Physical Layer Security in Three-Tier Wireless Sensor Networks: A Stochastic Geometry Approach

Yansha Deng, *Student Member, IEEE*, Lifeng Wang, *Student Member, IEEE*, Maged Elkashlan, *Member, IEEE*, Arumugam Nallanathan, *Senior Member, IEEE*, and Ranjan K. Mallik, *Fellow, IEEE*

Abstract—**This paper develops a tractable framework for exploiting the potential benefits of physical layer security in three-tier wireless sensor networks. In such networks, the sensing data from the remote sensors are collected by sinks with the help of access points, and the external eavesdroppers intercept the data transmissions. We adopt the stochastic geometry approach to model the random locations and spatial densities of the sensors, access points, sinks, and eavesdroppers. We focus on the secure transmission in two scenarios: i) the active sensors transmit their sensing data to the access points, and ii) the active access points forward the data to the sinks. We derive new compact expressions for the average secrecy rate in these two scenarios. We also derive a new compact expression for the overall average secrecy rate. Numerical results corroborate our analysis and show that multiple antennas at the access points can enhance the security of three-tier wireless sensor networks. Our results show that increasing the number of access points increases the overall average secrecy rate, although it decreases the average secrecy rate between the access point and its associated sink. We also show that there is a critical value beyond which increasing the number of access points decreases the overall average secrecy rate. When increasing the number of active sensors, both the average secrecy rate between the sensor and its associated access point and the overall average secrecy rate decrease. In contrast, increasing the number of sinks improves both the average secrecy rate between the access point and its associated sink, as well as the overall average secrecy rate.**

Index Terms—**Wireless sensor networks, physical layer security, stochastic geometry, beamforming, decode-and-forward.**

I. Introduction

Due to its wide applications such as environmental sensing, health monitoring, and military communications [1], wireless sensor networks (WSNs) have attracted considerable attention from the industry and academia. The security of WSNs is a big concern, since the broadcast nature of wireless channels is susceptible to eavesdropping and the sensing data needs to be protected. In practice, the small-size, low-cost and low-power sensors are randomly deployed to sense the data, which is sent back to the sinks by multihop transmissions. Multihop architectures pose great challenges to conventional cryptographic methods involving key distribution and management, and result in high complexity in data encryption and decryption. Physical layer security has emerged as an appealing low-complexity approach to secure the information transmission. The core idea behind it is to exploit the characteristics of wireless channels such as fading or noise to transmit a message from a source to an intended destination while keeping the message confidential from eavesdroppers [2]. Motivated by this, the potential applications of physical layer security have been investigated in various wireless networks such as cellular networks, cognitive radio, ad-hoc, etc.

A. Physical Layer Security: The Current State-of-the-Art

In the 1970s, Aaron D. Wyner first introduced physical layer security [3]. Triggered by the rapid evolution of wireless network architectures, the idea of enabling security at physical layer has drawn the attention of the wireless community [4]. In cellular networks, physical layer security is important for adding an extra level of protection [5, 6]. In [5], secure downlink transmission in cellular networks was investigated, and the secrecy using linear precoding based on regularized channel inversion was examined. In multi-cell environments, the cell association and location information of mobile users play an important role in secrecy performance [6]. Although it can alleviate the scarcity of radio frequency spectrum, security of cognitive radio networks is critical as it is easily exposed to external threats [7–9]. In [7], the optimal secrecy beamforming in a multiple-input single-output (MISO) cognitive radio wiretap channel was proposed. The secure relay beamforming over cooperative cognitive radio networks was introduced in [8]. In [9], the secrecy performance of antenna selection in cognitive radio wiretap channel was derived. In cooperative networks, relays are deployed to boost the coverage and reliability, however, the relay can be trusted [10, 11] or untrusted [12, 13] where the untrusted relay is thought of as an eavesdropper. In [10], the design of trusted relay weights and allocation of transmit power under different relay protocols such as amplify-and-forward (AF), decode-and-forward (DF), and cooperative jamming (CJ) was considered. In [11], trusted relay selection schemes based on the AF and DF protocols were proposed to improve physical layer security. In untrusted relay networks, CJ was introduced to confuse the untrusted relay [12]. Joint power allocation and CJ was developed in [13], and it was shown that a positive secrecy rate can be guaranteed. In decentralized networks such as ad-hoc, the public-key cryptography is expensive and difficult [14–16]. In [14], the secure connectivity in wireless random networks was studied, and the eigen-beamforming

Y. Deng and L. Wang and M. Elkashlan are with Queen Mary University of London, London, UK (e-mail: {y.deng, lifeng.wang, maged.elkashlan}@qmul.ac.uk).

A. Nallanathan is with King's College London, London, UK (e-mail: arumugam.nallanathan@kcl.ac.uk).

R. K. Mallik is with the Department of Electrical Engineering, Indian Institute of Technology - Delhi, Hauz Khas, New Delhi 110016, India (e-mail: rkmallik@ee.iitd.ernet.in).

was implemented to maximize the signal strength to the the intended receiver. In [15], the secrecy transmission capacity in wireless ad-hoc networks was analyzed, and the secrecy guard zone was introduced to improve the secrecy transmission capacity. In [16], the transmit beamforming with artificial noise strategies were used to enhance the secrecy in large-scale ad-hoc networks.

Physical layer security schemes have been recently proposed for WSNs to combat eavesdropping [17–20]. In [17], the downlink secure transmission from the mobile agent to the authorized user was considered and perfect secrecy can be achieved by intentionally creating channel variation. In [18], a detection problem under physical layer secrecy constraints in an energy-constrained WSNs was addressed, and the optimal operative solutions were analyzed. In [19], sensor transmissions were observed by the authorized fusion center (FC) and unauthorized (third party) FC. It was shown that physical layer security for distributed detection is scalable due to its low computational complexity. More recently in [20], compressed sensing (CS) was introduced to provide secrecy against eavesdropping in addition to the other CS benefits.

B. Approach and Contributions

In this paper, we examine the potential benefits of physical layer security in a three-tier WSN using stochastic geometry modeling. In three-tier WSNs, the sensors are located far from the sinks, and the access points are deployed to help the sensors forward their data to the sinks. Confidential information transmissions are intercepted by the eavesdroppers. Considering the fact that sensors are densely deployed and their locations are randomly distributed [1], we introduce stochastic geometry to model the locations of the nodes in WSNs. Such a modeling approach has been applied in heterogeneous networks [21] and cognitive radio networks [22]. Our main contributions are summarized as follows.

- We develop a new analytical framework to examine the implementation of physical layer security in three-tier WSNs. The locations and spatial densities of sensors, access points, sinks, and eavesdroppers are modeled using stochastic geometry. Each access point is equipped with multiple antennas and uses the low-complexity maximal-ratio combining (MRC) to receive the data signals from the sensors and maximal-ratio transmission (MRT) beamformer to transmit the signals. We investigate the secure transmissions between the active sensors and access points, and beween the active access points and sinks.
- We present new statistical properties, based on which we derive new compact expressions for the average secrecy rate between the typical sensor and its associated access point, and between the typical access point and its associated sink. We also derive the minimum number of sinks required for a target average secrecy rate. Particularly, we derive a new compact expression for overall average secrecy rate in three-tier WSNs.
- We show that using MRC/MRT at access points can enhance the secure transmission. Based on the proposed analysis and simulations, several important observations are reached: 1) the average secrecy rate decreases as the number of sensors grows large, due to more interference from sensors, 2) the average secrecy rate increases with increasing the number of sinks, because of the shorter distances between the access points and their associated sinks, and 3) the overall average secrecy rate increases with increasing the number of access points. However, beyond a critical value, the overall average secrecy rate decreases with increasing the number of access points.

TABLE I
NOTATION

$\Phi_{s,a}$	Poison point process (PPP) of sensor locations
λ_s	Intensity of Φ_s
$\Phi_{ap,a}$	PPP of access points locations
λ_{ap}	Intensity of Φ_{ap}
Φ_{sk}	PPP of sinks locations
λ_{sk}	Intensity of Φ_{sk}
ρ_s	The probability that sensor is triggered to transmit the data
ρ_{ap}	The activity probability of access point that forwards the data to the sinks
$\Phi_{s,e}$	PPP of eavesdropper locations, where the eavesdroppers intercept the sensors' data
$\Phi_{ap,e}$	PPP of eavesdropper locations, where the eavesdroppers intercept the access points' data
λ_e^s	Intensity of Φ_e^s
λ_e^{ap}	Intensity of Φ_e^{ap}
$\dagger$	Conjugate transpose

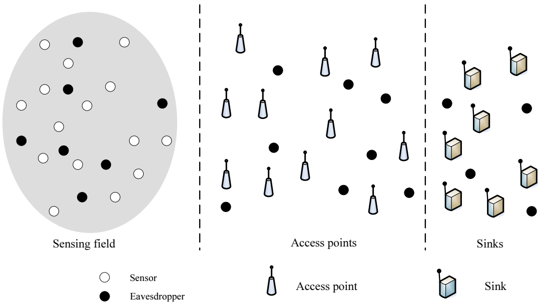

Fig. 1. Illustration of three-tier wireless sensor networks, where the sensors transmit the data to the sinks via the access points, in the presence of eavesdropping.

The notation of this paper is given in Table I-B.

