Secure transmission in the random cognitive radio networks with secrecy guard zone and artificial noise

Yueming Cai, Xiaoming Xu, Weiwei Yang

College of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, People’s Republic of China
E-mail: xiaomingxu.plaust@gmail.com

Abstract: The authors study the secure transmission design in random cognitive radio networks where the primary users, the secondary users and the eavesdroppers are randomly distributed according to Poisson point processes. Centring on this scenario, the authors propose a simple and decentralised secure transmission scheme by jointly incorporating the secrecy guard zone and artificial noise. In particular, this transmission scheme helps to enhance secrecy performance via differentiating between secondary transmitters in accordance with the eavesdropping environment. Then they analyse the connection outage and secrecy outage performance of the secondary network, based on which they obtain the closed-form expression of the secrecy throughput. They further determine the optimal transmission power of the secondary transmitters and the optimal power allocation between the information-bearing signal and the artificial noise. Numerical results show how the system parameters affect the achievable maximum secrecy throughput, the optimal transmission power and the optimal power allocation between the information-bearing signal and the artificial noise.

1 Introduction

With the rapid adoption of wireless devices, there is an unprecedented growth in the demand for radio spectrum in 5G mobile communication systems. To address the conflict between spectrum scarcity and spectrum underutilisation, cognitive radio (CR) has been regarded as a promising technology to solve the problem of inefficient spectrum usage in 5G wireless networks, like the cognitive cellular networks. Nevertheless, allowing the spectrum sharing in the cognitive radio network (CRN) is not without drawbacks. The coexistence of licensed and unlicensed users in the same spectrum makes the data transmissions more vulnerable to security attacks [1] compared with the traditional wireless networks. Thus, the secrecy transmission in CRNs becomes a critical issue. As a powerful complement to the traditional cryptographic techniques [2], the physical layer security [3] has been proposed to achieve perfect secrecy without requiring key distribution and complex encryption/decryption algorithms. The fundamental principle of physical layer security is to exploit intrinsic properties of communication channels to restrict the amount of confidential messages that is possibly intercepted by unauthorised receivers [4].

In the past few years, there has been increasing interest in the security issue of CRNs, due to the rapid growing amount of private and sensitive data transmitted in the limited spectrum. From an information-theoretic perspective, the performance of physical layer security in CRNs was studied in, e.g. [5–7]. More recently, various signal processing techniques and system design protocols were proposed to improve the secrecy performance of the CRNs [8, 9]. However, the aforementioned works did not take a random network topology into account when analysing the secrecy performance of the CRNs. In other words, they only concerned a small number of legitimate nodes and eavesdroppers and assumed that their locations are exactly known and fixed at all times. In a practical network, the location and the number of nodes are usually randomised due to terrain features, site availability and local coverage requirements. In future 5G cellular networks with heterogeneous and smaller cells, the randomness of macro-cell BS locations or small-cell BS locations is expected to increase. Moreover, a passive eavesdropper would not reveal its channel state information (CSI) or location information to the legitimate nodes. Therefore, such concerns and assumptions are not always valid.

With respect to the random topology nature, stochastic geometry model enables a wide range of analytical studies. The performance and design of CRNs with random topology was studied using stochastic geometry in [10, 11]. Furthermore, the stochastic geometry modelling has been shown to yield tractable results for secrecy performance of wireless networks. Chae et al. [12] investigated the optimal utilisation of artificial noise for secrecy communication. Zhou et al. [13] introduced secrecy transmission capacity to quantify the achievable rate of successful transmission of secret message per unit area and exploited secrecy guard zone to improve the network throughput. Zheng et al. [14] studied the secure multi-antenna transmission with artificial noise under slow fading channels coexisting with randomly located eavesdroppers. However, the results in [12–14] were only limited in one single link or one single network. Shu et al. [15] characterised the secrecy capacity of primary network considering a Poisson CR network, but only focused on the effect of large-scale fading on the secrecy performance ignoring that of small-scale fading. Recently, Win et al. [16] showed that cognitive interference was beneficial for the security of CRNs, while proposed corresponding interference engineering strategies.

In this paper, we study the secure transmission in a random CRN where the primary users (PUs), the secondary users (SUs) and eavesdroppers are randomly distributed according to Poisson point processes (PPPs). The main contribution of this paper can be summarised as follows.

For transmission design, we propose a simple and decentralised transmission scheme to safeguard the secure transmission in the secondary network against the eavesdropping. We jointly
incorporate the secrecy guard zone and the artificial noise in the transmission scheme. Specifically, we exploit the secrecy guard zone centred at each secondary transmitter (SU-Tx) to classify all the SU-Txs into two types: the first-type SU-Txs are the ones in whose secrecy guard zone there exists no eavesdropper and the second-type SU-Txs are the ones in whose secrecy guard zone there exist one or more eavesdroppers. We differentiate between the first-type SU-Txs and the second-type SU-Txs: the first-type SU-Txs only transmit information-bearing signal while the second-type SU-Txs transmit artificial noise along with information-bearing signal. Our analysis highlights that introducing the secrecy guard zone provides better security performance, and the artificial noise performs an additional interference to insert a control between the reliability and security. For information-theory analysis, we derive the secrecy outage probabilities (SOPs) of the first-type and the second-type secondary links to characterise the security performance, the connection outage probabilities (COPs) of the primary link, the first-type and the second-type secondary links to characterise the reliability performance. We find that both the transmission power of the SU-Txs and the artificial noise give positive and negative effects on the reliability and security performance. Specifically, the transmission power of the SU-Txs arouses a tradeoff between the reliability performance and the security performance of both the first-type and second-type secondary links. The artificial noise acts as an additional noise to arouse a tradeoff between the reliability performance and the security performance of the second-type secondary links. Finally, the overall performance of the secondary network is measured by the secrecy throughput defined as the achievable average rate of secure and reliable transmissions per unit area.

