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

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 CRNs 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-
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

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) \(\phi_s\) with intensity \(\lambda_s\). To envisage inadvertent deployment of APs and FCs the random positions of the APs and FCs are approximated as a complete random HPPPs \(\Phi_{ap}\) and \(\Phi_{fc}\) with intensities \(\lambda_{ap}\) and \(\lambda_{fc}\), 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 \(\rho_s\), \(0 < \rho_s < 1\), and the probability that an AP is activated to amplifies and forwards the sensing data to the FC is represented as \(\rho_{ap}\), \(0 < \rho_{ap} < 1\). 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 \(\Phi_{cr,s}\) and \(\Phi_{cr,ap}\), with densities \(\lambda_{cr,s}\) and \(\lambda_{cr,ap}\), respectively. It is assumed that the eavesdroppers are non-collaboration and that eavesdroppers’ positions are modelled as completely random HPPPs \(\Phi_{e,s}\) and \(\Phi_{e,ap}\), with densities \(\lambda_{e,s}\) and \(\lambda_{e,ap}\), 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].
hijacked by the eavesdroppers in $\Phi_{e,s}$, and the sensing data transmitted through the AP is hijacked by the eavesdroppers in $\Phi_{ap,s}$.

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 SU's and FCs have a single antenna. The APs use maximal-ratio combining to receive the SU's 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

$$\gamma_{ap} = \frac{\|\mathbf{h}_{o,ap}\|^2 |X_{o,ap}|^{\alpha} }{ I_{cx,ap} + I_{ap,ap} + \delta^2 / P_{ap} },$$  

(1)

where $I_{cx,ap} = \sum_{o \in \Phi_{ap,s}, \langle e, o \rangle} \left( \mathbf{h}_{e,ap} \right)^\dagger \left( \mathbf{h}_{e,ap} \right) |X_{e,ap}|^{-\alpha}$,

$$I_{ap,ap} = \mu \sum_{j \in \Phi_{ap,s}, \langle ap, j \rangle} \left( \mathbf{h}_{ap,j} \right)^\dagger \left( \mathbf{H}_{ap,j} \right) \left( \mathbf{h}_{ap,j} \right) |X_{ap,j}|^{-\alpha},$$

and $\mu = P_{ap} / P_{ap}$. Interfering APs conveys their individual valuable sensing data to their corresponding FCs using maximal-ratio-transmission beamformer vector $\mathbf{h}_{j,fc}$. These are received and combined at the distinctive AP with maximal-ratio combining vector $\mathbf{h}_{o,ap}$, where $\mathbf{h}_{e,ap}$ is the channel fading vector and $|X_{e,ap}|$ is the distance from the distinctive SU to its distinctive AP. Where $\alpha$ represents the path-loss exponent, $\mathbf{h}_{o,ap} \in \mathbb{C}^{M \times 1}$ is the channel fading vector from the $i$-th SU to the distinctive AP and $|X_{i,ap}|$ the distance from the $i$-th SU to the distinctive AP. $\mathbf{H}_{ap,j}$ is the channel fading matrix amongst the interfering $j$-th AP and the distinctive AP, while $|X_{ap,j}|$ is the distance amongst the interfering $j$-th AP and the distinctive AP.

$\mathbf{h}_{j,fc} \in \mathbb{C}^{1 \times M}$ is the channel fading vector amongst the interfering $j$-th AP and its equivalent FC, $\delta^2$ is the noise power, $P_{ap}$ 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 posses the uppermost received SINR dictates the secrecy rate [15]. A random eavesdropper $e_s$ 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 SU and active AP. $e_s$ is impaired by the interfering signals transmitted from additional interfering AP using the maximal-ratio-transmission beamformer $\mathbf{h}_{j,fc}$. Hence, the received SINR at the most unfavourable eavesdropper in $\Phi_{e,s}$ for the SU and the AP transmission is known by

$$\gamma_{e,s} = \max_{e \in \Phi_{e,s}} \left( \frac{|\mathbf{h}_{o,ap}|^2 |X_{o,ap}|^{\alpha} }{ I_{cx,e} + I_{ap,e} + \delta^2 / P_{ap} } \right),$$  

(2)

where $I_{cx,e} = \sum_{o \in \Phi_{e,s}, \langle e, o \rangle} |\mathbf{h}_{e,ap}|^2 |X_{e,ap}|^{-\alpha}$ and

$$I_{ap,e} = \mu \sum_{j \in \Phi_{e,s}, \langle ap, j \rangle} |\mathbf{h}_{ap,j}|^2 |X_{ap,j}|^{-\alpha},$$

$|\mathbf{h}_{e,ap}|$ are distinctive SU and the $e_s$, correspondingly.

