sensors

MDPI

Article

A Novel Friendly Jamming Scheme in Industrial Crowdsensing Networks against Eavesdropping Attack

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

[1] Faculty of Information Technology, Macau University of Science and Technology, Macau SAR, China; lxrget@163.com (X.L.); qiu_wang@foxmail.com (Q.W.)

[2] Department of ICT and Natural Sciences, Faculty of Information Technology and Electrical Engineering, Norwegian University of Science and Technology, Postboks 1517, NO-6025 Aalesund, Norway

* Correspondence: hndai@ieee.org (H.-N.D.); hawa@ntnu.no (H.W.); Tel.: +852-8897-2154 (H.-N.D.); +47-70-16-15-34 (H.W.)

Received: 10 May 2018; Accepted: 11 June 2018; Published: 14 June 2018

Abstract: Eavesdropping attack is one of the most serious threats in industrial crowdsensing networks. In this paper, we propose a novel anti-eavesdropping scheme by introducing friendly jammers to an industrial crowdsensing network. In particular, we establish a theoretical framework considering both the probability of eavesdropping attacks and the probability of successful transmission to evaluate the effectiveness of our scheme. Our framework takes into account various channel conditions such as path loss, Rayleigh fading, and the antenna type of friendly jammers. Our results show that using jammers in industrial crowdsensing networks can effectively reduce the eavesdropping risk while having no significant influence on legitimate communications.

Keywords: friendly jamming; crowdsensing; industrial internet of things; security

1. Introduction

Crowdsensing is a technique leveraging the crowd power to accomplish sensing tasks collaboratively at a low cost. The participants in crowdsensing networks sense the information and upload the sensed data to crowdsensing platforms voluntarily. As a result, the quality of sensing tasks heavily relies on whether the number of participants is sufficient. However, due to the consumption on time, battery and data, recruiting the participants in crowdsensing networks is difficult, although some incentive mechanisms were proposed [1]. Therefore, to guarantee the sensing quality of accomplished tasks, mobile crowdsensing as the complement of traditional statically deployments has been extensively investigated [2,3].

In recent years, the combination of crowdsensing and Industrial Internet of Things (IIoT) has drawn extensive attention [4,5]. There are a lot of benefits in introducing crowdsensing to IIoT, including: (1) providing mobile and scalable measures; (2) monitoring new areas without installing additional dedicated devices; (3) integrating human wisdom into machine intelligence straight forwardly; (4) sharing information and making decision among the whole industrial community [4]. The performance of personal monitoring, process monitoring and product quality checking in IIoT will be improved with the help of crowdsensing [5].

With the proliferation of wireless sensor devices, the security of transmitting data in such IIoT based crowdsensing networks deserves much attention, especially for the confidential data related with commercial interest and privacy concern. To protect the security of crowdsensing networks, some security encryption schemes were proposed, such as privacy-preserving participant selection scheme [6] and reputation management schemes [7]. Moreover, some encryption schemes for IIoT were

presented in [8]. The encryption schemes are feasible for devices with sufficient computing capability and power, such as smart phones or tablet computers. However, the encryption schemes may not be suitable for power-constraint sensor devices in crowdsensing networks (e.g., pulse-sensor-embedded wrists) and machinery in factories, since these schemes often require conducting compute-intensive tasks, consequently consuming a lot of power.

Different from the security encryption schemes, friendly-jamming schemes have been recognized as a promising approach to enhance the network security without bringing extra computing tasks [9–13]. The main idea of friendly-jamming schemes is introducing some friendly jammers to wireless networks, where these friendly jammers can generate a jamming signal to increase the noise level at the eavesdroppers, so that they cannot successfully wiretap the legitimate communications [14–16]. Using friendly-jamming schemes to decrease the possibility of eavesdropping attacks has received extensive attention [17,18]. The benefits of friendly jamming schemes is that there is no requirement for strong-computing capability of nodes, and no necessity for centralizing security schemes [19]. Therefore, friendly-jamming schemes can be applied in crowdsensing networks with power-constraint devices.

To mitigate the eavesdropping attack of crowdsensing networks, we propose a novel friendly jamming scheme in this paper. In this scheme, we place multiple jammers at a circular boundary around the protected communication area. Being implied by previous studies [20,21], we also consider equipping directional antennas at jammers. We name such jamming scheme with directional antennas as DFJ. Moreover, we also consider equipping omnidirectional antennas at jammers. We name such a jamming scheme with omnidirectional antennas as OFJ. For comparison purposes, we also consider the case without jammers (named as NFJ).

The main contributions of this paper are summarized as follows.

- We propose friendly jamming schemes (DFJ and OFJ) to protect confidential communications from eavesdropping attacks.
- We establish a theoretical model to analyze the *probability of eavesdropping attacks* and the *probability of successful transmission* to evaluate the effectiveness of our proposed scheme.
- We conduct extensive simulations to verify the accuracy of our theoretic model. The results also show that using jammers in crowdsensing networks can effectively reduce the eavesdropping risk while having no significant influence on legitimate communications.

Our proposed schemes have many more merits than other existing anti-eavesdropping schemes. Firstly, our schemes are less resource-intensive (i.e., no extensive computing resource needed) and it does not require any modifications on existing network infrastructure. Secondly, our schemes are quite general since the circular area with jammers can essentially circumscribe any buildings due to the feature that every simple polygon (i.e., the shape of a building) always has a circumscribed circle [22]. As a result, the effective jamming to eavesdroppers can be achieved. Moreover, our schemes can offer a larger effective protection area compared with other friendly jamming schemes like placing jammers at polygons [14] or other shapes [23] due to the largest coverage area of a circle.

2. System Models

In this section, we introduce the models used in this paper. We mainly focus on the uplink transmission from sensor devices (legitimate transmitter) to the receiver. The descriptions of notations are given in Table 1.

2.1. Network Model

In this paper, we consider a finite disk communication area with radius R, as shown in Figure 1. In this area, a number of legitimate transmitters are distributed according to Poisson point process (PPP) with density λ. In particular, each transmitter is assumed to follow uniformly independent identical distribution (i.i.d.). We consider a legitimate receiver, located in the center of this network. We assume there is an eavesdropper E with distance D away from the boundary of this communication

area, trying to wiretap the confidential communications within the communication area. In order to protect the legitimate transmission, we place multiple friendly jammers at the circular boundary around the protected communication area.

We assume the channel experience Rayleigh fading and path loss. Therefore, the received power of a receiver with distance r from a transmitter is $hr^{-\alpha}$, where h is a random variable following an exponential distribution with mean 1 and α is the path loss factor.

Table 1. Notation Summary.

Notation	Description
R	Radius of protected circular legitimate communication area
D	Distance between eavesdropper to the boundary of protected circular area
P_t, P_j	Transmission power of legitimate user and friendly jammer
l, r	Distance between the legitimate transmitter and eavesdropper/legitimate receiver
h	Fading random variable
α	Path loss exponent
Φ, λ	Point process and intensity of legitimate users
T, β	SINR threshold for a successful legitimate transmission/eavesdropping attack
M	Expectation of the number of legitimate transmitters
N	Number of friendly jammers
$\mathbb{E}(X)$	Expectation of random variable X
G_m, G_s	Antenna gain of main lobe, antenna gain of side lobe
θ_m	Main lobe beamwidth of the directional antenna
G_t, G_e, G_j	Antenna gain of the legitimate transmitters/eavesdropper/friendly jammers
$\mathbb{P}_E$	Probability of eavesdropping attacks
$\mathbb{P}_e$	Probability of eavesdropping a certain transmitter successfully
$\mathbb{P}_T$	Probability of successful transmission
I_t, I_j	Cumulative interference from legitimate transmitters/friendly jammers on the receiver
I_te, I_je	Cumulative interference from legitimate transmitters/friendly jammers on the eavesdropper
σ^2	Noise power of Gaussian Addictive White Noise

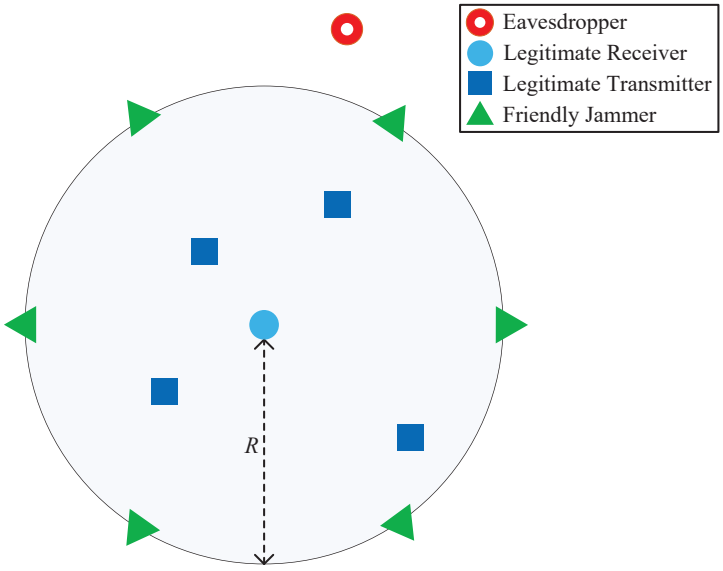


Figure 1. Network model.

2.2. Antennas

There are two types of antennas used in our network: an *omni-directional* antenna and a *directional antenna*. Omni-directional antennas radiate/collect radio signals into/from all directions equally. The antenna gain of omni-directional antenna is a constant in all directions, i.e., $G_o = 1$. Different from

an omni-directional antenna, a directional antenna can concentrate transmitting or receiving capability on some desired directions. Due to the high complexity to approximate a realistic directional antenna, we consider a simplified directional antenna model used in [24,25], as shown in Figure 2. This simplified directional antenna model consists of a main lobe G_m within the beamwidth θ_m and a side lobe G_s for all other directions. When G_m and θ_m is given, G_s can be calculated as follows [25],

$$G_s = \frac{2 - G_m(1 - \cos(\frac{\theta_m}{2}))}{1 + \cos\frac{\theta_m}{2}}. \quad (1)$$

In this paper, the receiver, the transmitters and the eavedropper are assumed to be equipped with omni-directional antennas. Then, with respect to jammers, we consider two jammer strategies in this network: (i) OFJ scheme, in which jammers are equipped with omni-directional antennas; (ii) DFJ scheme, in which jammers equipped with directional antennas. For comparison purposes, we also consider a scheme: NFJ scheme, in which no friendly jammers are deployed.