We further optimise the design of the transmission scheme. To this end, we study the optimisation problem of achieving the maximal secrecy throughput of the secondary network with respect to the transmission power and power fraction factor with given COP and SOP constraints. We first study the conditions on the constraints under which a non-zero secrecy throughput is achievable. We then obtain the closed-form solutions of the optimal power fraction factor \( \kappa \) for information-bearing signal with given transmission power \( P_S \) and numerically find the optimal transmission power \( P_S \) that maximise the secrecy throughput. Numerical results show how the system parameters affect the maximal value of the secrecy throughput, the optimal transmission power and the optimal power allocation between the artificial noise and the information-bearing signal. It is also verified that our proposed transmission scheme can provide an enhancement of the secrecy throughput.

The rest of this paper is organised as follows. Section 2 gives the network descriptions and performance metrics. Sections 3 and 4 evaluate and optimise the transmission protocols, respectively. Section 5 presents the numerical results. Finally, Section 6 concludes the paper.

2 System model

2.1 Network descriptions

As Fig. 1 illustrated, we consider an underlaid CRN consisting of primary transmitter–receiver pairs, secondary transmitter–receiver pairs and a set of eavesdroppers over a large two-dimensional space. The secondary network shares ratio frequency channels with the primary networks while satisfying the primary network outage constraint. In addition, the eavesdroppers try to intercept the secret message transmission of the secondary network.

The distribution of the primary transmitters (PU-Txs) follows a homogeneous PPP \( \Phi_P \) with spatial density \( \lambda_P \). The distribution of the SU-Txs also follows a PPP \( \Phi_S \) with spatial density \( \lambda_S \). Moreover, the distribution of the eavesdroppers follows another PPP \( \Phi_E \) with density \( \lambda_E \). Different from the deterministic model, the spatial PPP introduces total randomness for the node deployment, and only the node density variable is required to characterise this stochastic process. In addition, the randomness introduced by the PPP-based model has the advantage of being tractable in performance analysis, since it often leads to closed-form results on statistical analysis for signal attenuation laws [17].

Some detail settings and assumptions are given below:

(a) All the nodes are assumed with single antenna due to size, cost or hardware limitations, e.g. handsets and sensors. Each PU-Tx or SU-Tx communicates with one intended receiver with transmission power \( P_P \) or \( P_S \). The associated primary receiver (PU-Rx) or secondary receiver (SU-Rx) is assumed to be located at a fixed (It is noted that other distance distributions can be easily incorporated into the framework.) distance \( l_P \) or \( l_S \) away from the transmitter with isotropic directions. In addition, each transmitter is assumed to have no CSI of the intended link due to the lack of feedback.

(b) The secondary links are assumed to be eavesdropped in the model. The eavesdroppers are assumed to be passive and thus, they do not feed any CSI of the eavesdropping links back to the SU-Txs. In addition, the eavesdroppers do not collude with each other and hence, must decode the confidential message individually. Therefore, the security level is determined by the eavesdropper with the highest received power.

(c) To fight against eavesdropping, each SU-Tx adopts Wyner code [3] to encode the data before transmission. Since each SU-Tx does not have any CSI of the legitimate link and the eavesdropping link, a constant secret message rate \( R_s \) is preferred. By arbitrarily selecting codeword transmission rate \( R_t \) (\( R_t > R_s \)), a Wyner’s codebook can be constructed, where a codebook of rate \( R_t \) for secret message is nested in a codebook of rate \( R_s \) for transmitted codewords.

To enhance the secure transmission of the secondary network, we propose a simple and decentralised transmission scheme, which jointly incorporates the secrecy guard zone and artificial noise. We assume that the SU-Txs are able to detect the existence of eavesdroppers within a finite range (A transmitter can detect the existence of eavesdroppers by scanning nearby devices with the help of various detecting devices such as a metal detector, X-ray detector, evolved heat detector or the leaked local oscillator power detector [18] before transmission.). As per the mechanism of secrecy guard zone [13, 19], we model this range as a disk with radius \( D \) centred at each SU-Tx. Through the secrecy guard zones, we classify all the SU-Txs into two types: the first-type SU-Txs are the ones in whose secrecy guard zone there exist no eavesdropper; the second-type SU-Txs are the ones in whose secrecy guard zone there exist one or more eavesdroppers. Obviously, the second-type SU-Txs are under serious security threats. In order to enhance the security, the second-type SU-Tx sends artificial Gaussian noise along with information-bearing signal. Specifically, the second class SU-Tx transmits the information-bearing signal with power \( \kappa P_S \) and transmits the artificial noise with power \( (1 - \kappa)P_S \) simultaneously by applying

---

**Fig. 1** Illustration of a random CRN where primary, secondary and eavesdropper nodes are randomly distributed according to PPPs. (The squares are the primary nodes, the triangles are the eavesdroppers, the black circles are the first-type secondary nodes and the red circles are the second-type secondary nodes. Besides, the grey disks are the secrecy guard zones.)
superposition coding [20], where $\kappa \in (0, 1]$ is the power allocation factor for the information-bearing signal. The first-type SU-Txs still only transmit information-bearing signal with power $P_s$. Since each SU-Tx only needs the local information about the existence of eavesdroppers, the proposed transmission scheme can be applied in a decentralised way. The set of the first-type SU-Tx locations is denoted by $\Phi^0_S$ with the density of $\lambda^0_S = \lambda_S \exp(-\pi D^2 \lambda_S)$, where the exponential term is the probability of no eavesdropper located inside the secrecy guard zone of an arbitrary SU-Tx. The set of the second-type SU-Tx locations is denoted by $\Phi^0_{II}$ with the density of $\lambda^0_{II} = \lambda_{II} [1 - \exp(-\pi D^2 \lambda_{II})]$.

It is worth mentioning that similar secrecy guard zone transmission schemes have been previously studied in, e.g. [13, 21] and the references therein. In these works, the transmission of information-bearing signal only happens at the transmitter where there is no eavesdropper inside the secrecy guard zone. Different from the existing works, both the first-type SU-Txs and the second-type SU-Txs transmit information-bearing signal in our proposed transmission scheme. We further exploit the artificial noise to insert an intelligence control of the positive and the negative effects for the second-type SU-Txs.