II. System Description

As shown in Figure 1, a three-tier WSN is considered, where the geographically remote sensors transmit the sensed data to the sinks with the help of half-duplex decode-and-forward (DF) access points with no direct links between sensors and sinks. The eavesdroppers overhears the data transmission without modifying it. In the sensing field, sensors are randomly located according to a homogeneous Poisson point process (HPPP) $\Phi_{s,a}$ with intensity λ_s. The access points and sinks are randomly located according to independent HPPPs $\Phi_{ap,a}$ and Φ_{sk} with intensities λ_{ap} and λ_{sk}, respectively. Since the sensors may transmit data intermittently, the activity probability of sensor that is triggered to transmit the data is denoted as ρ_s $(0 < \rho_s < 1)$, and the activity probability of access point that forwards the data to the sink is denoted as ρ_{ap} $(0 < \rho_{ap} < 1)$. Non-colluding eavesdroppers are considered and eavesdroppers' locations are modeled as two independent HPPPs $\Phi_{s,e}$ and $\Phi_{ap,e}$ with intensities λ_e^s and λ_e^{ap}, respectively. The eavesdroppers in $\Phi_{s,e}$ intercept the data transmitted by the sensors and the eavesdroppers in $\Phi_{ap,e}$ intercept the data transmitted by the access points. Note that the eavesdroppers in $\Phi_{s,e}$ and in $\Phi_{ap,e}$ are far from each other.

In this three-tier network, the sensor is associated with its nearest access point and the access point is associated with its nearest sink. Each access point is equipped with M antennas, and the sensors and sinks are single-antenna nodes. To enhance the information transmission, the access points use MRC to receive the sensors' data signals and MRT beamformer to transmit the signals. The wireless channels are modeled as independent quasi-static Rayleigh fading. For an arbitrary typical sensor o, the receive signal-to-interference-plus-noise ratio (SINR) after MRC at its corresponding typical access point is given by

$$\gamma_{ap} = \frac{\left\|\mathbf{h}_{s_0,ap_0}\right\|^2 \left|X_{s_0,ap_0}\right|^{-\alpha}}{\underbrace{I_{s,ap} + I_{ap,ap}}_{In_{ap}} + \delta^2/P_s}, \tag{1}$$

where $I_{s,ap} = \sum_{i \in \Phi_{s,a} \backslash \{s_0\}} \left| \frac{\mathbf{h}_{s_0,ap_0}{}^{\dagger}}{\left\|\mathbf{h}_{s_0,ap_0}\right\|} \mathbf{h}_{i,ap_0} \right|^2 \left|X_{i,ap_0}\right|^{-\alpha}$, $I_{ap,ap} = \mu \sum_{j \in \Phi_{ap,a} \backslash \{ap_0\}} \left| \frac{\mathbf{h}_{s_0,ap_0}{}^{\dagger}}{\left\|\mathbf{h}_{s_0,ap_0}\right\|} \mathbf{H}_{j,ap_0} \frac{\mathbf{h}_{j,sk_j}{}^{\dagger}}{\left\|\mathbf{h}_{j,sk_j}\right\|} \right|^2 \left|X_{j,ap_0}\right|^{-\alpha}$, and $\mu = P_{ap}/P_s$. Here, $\Phi_{s,a}$ and $\Phi_{ap,a}$ are the locations of active sensors and active access points, $\mathbf{h}_{s_0,ap_0}$ and $\left|X_{s_0,ap_0}\right|$ are the channel fading vector and distance between the typical sensor and its typical access point, respectively, α is the path loss exponent, $\mathbf{h}_{i,ap_0} \in \mathcal{C}^{M \times 1}$ and $\left|X_{i,ap_0}\right|$ are the channel fading vector and distance between the sensor i and the typical access point, respectively, $\mathbf{H}_{j,ap_0}$ and $\left|X_{j,ap_0}\right|$ are the channel fading matrix and distance between the access point j and the typical access point, respectively, $\mathbf{h}_{j,sk_j} \in \mathcal{C}^{1 \times M}$ is the channel fading vector between the access point j and its corresponding sink, P_s is the sensor's transmit power, P_{ap} is the access point's transmit power, and δ^2 is the noise power.

We consider the non-colluding eavesdropping scenario, in which the most detrimental eavesdropper that has the highest receive SINR dominates the secrecy rate [10]. Thus, the received SINR at the most detrimental eavesdropper in Φ_e^s for the sensor and the access point transmission is given by

$$\gamma_{s,e} = \max_{e_k \in \Phi_{s,e}} \left\{ \frac{\left|h_{s_0,e_k}\right|^2 \left|X_{s_0,e_k}\right|^{-\alpha}}{\underbrace{I_{s,e} + I_{ap,e}}_{In_{s,e}} + \delta^2/P_s} \right\}, \tag{2}$$

where $I_{s,e} = \sum_{i \in \Phi_{s,a} \backslash \{s_0\}} \left|h_{i,e_k}\right|^2 \left|X_{i,e_k}\right|^{-\alpha}$ and $I_{ap,e} = \sum_{j \in \Phi_{ap,a} \backslash \{ap_0\}} \mu \left| \mathbf{h}_{j,e_k} \frac{\mathbf{h}_{j,sk_j}{}^{\dagger}}{\left\|\mathbf{h}_{j,sk_j}\right\|} \right|^2 \left|X_{j,e_k}\right|^{-\alpha}$, h_{s_0,e_k} and $\left|X_{s_0,e_k}\right|$ are the channel fading coefficient and distance between the typical sensor and the eavesdropper, respectively, h_{i,e_k} and $\left|X_{i,e_k}\right|$ are the channel fading coefficient and distance between sensor i and the eavesdropper, respectively, and $\mathbf{h}_{j,e_k}$ and $\left|X_{j,e_k}\right|$ are the channel fading vector and distance between the access point j and the eavesdropper, respectively.

After receiving the sensors' data, access points will forward them to the nearest sinks for data collection. In this scenario, we select an arbitrary access point as a typical node ap_0, and the received SINR at the typical sink sk_0 is given by

$$\gamma_{sk} = \frac{\left\|\mathbf{g}_{ap_0,sk_0}\right\|^2 \left|X_{ap_0,sk_0}\right|^{-\beta}}{In_{ap,sk} + \delta^2/P_{ap}}, \tag{3}$$

where $In_{ap,sk} = \sum_{j \in \Phi_{ap,a} \backslash \{ap_0\}} \left| \mathbf{g}_{j,sk_0} \frac{\mathbf{h}_{j,sk_j}{}^{\dagger}}{\left\|\mathbf{h}_{j,sk_j}\right\|} \right|^2 \left|X_{j,sk_0}\right|^{-\beta}$, $\mathbf{g}_{ap_0,sk_0} \in \mathcal{C}^{1 \times M}$ and $\left|X_{ap_0,sk_0}\right|$ are the channel fading vector and distance between the typical access point and its typical sink, respectively, β is the path loss exponent, $\mathbf{g}_{j,sk_0} \in \mathcal{C}^{1 \times M}$ and $\left|X_{j,sk_0}\right|$ are the channel fading vector and distance between the access point j and the typical sink, and $\mathbf{h}_{j,sk_j} \in \mathcal{C}^{1 \times M}$ is the channel fading vector between the access point j and its associated sink. In this case, the received SINR at the most detrimental eavesdropper for the access point and the sink transmission is given by

$$\gamma_{ap,e} = \max_{e_k \in \Phi_{ap,e}} \left\{ \frac{\left| \mathbf{g}_{ap_0,e_k} \frac{\mathbf{g}_{ap_0,sk_0}{}^{\dagger}}{\left\|\mathbf{g}_{ap_0,Sk_0}\right\|} \right|^2 \left|X_{ap_0,e_k}\right|^{-\beta}}{In_{ap,e} + \sigma^2/P_{ap}} \right\}, \tag{4}$$

where $In_{ap,e} = \sum_{j \in \Phi_{ap,a} \backslash \{ap_0\}} \left| \mathbf{g}_{j,e_k} \frac{\mathbf{h}_{j,sk_k}{}^{\dagger}}{\left\|\mathbf{h}_{j,sk_k}\right\|} \right|^2 \left|X_{j,e_k}\right|^{-\beta}$, g_{ap_0,e_k} and $\left|X_{ap_0,e_k}\right|$ are the channel fading coefficient and distance between the typical access point and the eavesdropper, respectively, and $\mathbf{g}_{j,e_k}$ and $\left|X_{j,e_k}\right|$ are the channel fading vector and distance between the access point j and the eavesdropper, respectively.

III. Secrecy Performance Evaluations

In this section, we characterize the secrecy performance in terms of average secrecy rate. Before exhibiting the overall secrecy performance behaviors, we evaluate the secrecy of two different links, namely the link between the sensor and access point, and the link between the access point and sink. We derive new analytical expressions for the average secrecy rate, and analyze the impact of the two links on the overall average secrecy rate.

A. Average Secrecy Rate between the Sensor and the Access Point

We evaluate the average secrecy rate based on the worst-case, i.e., the average secrecy rate is dominated by the eavesdropper with the best channel [10]. Hence, for a typical link between a typical sensor and its associated access point, the instantaneous secrecy rate is defined as [23]

$$C_s^{ap} = \left[C_{ap} - C_{s,e}\right]^+, \tag{5}$$

where $[x]^+ = \max\{x, 0\}$, $C_{ap} = \log_2\left(1 + \gamma_{ap}\right)$ is the capacity of the channel between the typical sensor and access point, and $C_{s,e} = \log_2\left(1 + \gamma_{s,e}\right)$ is the capacity of the eavesdropping channel between the typical sensor and the most detrimental eavesdropper.

1) New Statistics: We derive the cumulative distribution functions (CDFs) of SINRs at the typical access point and the most detrimental eavesdropper that intercepts the transmission between the typical sensor and the access point in **Lemma 1** and **Lemma 2**, respectively.