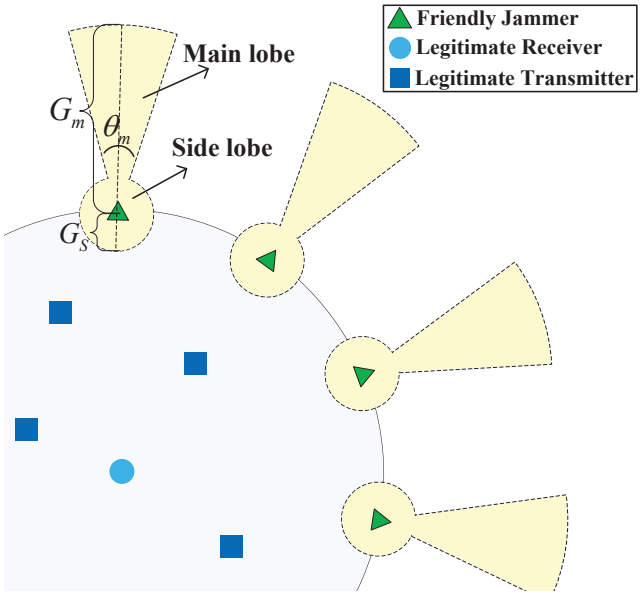


Figure 2. Friendly Jammers with Directional Antennas.

3. Impacts of Jamming Schemes on Legitimate Transmission

In this section, we investigate the impacts of different schemes on the legitimate communications. In particular, we consider the probability of successful transmission as a metric to evaluate the transmission quality of legitimate communications. The probability of successful transmission is defined as follows,

Definition 1. *The probability of successful transmission is the expectation of the probability that a reference transmitter can successfully transmit with the legitimate receiver according to the distance between the receiver and the reference transmitter.*

To guarantee the successful transmission of legitimate communication, the signal-to-interference-noise-ratio (SINR) at the legitimate receiver, denoted by $SINR_T$, must be no less than a threshold T. In particular, when we consider the communication between a reference transmitter t_0 and the receiver with distance r_0, $SINR_T$ can be expressed as

$$SINR_T = \frac{G_t G_r P_t h_0 {r_0}^{-\alpha}}{\sigma^2 + I_t + I_j} = \frac{P_t h_0 {r_0}^{-\alpha}}{\sigma^2 + I_t + I_j}, \tag{2}$$

where P_t is the transmission power of transmitters, G_t and G_r are the antenna gains of the reference transmitter and the receiver, respectively (where we have $G_t = G_r = 1$ since that the transmitters and receivers are equipped with omni-directional antennas), $I_t = \sum_{i \in \Phi / t_0} G_t G_r P_t h_i r_i^{-\alpha} = \sum_{i \in \Phi / t_0} P_t h_i r_i^{-\alpha}$ is the cumulative interference from legitimate users (where r_i is the distance between the ith transmitter and the receiver), $I_j = \sum_{k=1}^{N} G_j G_r P_j h_k R^{-\alpha} = \sum_{k=1}^{N} G_j P_j h_k R^{-\alpha}$ is the cumulative interference from N jammers to the receiver (where P_j is the transmission power of the jammers and G_j is the antenna gain of the jammers), and σ^2 is the noise power.

Thus, we have the probability of successful transmission, denoted by $\mathbb{P}_T$, as follows,

$$\mathbb{P}_T = \int_0^R \mathbb{P}\left[SINR_T \geq T \,|r_0\right] f_r(r_0) dr_0 = \int_0^R \mathbb{P}\left[\frac{P_t h_0 {r_0}^{-\alpha}}{\sigma^2 + I_t + I_j} \geq T \,|r_0\right] f_r(r_0) dr_0, \tag{3}$$

where $f_r(r_0)$ is the probability density function of the distance between the reference transmitter and the receiver r_0.

Then, we investigate the probability of successful transmission $\mathbb{P}_T$ according to the three jammer strategies: NFJ, OFJ, and DFJ schemes.

3.1. Impact of NFJ Scheme

In NFJ scheme, there is no friendly jammer at the boundary of the communication area. Therefore, the cumulative interference from friendly jammers $I_j = 0$. Then we have $\mathbb{P}_T$ in the NFJ scheme as in the following theorem.

Theorem 1. *In the NFJ scheme, the probability of successful transmission is*

$$\mathbb{P}_T = \frac{2^M}{R^{2M}} \int_0^R \exp\left(-T_p {r_0}^{\alpha} \sigma^2\right) \left(\int_0^R \frac{r^{1+\alpha}}{r^{\alpha} + T {r_0}^{\alpha}} dr \right)^{M-1} dr_0, \tag{4}$$

where $T_p = T/P_t$, and M is the expectation of the number of legitimate transmitters in the communication area.

Proof. Let the distance between the receiver and a transmitter be r. Since the receiver is located at the center of the circular area and each transmitter follows uniformly i.i.d., the probability density function of r is as follows,

$$f_r(r) = \frac{2\pi r}{\pi R^2} = \frac{2r}{R^2}, 0 < r \leq R. \tag{5}$$

After combining Equations (5) and (2), we have $\mathbb{P}_T$ as follows,

$$\begin{aligned} \mathbb{P}_T &= \int_0^R \mathbb{P}\left[\frac{P_t h_0 {r_0}^{-\alpha}}{\sigma^2 + I_t} \geq T | r_0\right] f_r(r_0) dr_0 \\ &= \int_0^R \mathbb{P}[h_0 \geq T_p {r_0}^{\alpha} (\sigma^2 + I_t) | r_0] 2 r_0 R^{-2} dr_0, \end{aligned} \tag{6}$$

where $T_p = T/P_t$.

Since h is a random variable following an exponential distribution with mean 1, $\mathbb{P}[h_0 \geq T_p r_0^{\alpha} (\sigma^2 + I_t) | r_0]$ in Equation (6) can be expressed as

$$\begin{aligned}&\mathbb{P}[h_0 \geq T_p r_0^{\alpha}(\sigma^2 + I_t)|r_0]\\&= \mathbb{E}_{I_t}[\exp((-T_p {r_0}^{\alpha})(\sigma^2 + I_t))|r_0]\\&= e^{-T_p {r_0}^{\alpha}\sigma^2}\mathbb{E}_{I_t}[\exp(-T_p {r_0}^{\alpha} I_t)].\end{aligned} \tag{7}$$

Next, we calculate $\mathbb{E}_{I_t}[\exp(-T_p {r_0}^{\alpha} I_t)]$. If we denote the expected number of legitimate transmitters by M, we can derive the expression of $\mathbb{E}_{I_t}[\exp(-T_p {r_0}^{\alpha} I_t)]$ as follows,

$$\begin{aligned}\mathbb{E}_{I_t}[\exp(-T_p {r_0}^{\alpha} I_t)] =&\mathbb{E}_{\Phi,\{h_i\}}[\exp(-T_p {r_0}^{\alpha} \sum_{i\in\Phi/t_0} P_t h_i r_i^{-\alpha})]\\=&\mathbb{E}_{\{r_i\},\{h_i\}}[\exp(-T_p P_t {r_0}^{\alpha} \sum_{i=1}^{M-1} h_i r_i^{-\alpha})]\\=&\mathbb{E}_{\{r_i\},\{h_i\}}[\prod_{i=1}^{M-1} \exp(-T {r_0}^{\alpha} h_i r_i^{-\alpha})]\\\overset{(a)}{=}&\left[\mathbb{E}_{r,h}(\exp(-T {r_0}^{\alpha} h r^{-\alpha}))\right]^{M-1}\\\overset{(b)}{=}&\left[\mathbb{E}_r\left(\frac{1}{1+T {r_0}^{\alpha} r^{-\alpha}}\right)\right]^{M-1}\\=&\left[\int_0^R (\frac{1}{1+T(r_0/r)^{\alpha}}) f_r(r) dr\right]^{M-1}\\=&\left[\frac{2}{R^2}\int_0^R (\frac{r^{1+\alpha}}{r^{\alpha}+T {r_0}^{\alpha}}) dr\right]^{M-1},\end{aligned} \tag{8}$$

where (a) is derived from the assumption that Rayleigh fading factor of each channel follows exponentially i.i.d., and (b) can be derived from the property of moment generating function of exponential variable.

Substituting Equation (8) into the corresponding part of Equation (7), we have

$$\mathbb{P}[h_0 \geq T_P r^{\alpha}(\sigma^2 + I_t)] = \exp(-T_p {r_0}^{\alpha}\sigma^2) \cdot \left(\frac{2}{R^2}\int_0^R \frac{r^{1+\alpha}}{r^{\alpha}+T\cdot {r_0}^{\alpha}} dr\right)^{M-1}. \tag{9}$$

After plugging Equation (9) into Equation (6), we can obtain $\mathbb{P}_T$ in Theorem 1. □

3.2. Impact of OFJ Scheme

In the OFJ scheme, the friendly jammers placed at the boundary of communication area are equipped with omni-directional antennas, i.e., the antenna gain of jammers is $G_j = G_o = 1$. Therefore, I_j in Equation (3) can be expressed as $\sum_{k=1}^{N} P_j h_k R^{-\alpha}$. Then we give $\mathbb{P}_T$ in the OFJ scheme by the following theorem.

Theorem 2. *In the OFJ Scheme, the probability of successful transmission is*

$$\mathbb{P}_T = \frac{2^M}{R^{2M}}\int_0^R \exp\left(-T_p {r_0}^{\alpha}\sigma^2\right)[1 + T_p (r_0 R)^{-\alpha} P_j]^{-N}\left(\int_0^R \frac{r^{1+\alpha}}{r^{\alpha}+T {r_0}^{\alpha}} dr\right)^{M-1} dr_0. \tag{10}$$

Proof. Similar to the proof of Theorem 1, the probability of successful transmission $\mathbb{P}_T$ in the OFJ scheme can be expressed as follows,

$$\mathbb{P}_T = \int_0^R P[h_0 \geq T_p {r_0}^{\alpha}(\sigma^2 + I_t + I_j)|r_0] 2 r_0 R^{-2} dr_0, \tag{11}$$

where $P[h_0 \geq T_p {r_0}^{\alpha}(\sigma^2 + I_t + I_j)|r_0]$ can be derived as follows,

$$\begin{aligned}
&\mathbb{P}[h_0 \geq T_p r^{\alpha}(\sigma^2 + I_t + I_j)|r_0] \\
&= \mathbb{E}_{I_t, I_j}[\exp((-T_p {r_0}^{\alpha})(\sigma^2 + I_t + I_j))|r_0] \\
&= e^{-T_p {r_0}^{\alpha}\sigma^2}\mathbb{E}_{I_t}[\exp(-T_p {r_0}^{\alpha} I_t)]\mathbb{E}_{I_j}[\exp(-T_p {r_0}^{\alpha} I_j)],
\end{aligned} \tag{12}$$

where $\mathbb{E}_{I_t}[\exp(-T_p {r_0}^{\alpha} I_t)]$ is given by Equation (8), and $\mathbb{E}_{I_j}[\exp(-T_p {r_0}^{\alpha} I_j)]$ can be calculated by

$$\begin{aligned}
\mathbb{E}_{I_j}[\exp(-T_p {r_0}^{\alpha} I_j)] =& \mathbb{E}_h[\exp(-T_p {r_0}^{-\alpha} \sum_{n=1}^{N} P_j h_n R^{-\alpha})] \\
=& \mathbb{E}_h[\prod_{n=1}^{N} \exp(-T_p {r_0}^{-\alpha} P_j R^{-\alpha} h_n)] \\
=& \prod_{n=1}^{N} \mathbb{E}_h[\exp(-T_p {r_0}^{-\alpha} P_j R^{-\alpha} h_n)] \\
=& [1 + T_p (r_0 R)^{-\alpha} P_j]^{-N}.
\end{aligned} \tag{13}$$

