the relay nodes can decode the source information correctly.

From (9) to (13), the secrecy outage probability, considering high SNR, can be written as

$$P_{\text{sop}} = \Pr\left\{ \max_{R \in S_{\text{relays}}} \frac{|h_{\text{SD}}|^2 + |h_{\text{RD}}|^2}{|h_{\text{SE}}|^2 + |h_{\text{RE}}|^2} < \beta \right\}$$
$$\Pr(IN_{\text{p}}^R \le \Gamma) + \Pr(IN_{\text{p}}^R > \Gamma) \qquad (38)$$

Define $\beta = 2^{2R_{\text{s}}}$

$\therefore h_{ij}$ are Rayleigh random variables, $|h_{ij}|^2$ are exponential random variables with parameter λ.

$$f_{X_1}(x_1) = \lambda \mathrm{e}^{-\lambda x_1} \quad \text{PDF of the } |h_{ij}|^2 \tag{39}$$

$$F_{X_1}(x_1) = 1 - \mathrm{e}^{-\lambda x_1} \quad \text{CDF of the } |h_{ij}|^2 \tag{40}$$

Let $X \triangleq |\mathrm{h}_{\mathrm{SD}}|^2 + |h_{\mathrm{RD}}|^2$, $Y \triangleq |h_{\mathrm{SE}}|^2 + |h_{\mathrm{RE}}|^2$

If X_1 and X_2 are two i.i.d. exponential random variables with parameter λ, the probability density function (PDF) of the new random variable $X = X_1 + X_2$ can be defined as

$$f_X(x) = \int_{-\infty}^{+\infty} f_{X_1}(x - x_2) f_{X_2}(x_2)\,\mathrm{d}x_2$$

Therefore the PDF and cumulative distribution function (CDF) of the random variable X are given by

$$f_X(x) = \lambda^2 x\,\mathrm{e}^{-\lambda x} \tag{41}$$

$$F_X(x) = 1 - \mathrm{e}^{-\lambda x}(1 + \lambda x) \tag{42}$$

The random variable Y is the same distribution.

$$f_Y(y) = \lambda^2 y\,\mathrm{e}^{-\lambda y} \tag{43}$$

$$F_Y(y) = 1 - \mathrm{e}^{-\lambda y}(1 + \lambda y) \tag{44}$$

Define $Z \triangleq (X/Y)$

From (39)–(44), we can compute the following probability

$$\begin{aligned}\Pr(Z < \beta) &= \int_0^{\infty}\int_0^{\beta y} f_Y(y) f_X(x)\,\mathrm{d}x\,\mathrm{d}y \\ &= \int_0^{\infty} [1 - \mathrm{e}^{-\lambda\beta y}(1 + \lambda\beta y)]\lambda^2 y \mathrm{e}^{-\lambda y}\,\mathrm{d}y\end{aligned} \tag{45}$$

From [18]

$$\int x^n \mathrm{e}^{cx}\,\mathrm{d}x = \frac{1}{c} x^n \mathrm{e}^{cx} - \frac{n}{c}\int x^{n-1}\mathrm{e}^{cx}\,\mathrm{d}x \tag{46}$$

Therefore

$$\therefore \Pr(Z < \beta) = \left[1 - \frac{1}{(1+\beta)^2} - \frac{2\beta}{(1+\beta)^3}\right] \tag{47}$$

Note that there are N different realisations of the random variable Z, which correspond to N different selections of the relay node. It is clear from (38) that these random variables are dependent. Finding the order statistics of dependent random variables requires the joint PDF of the random variables [19], which is intractable in our case. Therefore we assume independent random variables and the obtained asymptotic secrecy outage probability. The outage probability, then, using order statistics [20], is derived as

Define T as the maximum of N random variables $Z_1, Z_2, \ldots, Z_N$

Then $F_T(t) = \Pr(Z_1 \le t, Z_2 \le t, \ldots, Z_N \le t)$

Therefore the first term in (38) can be written as

$$\therefore \Pr(\max_{i \in N}(Z_i) < \beta) = \left[1 - \frac{1}{(1+\beta)^2} - \frac{2\beta}{(1+\beta)^3}\right]^N \tag{48}$$

w.r.t

$\Pr(IN_p^R < \Gamma)$

$$IN_p^R = N_0 + P_S|h_{\mathrm{SP}}|^2 + P_R|h_{\mathrm{RP}}|^2 \tag{49}$$

Under the assumption of high SNR and $P = P_S = P_R$.

