Sensor Networks

Secrecy Performance Analysis of Wireless Sensor Networks

Yun Ai[1*], Michael Cheffena[1], Tomoaki Ohtsuki[2**], and He Zhuang[2]

[1] *Faculty of Engineering, Norwegian University of Science and Technology, 2815 Gjøvik, Norway*
[2] *Department of Information and Computer Science, Keio University, Yokohama 223-8522, Japan*
[*] *Member, IEEE*
[**] *Senior Member, IEEE*

Manuscript received Month Day, 2019; revised Month Day, 2019.

Abstract—Wireless sensor network (WSN) plays a fundamentally important role in the realization of Internet of Things and Industry 4.0. In this letter, we study the physical layer security performance of a large-scale ad hoc and homogeneous WSN. To accurately evaluate the secrecy performance of the large-scale WSN, we take into account the randomness of the interfering nodes (both in terms of the number of nodes and their respective position) based on Poisson point process (PPP) in our analysis. We derive novel expressions for the average secrecy capacity (ASC) and secrecy outage probability (SOP) including the effects of fading, path loss, and the network's spatial randomness. The results demonstrate the impacts of several factors such as node intensity, transmission power in large-scale WSN on secrecy performance, which should be seriously taken into consideration while designing WSNs.

Index Terms—Physical layer security, wireless sensor network (WSN), Poisson point process (PPP), fading channels, interference.

I. INTRODUCTION

Physical layer security (PLS) has been widely considered as a complementary instrument to the conventional cryptographic techniques in enhancing the communication secrecy in communication systems [1]–[4]. PLS was proposed to achieve information-theoretic security in communication systems by exploiting the randomness in the propagation channels. Due to the broadcasting nature of the wireless channels, the security of WSNs is a big concern considering the importance of secure data transmission in the Internet of Things and Industry 4.0 era. To this end, there has an increasing number of research exploring the physical layer secrecy performance of wireless systems with different configurations over various channel conditions.

The secrecy transmission capacity (STC) of wireless networks was studied in [5], where the secrecy transmission capacity is defined in terms of connection outage probability and rate of confidential message. The secrecy transmission capacity proposed in [5] is different from the widely investigated average secrecy capacity (ASC) in the sense that the former concept focuses on the area spectral efficiency of wireless network. The effect of noise power on the STC in a wireless ad hoc network was investigated in [6], which reveal that an appropriate amount of noise can enhance the secrecy transmission capacity. The uplink secrecy performance of a D2D cellular network with the presence of multiple D2D nodes and eavesdroppers was analyzed in [7] with interferences being neglected. The PLS performance of a ultra-dense network was studied in [8] by considering the close proximity of the users to the cells and the most detrimental eavesdropper. The secrecy outage performance of a wireless sensor network with a single sink in the presence of a single eavesdropper under sensor scheduling scheme was analyzed in [9], where it was also assumed that the positions of the sensor nodes are fixed.

Motivated by the advances in PLS and considering the wide applications of WSN, we analyze in this letter the secrecy performance of a large-scale homogeneous sensor network by taking into account path loss, fading, the randomness of sensor nodes as well as the interferences from randomly located neighboring nodes. More specifically, the randomness of peer nodes with concurrent transmission is accommodated by modeling the nodes in the sensor network as a homogeneous Poisson point process (PPP). Exact and novel expressions for the ASC and secrecy outage probability (SOP) are derived. The conducted analysis featuring ASC and SOP in this letter focuses on the secrecy performance of a typical link. This significantly differs from the previous work focusing on STC, where the analysis is done from the perspective of the network.

Notations: $\|x-y\|$ denotes the Euclidean distance between positions x and y, $\mathbb{E}\{\cdot\}$ represents the expectation operator, $B(x,y)$ is the Beta function, $G_{p,q}^{m,n}(\cdot)$ is the Meijer G-function [10, Eq. 8.2.1], $H_{p,q}^{m,n}(\cdot)$ is the Fox H-function [11, Eq. 1.2], and $H_{p,q:u,v:e,f}^{m,n:s,t:i,j}(\cdot)$ is the extended generalized bivariate Fox H-function (EGBFHF) [11, Eq. 2.56], which can be readily evaluated with Mathematica [12, Table I].