Substituting Equations (8) and (13) into the corresponding parts of Equation (12), we have

$$\mathbb{P}[h_0 \geq T_P r^{\alpha}(\sigma^2 + I_t + I_j)] = \exp(-T_p {r_0}^{\alpha}\sigma^2) \cdot [1 + T_p (r_0 R)^{-\alpha} P_j]^{-N} \cdot \left(\frac{2}{R^2}\int_0^R \frac{r^{1+\alpha}}{r^{\alpha} + T \cdot {r_0}^{\alpha}} dr\right)^{M-1}. \tag{14}$$

By plugging Equation (14) into Equation (11), we can obtain $\mathbb{P}_T$ of OFJ scheme in Theorem 2. □

3.3. Impact of DFJ Scheme

In DFJ scheme, the jammers placed at the boundary are equipped with directional antennas. In particular, we can find that the receiver can be only affected by the side lobe of directional antennas, as shown in Figure 2. Therefore, we have $G_j = G_s$. Thus, I_j in Equation (3) can be expressed as $\sum_{k=1}^{N} G_s P_j h_k R^{-\alpha}$. Then, we obtain $\mathbb{P}_T$ in the DFJ scheme by the following theorem.

Theorem 3. *In the DFJ scheme, the probability of successful transmission is*

$$\mathbb{P}_T = \frac{2^M}{R^{2M}} \int_0^R \exp\left(-T_p {r_0}^{\alpha}\sigma^2\right)[1 + T_p (r_0 R)^{-\alpha} P_j G_s]^{-N} \left(\int_0^R \frac{r^{1+\alpha}}{r^{\alpha} + T {r_0}^{\alpha}} dr\right)^{M-1} dr_0. \tag{15}$$

Proof. Similar to the proof of Theorems 1 and 2, $\mathbb{P}_T$ in DFJ can be expressed as

$$\begin{aligned}
\mathbb{P}_T &= \int_0^R P\left[\frac{P_t h_0 {r_0}^{-\alpha}}{\sigma^2 + I_t + I_j} \geq T | r_0\right] f_r(r_0) dr_0 \\
&= \int_0^R \mathbb{E}_{I_t}[\exp(-T_p {r_0}^{\alpha} I_t)]\mathbb{E}_{I_j}[\exp(-T_p {r_0}^{\alpha} I_j)] \cdot 2 r_0 R^{-2} e^{-T_p {r_0}^{\alpha}\sigma^2} dr_0,
\end{aligned} \tag{16}$$

where $\mathbb{E}_{I_t}[\exp(-T_p {r_0}^{\alpha} I_t)]$ is given by Equation (8), and $\mathbb{E}_{I_j}[\exp(-T_p {r_0}^{\alpha} I_j)]$ can be calculated by

$$\begin{aligned}
\mathbb{E}_{I_j}[\exp(-T_p {r_0}^{\alpha} I_j)] =& \mathbb{E}_h[\exp(-T_p {r_0}^{-\alpha} \sum_{n=1}^{N} P_j G_s h_n R^{-\alpha})] \\
=& \prod_{n=1}^{N} \mathbb{E}_h[\exp(-T_p {r_0}^{-\alpha} P_j G_s R^{-\alpha} h_n)] \\
=& [1 + T_p (r_0 R)^{-\alpha} P_j G_s]^{-N}.
\end{aligned} \tag{17}$$

After plugging Equations (8) and (17) into Equation (16), we can obtain $\mathbb{P}_T$ of DFJ scheme in Theorem 3. □

4. Analysis on Probability of Eavesdropping Attacks

In this section, we analyze the influence of friendly jammers on the probability of an eavesdropping attack of this network. In particular, we use the probability of an eavesdropping attack as the metric to evaluate the possibility of being eavesdropped on in this network. We assume that if the eavesdropper can wiretap any of the transmitters, this network can be seen as being attacked. Based on this assumption, we give the definition of the probability of eavesdropping attack as follows.

Definition 2. *The probability of an eavesdropping attack is the probability that the eavesdropper can wiretap any of the transmitters.*

Before we analyze the probability of an eavesdropping attack, we first analyze the probability that a certain transmitter can be wiretapped by the eavesdropper, denoted by $\mathbb{P}_e$. If the eavesdropper can wiretap a transmitter t_0 with distance l_0, the SINR at the eavesdropper, denoted by $SINR_E$, has to be no less than a threshold β. Thus, $\mathbb{P}_e$ can be expressed as follows,

$$\begin{aligned}\mathbb{P}_e=\mathbb{E}_{l_0}[\mathbb{P}(SINR_E \geq \beta|l_0)] &= \int_D^{D+2R} \mathbb{P}\left[\frac{G_t G_e P_t h_0 {l_0}^{-\alpha}}{\sigma^2 + I_{te} + I_{je}} \geq \beta|l_0\right] f_l(l_0) dl_0 \\ &= \int_D^{D+2R} \mathbb{P}\left[\frac{P_t h_0 {l_0}^{-\alpha}}{\sigma^2 + I_{te} + I_{je}} \geq \beta|l_0\right] f_l(l_0) dl_0\end{aligned} \tag{18}$$

where G_e is the antenna gain of the eavesdropper (we have $G_e = 1$ since the eavesdropper is equipped by an omni-directional antenna), $I_{te} = \sum_{i \in \Phi/t_0} G_t G_e P_t h_i l_i^{-\alpha} = \sum_{i \in \Phi/t_0} P_t h_i l_i^{-\alpha}$ is the cumulative interference from transmitters to the eavesdropper (where l_i is the distance between the ith transmitter and the eavesdropper), I_{je} is the cumulative interference from the jammers to the eavesdropper, which will be elaborated later according to different jammer schemes, and $f_l(l_0)$ is the probability density function of l_0.

Next, based on the analysis of $\mathbb{P}_e$, we give the probability of eavesdropping attack, denoted by P_E, as follows,

$$\mathbb{P}_E = 1 - (1 - \mathbb{P}_e)^M. \tag{19}$$

The impact of friendly jammers on the eavesdropping attacks will then be investigated. In particular, we will derive the probability of an eavesdropping attack $\mathbb{P}_E$ of an eavesdropper in the NFJ scheme, OFJ scheme and DFJ scheme as follows, respectively.

4.1. Impact of NFJ Scheme

Firstly we consider the NFJ scheme in which there is no friendly jammer on the boundary of communication area. In this case, the interference from friendly jammers to eavesdropper $I_{je} = 0$, then we have the following theorem:

Theorem 4. *In the NFJ scheme, the probability of eavesdropping attack $\mathbb{P}_E$ is*

$$\mathbb{P}_E = 1 - \left(1 - \left(\frac{2}{\pi R^2}\right)^M \cdot \int_D^{D+2R} \exp(-\beta_p {l_0}^{\alpha} \sigma^2) l_0 Z(l_0)^{M-1} \cdot \arccos\left[\frac{D}{l_0} + \frac{{l_0}^2 - D^2}{2l_0(R+D)}\right] dl_0\right)^M, \tag{20}$$

where $\beta_p = \frac{\beta}{P_t}$, $V(l_0) = \beta_p {l_0}^{\alpha} P_j$ *and*

$$Z(l_0) = \int_D^{D+2R} \left(\frac{l^{\alpha+1}}{l^{\alpha} + \beta {l_0}^{\alpha}}\right) \arccos\left[\frac{D}{l} + \frac{l^2 - D^2}{2l(R+D)}\right] dl.$$

Proof. We denote the distance between the eavesdropper and a transmitter by l. The probability density function of l can be expressed as follows [26],

$$f_l(l) = \frac{2l}{\pi R^2} \arccos\left[\frac{D}{l} + \frac{l^2 - D^2}{2l(R+D)}\right], D \le l \le D + 2R. \tag{21}$$

Then $\mathbb{P}_e$ can be expressed as

$$\mathbb{P}_e = \int_D^{D+2R} \frac{2l_0}{\pi R^2} \mathbb{P}[h_0 \ge \beta_p {l_0}^{\alpha}(\sigma^2 + I_{te})|l_0] \cdot \arccos\left(\frac{d}{l_0} + \frac{{l_0}^2 - d^2}{2l_0(R+d)}\right) dl_0, \tag{22}$$

where $\beta_p = \frac{\beta}{P_t}$.