Define $G = |h_{\mathrm{SP}}|^2 + |h_{\mathrm{RP}}|^2$, where $|h_{ij}|^2$ are exponential random variables with parameter λ as in (39), the PDF of the random variable G is given by

$$f_G(g) = \lambda^2 g\mathrm{e}^{-\lambda g}$$

For the random variable G, which multiplies by constant P, the distribution of the new random variable is given by

$$Q = PG$$

$$\begin{aligned} f_Q(q) &= \frac{\lambda^2}{P^2} q\mathrm{e}^{-(\lambda q/P)} \\ F_Q(q) &= 1 - \mathrm{e}^{-(\lambda q/P)}\left[\frac{\lambda q}{P} + 1\right]\end{aligned} \tag{50}$$

From (49) and (50)

$$\therefore \Pr(IN_{\mathrm{p}}^R \le \Gamma) = 1 - \mathrm{e}^{(-\lambda/P)\Gamma}\left[\frac{\lambda}{P}\Gamma + 1\right] \tag{51}$$

The outage probability, then, using (48) and (51), is given by

$$\begin{aligned} P_{\mathrm{sop}} = &\left[1 - \frac{1}{(1+\beta)^2} - \frac{2\beta}{(1+\beta)^3}\right]^N \left[1 - \mathrm{e}^{(-\lambda/P)\Gamma}\left(\frac{\lambda}{P}\Gamma + 1\right)\right] \\ &+ \left[\mathrm{e}^{(-\lambda/P)\Gamma}\left(\frac{\lambda}{P}\Gamma + 1\right)\right]\end{aligned} \tag{52}$$

10 Appendix 2

10.1 *Asymptotic secrecy outage probability of OS (multiple eavesdroppers)*

From (16)–(18), the outage probability considering high SNR is given by

$$\begin{aligned} P_{\mathrm{sop}} = \Pr&\left\{\max_{R \in S_{\mathrm{relays}}}\left\{\frac{|h_{SD}|^2 + |h_{RD}|^2}{\max_{E_m \in S_{\mathrm{evs}} \forall m}\{|h_{SE_m}|^2 + |h_{RE_m}|^2\}}\right\} < \beta\right\} \\ &\Pr(IN_p^R \le \Gamma) + \Pr(IN_p^R > \Gamma)\end{aligned} \tag{53}$$

Let $X \triangleq |h_{\mathrm{SD}}|^2 + |\mathrm{h}_{\mathrm{RD}}|^2$, $Y \triangleq \max_{E_{\mathrm{m}} \in S_{\mathrm{evs}}}\{|h_{\mathrm{SE_m}}|^2 + |h_{\mathrm{RE_m}}|^2\}$

The PDF and CDF of the random variable X are given by

$$f_X(x) = \lambda^2 x\mathrm{e}^{-\lambda x} \tag{54}$$

$$F_X(x) = 1 - \mathrm{e}^{-\lambda x}(1 + \lambda x) \tag{55}$$

Using order statistics, the PDF and CDF of the random variable Y are given by

$$f_Y(y) = M(\lambda^2 y\mathrm{e}^{-\lambda y})[1 - \mathrm{e}^{-\lambda y}(1 + \lambda y)]^{M-1} \tag{56}$$

$$F_Y(y) = [1 - \mathrm{e}^{-\lambda y}(1 + \lambda y)]^M \tag{57}$$

Define new random variable $Z \triangleq (X/Y)$

Let us compute the following probability using (54)–(57)

$$\begin{aligned}\Pr(Z < \beta) &= \int_0^{\infty}\int_0^{\beta y} f_Y(y) f_X(x)\,\mathrm{d}x\,\mathrm{d}y \\ &= M\int_0^{\infty}[1-\mathrm{e}^{-\lambda\beta y}(1+\lambda\beta y)](\lambda^2 y\mathrm{e}^{-\lambda y}) \\ &\quad\times[1-\mathrm{e}^{-\lambda y}(1+\lambda y)]^{M-1}\,\mathrm{d}y \qquad (58)\end{aligned}$$

There are N different realisations of the random variable Z. Therefore we assume independent random variables and obtained asymptotic secrecy outage probability.

$$\therefore \Pr(\max_{i\in N}(Z_i) < \beta) = \left[M\int_0^{\infty}[1-\mathrm{e}^{-\lambda\beta y}(1+\lambda\beta y)] (\lambda^2 y\mathrm{e}^{-\lambda y})[1-\mathrm{e}^{-\lambda y}(1+\lambda y)]^{M-1}\right]^N \qquad (59)$$

With respect to $\Pr(IN_p^R \le \Gamma)$, it is derived in Appendix 1.

