A Stochastic based Physical Layer Security in Cognitive Radio Networks: Cognitive Relay to Fusion Center

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*— Cognitive radio networks (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. A framework for developing the accomplishable benefits of physical layer security (PLS) 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 the spectrum sensing data from secondary users (SU) are collected by a fusion center (FC) with the assistance of access points (AP) as cognitive relays, and when malicious eavesdropping SU are listening. In this paper we focus on the secure transmission of active APs relaying their spectrum sensing data to the FC. Closed expressions for the average secrecy rate are presented. Analytical formulations and results substantiate our analysis and demonstrate that multiple antennas at the APs is capable of improving the security of an AF-CSS-CRN. The obtained numerical results also show that increasing the number of FCs, leads to an increase in the secrecy rate between the AP and its correlated FC.**

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

I. Introduction

Due to the broadcast nature of transmission techniques 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 the problem, traditional cryptographic methods are set out on the higher layers of network protocols. Traditional security techniques are not essentially 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 distinctive features from the lower layer, has become a new research focus for several wireless communication networks.

A. Related Work

The fundamental research on physical layer secure communication was researched 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 were researched by [5]. Where 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 approaches for a relay node to improve the secrecy of a wiretap channel were explored in [8-10]. A technique of employing channel diversity to improve the 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 CRNs are not exempt. Especially, security of CRN is perilous [15-19]. The proposal of reliable weighted relays and distribution of transmission power with diverse relaying protocols, for instance amplify-and-forward (AF), decode-and-forward (DF), in addition to cooperative jamming were presented in [20]. Relay preference was proposed for secure CRN with a sole eavesdropper was suggested in [21]. To exploit the security feature of CRNs, 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 primary users (PU) is of the utmost importance of CRNs. Nevertheless, this mechanism introduces susceptibilities that may permit an attacker to disguise as a PU that occupies a licensed share of the spectrum and cause a denial-of-

Accepted Manuscript.
Paper presented at the IEEE 38th International Performance Computing and Communications Conference (IPCCC) 2019, 21/10/19 - 31/10/19,
https://doi.org/10.1109/IPCCC47392.2019.8958756

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 problem in 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 ideal solution because the unfilled diversity paths are underutilized. It provides the inspiration in this paper to use maximal-ratio combining for increased security. In this paper, a channel diversity with maximal-ratio combining is proposed to increase the secrecy capacity as in comparison to the SC scheme proposed in [25], by taking advantage of the physical characteristics in the wireless channels to achieve ideal secrecy against eavesdroppers [24, 26].

B. *Method and Contributions*

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 are proposed in this paper. In an AF-CSS-CRN, the SUs are positioned remote from the FC, and the access points (AP) are positioned to support the SUs transmit individual sensing data to the FC. This private data transmission can be hijacked by malicious eavesdroppers. Assuming that SUs are heavily deployed and their positions are randomly distributed, a stochastic geometry, namely a homogeneous Poisson point process is used to model the positions of the CRs in the CRN. The spectrum sensing and amplification technique used in this work can be found in the author's previous work in [27]. The main contributions of this paper are listed as follows:

1. An analytical framework to analyze the implementation of physical layer security in AF-CSS-CRN is developed.
2. The positions and spatial densities of SUs, APs, FCs, and eavesdroppers are modeled by means of stochastic geometry. Individually APs are furnished with MIMO antennas and make use of the low complexity maximal-ratio-combining to receive the sensing data from the SUs and maximal-ratio-transmission beamformer to transmit the signals.
3. Statistical properties are presented, centered on which new closed formulation relating to the average secrecy rate between the distinctive AP and its correlated FC are derived[*1].
4. A novel compact expression for the average secrecy rate between the AP and the FC is derived.

This paper is organized as follows: Section II presents the system model. Section III presents the average secrecy rate between the APs and FCs. Section IV presents the numerical results corroborating with detailed analysis and finally Section V provides concluding remarks.

