A Stochastic Method to Physical Layer Security of an Amplify-and-Forward Spectrum Sensing in Cognitive Radio Networks: Secondary User to Relay

Oluyomi Simpson and Yichuang Sun
School of Engineering and Technology, University of Hertfordshire, Hatfield, AL10 9AB United Kingdom
o.simpson@herts.ac.uk and y.sun@herts.ac.uk

***Abstract*— In this paper, a framework for capitalizing on the potential benefits of physical layer security in an amplify-and-forward cooperative spectrum sensing (AF-CSS) in a cognitive radio network (CRN) using a stochastic geometry is proposed. In the CRN network the sensing data from secondary users (SUs) are collected by a fusion center (FC) with the help of access points (AP) as relays, and when malicious eavesdropping secondary users (SUs) are listening. We focus on the secure transmission of active SUs transmitting their sensing data to the AP. Closed expressions for the average secrecy rate are presented. Numerical results corroborate our analysis and show that multiple antennas at the APs can enhance the security of the AF-CSS-CRN. The obtained numerical results show that average secrecy rate between the AP and its correlated FC decreases when the number of AP is increased. Nevertheless, we find that an increase in the number of AP initially increases the overall average secrecy rate, with a perilous value at which the overall average secrecy rate then decreases. While increasing the number of active SUs, there is a decrease in the secrecy rate between the sensor and its correlated AP.**

***Index Terms*— communication system security; physical layer security; cognitive radio networks; compressed sensing; Amplify-and-Forward**

I. INTRODUCTION

The transmission techniques of wireless communication links allow for a malicious eavesdropper to hijack. In reality, communication security in wireless networks is becoming ever more critical. As a means of solving a problem, traditional cryptographic methods are set out on upper layers of network protocols. Traditional security techniques are not necessarily effective against potential attacks from the open wireless environment any longer. These traditional cryptographic techniques are likewise becoming costly. Equally a substitute, physical layer security, exploiting unique features from the lower layer, has become a new research focus for several wireless communication systems networks.

A. Physical Layer Security

The fundamental research on physical layer secure communication was studied in depth by [1]. A wiretap channel model, with the secrecy rate defined as the rate at which information can be transmitted secretly from a source to its proposed destination, was considered in [2, 3]. Especially, it is conceivable to achieve a non-zero secrecy rate without distribution of a key, where the malicious eavesdropper is restricted to learn virtually nil from the transmissions. In [4] an addition of this research led to the case of the broadcast channel with confidential information being proposed. The average secure communication rates as well as the outage probability with an eavesdrop-per listening to the transmission over an additional independent fading channel was researched by [5]. Discussions regarding the ergodic secrecy capacity region for a fading broadcast channel with confidential messages was explored in [6] . The secrecy capacity of a block-ergodic fading channel was presented in [7]. Numerous strategies for a relay node to enhance the secrecy of a wiretap channel were explored in [8-10]. A technique of employing channel diversity to increase secrecy capacity in wireless communication is presented in [11].

Cognitive Radio Networks (CRNs) are becoming one of the most promising technologies that aim for efficient spectrum utilization and alleviating the spectrum scarcity problem caused by the demand for wireless bandwidth growing rapidly due to the increase in growth of various mobile and IoT application [12-14]. CRNs are found to be without difficulty wide-open to external malicious threats. Secure communication is an important prerequisite for forthcoming fifth-generation (5G) systems, and CRs are not exempt. Especially, security of CRN is perilous [15-19]. The proposal of trusted relay weighted and allocation of transmission power under diverse relay protocols for instance amplify and forward (AF), decode and forward (DF), and cooperative jamming were presented in [20]. Relay selection was proposed for secure CR with a sole eavesdropper in [21]. To exploit the security aspect of CR networks Game theory was employed in [17]. An overview of research outcomes in information-theoretic security by means of multiple wireless transmitters which focuses on distilling insights for designing wireless systems with secrecy was presented in [22].

The ability to sense the presence of a PU is of the utmost importance of CRNs. Nevertheless, this mechanism introduces susceptibilities that may permit an attacker to disguise as a primary (PU) that occupies a licensed share of the spectrum and cause a denial-of-service (DoS) attack for SUs. This method of attack is known as primary user emulation (PUE) attack [23]. To address the limits of key-based security, physical layer security is now emerging as a promising paradigm to address the security CRN by exploiting the physical characteristics of wireless channels to achieve perfect secrecy against eavesdropping [24]. A selection combing (SC) employing a preeminent SNR in the receiver of the destination and the eavesdropper is proposed in [25]. It is undoubtedly not the optimal solution because the unfilled diversity paths are not utilized. It gives the inspiration in