II. CHANNEL AND SYSTEM MODELS

We assume that in a large-scale WSN, there exists an eavesdropper node E that is particularly positioned close to a specific sensor node S to eavesdrop the measured data S is sending to a specific cluster head or sink node D (see Fig. 1). Under the framework of stochastic geometry, we construct the investigated scenario as follows: we first model the half-duplex source nodes of the WSN as a homogeneous PPP Φ_t with intensity λ considering the randomness of nodes. The dedicated receiver for each source node is uniformly distributed in a circle centered at its source node with some radius, which lead to another PPP Φ_r with the same intensity λ according to the Displacement Theorem[1] [13]. All links between the generated nodes undergo independent and identically distributed (i.i.d.) Nakagami-m fading. Next, an additional node is placed into the WSN, which serves as the source node S of our investigated security problem. It should be noted that the inclusion of node S at a fixed location does not change the distribution of the PPP according to the Slivnyak's Theorem [13]. By considering the Wyner's wiretap model [14], the source node

[1] It should be noted that the transmitting source nodes can be receiving destination nodes or even in sleeping mode in next time slot. However, we assume that at any time, the densities of the operating source and destination nodes in the considered large-scale network are constant being Φ_t and Φ_r, respectively.

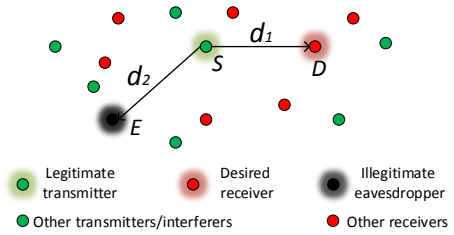

Fig. 1: Illustration of the investigated system.

S transmits confidential information to the desired receiver D over the main channel. The eavesdropper E attempts to intercept these messages by decoding its received signal through the eavesdropper channel. For mathematical tractability, we assume that the legitimate link S–D and leaked link S–E experience i.i.d. Rayleigh fading instead of the Nakagami-m fading. The distance between nodes S and D is d_1 while the distance is d_2 between nodes S and E. Additionally, it is practical to assume that all WSN nodes transmit with the same power P with single antenna.

Taking into account both path loss and small-scale fading, the channel power gain of the link with the transmitter at x and receiver at y is

$$|g_{xy}|^2 = |h_{xy}|^2 \cdot \ell(x-y), \tag{1}$$

where $|h_{xy}|^2$ is a Gamma or exponential random variable (RV) with unit mean resulting from the small-scale (Nakagami-m or Rayleigh) fading, the term $\ell(x-y) = \|x-y\|^{-\alpha}$ captures the path loss effect with $\alpha > 2$ being the path loss exponent [15].

We first consider the instantaneous signal-to-interference-plus-noise ratio (SINR) received at the desired node D, i.e.,

$$\gamma_D = \frac{|g_{SD}|^2 P}{\sum\limits_{x\in\Phi_t} |g_{xD}|^2 P + W} = \frac{|h_{SD}|^2 d_1^{-\alpha} P}{\sum\limits_{x\in\Phi_t} |h_{xD}|^2 \|x-D\|^{-\alpha} P + W}, \tag{2}$$

where W is the power of the additive white Gaussian noise (AWGN). For notational simplicity, we denote $S = |h_{SD}|^2 d_1^{-\alpha}$, $I = \sum\limits_{x\in\Phi_t} |h_{xD}|^2 \cdot \|x-D\|^{-\alpha}$, and $W_0 = W/P$ hereinafter. It should be noted that in (2), $|h_{SD}|$ is a Rayleigh RV while $|h_{xD}|$, $x \in \Phi_t$, follows Nakagami-m distribution.

The complementary cumulative distribution function (CDF) of the SINR γ_D can be derived according to its definition as

$$\begin{aligned}\bar{F}_{\gamma_D}(\theta) =& \Pr(S > \theta(I+W_0)) \overset{(a)}{=} \mathbb{E}_I\left(\exp\left(-\frac{\theta(I+W_0)}{d_1^{-\alpha}}\right)\right)\\ =& \exp\left(-\frac{\theta W_0}{d_1^{-\alpha}}\right)\cdot \mathbb{E}_I\left(\exp\left(-\frac{\theta I}{d_1^{-\alpha}}\right)\right),\end{aligned} \tag{3}$$

where the equality (a) is due to the fact that $|h_{SD}|^2$ is Rayleigh distributed with unit mean.