Since h_0 is a random variable following an exponential distribution with mean 1, $\mathbb{P}[h_0 \ge \beta_p {l_0}^{\alpha}(\sigma^2 + I_{te})|l_0]$ can be expressed as

$$\begin{aligned} &\mathbb{P}[h_0 \ge \beta_p {l_0}^{\alpha}(\sigma^2 + I_{te})|l_0] \\ &= \mathbb{E}_{I_{te}}[\mathbb{P}(h_0 \ge \beta_p {l_0}^{\alpha}(\sigma^2 + I_{te})|l_0)] \\ &= \mathbb{E}_{I_{te}}[\exp((-\beta_p {l_0}^{\alpha})(\sigma^2 + I_{te}))|l_0] \\ &= e^{-\beta_p {l_0}^{\alpha}\sigma^2} \cdot \mathbb{E}_{I_{te}}[\exp(-\beta_p {l_0}^{\alpha} I_{te})]. \end{aligned} \tag{23}$$

Following the similar approach in deriving Equation (8), the expression of $\mathbb{E}_{I_{te}}[\exp(-\beta_p l^{\alpha} I_{te})]$ can be derived by the following equation,

$$\begin{aligned} &\mathbb{E}_{I_{te}}[\exp(-\beta_p {l_0}^{\alpha} I_{te})] \\ &= \mathbb{E}_{\Phi,\{h_i\}}[\exp(-\beta_p {l_0}^{\alpha} \sum_{i \in \Phi / b_0} P_t h_i l_i^{-\alpha})] \\ &= \left[\int_D^{D+2R} \left(\frac{1}{1 + \beta(l_0/l)^{\alpha}}\right) f_l(l) dl\right]^{M-1} \\ &= \left[\frac{2}{\pi R^2} \int_D^{D+2R} \left(\frac{l^{\alpha+1}}{l^{\alpha} + \beta {l_0}^{\alpha}}\right) \arccos\left[\frac{D}{l} + \frac{l^2 - D^2}{2l(R+D)}\right] dl\right]^{M-1}. \end{aligned} \tag{24}$$

If we set $Z(l_0) = \int_D^{D+2R} \left(\frac{l^{\alpha+1}}{l^{\alpha} + \beta {l_0}^{\alpha}}\right) \arccos\left[\frac{D}{l} + \frac{l^2 - D^2}{2l(R+D)}\right] dl$, Equation (24) can be expressed as

$$\mathbb{E}_{I_{te}}[\exp(-\beta_p {l_0}^{\alpha} I_{te})] = \left[\frac{2Z(l_0)}{\pi R^2}\right]^{M-1}. \tag{25}$$

After plugging Equation (25) into the Equation (23), and substituting the new expression of Equation (23) into Equation (22), we obtain the result of $\mathbb{P}_e$ as follows,

$$\mathbb{P}_e = \left(\frac{2}{\pi R^2}\right)^M \cdot \int_D^{D+2R} \exp(-\beta_p {l_0}^{\alpha} \sigma^2) l_0 Z(l_0)^{M-1} \cdot \arccos\left[\frac{D}{l_0} + \frac{{l_0}^2 - D^2}{2l_0(R+D)}\right] dl_0. \tag{26}$$

Substituting $\mathbb{P}_e$ in Equation (26) into Equation (19), we derive the probability of eavesdropping attack $\mathbb{P}_E$ of the NFJ scheme as given in Theorem 4. □

4.2. Impact of OFJ Scheme

Then we investigate the OFJ scheme, where friendly jammers are equipped with omni-directional antennas. In order to derive $\mathbb{P}_e$, we need to calculate the interference from jammers to eavesdropper I_{je} first.

Figure 3 shows the geometrical relationships of the friendly jammers and the eavesdropper. Without loss of generality, we label the jammer which is nearest to the eavesdropper as J_1 and the jammer J_1 is at the left-hand-side of the eavesdropper. Then we label J_{2m} (where $m = 1, 2, 3, ...$) as mth nearest jammer at the right-hand-side of jammer J_1 separately. Similarly, we label J_{2n+1} (where $n = 1, 2, 3, ...$) as the nth nearest jammer at the left-hand-side of jammer J_1 separately.

From the observation point O, 2φ is the relative degree between neighbour jammers and γ is the degree between jammer J_1 and eavesdropper E. Since the number of jammers is N, we have $2\varphi = \frac{2\pi}{N}$. Due to the fact that the eavesdropper is randomly located outside of the protected communication area, we have the probability density function of variable γ,

$$f_\gamma(\gamma) = \frac{1}{\varphi}, 0 \leq \gamma \leq \varphi. \tag{27}$$

Then we can calculate the cumulative interference of the jammers to the eavesdropper based on their geometrical relationships, which is given by the following lemma.

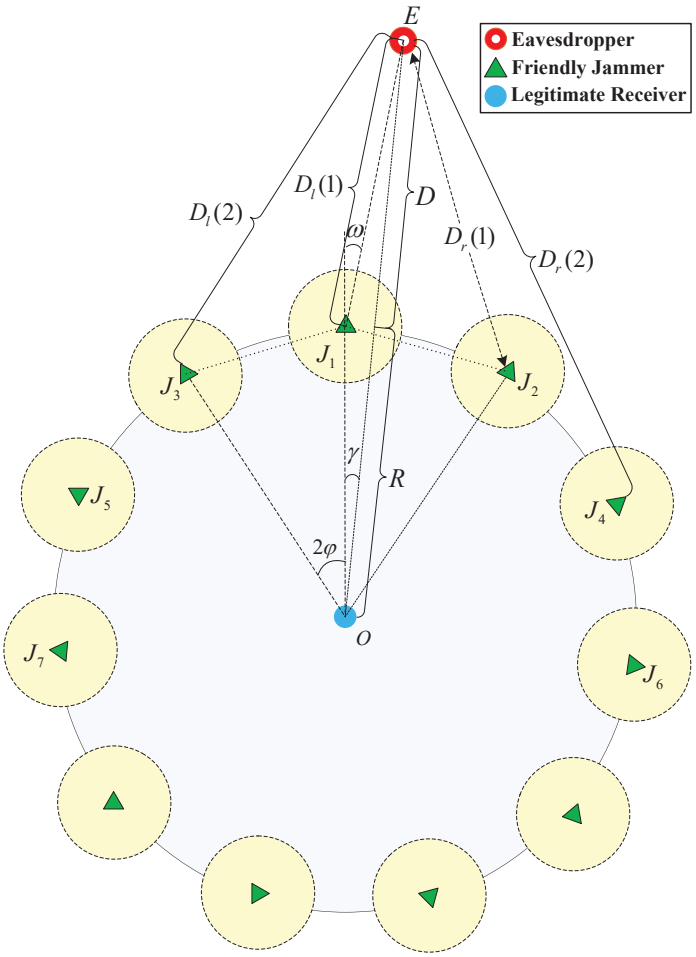


Figure 3. Geometrical relationship of the friendly jammers and the eavesdropper.

Lemma 1. *When the friendly jammers are equipped with omni-directional antennas, the cumulative interference from the jammers to the eavesdropper is*

$$I_{je} = \begin{cases} P_j \left[\sum_{x=-\frac{N-1}{2}}^{\frac{N-1}{2}} h_x D_{je}(x)^{-\alpha} \right], & N \text{ is odd} \\ P_j \left[\sum_{x=-\frac{N}{2}}^{\frac{N-2}{2}} h_x D_{je}(x)^{-\alpha} \right], & N \text{ is even} \end{cases}, \tag{28}$$

where $D_{je}(x) = \sqrt{R^2 + L^2 - 2RL\cos(2x\varphi + \gamma)}$.

Proof. We present the proof of Lemma 1 in Appendix A. □

With the interference from the jammers to the eavesdropper I_{je}, we obtain the probability of eavesdropping attack $\mathbb{P}_E$ as the following theorem.

Theorem 5. *In the OFJ scheme, the probability of an eavesdropping attack* $\mathbb{P}_E$ *of an eavesdropper is:*

$$\mathbb{P}_E = 1 - \left(1 - \left(\frac{2}{\pi R^2}\right)^M \int_D^{D+2R} \exp(-\beta_p {l_0}^\alpha \sigma^2) l_0 Z(l_0)^{M-1} W(l_0) \arccos\left[\frac{D}{l_0} + \frac{{l_0}^2 - D^2}{2l_0(R+D)}\right] dl_0\right)^M, \tag{29}$$

where

$$Z(l_0) = \int_D^{D+2R} \left(\frac{l^{\alpha+1}}{l^\alpha + \beta {l_0}^\alpha}\right) \arccos\left[\frac{D}{l} + \frac{l^2 - D^2}{2l(R+D)}\right] dl,$$

and

$$W(l_0) = \begin{cases} \prod_{x=-\frac{N-1}{2}}^{\frac{N-1}{2}} \int_0^\varphi \frac{1}{\varphi(1+V(l_0)D_{je}(x)^{-\alpha})} d\gamma, & N \text{ is odd} \\ \prod_{x=-\frac{N}{2}}^{\frac{N-2}{2}} \int_0^\varphi \frac{1}{\varphi(1+V(l_0)D_{je}(x)^{-\alpha})} d\gamma, & N \text{ is even} \end{cases},$$

in which $V(l_0) = \beta_p {l_0}^\alpha P_j$ *and* $\beta_p = \frac{\beta}{P_t}$.

Proof. Following the similar approach to the proof of Theorem 4, we can get the probability that a certain transmitter can be tapped denoted by $\mathbb{P}_e$ as follows,

$$\begin{aligned} \mathbb{P}_e &= \mathbb{E}_{l_0}[\mathbb{P}(SINR_E \geq \beta | l_0)] \\ &= \int_D^{D+2R} \mathbb{P}\left[\frac{P_t h_0 {l_0}^{-\alpha}}{\sigma^2 + I_{te} + I_{je}} \geq \beta | l_0\right] f_l(l_0) dl_0 \\ &= \int_D^{D+2R} \frac{2l_0}{\pi R^2} \mathbb{P}[h_0 \geq \beta_p {l_0}^\alpha (\sigma^2 + I_{te} + I_{je}) | l_0] \cdot \arccos\left(\frac{d}{l_0} + \frac{{l_0}^2 - d^2}{2l_0(R+d)}\right) dl_0, \end{aligned} \tag{30}$$

where $\beta_p = \frac{\beta}{P_t}$.

Since h_0 is a random variable following an exponential distribution with mean 1, $\mathbb{P}[h_0 \geq \beta_p {l_0}^\alpha (\sigma^2 + I_{te} + I_{je}) | l_0]$ can be expressed as

$$\mathbb{P}[h_0 \geq \beta_p {l_0}^\alpha (\sigma^2 + I_{te} + I_{je}) | l_0] = e^{-\beta_p {l_0}^\alpha \sigma^2} \cdot \mathbb{E}_{I_{te}}[\exp(-\beta_p {l_0}^\alpha I_{te})] \cdot \mathbb{E}_{I_{je}}[\exp(-\beta_p {l_0}^\alpha I_{je})], \tag{31}$$

where $\mathbb{E}_{I_{te}}[\exp(-\beta_p {l_0}^\alpha I_{te})] = \left[\frac{2Z(l_0)}{\pi R^2}\right]^{M-1}$ given by Equation (24).