II. System Model

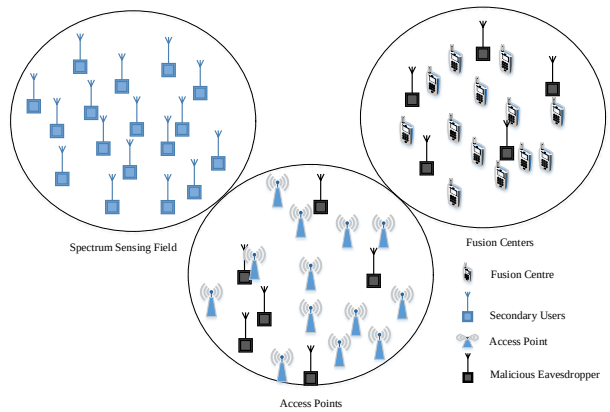

Fig. 1. An AF-CSS-CRN: the SUs transmit sensing data to the FCs through the APs, when eavesdroppers are present.

The CRN system model is presented in Fig. 1, the SUs transmit sensing data to the fusion centre (FC) by means of a half duplex amplify-and-forward (AF) access points (APs) without straight links amongst SUs and FCs. The eavesdroppers listen into both sensing data transmissions devoid of altering the data. SUs are unsystematically 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 a complete random HPPPs Φ_{ap} and Φ_{fc} with intensities λ_{ap} and λ_{fc}, respectively, that is appropriate in wide scale systems [28]. The SUs transmit spectrum sensing data sporadically. Therefore, the probability that a SU is prompted into transmitting the sensing data is represented as ρ_{cr}, $0<\rho_{cr}<1$, and the probability that an AP is activated to amplifies and forwards the sensing data to the FC is represented as ρ_{cr}, $0<\rho_{cr}<1$. The probability of being an active SU or AP is assumed to be completely random of the SU or AP position. Hence the active SU or AP is made up of complete random 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 completely random HPPPs $\Phi_{cr,e}$ and $\Phi_{ap,e}$ with intensities λ_e^{cr} and λ_e^{ap}, respectively. The data transmitted by the SU is

[1] The average secrecy rate between the distinctive SU and its correlated AP are derived in in the author's previous work in [29].

Accepted Manuscript.
Paper presented at the IEEE 38th International Performance Computing and Communications Conference (IPCCC) 2019, 21/10/19 - 31/10/19,
https://doi.org/10.1109/IPCCC47392.2019.8958756

hijacked by the eavesdroppers in $\Phi_{cr,e}$ and the sensing data transmitted through the AP is hijacked by the eavesdroppers in $\Phi_{ap,e}$.

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

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

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 individual valuable sensing data to their corresponding FCs using maximal-ratio-transmission 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 maximal-ratio combining vector $\frac{\mathbf{h}_{cr_0,ap_0}^{\dagger}}{\left\|\mathbf{h}_{cr_0,ap_0}\right\|}$, where $\mathbf{h}_{cr_0,ap_0}$ is the channel fading vector and $\left|X_{cr_0,ap_0}\right|$ is the distance from the distinctive SU to its distinctive AP. Where α represents the path-loss exponent, $\mathbf{h}_{i,ap_0} \in C^{M\times 1}$ is the channel fading vector from the *i*-th SU to the distinctive AP and $\left|X_{i,ap_0}\right|$ the distance from the *i*-th SU to the distinctive AP. $\mathbf{H}_{j,ap_0}$ is the channel fading matrix amongst the interfering *j*-th AP and the distinctive AP, while $\left|X_{j,ap_0}\right|$ is the distance amongst the interfering *j*-th AP and the distinctive AP. $\mathbf{h}_{j,fc_j} \in C^{1\times M}$ is the channel fading vector amongst the interfering *j*-th AP and its equivalent FC, δ^2 is the noise power, P_{cr} is the SU's transmission power, and P_{ap} is the AP's transmission power.