By denoting $s = \frac{\theta}{d_1^{-\alpha}}$ in the expectation operator in (3), it is obvious that the expectation of the exponential term in (3) is exactly the Laplace transform of the RV I. Based on the theory of point processes and the fact that the fading is i.i.d., the Laplace transform of I can be further expressed as

$$\begin{aligned}\mathcal{L}(s) =& \mathbb{E}\left(\prod_{x\in\Phi_t} \exp\left(-s|h_{xD}|^2\cdot\|x-D\|^{-\alpha}\right)\right)\\ =& \mathbb{E}_\Phi\left(\prod_{x\in\Phi_t} \mathbb{E}_h\left(\exp\left(-s|h_{xD}|^2\cdot\|x-D\|^{-\alpha}\right)\right)\right).\end{aligned} \tag{4}$$

Next, utilizing the mapping theorem [13] and with the help of probability generating functional (PGFL) [16, p. 245], the Laplace transform of the interference I with links experiencing Nakagami-m fading can be solved as [13], [16]

$$\mathcal{L}(s) = \exp\left(-\pi\lambda s^{\frac{2}{\alpha}} m^{\frac{2}{\alpha}} \frac{\Gamma(m+\frac{2}{\alpha})\cdot\Gamma(1-\frac{2}{\alpha})}{\Gamma(m)}\right), \tag{5}$$

where m is the Nakagami-m fading parameter.

Utilizing (5) in (3) and relationship between cumulative CDF and CDF, the CDF $F_{\gamma_D}(\theta)$ of the SINR γ_D can be written as

$$F_{\gamma_D}(\theta) = 1 - \exp\left(-\frac{W\theta}{d_1^{-\alpha}P} - \pi\lambda d_1^2 (m\theta)^{\frac{2}{\alpha}} \frac{\Gamma(m+\frac{2}{\alpha})\Gamma(1-\frac{2}{\alpha})}{\Gamma(m)}\right). \tag{6}$$

The probability density function (PDF) $f_{\gamma_D}(\theta)$ of the SINR γ_D can be derived from its relation with CDF as

$$\begin{aligned}f_{\gamma_D}(\theta) =& \exp\left(-\frac{W}{d_1^{-\alpha}P}\theta - \pi\lambda d_1^2 m^{\frac{2}{\alpha}} \frac{\Gamma(m+\frac{2}{\alpha})\Gamma(1-\frac{2}{\alpha})}{\Gamma(m)}\theta^{\frac{2}{\alpha}}\right)\\ &\cdot\left(\frac{W}{d_1^{-\alpha}P} + \frac{2\pi}{\alpha}\lambda d_1^2 m^{\frac{2}{\alpha}} \frac{\Gamma(m+\frac{2}{\alpha})\Gamma(1-\frac{2}{\alpha})}{\Gamma(m)}\theta^{\frac{2}{\alpha}-1}\right).\end{aligned} \tag{7}$$

Due to the homogeneity of homogeneous PPP, the CDF $F_{\gamma_E}(\theta)$ and PDF $f_{\gamma_E}(\theta)$ of the SINR γ_E can be directly obtained by replacing d_1 with d_2 in (6) and (7). Also, we denote $\mathcal{A} = \pi\lambda m^{\frac{2}{\alpha}} \frac{\Gamma(m+\frac{2}{\alpha})\Gamma(1-\frac{2}{\alpha})}{\Gamma(m)}$ for simplicity in the following.

Remark 1: If all interfering links also undergo Rayleigh fading, the corresponding CDF $F_{\gamma_X}(\theta)$ of the SINR γ_X, $X \in \{D, E\}$, follows immediately by setting $m = 1$ in (6) as

$$F_{\gamma_D}(\theta) = 1 - \exp\left(-\frac{W\theta}{d_1^{-\alpha}P}\right)\cdot\exp\left(-\pi\lambda d_1^2\theta^{\frac{2}{\alpha}}\cdot B\left(1-\frac{2}{\alpha}, 1+\frac{2}{\alpha}\right)\right). \tag{8}$$

III. SECRECY PERFORMANCE ANALYSIS

A. Secrecy Capacity Analysis

The instantaneous secrecy capacity of the considered system is defined as $C_s(\gamma_D, \gamma_E) = \max\{\ln(1+\gamma_D) - \ln(1+\gamma_E), 0\}$ [17]. The average secrecy capacity is a fundamental secrecy performance metric and the ASC $\overline{C}_s$ can be obtained from [18]

$$\begin{aligned}\overline{C}_s =& \mathbb{E}\{C_s(\gamma_D,\gamma_E)\} = \int_0^\infty \frac{F_{\gamma_E}(\gamma)}{1+\gamma}\left[\int_\gamma^\infty f_{\gamma_D}(\gamma_D)\,d\gamma_D\right]d\gamma\\ =& \int_0^\infty \frac{F_{\gamma_E}(\gamma)}{1+\gamma}\cdot\left[1-F_{\gamma_D}(\gamma)\right]d\gamma.\end{aligned} \tag{9}$$