$|\mathbf{h}_{ap,j}|$ is the channel fading coefficient and $|X_{ap,j}|$ is the distance between the $i$-th SUs and the eavesdropper. $|\mathbf{h}_{j,fc}|$ is the channel fading vector and $|X_{j,fc}|$ is the distance from the $j$-th AP to the eavesdropper.

The distinctive AP $ap$ will forward the sensed data to the closest FC $fc$ 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 $fc$ is given by

$$\gamma_{fc} = \frac{|\mathbf{g}_{ap,fc}|^2 |X_{ap,fc}|^\beta }{ I_{ap,fc} + \delta^2 / P_{ap} }$$  

(3)

where $I_{ap,fc} = \sum_{j \in \Phi_{e,s}, \langle ap, j \rangle} |\mathbf{g}_{j,fc}|^2 |X_{ap,j}|^{-\beta}$, $\mathbf{g}_{ap,fc} \in \mathbb{C}^{1 \times M}$ is the channel fading vector and $|X_{ap,fc}|$ is the distance between the distinctive AP and its distinctive FC. Where $\beta$ is the path-loss exponent.
the capacity of the channel between the AP and the FC, and $C_{ap,e}$ is the capacity of the eavesdropping channel between the AP and the eavesdropper. The cumulative distribution functions (CDFs) of SINRs at the AP and the worst detrimental eavesdropper that hijacks the AP are derived in the following subsection.

A. CDF of SINR at the distinctive FC

Taking (3) into consideration, the CDF of $\gamma_{fe}$ is presented as

$$
F_{\gamma_{fe}}(x) = \int_0^x f_{\gamma_{fe}}(r) dr
$$

where $f_{\gamma_{fe}}(r)$ 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

$$
\Pr \left[ \frac{\|g_{ap,f_i}\|^{-\beta}}{\ln_{ap,fe} + \delta^2 / P_{ap}} \leq \gamma_{fe} \right] = 1 - \sum_{m=0}^{M-1} \frac{1}{m!} \Phi_{\phi_{ap}}
$$

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

$$
\Pr \left[ \frac{\|g_{ap,f_i}\|^{-\beta}}{\ln_{ap,fe} + \delta^2 / P_{ap}} \leq \gamma_{fe} \right] = 1 - \mathbb{E}_{\phi_{ap}} \left[ \int_0^{(\ln_{ap,fe} + \delta^2 / P_{ap})/\gamma_{fe}} dPr \right]
$$

Subsequently,

$$
\ln_{ap,fe} = \sum_{j=0}^{M-1} g_{j,fe} h_{j,fe}^\top \left| X_{j,fe} \right|^{-\beta}
$$

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

$$
C_{fe}^{s} = (C_{fe} - C_{ap,e})
$$

where $[x] = \max \{1, x\}$, $C_{fe} = \log_2(1 + \gamma_{fe})$ is the capacity of the channel between the AP and the FC, and $C_{ap,e} = \log_2(1 + \gamma_{ap,e})$ is the capacity of the eavesdropping channel between the AP and the utmost detrimental eavesdropper. The cumulative distribution functions (CDFs) of SINRs at the distinctive AP and the worst detrimental eavesdropper that hijacks the transmission between the distinctive SU and AP are derived in the following subsection.