In the non- collaboration eavesdropping situation, the greatest damaging eavesdropper that possess the uppermost received SINR dictates the secrecy rate [15]. A random eavesdropper e_k that hijacks the SU and the AP transmission listen to the valuable sensing data from the distinctive SU to the distinctive AP, and concurrently acquires the interfering sensing data from the additional active SUs and active AP. e_k is impaired by the interfering signals transmitted from additional interfering AP using the maximal-ratio-transmission 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 SU and the AP transmission is known by

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

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

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

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

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

where $In_{ap,fc} = \sum_{j\in\Phi_{ap,a}\setminus\{ap_0\}} \left| \mathbf{g}_{j.fc_0} \frac{\mathbf{h}_{j,fc_j}^{\dagger}}{\left\|\mathbf{h}_{j,fc_j}\right\|} \right|^2 \left|X_{j,fc_0}\right|^{-\beta}$,

$\mathbf{g}_{ap_0,fc_0} \in C^{1\times M}$ is the channel fading vector and $\left|X_{ap_0,fc_o}\right|$ is the distance between the distinctive AP and its distinctive FC. Where β is the path-loss exponent,

Accepted Manuscript.
Paper presented at the IEEE 38th International Performance Computing and Communications Conference (IPCCC) 2019, 21/10/19 - 31/10/19,
https://doi.org/10.1109/IPCCC47392.2019.8958756

$\mathbf{g}_{j,fc_0} \in C^{1\times M}$ and $\left|X_{j,fc_0}\right|$ are the channel fading vector and distance between the *j*-th AP and the distinctive FC, and $\mathbf{h}_{j,fc_0} \in C^{1\times M}$ is the channel fading vector between the *j*-th AP and its correlated FC. A random eavesdropper e_k which hijacks the distinctive AP and the distinctive FC sensing data transmission listens into the signal which is transmitted by the distinctive AP with the maximal-ratio-transmission beamformer $\frac{\mathbf{g}_{ap_0,fc_0}^{\dagger}}{\left\|\mathbf{g}_{ap_0,fc_0}\right\|}$, and experience degradation due to the interfering signals caused through other interfering APs emission with the maximal-ratio-transmission beamformer $\frac{\mathbf{h}_{j,fc_k}^{\dagger}}{\left\|\mathbf{h}_{j,fc_k}\right\|}$. Consequently, the receive SINR possessed at the utmost unfavourable eavesdropper for the AP and the FC transmission is given as

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

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 $\mathbf{g}_{j,e_k}$ is the channel fading vector and $\left|X_{j,e_k}\right|$ is the distance from the *j*-th AP to the eavesdropper, respectively.

III. Secrecy Rate Between AP and FC

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, in the case of a distinctive link between a distinctive AP and its correlated FC, the momentary secrecy rate is given by

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

where $[x]^{\diamond} = \max\{y, 0\}$, $C_{fc} = \log_2(1+\gamma_{fc})$ is the capacity of the channel between the distinctive AP and FC, and $C_{ap,e} = \log_2(1+\gamma_{ap,e})$ is the capacity of the eavesdropping channel between the distinctive AP 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 SU and AP are derived in the following subsection.

A. CDF of SINR at the distinctive FC

Taking (3) into consideration, the CDF of γ_{fc} is presented as

$$\begin{aligned} F_{\gamma_{ap}}(\gamma th) &= \int_0^{\infty} \Pr\left[\frac{\left\|\mathbf{g}_{ap_0,fc_0}\right\|^2 r^{-\beta}}{In_{ap,fc} + \delta^2 / P_{ap}} \le \gamma_{th}\right] f_{\left|X_{ap_0,fc_0}\right|}(r)\, dr \\ &= \int_0^{\infty} \Pr\left[\frac{\left\|\mathbf{g}_{ap_0,fc_0}\right\|^2 r^{-\beta}}{In_{ap,fc} + \delta^2 / P_{ap}} \le \gamma_{th}\right] 2\pi\lambda_{fc} r \\ &\quad \times \exp(-\pi\lambda_{fc} r^2) \end{aligned} \tag{6}$$