Therefore using (51) and (59), the outage probability is given by (see (60))

11 Appendix 3

11.1 Asymptotic secrecy outage probability of OS (multiple PUs)

From (21)–(23), the outage probability considering high SNR is given by

$$P_{\mathrm{sop}} = \Pr\left\{\max_{R\in S_{\mathrm{relays}}}\left\{\frac{|h_{\mathrm{SD}}|^2+|h_{\mathrm{RD}}|^2}{\max_{E_{\mathrm{m}}\in S_{\mathrm{evs}}\forall\mathrm{m}}\{|h_{\mathrm{SE_m}}|^2+|h_{\mathrm{RE_m}}|^2\}}\right\} < \beta\right\} \Pr(\max_{p_l\in S_{PU}}\{IN_{p_l}^R\} \le \Gamma) + \Pr(\max_{p_l\in S_{PU}}\{IN_{p_l}^R\} > \Gamma) \qquad (61)$$

The first term of (61) is already derived in Appendix 2 (see (62))

Let us compute the following probability

$$\Pr(\max_{p_l\in S_{PU}}\{IN_{p_l}^R\} \le \Gamma)$$

$$IN_{p_l}^R = N_0 + P_S|h_{Sp_l}|^2 + P_R|h_{Rp_l}|^2, \quad l = 1, 2, \ldots, L \qquad (63)$$

With the same assumption in Appendix 1

$$G = |h_{\mathrm{SP}}|^2 + |h_{\mathrm{RP}}|^2$$

$$f_G(g) = \lambda^2 g\mathrm{e}^{-\lambda g}$$

Define new random variable $Q = PG$, The CDF of random variable Q are given by

$$F_Q(q) = 1 - \mathrm{e}^{-(\lambda q/P)}\left[\frac{\lambda q}{P} + 1\right] \qquad (64)$$

Note that there are L different realisations of the random variable Q. Using order statistics; we can derive the following probability

$$\Pr(\max_{p_l\in S_{PU}}\{IN_{p_l}^R\} \le \Gamma) = \left[1 - \mathrm{e}^{(-\lambda/P)\Gamma}\left(\frac{\lambda}{P}\Gamma + 1\right)\right]^L \qquad (65)$$

Therefore from (62) and (65), the outage probability is given by (see (66))

$$\begin{aligned}P_{\mathrm{sop}} \simeq{}& \left[M\int_0^{\infty}[1-\mathrm{e}^{-\lambda\beta y}(1+\lambda\beta y)](\lambda^2 y\mathrm{e}^{-\lambda y})[1-\mathrm{e}^{-\lambda y}(1+\lambda y)]^{M-1}\right]^N \\ &\times\left[1-\mathrm{e}^{(-\lambda/P)\Gamma}\left(\frac{\lambda}{P}\Gamma+1\right)\right] + \left[\mathrm{e}^{(-\lambda/P)\Gamma}\left(\frac{\lambda}{P}\Gamma+1\right)\right] \qquad (60)\end{aligned}$$

$$\begin{aligned}&\Pr\left\{\max_{R\in S_{\mathrm{relays}}}\left\{\frac{|h_{\mathrm{SD}}|^2+|h_{\mathrm{RD}}|^2}{\max_{E_{\mathrm{m}}\in S_{\mathrm{evs}}\forall\mathrm{m}}\{|h_{SE_{\mathrm{m}}}|^2+|h_{\mathrm{RE_m}}|^2\}}\right\} < \beta\right\} \\ &= \left[M\int_0^{\infty}[1-\mathrm{e}^{-\lambda\beta y}(1+\lambda\beta y)](\lambda^2 y\mathrm{e}^{-\lambda y})[1-\mathrm{e}^{-\lambda y}(1+\lambda y)]^{M-1}\,\mathrm{d}y\right]^N \qquad (62)\end{aligned}$$