Substituting the CDFs $F_{\gamma_D}(\cdot)$ and $F_{\gamma_E}(\cdot)$ into (9), the ASC can be rewritten in terms of two integrals as

$$\overline{C}_s = \mathcal{I}_1 - \mathcal{I}_2, \tag{10}$$

where $\mathcal{I}_1 = \int_0^\infty \frac{1}{1+\gamma}\cdot\exp\left(-W_0 d_1^\alpha\gamma\right)\cdot\exp\left(-\mathcal{A}d_1^2\gamma^{\frac{2}{\alpha}}\right)d\gamma$ and $\mathcal{I}_2 = \int_0^\infty \frac{1}{1+\gamma}\cdot\exp\left(-W_0(d_1^\alpha+d_2^\alpha)\gamma\right)\cdot\exp\left(-\mathcal{A}(d_1^2+d_2^2)\gamma^{\frac{2}{\alpha}}\right)d\gamma$.

We first solve the integral $\mathcal{I}_1$. Expressing the terms in $\mathcal{I}_1$ in their corresponding Meijer-G representations [14], we can obtain the following expression in terms of contour integral:

$$\begin{aligned}\mathcal{I}_1 \overset{(b)}{=}& \frac{1}{2\pi j}\oint_{L_1}\Gamma(s)(\mathcal{A}d_1^2)^{-s}\int_0^\infty \gamma^{-\frac{2}{\alpha}s} G_{1,1}^{1,1}\left(\gamma\middle|\begin{matrix}0\\0\end{matrix}\right) G_{0,1}^{1,0}\left(d_1^\alpha W_0\gamma\middle|\begin{matrix}-\\0\end{matrix}\right)d\gamma ds\\ \overset{(c)}{=}& \frac{1}{2\pi j}\oint_{L_1}\Gamma(s)(\mathcal{A}d_1^2)^{-s} H_{1,2}^{2,1}\left(W_0 d_1^\alpha\middle|\begin{matrix}(\frac{2}{\alpha}s,1)\\(0,1),(\frac{2}{\alpha}s,1)\end{matrix}\right)d\gamma,\end{aligned} \tag{11}$$

where (b) follows by employing the definition of Meijer G-function in terms of Mellin-Barnes type contour integral [19, Eq. 9.30] for the last term and changing the integration order. The equality (c) is obtained by solving the inner integral using [10, Eq. 8.4.51] and [11, Chpt. 2.3].

$$\overline{C}_s = \frac{d_1^{-\alpha}}{W_0} H^{0,1:1,1:1,0}_{1,0:1,1:0,1}\left(\begin{matrix}(0;1,\frac{2}{\alpha})\\ -\end{matrix}\middle|\begin{matrix}(0,1)\\(0,1)\end{matrix}\middle|\begin{matrix}-\\(0,1)\end{matrix}\middle|\begin{matrix}\frac{d_1^{-\alpha}}{W_0},\frac{\mathcal{A}}{W_0^{\frac{2}{\alpha}}}\end{matrix}\right) - \frac{(d_1^{\alpha}+d_2^{\alpha})^{-1}}{W_0} H^{0,1:1,1:1,0}_{1,0:1,1:0,1}\left(\begin{matrix}(0;1,\frac{2}{\alpha})\\ -\end{matrix}\middle|\begin{matrix}(0,1)\\(0,1)\end{matrix}\middle|\begin{matrix}-\\(0,1)\end{matrix}\middle|\begin{matrix}\frac{(d_1^{\alpha}+d_2^{\alpha})^{-1}}{W_0},\frac{\mathcal{A}(d_1^2+d_2^2)}{[W_0(d_1^{\alpha}+d_2^{\alpha})]^{\frac{2}{\alpha}}}\end{matrix}\right). \quad (14)$$

$$SOP = 1 - \mathcal{B}\cdot\left\{\frac{2\mathcal{A}\mathcal{D}d_2^2}{\alpha\cdot[W_0\cdot(\Theta d_1^{\alpha}+d_2^{\alpha})]^{\frac{2}{\alpha}}}\cdot H^{0,1:1,0:1,1}_{1,0:0,1:1,1}\left(\begin{matrix}(1-\frac{2}{\alpha};\frac{2}{\alpha},1)\\ -\end{matrix}\middle|\begin{matrix}-\\(0,1)\end{matrix}\middle|\begin{matrix}(\frac{2k}{\alpha}+1,1)\\(0,1)\end{matrix}\middle|\begin{matrix}\frac{\mathcal{A}d_2^2}{[W_0\cdot(\Theta d_1^{\alpha}+d_2^{\alpha})]^{\frac{2}{\alpha}}},\frac{\frac{\Theta}{\Theta-1}}{W_0\cdot(\Theta d_1^{\alpha}+d_2^{\alpha})}\end{matrix}\right) + \frac{\mathcal{D}d_2^{\alpha}}{(\Theta d_1^{\alpha}+d_2^{\alpha})}\cdot H^{0,1:1,0:1,1}_{1,0:0,1:1,1}\left(\begin{matrix}(0;\frac{2}{\alpha},1)\\ -\end{matrix}\middle|\begin{matrix}-\\(0,1)\end{matrix}\middle|\begin{matrix}(\frac{2k}{\alpha}+1,1)\\(0,1)\end{matrix}\middle|\begin{matrix}\frac{\mathcal{A}d_2^2}{[W_0\cdot(\Theta d_1^{\alpha}+d_2^{\alpha})]^{\frac{2}{\alpha}}},\frac{\frac{\Theta}{\Theta-1}}{W_0\cdot(\Theta d_1^{\alpha}+d_2^{\alpha})}\end{matrix}\right)\right\}. \quad (21)$$