where $f_{\left|X_{ap_0,fc_0}\right|}(r)$ is the PDF of the nearest distance between the SU and the distinctive FC. The CDF of the FC SINR at distance *r* from its corresponding AP is given by

$$\begin{aligned} &\Pr\left[\frac{\left\|\mathbf{g}_{ap_0,fc_0}\right\|^2 r^{-\beta}}{In_{ap,fc} + \delta^2 / P_{ap}} \le \gamma_{th}\right] \\ &= 1 - \sum_{m=0}^{M-1} \frac{1}{m!} \mathbb{E}_{\Phi_{ap,a}} \\ &\times \{\int_0^{\infty} [\gamma_{th} r^{\beta} (\tau + \delta^2 / P_{ap})]^m \\ &\exp[-\gamma_{th} r^{\beta} \times (\tau + \delta^2 / P_{ap}) d \Pr(In_{ap,fc} \le \tau)\}. \end{aligned} \tag{7}$$

Substituting

$$(-(\tau + \delta^2 / P_{ap})\gamma_{th})^m e^{-(\tau+\delta^2/P_{ap})\gamma_{\gamma_{th}}^{(s)} r^{\beta}} = \left.\frac{d^m (e^{-\gamma_{th} x(\tau+\delta^2/P_{ap})})}{dx^m}\right|_{x=r^{\beta}}$$

into (7), and rewriting the CDF in relation to the FC SINR at distance *r* from its correlated AP gives

$$\begin{aligned} &\Pr\left[\frac{\left\|\mathbf{g}_{ap_0,fc_0}\right\|^2 r^{-\beta}}{In_{ap,fc} + \delta^2 / P_{ap}} \le \gamma_{th}\right] \\ &= 1 - \mathbb{E}_{\Phi_{fc,a}} \{\int_0^{\infty} \exp[-\gamma_{th} r^{\beta} (\tau + \delta^2 / P_{cr})]\, d \Pr \\ &\times (In_{ap,fc} \le \tau)\} - \sum_{m=1}^{M-1} \frac{(r^{\beta})^m}{m!(-1)^m} \mathbb{E}_{\Phi_{ap,a}} \\ &\times \{\int_0^{\infty} \left.\frac{d^m (e^{-\gamma_{th} x(\tau+\delta^2/P_{ap})})}{dx^m}\right|_{x=r^{\beta}} d \Pr\ (In_{ap,fc} \le \tau)\} \\ &= 1 - \exp(-\gamma_{th} r^{\beta} \delta^2 / P_{ap}) \zeta_{in_{ap,fc}}(\gamma_{th} r^{\beta}) \\ &- \sum_{m=1}^{M-1} \frac{(r^{\beta})^m}{m!(-1)^m} \cdot \left.\frac{d^m (\exp(-\gamma_{th} x \delta^2 / P_{ap}) \zeta_{in_{ap,fc}}(\gamma_{th} x))}{dx^m}\right|_{x=r^{\beta}} \end{aligned} \tag{8}$$

Subsequently,

$$In_{ap,fc} = \sum_{j\in\Phi_{ap,a}\setminus\{ap_0\}} \left|\mathbf{g}_{j,fc_0} \mathbf{h}_{j,fc_j}^{\dagger} \Big/ \left\|\mathbf{h}_{j,fc_j}\right\|\right|^2 \left|X_{j,fc_0}\right|^{-\beta}$$

obtained from the HPPP in [16] and

Accepted Manuscript.
Paper presented at the IEEE 38th International Performance Computing and Communications Conference (IPCCC) 2019, 21/10/19 - 31/10/19, https://doi.org/10.1109/IPCCC47392.2019.8958756

