sensors

Article

On Performance Analysis of Protective Jamming Schemes in Wireless Sensor Networks

Xuran Li [1], Hong-Ning Dai [1,*], Hao Wang [2] and Hong Xiao [3]

[1] Faculty of Information Technology, Macau University of Science and Technology, Macau, China; 1509853dii30001@student.must.edu.mo

[2] Big Data Lab, Norwegian University of Science and Technology in Aalesund, 6009 Aalesund, Norway; hawa@ntnu.no

[3] Faculty of Computer, Guangdong University of Technology, Guangzhou 510006, China; wh_red@gdut.edu.cn

* Correspondence: hndai@ieee.org; Tel.: +853-8897-2154

Academic Editors: Mianxiong Dong, Zhi Liu, Anfeng Liu and Didier El Baz
Received: 31 October 2016; Accepted: 20 November 2016; Published: 24 November 2016

Abstract: Wireless sensor networks (WSNs) play an important role in Cyber Physical Social Sensing (CPSS) systems. An eavesdropping attack is one of the most serious threats to WSNs since it is a prerequisite for other malicious attacks. In this paper, we propose a novel anti-eavesdropping mechanism by introducing friendly jammers to wireless sensor networks (WSNs). In particular, we establish a theoretical framework to evaluate the eavesdropping risk of WSNs with friendly jammers and that of WSNs without jammers. Our theoretical model takes into account various channel conditions such as the path loss and Rayleigh fading, the placement schemes of jammers and the power controlling schemes of jammers. Extensive results show that using jammers in WSNs can effectively reduce the eavesdropping risk. Besides, our results also show that the appropriate placement of jammers and the proper assignment of emitting power of jammers can not only mitigate the eavesdropping risk but also may have no significant impairment to the legitimate communications.

Keywords: security; wireless sensor networks; friendly jamming; analysis

1. Introduction

Cyber Physical Social Sensing (CPSS) has emerged as a promising paradigm to enable the interactions between humans and the physical environment [1–4]. As a key component of CPSS systems, wireless sensor networks (WSNs) play an important role in sensing, collecting and transmitting confidential information [5,6]. However, WSNs are also susceptible to various malicious attacks due to the vulnerability of sensor nodes [7]. *Eavesdropping* attack, as one of typical malicious attacks in WSNs has attracted considerable attention recently. It is difficult to detect eavesdropping behaviours since *malicious* nodes (also called eavesdroppers) passively wiretap the confidential information without disclosure of their existence.

Encryption has been typically used to protect the confidential communications in wireless networks. For example, Cellular Message Encryption Algorithm has been used in cellular networks [8] and KASUMI has been used in 3G networks [9] while wireless local area networks (WLANs) have adopted Wired Equivalent Privacy (WEP) [10], Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) [11]. However, the traditional cryptographic methods may not be feasible to WSNs due to the following constraints: (1) the limited battery power of sensor nodes; (2) the inferior computational capability of sensor nodes and (3) the difficulty of managing distributed sensor nodes in a centralized way, which is however necessary for many encryption algorithms [12].

In this paper, we propose a novel anti-eavesdropping mechanism to protect confidential communications in WSNs. In particular, we deploy a small number of *friendly jammers* in WSNs, which can generate sufficient interference to prevent eavesdroppers from snooping legitimate communications. We name such schemes as Friendly-Jamming (Fri-Jam) schemes. Recently, [13–17] also proposed a similar approach named *Protective Jamming* (Pro-Jam) to prohibit the eavesdropping attacks in RFID-like networks. However, Pro-Jam is mainly designed for the environment with a fence at the boundary of the network, where jammers are placed outside the fence. This assumption is impractical to WSNs since eavesdroppers can appear at any location in WSNs. Besides, most of the study on Pro-Jam scheme have been focused on the power assignment in a specific scenario. To the best of our knowledge, *there is a lack of performance analysis on friendly-jamming schemes*.

In this paper, we establish a general analytical model to evaluate the performance of Fri-Jam schemes. The primary contributions of this paper can be summarized as follows.

- In particular, we propose a general theoretical model to quantify the eavesdropping risk (measured by the eavesdropping probability) and evaluate the impact of Fri-Jam schemes on the legitimate communications (measured by the transmission probability).
- We consider three types of Fri-Jam schemes: random placement of jammers (named FJ-Ran scheme), regular placement of jammers (named FJ-Reg scheme) and FJ-Reg scheme with power control (named FJ-PC scheme).
- We compare the eavesdropping probability of WSNs without jammers with that with friendly jammers (FJ-Ran, FJ-Reg and FJ-PC schemes). We find that all of three Fri-Jam schemes can effectively reduce the eavesdropping probability in contrast to no-jamming scenarios.
- Our results also show that the appropriate placement of friendly jammers in WSNs can significantly reduce the eavesdropping probability whilst there is no significant impairment on legitimate communications. Besides, to adjust emitting power of jammers properly can mitigate the eavesdropping risk while has no significant impairment to the legitimate transmission.

The rest of this paper is organized as follows. We summarize the related works in Section 2. Section 3 introduces the models used in this paper. We then analyze the eavesdropping probability of different Fri-Jam schemes in Section 4. We next show the results in Section 5. Finally, Section 6 concludes this paper.

2. Related Work

It is difficult to detect eavesdropping attacks in WSNs since eavesdroppers passively snoop the confidential communications with concealment of their presence. Encryption is one of the most commonly used techniques to protect confidential communications, which is shown to work effectively in WLANs (e.g., WEP [10], WPA and WPA2 [11]), in cellular networks (e.g., CMEA [8] and KASUMI [9]) and in wireless personal area networks (WPANs) [18]. However, applying such cryptography-based techniques help hiding the meaning of the information being transmitted, but not the existence of the information itself. In addition, the techniques are designed to make it computationally difficult for the adversary to understand the true meaning of the information while the adversary is still able to access all the information [19]. Furthermore, it is quite challenging to apply the conventional ciphers (encryption algorithms) to WSNs due to the following inherent constraints of WSNs [12]: (a) the inferior computational capability of wireless nodes; (b) the limited battery power of wireless nodes; (c) the difficulty of managing the distributed sensor nodes in the centralized manner. In addition, the cryptographic authentication and identification in higher layer will introduce a significant computational overhead [20].

There are a number of anti-eavesdropping counter-measures in WSNs. We roughly categorize them into three types: (i) lightweight encryption schemes [21–24]; (ii) generating artificial noise to limit the amount of information that can be extracted by eavesdroppers [25–27]; and (iii) mitigating the eavesdropping risk by controlling the transmitting power [28]. Table 1 summarizes these schemes.

In particular, a number of lightweight encryption schemes based on physical layer features of wireless networks have been proposed [21–24]. The main idea of physical-layer encryption schemes is to exploit the inherent randomness of communication channels so that the amount of information that can be extracted by an eavesdropper is mitigated. However, the encryption schemes are still computational intensive and power-consuming.

Table 1. Comparison of related anti-eavesdropping schemes in WSNs.

	Encryption	**Artificial Noise**	**Power Control**
References	[8–11,18,21–24]	[25–27]	[28]
Limitations	computational intensive and power consuming	too specific (only apply for some specific scenarios)	deteriorate legitimate communications

Some recent studies [25,27] exploit the artificial noise generated by RFID readers to alleviate the eavesdropping capability of malicious nodes. However, these schemes can only be applied to the scenarios of Internet-of-Things (IoT) based on RFID. Besides, a transmitting power control method is proposed in [28] to mitigate the eavesdropping risk while to adjust the transmitting power may deteriorate the legitimate communications [29].

Although [15–17] also proposed an approach similar to our Fri-Jam schemes, their methods are mainly designed for the IoT scenario, in which jammers are placed outside the fence surrounding the boundary of the network. These schemes are not feasible to WSNs since eavesdroppers can appear at any location in WSNs. Besides, most of the studies on protective jamming schemes [15–17] are mainly focused on a specific scenario.

3. System Models

This section first presents three kinds of Fri-Jam schemes in Section 3.1. Then, Section 3.2 gives the channel model used in this paper. Section 3.3 presents the definitions on eavesdropping probability and transmission probability.