Then we calculate $\mathbb{E}_{I_{je}}[\exp(-\beta_p {l_0}^\alpha I_{je})]$. For simplicity, we denote $W(l_0) = \mathbb{E}_{I_{je}}[\exp(-\beta_p {l_0}^\alpha I_{je})]$, $V(l_0) = \beta_p {l_0}^\alpha P_j$. With the expression of I_{je} given in Lemma 1, we can obtain $W(l_0)$ given by the following equation,

$$
\begin{aligned}
W(l_0) &= \mathbb{E}_{I_{je}}[\exp(-\beta_p {l_0}^{\alpha} I_{je})] \\
&= \begin{cases} \mathbb{E}_{h,\gamma}\left[\exp\left(-\sum\limits_{x=-\frac{N-1}{2}}^{\frac{N-1}{2}} V(l_0) h_k D_{je}(x)^{-\alpha}\right)\right], & N \text{ is odd;} \\ \mathbb{E}_{h,\gamma}\left[\exp\left(-\sum\limits_{x=-\frac{N}{2}}^{\frac{N-2}{2}} V(l_0) h_k D_{je}(x)^{-\alpha}\right)\right], & N \text{ is even.} \end{cases} \\
&\overset{(c)}{=} \begin{cases} \mathbb{E}_{\gamma}\left[\prod\limits_{x=-\frac{N-1}{2}}^{\frac{N-1}{2}} \mathbb{E}_h\left[\exp\left(-V(l_0) D_{je}(x)^{-\alpha} h_k\right)\right]\right], & N \text{ is odd;} \\ \mathbb{E}_{\gamma}\left[\prod\limits_{x=-\frac{N}{2}}^{\frac{N-2}{2}} \mathbb{E}_h\left[\exp\left(-V(l_0) D_{je}(x)^{-\alpha} h_k\right)\right]\right], & N \text{ is even.} \end{cases} \\
&\overset{(d)}{=} \begin{cases} \prod\limits_{x=-\frac{N-1}{2}}^{\frac{N-1}{2}} \mathbb{E}_{\gamma}\left[\frac{1}{1+V(l_0) D_{je}(x)^{-\alpha}}\right], & N \text{ is odd;} \\ \prod\limits_{x=-\frac{N}{2}}^{\frac{N-2}{2}} \mathbb{E}_{\gamma}\left[\frac{1}{1+V(l_0) D_{je}(x)^{-\alpha}}\right], & N \text{ is even.} \end{cases} \\
&\overset{(e)}{=} \begin{cases} \prod\limits_{x=-\frac{N-1}{2}}^{\frac{N-1}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V(l_0) D_{je}(x)^{-\alpha})} d\gamma, & N \text{ is odd;} \\ \prod\limits_{x=-\frac{N}{2}}^{\frac{N-2}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V(l_0) D_{je}(x)^{-\alpha})} d\gamma, & N \text{ is even.} \end{cases}
\end{aligned} \tag{32}
$$

where (c) is derived from the independence between an eavesdropper's location and the distribution of fading channel, (d) follows from the property of moment generating function of exponential variable, (e) is derived with the probability density function of γ as given in Equation (27).

After plugging Equation (32) into Equation (31), and substituting the new expression of Equation (31) into Equation (30), we obtain the result of $\mathbb{P}_e$ as given in the following expression,

$$
\mathbb{P}_e = \left(\frac{2}{\pi R^2}\right)^M \cdot \int_D^{D+2R} \exp(-\beta_p {l_0}^{\alpha} \sigma^2) l_0 Z(l_0)^{M-1} W(l_0) \arccos\left[\frac{D}{l_0} + \frac{{l_0}^2 - D^2}{2 l_0 (R+D)}\right] dl_0, \tag{33}
$$

Substituting the $\mathbb{P}_e$ in Equation (33) into Equation (19), we obtain the result of $\mathbb{P}_E$ given in Theorem 5. □

4.3. Impact of DFJ Scheme

In order to derive the probability of an eavesdropping attack $\mathbb{P}_E$ in the DJF scheme, we need to evaluate the interference from the friendly jammers equipped with directional antenna to the eavesdropper.

However, when the jammers are deployed densely or the distance between the eavesdropper and the commmunication area D is large, there may be more than one jammer that interferes with the eavesdropper via their main lobes simultaneously (as shown in Figure 4). Therefore, we first investigate the number of friendly jammers which interfere with the eavesdropper via main lobes.

In Figure 4, we show the main lobes of 3 jammers. Due to the fact that the eavesdropper is nearest to the jammer J_1, the eavesdropper locates in the area between line a and line b, where line a is the extended line of OJ_1 and line b is the perpendicular bisector of segment J_1J_2.

The term of ω in Figure 4 is the degree between line a and J_1E. When $\omega \geq \frac{\theta_m}{2}$, the eavesdropper locates in area A_0, there is no jammers interfering it with its main lobe. When $\omega \leq \frac{\theta_m}{2}$, the area that the eavesdropper locates depends on the distance D. When $\omega \leq \frac{\theta_m}{2}$, the eavesdropper locates in A_1 if $D \leq d$, there will be one jammer interfering with the eavesdropper via its main lobe; the eavesdropper locates in A_2 if $D \geq d$, there will be two jammers interfering with the eavesdropper via their main lobes.

Similarly, we denote A_k to be the intersection area of k jammers' main lobe directions between line a and line b. When the eavesdropper locates in area A_k, there will be k jammers interfering with the eavesdropper via their main lobes. We denote the number of friendly jammers (interfering the

eavesdropper via their main lobes) by N_d. When N_d is fixed, the interference of directional jammers to eavesdroppers is shown in the following lemma.

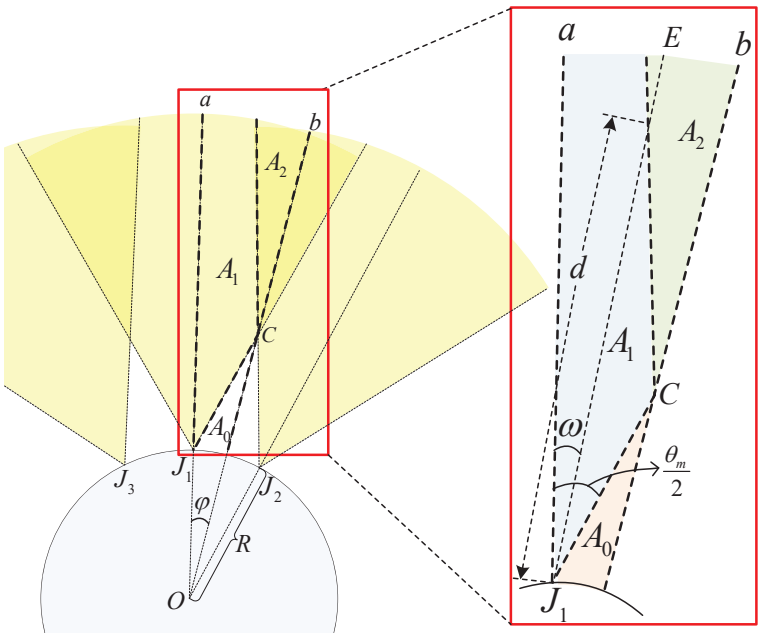


Figure 4. Geometrical relationship of friendly jammers (three jammers are shown).

Lemma 2. *When $N_d = k$, the interference of jammers on eavesdropper in the DFJ scheme is*

$$I_{je} = \begin{cases} P_j G_n \left[\sum\limits_{x=-\frac{k-1}{2}}^{\frac{k-1}{2}} h_x D_{je}(x)^{-\alpha} \right] + I_{js}, & k \text{ is odd} \\ P_j G_n \left[\sum\limits_{x=-\frac{k}{2}}^{\frac{k-2}{2}} h_x D_{je}(x)^{-\alpha} \right] + I_{js}, & k \text{ is even and } k \neq 0 \\ I_{js}, & k = 0 \end{cases}, \tag{34}$$

where $G_n = G_m - G_s$, $D_{je}(x) = \sqrt{R^2 + L^2 - 2RL\cos(2x\varphi + \gamma)}$, and

$$I_{js} = \begin{cases} P_j G_s \left[\sum\limits_{x=-\frac{N-1}{2}}^{\frac{N-1}{2}} h_x D_{je}(x)^{-\alpha} \right], & N \text{ is odd;} \\ P_j G_s \left[\sum\limits_{x=-\frac{N}{2}}^{\frac{N-2}{2}} h_x D_{je}(x)^{-\alpha} \right], & N \text{ is even.} \end{cases}$$

Proof. We present the proof of Lemma 2 in Appendix B. □

With the interference from the jammers to the eavesdropper, we obtain the probability of eavesdropping attack $\mathbb{P}_E$ as the following theorem,

Theorem 6. *In DFJ scheme, the upper bound of probability of eavesdropping attack $\mathbb{P}_E$ is given by*

$$\mathbb{P}_E = \frac{\varphi - \gamma_0}{\varphi} \cdot \left[1 - \left(1 - \mathbb{P}_e(N_d = 0) \right)^M \right] + \frac{\gamma_0}{\varphi} \cdot \left[1 - \left(1 - \mathbb{P}_e(N_d = 1) \right)^M \right],$$

where $\mathbb{P}_e(N_d = k) = \left(\frac{2}{\pi R^2} \right)^M \int_D^{D+2R} \exp(-\beta_p {l_0}^\alpha \sigma^2) l_0 Z(l_0)^{M-1} W'(l_0, k) \arccos[\frac{D}{l_0} + \frac{{l_0}^2 - D^2}{2l_0(R+D)}] dl_0,$

$$\beta_p = \frac{\beta}{P_t}, \quad V_1(l_0) = \beta_p {l_0}^{\alpha} P_j G_s, \quad V_2(l_0) = \beta_p {l_0}^{\alpha} P_j G_n, \quad Z(l_0) = \int_D^{D+2R} \left(\frac{l^{\alpha+1}}{l^{\alpha}+\beta {l_0}^{\alpha}}\right) \arccos\left[\frac{D}{l} + \frac{l^2-D^2}{2l(R+D)}\right] dl, \gamma_0 = \frac{\theta_m}{2} - \arcsin\left(R \sin\left(\frac{\theta_m}{2}\right)/L\right),$$

$$and\ W'(l_0,k) = \begin{cases} \prod_{x=-\frac{N-1}{2}}^{\frac{N-1}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V_1(l_0)D_{je}(x)^{-\alpha})} d\gamma, \ N \text{ is odd}, \ k \text{ is } 0; \\ \prod_{x=-\frac{N}{2}}^{\frac{N-2}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V_1(l_0)D_{je}(x)^{-\alpha})} d\gamma, \ N \text{ is even}, \ k \text{ is } 0; \\ \prod_{x=-\frac{N-1}{2}}^{\frac{N-1}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V_1(l_0)D_{je}(x)^{-\alpha})} d\gamma \cdot \prod_{y=-\frac{k-1}{2}}^{\frac{k-1}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V_2(l_0)D_{je}(y)^{-\alpha})} d\gamma, \ N \text{ is odd}, \ k \text{ is odd}; \\ \prod_{x=-\frac{N-1}{2}}^{\frac{N-1}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V_1(l_0)D_{je}(x)^{-\alpha})} d\gamma \cdot \prod_{y=-\frac{k}{2}}^{\frac{k-2}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V_2(l_0)D_{je}(x)^{-\alpha})} d\gamma \ N \text{ is odd}, \ k \text{ is even}. \\ \prod_{x=-\frac{N}{2}}^{\frac{N-2}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V_1(l_0)D_{je}(x)^{-\alpha})} d\gamma \cdot \prod_{y=-\frac{k-1}{2}}^{\frac{k-1}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V_2(l_0)D_{je}(y)^{-\alpha})} d\gamma, \ N \text{ is even}, \ k \text{ is odd}; \\ \prod_{x=-\frac{N}{2}}^{\frac{N-2}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V_1(l_0)D_{je}(x)^{-\alpha})} d\gamma \cdot \prod_{y=-\frac{k}{2}}^{\frac{k-2}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V_2(l_0)D_{je}(x)^{-\alpha})} d\gamma \ N \text{ is even}, \ k \text{ is even}. \end{cases}$$

Proof. We present the proof of Theorem 6 in Appendix C. □

5. Results

In this section, we present the simulation results of probability of successful transmission $\mathbb{P}_T$ and probability of eavesdropping attack $\mathbb{P}_E$ considering the NFJ, OFJ and DFJ schemes. The simulation results are generated via Monte Carlo simulations with 50,000 runs and the parameters are given in Table 2.