$$
\begin{aligned}
F_{\gamma_{fc}}(x) = {} & 1 - 2\pi\lambda_{fc}\int_0^{\infty} r\exp\left\{-\lambda_{ap}\rho_{ap}\pi\ \Gamma(1+2/\beta)\Gamma(1-2/\beta)(\gamma th)^{\frac{2}{\beta}} r^2 - \gamma_{th} r^{\beta}\delta^2 / P_{ap} - \pi\lambda_{fc} r^2\right\} dr \\
& - 2\pi\lambda_{fc}\sum_{m=1}^{M-1}\frac{1}{(-1)^m}\sum\frac{1}{\prod_{l=1}^{m} m_l!\, l!^{ml}} \\
& \times\int_0^{\infty} r^{\beta m+1}\exp\left\{-(\lambda_{ap}\rho_{ap}\pi\ \Gamma(1+2/\beta)\ \Gamma(1-2/\beta)(\gamma th)^{\frac{2}{\beta}} r^2 - \gamma thr^{\beta}\delta^2 / P_{ap} - \pi\lambda_{fc} r^2\right\} \\
& \times[-\lambda_{ap}\rho_{ap}\pi\frac{2}{\beta}\ \Gamma(1+2/\beta)\ \Gamma(1-2/\beta)(\gamma th)^{\frac{2}{\beta}} r^{(2-\beta)} - \gamma_{th}\delta^2 / P_{ap}]^{m1}\prod_{l=2}^{m} \\
& \times[-\lambda_{ap}\rho_{ap}\pi\ \Gamma(1+2/\beta)\ \Gamma(1-2/\beta)(\gamma th)^{\frac{2}{\beta}}\prod_{j=0}^{l-1}(2/\beta - j) r^{2-l\beta}]^{m_l}\, dr
\end{aligned}
\tag{12}
$$

$\left|\mathbf{g}_{j,fc_0}\mathbf{h}_{j,fc_j}{}^{\dagger}\Big/\left\|\mathbf{h}_{j,fc_j}\right\|\right|^2 \sim \exp(1)$. Considering Slivnyak-Mecke poisson process theorem, the Laplace transform of $In_{ap,sk}$ is given as

$$
\begin{aligned}
& \zeta_{In_{ap,}cr}(cr) \\
& = \mathbb{E}_{\Phi_{ap,a}}\left[\exp\left\{-ap\sum_{i\in\Phi_{ap,a}\setminus\{cr_0\}}\left|\mathbf{g}_{j,fc_0}\frac{\mathbf{h}_{j,fc_j}{}^{\dagger}}{\left\|\mathbf{h}_{j,fc_j}\right\|}\right|^2\left|X_{j,fc_0}\right|^{-\beta}\right\}\right] \\
& = \exp\left\{-2\pi\lambda_{ap}p_{ap}\int_0^{\infty}\left(1-\zeta_{j.\frac{\mathbf{h}_{j,fc_j}{}^{\dagger}}{\left\|\mathbf{h}_{j,fc_j}\right\|}\mathbf{g}_{j,fc_0}}(cry^{-\beta})\right)ydy\right\} \quad (9.1) \\
& = \exp\left\{-2\pi\lambda_{ap}p_{ap}\int_0^{\infty}\left(1-\frac{1}{1+cry^{-\beta}}\right)ydy\right\} \quad (9.2) \\
& = \exp\left\{-\lambda_{ap}p_{ap}\pi\ \Gamma(1+2/\beta)\Gamma(1-2/\beta)cr^{2/\beta}\right\}
\end{aligned}
$$