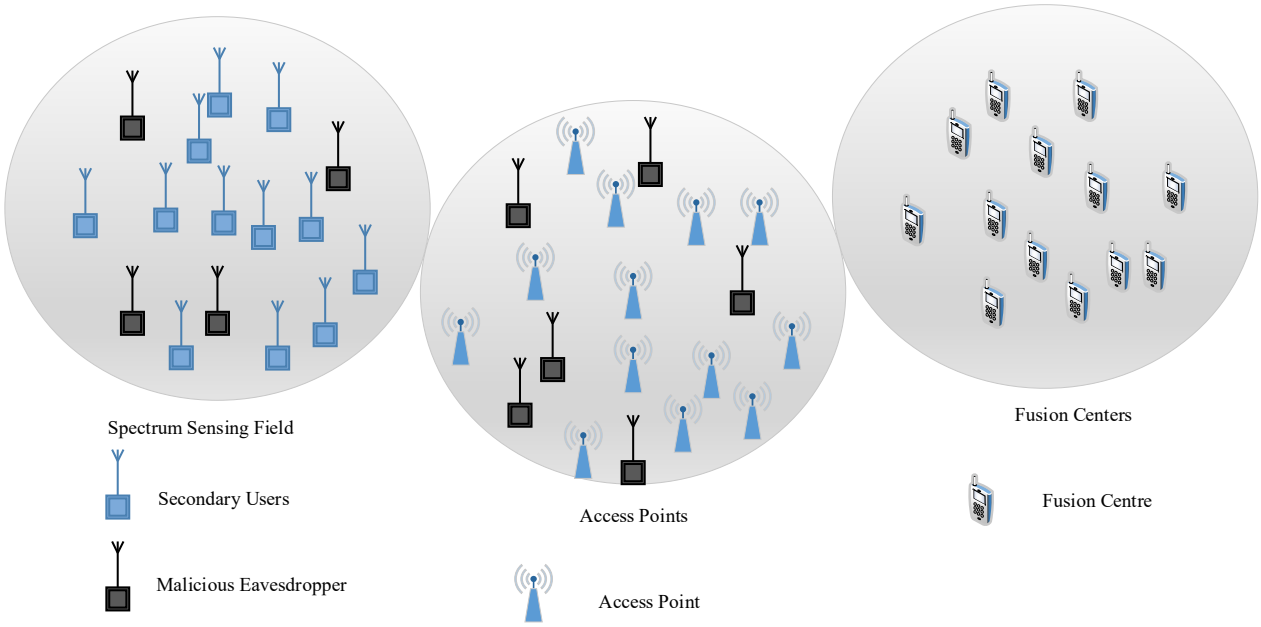

Fig. 1. An AF-CSS-CRN, where the SUs transmit the data to the FCs via the APs, in the presence of eavesdropping.

this paper to use maximal-ratio combining (MRC) for better security. We propose a channel diversity with MRC to increase the secrecy capacity as compared to the SC scheme proposed in [27]. of CRN by exploiting the physical characteristics of wireless channels to achieve perfect secrecy against eavesdropping [24].

B. Approach and Contributions

In this paper, the potential benefits of physical layer security in an amplify-and-forward cooperative spectrum sensing (AF-CSS) in a cognitive radio network (CRN) using a stochastic geometry is proposed. In an AF-CSS-CRN, the SU are located far from the FCs, and the access points (AP) are deployed to help the SUs forward their sensing data to the FC. This confidential data transmission can be hijacked by malicious eavesdroppers. Assuming that SUs are densely deployed and their positions are randomly distributed a stochastic geometry to model the positions of the nodes in the CRN. The spectrum sensing and amplification technique used in this work can be found in the author's previous work in [26]. The main contributions of our work are listed as follows:

1. An analytical framework to analyze the implementation of physical layer security in AF-CSS-CRN is developed. The positions and spatial densities of SUs, APs, FCs, and eavesdroppers are modeled by means of stochastic geometry. Individually APs are equipped with multiple antennas and make use of the low complexity maximal ratio combining (MRC) to receive the sensing data from the SUs and maximal-ratio transmission (MRT) beamformer to transmit the signals.
2. Novel statistical properties are presented, centered on which new closed expressions for the average secrecy rate between the distinctive SU and its correlated AP are derived. A novel compact expression for overall average secrecy rate in an AF-CSS-CRN is derived.

This paper is organized as follows: In section II the AF-CSS-CRN system model is presented. In Section III the average secrecy rate between the SU and AP are presented. In section IV numerical results alongside detailed analyses are presented. Finally, in Section V concluding remarks are provided.

II. System Model

In Fig. 1, the CRN system model is presented, the CRs transmit sensed data to the fusion centre (FC) with the aid of half-duplex amplify-and-forward (AF) access points (APs) with no direct links between CRs and FCs. The eavesdroppers listen in to both data transmission without modifying the data. CRs are randomly positioned in the spectrum sensing field based on a homogeneous Poisson point process (HPPP) Φ_{cr} with intensity λ_{cr}. To envisage inadvertent deployment of APs and FCs the random positions of the APs and FCs are approximated as independent HPPPS Φ_{ap} and Φ_{fc} with intensities λ_{ap} and λ_{fc}, respectively, which is appropriate in large scale networks [27]. The CRs transmit spectrum sensing data sporadically. Therefore, the probability that a CR is triggered to transmit the sensing data is denoted as ρ_{cr}, $0 < \rho_{cr} < 1$, and the probability of an AP that amplifies and forwards the sensing data to the FC is denoted as ρ_{cr}, $0 < \rho_{cr} < 1$. The probability of being an active CR or AP is assumed to be independent of the CR or AP position. Hence the active CR or AP is made up of independent HPPPs $\Phi_{cr,a}$ and $\Phi_{ap,a}$ with intensities $\lambda_{cr}\rho_{cr}$ and $\lambda_{ap}\rho_{ap}$, respectively. It is assumed that the eavesdroppers are non-collaboration and that eavesdroppers' positions are modelled as independent HPPPs $\Phi_{cr,e}$ and $\Phi_{ap,e}$ with intensities λ_e^{cr} and λ_e^{ap}, respectively. The data transmitted by the CR is hijacked by the eavesdroppers in $\Phi_{cr,e}$ and the data transmitted by the AP is hijacked by the eavesdroppers in $\Phi_{ap,e}$.