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
\[ F_{\gamma}(x) = 1 - 2\pi\lambda_{f_c} \int_0^x \exp\left\{ -\lambda_{a_p} \rho_{a_p} \pi \frac{r^2}{\Gamma(1 + 2/\beta) \Gamma(1 - 2/\beta) (\gamma \theta r)^{2/\beta} - (\gamma \theta r)^{2/\beta}} \right\} dr \]

\[ \times \int_0^{\infty} r^{\beta - 1} \exp\left\{ -\left(\lambda_{a_p} \rho_{a_p} \pi \frac{\Gamma(1 + 2/\beta) \Gamma(1 - 2/\beta) (\gamma \theta r)^{2/\beta} - (\gamma \theta r)^{2/\beta}}{\rho_{a_p}} \right) \right\} dr \]

\[ \times \left[ -\lambda_{a_p} \rho_{a_p} \pi \frac{2}{\beta} \Gamma(1 + 2/\beta) \Gamma(1 - 2/\beta) (\gamma \theta r)^{2/\beta - 2} - (\gamma \theta r)^{2/\beta - 2} / \rho_{a_p} \right] \prod_{r = 2}^{m} \left( 2/\beta - j \right) x^{2/\beta - j} \]  \[ \times \left[ -\lambda_{a_p} \rho_{a_p} \pi \frac{2}{\beta} \Gamma(1 + 2/\beta) \Gamma(1 - 2/\beta) (\gamma \theta r)^{2/\beta - 2} - (\gamma \theta r)^{2/\beta - 2} / \rho_{a_p} \right] \prod_{r = 2}^{m} \left( 2/\beta - j \right) x^{2/\beta - j} \]

\[ \frac{d^n[\exp(W(x))]}{dx^n} \bigg|_{x = r^\beta} = \sum_{i = 1}^{\infty} \frac{1}{m!} \exp\left\{ -\lambda_{a_p} \rho_{a_p} \pi \Gamma(1 + 2/\beta) \Gamma(1 - 2/\beta) \right\} \]

\[ \times \left[ \left( \gamma \theta r \right)^{2/\beta}, - (\gamma \theta r)^{2/\beta} / \rho_{a_p} \right] \]

\[ \times \left[ -\lambda_{a_p} \rho_{a_p} \pi \frac{2}{\beta} \Gamma(1 + 2/\beta) \Gamma(1 - 2/\beta) (\gamma \theta r)^{2/\beta}, - (\gamma \theta r)^{2/\beta} / \rho_{a_p} \right] \prod_{r = 2}^{m} \left( 2/\beta - j \right) x^{2/\beta - j} \]

Subsequently substituting the derivation from (11) and (10) into (6) gives the CDF of \( \gamma_{f_c} \) 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 \( \gamma_{a_p, f_c} \) is derived as follows:

\[ F_{\gamma_{a_p, f_c}}(x) = \exp\left\{ -\lambda_{a_p} \rho_{a_p} \pi \frac{r^2}{\Gamma(1 + 2/\beta) \Gamma(1 - 2/\beta) (\gamma \theta r)^{2/\beta} - (\gamma \theta r)^{2/\beta}} \right\} \]

\[ \times \left[ \left( \gamma \theta r \right)^{2/\beta}, - (\gamma \theta r)^{2/\beta} / \rho_{a_p} \right] \times \left[ -\lambda_{a_p} \rho_{a_p} \pi \frac{2}{\beta} \Gamma(1 + 2/\beta) \Gamma(1 - 2/\beta) (\gamma \theta r)^{2/\beta}, - (\gamma \theta r)^{2/\beta} / \rho_{a_p} \right] \prod_{r = 2}^{m} \left( 2/\beta - j \right) x^{2/\beta - j} \]

\[ \text{where } W(x) = \exp\left\{ -\lambda_{a_p} \rho_{a_p} \pi \frac{r^2}{\Gamma(1 + 2/\beta) \Gamma(1 - 2/\beta) (\gamma \theta r)^{2/\beta} - (\gamma \theta r)^{2/\beta}} \right\} \]

\[ \times \left[ \left( \gamma \theta r \right)^{2/\beta}, - (\gamma \theta r)^{2/\beta} / \rho_{a_p} \right] \times \left[ -\lambda_{a_p} \rho_{a_p} \pi \frac{2}{\beta} \Gamma(1 + 2/\beta) \Gamma(1 - 2/\beta) (\gamma \theta r)^{2/\beta}, - (\gamma \theta r)^{2/\beta} / \rho_{a_p} \right] \prod_{r = 2}^{m} \left( 2/\beta - j \right) x^{2/\beta - j} \]