(9.1) is obtained from the HPPP in [16], (9.2) is obtained from $\left|\mathbf{g}_{j,fc_0}\frac{\mathbf{h}_{j,fc_j}{}^{\dagger}}{\left\|\mathbf{h}_{j,fc_j}\right\|}\right|^2$. Substituting (8) into (9) gives

$$
\begin{aligned}
& \Pr\left[\frac{\left\|\mathbf{g}_{ap_0,fc_0}\right\|^2 r^{-\beta}}{In_{ap,fc}+\delta^2/P_{ap}} \le \gamma_{th}\right] \\
& = 1-\exp\left\{-\lambda_{ap}p_{ap}\pi\ \Gamma(1+2/\beta)\Gamma(1-2/\beta)cr^{2/\beta}\right\} \quad (10) \\
& \times\{(\gamma_{th})^{2/\beta}r^2 - \gamma_{th}r^{\beta}\delta^2/P_{ap})\} \\
& -\sum_{m=1}^{M-1}\frac{(r^{\beta})^m}{m!(-1)^m}\cdot\left.\frac{d^m(W(x))}{dx^m}\right|_{x=r^{\beta}}
\end{aligned}
$$

where $W(x) = \exp\{-\lambda_{ap}p_{ap}\pi\ \Gamma(1+2/\beta)\Gamma(1-2/\beta)$ $(\gamma_{th}x)^{2/\beta} - \gamma_{th}x\delta^2/P_{ap}\}$. By applying the Fao de Bruno's formula to workout the derivation of the *m*-th order the following is obtained:

$$
\begin{aligned}
& \left.\frac{d^m[\exp(W(x))]}{dx^m}\right|_{x=r^{\beta}} \\
& = \sum\frac{1}{\prod_{l-1}^{m} m_l!\, l!^{ml}}\exp\{-\lambda_{ap}p_{ap}\pi\ \Gamma(1+2/\beta)\Gamma(1-2/\beta \\
& \times(\gamma_{th})^{2/\beta}r^2 - \gamma_{th}r^{\beta}\delta^2/P_{ap})\} \\
& \times[-\lambda_{ap}p_{ap}\pi\ \frac{2}{\beta}\Gamma(1+2/\beta)\ \Gamma(1-2/\beta) \quad (11) \\
& \times(\gamma_{th})^{2/\beta}x^{2/\beta-1} - \gamma_{th}\delta^2/P_{ap})]^{m_l} \\
& \times\prod_{l-2}^{m}[-\lambda_{ap}p_{ap}\pi\ \Gamma(1+2/\beta\ \Gamma(1-2/\beta) \\
& \times(\gamma_{th})^{2/\beta}\prod_{j=0}^{l-1}(2/\beta - j)x^{2/\beta-l}]^{m_l}
\end{aligned}
$$

Subsequently substituting the derivation from (11) and (10) into (6) gives the CDF of γ_{fc} as shown in (12).

B. The CDF of SINR at the most detrimental eavesdropper between the APs and FCs

The CDF of SINR at the utmost unfavourable eavesdropper which hijacks the transmitted signal between the distinctive AP and the FC is solved by taking (4) into consideration, the CDF of $\gamma_{ap,e}$ is derived as follows:

$$
\begin{aligned}
& F_{\gamma_{cr,e}}(\gamma th) = \\
& \mathbb{E}_{\Phi_{ap,a}}\left\{\mathbb{E}_{\Phi_{ap,e}}\left\{\prod_{e\Phi_{ap,e}}\Pr\left\{\frac{\left|g_{ap_0,e_k}\right|^2\left|X_{ap_0,e_k}\right|^{-\beta}}{In_{ap,e}+\delta^2/P_{ap}}\right\}\le\gamma_{th}\left|\Phi_{ap,a}\Phi_{ap,e}\right|\right\}\right\} \\
& = \exp\left\{-\lambda_e^{ap}\int_{R^2} e^{-\delta^2\gamma_{th}\left|X_{ap0,ek}\right|^{\beta}/P_{ap}}\zeta_{In_{ap,e}}(\gamma_{th}\left|X_{ap_0,e_k}\right|^{\beta})\, dr\right\} \quad (13.1) \\
& = \exp\left\{-2\pi\lambda_e^{ap}\int_0^{\infty} e^{-\delta^2\gamma_{th}r^{\beta}/P_{ap}}\zeta_{In_{ap,e}}\times(\gamma_{th}r^{\beta})r\ dr\right\} \quad (13.2)
\end{aligned}
$$