In this CRN model, the CR is correlated with its closest AP to receive the CR's sensing data and the AP is correlated with its closest FC to receive the AP's sensing data. Individual AP utilise *M* antennas, and the CRs and FCs have single-antenna. The APs use MRC to receive the CRs' data signals and MRT beamformer to transmit the signals to the FC, this amplifies the sensing data transmission. The wireless channels between the CR and AP and AP and FC are modelled as independent quasi-static Rayleigh fading, respectively. A distinctive AP receives data form its nearest arbitrary distinctive CR o. The distinctive AP receives valuable data from the distinctive CR and interference from other active CR and active AP. Consequently, the receive signal to interference and noise ratio (SINR) after MRC at its corresponding distinctive AP can be presented by

$$\gamma_{ap} = \frac{\left\|\mathbf{h}_{cr_0,ap_0}\right\|^2 \left|X_{cr_0,ap_0}\right|^{-\alpha}}{\underbrace{I_{cr,ap} + I_{ap,ap}}_{In_{ap}} + \delta^2 / P_{cr}}, \quad (1)$$

where $I_{cr,ap} = \sum_{i\in\Phi_{cr,a}\setminus\{cr_0\}} \left| \frac{\mathbf{h}_{cr_0,ap_0}^{\dagger}}{\left\|\mathbf{h}_{cr_0,ap_0}\right\|} \mathbf{h}_{i,ap_0} \right|^2 \left|X_{i,ap_0}\right|^{-\alpha}$,

$I_{ap,ap} = \mu \sum_{j\in\Phi_{ap,a}\setminus\{ap_0\}} \left| \frac{\mathbf{h}_{cr_0,ap_0}}{\left\|\mathbf{h}_{cr_0,ap_0}\right\|} \mathbf{H}_{j,ap_0} \frac{\mathbf{h}_{j,fc_j}^{\dagger}}{\left\|\mathbf{h}_{j,fc_j}\right\|} \right|^2 \left|X_{j,ap_0}\right|^{-\alpha}$, and $\mu = P_{ap} / P_{cr}$. Interfering APs conveys their own valuable data to their corresponding FCs using MRT beamformer vector $\frac{\mathbf{h}_{j,fc_j}^{\dagger}}{\left\|\mathbf{h}_{j,fc_j}\right\|}$. These are received and combined at the distinctive AP with MRC vector $\frac{\mathbf{h}_{cr_0,ap_0}^{\dagger}}{\left\|\mathbf{h}_{cr_0,ap_0}\right\|}$, where $\mathbf{h}_{cr_0,ap_0}$ and $\left|X_{cr_0,ap_0}\right|$ are the channel fading vector and distance from the distinctive CR to its distinctive AP, respectively, where α is the path loss exponent, $\mathbf{h}_{i,ap_0} \in C^{M\times 1}$ and $\left|X_{i,ap_0}\right|$ are the channel fading vector and distance from the CR *i* to the distinctive AP, respectively, $\mathbf{H}_{j,ap_0}$ and $\left|X_{j,ap_0}\right|$ are the channel fading matrix and distance between the interfering AP *j* and the distinctive AP, respectively, $\mathbf{h}_{j,fc_j} \in C^{1\times M}$ is the channel fading vector between the interfering AP *j* and its corresponding FC, δ^2 is the noise power, P_{cr} is the CR's transmit power, and P_{ap} is the AP's transmit power.

In the non-collaboration eavesdropping situation, the greatest damaging eavesdropper that has the uppermost receive SINR dictates the secrecy rate [15]. A random eavesdropper e_k that hijacks the CR and the AP transmission listens to the valuable sensing data from the distinctive CR to the distinctive AP, and concurrently acquires the interfering data from the additional active CRs and active AP. e_k is impaired by the interfering signals emitted by the other interfering AP using the MRT beamformer $\frac{\mathbf{h}_{j,fc_k}^{\dagger}}{\left\|\mathbf{h}_{j,fc_k}\right\|}$. Hence, the received SINR at the most unfavourable eavesdropper in $\Phi_{cr,e}$ for the CR and the AP transmission is known by

$$\gamma_{cr,e} = \max_{e_k\in\Phi_{cr,e}} \left\{ \frac{\left|h_{cr_0,e_k}\right|^2 \left|X_{cr_0,e_k}\right|^{-\alpha}}{\underbrace{I_{cr,e} + I_{ap,e}}_{In_{cr,e}} + \delta^2 / P_{cr}} \right\} \quad (2)$$

where $I_{cr,e} = \sum_{i\in\Phi_{cr,a}\setminus\{cr_0\}} \left|h_{i,e_k}\right|^2 \left|X_{i,e_k}\right|^{-\alpha}$ and $I_{ap,e} = \sum_{j\in\Phi_{ap,a}\setminus\{ap_0\}} \mu \left| h_{j,e_k} \frac{\mathbf{h}_{j,fc_j}^{\dagger}}{\left\|\mathbf{h}_{j,fc_j}\right\|} \right|^2 \left|X_{j,e_k}\right|^{-\alpha}$, h_{cr_0,e_k} and $\left|X_{cr_0,e_k}\right|$ are the channel fading coefficient and distance between distinctive CR and the eavesdropper e_k, respectively. h_{i,e_k} and $\left|X_{i,e_k}\right|$ are the channel fading coefficient and distance between the *i*-th CR and the eavesdropper e_k, respectively, and h_{j,e_k} and $\left|X_{j,e_k}\right|$ are the channel fading vector and distance from the AP *j* to the eavesdropper, respectively.