Table 2. Notation and parameters.

Parameters	Values
Radius of protected communication area R	20
Transmission power of legitimate users P_t	20 dBm
Transmission power of friendly jammers P_j	20 dBm
Noise power	−90 dBm
Antenna gain of main lobe G_m	10 dBi
Main lobe beamwidth θ_m	$\frac{\pi}{3}$

In Figure 5, we present the numerical and simulation results of probability of successful transmission $\mathbb{P}_T$ and probability of eavesdropping attack $\mathbb{P}_E$ with different schemes. From Figure 5a, we find $\mathbb{P}_T$ decreases when the number of legitimate transmitters denoted by M increases. Since the receiver only receives the information from the protected transmitter, the cumulative interference from legitimate transmitters to the receiver increases with M. When we introduce friendly jammers into the network, compared with the NFJ scheme, $\mathbb{P}_T$ decreases. The performance of $\mathbb{P}_T$ with DFJ scheme is better than $\mathbb{P}_T$ with OFJ scheme. This is because the lower antenna gain of side lobe in the DFJ scheme leads to less interference to the legitimate transmission.

In Figure 5b, the red curve represents the probability of eavesdropping attack $\mathbb{P}_E$ of the NFJ scheme. From numerical results, we find that the red line decreases very slowly, especially when M is larger than 2. For example, when $M = 4$, $\mathbb{P}_E$ of NFJ scheme is 0.9626, while $\mathbb{P}_E$ becomes 0.9619 and 0.9602 when M becomes 6 and 8, respectively. This result lies in the fact that the eavesdropper may eavesdrop any one of the M legitimate transmitters, rather than a specially appointed transmitter. When M increases, the interference on the eavesdropper increases. However, the eavesdropper may tap more transmitters as the total number of transmitters is increased. In addition, the performance

of $\mathbb{P}_E$ of DFJ scheme is still better than that of the OFJ scheme, because of the higher antenna gain of main lobe.

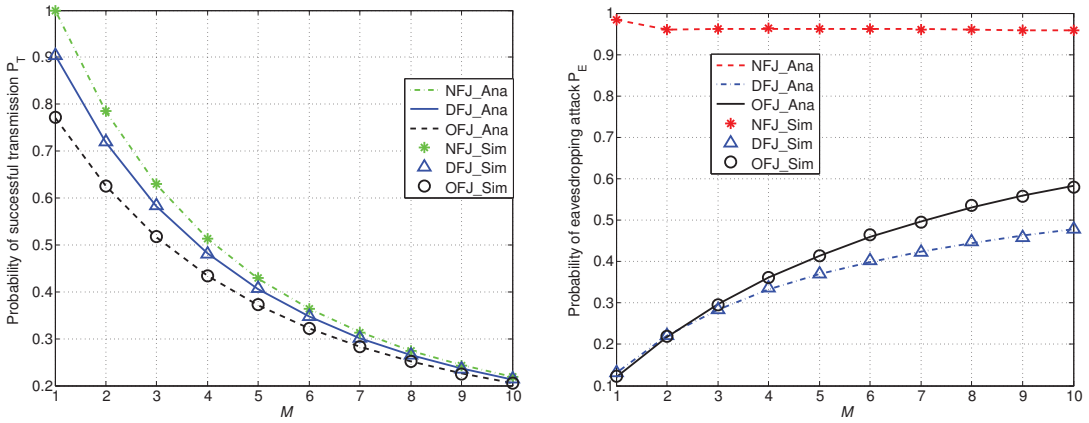
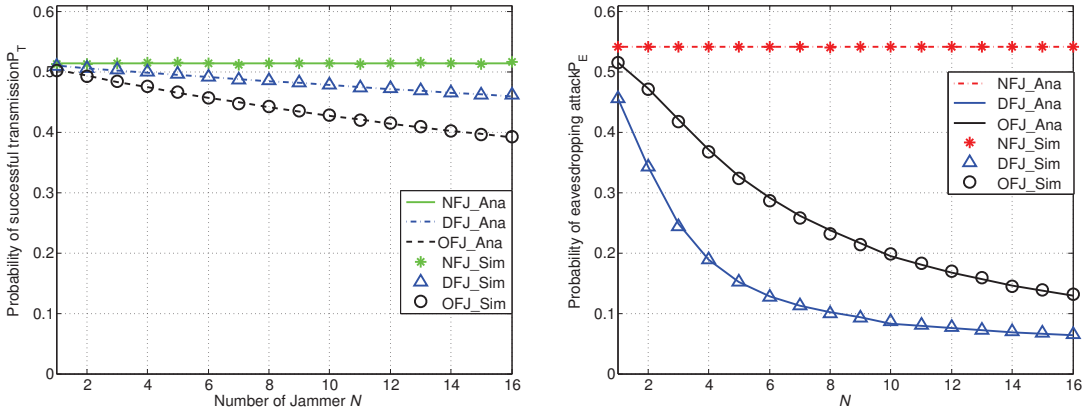


Figure 5. $\mathbb{P}_T$ and $\mathbb{P}_E$ with DFJ scheme and OFJ scheme versus NFJ scheme when $\alpha = 4$, $D = 10$, $N = 9$ and M varies from 1 to 10. (**a**) Probability of successful transmission $\mathbb{P}_T$; (**b**) Probability of eavesdropping attack $\mathbb{P}_E$.

From Figure 5a,b we find that introducing friendly jammers into the network will lead to the decrement on both $\mathbb{P}_T$ and $\mathbb{P}_E$. However, the influence of friendly jammers on $\mathbb{P}_E$ is more obvious than the influence on $\mathbb{P}_E$. For example, when $M = 5$, compared with the NFJ scheme, the reduction of $\mathbb{P}_T$ with OFJ scheme is 0.0574 (i.e., 13.4% reduced), while the reduction of $\mathbb{P}_E$ is 0.5485 (i.e., 56.99% reduced). When $M = 5$, compared with the NFJ scheme, the reduction of $\mathbb{P}_T$ with DFJ scheme is 0.023 (i.e., 5.4% reduced), the reduction of $\mathbb{P}_E$ is 0.5935 (i.e., 61.66% reduced). Therefore, the DFJ scheme can reduce the probability of eavesdropping attacks more significantly while maintaining the lower impairment to the legitimate communications than the OFJ scheme. This result implies that using friendly jammers can reduce the eavesdropping attack without causing obvious damage on legitimate transmission.

Figure 6 shows the comparison of $\mathbb{P}_T$ and $\mathbb{P}_E$ in different schemes with the varied number of friendly jammers denoted by N. In Figure 6a, we find that both $\mathbb{P}_T$ of the DFJ scheme and that of the OFJ scheme decrease when N increases. The decrement of $\mathbb{P}_T$ lies in the increased cumulative interference from friendly jammers. Moreover, Figure 6b shows that $\mathbb{P}_E$ decreases rapidly when the number of friendly jammers N increases, especially when friendly jammers are equipped with directional antennas (i.e., in DFJ scheme). This result can help to verify the effectiveness of OFJ and DFJ schemes in reducing the probability of eavesdropping attacks $\mathbb{P}_E$.

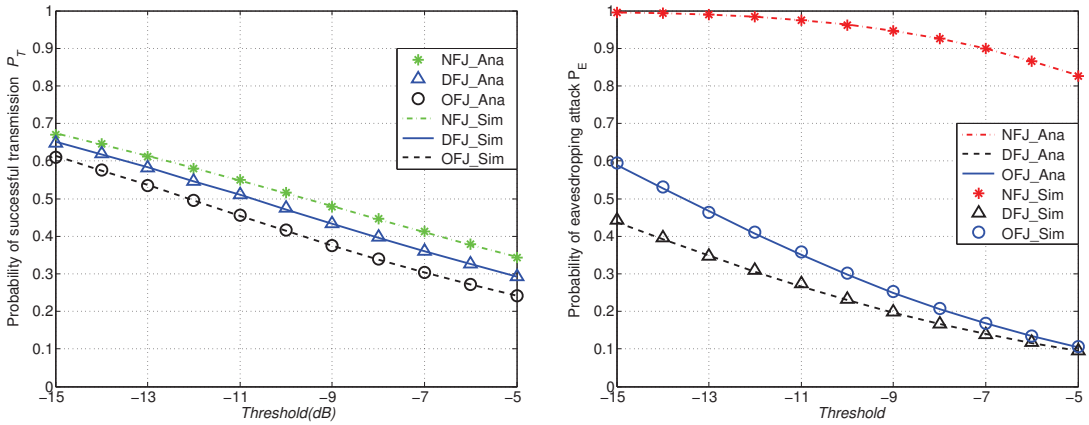
The results as shown in Figure 6 imply that it may not be necessary to deploy too many friendly jammers in the network. In particular, in the DFJ scheme, we can significantly reduce the probability of eavesdropping attacks while only slightly impairing legitimate communications by introducing a few friendly jammers. For example, when $N = 8$, compared with NFJ scheme, the reduction of $\mathbb{P}_T$ in DFJ scheme is 0.0291 (i.e., 5.66% reduction), while the reduction of $\mathbb{P}_E$ in the DFJ scheme is 0.4399 (i.e., 81.24% reduction).



(**a**) (**b**)

Figure 6. $\mathbb{P}_T$ and $\mathbb{P}_E$ with the DFJ scheme and the OFJ scheme versus the NFJ scheme when $\alpha = 4$, $D = 10$, $M = 4$ and N varies from 1 to 16. (**a**) Probability of successful transmission $\mathbb{P}_T$; (**b**) Probability of eavesdropping attack $\mathbb{P}_E$.