Note that since spectrum-sharing networks can be regarded as interference-limited environments, the thermal noise is ignored and the signal-to-interference ratio (SIR) is used for the sake of simplicity [22]. Let $G_a$ and $L_a$ denote the Rayleigh fading channel gain and the distance between node $a$ and node $b$, respectively. Then, the instantaneous SIR received by a PU-Rx $v_0$ from a PU-Tx $u_0$ is given by

$$\gamma_{s} = \frac{P_s G_{v_0 u_0}}{\sum_{i \in \Phi_s} P_s G_{v_0 u_i} + \sum_{j \in \Phi_p} P_p G_{v_0 u_j}}.$$

(1)

The instantaneous SIR received by a SU-Rx $v_1$ from a first-type SU-Tx $u_1$ is given by

$$\gamma_{s}^{(1)} = \frac{P_s G_{v_1 u_1}}{\sum_{i \in \Phi_s} P_s G_{v_1 u_i} + \sum_{j \in \Phi_p} P_p G_{v_1 u_j}}.$$

(2)

Similarly, the instantaneous SIR received by an eavesdropper $e_1$ from the first-type SU-Tx $u_1$ is given by

$$\gamma_{e}^{(1)} = \frac{P_s G_{e_1 u_1}}{\sum_{i \in \Phi_s} P_s G_{e_1 u_i} + \sum_{j \in \Phi_p} P_p G_{e_1 u_j}}.$$

(3)

On the other hand, since the second-type SU-Tx sends artificial noise along with secret message, the instantaneous SIR received by a SU-Rx $v_2$ from a second-type SU-Tx $u_2$ is given by (see (4))

$$\gamma_{s}^{(1)} = \frac{P_s G_{v_2 u_2}}{\sum_{i \in \Phi_s} P_s G_{v_2 u_i} + \sum_{j \in \Phi_p} P_p G_{v_2 u_j}}.$$

(4)

Similarly, the instantaneous SIR received by an eavesdropper $e_2$ from the second-type SU-Tx $u_2$ is given by (see (5))

$$\gamma_{e}^{(1)} = \frac{P_s G_{e_2 u_2}}{\sum_{i \in \Phi_s} P_s G_{e_2 u_i} + \sum_{j \in \Phi_p} P_p G_{e_2 u_j}}.$$

(5)

From the SIR expressions (1)–(5), we find that interferences give both positive and negative impacts on the secure transmission since they degrade not only the received SIR at the legitimate receiver but also the received SIR at the eavesdroppers. It is also shown that for the second-type SU-Tx, the artificial noise acts as an additional interference and asymmetrically amplifies the positive and the negative effects of the interference.

2.2 Performance metric

2.2.1 Connection outage probability: In both primary network and secondary network, if the capacity of the channel from the legitimate transmitter to the legitimate receiver is less than the transmission rate, there will be a connection outage event. The probability of this event happening is referred to as the COP. We denote the COPs of the primary link, the first-type secondary link and the second-type secondary link by $p_{co,P}, p_{co,S}^{(1)}$ and $p_{co,S}^{(II)}$, respectively.

Note that the coexistence of the primary and the secondary networks requires that the secondary network guarantees the predefined outage probability of the primary network, i.e. $p_{co,P} \leq \delta_p$, where $\delta_p$ is the predefined COP constraint of the primary network.

2.2.2 Secrecy outage probability: In secondary network, if the capacity of the channel from the transmitter to one or more eavesdroppers is larger than the rate increment $R_s - R_e$, there will be a secrecy outage event. The probability of this event happening is referred to as the SOP. We denote the SOPs of the first-type secondary link and the second-type secondary link by $p_{so,S}^{(1)}$ and $p_{so,S}^{(II)}$, respectively.

2.2.3 Secrecy throughput: The overall performance of the system is measured by the secrecy throughput taking into account the network density, the security performance and the reliability performance together. We define the secrecy throughput of a network as the product of the transmitter density, the connection probability, the secrecy probability and the secrecy rate, which is given by [23, 24]

$$\eta = \lambda (1 - p_{co})(1 - p_{so})R_s.$$

(6)

where $p_{co}$ and $p_{so}$ are the COP and the SOP of the typical link in the network.

It is worth mentioning that the definition of secrecy throughput in (6) is different from the definition adopted in [25, 26], which quantises the average secrecy rate at which the messages are reliably transmitted. We find that the definition of throughput in [25, 26] does not reflect whether the transmission is secure, and hence it is not very appropriate to characterise the overall performance of the secure transmission. Of course, it is impossible for the receiver to identify which messages are securely transmitted and which messages are leaked in the passive eavesdropping scenario. However, the secrecy throughput definition in our paper is still meaningful since it quantifies the average amount of the reliably and securely transmitted messages and provides the transmitter useful insights for transmission design.

In our work, the secrecy throughput of the whole secondary network is the sum of the secrecy throughput of the first-type SUs and the secrecy throughput of the second-type SUs. Denote $\eta_s^{(1)}$ and $\eta_s^{(II)}$ as the secrecy throughput of the first-type SUs and the second-type SUs. Then, the secrecy throughput of the secondary network is expressed as

$$\eta_s = \eta_s^{(1)} + \eta_s^{(II)} = \sum_{i \in \Phi_s} \left(1 - p_{so,S}^{(1)} \right) \left(1 - p_{so,S}^{(II)} \right) R_s + \lambda_{II} \left(1 - p_{co,S}^{(1)} \right) \left(1 - p_{so,S}^{(II)} \right) R_s,$$

(7)
3 Performance analysis

In this section, we derive the closed-form expressions for the COP, SOP and the secrecy throughput. We first seek to understand the effects of the system parameters on the outage probabilities. Then, we will derive the secrecy throughput of the secondary network. Note that we focus on analysing the performance of typical links since the signal-reception statistics experienced by the other links are the same with that experienced by the typical links, which comes from the stationarity of Poisson process.