The distinctive AP ap_0 will forward the sensed data to the nearest FC fc_0 for data collection after receiving the distinctive CR's data. Owing to the present transmission from additional active AP, the distinctive FC suffers from their interferences. Per se, the received SINR at the distinctive FC fc_0 is given by

$$\gamma_{fc} = \frac{\left\|\mathbf{g}_{ap_0,fc_0}\right\|^2 \left|X_{ap_0,fc_o}\right|^{-\beta}}{In_{ap,fc} + \delta^2 / P_{ap}}, \quad (3)$$

where $In_{ap,fc} = \sum_{j\in\Phi_{ap,a}\setminus\{ap_0\}} \left| \mathbf{g}_{j.fc_0} \frac{\mathbf{h}_{j,fc_j}^{\dagger}}{\left\|\mathbf{h}_{j,fc_j}\right\|} \right|^2 \left|X_{j,fc_0}\right|^{-\beta}$, $\mathbf{g}_{ap_0,fc_0} \in C^{1\times M}$ and $\left|X_{ap_0,fc_o}\right|$ are the channel fading vector and distance between the distinctive AP and its distinctive FC, respectively, β is the path loss exponent, $\mathbf{g}_{j,fc_0} \in C^{1\times M}$ and $\left|X_{j,fc_0}\right|$ are the channel fading vector and distance between the AP *j* and the distinctive FC, and $\mathbf{h}_{j,fc_0} \in C^{1\times M}$ is the channel fading vector between the AP *j* and its correlated FC. A random eavesdropper e_k that hijacks the distinctive AP and the distinctive FC transmission listens in to the signal transmitted by the distinctive AP with the MRT beamformer $\frac{\mathbf{g}_{ap_0,fc_0}^{\dagger}}{\left\|\mathbf{g}_{ap_0,fc_0}\right\|}$, and suffers from the interfering signals emitted by other interfering APs with the MRT beamformer $\frac{\mathbf{h}_{j,fc_k}^{\dagger}}{\left\|\mathbf{h}_{j,fc_k}\right\|}$. Thus, the received SINR at the most detrimental eavesdropper for the AP and the sink transmission is given by

$$\gamma_{ap,e=} \max_{e_k\in\Phi_{ap,e}} \left\{ \frac{\left| \mathbf{g}_{ap_0,e_k} \frac{\mathbf{g}_{ap_0,fc_k}^{\dagger}}{\left\|\mathbf{g}_{ap_0,fc_k}\right\|} \right|^2 \left|X_{ap_0,e_k}\right|^{-\beta}}{In_{ap,e} + \delta^2 / P_{ap}} \right\} \quad (4)$$

where $In_{ap,e} = \sum_{j\in\Phi_{ap,a}\setminus\{ap_0\}} \left| \mathbf{g}_{j,e_k} \frac{\mathbf{h}_{j,fc_k}^{\dagger}}{\left\|\mathbf{h}_{j,fc_k}\right\|} \right|^2 \left|X_{j,e_k}\right|^{-\beta}$, $\mathbf{g}_{ap_0,e_k}$ and $\left|X_{ap_0,e_k}\right|$ are the channel fading coefficient and distance from the distinctive AP to the eavesdropper, respectively, and $\mathbf{g}_{j,e_k}$ and $\left|X_{j,e_k}\right|$ are the channel fading vector and distance from the AP *j* to the eavesdropper, respectively.

III. Average Secrecy Rate Between SU and AP

The average secrecy rate that is established on the worst case is evaluated. In order to calculate the average secrecy rate, the eavesdropper with the best SINR is considered [20]. Therefore, for a distinctive link between a distinctive CR and its correlated AP, the momentary secrecy rate is given by

$$C_{cr}^{ap} = [C_{ap} - C_{cr,e}]^+ \tag{5}$$

where $[x]^+ = \max\{x, 0\}$, $C_{ap} = \log_2(1+\gamma_{ap})$ is the capacity of the channel between the distinctive CR and AP, and $C_{cr,e} = \log_2(1+\gamma_{cr,e})$ is the capacity of the eavesdropping channel between the distinctive CR and the utmost detrimental eavesdropper. The cumulative distribution functions (CDFs) of SINRs at the distinctive AP and the most detrimental eavesdropper that hijacks the transmission between the distinctive CR and AP are derived.

A. CDF of SINR at the typical AP

Taking (1) into consideration, the CDF of γ_{ap} is presented as

$$\begin{aligned} F_{\gamma_{ap}}(\gamma th) &= \int_0^\infty \Pr\left[\frac{\left\|\mathbf{h}_{cr_0,ap_0}\right\|^2 r^{-\alpha}}{In_{ap}+\delta^2/P_{cr}} \le \gamma_{th}\right] f_{\left|X_{cr_0,ap_0}\right|}(r)dr \\ &= \int_0^\infty \Pr\left[\frac{\left\|\mathbf{h}_{cr_0,ap_0}\right\|^2 \left|X_{cr_0,ap_0}\right|^{-\alpha}}{In_{ap}+\delta^2/P_{cr}} \le \gamma_{th}\right] 2\pi\lambda_{ap} \\ &\quad \times (1-\rho_{ap}) r \exp(-\pi\lambda_{ap}(1-\rho_{ap})r^2)dr \end{aligned} \tag{6}$$

where $f_{\left|X_{cr_0,ap_0}\right|}(r)$ is the PDF of the nearest distance between the AP and the distinctive CR. The CDF of the AP SINR at distance *r* from its corresponding CR is

$$\begin{aligned} &\Pr\left[\frac{\left\|\mathbf{h}_{cr_0,ap_0}\right\|^2 r^{-\alpha}}{In_{ap}+\delta^2/P_{cr}} \le \gamma_{th}\right] \\ &= 1 - \sum_{m=0}^{M-1} \frac{1}{m!} \mathbb{E}_{\Phi_{cr,a}} \\ &\times \{\mathbb{E}_{\Phi_{ap,a}}\{\int_0^\infty [\gamma_{th} r^a (\tau+\delta^2/P_{cr})]^m \\ &\exp[-\gamma_{th} r^a (\tau+\delta^2/P_{cr})] d\Pr(In_{ap} \le \tau)\}\}. \end{aligned} \tag{7}$$