3.1. Fri-Jam Schemes

In this paper, we assume that the network is placed in a torus [30]. In this manner, the border effect can be ignored. We consider three types of users in our network: legitimate users, eavesdroppers and friendly jammers. The legitimate users are distributed according to homogeneous Poisson point process (PPP). Legitimate users transmit data packets, which might be passively snooped by eavesdroppers while legitimate users are unaware of the reconnaissance. Similar to [28], we assume that the eavesdropper is located at the center of the network without loss of generality since the network is placed in a symmetric torus.

The interference caused by friendly jammers heavily depends on the location of jammers and the emitting power of each jammer. In this paper, we consider two placement strategies of friendly jammers in WSNs: (i) FJ-Reg scheme, in which jammers are regularly placed at deterministic locations and (ii) FJ-Ran scheme, in which jammers are regularly placed at random locations. Specifically, in the FJ-Reg scheme, friendly jammers are regularly placed in a grid manner, as shown in Figure 1. In the FJ-Ran scheme, friendly jammers are randomly distributed according to according to PPP, as shown in Figure 2. In addition to FJ-Reg and FJ-Ran schemes, we also consider adjusting the emitting power of jammers. In particular, we consider a modified FJ-Reg scheme with power control (named FJ-PC scheme) in this paper.

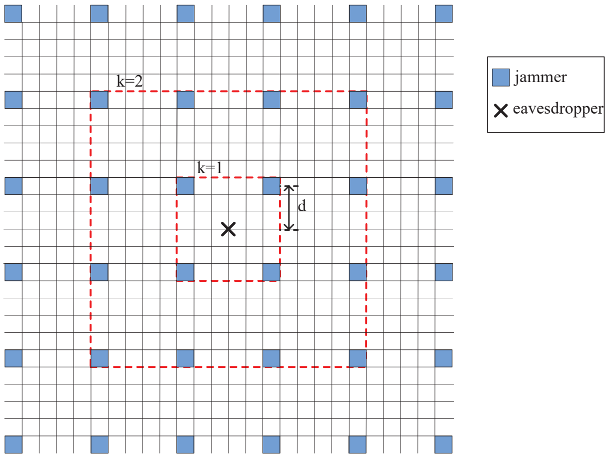


Figure 1. FJ-Reg Scheme: every jammer is placed at a gray square. Note that we only show a part of the whole network.

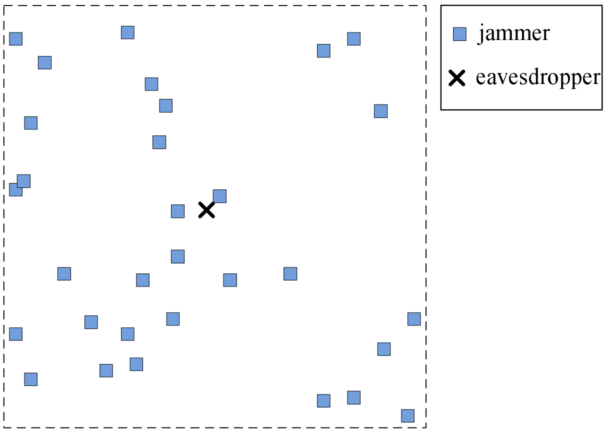


Figure 2. FJ-Ran Scheme: every jammer is randomly placed according to homogeneous Poisson Point Process (PPP). Note that we only show a part of the whole network.

3.2. Channel Model

We assume that the radio channel experiences Rayleigh fading and path loss. The received power of a receiver (i.e., a legitimate user or an eavesdropper) at a distance r from its nearest transmitter (legitimate user or friendly jammer) is $hr^{-\alpha}$, where h is a random variable following an exponential distribution with mean $\frac{1}{\mu}$ and α is the path loss factor. More specifically, we denote $h \sim \exp(\mu)$.

We then consider the *Signal to Interference plus Noise Ratio* (SINR) model. The SINR of the receiver at a random distance r from its transmitter is expressed as

$$\text{SINR} = \frac{P_t h r^{-\alpha}}{\sigma^2 + I_t + I_j}, \tag{1}$$

where σ^2 is the noise power, $I_t = \sum\limits_{i \in \Phi / t_0} P_t h_i R_i^{-\alpha}$ denotes the cumulative interference from all the legitimate users except for the transmitter denoted by t_0, Φ denotes the set of legitimate users, P_t denotes the transmitting power of the legitimate transmitter and I_j denotes the cumulative interference generated by friendly jammers. The value of I_j heavily depends on the placements of friendly jammers, which will be analyzed in Section 4.

We then define the *eavesdropping condition* to determine whether the transmission from a certain legitimate user can be wiretapped by an eavesdropper.

Definition 1. *Eavesdropping Condition. A confidential transmission can be snooped by an eavesdropper if and only if* SINR $> T$*, where* T *is the received power threshold that an eavesdropper can successfully decode the transmission.*

3.3. Problem Definition

Based on the eavesdropping condition, we then define the *eavesdropping probability* denoted by $P(E)$ as follows.

Definition 2. *Eavesdropping Probability is the probability that at least one transmission has been wiretapped by an eavesdropper.*

From the definition we know $P(E)$ is the probability to show how likely is any transmission eavesdropped. In order to derive $P(E)$, we need to calculate the probability that one transmission has been eavesdropped, which is denoted by P_e. Considering the situation that no transmission being eavesdropped will be easier than considering all the situations that a certain number of transmissions being eavesdropped. Then, we find that $P(E)$ can be expressed by P_e as follows,

$$P(E) = 1 - (1 - P_e)^N, \tag{2}$$

where N is the expected number of legitimate users in the network.

Another concern of this paper is to investigate the impacts of our Fri-Jam schemes on the legitimate communications. Thus, we define the transmission probability denoted by $P(C)$ as follows.

Definition 3. *Transmission Probability is the probability that a legitimate user (transmitter) can successfully transmit with another legitimate user (receiver).*

To ensure the legitimate transmission, we require SINR $> \beta$ at the legitimate receiver, where β is the threshold value of the receiving power for a successful reception. Thus, we have $P(C) \overset{\Delta}{=} P(\text{SINR} > \beta)$. Following a similar approach to [31], we can obtain $P(C)$.

4. Analysis on Eavesdropping Probability

We first present the analytical results on the eavesdropping probability of Non-Jam scheme in Section 4.1 and then present the results on the eavesdropping probability of Fri-Jam schemes in Section 4.2.

4.1. Analysis of Non-Jam Scheme

According to the definition of the eavesdropping probability $P(E)$, we need to derive the probability P_e that one transmission has been eavesdropped first. In particular, we have P_e of Non-Jam scheme as follows.

Theorem 1. *In Non-Jam scheme, the eavesdropping probability* P_e *that one transmission has been eavesdropped is*

$$P_e = \int\limits_{r>0} e^{-\mu T_p r^{\alpha} \sigma^2 - \pi r^2 \lambda(\rho(T,\alpha)+1)} 2\pi\lambda r dr, \tag{3}$$

where $\rho(T_p,\alpha) = T_p^{-2/\alpha} \int_{T_p^{-2/\alpha}}^{\infty} \frac{1}{1+\mu^{\alpha/2}} d\mu$ *and* $T_p = \frac{T}{Pt}$ *for simplicity.*

Proof. We denote the distance between the eavesdropper and its nearest transmitter by r. Since the transmitters are distributed according to PPP, the probability density function (PDF) of r can be derived as the following steps.

Firstly, we have the probability that no transmitter is closer than R given by

$$P[r > R] = P[\text{No transmitter closer than } R] = e^{-\lambda\pi R^2}.$$

Then, the cumulative distribution function (CDF) of r is $P[r \leq R] = F_R(R) = 1 - e^{-\lambda\pi R^2}$. We next have the PDF of r as follows,

$$f_r(r) = \frac{dF_r(r)}{dr} = e^{-\lambda\pi r^2} 2\pi\lambda r.$$

Since the channel gain is h, the SINR at eavesdropper is

$$\text{SINR} = \frac{P_t h r^{-\alpha}}{\sigma^2 + I_t}, \tag{4}$$

where $I_t = \sum\limits_{i\in\Phi/t_0} P_t h_i R_i^{-\alpha}$.