$$\begin{aligned}P_{\mathrm{sop}} \simeq{}& \left[M\int_0^{\infty}[1-\mathrm{e}^{-\lambda\beta y}(1+\lambda\beta y)](\lambda^2 y\mathrm{e}^{-\lambda y})[1-\mathrm{e}^{-\lambda y}(1+\lambda y)]^{M-1}\right]^N \\ &\times\left[1-\mathrm{e}^{(-\lambda/P)\Gamma}\left(\frac{\lambda}{P}\Gamma+1\right)\right]^L + \left[1-\left(1-\mathrm{e}^{(-\lambda/P)\Gamma}\left(\frac{\lambda}{P}\Gamma+1\right)\right)^L\right] \qquad (66)\end{aligned}$$

12 Appendix 4

12.1 Asymptotic secrecy outage probability of DT (one eavesdropper)

From (26) and (27), the secrecy outage probability, considering high SNR, can be written as

$$P_{\text{sop}} = \Pr\left\{\frac{|h_{\text{SD}}|^2}{|h_{\text{SE}}|^2} < \alpha\right\}\Pr(IN_{\text{p}} \le \Gamma) + \Pr(IN_{\text{p}} > \Gamma) \quad (67)$$

Let $X \triangleq |h_{\text{SD}}|^2$, $Y \triangleq |h_{\text{SE}}|^2$

The PDF and CDF of the random variable X are given by

$$f_X(x) = \lambda \mathrm{e}^{-\lambda x} \quad (68)$$

$$F_X(x) = 1 - \mathrm{e}^{-\lambda x} \quad (69)$$

The distribution of random variable Y is the same for X.

Define new random variable $Z \triangleq (X/Y)$

Let us compute the following probability using (68) and (69)

$$\begin{aligned}\Pr(Z < \alpha) &= \int_0^\infty F_X(\alpha y) f_Y(y)\,\mathrm{d}y \\ &= 1 - \frac{1}{1+\alpha} = \frac{\alpha}{1+\alpha}\end{aligned} \quad (70)$$

w.r.t.

$\Pr(IN_{\text{p}} < \Gamma)$

$$IN_{\text{p}}^R = N_0 + P_S|h_{\text{SP}}|^2 \quad (71)$$

Let

$$Q = P_{\text{s}}|h_{\text{SP}}|^2$$

The PDF of the random variable Q are given by

$$f_Q(q) = \frac{\lambda}{P_{\text{s}}}\mathrm{e}^{-(\lambda q/P_s)} \quad (72)$$

At high SNR and using (72)

$$\therefore \Pr(IN_{\text{p}} \le \Gamma) = 1 - \mathrm{e}^{(-\lambda/P_s)\Gamma} \quad (73)$$

Using (70) and (73), the outage probability is given by

$$P_{\text{sop}} \simeq \frac{\alpha}{1+\alpha}[1 - \mathrm{e}^{(-\lambda/P_s)\Gamma}] + [\mathrm{e}^{(-\lambda/P_s)\Gamma}] \quad (74)$$

13 Appendix 5

13.1 Asymptotic secrecy outage probability of DT (multiple eavesdroppers)

From (29), the outage probability is given by

$$P_{\text{sop}} = \Pr\left\{\max_{R\in S_{\text{relays}}}\left\{\frac{|h_{\text{SD}}|^2}{\max_{E_{\text{m}}\in S_{\text{evs}}\forall m}\{|h_{\text{SE}_{\text{m}}}|^2\}}\right\} < \alpha\right\} \quad (75)$$

$$\Pr(IN_p \le \Gamma) + \Pr(IN_{\text{p}} > \Gamma)$$

Let $X \triangleq |h_{\text{SD}}|^2$, $K \triangleq |h_{\text{SE}_{\text{m}}}|^2$ and $Y \triangleq \max_{m=1,\ldots\ldots,M}\{K_m\}$

The PDF and CDF of the random variable X are given by:

$$f_X(x) = \lambda \mathrm{e}^{-\lambda x} \quad (76)$$

$$F_X(x) = 1 - \mathrm{e}^{-\lambda x} \quad (77)$$

The distribution of random variable K is the same for X.