Substituting

$$(-(\tau+\delta^2/P_{cr})\gamma_{th})^m e^{-(\tau+\delta^2/P_{cr})\gamma_{th}\{\sigma\} r^a} = \left.\frac{d^m(e^{-(\tau+\delta^2/P_{cr})})}{dx^m}\right|_{x=r^\alpha}$$ into (7),

and rewriting the CDF of the AP SINR at distance *r* from its correlated CR gives

$$\begin{aligned} &\Pr\left[\frac{\left\|\mathbf{h}_{cr_0,ap_0}\right\|^2 r^{-\alpha}}{In_{ap}+\delta^2/P_{cr}} \le \gamma_{th}\right] \\ &= 1 - \mathbb{E}_{\Phi_{cr,a}}\{\mathbb{E}_{\Phi_{ap,a}}\{\int_0^\infty \exp[\gamma_{th} r^a (\tau+\delta^2/P_{cr})] d\Pr \\ &\times (In_{ap} \le \tau)\}\} - = 1 - \sum_{m=0}^{M-1} \frac{(r^\alpha)^m}{m!(-1)^m} \mathbb{E}_{\Phi_{cr,a}} \\ &\times \{\mathbb{E}_{\Phi_{ap,a}}\{\int_0^\infty \left.\frac{d^m(e^{-\gamma_{th} x(\tau+\delta^2/P_{cr})})}{dx^m}\right|_{x=r^\alpha cr} d\Pr \\ &\times (In_{ap} \le \tau)\}\} \\ &= \left[\begin{array}{l} 1 - \exp(-\gamma_{th} r^a \delta^2/P_{cr}) \zeta_{in_{ap}}(\gamma_{th} r^\alpha) \\ -\sum_{m=0}^{M-1} \frac{(r^\alpha)^m}{m!(-1)^m} \left.\frac{d^m(\exp(-\gamma_{th} x\delta^2/P_{cr})\zeta_{in_{ap}}(\gamma_{th} x))}{dx^m}\right|_{x=r^\alpha} \end{array}\right] \end{aligned} \tag{8}$$

Considering Slivnyak's theorem, the Laplace transform of $I_{cr,ap}$ is given as

$$\begin{aligned} &\zeta_{I_{cr,ap}}(cr) \\ &= \mathbb{E}_{\Phi_{ap,a}}\left[\exp\left\{-cr \sum_{i\in\Phi_{cr,a}\setminus\{cr_0\}} \left|\frac{\mathbf{h}_{cr_0,ap_0}^{\dagger}}{\left\|\mathbf{h}_{cr_0,ap_0}\right\|}\mathbf{h}_{i,ap_0}\right|^2 \left|X_{i,ap_0}\right|^{-\alpha}\right\}\right] \\ &\overset{(q)}{=} \exp\left\{-2\pi\lambda_{cr} p_{cr} \int_0^\infty \left(1 - \zeta_{\frac{\mathbf{h}_{cr_0,ap_0}^{\dagger}}{\left\|\mathbf{h}_{cr_0,ap_0}\right\|}\mathbf{h}_{i,ap_0}}(cry^{-\alpha})\right) ydy\right\} \\ &\overset{(z)}{=} \exp\left\{-2\pi\lambda_{cr} p_{cr} \int_0^\infty \left(1 - \frac{1}{1+cry^{-\alpha}}\right) ydy\right\} \\ &= \exp\left\{-\lambda_{cr} p_{cr} \pi \Gamma(1+2/\alpha)\Gamma(1-2/\alpha) cr^{2/\alpha}\right\} \end{aligned} \tag{9}$$

From (9), (*q*) is obtained from the HPPP in [16], (*z*) is obtained from $\left|\frac{\mathbf{h}_{cr_0,ap_0}^{\dagger}}{\left\|\mathbf{h}_{cr_0,ap_0}\right\|}\mathbf{h}_{i,ap_0}\right|^2$. Subsequently,

$$\begin{aligned} I_{ap,ap} &= \mu \sum_{j\in\Phi_{ap,a}\setminus\{ap_0\}} \left|\frac{\mathbf{h}_{cr_0,ap_0}}{\left\|\mathbf{h}_{cr_0,ap_0}\right\|} \mathbf{H}_{j,ap_0} \frac{\mathbf{h}_{j,fc_j}^{\dagger}}{\left\|\mathbf{h}_{j,fc_j}\right\|}\right|^2 \left|X_{j,ap_0}\right|^{-\alpha} \\ &= \mu \sum_{j\in\Phi_{ap,a}\setminus\{ap_0\}} \mathbf{H}_j^{ap,ap} \left|X_{j,ap_0}\right|^{-\alpha} \end{aligned} \tag{10}$$

Through the Laplace transform of $I_{cr,ap}$ and $I_{ap,ap}$ the Laplace transform of In_{ap} is given by

$$\begin{aligned} \zeta_{In_{ap}}(cr) &= \zeta_{I_{cr,ap}}(cr)\zeta_{I_{ap,ap}}(cr) \\ &= \exp\{-(\lambda_{cr}\rho_{cr} + \lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}})\pi\Gamma(1+2/\alpha\} \\ &\quad \times\Gamma(1-2/\alpha) cr^{\frac{2}{\alpha}} \end{aligned} \tag{11}$$