3.1 COP analysis

Define a threshold SIR value for connection outage of the typical primary link as \( \theta_{\text{co,p}} = 2R_0 - 1 \), where \( R_0 \) is the transmission rate of the PU-Txs. Then, the COP of the typical primary link is given by

\[
P_{\text{co,p}} = P(\log(1 + \gamma_p) < R_p).
\]

(8)

Considering the random distributions of PU-Txs and SU-Txs, \( P_{\text{co,p}} \) is further expressed as [13]

\[
P_{\text{co,p}} = E_{\Phi_p} \left\{ E_{\Phi_s} \left\{ P_{\text{Tg}}G_{\text{a,p}}/p_{\text{a}} \left( \frac{\nu_p}{\nu_p} + I_0(v_p) \right) < \theta_{\text{co,p}} \right\} \right\} = E_{\Phi_p} \left\{ \exp \left[ -\frac{\theta_{\text{co,p}}}{\nu_p} I_0(v_p) \right] \right\} = L_{\nu_p}(v_p) \frac{\theta_{\text{co,p}}}{\nu_p} L_{\nu_p}(v_p) / \nu_p P_{\text{p}}, \]

(9)

where \( I_0(v_p) = \sum_{v_p \in \nu_p} P_{\text{Tg}}G_{\text{a,p}}/p_{\text{a}} \cdot I_0(v_p) = \sum_{v_p \in \nu_p} P_{\text{Tg}}G_{\text{a,p}}/p_{\text{a}} \cdot L_{\nu_p}(v_p) \) is the Laplace transform of \( I_0(v_p) \) and \( L_{\nu_p}(v_p) \) is the Laplace transform of \( I_0(v_p) \). Since the location sets of the PU-Txs and the SU-Txs follow independent HPPP distributions, the Laplace transforms are known in closed forms [27]. As such, the COP of the typical primary link is given by

\[
P_{\text{co,p}} = 1 - \exp \left[ -\pi_0 \nu_p^2 \theta_{\text{co,p}}^2 (P_{\text{p}} / P_{\text{p}}) ^{2/\nu_p} \lambda_s \right]. \]

(10)

where \( \pi_0 = \Gamma(1 + (2/\nu_p))\Gamma(1 - (2/\nu_p)) \). It is shown that \( P_{\text{co,p}} \) is an increasing function of \( P_{\text{p}} \). Therefore, \( P_{\text{co,p}} \) is upper bounded to satisfy the outage constraint of the primary network, i.e. \( P_{\text{co,p}} \leq \delta_{\text{p}} \), described as

\[
P_{\text{co,p}} \leq P_{S,\text{LB1}} = P_{\text{p}} \left( \frac{\ln (1/(1 - \delta_{\text{p}})) / \pi_0 \nu_p^2 \theta_{\text{co,p}}^2 (P_{\text{p}} / P_{\text{p}}) ^{2/\nu_p} \lambda_s }{\lambda_s} \right)^{-\nu_p/2}. \]

(11)

Similarly, define a threshold SIR value for connection outage of the typical first-type secondary link as \( \theta_{\text{co,s}} = 2R_0 - 1 \). Then, the COP of the typical first-type secondary link is given by

\[
P_{\text{co,s}} = P(\log(1 + \gamma_{\text{s}}) < R_{\text{s}}). \]

(12)

Following the same steps of (9), the COP of the typical first-type secondary link is given by

\[
P_{\text{co,s}} = E_{\Phi_p} \left\{ E_{\Phi_s} \left\{ P_{\text{Tg}}G_{\text{a,s}}/p_{\text{a}} \left( \frac{\nu_s}{\nu_s} + I_0(v_s) \right) < \theta_{\text{co,s}} \right\} \right\} = E_{\Phi_p} \left\{ \exp \left[ -\frac{\theta_{\text{co,s}}}{\nu_s} I_0(v_s) \right] \right\} = L_{\nu_s}(v_s) \frac{\theta_{\text{co,s}}}{\nu_s} L_{\nu_s}(v_s) / \nu_s P_{\text{p}}. \]

(16)

It is shown that \( P_{\text{co,s}} \) is a decreasing function of \( P_{\text{s}} \). Therefore, \( P_{\text{s}} \) is lower bounded to satisfy the connection outage constraint of the first-type secondary links, i.e. \( P_{\text{co,s}} \leq \delta_{\text{s,1}} \), described as

\[
P_{\text{s}} \geq P_{S,\text{LB1}} = P_{\text{p}} \left( \frac{\ln (1/(1 - \delta_{\text{s,1}})) / \pi_0 \nu_s^2 \theta_{\text{co,s}}^2 (P_{\text{p}} / P_{\text{p}}) ^{2/\nu_s} \lambda_s }{\lambda_s} \right)^{-\nu_s/2}. \]

(14)

On the other hand, since the second-type SU-Txs transmit the information-bearing signal with power \( \kappa P_{\text{s}} \) and artificial noise with power \( (1 - \kappa)P_{\text{s}} \) simultaneously, the COP of the typical second-type secondary link is given by

\[
P_{\text{co,s}} = P(\log(1 + \gamma_{\text{s}}) < R_{\text{s}}). \]

(15)

Considering the random distributions of PU-Txs and SU-Txs, we can express the COP of the typical second-type secondary link as (see (16))

\[
P_{\text{co,s}} = 1 - \exp \left[ -\pi_0 \nu_s^2 \theta_{\text{co,s}}^2 (P_{\text{s}} / P_{\text{s}}) ^{2/\nu_s} \lambda_s \right]. \]