Using order statistics

$$F_Y(y) = \Pr(K_1 \le y, K_2 \le y, \ldots, K_N \le y)$$

We assume independent random variables

$$\therefore F_Y(y) = \Pr(K_1 \le y)\Pr(K_2 \le y)\cdots\Pr(K_N \le y)$$

Therefore the PDF and CDF of the random variable Y are given by

$$f_Y(y) = M(\lambda \mathrm{e}^{-\lambda y})[1 - \mathrm{e}^{-\lambda y}]^{M-1} \quad (78)$$

$$F_Y(y) = [1 - \mathrm{e}^{-\lambda y}]^M \quad (79)$$

Define random variable $Z \triangleq (X/Y)$

Let us compute the following probability using (76)–(79)

$$\begin{aligned}\Pr(Z < \alpha) &= \int_0^\infty F_X(\alpha y) f_Y(y)\,\mathrm{d}y \\ &= M\int_0^\infty [1 - \mathrm{e}^{-\lambda\alpha y}](\lambda \mathrm{e}^{-\lambda y})[1 - \mathrm{e}^{-\lambda y}]^{M-1}\,\mathrm{d}y\end{aligned} \quad (80)$$

With respect to $\Pr(IN_{\text{p}} \le \Gamma)$, it is derived in Appendix 4.

Therefore the outage probability is given by

$$P_{\text{sop}} \simeq \left[M\int_0^\infty [1 - \mathrm{e}^{-\lambda\alpha y}](\lambda e^{-\lambda y})[1 - \mathrm{e}^{-\lambda y}]^{M-1}\,\mathrm{d}y\right]$$

$$[1 - \mathrm{e}^{(-\lambda/P_s)\Gamma}] + [\mathrm{e}^{(-\lambda/P_s)\Gamma}] \quad (81)$$

14 Appendix 6

14.1 Asymptotic secrecy outage probability of DT (multiple PUs)

The outage probability of this case is given by

$$P_{\text{sop}} = \Pr\left\{\max_{R\in S_{\text{relays}}}\left\{\frac{|h_{\text{SD}}|^2}{\max_{E_m\in S_{\text{evs}}\forall m}\{|h_{SE_m}|^2\}}\right\} < \alpha\right\} \quad (82)$$

$$\Pr(\max_{p_l\in S_{PU}}\{IN_{p_l}\} \le \Gamma) + \Pr(\max_{p_l\in S_{PU}}\{IN_{p_l}\} > \Gamma)$$

The first term of (82) is already derived in Appendix 5

doi: 10.1049/iet-com.2011.0638

$$\Pr\left\{\max_{R\in S_{\text{relays}}}\left\{\frac{|h_{\text{SD}}|^2}{\max\limits_{E_m\in S_{\text{evs}}\forall m}\{|h_{SE_m}|^2\}}\right\}<\alpha\right\}$$
$$= M\int_0^\infty [1-\mathrm{e}^{-\lambda\alpha y}](\lambda\mathrm{e}^{-\lambda y})[1-\mathrm{e}^{-\lambda y}]^{M-1}\,\mathrm{d}y \tag{83}$$

With respect to the remaining parts of the (82)

Let $X \triangleq \max_{P_l\in S_{PU}}\{|h_{SP_l}|^2\}$Using order statistics, the CDF of the random variable X are given by

$$F_X(x) = [1-\mathrm{e}^{-x(\lambda/P_s)}]^L \tag{84}$$

Using (83) and (84), the asymptotic secrecy outage probability is denoted by

$$P_{\text{sop}} \simeq \left[M\int_0^\infty [1-\mathrm{e}^{-\lambda\alpha y}](\lambda e^{-\lambda y})[1-\mathrm{e}^{-\lambda y}]^{M-1}\,\mathrm{d}y\right]$$
$$[1-\mathrm{e}^{(-\lambda/P_s)\Gamma}]^L + [1-(1-\mathrm{e}^{(-\lambda/P_s)\Gamma})^L] \tag{85}$$

15 Appendix 7

15.1 Asymptotic secrecy outage probability of CS

$$P_{\text{sop}} = \Pr\left\{\frac{|h_{\text{SD}}|^2 + \max\limits_{R\in S_{\text{relays}}}|h_{\text{RD}}|^2}{|h_{\text{SE}}|^2+|\mathrm{h}_{\text{RE}}|^2} < \beta\right\}$$
$$\Pr(IN_p^R \le \Gamma) + \Pr(IN_p^R > \Gamma) \tag{86}$$