Then, the eavesdropping probability P_e that one transmission has been eavesdropped is

$$\begin{aligned} P_e &= E_r[P(\text{SINR} > T|r)] \\ &= \int\limits_{r>0} P\left[\frac{P_t h r^{-\alpha}}{\sigma^2 + I_t} > T|r\right] e^{-\lambda\pi r^2} 2\pi\lambda r dr \\ &= \int\limits_{r>0} P[h > T_p r^{\alpha}(\sigma^2 + I_t)|r] e^{-\lambda\pi r^2} 2\pi\lambda r dr. \end{aligned} \tag{5}$$

Since h is a random variable following an exponential distribution with mean $\frac{1}{\mu}$, the probability becomes

$$\begin{aligned} P[h > T_p r^{\alpha}(\sigma^2 + I_t)|r] &= E_{I_t}[P[h > T_p r^{\alpha}(\sigma^2 + I_t)|r]] \\ &= E_{I_t}[\exp[-\mu T_p r^{\alpha}(\sigma^2 + I_t)]|r] \\ &= e^{-\mu T_p r^{\alpha}\sigma^2} \cdot E_{I_t}[\exp(-\mu T_p r^{\alpha} I_t)] \\ &= e^{-\mu T_p r^{\alpha}\sigma^2} \cdot L(\mu T_p r^{\alpha}), \end{aligned} \tag{6}$$

where $L(\cdot)$ denotes the Laplace transform.

More specifically, we have

$$\begin{aligned} L_{I_t}(s) &= E_{I_t}[e^{-sI_t}] \\ &= E_{\Phi,\{h_i\}}\left[\exp(-s \sum_{i\in\Phi/b_0} h_i R_i^{-\alpha})\right] \\ &= E_{\Phi}\left[\prod_{i\in\Phi/b_0} \frac{\mu}{\mu + sR_i^{-\alpha}}\right] \\ &= \exp\left(-2\pi\lambda \int_r^{\infty} (1 - \frac{\mu}{\mu + sv^{-\alpha}}) v dv\right). \end{aligned}$$

Replacing variable μ with $(\frac{v}{r{T_p}^{1/\alpha}})^2$, we then have

$$L[\mu T_p r^{\alpha}] = \exp(-\pi r^2 \lambda \rho(T_p, \alpha)), \tag{7}$$

where $\rho(T_p, \alpha) = T_p^{-2/\alpha} \int_{T_p^{-2/\alpha}}^{\infty} \frac{1}{1+\mu^{\alpha/2}} d\mu$. □

It is shown in Theorem 1 that the eavesdropping probability P_e heavily depends on the channel conditions (such as the path loss and Rayleigh fading).

4.2. Analysis of Fri-Jam Schemes

Recall that we consider three Fri-Jam schemes: FJ-Reg, FJ-Ran and FJ-PC schemes. Thus, we categorize our analysis into the following cases.

4.2.1. Case I: FJ-Reg Scheme

We first analyze the case of FJ-Reg, in which all the jammers are regularly placed in grid manner as shown in Figure 1. We denote the expectation of the cumulative interference generated by jammers by $E[I_j]$, which is given by Lemma 1.

Lemma 1. *The expectation of the cumulative interference of regular placed jammers is*

$$E[I_j] = \frac{1}{\mu} \sum_{m=1}^{n} E[I_j(m)]. \tag{8}$$

We present the proof in Appendix A.

We then derive the probability P_e that one transmission has been eavesdropped, which is given by Theorem 2.

Theorem 2. *In FJ-Reg scheme, the probability P_e that one transmission has been eavesdropped is*

$$P_e = \int\limits_{r>0} e^{-\mu T_p r^{\alpha}(\sigma^2 + E[I_j]) - \pi r^2 \lambda(\rho(T_p,\alpha)+1)} 2\pi\lambda r dr, \tag{9}$$

where $\rho(T_p, \alpha) = T_p^{-2/\alpha} \int_{T_p^{-2/\alpha}}^{\infty} \frac{1}{1+\mu^{\alpha/2}} d\mu$ and $E[I_j]$ is given by Equation (8).

Proof. First, the SINR at a random distance r from its nearest transmitter can be expressed as $\text{SINR} = \frac{hr^{-\alpha}}{\sigma^2 + I_t + I_j}$. Then, from the definition of P_e, we have

$$\begin{aligned} P_e &= \int\limits_{r>0} P\left[\frac{hr^{-\alpha}}{\sigma^2 + I_t + I_j} > T_p|r\right] e^{-\lambda\pi r^2} 2\pi\lambda r dr \\ &= \int\limits_{r>0} P[h > T_p r^{\alpha}(\sigma^2 + I_t + I_j)|r] e^{-\lambda\pi R^2} 2\pi\lambda r dr. \end{aligned}$$

According to the channel model (given in Section 3.2), we have

$$\begin{aligned} & P[h > T_p r^{\alpha}(\sigma^2 + I_t + I_j)|r] \\ & \quad = E_{I_t}[\exp(-\mu T_p r^{\alpha})(\sigma^2 + I_t + I_j)|r] \\ & \quad = e^{-\mu T_p r^{\alpha}(\sigma^2 + E[I_j])} \cdot E_{I_t}[\exp(-\mu T_p r^{\alpha} I_t)] \\ & \quad = e^{-\mu T_p r^{\alpha}(\sigma^2 + E[I_j])} \cdot L(\mu T_p r^{\alpha}), \end{aligned}$$

where $L(\mu T_p r^{\alpha}) = \exp(-\pi r^2 \lambda \rho(T_p, \alpha))$, $\rho(T_p, \alpha) = T_p^{-2/\alpha} \int_{T_p}^{\infty} \frac{1}{1+(\mu)^{\alpha/2}} d\mu$ and $E[I_j]$ is given by Equation (8). □

It is shown in Theorem 2 that the probability P_e heavily depends on the path loss factor α, the Rayleigh fading factor μ, the noise σ and the placement parameter d. Section 5 will give the numerical results that will further confirm this observation.

4.2.2. Case II: FJ-Ran Scheme

We then analyze the case of FJ-Ran, in which all the jammers are randomly distributed in the network. Recall that both jammers and legitimate users are distributed according to PPP while they have the different distribution parameters. In particular, we denote the density of legitimate users by λ_1 and the density of friendly jammers by λ_2. Based on the well-known stochastic geometric results [31], we can obtain Theorem 3 on the probability P_e that one transmission has been eavesdropped as follows.

Theorem 3. *In FJ-Ran scheme, the probability P_e that one transmission has been eavesdropped is*

$$P_e = \int\limits_{r>0} e^{-\mu T_p r^\alpha \sigma^2} \cdot L_{I_t}(\mu T_p r^\alpha) \cdot L_{I_j}(\mu T_p r^\alpha) e^{-\lambda_1 \pi R^2} 2\pi\lambda_1 r dr,$$

where $L_{I_t}[\mu T_p r^\alpha] = \exp(-\pi r^2 \lambda_1 \rho(T_p, \alpha))$, $L_{I_j}[\mu T_p r^\alpha] = \exp(-\pi r^2 \lambda_2 \rho(T_p, \alpha))$ *and* $\rho(T_p, \alpha) = T_p^{-2/\alpha} \int_{T_p^{-2/\alpha}}^{\infty} \frac{1}{1+\mu^{\alpha/2}} d\mu$.

Proof. According to the channel model defined in Section 3.2, we have the

$$\begin{aligned} P_e &= \int\limits_{r>0} P\left[\frac{P_t h r^{-\alpha}}{\sigma^2 + I_t + I_j} > T|r\right] e^{-\lambda \pi r^2} 2\pi\lambda r dr \\ &= \int\limits_{r>0} P[h > T_p r^\alpha(\sigma^2 + I_t + I_j)|r] e^{-\lambda_1 \pi R^2} 2\pi\lambda_1 r dr. \end{aligned} \tag{10}$$

Following the similar analysis procedure to [31], we then have

$$P[h > T_p r^\alpha(\sigma^2 + I_t + I_j)|r] = e^{-\mu T_p r^\alpha \sigma^2} \cdot L_{I_t}(\mu T_p r^\alpha) \cdot L_{I_j}(\mu T_p r^\alpha). \tag{11}$$

Substituting $P[h > T_p r^\alpha(\sigma^2 + I_t + I_j)|r]$ in Equation (10) by RHS of Equation (11), we finally prove the above result. □

It is shown in Theorem 3 that the probability P_e heavily depends on both the node density λ_1 of legitimate users and the node density λ_2 of jammers, and the channel conditions.