Accepted Manuscript.
Paper presented at the IEEE 38th International Performance Computing and Communications Conference (IPCCC) 2019, 21/10/19 - 31/10/19,
https://doi.org/10.1109/IPCCC47392.2019.8958756

where, (13.1) and (13.2) are obtained from the HPPP and polar coordinates, respectively. From the functional HPPP in [16] the Laplace transform of $I_{ap,e}$ is given as

$$\zeta_{In_{ap,e}}(cr) = \exp\{-\lambda_{ap}\rho_{ap}\pi\ \Gamma(1+2/\beta) \times \Gamma(1-2/\beta)cr^{2/\beta}\} \quad (14)$$

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

$$F_{\gamma_{ap,e}}(\gamma th) = \exp\{-\pi\lambda_e^{ap} \times \int_0^\infty \exp\left\{-(\lambda_{ap}\rho_{ap}\pi\ \Gamma(1+2/\beta)\Gamma(1-2/\beta)\right\} \times \Gamma(1-2/\beta)(\gamma_{th})^{2/\beta}t - \sigma^2\gamma_{th}t^{\beta/2}/P_{ap}\}dt\} \quad (15)$$

C. Average Secrecy Rate

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

$$\bar{C}_{cr}^{fc} = 1/\ln 2\int_0^\infty \frac{F_{\gamma_{fc}}(x)}{1+x}(1-F_{\gamma_{ap,e}}(x))dx \quad (16)$$

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

IV. Numerical Results and Analysis

TABLE I
SUMMARY OF PARAMETERS

Parameters	Values
SUs transmit power P_{cr}	12 dBm
Power Spectral Density of Noise N_0	–160 dBm/Hz
Channel Gain	complex Gaussian distribution with zero mean and unit variance
Bandwidth	1.5 MHz
Number of Antennas M	1 - 4

Numerical examples are presented to show the average secrecy rate of the AF-CSS-CRN between the APs and FCs. A summary of the parameters used are presented in Table 1. In Fig. 2 and Fig. 3, an exact match between the simulations and the precise analytical curves are presented, which validated the theoretical formulations.

In Fig. 2 the average secrecy rate between the AP and the FC versus $\lambda_e^{ap}/\lambda_{ap}$ for different λ_e^{ap} and M is observed, where $\rho_{ap} = 0.2$, $\beta = 3.0$, $\lambda_{fc} = 10^{-3}$ and $P_{ap} = 18$ dBm. The numerical results are acquired from (16). Firstly, it can be seen that the average secrecy rate decreases as $\lambda_e^{ap}/\lambda_{ap}$ increases, which points toward the fact that more APs are needed as the intensity of eavesdroppers who hijack the transmitted sensing data between AP and FC increases, owing to the damaging consequences of eavesdropping. Secondly, as the number of antennas M at the AP increases, the average secrecy rate between the AP and FC increases due to the array gain brought about by using maximal-ratio combining at the AP. Using the identical number of antennas at the AP, the average secrecy rate decreases as λ_e^{ap} increases.

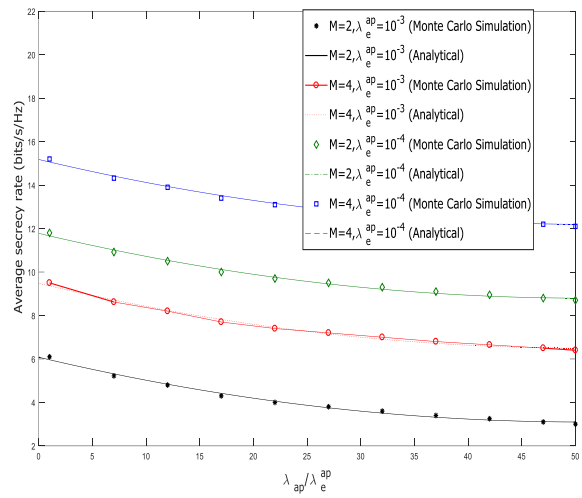

Fig. 2. Average secrecy rate versus $\lambda_{ap}/\lambda_e^{ap}$.