Lemma 1. *The CDF of SINR at the typical access point is derived as* (6) *at the top of next page.*

Proof. See Appendix A. □

Lemma 2. *The CDF of SINR at the most detrimental eavesdropper which intercepts the transmission between the typical sensor and the access point is derived as*

$$\begin{aligned}&F_{\gamma_{s,e}}\left(\gamma_{th}\right)=\\&\exp\Big\{-\pi\lambda_e^s\int_0^\infty\exp\Big\{-\left(\lambda_s\rho_s+\lambda_{ap}\rho_{ap}\mu^{2/\alpha}\right)\pi\\&\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)\left(\gamma_{th}\right)^{\frac{2}{\alpha}}t-\delta^2\gamma_{th}t^{\alpha/2}\Big/P_s\Big\}dt.\end{aligned}\tag{7}$$

Proof. See Appendix B. □

2) Average Secrecy Rate: Based on our fundamental work in [24], the average secrecy rate between the sensor and the access point is the average of secrecy rate C_s^{ap} over $\gamma_{s,e}$ and γ_{ap}, which can be written as

$$\bar{C}_s^{ap}=\frac{1}{\ln 2}\int_0^\infty\frac{F_{\gamma_{s,e}}\left(x\right)}{1+x}(1-F_{\gamma_{ap}}\left(x\right))dx.\tag{8}$$

By substituting the CDF of γ_{ap} in (6) and the CDF of $\gamma_{s,e}$ in (7) into (8), we can obtain the average secrecy rate between the sensor and the access point.

Note that the derived average secrecy rate between the sensor and the access point in (8) is not in a simple form. As such, in the following corollary, we present the interference-limited case for the average secrecy rate with a single antenna at the access point.

Corollary 1. *When the access points are equipped with single antenna in the interference-limited scenario, the average secrecy rate between the sensor and the access point is given by*

$$\begin{aligned}&\bar{C}_s^{ap}=\\&\frac{\pi\lambda_{ap}\left(1-\rho_{ap}\right)}{\ln 2}\int_0^\infty\frac{\exp\left\{-\pi\lambda_e^s/\left(\Lambda_1x^{2/\alpha}\right)\right\}}{(1+x)\left(\Lambda_1x^{2/\alpha}+\pi\lambda_{ap}\left(1-\rho_{ap}\right)\right)}dx,\end{aligned}\tag{9}$$

where $\Lambda_1=\left(\lambda_s\rho_s+\lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}}\right)\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right).$

B. Average Secrecy Rate between the Access Point and the Sink

Similar to (5), for a typical access point and its associated sink, the instantaneous secrecy rate is defined as

$$C_s^{sk}=[C_{sk}-C_{ap,e}]^+,\tag{10}$$

where $C_{sk}=\log_2\left(1+\gamma_{sk}\right)$ and $C_{ap,e}=\log_2\left(1+\gamma_{ap.e}\right)$.

1) New Statistics: We derive the CDFs of SINRs at the typical sink and the most detrimental eavesdropper that intercepts the transmission between the typical access point and the sink in **Lemma 3** and **Lemma 4**, respectively.

Lemma 3. *The CDF of SINR at the typical sink is derived as*

$$\begin{aligned}&F_{\gamma_{sk}}\left(x\right)=1-2\pi\lambda_{sk}\int_0^\infty r\exp\Big\{-\lambda_{ap}\rho_{ap}\pi\Gamma\left(1+2/\beta\right)\\&\Gamma\left(1-2/\beta\right)\left(\gamma_{th}\right)^{\frac{2}{\beta}}r^2-\gamma_{th}r^\beta\delta^2/P_{ap}-\pi\lambda_{sk}r^2\Big\}dr-2\pi\lambda_{sk}\\&\sum_{m=1}^{M-1}\frac{1}{(-1)^m}\sum\frac{1}{\prod\limits_{l=1}^{m}m_l!l!^{m_l}}\int_0^\infty r^{\beta m+1}\exp\Big\{-\lambda_{ap}\rho_{ap}\pi\\&\Gamma\left(1+2/\beta\right)\Gamma\left(1-2/\beta\right)\left(\gamma_{th}\right)^{\frac{2}{\beta}}r^2-\gamma_{th}r^\beta\delta^2/P_{ap}-\pi\lambda_{sk}r^2\Big\}\\&\Big[-\lambda_{ap}\rho_{ap}\pi\frac{2}{\beta}\Gamma\left(1+2/\beta\right)\Gamma\left(1-2/\beta\right)\left(\gamma_{th}\right)^{\frac{2}{\beta}}r^{2-\beta}-\gamma_{th}\\&\delta^2/P_{ap}\Big]^{m_1}\prod_{l=2}^{m}\Big[-\lambda_{ap}\rho_{ap}\pi\Gamma\left(1+2/\beta\right)\Gamma\left(1-2/\beta\right)\left(\gamma_{th}\right)^{\frac{2}{\beta}}\\&\prod_{j=0}^{l-1}\left(2/\beta-j\right)r^{2-l\beta}\Big]^{m_l}dr.\end{aligned}\tag{11}$$

Proof. See Appendix C. □

Lemma 4. *The CDF of SINR at the most detrimental eavesdropper which intercepts the transmission between the typical access point and the sensor is derived as*

$$\begin{aligned}F_{\gamma_{ap,e}}\left(x\right)=\exp\Big\{-\pi\lambda_e^{ap}\int_0^\infty\exp\left\{-\lambda_{ap}\rho_{ap}\pi\Gamma\left(1+2/\beta\right)\right.\\\left.\Gamma\left(1-2/\beta\right)\gamma_{th}{}^{\frac{2}{\beta}}t-\sigma^2\gamma_{th}t^{\beta/2}\Big/P_{ap}\right\}dt\Big\}.\end{aligned}\tag{12}$$

Proof. See Appendix D. □

2) Average Secrecy Rate: The average secrecy rate between the access point and the sink is the average of the secrecy rate C_s^{sk} over γ_{sk} and $\gamma_{ap,e}$, which is given by

$$\bar{C}_s^{sk}=\frac{1}{\ln 2}\int_0^\infty\frac{F_{\gamma_{sk}}\left(x\right)}{1+x}(1-F_{\gamma_{ap,e}}\left(x\right))dx.\tag{13}$$

By substituting the CDF of γ_{sk} in (11) and the CDF of $\gamma_{ap,e}$ in (12) into (13), we can obtain the average secrecy rate between the access point and the sink.

Note that the derived the average secrecy rate between the access point and the sink is also not in a simple form, we present the interference-limited case for the average secrecy rate with single antenna at the access point in the following corollary.

Corollary 2. *When the access points are equipped with single antenna in the interference-limited scenario, the average secrecy rate between the access point and the sink is given by*

$$\bar{C}_s^{sk}=\frac{\pi\lambda_{sk}}{\ln 2}\int_0^\infty\frac{\exp\left\{-\pi\lambda_e^{ap}/\Lambda_2x^{2/\beta}\right\}}{(1+x)\left(\Lambda_2x^{2/\beta}+\pi\lambda_{sk}\right)}dx,\tag{14}$$

$$\begin{aligned}
&F_{\gamma_{ap}}\left(\gamma_{th}\right) = 1 - 2\pi\lambda_{ap}\left(1-\rho_{ap}\right)\int_0^\infty r\exp\Big\{-\Big(\lambda_s\rho_s + \lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}}\Big)\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)\left(\gamma_{th}\right)^{\frac{2}{\alpha}}r^2 - \gamma_{th}r^\alpha\delta^2/P_s \\
&-\pi\lambda_{ap}\left(1-\rho_{ap}\right)r^2\Big\}dr - 2\pi\lambda_{ap}\left(1-\rho_{ap}\right)\sum_{m=1}^{M-1}\frac{\left(r^\alpha\right)^m}{\left(-1\right)^m}\sum\frac{1}{\prod\limits_{l=1}^{m} m_l!l!^{m_l}}\int_0^\infty r\exp\Big\{-\Big(\lambda_s\rho_s + \lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}}\Big)\pi\Gamma\left(1+2/\alpha\right) \\
&\Gamma\left(1-2/\alpha\right)\left(\gamma_{th}\right)^{\frac{2}{\alpha}}r^2 - \gamma_{th}r^\alpha\delta^2/P_s - \pi\lambda_{ap}\left(1-\rho_{ap}\right)r^2\Big\}\Big[-2/\alpha\Big(\lambda_s\rho_s + \lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}}\Big)\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)\left(\gamma_{th}\right)^{2/\alpha} \\
&r^{(2-\alpha)} - \gamma_{th}\delta^2/P_s\Big]^{m_1}\prod_{l=2}^{m}\Big[-\Big(\lambda_s\rho_s + \lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}}\Big)\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)(\gamma_{th})^{2/\alpha}\prod_{j=0}^{l-1}\left(2/\alpha - j\right)r^{2-l\alpha}\Big]^{m_l}dr, \qquad (6)
\end{aligned}$$

where $\sum\limits_{l=1}^{m} l\cdot m_l = m$.

where $\Lambda_2 = \lambda_{ap}\rho_{ap}\pi\Gamma\left(1+2/\beta\right)\Gamma\left(1-2/\beta\right)$. Based on (14), for a specific target average secrecy rate $\bar{C}_0$ between the access point and the sink, the number of sinks must satisfy

$$\lambda_{sk} > \bar{C}_0\Lambda_2\frac{\ln 2}{\pi\varepsilon}, \qquad (15)$$

where $\varepsilon = \int_0^\infty \frac{\exp\left\{-\pi\lambda_e^{ap}/\left(\Lambda_2 x^{2/\beta}\right)\right\}}{(1+x)x^{2/\beta}}dx$.