Next, introducing the definition of the Fox H-function [11, Eq. 1.2] in (11) leads to the following double contour integral:

$$\mathcal{I}_1 = -\frac{1}{4\pi^2}\oint_{L_1}\oint_{L_2}\frac{\Gamma(s)\Gamma(\xi)}{(\mathcal{A}d_1^2)^s}\Gamma\Big(\frac{2s}{\alpha}+\xi\Big)\Gamma\Big(1-\frac{2s}{\alpha}-\xi\Big)(W_0 d_1^{\alpha})^{-\xi}\,d\xi\,ds. \quad (12)$$

From the definition and properties of the EGBFHF [11, Eq. 2.56], the double integral $\mathcal{I}_1$ in (12) can be expressed in terms of EGBFHF after some algebra as follows:

$$\mathcal{I}_1 = \frac{1}{W_0 d_1^{\alpha}}\cdot H^{0,1:1,1:1,0}_{1,0:1,1:0,1}\left(\begin{matrix}(0;1,\frac{2}{\alpha})\\ -\end{matrix}\middle|\begin{matrix}(0,1)\\(0,1)\end{matrix}\middle|\begin{matrix}-\\(0,1)\end{matrix}\middle|\begin{matrix}\frac{1}{W_0 d_1^{\alpha}},\frac{\mathcal{A}}{W_0^{\frac{2}{\alpha}}}\end{matrix}\right). \quad (13)$$

The integral $\mathcal{I}_2$ can be solved by following the same rationale. Finally, substituting $\mathcal{I}_1$ and $\mathcal{I}_2$ into (10), we can obtain the exact expression for ASC as shown in (14).

Remark 2: When the transmit power P is much larger than the noise power W, or when the network is interference dominant, the SINR reduces to the signal-to-interference ratio (SIR). In these scenarios, the ASC can be simplified as

$$\overline{C}_s = H^{2,1}_{1,2}\Big(\mathcal{A}d_1^2\Big|^{(0,\frac{2}{\alpha})}_{(0,1),(0,\frac{2}{\alpha})}\Big) - H^{2,1}_{1,2}\Big(\mathcal{A}(d_1^2+d_2^2)\Big|^{(0,\frac{2}{\alpha})}_{(0,1),(0,\frac{2}{\alpha})}\Big). \quad (15)$$

Remark 3: By utilizing the asymptotic analysis of the Fox H-function [20], it can be shown that in interference dominant network, the ASC can be approximated by

$$\overline{C}_s \cong \frac{\alpha}{2}\cdot\Gamma\Big(\frac{\alpha}{2}\Big)\cdot\Big[(\mathcal{A}d_1^2)^{-\frac{\alpha}{2}} - (\mathcal{A}d_1^2+\mathcal{A}d_2^2)^{-\frac{\alpha}{2}}\Big]. \quad (16)$$

Analyzing the above expression (16), the following relation between ASC and node intensity λ holds in interference dominant network: $\overline{C}_s \propto \mathcal{F}_1\cdot\big(\frac{1}{\lambda}\big)^{\frac{\alpha}{2}}$, where the factor $\mathcal{F}_1$ is related to the parameters including α and m. From (16), it can also be concluded that d_1 has less impact on the ASC when d_2 is small, and d_2 has a larger impact on ASC when d_1 is small.

B. Secrecy Outage Analysis

The SOP is a useful secrecy performance metric for the passive eavesdropping scenario [21]. The SOP is expressed as the probability that the secrecy capacity falls below a target rate R_s [18], i.e.,

$$SOP = \Pr[\gamma_D \le \Theta\gamma_E + \Theta - 1] = \int_0^{\infty} f_{\gamma_E}(\gamma_E)\int_0^{(1+\gamma_E)\Theta-1} f_{\gamma_D}(\gamma_D)\,d\gamma_D\,d\gamma_E, \quad (17)$$

where $\Theta = \exp(R_s) \ge 1$.