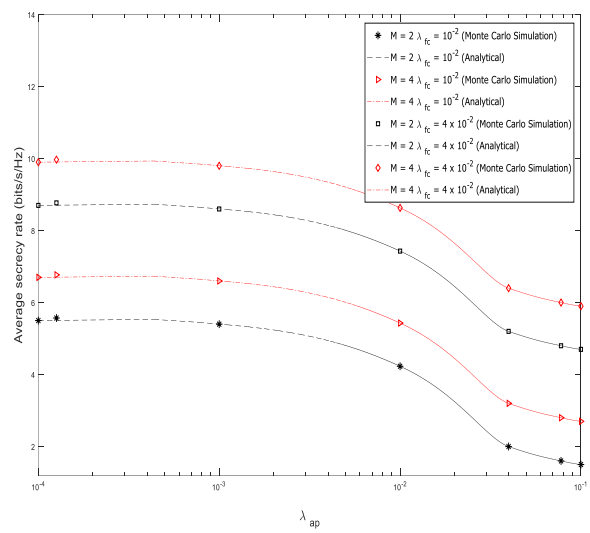

Fig. 3. Average secrecy rate versus λ_{ap}.

In Figure 3, the average secrecy rate between the AP and the FC versus λ_{ap} for different values of λ_{fc} and M are presented, where $\lambda_{ap}.\rho_{ap} = 0.2$, $\lambda_e^{ap} = 10^{-3}$, $\beta = 3.0$, and $P_{ap} = 20$ dBm. The numerical results are acquired from (16). Firstly, it can be seen that the average secrecy rate changes marginally when $\lambda_{ap} < 3\times10^{-3}$, and decreases as λ_{ap} increases when $\lambda_{ap} > 3\times10^{-3}$, due to the fact that when $\lambda_{ap} < 3\times10^{-3}$, the interference from additional active APs is comparatively small in relation to the noise, while increasing the number of AP hardly has an effect on the system performance. Nevertheless, when $\lambda_{ap} > 3\times10^{-3}$ the interference from the APs has a significant effect on the SINR between the AP and the

Accepted Manuscript.
Paper presented at the IEEE 38th International Performance Computing and Communications Conference (IPCCC) 2019, 21/10/19 - 31/10/19, https://doi.org/10.1109/IPCCC47392.2019.8958756

FC. Consequently, an increase in the interference from the AP worsens the average secrecy rate. Finally, it can be realised that the average secrecy rate between the AP and FC increases when the density of the FC increases. This is due to the fact that the distance between the distinctive AP and the corresponding FC turns out to be shorter.

V. Conclusion

In this paper, we have presented and analyzed the physical layer security of an AF-CSS-CRN scheme. The impact of random positions and spatial densities of SU, AP and FC and external eavesdroppers and number of antennas at the AP on the secrecy performance have been analyzed. A vital result presented by analytical formulations and Monte Carlo simulation is the least total of FCs necessary when the average secrecy rate is set, that assists secure SU cognitive radio deployment in CRNs. The results presented have highlighted the importance of secure transmission in a practical and applied 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] Y. Deng, L. Wang, M. Elkashlan, A. Nallanathan, and R. K. Mallik, "Physical Layer Security in Three-Tier Wireless Sensor Networks: A Stochastic Geometry Approach," *IEEE Transactions on Information Forensics and Security,* vol. 11, no. 6, pp. 1128-1138, 2016.

[27] 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.

[28] 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.

[29] O. Simpson and Y. Sun, "A Stochastic Method to Physical Layer Security of an Amplify-and-Forward Spectrum Sensing in Cognitive Radio Networks: Secondary User to Cognitive Relay," *15th International Wireless Communication and Mobile Computing (IWCMC)*, accepted in press, 2019.