C. Overall Average Secrecy Rate

In this subsection, we derive the overall average secrecy rate in three-tier WSNs. The instantaneous secrecy rate is defined as $C_s = \min\left(C_s^{ap}, C_s^{sk}\right)$. As such, the overall average secrecy rate is calculated as

$$\bar{C}_s = \int_0^\infty x f_{C_s}\left(x\right)dx = \int_0^\infty \left(1 - F_{C_s}\left(x\right)\right)dx, \qquad (16)$$

where $f_{C_s}\left(x\right)$ and $F_{C_s}\left(x\right)$ is the probability density function (PDF) and the CDF of C_s, respectively. The CDF of C_s is calculated as

$$\begin{aligned}
F_{C_s}\left(x\right) &= \Pr\left(\min\left(C_s^{ap}, C_s^{sk}\right) < x\right) \\
&= 1 - \Pr\left(\min\left(C_s^{ap}, C_s^{sk}\right) > x\right) \\
&= 1 - \Pr\left(C_s^{ap} > x\right)\Pr\left(C_s^{sk} > x\right). \qquad (17)
\end{aligned}$$

Substituting (17) into (16), we have

$$\bar{C}_s = \int_0^\infty \Pr\left(C_s^{ap} > x\right)\Pr\left(C_s^{sk} > x\right)dx, \qquad (18)$$

where

$$\Pr\left(C_s^{ap} > x\right) = 1 - \int_0^\infty f_{\gamma_{s,e}}\left(t\right)F_{\gamma_{ap}}\left(2^x\left(1+t\right) - 1\right)dt \qquad (19)$$

and

$$\Pr\left(C_s^{sk} > x\right) = 1 - \int_0^\infty f_{\gamma_{ap,e}}\left(t\right)F_{\gamma_{sk}}\left(2^x\left(1+t\right) - 1\right)dt. \qquad (20)$$

Here, $f_{\gamma_{s,e}}$ is the derivative of $F_{\gamma_{s,e}}$ given in (7), and $f_{\gamma_{ap,e}}$ is the derivative of $F_{\gamma_{ap,e}}$ given in (12).

Unfortunately, the derived overall average secrecy rate between the sensor and the sink is not in a simple form, which motivates us to consider the interference-limited case with single antenna at the access point, as presented in the following corollary.

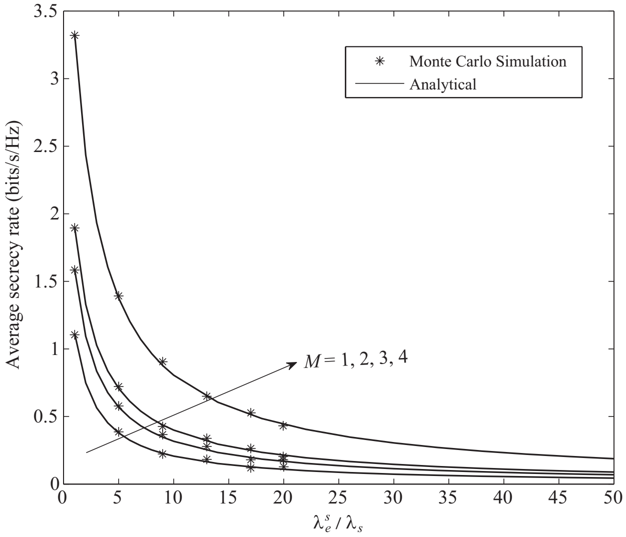

Fig. 2. The average secrecy rate versus $\frac{\lambda_e^s}{\lambda_s}$. $\lambda_s = 10^{-2}$, $\rho_s = 0.01$, $\lambda_{ap} = 10^{-2}$, $\rho_{ap} = 0.1$, $\alpha = 3.5$, $P_{ap} = 25$ dBm.

Corollary 3. *When the access points are equipped with single antenna in the interference-limited scenario, the overall average secrecy rate between the sensor and the sink is given by*

$$\begin{aligned}
\bar{C}_s = \int_0^\infty &\Bigg[\int_0^\infty \frac{2\pi\lambda_e^s}{\alpha\Lambda_1 y^{2/\alpha+1}}\exp\left\{-\pi\lambda_e^s\Big/\left(\Lambda_1 y^{2/\alpha}\right)\right\} \\
&\frac{\pi\lambda_{ap}\left(1-\rho_{ap}\right)}{\Lambda_1\left(2^x\left(1+y\right)-1\right)^{2/\alpha} + \pi\lambda_{ap}\left(1-\rho_{ap}\right)}dy\Bigg] \\
&\left[\int_0^\infty \frac{2\pi^2\lambda_e^{ap}\lambda_{sk}\exp\left\{-\pi\lambda_e^{ap}/\Lambda_2 y^{2/\beta}\right\}}{\beta\Lambda_2 y^{2/\beta+1}\left(\Lambda_2\left(2^x\left(1+y\right)-1\right)^{2/\beta} + \pi\lambda_{sk}\right)}dy\right]dx, \\
&\qquad (21)
\end{aligned}$$

where $\Lambda_1 = \left(\lambda_s\rho_s + \lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}}\right)\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)$

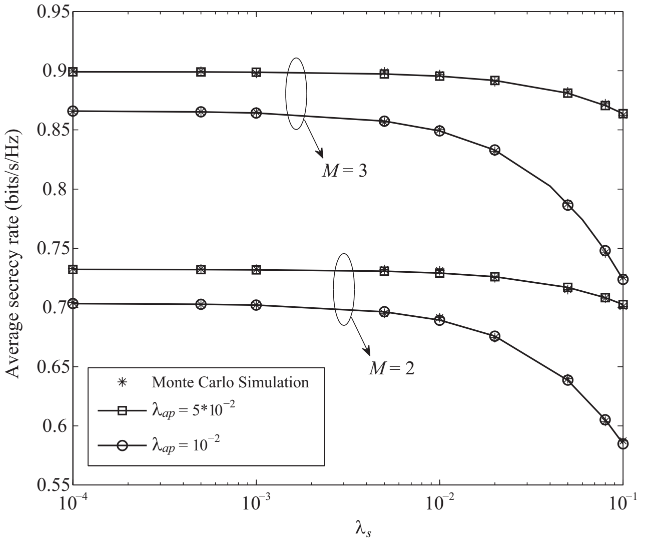

Fig. 3. The average secrecy rate versus λ_s. $\rho_s = 0.05$, $\rho_{ap} = 0.5$, $\lambda_e^s = 10^{-3}$, $\alpha = 3.5$, $P_{ap} = 25$ dBm.

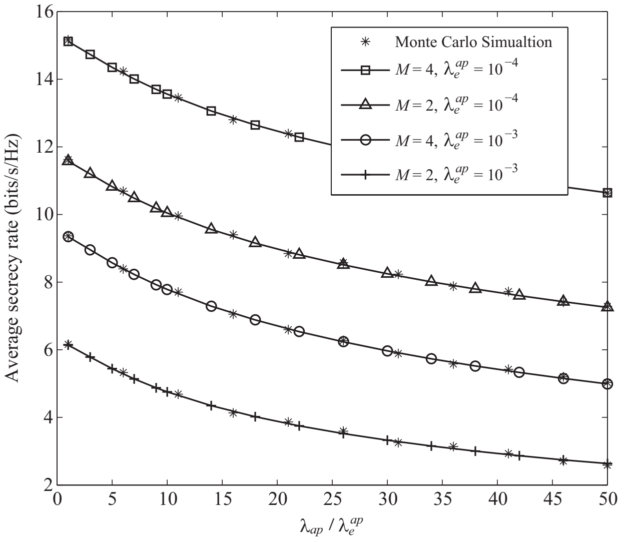

Fig. 4. The average secrecy rate versus $\frac{\lambda_{ap}}{\lambda_e^{ap}}$. $\rho_{ap} = 0.1$, $\lambda_{sk} = 10^{-2}$, $\beta = 3.5$, $P_{ap} = 15$ dBm.

and $\Lambda_2 = \lambda_{ap}\rho_{ap}\pi\Gamma\left(1 + 2/\beta\right)\Gamma\left(1 - 2/\beta\right).$

IV. Numerical Examples

In this section, we present numerical examples to show the average secrecy rate of the three-tier WSN. We assume that the sensor's transmit power $P_s = 15$ dBm, the power spectral density of noise is -170 dBm/Hz, and the bandwidth is 1 MHz. In all the figures, we see a precise match between the simulations and the exact analytical curves, which validate our analysis.

A. Average Secrecy Rate between the Sensor and Access Point

Fig. 2 plots the average secrecy rate between the sensor and the access point versus λ_e^s/λ_s. The analytical results are obtained from (8). We first see that the average secrey rate decreases with increasing the density of eavesdroppers that intercepts the tranmission between sensor and access point, due to the detrimental effects of eavesdropping. We also see that the average secrecy rate increases with increasing the number of antennas at the access point, which results from the array again brought by using MRC at the access point.

Fig. 3 plots the average secrecy rate between the sensor and the access point versus λ_s for various λ_{ap} and M. The analytical results are obtained from (8). An interesting observation is that for the same number of antennas M, the average secrecy rate is nearly invariable for $\lambda_s < 2 \times 10^{-3}$, since the interference from other sensors is much smaller than the interference from the active access points, and slightly increasing the interference from the sensor imposes negligible effect on the performance. However, when $\lambda_s > 2 \times 10^{-3}$, the interference from other sensors is comparable with the interference from the active access points, and increasing the interference from the sensor degrades the secrecy performance. We also observe that increasing λ_{ap} increases the average secrecy rate. This is because with more access points, the distance between the typical sensor and the typical access point becomes shorter, which improves the average secrecy rate. In additiona, we find that increasing λ_{ap} slows down the decreasing trend of average secrecy rate when λ_s increases.