4.2.3. Case III: FJ-PC Scheme

We next analyze the case of FJ-PC scheme, in which jammers are placed in grid as the same as FJ-Reg scheme. We then assign the emitting power of jammers according to the different layers (as shown in Figure 1). We denote the layer number by k, which is ranging from 1 to n. The emitting power of jammers at the same layer is assigned with the same value. Specifically, we assign the emitting power at jammers in FJ-Reg scheme according to the following rule.

Property 1. *We assign the emitting power of jammers at the kth layer according to the following equation:*

$$P_j(k) = P_J \cdot \zeta^{1-k}, \tag{12}$$

where P_J is the transmitting power of the jammers at the first layer and ζ is the power control factor.

In FJ-PC scheme, the transmission probability of a legitimate user cannot be derived directly by using the existing approaches in [31–34] since the cumulative interference from jammers in FJ-PC scheme is quite different from that in FJ-Reg scheme. In particular, we have the following lemma to calculate the average cumulative interference.

Lemma 2. *In FJ-PC scheme, the average cumulative interference from power controlled jammers to a legitimate transmitter is*

$$E[I_c] = \frac{\sum\limits_{k=1}^{n}\left(I_{k,t_0} + I_{k,t_k} + 2\sum\limits_{t=t_1}^{t_{k-1}} I_{k,t_x}\right)}{\sum\limits_{k=1}^{n} 2k}, \tag{13}$$

where I_{k,t_x} is the interference at t_x, which can be calculated by

$$\begin{aligned}
I_{k,t_x} = {} & \sum_{m=1}^{k}\sum_{v=1}^{m}\left(2P_j(m)\left(\sqrt{\left[\left(v-\frac{1}{2}+t_x\right)\cdot 2d\right]^2+\left[\left(k-m+\frac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha}\right.\right.\\
& \left.\left.+\sqrt{\left[\left(v-\frac{1}{2}+t_x\right)\cdot 2d\right]^2+\left[\left(k+m-\frac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha}\right)\right)\\
& +\sum_{m=1}^{k}\sum_{w=k-m+1}^{k+m} 2P_j(m)\sqrt{\left[\left(m-\frac{1}{2}+t_x\right)\cdot 2d\right]^2+\left[\left(w-\frac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha}\\
& +\sum_{q=k}^{n}\sum_{z=q-k-1}^{q+k} 2P_j(q)\sqrt{\left[\left(q-\frac{1}{2}+t_x\right)\cdot 2d\right]^2+\left[\left(z+\frac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha}\\
& +\sum_{q=k}^{n}\sum_{s=1}^{q}\left(2P_j(q)\left(\sqrt{\left[\left(s-\frac{1}{2}+t_x\right)\cdot 2d\right]^2+\left[\left(q-k-\frac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha}\right.\right.\\
& \left.\left.+\sqrt{\left(\left(s-\frac{1}{2}+t_x\right)\cdot 2d\right)^2+\left[\left(q+k+\frac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha}\right)\right)
\end{aligned} \tag{14}$$

We present the proof in Appendix B.

We then derive the transmission probability $P(C)$ of a legitimate user, which is given by Theorem 4.

Theorem 4. *In FJ-PC scheme, the transmission probability $P(C)$ is*

$$P(C) = \int\limits_{r>0} e^{-\mu\beta_p r^{\alpha}(\sigma^2+E[I_c])-\pi r^2\lambda(\rho(\beta_p,\alpha)+1)} 2\pi\lambda r dr, \tag{15}$$

where $\rho(\beta_p,\alpha) = {\beta_p}^{-2/\alpha}\int_{{\beta_p}^{-2/\alpha}}^{\infty}\frac{1}{1+\mu^{\alpha/2}}d\mu$, $\beta_p = \frac{\beta}{Pt}$ and $E[I_c]$ is given by Equation (13).

Proof. The SINR of the receiver at a random distance r from its nearest transmitter can be expressed as $\text{SINR} = \frac{P_t h r^{-\alpha}}{\sigma^2+I_t+I_c}$, where I_c is the cumulative interference caused by power controlled jammers on the recevier. Then, from the definition of $P(C)$, we have

$$\begin{aligned}
P(C) &= \int\limits_{r>0} P\left[\frac{P_t h r^{-\alpha}}{\sigma^2+I_t+I_c} > \beta|r\right] e^{-\lambda\pi r^2} 2\pi\lambda r dr\\
&= \int\limits_{r>0} P[h > \beta_p r^{\alpha}(\sigma^2+I_t+I_c)|r] e^{-\lambda\pi R^2} 2\pi\lambda r dr.
\end{aligned}$$

According to the channel model (given in Section 3.2), we have

$$\begin{aligned}
&P[h > \beta_p r^\alpha(\sigma^2 + I_t + I_c)|r] \\
&= E_{I_t}[\exp(-\mu\beta_p r^\alpha)(\sigma^2 + I_t + I_c)|r] \\
&= e^{-\mu\beta_p r^\alpha(\sigma^2+E[I_c])} \cdot E_{I_t}[\exp(-\mu\beta_p r^\alpha I_t)] \\
&= e^{-\mu\beta_p r^\alpha(\sigma^2+E[I_c])} \cdot L(\mu\beta_p r^\alpha),
\end{aligned}$$

where $L(\mu\beta_p r^\alpha) = \exp(-\pi r^2\lambda\rho(\beta_p,\alpha))$, $\rho(\beta_p,\alpha) = \beta_p{}^{-2/\alpha}\int_{\beta_p}^{\infty}\frac{1}{1+(\mu)^{\alpha/2}}d\mu$ and $E[I_j]$ is given by Equation (8). □

We then have the eavesdropping probability P_e in FJ-PC scheme as the following theorem.

Theorem 5. *In FJ-PC scheme, the eavesdropping probability P_e that one transmission has been eavesdropped is*

$$P_e = \int\limits_{r>0} e^{-\mu T_p r^\alpha(\sigma^2+E[I_j{}'])-\pi r^2\lambda(\rho(T_p,\alpha)+1)}2\pi\lambda r dr, \tag{16}$$

where $E[I_j{}'] = E\left[4\sum_{k=1}^{n}P_j(k)\left(2\left(d\cdot\sqrt{(2k-3)^2+(2k-1)^2}\right)^{-\alpha}+\left(d\cdot\sqrt{2(2k-1)^2}\right)^{-\alpha}\right)\right]$.

Proof. The derivation of eavesdropping probability P_e in FJ-PC scheme is similar to the derivation of Equation (15) in Theorem 4 and the main difference is the cumulative interference from jammers. In particular, the calculation of interference from nth layer jammers in FJ-PC scheme I_j' is similar to Equation (A3) in Appendix A, which is shown in the following equation:

$$\begin{aligned}
I_j(n)' \quad = \quad & 4\sum_{k=1}^{n}P_j(k)\left\{2\left(d\cdot\sqrt{(2k-3)^2+(2k-1)^2}\right)^{-\alpha}\right. \\
& \left.+\left(d\cdot\sqrt{2(2k-1)^2}\right)^{-\alpha}\right\}.
\end{aligned} \tag{17}$$

Then we have the averaged cumulative interference from all the jammers as follows,

$$E[I_j{}'] = E[\sum_{m=1}^{n} I_j(m)'].$$

□

According to the definition of the probability of eavesdropping attack $P(E)$, we have

$$P(E) = 1-(1-P_e)^N,$$

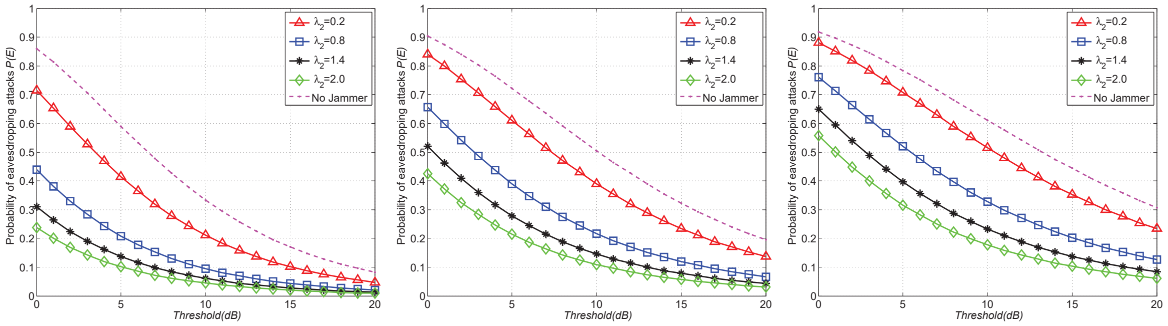
where P_e can be replaced by the different values as specified in Non-Jam scheme, FJ-Reg scheme, FJ-Ran scheme and FJ-PC Scheme, which can be obtained by Theorem 1, Theorem 2, Theorem 3 and Theorem 5, respectively. In the next section, we will present numerical results of $P(E)$ based on the above schemes.