By applying the Fao de Bruno’s formula to workout the derivation of the \( m \)-th order the following is obtained:

\[ \frac{d^n[\exp(W(x))]}{dx^n} \bigg|_{x = r^\beta} = \sum_{i = 1}^{\infty} \frac{1}{m!} \exp\left\{ -\lambda_{a_p} \rho_{a_p} \pi \Gamma(1 + 2/\beta) \Gamma(1 - 2/\beta) \right\} \]

\[ \times \left[ \left( \gamma \theta r \right)^{2/\beta}, - (\gamma \theta r)^{2/\beta} / \rho_{a_p} \right] \times \left[ -\lambda_{a_p} \rho_{a_p} \pi \frac{2}{\beta} \Gamma(1 + 2/\beta) \Gamma(1 - 2/\beta) (\gamma \theta r)^{2/\beta}, - (\gamma \theta r)^{2/\beta} / \rho_{a_p} \right] \prod_{r = 2}^{m} \left( 2/\beta - j \right) x^{2/\beta - j} \]
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
$$
\zeta_{M,s} (cr) = \exp\{-\lambda_{ap} \rho_{ap} \pi \Gamma(1 + 2/\beta) \times \Gamma(1 - 2/\beta) cr^{2/\beta}\}
$$
(14)
Substituting (13) into (14) the CDF of $\gamma_{ap}$ is solved as
$$
F_{\gamma_{ap}} (\gamma) = \exp\{-\pi \lambda_{ap} \rho_{ap} \pi \Gamma(1 + 2/\beta) \Gamma(1 - 2/\beta) \}
\times \Gamma(1 - 2/\beta) (\gamma_{ap})^{2/\beta} t - \sigma_a I_{ap} \right / \rho_{ap} \}
\}
$$
(15)
C. Average Secrecy Rate
The average of secrecy rate $C_{cr}$ over $\gamma_{ap}$ and $\gamma_{ap,e}$ is average secrecy rate between the AP and the FC, that is given as
$$
C_{cr} = 1/\ln 2 \int_0^\infty \frac{F_{\gamma_{ap}}(x)}{1 + x} (1 - F_{\gamma_{ap,e}}(x)) dx
$$
(16)
Substituting the CDF of $\gamma_{ap}$ 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>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>SU transmit power $P_s$</td>
<td>12 dBm</td>
</tr>
<tr>
<td>Power Spectral Density of Noise $N_0$</td>
<td>-160 dBm/Hz</td>
</tr>
<tr>
<td>Channel Gain</td>
<td>complex Gaussian distribution with zero mean and unit variance</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>1.5 MHz</td>
</tr>
<tr>
<td>Number of Antennas $M$</td>
<td>1-4</td>
</tr>
</tbody>
</table>

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 $\lambda_{ap}$ for different $\lambda_{cr}$ and $M$ is observed, where $\rho_{ap} = 0.2$, $\beta = 3.0$, $\lambda_{cr} = 10^{-3}$ and $P_{ap} = 18$ dBm. The numerical results are acquired from (16). Firstly, it can be seen that the average secrecy rate decreases as $\lambda_{cr} / \lambda_{ap}$ 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 $\lambda_{ap}$ increases.

In Figure 3, the average secrecy rate between the AP and the FC versus $\lambda_{ap}$ for different values of $\lambda_{cr}$ and $M$ are presented, where $\rho_{ap} = 0.2$, $\lambda_{cr} = 10^{-3}$, $\beta = 3.0$, 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 $\lambda_{ap} < 3 \times 10^{-3}$, and decreases as $\lambda_{ap}$ increases when $\lambda_{ap} > 3 \times 10^{-3}$, due to the fact that when $\lambda_{ap} < 3 \times 10^{-3}$, 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 $\lambda_{ap} > 3 \times 10^{-3}$ the interference from the APs has a significant effect on the SINR between the AP and the
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