B. Average Secrecy Rate between the Access point and Sink

Fig. 4 plots the average secrecy rate between the access point and the sink versus $\lambda_e^{ap}/\lambda_{ap}$ for various λ_{ap} and M. The analytical results are obtained from (13). We first observe that the average secrecy rate decreases with increasing $\lambda_e^{ap}/\lambda_{ap}$, which indicates that more access points need to be deployed as the density of eavesdroppers increases, to combat eavesdropping. Second, with the same number of antennas at the access point, the average secrecy rate decreases with increasing λ_e^{ap}. The average secrecy rate between the access point and the sink improves with increasing the number of antennas at the access point M.

Fig. 5 plots the average secrecy rate between the access point and the sink versus λ_{ap} for various λ_{sk} and M. The analytical results are obtained from (13). We observe that the average secrecy rate alters slightly for $\lambda_{ap} < 2 \times 10^{-3}$, and decreases with increasing λ_{ap} for $\lambda_{ap} > 2 \times 10^{-3}$. This can be explained by the fact that for $\lambda_{ap} < 2 \times 10^{-3}$, the interference from the active access points is relatively small compared with the noise, and increasing the number of access points scarcely influence the performance. However, for $\lambda_{ap} > 2 \times 10^{-3}$, the interference from the access point imposes a dominant impact on the SINR between the access point and the sink, thus increasing the interference from the access points degrades the average secrecy rate. Another observation is that the average secrecy rate improves with increasing the density of sink, because the distance between the typical access point and the corresponding sink becomes shorter.

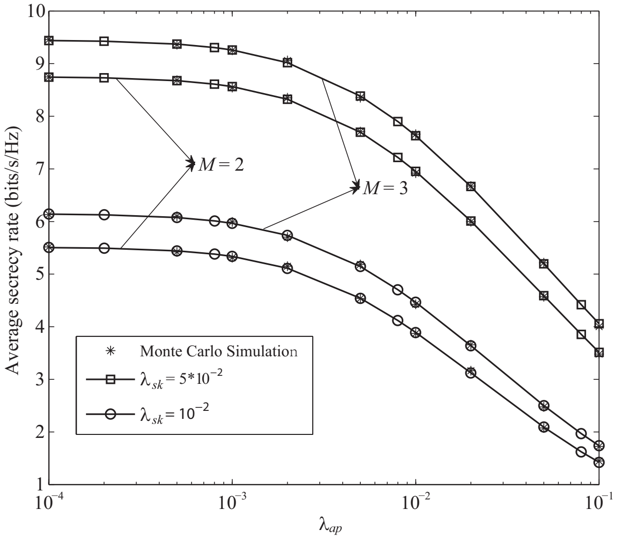

Fig. 5. The average secrecy rate versus λ_{ap}. $\rho_{ap} = 0.1$, $\beta = 3$, $\lambda_e^{ap} = 10^{-3}$, $P_{ap} = 25$ dBm,

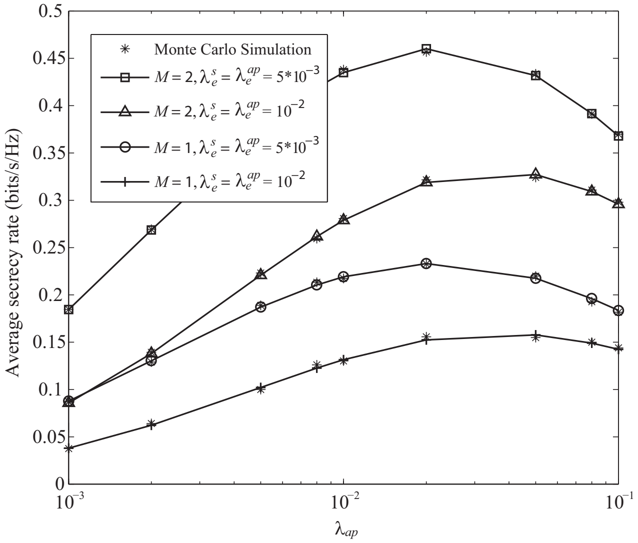

Fig. 7. The average secrecy rate versus λ_{ap}. $P_{ap} = 30$ dBm, $\rho_s = 0.01$, $\rho_{ap} = 0.1$, $\alpha = 2.8$, $\beta = 3.2$, $\lambda_s = \lambda_{sk} = 10^{-2}$.

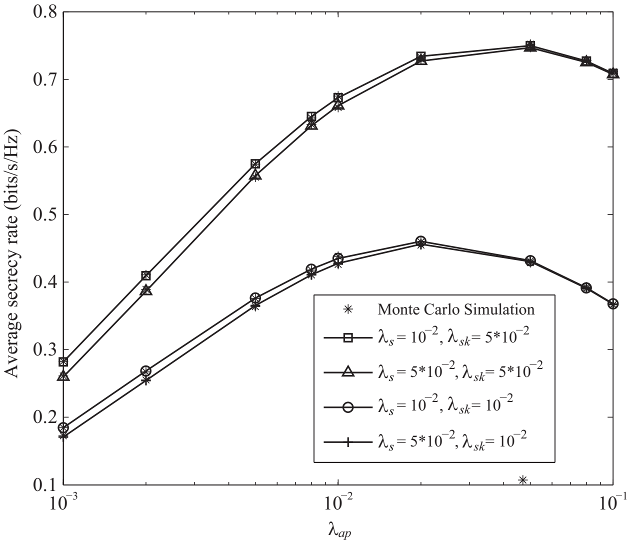

Fig. 6. The average secrecy rate versus λ_{ap}. $P_{ap} = 30$ dBm, $M = 2$, $\rho_s = 0.01$, $\rho_{ap} = 0.1$, $\alpha = 2.8$, $\beta = 3.2$, $\lambda_e^s = \lambda_e^{ap} = 5 * 10^{-3}$.

C. Overall Average Secrecy Rate

Fig. 6 plots the overall average secrecy rate versus λ_{ap} for various λ_s and λ_{sk}. The analytical results are obtained from (18). Interestingly, we find that the overall average secrecy rate first increases, and then decreases with increasing λ_{ap}, which implies that there exists an optimal λ_{ap} to achieve the maximum average secrecy rate. This phenomenon can be well explained by the tradeoff between the benefits brought by the shorter distance from the typical sensor to the typical access point and the detrimental effects caused by more interference from the active access points due to increasing λ_{ap}. It is also seen that the overall average secrecy rate can be improved by deploying more sinks, due to the shorter distance between the access point and the sink. It is further demonstrated that deploying more sensors in this network may not greatly degrade the average secrecy rate due to the low transmit power of sensors. More importantly, it is shown that the optimal λ_{ap} is more dependent on the λ_{sk}.

Fig. 7 plots the overall average secrecy rate versus λ_{ap} for various λ_e^s, λ_e^{ap} and M. The analytical results are obtained from (18). Similar as Fig. 6, we see that the overall average secrecy rate first increases, and then decreases with increasing λ_{ap}. As expected, the average secrecy rate decreases with increasing eavesdroppers. It is indicated that the optimal λ_{ap} for achieving the maximum average secrecy rate does not alter drastically with different λ_e^s and λ_e^{ap}.

V. Conclusions

We took into account the physical layer security of three-tier WSNs. We examined the impact of random locations and spatial densities of sensors, access points, sinks, and external eavesdroppers on the secrecy performance. We obtained new expressions for the average secrecy rate. Based on our analysis, we established the importance of physical layer security in three-tier WSNs, where our results support useful guidelines on secure transmission in practical WSNs. For example, we derived the minimum number of sinks required for a target average secrecy rate, which facilitates secure node deployment design in WSNs.

Appendix A
A Proof of Lemma 1

From (1), the CDF of γ_{ap} is given by

$$\begin{aligned} F_{\gamma_{ap}}\left(\gamma_{th}\right) =& \int_0^\infty \Pr\left[\frac{\left\|\mathbf{h}_{s_0,ap_0}\right\|^2 r^{-\alpha}}{In_{ap}+\delta^2/P_s} \le \gamma_{th}\right] f_{\left|X_{s_0,ap_0}\right|}\left(r\right) dr \\ =& \int_0^\infty \Pr\left[\frac{\left\|\mathbf{h}_{s_0,ap_0}\right\|^2 \left|X_{s_0,ap_0}\right|^{-\alpha}}{In_{ap}+\delta^2/P_s} \le \gamma_{th}\right] 2\pi\lambda_{ap} \\ & \left(1-\rho_{ap}\right) r \exp\left(-\pi\lambda_{ap}\left(1-\rho_{ap}\right) r^2\right) dr, \end{aligned} \tag{A.1}$$

where $f_{\left|X_{s_0,ap_0}\right|}\left(r\right)$ is the PDF of the nearest distance between the access point and the typical sensor. The CDF of the access point SINR at distance r from its corresponding sensor is given as

$$\begin{aligned} \Pr\left[\frac{\left\|\mathbf{h}_{s_0,ap_0}\right\|^2 r^{-\alpha}}{In_{ap}+\delta^2/P_s} \le \gamma_{th}\right] =& \mathbb{E}_{\Phi_{s,a}}\left\{\mathbb{E}_{\Phi_{ap,a}}\left\{\Pr\left[\left\|\mathbf{h}_{s_0,ap_0}\right\|^2 .\right.\right.\right. \\ & \left.\left.\left.\le \gamma_{th} r^\alpha \left(In_{ap}+\delta^2/P_s\right)\right| \Phi_{s,a}, \Phi_{ap,a}\right]\right\}\right\} \\ =& 1-\sum_{m=0}^{M-1}\frac{1}{m!}\mathbb{E}_{\Phi_{s,a}}\left\{\mathbb{E}_{\Phi_{ap,a}}\left\{\int_0^\infty \left[\gamma_{th} r^\alpha\left(\tau+\delta^2/P_s\right)\right]^m\right.\right. \\ & \left.\left.\exp\left[-\gamma_{th} r^\alpha\left(\tau+\delta^2/P_s\right)\right] d\Pr\left(In_{ap}\le\tau\right)\right\}\right\}. \end{aligned} \tag{A.2}$$