5. Numerical Results

In this section, we first present the numerical results of the probability of eavesdropping attacks $P(E)$ with comparisons among different schemes in Section 5.1. Then we will show the impacts of friendly jammers on the legitimate communications in Section 5.2.

5.1. Comparisons of Different Schemes

In the first set of results, we compare the probability of eavesdropping attacks $P(E)$ of FJ-Ran scheme with that of Non-Jam scheme. Note that the larger node density λ_2 in FJ-Ran scheme and the smaller d in FJ-Reg scheme imply the higher cost (i.e., more jammers are deployed in the network). As shown in Figure 3, the results of Non-Jam scheme are shown in a dash curve and the results of FJ-Ran scheme are shown in solid curves with markers, where we choose the different values of node density λ_2 of friendly jammers (ranging from 0.2 to 2.0) and the value of node density λ_1 of legitimate user is 0.5. It is shown in Figure 3 that the Non-Jam scheme always has higher values of $P(E)$ than the FJ-Ran scheme, implying that *using friendly jammers in WSN can effectively reduce the probability of eavesdropping attacks*.



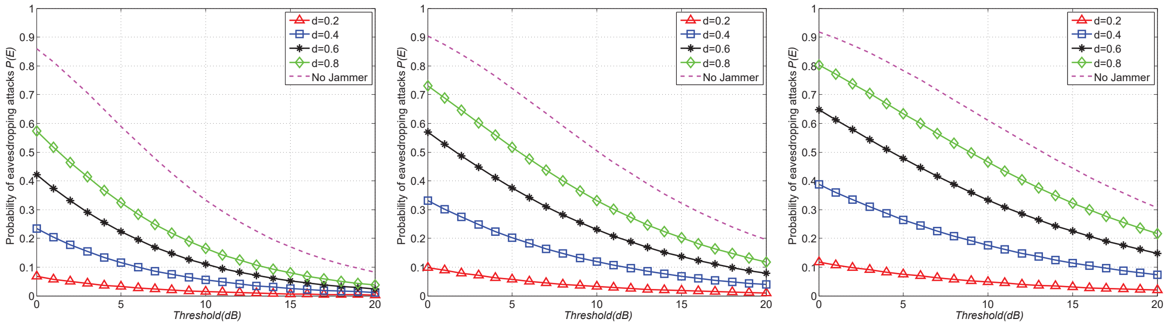
(a) $\alpha = 3$ (b) $\alpha = 4$ (c) $\alpha = 5$

Figure 3. Probability of eavesdropping attacks $P(E)$ with FJ-Ran scheme (PPP) versus Non-Jam scheme when $\alpha = 3, 4, 5$ with SINR threshold T ranging from 0 dB to 20 dB.

It is also shown in Figure 3 that the probability of eavesdropping attacks $P(E)$ decreases with the increment of jammers density λ_2, implying that *adding more jammers can further improve the effect of mitigating eavesdropping attacks*. For example, when $\alpha = 4$ and the threshold $T = 5$ dB (as shown in Figure 3b), $P(E)$ of the Non-Jam scheme is 0.719 while $P(E)$ of FJ-Ran scheme is reduced to 0.393 with jammers density $\lambda_2 = 0.8$ and 0.211 with jammers density $\lambda_2 = 2.0$.

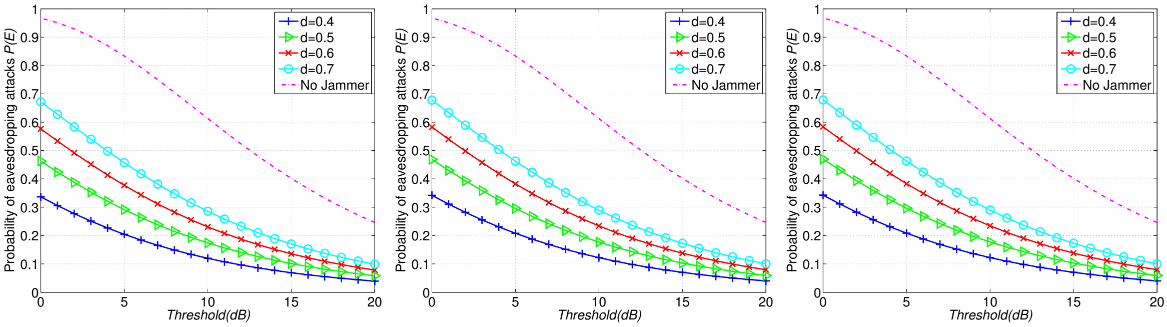
In the second set of results, we compare the probability of eavesdropping attacks $P(E)$ of the FJ-Reg scheme with that of the Non-Jam scheme. Figure 4 shows the results, where a dash curve represents $P(E)$ of the Non-Jam scheme and solid curves with markers depict the results of FJ-Reg scheme. Similar to Figure 3, we find that using friendly jammers can always reduce the eavesdropping probability compared with the Non-Jam scheme. Moreover, it is shown in Figure 4 that the probability of eavesdropping attacks $P(E)$ heavily depends on both the channel conditions and system parameter d. Specifically, it is shown in Figure 4b that the probability of eavesdropping attack $P(E)$ decreases with the decreased values of d. In fact, the d in FJ-Reg scheme plays a similar role to jammer density λ_2 in FJ-Ran scheme. In other words, decreasing d is equivalent to the effect of increasing jammer density λ_2. Take Figure 4b as an example again. When the threshold is $T = 5$ dB and $\alpha = 4$, $P(E)$ of Non-Jam scheme is 0.7176 while $P(E)$ becomes 0.072 with $d = 0.2$, implying that using more friendly jammers can further reduce the eavesdropping probability.

In the third set of results, we compare the probability of eavesdropping attacks $P(E)$ of FJ-PC scheme with that of Non-Jam scheme. Figure 5 shows the results, where a dash curve represents $P(E)$ of Non-Jam scheme and solid curves with markers depict the results of FJ-PC scheme. Similar to Figures 3 and 4, we find that using friendly jammers can always reduce the eavesdropping probability compared with the Non-Jam scheme. Furthermore, we also find that the FJ-PC scheme can further reduce the eavesdropping probability compared with FJ-Reg scheme. This is due to the power assigning strategy in our FJ-PC scheme. In particular, the eavesdropping capability of the eavesdropper is significantly weakened by the jammers in the first layer, which have been assigned with higher power as they are much closer to the eavesdropper than other jammers in other layers. Another benefit of the FJ-PC scheme is that it has less impairment to legitimate communications compared with FJ-Reg and FJ-Ran schemes. The following results will further confirm this observation.



(a) $\alpha = 3$ (b) $\alpha = 4$ (c) $\alpha = 5$

Figure 4. Probability of eavesdropping attacks $P(E)$ with FJ-Reg scheme (Grid) versus Non-Jam scheme when $\alpha = 3, 4, 5$ with SINR threshold T ranging from 0 dB to 20 dB.