For the fist part of (86)

$|h_{ij}|^2$ are exponential random variables with parameter λ.

$$f_{X_1}(x_1) = \lambda\mathrm{e}^{-\lambda x_1} \quad \text{PDF of the } |h_{ij}|^2 \tag{87}$$

$$F_{X_1}(x_1) = 1-\mathrm{e}^{-\lambda x_1} \quad \text{CDF of the } |h_{ij}|^2 \tag{88}$$

Let $X \triangleq |h_{\text{SD}}|^2 + \max_{R\in S_{\text{relays}}}|h_{\text{RD}}|^2$, $Y \triangleq |h_{\text{SE}}|^2 + |h_{\text{RE}}|^2$

Let $T \triangleq \max_{R\in S_{\text{relays}}}|h_{\text{RD}}|^2$

Using order statistics, the CDF of the random variable T are given by

$$F_T(t) = [1-\mathrm{e}^{-\lambda t}]^N \tag{89}$$

Therefore the PDF of the random variable X is derived as

$$f_X(x) = \int_0^x N\lambda^2\mathrm{e}^{-\lambda x}(1-\mathrm{e}^{-\lambda t})^{N-1}\,\mathrm{d}t$$

In order to solve this integration, we will use the binomial expansion theorems [18]

$$f_X(x) = N\lambda^2\mathrm{e}^{-\lambda x}\int_0^x\sum_{k=0}^{N-1}\binom{N-1}{k}(-\mathrm{e}^{-\lambda t})^k\,\mathrm{d}t$$
$$= N\lambda^2\mathrm{e}^{-\lambda x}\int_0^x\sum_{k=0}^{N-1}\binom{N-1}{k}(-1)^k\mathrm{e}^{-\lambda kt}\,\mathrm{d}t$$
$$f_X(x) = N\lambda^2\mathrm{e}^{-\lambda x}\sum_{k=0}^{N-1}\binom{N-1}{k}(-1)^k\frac{1}{k}(\mathrm{e}^{-\lambda kx}-1)^k \tag{90}$$

The PDF of the random variable Y, as in the pervious appendix, is given by

$$f_Y(y) = \lambda^2 y\mathrm{e}^{-\lambda y} \tag{91}$$

Define $Z \triangleq (X/Y)$

From (90) and (91), we can compute the following probability (see equation at the bottom of the page)

Therefore (see (92))

From the pervious appendix

$$\Pr(IN_p^R \le \Gamma) = 1-\mathrm{e}^{(-\lambda/P)\Gamma}\left[\frac{\lambda}{P}\Gamma+1\right] \tag{93}$$

Using (92) and (93), the asymptotic secrecy outage probability of CS is denoted by (see (94))

$$\Pr(Z<\beta) = \Pr(X<\beta Y) = \int_0^\infty\int_0^{\beta y} f_Y(y)f_X(x)\,\mathrm{d}x\,\mathrm{d}y$$
$$= \int_0^\infty\int_0^{\beta y}\lambda^2 ye^{-\lambda y}N\lambda^2\mathrm{e}^{-\lambda x}\sum_{k=0}^{N-1}\binom{N-1}{k}(-1)^k\frac{1}{k}(\mathrm{e}^{-\lambda kx}-1)^k\,\mathrm{d}x\,\mathrm{d}y$$

$$\Pr(Z<\beta) = N\sum_{k=0}^{N-1}\binom{N-1}{k}(-1)^k\frac{1}{k}\left[\frac{1}{(k+1)(1+\beta+k\beta)^2}-\frac{1}{(1+\beta)^2}+\frac{k}{k+1}\right] \tag{92}$$

$$P_{\text{sop}} \simeq \left[N\sum_{k=0}^{N-1}\binom{N-1}{k}(-1)^k\left(\frac{1}{k(k+1)(1+\beta+k\beta)^2}-\frac{1}{k(1+\beta)^2}+\frac{1}{k+1}\right)\right]$$
$$\times\left[1-\mathrm{e}^{(-\lambda/P)\Gamma}\left(\frac{\lambda}{P}\Gamma+1\right)\right]+\left[\mathrm{e}^{(-\lambda/P)\Gamma}\left(\frac{\lambda}{P}\Gamma+1\right)\right] \tag{94}$$