Substituting (11) into (8) and applying the Faa di Bruno formula to solve the derivation of *m*-th order, and then subsequently substituting the derivation into (6), the CDF of γ_{ap} is given in (12) at the top of the next page.

$$
\begin{aligned}
F_{\gamma_{ap}}(\gamma th) &= 1-2\pi\lambda_{ap}(1-\rho_{ap})\int_0^{\infty} r\exp\left\{-\left(\lambda_{cr}\rho_{cr}+\lambda_{ap}\rho_{cr}\mu^{\frac{2}{\alpha}}\right)\pi\ \Gamma(1+2/\alpha)\Gamma(1-2/\alpha)(\gamma th)^{\frac{2}{\alpha}}r^2-\gamma thr^{\alpha}\delta^2/P_{cr}-\pi\lambda_{ap}(1-\rho_{cr})r^2\right\}dr \\
&-2\pi\lambda_{ap}(1-\rho_{cr})\sum_{m=1}^{M-1}\frac{(r^{\alpha})^m}{(-1)^m}\sum\frac{1}{\prod_{l=1}^{m}m_l!l!} \\
&\times\int_0^{\infty} r\exp\left\{-(\lambda_{cr}\rho_{cr}+\lambda_{ap}\rho_{cr}\mu^{\frac{2}{\alpha}})\pi\ \Gamma(1+2/\alpha)\ \Gamma(1-2/\alpha)(\gamma th)^{\frac{2}{\alpha}}r^2-\gamma thr^{\alpha}\delta^2/P_{cr}-\pi\lambda_{ap}(1-\rho_{ap})r^2\right\} \\
&\times[-2/\alpha(\lambda_{cr}\rho_{cr}+\lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}})\pi\ \Gamma(1+2/\alpha)\ \Gamma(1-2/\alpha)(\gamma th)^{\frac{2}{\alpha}}r^{(2-a)}-\gamma th\delta^2/P_s]^{m1}\prod_{l=2}^{m} \\
&\times[-(\lambda_{cr}\rho_{cr}+\lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}})\pi\ \Gamma(1+2/\alpha)\ \Gamma(1-2/\alpha)(\gamma th)^{\frac{2}{\alpha}}\prod_{l=2}^{m}(2/\alpha-j)r^{2-l\alpha}]^{m_1}dr
\end{aligned}
\tag{12}
$$

B. CDF of SINR at the Eavesdropper

Taking (2) into consideration, the CDF of $\gamma_{cr,e}$ is presented as

$$
\begin{aligned}
F_{\gamma_{cr,e}}(\gamma th) &= \left\{\max_{e_k\in\Phi_{cr,e}}\left\{\frac{\left|h_{cr_0,e_k}\right|^2\left|X_{cr_0,e_k}\right|^{-\alpha}}{In_{cr,e}+\delta^2/P_{cr}}\right\}\le\gamma_{th}\right\} \\
&\overset{(q)}{=}\exp-\lambda_e^{cr}\int_{R^2}e^{-\delta^2\gamma_{th}\left|X_{cr_0,e_k}\right|^{\alpha}/P_{cr}}\zeta_{In_{cr,e}} \\
&\times\ (\gamma_{th}\left|X_{cr_0,e_k}\right|^{\alpha})d\left|X_{cr_0,e_k}\right| \\
&\overset{(z)}{=}\exp\left\{-2\pi\lambda_e^{cr}\int_0^{\infty}e^{-\delta^2\gamma_{th}r^{\alpha}/P_{cr}}\zeta_{In_{cr,e}}\times(\gamma_{th}r^{\alpha})rdr\right\}
\end{aligned}
\tag{12}
$$

where, (q and (z)) are obtained from the HPPP and polar coordinates, respectively. From the functional HPPP the Laplace transform of $I_{cr,e}$ and $I_{ap,e}$, are derived respectively. From the Laplace transform of $I_{cr,e}$ and $I_{ap,e}$, the Laplace transform of $In_{cr,e}$ is given by

$$
\begin{aligned}
&\zeta_{In_{cr,e}}(cr)=\exp\{-\lambda_{cr}\rho_{cr}\pi\Gamma(1+2)\Gamma(1-2/\alpha)cr^{2/\alpha}-\lambda_{ap} \\
&\times\rho_{ap}\pi\mu^{2/\alpha}\Gamma(1+2/\alpha)\Gamma(1-2/\alpha)cr^{2/\alpha}\}
\end{aligned}
\tag{13}
$$

Substituting (14) into (13) the CDF of $\gamma_{cr,e}$ is given as

$$
\begin{aligned}
F_{\gamma_{cr,e}}(\gamma th) &= \exp\left\{-\pi\lambda_e^{cr}\int_0^{\infty}\exp\left\{-(\lambda_{cr}\rho_{cr}+\lambda_{ap}\rho_{ap}\mu^{2/\alpha}\right\}\pi\right\} \\
&\Gamma(1+2/\alpha)\Gamma(1-2/\alpha)(\gamma th)^{2/\alpha}t-\delta^2\gamma tht^{\alpha/2}/P_s\}dt
\end{aligned}
\tag{14}
$$

C. Average Secrecy Rate

The average secrecy rate between the CR and the AP is the average of secrecy rate C_{cr}^{ap} over γ_{ap} and $\gamma_{cr,e}$ is given by

$$
\bar{C}_{cr}^{ap}=1/\ln 2\int_0^{\infty}\frac{F_{\gamma_{cr,e}}(x)}{1+x}(1-F_{\gamma_{ap}}(x))dx \tag{15}
$$

Substituting the CDF of γ_{ap} in (12) and the CDF of $\gamma_{cr,e}$ in (15) into (16), the average secrecy rate between the CR and the AP can be obtained.