(17)

where \( \theta_{\text{co,s}} = \theta_{\text{co,s}}/(\kappa - (1 - \kappa)\theta_{\text{co,s}}) \). It is shown that \( P_{\text{co,s}} \) is a decreasing function of \( P_{\text{s}} \) and \( \kappa \). Therefore, for a given \( \kappa \), \( P_{\text{s}} \) is lower bounded to satisfy the connection outage constraint of the second-type secondary links, i.e. \( P_{\text{co,s}} \leq \delta_{\text{s,2}} \), described as

\[
P_{\text{s}} \geq P_{S,\text{LB2}} = P_{\text{p}} \left( \frac{\ln (1/(1 - \delta_{\text{s,2}})) / \pi_0 \nu_s^2 \theta_{\text{co,s}}^2 (P_{\text{s}} / P_{\text{s}}) ^{2/\nu_s} \lambda_s }{\lambda_s} \right)^{-\nu_s/2}. \]

(18)

Also, for a given \( P_{\text{s}} \), \( \kappa \) is lower bounded to satisfy the connection outage constraint of the second-type secondary links, described as

\[
\kappa \geq \kappa_{\text{s,LB}} = \min \left\{ \frac{\theta_{\text{co,s}}}{1 + \theta_{\text{co,s}}} \left[ 1 + \frac{\ln (1/(1 - \delta_{\text{s,2}})) / \pi_0 \nu_s^2 \theta_{\text{co,s}}^2 (P_{\text{s}} / P_{\text{s}}) ^{2/\nu_s} \lambda_s }{\lambda_s} \right]^{-\nu_s/2} \left[ 1, \right] \right\}. \]

(19)

From (10) and (13), we see that \( P_{\text{s}} \) arouses a tradeoff between the COP of the primary link and the COP of the first-type secondary link. From (10) and (17), we see that \( P_{\text{s}} \) arouses a tradeoff
between the COP of the primary link and the COP of the second-type secondary link. Therefore, to satisfy the COP constraint of the primary network, the reliability performance of the secondary network should be compromised (i.e., larger values of $\rho^{(1)}_{\text{S},\text{UB}}$ and $\rho^{(2)}_{\text{S},\text{UB}}$). In other words, to satisfy the COP constraints of the primary network and the secondary network simultaneously, a moderate value of $P_S$ is preferred.

### 3.2 Secrecy outage probability

In this subsection, we derive the SOP of the secondary network to characterise the security performance. The SOP equals to the probability that at least one of the eavesdroppers in $\Phi_B$ causes a secrecy outage. Define a threshold SIR value for secrecy outage of the secondary network as $\theta_{\text{S},\text{UB}} = 2^{\rho_{\text{S},\text{UB}}} - R_1 - 1$. Then, the SOP of the typical second-type secondary link is expressed as (see (20))

$$P_{\text{S}} = \exp\left[-\frac{\lambda_\text{E} - \rho_{\text{S},\text{UB}}\rho_{\text{S}}^2}{P_{\text{S}} - 2}\frac{\lambda_\text{E}}{\rho_{\text{S}}^2}\right] \cdot (24)$$

where $\rho_{\text{S},\text{UB}}$ is the upper bound on $\rho_{\text{S},\text{UB}}$ as (see (22))

$$\rho_{\text{S},\text{UB}} \leq \rho_{\text{S}} = P_{\text{S}} \exp\left[-\frac{\lambda_\text{E}}{P_{\text{S}}\rho_{\text{S}}^2}\right] + \int_{D_{\text{S}}} P_{\text{S}} \exp\left[-\frac{\lambda_\text{E}}{P_{\text{S}}\rho_{\text{S}}^2}\right] d\rho_{\text{S}} \cdot (22)$$

It is shown that $P_{\text{S}}$ is a decreasing function of $D$. This means that a larger secrecy guard zone can achieve a higher security level. However, at the same time, a larger secrecy guard zone will certainly increase the hardware complexity and realisation difficulty. In addition, $\rho_{\text{S},\text{UB}}$ is an increasing function of $P_S$. Therefore, $P_S$ is upper bounded to satisfy the secrecy outage constraint of the first-type secondary link, i.e., $P_{\text{S},\text{UB}} \leq \rho_{\text{S},\text{UB}}$, described as

$$P_S \leq P_{\text{S},\text{UB}} = \exp\left[-\frac{\lambda_\text{E}}{P_{\text{S}}\rho_{\text{S}}^2}\right] + \int_{D_{\text{S}}} P_{\text{S}} \exp\left[-\frac{\lambda_\text{E}}{P_{\text{S}}\rho_{\text{S}}^2}\right] d\rho_{\text{S}} \cdot (22)$$

Similarly, the SOP of the typical second-type secondary link is expressed as (see (25))

$$P_{\text{S}} \leq P_{\text{S},\text{UB}} = \exp\left[-\frac{\lambda_\text{E}}{P_{\text{S}}\rho_{\text{S}}^2}\right] + \int_{D_{\text{S}}} P_{\text{S}} \exp\left[-\frac{\lambda_\text{E}}{P_{\text{S}}\rho_{\text{S}}^2}\right] d\rho_{\text{S}} \cdot (22)$$

Also, for a given $P_S$, $\kappa$ is upper bounded to satisfy the secrecy outage constraint of the second-type secondary link, described as (see (28) at the bottom of the next page)

Not that the upper bound technique gives accurate approximations of $\rho_{\text{S},\text{UB}}$ and $\rho_{\text{S}}$ over the whole range of (0, 1] [29]. We also verified the accuracy of the upper bounds in the numerical results section. Thus, we can use it in the following analysis and discussion.
3.3 Secrecy throughput analysis

In this subsection, we quantify the secrecy throughput of the secondary network. Having $P^{(2)}_{co,S}$ in (13) and $P^{(1)}_{co,S}$ in (23), a lower bound on the secrecy throughput of the first-type SUs is obtained as

$$\eta^{(1)}_S = \lambda_S \exp(-\pi D^2 A_S) \exp \left[ -\pi c_0 \theta^{1/\alpha}_{co,S} / 2^\alpha \left( A_S + \frac{P_S}{P_S} \right) \right] - \lambda_S \exp \left[ -c_0 \theta^{1/\alpha}_{co,S} / 2^\alpha \left( A_S + \frac{P_S}{P_S} \right) \right] \cdot \frac{D^2}{1 - \delta_{S,1}}. \tag{29}$$

Similarly, having $P_{co,S}$ in (17) and $P^{(1)}_{co,S}$ in (26), a lower bound on the secrecy throughput of the second-type SUs is obtained as (see (30))

Then, the secrecy throughput of the secondary network is obtained as a sum of $\eta^{(1)}_S$ and $\eta^{(2)}_S$.