We then substitute $\left(-\left(\tau+\delta^2/P_s\right)\gamma_{th}\right)^m e^{-\left(\tau+\delta^2/P_s\right)\gamma_{th}^{\{s\}} r^\alpha} = \left.\frac{d^m\left(e^{-\gamma_{th} x\left(\tau+\delta^2/P_s\right)}\right)}{dx^m}\right|_{x=r^\alpha}$ into (A.2), we rewrite the CDF of the access point SINR at distance r from its corresponding sensor as

$$\begin{aligned} \Pr\left[\frac{\left\|\mathbf{h}_{s_0,ap_0}\right\|^2 r^{-\alpha}}{In_{ap}+\delta^2/P_s} \le \gamma_{th}\right] =& 1-\mathbb{E}_{\Phi_{s,a}}\left\{\mathbb{E}_{\Phi_{ap,a}}\left\{\right.\right. \\ & \left.\left.\int_0^\infty \exp\left[-\gamma_{th} r^\alpha\left(\tau+\delta^2/P_s\right)\right] d\Pr\left(In_{ap}\le\tau\right)\right\}\right\} \\ & -\sum_{m=1}^{M-1}\frac{\left(r^\alpha\right)^m}{m!(-1)^m}\mathbb{E}_{\Phi_{s,a}}\left\{\mathbb{E}_{\Phi_{ap,a}}\left\{\right.\right. \\ & \left.\left.\int_0^\infty \left.\frac{d^m\left(e^{-\gamma_{th} x\left(\tau+\delta^2/P_s\right)}\right)}{dx^m}\right|_{x=r^\alpha} d\Pr\left(In_{ap}\le\tau\right)\right\}\right\} \\ =& 1-\exp\left(-\gamma_{th} r^\alpha \delta^2/P_s\right)\mathcal{L}_{In_{ap}}\left(\gamma_{th} r^\alpha\right) \\ & -\sum_{m=1}^{M-1}\frac{\left(r^\alpha\right)^m}{m!(-1)^m}\left.\frac{d^m\left(\exp\left(-\gamma_{th} x\delta^2/P_s\right)\mathcal{L}_{In_{ap}}\left(\gamma_{th} x\right)\right)}{dx^m}\right|_{x=r^\alpha}. \end{aligned} \tag{A.3}$$

Remind that $I_{s,ap} = \sum_{i\in\Phi_{s,a}\setminus\{s_0\}}\left|\frac{\mathbf{h}_{s_0,ap_0}{}^\dagger}{\left\|\mathbf{h}_{s_0,ap_0}\right\|}\mathbf{h}_{i,ap_0}\right|^2\left|X_{i,ap_0}\right|^{-\alpha}$, using Slivnyak's theorem, the Laplace transform of $I_{s,ap}$ is

$$\begin{aligned} &\mathcal{L}_{I_{s,ap}}\left(s\right) \\ &= \mathbb{E}_{\Phi_s}\left[\exp\left\{-s\sum_{i\in\Phi_{s,a}\setminus\{s_0\}}\left|\frac{\mathbf{h}_{s_0,ap_0}{}^\dagger}{\left\|\mathbf{h}_{s_0,ap_0}\right\|}\mathbf{h}_{i,ap_0}\right|^2\left|X_{i,ap_0}\right|^{-\alpha}\right\}\right] \\ &\overset{(a)}{=} \exp\left\{-2\pi\lambda_s\rho_s\int_0^\infty\left(1-\mathcal{L}_{\frac{\mathbf{h}_{s_0,ap_0}{}^\dagger}{\left\|\mathbf{h}_{s_0,ap_0}\right\|}\mathbf{h}_{i,ap_0}}\left(sy^{-\alpha}\right)\right) ydy\right\} \\ &\overset{(b)}{=} \exp\left\{-2\pi\lambda_s\rho_s\int_0^\infty\left(1-\frac{1}{1+sy^{-\alpha}}\right) ydy\right\} \\ &= \exp\left\{-\lambda_s\rho_s\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)s^{2/\alpha}\right\}, \end{aligned} \tag{A.4}$$

In (A.4), (a) follows from the Generating functionnal of HPPP in [25], (b) follows from the fact that $\left|\frac{\mathbf{h}_{s_0,ap_0}{}^\dagger}{\left\|\mathbf{h}_{s_0,ap_0}\right\|}\mathbf{h}_{i,ap_0}\right|^2 \sim \exp\left(1\right)$.

Since $I_{ap,ap} = \mu\sum_{j\in\Phi_{ap,a}\setminus\{ap_0\}}\left|\frac{\mathbf{h}_{s_0,ap_0}{}^\dagger}{\left\|\mathbf{h}_{s_0,ap_0}\right\|}\mathbf{H}_{j,ap_0}\frac{\mathbf{h}_{j,sk_j}{}^\dagger}{\left\|\mathbf{h}_{j,sk_j}\right\|}\right|^2 \left|X_{j,ap_0}\right|^{-\alpha} = \mu\sum_{j\in\Phi_{ap}\setminus\{ap_0\}}H_j^{ap,ap}\left|X_{j,ap_0}\right|^{-\alpha}$, the Laplace transform of $I_{ap,ap}$ is

$$\begin{aligned} &\mathcal{L}_{I_{ap,ap}}\left(s\right) \\ &\quad= \exp\left(-\int\left[1-\mathbb{E}_h\left(\exp\left(-s\mu H_j^{ap,ap}y^{-\alpha}\right)\right)\right]\lambda_{ap}\rho_{ap}2\pi ydy\right) \\ &\quad\overset{(c)}{=} \exp\left\{-\lambda_{ap}\rho_{ap}\pi\mu^{\frac{2}{\alpha}}\mathbb{E}_h\left\{\left(H_j^{ap,ap}\right)^{\frac{2}{\alpha}}\right\}\Gamma\left(1-\frac{2}{\alpha}\right)s^{\frac{2}{\alpha}}\right\} \\ &\quad\overset{(d)}{=} \exp\left\{-\lambda_{ap}\rho_{ap}\pi\mu^{\frac{2}{\alpha}}\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)s^{2/\alpha}\right\}, \end{aligned} \tag{A.5}$$

where (c) follows from the Generating functionnal of HPPP in [25], (d) follows from $H_j \sim \exp\left(1\right)$.

With the Laplace transform of $I_{s,ap}$ and $I_{ap,ap}$, we derive the Laplace transform of In_{ap} as

$$\begin{aligned} &\mathcal{L}_{In_{ap}}\left(s\right) = \mathcal{L}_{I_{s,ap}}\left(s\right)\mathcal{L}_{I_{ap,ap}}\left(s\right) = \\ &\exp\left\{-\left(\lambda_s\rho_s+\lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}}\right)\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)s^{2/\alpha}\right\}. \end{aligned} \tag{A.6}$$

Substituting (A.6) into (A.3), we obtain

$$\begin{aligned} \Pr\left[\frac{\left\|\mathbf{h}_{s_0,ap_0}\right\|^2 r^{-\alpha}}{In_{ap}+\delta^2/P_s} \le \gamma_{th}\right] =& 1-\exp\left\{-\left(\lambda_s\rho_s+\lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}}\right)\right. \\ & \left.\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)\left(\gamma_{th}\right)^{2/\alpha}r^2-\gamma_{th}r^\alpha\delta^2/P_s\right\} \\ & -\sum_{m=1}^{M-1}\frac{\left(r^\alpha\right)^m}{m!(-1)^m}\left.\frac{d^m\left(V\left(x\right)\right)}{dx^m}\right|_{x=r^\alpha}, \end{aligned} \tag{A.7}$$

where $V\left(x\right) = \exp\left\{-\left(\lambda_s\rho_s+\lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}}\right)\pi\Gamma\left(1+2/\alpha\right)\right.$ $\left.\Gamma\left(1-2/\alpha\right)\left(\gamma_{th}x\right)^{2/\alpha}-\gamma_{th}x\delta^2/P_s\right\}$.

We then apply the Fa$\grave{a}$ di Bruno's formula to solve the derivative of mth order as follows:

$$\begin{aligned}&\Pr\left[\frac{\left\|\mathbf{h}_{s_0,ap_0}\right\|^2 r^{-\alpha}}{In_{ap}+\delta^2/P_s}\le\gamma_{th}\right]=1-\exp\left\{-\left(\lambda_s\rho_s+\lambda_{ap}\rho_{ap}\mu^{\frac{2}{\alpha}}\right)\right.\\&\left.\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)\left(\gamma_{th}\right)^{2/\alpha}r^2-\gamma_{th}r^\alpha\delta^2/P_s\right\}-\\&\sum_{m=1}^{M-1}\frac{\left(r^\alpha\right)^m}{\left(-1\right)^m}\sum\frac{1}{\prod\limits_{l=1}^{m}m_l!l!^{m_l}}\exp\left\{-\left(\lambda_s\rho_s+\lambda_{ap}\rho_{ap}\mu^{2/\alpha}\right)\right.\\&\left.\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)\left(\gamma_{th}\right)^{2/\alpha}r^2-\gamma_{th}r^\alpha\delta^2/P_s\right\}\\&\left[-2/\alpha\left(\lambda_s\rho_s+\lambda_{ap}\rho_{ap}\mu^{2/\alpha}\right)\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)\right.\\&\left.\left(\gamma_{th}\right)^{\frac{2}{\alpha}}r^{(2-\alpha)}-\gamma_{th}\delta^2/P_s\right]^{m_1}\prod_{l=2}^{m}\left[-\left(\lambda_s\rho_s+\lambda_{ap}\rho_{ap}\mu^{2/\alpha}\right)\right.\\&\left.\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)\left(\gamma_{th}\right)^{\frac{2}{\alpha}}\prod_{j=0}^{l-1}\left(2/\alpha-j\right)r^{2-l\alpha}\right]^{m_l}.\end{aligned}\tag{A.8}$$

Substituting (A.8) into (A.1),we derive the CDF of γ_{ap} in (6).