IV. Numerical Results and Analysis

Numerical examples are presented to show the average secrecy rate of the AF-CSS-CRN. A summary of the parameters used are presented in Table 1.

TABLE I
SUMMARY OF PARAMETERS

Parameters	Values
SUs transmit power P_{cr}	12 dBm
Power Spectral Density of Noise N_0	150 dBm/Hz
Channel Gain	complex Gaussian distribution with zero mean and unit variance
Bandwidth	1 Mhz
Number of Antennas M	1 - 4

In Fig. 2 and Fig. 3, an exact match between the simulations and the precise analytical curves are presented, that validated the analysis. In Fig. 2 the average secrecy rate between the CR and the AP versus $\lambda_e^{cr}/\lambda_{cr}$ is presented where $\lambda_{cr}=10^{-3}$, $\rho_{cr}=0.02$, $\lambda_{ap}=10^{-3}$, $\rho_{ap}=0.2$, $\alpha=3.0$, $P_{ap}=20$ dBm. Firstly, it can be seen that the average secrecy rate decreases as the density of eavesdroppers that hijacks the transmission between the CR and AP increases, owing to the damaging effects of eavesdropping. Secondly, as the number of antennas M at the AP increases, the average secrecy rate increases, due to the array gain brought about by using MRC at the AP.

In Fig. 3, the average secrecy rate between the CR and AP versus λ_{cr} for different values of λ_{ap} and M are presented, where $\lambda_{cr}.\rho_s=0.04$, $\rho_{ap}=0.4$ $\lambda_e^{cr}=10^{-3}$, $\alpha=3.0$, $P_{ap}=20$ dBm. It can be seen that the average secrecy rate increases as λ_{ap} increases due to the distance between the distinctive CR and distinctive AP decreasing. It can be observed that for equal number of antennas M, the average secrecy rate is nearly constant for $\lambda_{cr}<10^{-3}$, this is because the interference from other CRs are less significant than that from active APs. Increasing the interference marginally from CRs imposes insignificant effects on the system performance. Nevertheless, when $\lambda_{cr}>10^{-3}$, the interference from additional CRs is akin with the interference from the active APs, and increasing the interference from the CR is detrimental on the secrecy performance. Finally, an increase in λ_{ap} lessens the decreasing trend of the average secrecy rate when λ_{cr} increases.

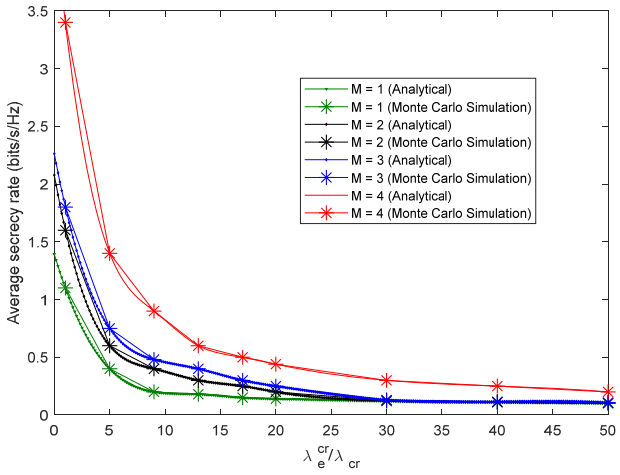

Fig. 2. Average secrecy rate versus $\lambda_e^{cr}/\lambda_{cr}$, $\lambda_{cr}=10^{-3}$, $\rho_{cr}=0.02$, $\lambda_{ap}=10^{-3}$, $\rho_{ap}=0.2$, $\alpha=3.0$, $P_{ap}=20$ dBm.

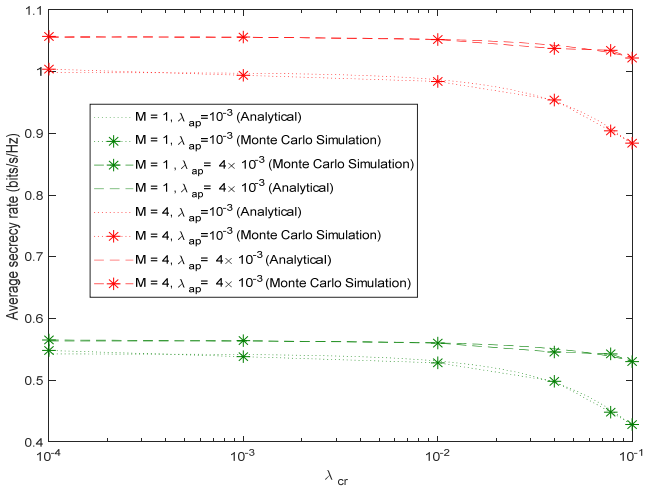

Fig. 3. Average secrecy rate versus λ_{cr}.$\rho_s=0.04$, $\rho_{ap}=0.4$ $\lambda_e^{cr}=10^{-3}$, $\alpha=3.0$, $P_{ap}=20$ dBm.

V. Conclusion

In this paper, we have analyzed the physical layer security of an AF-CSS-CRN scheme. The impact of random positions and spatial densities of CR and AP and external eavesdroppers on the secrecy performance have been analyzed. The results presented have highlight the importance of secure transmission in a practical CRN.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal,* vol. 28, no. 4, pp. 656-715, 1949.