4 Secrecy throughput optimisation

From previous sections, we find that each of $P_S$ and $\kappa$ play a very important role in the performance of the secure transmission. Specifically, the value of $\kappa$ incurs a tradeoff between the reliability performance and the security performance of the two-type secondary links. The value of $P_S$ arouses tradeoffs between the reliability performance and the security performance of both the first-type and the second-type secondary links.

Thus, to optimise the performance of the transmission protocols, in this section, we obtain the optimal $\kappa$ and $P_S$ that maximise the secrecy throughput subject to outage conduction and outage constraints. The optimisation problem is formulated as

$$\max_{P_S, \kappa} \eta_S \quad \text{s.t.} \quad P_{co,P} \leq \delta_P, \ P^{(1)}_{co,P} \leq \delta_{S,1}, \ P^{(1)}_{co,S} \leq \delta_{S,2}, \ P^{(1)}_{co,S} \leq \delta_{S,1}, \ P^{(1)}_{co,S} \leq \delta_{S,2}, \ P^{(1)}_{co,S} \leq \delta_{S,1}, \ P^{(1)}_{co,S} \leq \delta_{S,2} \tag{31}$$

where $\delta_P$ denotes the COP constraint of the primary network, $\delta_{S,1}$ and $\delta_{S,2}$ denote the COP constraint and the SOP constraint of the first-type secondary links, $\delta_{S,1}$ and $\delta_{S,2}$ denote the COP constraint and the SOP constraint of the second-type secondary links.

$$\kappa \leq \kappa_{ub} = \min \left\{ \frac{\theta^{1/\alpha}_{co,S}}{1 + \theta^{1/\alpha}_{co,S}} \left[ 1 + \frac{\lambda_E}{\pi c_0 \ln (1/(1 - e_{S,2})) (A_S + \frac{P_S}{P_S} \lambda_S)} \right]^{-1/\alpha} \right\}. \tag{28}$$

$$\eta^{(1)}_S = \lambda_S [1 - \exp(-\pi D^2 A_S)] \exp \left[ -\pi c_0 \theta^{1/\alpha}_{co,S} / 2^\alpha \left( A_S + \frac{P_S}{P_S} \right) \right] \cdot \frac{D^2}{1 - \delta_{S,1}}. \tag{30}$$

COP constraint represents the required reliability level while the SOP constraint represents the required security level. Note that when all of the COP and the SOP constraints are satisfied, non-zero secrecy throughput of the secondary network can be achieved. As such, we first give the condition under which the non-zero secrecy throughput exists before solving the optimisation problem.

4.1 Condition for non-zero secrecy throughput

From the COP and SOP results in previous section, we obtain the conditions for non-zero secrecy throughput of the first-type SUs and the second-type SUs in the following theorems.

Theorem 1: The conditions under which non-zero secrecy throughput of secondary network exist are given by

$$\begin{align*}
\left( \frac{\ln (1/(1 - \delta_P))}{\pi c_0 \theta^{1/\alpha}_{co,P} \lambda_{S,1}} - 1 \right) \left( \frac{\ln (1/(1 - \delta_{S,1}))}{\pi c_0 \theta^{1/\alpha}_{co,S} \lambda_{S,1}} - 1 \right) > 1, \\
\left( \frac{\ln (1/(1 - \delta_{S,1}))}{\pi c_0 \theta^{1/\alpha}_{co,S} \lambda_{S,1}} - 1 \right) \left( \frac{\ln (1/(1 - \delta_{S,2}))}{\pi c_0 \theta^{1/\alpha}_{co,S} \lambda_{S,2}} - 1 \right) > 1, \\
\left( \frac{1}{1 - \delta_{S,1}} \right)^2 \frac{\theta^{1/\alpha}_{co,S} D^2}{\lambda_{S,1}} \ln \frac{1}{1 - \delta_{S,1}} \ln \frac{1}{1 - e_{S,1}} > \frac{\lambda_E}{c_0^{1/\alpha} \theta^{2/\alpha}_{co,S} D^2}. \tag{34}
\end{align*}$$

$$\begin{align*}
\left( \frac{1}{1 - \delta_{S,1}} \right)^2 \frac{\theta^{1/\alpha}_{co,S} D^2}{\lambda_{S,1}} \ln \frac{1}{1 - \delta_{S,1}} \ln \frac{1}{1 - e_{S,2}} > \frac{\lambda_E}{c_0^{1/\alpha} \theta^{2/\alpha}_{co,S} D^2}, \\
\left( \frac{1}{1 - \delta_{S,2}} \right)^2 \frac{\theta^{1/\alpha}_{co,S} D^2}{\lambda_{S,2}} \ln \frac{1}{1 - \delta_{S,2}} \ln \frac{1}{1 - e_{S,2}} > \frac{\lambda_E}{c_0^{1/\alpha} \theta^{2/\alpha}_{co,S} D^2}. \tag{36}
\end{align*}$$

Proof: Combining $P_{co,S} \leq \delta_P$ and $P^{(1)}_{co,S} \leq \delta_{S,1}$, we have the condition in (32). Similarly, combining any other two constraints in (31), we can have the conditions from (33)–(37). \hfill \square

Remark 2: The conditions in (32) and (33) give tradeoffs between the reliability level of the primary network and the reliability levels of secondary network. This implies that in order to achieve the higher reliability level, the reliability level of the secondary network should be compromised. The conditions in (34)–(37) give tradeoffs between the reliability level and the security level of the secondary network, which implies that in order to achieve a higher security level, the reliability level needs to be compromised in the secondary network. From (34)–(37), we find that the tradeoffs between the reliability and the security in the secondary network do not depend on the transmission power $P_S$, the density of SU-Txs $A_S$ and the density of PU-Txs $A_P$. This implies when the conditions are not met, only changing the transmission power and/or the density of the legitimate nodes cannot achieve non-zero secrecy throughput. We also find that the tradeoff can be improved by decreasing

IET Commun., 2016, Vol. 10, Iss. 15, pp. 1904–1913
This is an open access article published by the IET under the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/)
distance of the communication link $l_s$. Furthermore, comparing (34) and (35), we see that having the secrecy guard zone can also improve the tradeoffs.