Figure 7 shows the comparison of $\mathbb{P}_T$ and $\mathbb{P}_E$ with DFJ, OFJ schemes versus the NFJ scheme with different SINR threshold. It is shown in Figure 7 that $\mathbb{P}_T$ decreases with the threshold T and $\mathbb{P}_E$ decreases with the threshold β. From Figure 7a, similarly to Figure 5b, we find that using friendly jammers can always reduce the probability of eavesdropping attacks $\mathbb{P}_E$ compared with the NFJ scheme, and the DFJ scheme performs better than the OFJ scheme obviously.



(**a**) (**b**)

Figure 7. $\mathbb{P}_T$ and $\mathbb{P}_E$ with DFJ scheme and OFJ scheme versus NFJ scheme when $\alpha = 4$, $D = 10$, $M = 4$, $N = 9$, SINR threshold T and β varies from -15 dB to -5 dB. (**a**) Probability of successful transmission $\mathbb{P}_T$; (**b**) Probability of eavesdropping attacks $\mathbb{P}_E$.

In another set of simulations as presented in Figure 8, we compare the probability of eavesdropping attack $\mathbb{P}_E$ of different schemes with varied distance between the eavesdropper and the network boundary D. From Figure 8a, we can find that $\mathbb{P}_E$ of NFJ, OFJ and DFJ schemes vary slightly when path loss factor $\alpha = 3$. It means when $\alpha = 3$, path loss effect has no obvious impact on $\mathbb{P}_E$. This result lies in the fact that path loss has the influence on both useful signal and interference. However, when the path loss factor α increases from 3 to 4, as shown in Figure 8b, $\mathbb{P}_E$ of three schemes decreases rapidly, especially in the NFJ scheme. This result implies that the path loss has a more obvious influence on useful signal than that on interference. From Figure 8, we also find that using friendly jammers can reduce the probability of eavesdropping attacks $\mathbb{P}_E$ compared with the NFJ scheme.

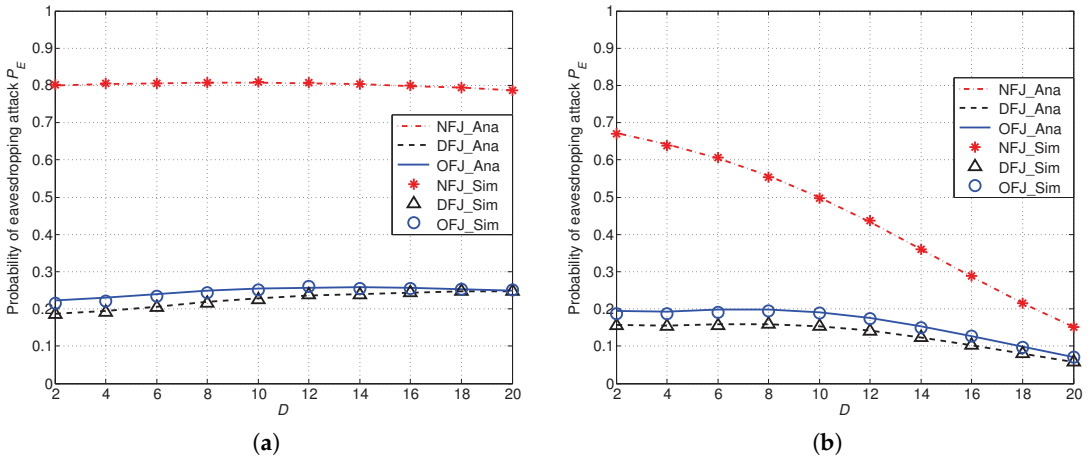


Figure 8. Probability of eavesdropping attacks $\mathbb{P}_E$ with DFJ scheme and OFJ scheme versus NFJ scheme when $\alpha = 3, 4$ with distance D ranging from 2 to 20. (**a**) $\alpha = 3$; (**b**) $\alpha = 4$.

6. Discussions

In this section, we first discuss the impact of our friendly jamming schemes when the eavesdropper is located inside the network. Then we discuss the impact of our friendly jamming schemes on legitimate transmissions in other networks.

6.1. Impact on the Eavesdropper Inside of Network

In Section 4, we analyze the impact of friendly jamming schemes on the eavesdropper who is prevented from entering the protected area. It is feasible in a practical industrial environment that the eavesdropper has the difficulty of entering the protected network area (e.g., the barbed wire entanglement around a plant). However, we can also apply our previous results in [27] to analyze the scenario in which an eavesdropper enters the network area. In particular, we consider that friendly jammers are regularly placed at deterministic locations [27] and the eavesdropper is located at the center of this area, as shown in Figure 9. We then apply the general theoretical models presented in [27] to derive the eavesdropping probability.

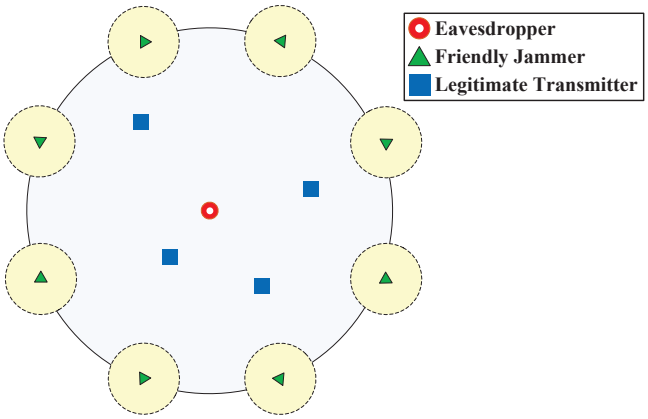


Figure 9. Eavesdropper inside of the network.

Regarding the case in which the eavesdropper is not located at the center of the network, we can first calculate the cumulative distance from the eavesdropper to each of friendly jammers via the approach proposed in [26] and used [28]. We can then derive the impact of friendly jammers on the eavesdropper inside of network by following the similar steps in [27] and plugging in the cumulative

distance. Due to the space limitation and the similarity to our previous method [27], we ignore the derivation of the eavesdropping probability in the scenario that an eavesdropper enters the network.

6.2. Impact on Legitimate Transmissions in Other Networks

In Section 3, we investigated the impact of friendly jamming schemes on legitimate transmissions in our protected network area. Since our friendly jammers are deployed on the boundary of our protected transmission area, the networks near this area may possibly be interfered with by our friendly jamming schemes. Therefore, we next investigate the impacts of friendly jamming schemes on legitimate transmissions in other networks.

In Figure 10, we show the relationship between our protected network (at the left hand side) and another network nearby (at the right hand side). It is worth mentioning that a crowdsensing device in our protected network often has the multi-homing capability [29], i.e., accessing two different networks (e.g., a small cell and a macro cell). The impact of our friendly jamming schemes on legitimate transmissions of another network can be analyzed according to two different scenarios: (1) both protected network and another network are using different channels; (2) both protected network and another network are using the same channel. In the first scenario in which different frequencies are allocated to the protected network and another network. In this scenario, the interference of our friendly jamming schemes is negligible on legitimate transmissions in other networks.

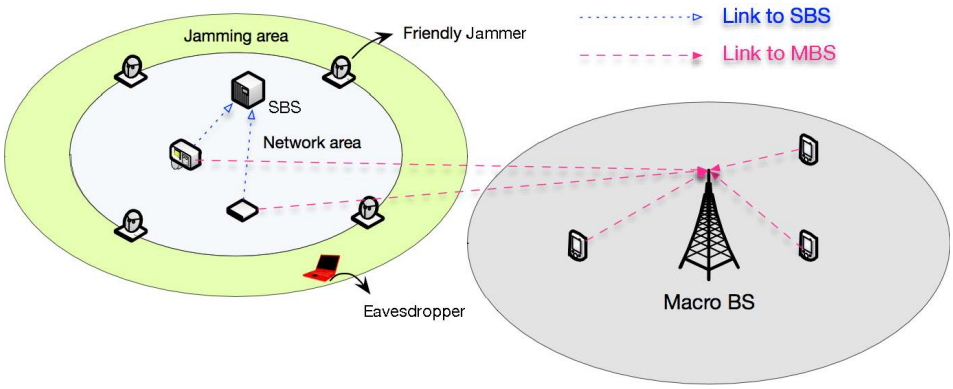


Figure 10. Impact of friendly jammers on other networks.

Then we analyze the second scenario. In this scenario, both the protected network and another network are using different channels. It is obvious that the analytical result in Section 4 can be trivially used to investigate the interference from friendly jammers on legitimate transmissions in another network. In particular, the interference generated by the OFJ scheme on legitimate transmissions outside the network is given by Lemma 1 in Section 4. The interference from the DFJ scheme on legitimate transmissions outside the network is given by Lemma 2 in Section 4.

Another concern related to our friendly jamming schemes is legitimacy. For example, jamming schemes are restricted in US and Europe. In Europe, the transmitting power of jammers is limited to be less than 20 dBm for 2.4 GHz band [30]. Therefore, we can either *limit the jamming range* or *restrict the jamming* period so that the impact on other legitimate communications will be minimized. The analytical results of OFJ and DFJ imply that the intensity of interference generated by our friendly jamming scheme heavily relies on the channel factors, for example, the transmitting power of jammers, antenna gain, path loss, etc. Therefore, we can adjust the transmitting power and the antenna gain of friendly jammers so that the jamming range can be minimized. Another approach of limiting the impact of friendly jamming schemes is restricting the time of the emitting jamming signal. For example, we can only send the jamming signal at the crucial stages (e.g., key generation phase [31] or vulnerable phase [14]).

7. Conclusions

In this paper, we propose a novel friendly jamming scheme to protect confidential communications from eavesdropping attacks. To evaluate the effectiveness of our scheme, we establish a theoretical model to analyze the probability of eavesdropping attacks and the probability of successful transmission. Moreover, we verify our model with extensive simulations. The agreement between analysis and simulation results verifies the accuracy of our analysis.

Our results show that our scheme can significantly decrease the eavesdropping risk compared with the no friendly jamming scenario and meanwhile that it maintains low decrease on the transmission probability. In addition, we find that using directional antennas compared with omni-directional antennas on friendly jammers can further decrease the eavesdropping risk while obviously mitigating the influence on the transmission probability.

Author Contributions: X.L. proposed the idea, derived the results and wrote the paper. H.-N.D. supervised the work and revised versions. Q.W. contributed to proofreading and revising the article. H.W. gave valuable suggestions on the motivation of proposing anti-eavesdropping schemes and assisted in revising the paper.

Funding: The work described in this paper was partially supported by Macao Science and Technology Development Fund under Grant No. 0026/2018/A1, the National Natural Science Foundation of China under Grant No. 61672170 and the Science and Technology Planning Project of Guangdong Province under Grant No. 2017A050501035. The authors would like to express their appreciation for Gordon K.-T. Hon for his thoughtful discussions. The authors would also like to thank the anonymous reviewers for their constructive comments.