[2] L. Lai, H. E. Gamal, and H. V. Poor, "The Wiretap Channel With Feedback: Encryption Over the Channel," *IEEE Transactions on Information Theory,* vol. 54, no. 11, pp. 5059-5067, 2008.

[3] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal,* vol. 54, no. 8, pp. 1355-1387, 1975.

[4] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory,* vol. 24, no. 3, pp. 339-348, 1978.

[5] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless Information-Theoretic Security," *IEEE Transactions on Information Theory,* vol. 54, no. 6, pp. 2515-2534, 2008.

[6] Y. Liang, H. V. Poor, and S. Shamai, "Secure Communication Over Fading Channels," *IEEE Transactions on Information Theory,* vol. 54, no. 6, pp. 2470-2492, 2008.

[7] P. K. Gopala, L. Lai, and H. E. Gamal, "On the Secrecy Capacity of Fading Channels," *IEEE Transactions on Information Theory,* vol. 54, no. 10, pp. 4687-4698, 2008.

[8] Y. Oohama, "Coding for relay channels with confidential messages," in *Proceedings 2001 IEEE Information Theory Workshop (Cat. No.01EX494)*, 2001, pp. 87-89.

[9] D. Lun, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in *2008 46th Annual Allerton Conference on Communication, Control, and Computing*, 2008, pp. 1132-1138.

[10] M. Yuksel and E. Erkip, "Secure Communication with a Relay Helping the Wire-tapper," in *2007 IEEE Information Theory Workshop*, 2007, pp. 595-600.

[11] F. He, H. Man, and W. Wang, "Maximal Ratio Diversity Combining Enhanced Security," *IEEE Communications Letters,* vol. 15, no. 5, pp. 509-511, 2011.

[12] H. Ding, Y. Fang, X. Huang, M. Pan, P. Li, and S. Glisic, "Cognitive Capacity Harvesting Networks: Architectural Evolution Toward Future Cognitive Radio Networks," *IEEE Communications Surveys & Tutorials,* vol. 19, no. 3, pp. 1902-1923, 2017.

[13] M. Cui, B. Hu, X. Li, H. Chen, S. Hu, and Y. Wang, "Energy-Efficient Power Control Algorithms in Massive MIMO Cognitive Radio Networks," *IEEE Access,* vol. 5, pp. 1164-1177, 2017.

[14] M. Luís, R. Oliveira, R. Dinis, and L. Bernardo, "RF-Spectrum Opportunities for Cognitive Radio Networks Operating Over GSM Channels," *IEEE Transactions on Cognitive Communications and Networking,* vol. 3, no. 4, pp. 731-739, 2017.

[15] I. Stanojev and A. Yener, "Improving Secrecy Rate via Spectrum Leasing for Friendly Jamming," *IEEE Transactions on Wireless Communications,* vol. 12, no. 1, pp. 134-145, 2013.

[16] A. Singh, M. R. Bhatnagar, and R. K. Mallik, "Physical Layer Security of a Multiantenna-Based CR Network With Single and Multiple Primary Users," *IEEE Transactions on Vehicular Technology,* vol. 66, no. 12, pp. 11011-11022, 2017.

[17] Y. Wu and K. J. R. Liu, "An Information Secrecy Game in Cognitive Radio Networks," *IEEE Transactions on Information Forensics and Security,* vol. 6, no. 3, pp. 831-842, 2011.

[18] I. K. Ahmed and A. O. Fapojuwo, "Stackelberg Equilibria of an Anti-Jamming Game in Cooperative Cognitive Radio Networks," *IEEE Transactions on Cognitive Communications and Networking,* vol. 4, no. 1, pp. 121-134, 2018.

[19] W. Wang, A. Kwasinski, D. Niyato, and Z. Han, "Learning for Robust Routing Based on Stochastic Game in Cognitive Radio Networks," *IEEE Transactions on Communications,* vol. 66, no. 6, pp. 2588-2602, 2018.

[20] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," *IEEE Transactions on Signal Processing,* vol. 58, no. 3, pp. 1875-1888, 2010.

[21] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Communications,* vol. 6, no. 16, pp. 2676-2687, 2012.

[22] A. Yener and S. Ulukus, "Wireless Physical-Layer Security: Lessons Learned From Information Theory," *Proceedings of the IEEE,* vol. 103, no. 10, pp. 1814-1825, 2015.

[23] D. Ta, N. Nguyen-Thanh, P. Maillé, and V. Nguyen, "Strategic Surveillance Against Primary User Emulation Attacks in Cognitive Radio Networks," *IEEE Transactions on Cognitive Communications and Networking,* vol. 4, no. 3, pp. 582-596, 2018.

[24] Y. Zou, J. Zhu, L. Yang, Y. Liang, and Y. Yao, "Securing physical-layer communications for cognitive radio networks," *IEEE Communications Magazine,* vol. 53, no. 9, pp. 48-54, 2015.

[25] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the Security of Cognitive Radio Networks," *IEEE Transactions on Vehicular Technology,* vol. 64, no. 8, pp. 3790-3795, 2015.

[26] O. Simpson, Y. Abdulkadir, Y. Sun, and B. Chi, "Relay-Based Cooperative Spectrum Sensing with Improved Energy Detection In Cognitive Radio," in *2015 10th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA)*, 2015, pp. 227-231.

[27] T. Kwon and J. M. Cioffi, "Random Deployment of Data Collectors for Serving Randomly-Located Sensors," *IEEE Transactions on Wireless Communications,* vol. 12, no. 6, pp. 2556-2565, 2013.