### 4.2 Solution

Since $k$ only affects the secrecy throughput of the second-type SUs, we first determine optimal value of $k$ for given $P_S$. The optimisation problem with respect to $k$ is formulated as

$$
\max_k \eta_S^{(1)}
$$

s.t. \ $k_{LB} \leq k \leq k_{UB}$.

Then, the optimal value of $k$ is given in the following theorem.

**Theorem 2:** For given transmission power $P_S$, the optimal power fraction that maximises the secrecy throughput of the second-type SUs for given connection and secrecy outage constraints is given by

$$
k_{opt} = \begin{cases} 
k_{LB}, & \text{if } F(k_{LB}) > 0, \\ k', & \text{if } \exists k \in [k_{LB}, k_{UB}]: F(k) = 0, \\ k_{UB}, & \text{if } F(k_{UB}) < 0,
\end{cases}
$$

where $k'$ is the value of $k \in [k_{LB}, k_{UB}]$ satisfying $F(k) = 0$, $F(k)$ is given by

$$
F(k) = \left( k - \frac{\theta_{o,S}}{1 + \theta_{o,S}} \right)^{2/\alpha} + c_1 \left( \frac{\theta_{o,S}}{1 + \theta_{o,S}} \right)^{2/\alpha},
$$

where $c_1 = (1/\lambda_o) \pi w_s^2 (\lambda_s + (P_P/P_S)^{2/\alpha} A_P)^2$.

**Proof:** See proof in Appendix.
Remark 3: From Theorem 2, we can see that the optimal $k$ depends on the ratio $\frac{\lambda_S + (P_P/P_S)^2/\lambda_P}{\lambda_E}$. Specifically, as the ratio increases, $k_{opt}$ increases and approaches to 1. This is because higher density of interferences and longer communication distance make the connection outage more dominant than the secrecy outage. On the contrary, as the ratio decreases, $k_{opt}$ decreases and approaches to $\frac{\lambda_{co,S}}{(1 + \lambda_{co,S})}$. This is because higher density of eavesdroppers makes the secrecy outage more dominant than the connection outage.

Next, we determine the optimal value of $P_S$ that maximises the secrecy throughput of the secondary network. The optimisation problem is formulated as

$$\max_{P_S} \eta_S,$$

s.t. $P_{co,P} \leq \delta_{S,1}$, $P_{co,S} \leq \delta_{S,2}$, $P_{co,x} \leq \delta_{S,1}$, $P_{co,y} \leq \delta_{S,2}$.

(41)

We note that the closed-form expression for the optimal $P_S$ is mathematically intractable due to the sum formulation of the secrecy throughput of the secondary network. As such, we present Algorithm 1 (see Fig. 2) to numerically determine the optimal value of $P_S$, denoted as $P_{S,opt}$, and the maximum value of $\eta_S$, denoted as $\eta_{S,max}$. Note that the value of $k_{opt}$ can also be obtained by using (39) with $P_{S,opt}$.

5 Numerical results

In this section, we first present the impacts of the transmission power of SU-Txs $P_S$ and power fraction factor for secret message $k$ on the reliability and security performance. Then, we show the interaction of different design parameters and their impacts on the maximised secrecy throughput. Finally, we compare the performance of the proposed transmission protocol to two other transmission protocols to show the performance improvement. The system parameters are assumed as: $P_p = 40 \text{dBm}$, $P_s = 25 \text{dBm}$, $\alpha = 4$, $l_p = 10 \text{m}$, $l_s = 5 \text{m}$, $\lambda_p = \lambda_s = 2 \times 10^{-4} \text{units/m}^2$, $\lambda_E = 0.4 \times 10^{-4} \text{units/m}^2$, $\theta_p = 29 \text{dBm}$, $\theta_s = 25 \text{dBm}$, $\delta_p = 0.1$, $\delta_{S,1} = \delta_{S,2} = 0.3$, $\varepsilon_{S,1} = \varepsilon_{S,2} = 0.2$, and $D = 10 \text{m}$, unless otherwise stated. We consider a two dimensional square network (i.e. $[-1000, 1000] \times [-1000, 1000]$).

We first show the impacts of $P_S$ and $k$ on the COPs and SOPs, respectively. Fig. 3 plots $p_{co,P}^{(i)}$, $p_{co,S}^{(i)}$, $p_{co,x}^{(i)}$, $p_{co,y}^{(i)}$, $p_{so,P}^{(ii)}$, and $p_{so,S}^{(ii)}$ versus...
In this paper, we studied the secure transmission in a random CRN where the PUs, the SUs and the eavesdroppers are randomly distributed according to PPP. We proposed a simple and decentralised transmission scheme, which jointly incorporates the secrecy guard zone and artificial noise. Then, we derived the secrecy performance gain.