Appendix B
A Proof of Lemma 2

From (2), the CDF of $\gamma_{s,e}$ is given by

$$\begin{aligned}&F_{\gamma_{s,e}}\left(\gamma_{th}\right)=\Pr\left\{\max_{e_k\in\Phi_{s,e}}\left\{\frac{\left|h_{s_0,e_k}\right|^2\left|X_{s_0,e_k}\right|^{-\alpha}}{In_{s,e}+\delta^2/P_s}\right\}\le\gamma_{th}\right\}\\&=\mathbb{E}_{\Phi_{s,a}}\left\{\mathbb{E}_{\Phi_{ap,a}}\left\{\mathbb{E}_{\Phi_{s,e}}\left\{\prod_{e_k\in\Phi_{s,e}}\Pr\left\{\frac{\left|h_{s_0,e_k}\right|^2\left|X_{s_0,e_k}\right|^{-\alpha}}{In_{s,e}+\delta^2/P_s}\right.\right.\right.\right.\\&\qquad\left.\left.\left.\left.\le\gamma_{th}\middle|\Phi_{s,a},\Phi_{ap,a},\Phi_{s,e}\right\}\right\}\right\}\right\}\\&=\mathbb{E}_{\Phi_{s,a}}\left\{\mathbb{E}_{\Phi_{ap,a}}\left\{\mathbb{E}_{\Phi_{s,e}}\left\{\prod_{e_k\in\Phi_{s,e}}\left(1-\right.\right.\right.\right.\\&\qquad\left.\left.\left.\left.\int_0^\infty e^{-\left(\tau+\delta^2/P_s\right)\gamma_{th}\left|X_{s_0,e_k}\right|^\alpha}d\Pr\left(In_{s,e}\le\tau\right)\right)\right\}\right\}\right\}\\&=\mathbb{E}_{\Phi_{s,e}}\{\prod_{e_k\in\Phi_{s,e}}\left(1-e^{-\delta^2\gamma_{th}\left|X_{s_0,e_k}\right|^\alpha/P_s}\right.\\&\qquad\left.\mathcal{L}_{In_{s,e}}\left(\gamma_{th}\left|X_{s_0,e_k}\right|^\alpha\right)\right)\}\\&\overset{(a)}{=}\exp\left\{-\lambda_e^s\int\limits_{R^2}e^{-\delta^2\gamma_{th}\left|X_{s_0,e_k}\right|^\alpha/P_s}\mathcal{L}_{In_{s,e}}\left(\gamma_{th}\left|X_{s_0,e_k}\right|^\alpha\right)\right.\\&\qquad d\left|X_{s_0,e_k}\right|\}\\&\overset{(b)}{=}\exp\left\{-2\pi\lambda_e^s\int_0^\infty e^{-\delta^2\gamma_{th}r^\alpha/P_s}\mathcal{L}_{In_{s,e}}\left(\gamma_{th}r^\alpha\right)rdr\right\},\end{aligned}\tag{B.1}$$

where (a) follows from the Generating functionnal of HPPP in [25], (b) is obtained by converting cartesian coordinates to polar coordinates.

Using the Generating functionnal of HPPP in [25], $\left|h_{i,e_k}\right|^2\sim\exp\left(1\right)$, and $H_j^{ap,e}=\left|\mathbf{h}_{j,e_k}\frac{\mathbf{h}_{j,sk_j}{}^\dagger}{\left\|\mathbf{h}_{j,sk_j}\right\|}\right|^2\sim\exp\left(1\right)$, we derive the Laplace transform of $I_{s,e}$ and $I_{ap,e}$ as

$$\begin{aligned}&\mathcal{L}_{I_{s,e}}\left(s\right)\\&\quad=\exp\left(-\int\left[1-\mathbb{E}_h\left(\exp\left(-s\left|h_{i,e_k}\right|^2y^{-\alpha}\right)\right)\right]\lambda_s\rho_s2\pi ydy\right)\\&\quad=\exp\left\{-\lambda_s\rho_s\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)s^{2/\alpha}\right\},\end{aligned}\tag{B.2}$$

and

$$\begin{aligned}&\mathcal{L}_{I_{ap,e}}\left(s\right)\\&\quad=\exp\left(-\int\left[1-\mathbb{E}_h\left(\exp\left(-s\mu H_j^{ap,e}y^{-\alpha}\right)\right)\right]\lambda_{ap}\rho_{ap}2\pi ydy\right)\\&\quad=\exp\left\{-\lambda_{ap}\rho_{ap}\pi\mu^{\frac{2}{\alpha}}\mathbb{E}_h\left\{\left(H_j^{ap,e}\right)^{\frac{2}{\alpha}}\right\}\Gamma\left(1-2/\alpha\right)s^{2/\alpha}\right\}\\&\quad=\exp\left\{-\lambda_{ap}\rho_{ap}\pi\mu^{\frac{2}{\alpha}}\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)s^{2/\alpha}\right\},\end{aligned}\tag{B.3}$$

respectively.

With the Laplace transform of $I_{s,e}$ and $I_{ap,e}$, we derive the Laplace transform of $In_{s,e}$ as

$$\begin{aligned}\mathcal{L}_{In_{s,e}}\left(s\right)=&\exp\left\{-\lambda_s\rho_s\pi\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)s^{2/\alpha}-\lambda_{ap}\right.\\&\left.\rho_{ap}\pi\mu^{2/\alpha}\Gamma\left(1+2/\alpha\right)\Gamma\left(1-2/\alpha\right)s^{2/\alpha}\right\}.\end{aligned}\tag{B.4}$$

Substituting (B.4) into (D.1), we derive the CDF of $\gamma_{s,e}$ in (7).

Appendix C
A Proof of Lemma 3

From (3), the CDF of γ_{sk} is given by

$$\begin{aligned}&F_{\gamma_{sk}}\left(\gamma_{th}\right)\\&\quad=\int_0^\infty\Pr\left[\frac{\left\|\mathbf{g}_{ap_0,sk_0}\right\|^2r^{-\beta}}{In_{ap,sk}+\delta^2/P_{ap}}\le\gamma_{th}\right]f_{\left|X_{ap_0,sk_0}\right|}\left(r\right)dr\\&\quad=\int_0^\infty\Pr\left[\frac{\left\|\mathbf{g}_{ap_0,Sk_0}\right\|^2r^{-\beta}}{In_{ap,sk}+\delta^2/P_{ap}}\le\gamma_{th}\right]2\pi\lambda_{sk}r\\&\qquad\exp\left(-\pi\lambda_{sk}r^2\right)dr.\end{aligned}\tag{C.1}$$

where $f_{\left|X_{ap_0,Sk_0}\right|}\left(r\right)$ is the PDF of the nearest distance between the sink and the typical access point.

The CDF of the sink SINR at distance r from its corresponding access point is derived as

$$\begin{aligned}&\Pr\left[\frac{\left\|\mathbf{g}_{ap_0,sk_0}\right\|^2r^{-\beta}}{In_{ap,sk}+\delta^2/P_{ap}}\le\gamma_{th}\right]=\mathbb{E}_{\Phi_{ap,a}}\left\{\Pr\left[\left\|\mathbf{g}_{ap_0,sk_0}\right\|^2\le\right.\right.\\&\qquad\left.\left.\gamma_{th}r^\beta\left(In_{ap,sk}+\delta^2/P_{ap}\right)\middle|\Phi_{ap,a}\right]\right\}\\&\quad=1-\sum_{m=0}^{M-1}\frac{1}{m!}\mathbb{E}_{\Phi_{ap,a}}\left\{\int_0^\infty\left[\gamma_{th}r^\beta\left(\tau+\delta^2/P_{ap}\right)\right]^m\right.\\&\qquad\left.\exp\left[-\gamma_{th}r^\beta\left(\tau+\delta^2/P_{ap}\right)\right]d\Pr\left(In_{ap,sk}\le\tau\right)\right\}.\end{aligned}\tag{C.2}$$

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

$$\Pr\left[\frac{\|\mathbf{g}_{ap_0,sk_0}\|^2 r^{-\beta}}{In_{ap,sk}+\delta^2/P_{ap}}\le\gamma_{th}\right]=1-\mathbb{E}_{\Phi_{ap,a}}\left\{\int_0^\infty \exp\left[-\gamma_{th}r^\beta\left(\tau+\delta^2/P_{ap}\right)\right]d\Pr\left(In_{ap,sk}\le\tau\right)\right\}$$
$$-\sum_{m=1}^{M-1}\frac{\left(r^\beta\right)^m}{m!(-1)^m}\mathbb{E}_{\Phi_{ap,a}}\left\{\int_0^\infty \left.\frac{d^m\left(e^{-\gamma_{th}x\left(\tau+\delta^2/P_{ap}\right)}\right)}{dx^m}\right|_{x=r^\beta} d\Pr\left(In_{ap,sk}\le\tau\right)\right\}$$
$$=1-\exp\left(-\gamma_{th}r^\beta\delta^2/P_{ap}\right)\mathcal{L}_{In_{ap,sk}}\left(\gamma_{th}r^\beta\right)-\sum_{m=1}^{M-1}\frac{\left(r^\beta\right)^m}{m!(-1)^m}\left.\frac{d^m\left(\exp\left(-\gamma_{th}x\delta^2/P_{ap}\right)\mathcal{L}_{In_{ap,sk}}\left(\gamma_{th}x\right)\right)}{dx^m}\right|_{x=r^\beta}. \tag{C.3}$$