(a) $\zeta = 2$ (b) $\zeta = 10$ (c) $\zeta = 20$

Figure 5. Probability of eavesdropping attacks $P(E)$ with FJ-PC scheme versus Non-Jam scheme when $\zeta = 2, 10, 20$ with SINR threshold T ranging from 0 dB to 20 dB.

5.2. Impacts of Friendly Jammers on Legitimate Transmissions

Another concern is to investigate whether friendly jammers will significantly affect the legitimate transmissions. In order to differentiate the effect with jammers and the effect without jammers in terms of the eavesdropping probability and the transmission probability, we define the *eavesdropping deviation* $\mathcal{D}_E$ and the *transmission deviation* $\mathcal{D}_C$ as follows.

Definition 4. *Eavesdropping deviation* $\mathcal{D}_E$ *is equal to the difference between the eavesdropping probability* $P(E)$ *without jammers and the eavesdropping probability* $P(E)$ *with jammers.*

Definition 5. *Transmission deviation* $\mathcal{D}_C$ *is equal to the difference between the transmission probability* $P(C)$ *without jammers and the transmission probability* $P(C)$ *with jammers.*

We then derive the eavesdropping deviation $\mathcal{D}_E$ and the transmission deviation $\mathcal{D}_C$ in the first case of comparing FJ-Ran scheme with Non-Jam scheme. In particular, we have $\mathcal{D}_E(\text{Ran}) = P_{\text{Non-Jam}}(E) - P_{\text{FJ-Ran}}(E)$, where $P_{\text{Non-Jam}}(E)$ denotes the eavesdropping probability of Non-Jam scheme and $P_{\text{FJ-Ran}}(E)$ denotes the eavesdropping probability of FJ-Ran scheme. Besides, we have $\mathcal{D}_C(\text{Ran}) = P_{\text{Non-Jam}}(C) - P_{\text{FJ-Ran}}(C)$, where $P_{\text{Non-Jam}}(C)$ denotes the transmission probability of Non-Jam scheme and $P_{\text{FJ}-\text{Ran}}(C)$ denotes the transmission probability of FJ-Ran scheme. Note that $P(C)$ can be calculated by [31] and we omit the detailed derivations in this paper.

Table 2 shows the comparison results. As shown in Table 2, the eavesdropping deviation is much larger than the transmission deviation at the same network settings, implying that *using jammers in WSNs will not significantly affect the legitimate communications* compared with the reductions on the eavesdropping probability. For example, when $\lambda_2 = 2.0$, $\mathcal{D}_E = 0.5178$ while there is less than 0.1 reduction on the transmission probability (i.e., $\mathcal{D}_C = 0.0963$).

Similarly, we derive the eavesdropping deviation $\mathcal{D}_E$ and the transmission deviation $\mathcal{D}_C$ in the second case of comparing FJ-Reg scheme with Non-Jam scheme. Table 3 shows the comparison results. It is shown in Table 3 that FJ-Reg scheme can also significantly reduce the eavesdropping probability with only minor influence on the legitimate transmissions (e.g., the reduction of $P(E)$ is 0.6650 while the reduction of $P(C)$ is only 0.1143 when $d = 0.2$).

We next derive the eavesdropping deviation $\mathcal{D}_E$ and the transmission deviation $\mathcal{D}_C$ in the third case of comparing the FJ-PC scheme with the Non-Jam scheme. Table 4 shows the comparison results. It is shown in Table 4 that the FJ-PC scheme can significantly reduce the eavesdropping probability with only minor influence on the legitimate transmissions. For example, the $P(E)$ is 0.6128 and $P(c)$ is 0.1729 in the Non-Jam scheme and they become 0.1770 and 0.1367, respectively when FJ-PC scheme with $d = 0.6$ is applied. At this time, the reduction of $P(E)$ is 61.8% while the reduction of $P(C)$ is only 12.5% when $d = 0.6$ implying that the FJ-PC scheme can significantly reduce the eavesdropping probability while maintaining the minor impairment to the legitimate communications.

Table 2. Eavesdropping deviation and transmission deviation of comparing FJ-Ran scheme with Non-Jam scheme when $T = 10$ dB and $\alpha = 4$.

Density λ_2	**Eavesdropping deviation** $\mathcal{D}_E$**(Ran)**	**Transmission deviation** $\mathcal{D}_C$**(Ran)**
0.2	0.1120	0.0303
0.8	0.3316	0.0718
1.4	0.4470	0.0880
2.0	0.5178	0.0963

Table 3. Eavesdropping deviation and transmission deviation of comparing FJ-Reg scheme with Non-Jam scheme when $T = 10$ dB and $\alpha = 4$.

Distance d	**Eavesdropping deviation** $\mathcal{D}_E$**(Reg)**	**Transmission deviation** $\mathcal{D}_C$**(Reg)**
0.2	0.6650	0.1143
0.4	0.5195	0.0977
0.6	0.3467	0.0742
0.8	0.2054	0.0500

Table 4. Eavesdropping deviation and transmission deviation of comparing FJ-PC scheme with Non-Jam scheme when $T = 10$ dB, $\zeta = 10$ and $\alpha = 4$.

Distance d	**Eavesdropping deviation** $\mathcal{D}_E$**(PC)**	**Transmission deviation** $\mathcal{D}_C$**(PC)**
0.4	0.4909	0.0594
0.5	0.4358	0.0362
0.6	0.3788	0.0217
0.7	0.3234	0.0132

6. Conclusions

Wireless sensor networks (WSNs) are serving as a crucial component in cyber-physical social sensing systems. The security of WSNs has received extensive attention recently. One of the serious security threats in WSNs is eavesdropping attacks. In this paper, a novel anti-eavesdropping scheme has been proposed to alleviate eavesdropping attacks in WSNs. In particular, we deploy a number of friendly jammers that emit artificial noise to mitigate the eavesdropping capability of adversaries. More specifically, we consider three types of jamming schemes, such as regular placement of jammers (FJ-Reg), random placement of jammers (FJ-Ran) and regular placement of jammers with power control (FJ-PC). We establish a theoretical model to evaluate the performance of these jamming schemes. Our results show that to introduce friendly jammers in WSNs can significantly reduce the eavesdropping probability without the significant influence on the legitimate communications with the appropriate placement of jammers and the proper assignment of emitting power of jammers.

Acknowledgments: The work described in this paper was supported by Macao Science and Technology Development Fund under Grant No. 096/2013/A3 and the National Natural Science Foundation of China under Grant No. 61672170. The authors would like to thank Gordon K.-T. Hon for his excellent comments.

Author Contributions: Xuran Li derived the results, conducted the numeral results and wrote the paper. Hong-Ning Dai supervised the work and revised versions. Hao Wang gave valuable suggestions on the motivation of conducting analysis on protective jamming schemes in wireless sensor networks and assisted in revising the paper. Hong Xiao contributed to revising and proofreading of the article.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Proof of Lemma 1. We consider a coordinate system that is centered at the eavesdropper as shown in Figure 1. Since jammers are placed in a grid, each friendly jammer is $2d$ away from its nearest neighbor in the same axis. The transmitting power of each jammer is assumed to be P_J, which is same as the transmitting power of legitimate transmitters. From the channel model defined in Section 3.2, the radio signal received at an eavesdropper experiences both Rayleigh fading and the path loss. We consider the path loss effect first and then extend our analysis with consideration of Rayleigh fading effect.