Substituting the PDF $f_{\gamma_E}(\cdot)$ of the SINR γ_E and the PDF $f_{\gamma_D}(\cdot)$ of the SINR γ_D into (17), the SOP can be rewritten as

$$SOP = 1 - \mathcal{B}\cdot\left[\frac{2\mathcal{A}d_2^2}{\alpha}\underbrace{\int_0^{\infty} x^{\frac{2}{\alpha}-1}\mathcal{F}_2(x)\,dx}_{\mathcal{I}_3} + W_0 d_2^{\alpha}\underbrace{\int_0^{\infty}\mathcal{F}_2(x)\,dx}_{\mathcal{I}_4}\right], \quad (18)$$

where $\mathcal{B} = \exp[-W_0 d_1^{\alpha}(\Theta-1)]$ and $\mathcal{F}_2(x) = \exp(-\mathcal{A}d_2^2 x^{\frac{2}{\alpha}})\cdot\exp[-W_0(\Theta d_1^{\alpha}+d_2^{\alpha})x]\cdot\exp[-\mathcal{A}d_1^2(\Theta x+\Theta-1)^{\frac{2}{\alpha}}]$.

We first solve the integral $\mathcal{I}_3$. Expanding the exponential term $\exp[-\mathcal{A}d_1^2(\Theta x+\Theta-1)^{\frac{2}{\alpha}}]$ in series [19, Eq. 1.211.1], we obtain

$$\mathcal{I}_3 = \sum_{k=0}^{\infty}\frac{(-\mathcal{A}d_1^2\Theta^{\frac{2}{\alpha}})^k}{k!}\int_0^{\infty} x^{\frac{2}{\alpha}-1}\cdot\exp\big[-W_0(\Theta d_1^{\alpha}+d_2^{\alpha})x\big] \cdot\exp\big(-\mathcal{A}d_2^2 x^{\frac{2}{\alpha}}\big)\cdot\Big(x+\frac{\Theta-1}{\Theta}\Big)^{\frac{2k}{\alpha}}dx. \quad (19)$$

Now, expressing the relevant terms in (19) with the Fox H-functions using [10, Chpt. 8.4] and [10, Eq. 8.4.51], the integral $\mathcal{I}_3$ becomes

$$\begin{aligned}\mathcal{I}_3 =& \mathcal{D}\cdot\int_0^{\infty} x^{\frac{2}{\alpha}-1}\cdot H^{1,0}_{0,1}\Big(W_0(\Theta d_1^{\alpha}+d_2^{\alpha})x\Big|^{-}_{(0,1)}\Big) \cdot H^{1,0}_{0,1}\Big(\mathcal{A}d_2^2 x^{\frac{2}{\alpha}}\Big|^{-}_{(0,1)}\Big)\cdot H^{1,1}_{1,1}\Big(\frac{\Theta}{\Theta-1}x\Big|^{(\frac{2k}{\alpha}+1,1)}_{(0,1)}\Big)dx\\ =& \mathcal{D}\cdot H^{0,1:1,0:1,1}_{1,0:0,1:1,1}\left(\begin{matrix}(1-\frac{2}{\alpha};\frac{2}{\alpha},1)\\ -\end{matrix}\middle|\begin{matrix}-\\(0,1)\end{matrix}\middle|\begin{matrix}(\frac{2k}{\alpha}+1,1)\\(0,1)\end{matrix}\middle|\mathcal{E}_1,\mathcal{E}_2\right) \cdot[W_0\cdot(\Theta d_1^{\alpha}+d_2^{\alpha})]^{-\frac{2}{\alpha}}, \end{aligned} \quad (20)$$

where the symbols $\mathcal{D} = \sum_{k=0}^{\infty}\frac{(-\mathcal{A}d_1^2\Theta^{\frac{2}{\alpha}})^k}{k!}\cdot\big(\frac{\Theta-1}{\Theta}\big)^{\frac{2k}{\alpha}}\cdot\frac{1}{\Gamma(-\frac{2k}{\alpha})}$, $\mathcal{E}_1 = \frac{\mathcal{A}d_2^2}{[W_0\cdot(\Theta d_1^{\alpha}+d_2^{\alpha})]^{\frac{2}{\alpha}}}$, and $\mathcal{E}_2 = \frac{\frac{\Theta}{\Theta-1}}{W_0\cdot(\Theta d_1^{\alpha}+d_2^{\alpha})}$; and the last equality is from the property of the H-function [22, Eq. 2.3].