Since $In_{ap,sk}=\sum_{j\in\Phi_{ap,a}\backslash\{ap_0\}}\left|\mathbf{g}_{j,sk_0}\frac{\mathbf{h}_{j,sk_j}{}^\dagger}{\|\mathbf{h}_{j,sk_j}\|}\right|^2|X_{j,sk_0}|^{-\beta}$, using the Generating functionnal of HPPP and $\left|\mathbf{g}_{j,Sk_0}\frac{\mathbf{h}_{j,sk_j}{}^\dagger}{\|\mathbf{h}_{j,sk_j}\|}\right|^2 \sim \exp(1)$, we derive the Laplace transform of $In_{ap,sk}$ as

$$\mathcal{L}_{In_{ap,sk}}(s)=\exp\left\{-\lambda_{ap}\rho_{ap}\pi\Gamma\left(1+2/\beta\right)\Gamma\left(1-2/\beta\right)s^{2/\beta}\right\}. \tag{C.4}$$

Substituting (C.4) into (C.3), we obtain

$$\Pr\left[\frac{\|\mathbf{g}_{ap_0,sk_0}\|^2 r^{-\beta}}{In_{ap,sk}+\delta^2/P_{ap}}\le\gamma_{th}\right]=1-\exp\left\{-\lambda_{ap}\rho_{ap}\pi\Gamma\left(1+2/\beta\right)\Gamma\left(1-2/\beta\right)\left(\gamma_{th}\right)^{2/\beta}r^2-\gamma_{th}r^\beta\delta^2/P_{ap}\right\}$$
$$-\sum_{m=1}^{M-1}\frac{\left(r^\beta\right)^m}{m!(-1)^m}\left.\frac{d^m\left(U\left(x\right)\right)}{dx^m}\right|_{x=r^\beta} \tag{C.5}$$

with $U\left(x\right)=\exp\left\{-\lambda_{ap}\rho_{ap}\pi\Gamma\left(1+2/\beta\right)\Gamma\left(1-2/\beta\right)\left(\gamma_{th}x\right)^{2/\beta}-\gamma_{th}x\delta^2/P_{ap}\right\}$.

We then apply the Fa$\grave{a}$ di Bruno's formula to solve the derivative of mth order as follows:

$$\left.\frac{d^m\left[\exp\left(U\left(x\right)\right)\right]}{dx^m}\right|_{x=r^\beta}=\sum\frac{1}{\prod\limits_{l=1}^{m}m_l!l!^{m_l}}\exp\left\{-\lambda_{ap}\rho_{ap}\pi\Gamma\left(1+2/\beta\right)\Gamma\left(1-2/\beta\right)\left(\gamma_{th}\right)^{2/\beta}r^2-\gamma_{th}r^\beta\delta^2/P_{ap}\right\}\Big[-\lambda_{ap}\rho_{ap}\pi\frac{2}{\beta}\Gamma\left(1+2/\beta\right)\Gamma\left(1-2/\beta\right)\left(\gamma_{th}\right)^{2/\beta}x^{2/\beta-1}-\gamma_{th}\delta^2/P_{ap}\Big]^{m_1}$$
$$\prod_{l=2}^{m}\Big[-\lambda_{ap}\rho_{ap}\pi\Gamma\left(1+2/\beta\right)\Gamma\left(1-2/\beta\right)\left(\gamma_{th}\right)^{2/\beta}\prod_{j=0}^{l-1}\left(2/\beta-j\right)x^{2/\beta-l}\Big]^{m_l}. \tag{C.6}$$

Based on (C.6), (C.5), and (C.1), we derive the CDF of γ_{sk} in (11).

Appendix D
A Proof of Lemma 4

From (4), the CDF of $\gamma_{ap,e}$ is given by

$$F_{\gamma_{s,e}}\left(\gamma_{th}\right)=\mathbb{E}_{\Phi_{ap,a}}\left\{\mathbb{E}_{\Phi_{ap,e}}\left\{\prod_{e\Phi_{ap,e}}\Pr\left\{\frac{|g_{ap_0,e_k}|^2}{In_{ap,e}+\sigma^2/P_{ap}}|X_{ap_0,e_k}|^{-\beta}\le\gamma_{th}\middle|\Phi_{ap,a},\Phi_{ap,e}\right\}\right\}\right\}$$
$$=\mathbb{E}_{\Phi_{ap,a}}\left\{\mathbb{E}_{\Phi_{ap,e}}\left\{\prod_{e\Phi_{ap,e}}\left(1-\int_0^\infty e^{-\left(\tau+\sigma^2/P_{ap}\right)\gamma_{th}|X_{ap_0,e_k}|^\beta}d\Pr\left(In_{ap,e}\le\tau\right)\right)\right\}\right\}$$
$$=\mathbb{E}_{\Phi_{ap,e}}\left\{\prod_{\Phi_{ap,e}}\left(1-e^{-\sigma^2\gamma_{th}|X_{ap_0,e_k}|^\beta/P_{ap}}\mathcal{L}_{In_{ap,e}}\left(\gamma_{th}|X_{ap_0,e_k}|^\beta\right)\right)\right\}$$
$$\overset{(a)}{=}\exp\left\{-\lambda_e^{ap}\int_{R^2}e^{-\sigma^2\gamma_{th}|X_{ap_0,e_k}|^\beta/P_{ap}}\mathcal{L}_{In_{ap,e}}\left(\gamma_{th}|X_{ap_0,e_k}|^\beta\right)de\right\}$$
$$\overset{(b)}{=}\exp\left\{-2\pi\lambda_e^{ap}\int_0^\infty e^{-\sigma^2\gamma_{th}r^\beta/P_{ap}}\mathcal{L}_{In_{ap,e}}\left(\gamma_{th}r^\beta\right)rdr\right\}, \tag{D.1}$$

where (a) follows from the Generating functionnal of HPPP in [25], (b) is obtained by converting cartesian coordinates to polar coordinates.

Using the Generating functionnal of HPPP in [25], we derive the Laplace transform of $I_{ap,e}$ as

$$\mathcal{L}_{I_{ap,e}}(s)=\exp\left\{-\lambda_{ap}\rho_{ap}\pi\Gamma\left(1+2/\beta\right)\Gamma\left(1-2/\beta\right)s^{2/\beta}\right\}. \tag{D.2}$$

Plugging (D.2) into (D.1), we derive the CDF of $\gamma_{s,e}$ in (12).

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug 2002.

[2] L. Wang, K. Kim, T. Duong, M. Elkashlan, and H. Poor, "Security enhancement of cooperative single carrier systems," *IEEE Trans. Inf. Forensics Security*, 2014.

[3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Technol. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[4] H. V. Poor, "Information and inference in the wireless physical layer,," *IEEE Wireless Commun.*, pp. 40–47, Feb. 2012.

[5] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006–2021, June 2014.

[6] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2776–2787, June 2013.

[7] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, 2010.

[8] J. Zhang and M. C. Gursoy, "Secure relay beamforming over cognitive radio channels," in *Proc of 45th Annual Conference on Information Sciences and Systems (CISS)*, Baltimore, MD, Mar. 2011, pp. 1–5.

[9] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the security of cognitive radio networks," *IEEE Trans. Veh. Technol.*, 2014.

[10] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[11] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *Selected Areas in Communications, IEEE Journal on*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[12] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *IEEE Global Telecommun. Conf. (GLOBECOM)*, 2008, pp. 1–5.

[13] L. Wang, M. Elkashlan, J. Huang, N. H. Tran, and T. Q. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," vol. 3, no. 3, pp. 289–292, June 2014.

[14] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425–430, Feb. 2011.

[15] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjorungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, August 2011.

[16] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks," vol. 8, no. 11, pp. 1802–1814, Nov. 2013.

[17] X. Li, M. Chen, and E. P. Ratazzi, "Array-transmission based physical-layer security techniques for wireless sensor networks," in *IEEE Int. Conf. Mechatronics and Automation (ICMA)*, 2005, pp. 1618–1623.

[18] S. Marano, V. Matta, and P. K. Willett, "Distributed detection with censoring sensors under physical layer secrecy," *IEEE Trans. Signal Process.*, vol. 57, no. 5, pp. 1976–1986, May 2009.

[19] R. Soosahabi and M. Naraghi-Pour, "Scalable PHY-layer security for distributed detection in wireless sensor networks," vol. 7, no. 4, pp. 1118–1126, Aug 2012.

[20] J. E. Barcelo-Llado, A. Morell, and G. Seco-Granados, "Amplify-and-forward compressed sensing as a physical-layer secrecy solution in wireless sensor networks," vol. 9, no. 5, pp. 839–850, May 2014.

[21] H. S. Dhillon, R. K. Ganti, F. Baccelli, and J. G. Andrews, "Modeling and analysis of K-tier downlink heterogeneous cellular networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 3, pp. 550–560, April 2012.

[22] C. han Lee and M. Haenggi, "Interference and outage in Poisson cognitive networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 4, pp. 1392–1401, April 2012.

[23] M. Yuksel and E. Erkip, "Diversity-Multiplexing tradeoff for the multiple-antenna wire-tap channel," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 762–771, 2011.

[24] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 247–258, Feb. 2014.

[25] D. Stoyan, W. Kendall, and J. Mecke, "Stochastic geometry and its applications," *Wiley New York*, vol. 2, 1987.