Fig. 8 Comparison between the secrecy throughputs of different protocols

6 Conclusion

In this work, we presented the secure transmission in a random CRN where the PUs, the SUs and the eavesdroppers are randomly distributed according to PPP. We proposed a simple and decentralised transmission scheme, which jointly incorporates the secrecy guard zone and artificial noise. Then, we derived the secrecy throughput of secondary network based on the COP and SOP analyses of the first-type secondary links and the second-type secondary links. Furthermore, the optimal transmission power of the SU-Txs and the optimal power allocation between information-bearing signal and artificial noise were determined analytically by maximising the secondary throughput of the secondary network under the primary outage constraints and the secondary outage constraints. Our analysis highlighted that introducing the secrecy guard zone provides better security performance, and the artificial noise performs as additional interference to insert a control between the reliability and security.

7 Acknowledgments

This work was supported by the National Natural Science Foundation of China (No. 61371122, 61471393 and 61501512).

References

1 Wen, H., Zhu, X., Zhou, L.: ‘A framework of the PHY-layer approach to defense against security threats in cognitive radio networks’, IEEE Netw., 2013, 27, (3), pp. 34–39
2 Massey, J.L.: ‘An introduction to contemporary cryptology’, Proc. IEEE, 1988, 76, (5), pp. 533–549
3 Zhou, X., Song, L., Zhang, Y.: ‘Physical layer security in wireless communications’ (CRC Press, 2013)
4 Wyner, A.: ‘The wire-tap channel’, Bell Syst. Tech. J., 1975, 54, (8), pp. 1355–1387
5 Pei, Y., Liang, Y.-C., Teh, K.C., et al.: ‘Secure communication over MISO cognitive radio channels’, IEEE Trans. Wirel. Commun., 2010, 9, (4), pp. 1494–1502

This is an open access article published by the IET under the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/).
For \( \kappa_{LB} \leq \kappa \leq \kappa_{UB} \), the \( \eta_S^{\text{II}} \) in (30) can be expressed in the form of (see (42))

\[ A = \lambda_S(1 - \exp(-\pi D^2 \lambda_S)) > 0, \quad B = \pi \lambda_S^{2/\alpha} (\lambda_S + (P_p/P_s)^{2/\alpha} \lambda_S) > 0, \quad C = (\lambda_S / c_0 (\lambda_S + (P_p/P_s)^{2/\alpha} \lambda_S)) > 0 \quad \text{and} \quad (B/C) = c_1. \]

Then, the first derivative of \( \eta_S^{\text{II}} \) with respect to \( \kappa \) is given by

\[ \partial \eta_S^{\text{II}} / \partial \kappa = \eta_S^{\text{II}}(\kappa) \left[ B \left( \frac{\theta_{obs}^{u}}{1 + \theta_{obs}^{u}} \right)^{\frac{2}{\alpha}} \left( \frac{\kappa - \theta_{obs}^{u}}{\theta_{obs}^{u}} \right)^{-(2/\alpha) - 1} - C \left( \frac{\theta_{obs}^{u}}{1 + \theta_{obs}^{u}} \right)^{\frac{2}{\alpha}} \left( \frac{\kappa - \theta_{obs}^{u}}{\theta_{obs}^{u}} \right)^{-(2/\alpha) - 1} \right]. \]

The first derivative of \( F(\kappa) \) is given by

\[ \partial F(\kappa) / \partial \kappa = \left( \frac{\theta_{obs}^{u}}{1 + \theta_{obs}^{u}} \right)^{\frac{2}{\alpha}} \left( \frac{\kappa - \theta_{obs}^{u}}{\theta_{obs}^{u}} \right)^{-(2/\alpha) - 2} \cdot \frac{2}{\alpha} \left( 2\kappa - \theta_{obs}^{u} \right)^{\frac{2}{\alpha}} \left( \frac{\theta_{obs}^{u}}{1 + \theta_{obs}^{u}} \right) + \frac{\theta_{obs}^{u}}{1 + \theta_{obs}^{u}} \left( \frac{\theta_{obs}^{u}}{1 + \theta_{obs}^{u}} \right)^{\frac{2}{\alpha}} \cdot \left( \frac{\kappa - \theta_{obs}^{u}}{\theta_{obs}^{u}} \right)^{-(2/\alpha) - 2}. \]

which is larger than zero for any \( \kappa \in [\kappa_{LB}, \kappa_{UB}] \). Therefore, \( F(\kappa) \) is a strictly increasing function of \( \kappa \). Thus, there is at most one \( \kappa \) that satisfies \( F(\kappa) = 0 \). Specifically, when the maximal value of \( F(\kappa) \), i.e. \( F(\kappa_{UB}) \), is smaller than zero, \( \eta_S^{\text{II}} / \partial \kappa \) is always larger than zero. Therefore, in this case, i.e. \( F(\kappa_{UB}) < 0 \), \( \eta_S^{\text{II}} \) is a strictly increasing function of \( \kappa \) and \( \kappa_{opt} \) is equal to \( \kappa_{UB} \). When the minimal value of \( F(\kappa) \), i.e. \( F(\kappa_{LB}) \), is larger than zero, \( \eta_S^{\text{II}} / \partial \kappa \) is always smaller than zero. Therefore, in this case, i.e. \( F(\kappa_{LB}) > 0 \), \( \eta_S^{\text{II}} \) is a strictly decreasing function of \( \kappa \) and \( \kappa_{opt} \) is equal to \( \kappa_{LB} \). When \( F(\kappa_{UB}) \leq 0 \) and \( F(\kappa_{LB}) \geq 0 \), there exists one and only one \( \kappa \) satisfying \( F(\kappa) = 0 \). That is to say \( \eta_S^{\text{II}} \) has only one critical point \( \kappa^* \) in this case. Moreover, when \( \kappa < \kappa^* \), \( F(\kappa) > 0 \) and \( (\partial \eta_S^{\text{II}} / \partial \kappa) > 0 \); when \( \kappa > \kappa^* \), \( F(\kappa) < 0 \) and \( (\partial \eta_S^{\text{II}} / \partial \kappa) < 0 \). Hence, \( \eta_S^{\text{II}} \) is maximised at the critical point \( \kappa^* \).

Finally, the optimal value \( \kappa_{opt} \) is summarised by Theorem 2.