Utilizing the same approach, the integral $\mathcal{I}_4$ can be solved. Substituting the expressions of $\mathcal{I}_3$ and $\mathcal{I}_4$ into (18), we can obtain the exact expression for SOP as shown in (21).

IV. NUMERICAL RESULTS AND DISCUSSION

In this section, we evaluate the joint impact of fading, interference, and network randomness on the PLS performance of WSN. For evaluation purpose, we adopt the following simulation parameters unless otherwise specified: transmit SNR $\frac{P}{W}$ = 30 dB, path loss exponent α = 2.22, node intensity λ = 0.001, Nakagami parameter m = 1.8, and distances d_1 = 5 m, d_2 = 8 m.

Figure 2 shows the ASC of a WSN as function of node intensity λ. For the fixed value of transmit SNR, the node intensity λ does not have significant impact on the ASC until λ reaches some threshold. It can be also observed that in interference dominant WSN (i.e., large values of λ), the ASC is independent of the transmit power but depends on the Nakagami parameter m and path loss exponent α. By observing the interference dominant region of Fig. 2, it can be seen that when both ASC and λ are expressed in logarithmic scale, the parameters α and m jointly determine the horizontal shift while the slope of the declining ASC is only determined by α. This is in accordance with the analytical analysis in *Remark 3*. Figure 3 illustrates the impact of the S's and E's locations on the ASC performance. It is seen that d_1 poses less impact on ASC when the eavesdropper is close to the source node. The results reaffirms the analysis in *Remark 3* and also imply the potential application of the protected zone concept in [1] for the WSN security.

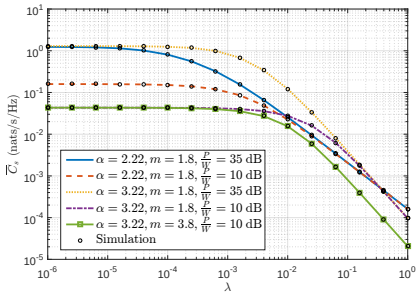

Fig. 2: The ASC vs. λ for varying α, m, and transmit SNR $\frac{P}{W}$ values.

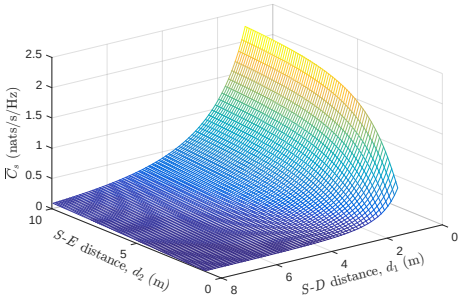

Fig. 3: The ASC vs. varying values of distances d_1 and d_2.

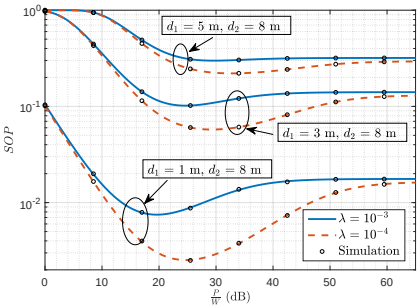

Fig. 4: The SOP vs. transmit SNR $\frac{P}{W}$ for varying d_1 and d_2 values.

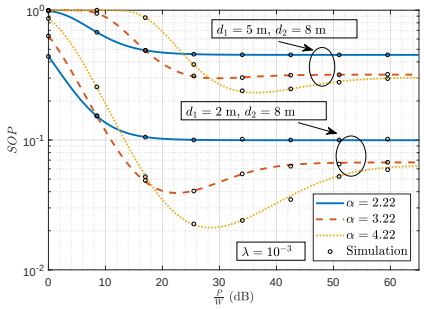

Fig. 5: The SOP vs. transmit SNR $\frac{P}{W}$ for varying α values.

Figure 4 depicts the impact of node locations of legitimate receiver and eavesdropper as well as the WSN node intensity on the SOP performance. It can be observed that there is not a monotonic relationship between the transmit SNR of WSN nodes and the SOP. More specifically, when the transmit power of WSN nodes is set low, the investigated system is still noise-constrained and better SOP performance can be achieved by increasing the transmit power. However, when the power increases to some threshold, the system performance is mainly hindered by the interference and further increasing the transmit power will degrade the performance. The results in Fig. 4 also enable the optimization between transmit power and node density, which implies that the optimal transmission power in terms of SOP decreases with the increase of node density. The non-monotonic relation is also observed between SOP and path loss exponent α in Fig. 5. This is due to the fact that secrecy capacity depends on the capacity difference of the legitimate and eavesdropper links even though greater values of path loss exponent indicate less capacity for both channels.