We first calculate the cumulative interference emitted from jammers at the 1st layer, which is shown as follows,

$$I_j(1) = 4P_J\left(\sqrt{2}d\right)^{-\alpha}.$$

Similarly, we have the interference from jammers at the 2nd layer as follows,

$$I_j(2) = 4P_J\left[2\left(\sqrt{10}d\right)^{-\alpha} + \left(3\sqrt{2}d\right)^{-\alpha}\right].$$

The interference from jammers at the 3rd layer is given by

$$I_j(2) = 4P_J\left\{2\cdot\left[\left(\sqrt{10}d\right)^{-\alpha} + \left(3\sqrt{2}d\right)^{-\alpha}\right] + \left(5\sqrt{2}d\right)^{-\alpha}\right\}.$$

Following the similar analysis, we have the interference from jammers at the $(n-1)$-th layer as follows,

$$\begin{aligned} I_j(n-1) &= 4P_J\Bigg\{2\cdot\Bigg[\left(d\cdot\sqrt{1+(2n-3)^2}\right)^{-\alpha} \\ &+\left(d\cdot\sqrt{9+(2n-3)^2}\right)^{-\alpha}+\cdots \\ &+\left(d\cdot\sqrt{(2n-5)^2+(2n-3)^2}\right)^{-\alpha}\Bigg] \\ &+\left(d\cdot\sqrt{2(2n-3)^2}\right)^{-\alpha}\Bigg\}. \end{aligned} \tag{A1}$$

Then, the interference from the n-th layer is given by

$$\begin{aligned} I_j(n) &= 4P_J\Bigg\{2\cdot\Bigg[\left(d\cdot\sqrt{1^2+(2n-1)^2}\right)^{-\alpha} \\ &+\left(d\cdot\sqrt{9+(2n-1)^2}\right)^{-\alpha}+\cdots \\ &+\left(d\cdot\sqrt{(2n-3)^2+(2n-1)^2}\right)^{-\alpha}\Bigg] \\ &+\left(d\cdot\sqrt{2(2n-1)^2}\right)^{-\alpha}\Bigg\}. \end{aligned} \tag{A2}$$

Summarizing them all, we then have

$$I_j(n) = 4P_J\sum_{k=1}^{n}\left\{2\left(d\cdot\sqrt{(2k-3)^2+(2k-1)^2}\right)^{-\alpha}+\left(d\cdot\sqrt{2(2k-1)^2}\right)^{-\alpha}\right\}. \tag{A3}$$

We next have the cumulative interference from all the jammers as follows,

$$I_j = \sum_{m=1}^{n} I_j(m).$$

Considering the Rayleigh fading effect, we finally prove the expectation the cumulative interference from all the jammers as given in Lemma 1. □

Appendix B

Proof of Lemma 2. We assume that the transmitter is located between kth layer and $k+1$th layer of the jammers. Since the jammers are distributed in a symmetric manner (around the eavesdropper), we only need to calculate the cumulative interference from one corner of the plane (e.g., the north-east corner). Summing the cumulative interference from all the four corners, we can obtain the cumulative inference from all the jammers.

Firstly, we consider the interference caused from friendly jammers at the center location between 1st layer and 2nd layer as shown in Figure 1 (see the red dashed line). Interference caused by jammers at the mth layer, which is surrounded by the jammers at the kth layer is calculated as the following equation,

$$
\begin{aligned}
I_j(m) = P_j(m)\Bigg\{ & 2\sqrt{\left(\frac{1}{2}\cdot 2d\right)^2 + \left[\left(k-m+\frac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} \\
& + 2\sqrt{\left(\frac{3}{2}\cdot 2d\right)^2 + \left[\left(k-m+\frac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} + \cdots \\
& + 2\sqrt{\left[\left(m-\frac{1}{2}\right)\cdot 2d\right]^2 + \left[\left(k-m+\frac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} \\
& + 2\sqrt{\left[\left(m-\frac{1}{2}\right)\cdot 2d\right]^2 + \left[\left(k-m+\frac{3}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} + \cdots \\
& + 2\sqrt{\left[\left(m-\frac{1}{2}\right)\cdot 2d\right]^2 + \left[\left(k+m-\frac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} \\
& + 2\sqrt{\left[\left(m-\frac{3}{2}\right)\cdot 2d\right]^2 + \left[\left(k+m-\frac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} + \cdots \\
& + 2\sqrt{\left(\frac{1}{2}\cdot 2d\right)^2 + \left[\left(k+m-\frac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} \Bigg\}.
\end{aligned}
\tag{B1}
$$

Summing all the terms in Equation (B1), we then obtain the simplified expression of $I_j(m)$ as follows,

$$
\begin{aligned}
I_j(m) \quad = 2P_j(m)\Bigg\{ & \sum_{v=1}^{m} \Bigg(\sqrt{\left[\left(v-\tfrac{1}{2}\right)\cdot 2d\right]^2 + \left[\left(k-m+\tfrac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} \\
& + \sqrt{\left[\left(v-\tfrac{1}{2}\right)\cdot 2d\right]^2 + \left[\left(k+m-\tfrac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} \Bigg) \\
& + \sum_{w=k-m+1}^{k+m} \sqrt{\left[\left(m-\tfrac{1}{2}\right)\cdot 2d\right]^2 + \left[\left(w-\tfrac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} \Bigg\}.
\end{aligned}
\tag{B2}
$$

Interference caused by jammers at the qth layer, which is placed outside of kth layer is calculated by this equation,

$$
\begin{aligned}
I_j(q) \quad = P_j(q)\Bigg\{ & 2\sqrt{\left(\tfrac{1}{2}\cdot 2d\right)^2 + \left[\left(q-k-\tfrac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} \\
& +2\sqrt{(\tfrac{3}{2}\cdot 2d)^2 + \left[\left(q-k-\tfrac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} + \cdots \\
& +2\sqrt{\left(\left(q-\tfrac{1}{2}\right)\cdot 2d\right)^2 + \left[\left(q-k-\tfrac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} \\
& +2\sqrt{\left(\left(q-\tfrac{1}{2}\right)\cdot 2d\right)^2 + \left[\left(q-k+\tfrac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} + \cdots \\
& +2\sqrt{\left(\left(q-\tfrac{1}{2}\right)\cdot 2d\right)^2 + \left[\left(q+k+\tfrac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} + \cdots \\
& +2\sqrt{\left(\tfrac{1}{2}\cdot 2d\right)^2 + \left[\left(q+k+\tfrac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} \Bigg\}.
\end{aligned}
\tag{B3}
$$

From Equation (B3) we can get the simplified expression of $I_j(q)$ as follows,

$$
\begin{aligned}
I_j(q) = 2P_j(q) \Bigg\{ \sum_{s=1}^{q} \Bigg(& \sqrt{\left(\left(s-\frac{1}{2}\right)\cdot 2d\right)^2 + \left[\left(q-k-\frac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} \\
& + \sqrt{\left(\left(s-\frac{1}{2}\right)\cdot 2d\right)^2 + \left[\left(q+k+\frac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} \Bigg) \\
& + \sum_{z=q-k-1}^{q+k} \sqrt{\left(\left(q-\frac{1}{2}\right)\cdot 2d\right)^2 + \left[\left(z+\frac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} \Bigg\}.
\end{aligned}
\tag{B4}
$$

Therefore, summing Equations (B2) and (B4), we obtain the cumulative interference of jammers at the location t_0 as the following equation,

$$
\begin{aligned}
I_{k,t_0} = \sum_{m=1}^{k} \sum_{v=1}^{m} \Bigg(2P_j(m) \Bigg(& \sqrt{\left[\left(v-\frac{1}{2}\right)\cdot 2d\right]^2 + \left[\left(k-m+\frac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} \\
& + \sqrt{\left[\left(v-\frac{1}{2}\right)\cdot 2d\right]^2 + \left[\left(k+m-\frac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} \Bigg) \Bigg) \\
& + \sum_{m=1}^{k} \sum_{w=k-m+1}^{k+m} 2P_j(m) \sqrt{\left[\left(m-\frac{1}{2}\right)\cdot 2d\right]^2 + \left[\left(w-\frac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} \\
& + \sum_{q=k}^{n} \sum_{z=q-k-1}^{q+k} 2P_j(q) \sqrt{\left[\left(q-\frac{1}{2}\right)\cdot 2d\right]^2 + \left[\left(z+\frac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} \\
& + \sum_{q=k}^{n} \sum_{s=1}^{q} \Bigg(2P_j(q) \Bigg(\sqrt{\left[\left(s-\frac{1}{2}\right)\cdot 2d\right]^2 + \left[\left(q-k-\frac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} \\
& + \sqrt{\left[\left(s-\frac{1}{2}\right)\cdot 2d\right]^2 + \left[\left(q+k+\frac{1}{2}\right)\cdot 2d\right]^2}^{\,-\alpha} \Bigg) \Bigg)
\end{aligned}
\tag{B5}
$$

The interference at t_x can be calculated by the similar approach in Equation (14).