V. CONCLUSION

In this letter, we studied the secrecy performance of homogeneous WSNs taking into account the node randomness, fading, and path loss. Our results demonstrate the impacts of the WSN nodes transmit power and node density on the secrecy performance. It is found that the optimal transmit power of the WSN nodes in terms of SOP decreases with the increase of node density. Furthermore, in interference dominant network, the slope of declining ASC against increasing node density is only determined by the path loss exponent.

REFERENCES

[1] W. Liu, Z. Ding, T. Ratnarajah *et al.*, "On ergodic secrecy capacity of random wireless networks with protected zones," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6146–6158, Aug. 2016.

[2] D. S. Karas, A.-A. A. Boulogeorgos, G. K. Karagiannidis *et al.*, "Physical layer security in the presence of interference," *IEEE Wireless Commun. Lett.*, vol. 6, no. 6, pp. 802–805, Dec. 2017.

[3] C. Liu, N. Yang, R. Malaney *et al.*, "Artificial-noise-aided transmission in multi-antenna relay wiretap channels with spatially random eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7444–7456, Nov. 2016.

[4] H. Lei, H. Luo, K.-H. Park *et al.*, "Secrecy outage analysis of mixed RF-FSO systems with channel imperfection," *IEEE Photon. J.*, vol. 10, no. 3, pp. 1–13, June 2018.

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

[6] J. Zhu, Y. Chen, Y. Shen *et al.*, "Secrecy transmission capacity in noisy wireless ad hoc networks," *Ad Hoc Netw.*, vol. 21, pp. 123–133, May 2014.

[7] Y. J. Tolossa, S. Vuppala, G. Kaddoum *et al.*, "On the uplink secrecy capacity analysis in D2D-enabled cellular network," *IEEE Systems J.*, vol. 12, no. 3, pp. 2297–2307, Sept. 2018.

[8] M. Kamel, W. Hamouda, and A. Youssef, "Physical layer security in ultra-dense networks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 5, pp. 690–693, Oct. 2017.

[9] F. Jameel, S. Wyne, and I. Krikidis, "Secrecy outage for wireless sensor networks," *IEEE Commun. Lett.*, vol. 21, no. 7, pp. 1565–1568, July 2017.

[10] A. Prudnikov, Y. Brychkov, and O. Marichev, *Integrals and Series. Volume 3: More Special Functions*. New York, USA: Gordon and Breach Sci. Publ., 1986.

[11] A. M. Mathai, R. K. Saxena, and H. J. Haubold, *The H-Function: Theory and Applications*. New York, USA: Springer, 2009.

[12] H. Lei, I. S. Ansari, G. Pan *et al.*, "Secrecy capacity analysis over α–μ fading channels," *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1445–1448, Jan. 2017.

[13] S. N. Chiu, D. Stoyan, W. S. Kendall *et al.*, *Stochastic Geometry and Its Applications*. West Sussex, UK: John Wiley & Sons, 2013.

[14] Y. Ai, M. Cheffena, A. Mathur *et al.*, "On physical layer security of double Rayleigh fading channels for vehicular communications," *IEEE Wireless Commun. Lett.*, vol. 7, no. 6, pp. 1038–1041, Dec. 2018.

[15] Y. Ai and M. Cheffena, "On multi-hop decode-and-forward cooperative relaying for industrial wireless sensor networks," *Sensors*, vol. 17, no. 4, p. 695, 2017.

[16] M. Haenggi and R. K. Ganti, "Interference in large wireless networks," *Foundations and Trends® in Networking*, vol. 3, no. 2, pp. 127–248, Nov. 2009.

[17] A. Mathur, Y. Ai, M. R. Bhatnagar *et al.*, "On physical layer security of α-η-κ-μ fading channels," *IEEE Commun. Lett.*, vol. 22, no. 10, pp. 2168–2171, Oct. 2018.

[18] Y. Ai, A. Mathur, M. Cheffena *et al.*, "Physical layer security of hybrid satellite-FSO cooperative systems," *IEEE Photon. J.*, vol. 11, no. 1, Feb. 2019.

[19] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Burlington, MA, USA: Academic Press, 2007.

[20] A. A. Kilbas and M. Saigo, "On the H-function," *J. Appl. Math. Stoch. Anal.*, vol. 12, no. 2, pp. 191–204, Sept. 1999.

[21] G. Pan, H. Lei, Y. Deng *et al.*, "On secrecy performance of MISO SWIPT systems with TAS and imperfect CSI," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3831–3843, Sept. 2016.

[22] P. Mittal and K. Gupta, "An integral involving generalized function of two variables," in *Proc. Indian Acad. Sci.*, vol. 75, no. 3, Mar. 1972, pp. 117–123.