We denote the number of all the possible locations of jammers placed between kth layer and $(k+1)$-th layer as N_k, which is equal to $(2k+1)^2 - (2k-1)^2 = 8k$. Finally, the averaged interference is calculated by taking an average over all the possible locations. The detailed calculation is shown as the following equation,

$$
E[I_c] = \frac{\sum_{k=1}^{n} \left(4I_{k,t_0} + 4I_{k,t_k} + 8 \sum_{t=t_1}^{t_{k-1}} I_{k,t} \right)}{\sum_{k=1}^{n} 8k} = \frac{\sum_{k=1}^{n} \left(I_{k,t_0} + I_{k,t_k} + 2 \sum_{t=t_1}^{t_{k-1}} I_{k,t} \right)}{\sum_{k=1}^{n} 2k}.
\tag{B6}
$$

□

References

1. Lee, E.A. The past, present and future of cyber-physical systems: A focus on models. *Sensors* **2015**, *15*, 4837–4869.

2. Huang, C.; Marshall, J.; Wang, D.; Dong, M. Towards Reliable Social Sensing in Cyber-Physical-Social Systems. In Proceedings of the 2016 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW), Chicago, IL, USA, 23–27 May 2016.
3. Dong, M.; Ota, K.; Liu, A. RMER: Reliable and Energy-Efficient Data Collection for Large-Scale Wireless Sensor Networks. *IEEE Int. Things J.* **2016**, *3*, 511–519.
4. Tang, Z.; Liu, A.; Huang, C. Social-Aware Data Collection Scheme Through Opportunistic Communication in Vehicular Mobile Networks. *IEEE Access* **2016**, *4*, 6480–6502.
5. Hu, Y.; Dong, M.; Ota, K.; Liu, A.; Guo, M. Mobile Target Detection in Wireless Sensor Networks with Adjustable Sensing Frequency. *IEEE Syst. J.* **2016**, *10*, 1160–1171.
6. Zhang, Q.; Liu, A. An unequal redundancy level-based mechanism for reliable data collection in wireless sensor networks. *EURASIP J. Wirel. Commun. Netw.* **2016**, *2016*, 258.
7. Liu, Y.; Dong, M.; Ota, K.; Liu, A. ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 2013–2027.
8. Wagner, D.; Schneier, B.; Kelsey, J. Cryptanalysis of the cellular message encryption algorithm. In *Advances in Cryptology–CRYPTO '97*; Springer: Berlin/Heidelberg, Germany, 1997.
9. 3GPP. *General Report on the Design, Speification and Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms*; Technical Report; 3GPP: Valbonne, France, 2009.
10. IEEE Standards Association. *802.11a-1999—IEEE Standard for Telecommunications and Information Exchange Between Systems— LAN/MAN Specific Requirements—Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High Speed Physical Layer in the 5 GHz Band*; Technical Report; IEEE: Piscataway, NJ, USA, 1999.
11. IEEE Standards Association. *802.11i-2004—IEEE Standard for Tnformation Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks-Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements*; Technical Report; IEEE: Piscataway, NJ, USA, 2004.
12. Shim, K.A. A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks. *IEEE Commun. Surv. Tutorials* **2016**, *18*, 577–601.
13. Han, Z.; Marina, N.; Debbah, M.; Hjørungnes, A. Physical Layer Security Game: Interaction Between Source, Eavesdropper, and Friendly Jammer. *EURASIP J. Wirel. Commun. Netw.* **2009**, *2009*, doi:10.1155/2009/452907.
14. Zhu, Q.; Saad, W.; Han, Z.; Poor, H.; Basar, T. Eavesdropping and jamming in next-generation wireless networks: A game-theoretic approach. In Proceedings of the 2010 Military Communications Conference, Baltimore, MD, USA, 7–10 November 2011.
15. Vilela, J.P.; Bloch, M.; Barros, J.; McLaughlin, S.W. Wireless Secrecy Regions With Friendly Jamming. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 256–266.
16. Sankararaman, S.; Abu-Affash, K.; Efrat, A.; Eriksson-Bique, S.D.; Polishchuk, V.; Ramasubramanian, S.; Segal, M. Optimization Schemes for Protective Jamming. In Proceedings of the 13th ACM MobiHoc, Hilton Head Island, SC, USA, 11–14 June 2012.
17. Kim, Y.S.; Tague, P.; Lee, H.; Kim, H. A Jamming Approach to Enhance Enterprise Wi-Fi Secrecy Through Spatial Access Control. *Wirel. Netw.* **2015**, *21*, 2631–2647.
18. IEEE Standards Association. *IEEE 802.15.4 Enabling Pervasive Wireless Sensor Networks*; Technical Report; IEEE: Piscataway, NJ, USA, 2011.
19. Lakshmanan, S.; Tsao, C.; Sivakumar, R.; Sundaresan, K. Securing Wireless Data Networks against Eavesdropping using Smart Antennas. In Proceedings of the 28th International Conference on Distributed Computing Systems, Beijing, China, 17–20 June 2008.
20. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proc. IEEE* **2016**, *104*, 1727–1765.
21. Ren, K.; Su, H.; Wang, Q. Secret key generation exploiting channel characteristics in wireless communications. *IEEE Wirel. Commun.* **2011**, *18*, 6–12.
22. Zafer, M.; Agrawal, D.; Srivatsa, M. Limitations of Generating a Secret Key Using Wireless Fading Under Active Adversary. *IEEE/ACM Trans. Netw.* **2012**, *20*, 1440–1451.
23. Zeng, K. Physical layer key generation in wireless networks: Challenges and opportunities. *IEEE Commun. Mag.* **2015**, *53*, 33–39.

24. Edman, M.; Kiayias, A.; Tang, Q.; Yener, B. On the Security of Key Extraction From Measuring Physical Quantities. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1796–1806.
25. Savry, O.; Pebay-Peyroula, F.; Dehmas, F.; Robert, G.; Reverdy, J. RFID Noisy Reader How to Prevent from Eavesdropping on the Communication? In Proceedings of the 2007 Cryptographic Hardware and Embedded Systems, Vienna, Austria, 10–13 September 2007; pp. 334–345.
26. Mukherjee, A.; Fakoorian, S.A.A.; Huang, J.; Swindlehurst, A.L. Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Commun. Surv. Tutorials* **2014**, *16*, 1550–1573.
27. Hassanieh, H.; Wang, J.; Katabi, D.; Kohno, T. Securing RFIDs by Randomizing the Modulation and Channel. In Proceedings of the 12th USENIX Symposium on Networked Systems Design and Implementation (NSDI 12), Oakland, CA, USA, 4–6 May 2015.
28. Kao, J.C.; Marculescu, R. Minimizing Eavesdropping Risk by Transmission Power Control in Multihop Wireless Networks. *IEEE Trans. Comput.* **2007**, *56*, 1009–1023.
29. Bashar, S.; Ding, Z. Optimum Power Allocation against Information Leakage in Wireless Network. In Proceedings of the 2009 Global Telecommunications Conference, Honolulu, HI, USA, 1–4 December 2009; pp. 1–6.
30. Gamal, A.E.; Mammen, J.; Prabhakar, B.; Shah, D. Optimal throughput-delay scaling in wireless networks-part I: The fluid model. *IEEE Trans. Inf. Theory* **2006**, *52*, 2568–2592.
31. Andrews, J.G.; Baccelli, F.; Ganti, R.K. A Tractable Approach to Coverage and Rate in Cellular Networks. *IEEE Trans. Commun.* **2011**, *59*, 3122–3134.
32. Min, G.; Wu, Y.; Al-Dubai, A.Y. Performance Modelling and Analysis of Cognitive Mesh Networks. *IEEE Trans. Commun.* **2012**, *60*, 1474–1478.
33. Wu, Y.; Min, G.; Al-Dubai, A.Y. A New Analytical Model for Multi-Hop Cognitive Radio Networks. *IEEE Trans. Wirel. Commun.* **2012**, *11*, 1643–1648.
34. Wu, Y.; Min, G.; Yang, L.T. Performance Analysis of Hybrid Wireless Networks Under Bursty and Correlated Traffic. *IEEE Trans. Veh. Technol.* **2013**, *62*, 449–454.