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

Appendix A

Proof of Lemma 1. From the relationship of ΔEJ_1O in Figure 3, we can calculate the distance between jammer J_1 and the eavesdropper E in the following equation,

$$D_r(1) = [R^2 + L^2 - 2RL\cos(2\varphi - \gamma)]^{\frac{1}{2}}.$$

From the relationship of ΔEJ_2O, we get the distance between eavesdropper E and jammer J_2:

$$D_l(1) = [R^2 + L^2 - 2RL\cos\gamma]^{\frac{1}{2}}.$$

Following the similar approach, we have the distance between eavesdropper E and the mth nearest jammer at the right-hand-side of jammer J_1 as follows,

$$D_r(m) = [R^2 + L^2 - 2RL\cos(2m\varphi - \gamma)]^{\frac{1}{2}}, \tag{A1}$$

and the distance between eavesdropper E and the nth nearest jammer at the left-hand-side of jammer J_1 as follows,

$$D_l(n) = \left[R^2 + L^2 - 2RL\cos[2(n-1)\varphi + \gamma]\right]^{\frac{1}{2}}. \tag{A2}$$

Combining Equations (A1) and (A2), we can have the expression of the distance between jammers and eavesdropper $D_{je}(x)$ as follows,

$$D_{je}(x) = \left[R^2 + L^2 - 2RL\cos(2x\varphi + \gamma)\right]^{\frac{1}{2}}, \tag{A3}$$

where x is an integer whose range depends on N. When N is odd, $x \in \left[-\frac{N-1}{2}, \frac{N-1}{2}\right]$; when N is even, $x \in \left[-\frac{N}{2}, \frac{N-2}{2}\right]$.

Substituting the distance into the channel model, we get the cumulative interference of jammers to the eavesdropper as given in Lemma 1. □

Appendix B

Proof of Lemma 2. From Section 4.2 we have the distance between eavesdropper and jammers as given in Equation (A3). Then we show the interference of friendly jammers on eavesdroppers according to different cases of N_d.

Case 0: when $N_d = 0$, the interference of friendly jammers on eavesdroppers is from side lobe of friendly jammers,

If N is even,

$$I_{je} = I_{js} = P_j G_s \left[\sum_{x=-\frac{N}{2}}^{\frac{N-2}{2}} h_x D_{je}(x)^{-\alpha} \right];$$

If N is odd,

$$I_{je} = I_{js} = P_j G_s \left[\sum_{x=-\frac{N-1}{2}}^{\frac{N-1}{2}} h_x D_{je}(x)^{-\alpha} \right].$$

Case 1: when $N_d = 1$, the interference of friendly jammers on eavesdroppers is

$$I_{je} = P_j G_n h D_{je}(0)^{-\alpha} + I_{js}.$$

Case 2: when $N_d = 2$, the interference of friendly jammers on eavesdroppers is

$$I_{je} = P_j G_n h [D_{je}(-1)^{-\alpha} + D_{je}(0)^{-\alpha}] + I_{js}.$$

Case 3: when $N_d = 3$, the interference of friendly jammers on eavesdroppers is

$$I_{je} = P_j G_n h [D_{je}(-1)^{-\alpha} + D_{je}(1)^{-\alpha} + D_{je}(1)^{-\alpha}] + I_{js}.$$

Case k: when $N_d = k$, the interference of friendly jammers on eavesdroppers is

If k is even,

$$I_{je} = P_j G_n \left[\sum_{x=-\frac{k}{2}}^{\frac{k-2}{2}} h_x D_{je}(x)^{-\alpha} \right] + I_{js},$$

If k is odd,

$$I_{je} = P_j G_n \left[\sum_{x=-\frac{k-1}{2}}^{\frac{k-1}{2}} h_x D_{je}(x)^{-\alpha} \right] + I_{js}.$$

Therefore, we obtain the expression of I_{je} in Lemma 2 by integrating the above cases. □

Appendix C

Proof of Theorem 6. According to the definition of the eavesdropping probability $\mathbb{P}_E$, we need to derive the probability $\mathbb{P}_e$ first. The derivation of eavesdropping probability $\mathbb{P}_e$ in DFJ scheme is similar to the derivation OFJ scheme in Theorem 5, while the main difference is the cumulative interference from friendly jammers. Therefore, we have the following expressions:

$$\mathbb{P}_e(N_d = k) = \int_D^{D+2R} \frac{2l_0}{\pi R^2} \mathbb{P}[h \geq \beta_p {l_0}^{\alpha} (\sigma^2 + I_{te} + I_{je}(k)) | l_0] \cdot \arccos\left(\frac{d}{l_0} + \frac{{l_0}^2 - d^2}{2l_0(R+d)}\right) dl_0, \quad \text{(A4)}$$

where $\beta_p = \frac{\beta}{P_t}$, and

$$\mathbb{P}[h_0 \geq \beta_p {l_0}^{\alpha}(\sigma^2 + I_{te} + I_{je}(k))|l_0] = e^{-\beta_p {l_0}^{\alpha}\sigma^2} \cdot \mathbb{E}_{I_{te}}[\exp(-\beta_p {l_0}^{\alpha} I_{te})] \cdot \mathbb{E}_{I_{je}(k)}[\exp(-\beta_p {l_0}^{\alpha} I_{je}(k))]. \tag{A5}$$

The influence of legitimate transmitters on the eavesdropper remains unchanged. Therefore, we have the $\mathbb{E}_{I_{te}}[\exp(-\beta_p {l_0}^{\alpha} I_{te})]$ given in Equation (24).

From the expression of interference from directional jammers on eavesdropper as given in the Lemma 2, we have

$$\begin{aligned} W'(l_0,k) &= \mathbb{E}_{I_{je}(k)}[\exp(-\beta_p {l_0}^{\alpha} I_{je}(k))] \\ &= \begin{cases} \mathbb{E}_{h,\gamma}\left[\exp\left(-\sum\limits_{x=-\frac{N-1}{2}}^{\frac{N-1}{2}} V_1(l_0) h_k D_{je}(x)^{-\alpha}\right)\right], & N \text{ is odd, } k \text{ is } 0 \\ \mathbb{E}_{h,\gamma}\left[\exp\left(-\sum\limits_{x=-\frac{N-1}{2}}^{\frac{N-1}{2}} V_1(l_0) h_k D_{je}(x)^{-\alpha}\right)\right], & N \text{ is even, } k \text{ is } 0 \\ \mathbb{E}_{h,\gamma}\left[\exp\left(-\sum\limits_{x=-\frac{N-1}{2}}^{\frac{N-1}{2}} V_1(l_0) h_k D_{je}(x)^{-\alpha}\right)\exp\left(-\sum\limits_{y=-\frac{k-1}{2}}^{\frac{k-1}{2}} V_2(l_0) h_k D_{je}(y)^{-\alpha}\right)\right], & N \text{ is odd, } k \text{ is odd,} \\ \mathbb{E}_{h,\gamma}\left[\exp\left(-\sum\limits_{x=-\frac{N-1}{2}}^{\frac{N-1}{2}} V_1(l_0) h_k D_{je}(x)^{-\alpha}\right)\exp\left(-\sum\limits_{y=-\frac{k}{2}}^{\frac{k-2}{2}} V_2(l_0) h_k D_{je}(y)^{-\alpha}\right)\right], & N \text{ is odd, } k \text{ is even,} \\ \mathbb{E}_{h,\gamma}\left[\exp\left(-\sum\limits_{x=-\frac{N}{2}}^{\frac{N-2}{2}} V_1(l_0) h_k D_{je}(x)^{-\alpha}\right)\exp\left(-\sum\limits_{y=-\frac{k-1}{2}}^{\frac{k-1}{2}} V_2(l_0) h_k D_{je}(y)^{-\alpha}\right)\right], & N \text{ is even, } k \text{ is odd,} \\ \mathbb{E}_{h,\gamma}\left[\exp\left(-\sum\limits_{x=-\frac{N}{2}}^{\frac{N-2}{2}} V_1(l_0) h_k D_{je}(x)^{-\alpha}\right)\exp\left(-\sum\limits_{y=-\frac{k}{2}}^{\frac{k-2}{2}} V_2(l_0) h_k D_{je}(y)^{-\alpha}\right)\right], & N \text{ is even, } k \text{ is even,} \end{cases} \\ &= \begin{cases} \prod\limits_{x=-\frac{N-1}{2}}^{\frac{N-1}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V_1(l_0)D_{je}(x)^{-\alpha})} d\gamma, & N \text{ is odd, } k \text{ is } 0; \\ \prod\limits_{x=-\frac{N}{2}}^{\frac{N-2}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V_1(l_0)D_{je}(x)^{-\alpha})} d\gamma, & N \text{ is even, } k \text{ is } 0; \\ \prod\limits_{x=-\frac{N-1}{2}}^{\frac{N-1}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V_1(l_0)D_{je}(x)^{-\alpha})} d\gamma \cdot \prod\limits_{y=-\frac{k-1}{2}}^{\frac{k-1}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V_2(l_0)D_{je}(y)^{-\alpha})} d\gamma, & N \text{ is odd, } k \text{ is odd;} \\ \prod\limits_{x=-\frac{N-1}{2}}^{\frac{N-1}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V_1(l_0)D_{je}(x)^{-\alpha})} d\gamma \cdot \prod\limits_{y=-\frac{k}{2}}^{\frac{k-2}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V_2(l_0)D_{je}(x)^{-\alpha})} d\gamma & N \text{ is odd, } k \text{ is even.} \\ \prod\limits_{x=-\frac{N}{2}}^{\frac{N-2}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V_1(l_0)D_{je}(x)^{-\alpha})} d\gamma \cdot \prod\limits_{y=-\frac{k-1}{2}}^{\frac{k-1}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V_2(l_0)D_{je}(y)^{-\alpha})} d\gamma, & N \text{ is even, } k \text{ is odd;} \\ \prod\limits_{x=-\frac{N}{2}}^{\frac{N-2}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V_1(l_0)D_{je}(x)^{-\alpha})} d\gamma \cdot \prod\limits_{y=-\frac{k}{2}}^{\frac{k-2}{2}} \int_0^{\varphi} \frac{1}{\varphi(1+V_2(l_0)D_{je}(x)^{-\alpha})} d\gamma & N \text{ is even, } k \text{ is even.} \end{cases} \end{aligned} \tag{A6}$$

where $V_1(l_0) = \beta_p {l_0}^{\alpha} P_j G_s$, $V_2(l_0) = \beta_p {l_0}^{\alpha} P_j G_n$ and $G_n = G_m - G_s$.

After plugging Equations (25) and (A6) into the Equation (A5), and substituting the new expression of Equation (A5) into Equation (A4), we obtain the result of $\mathbb{P}_e$ in the following expression,

$$\mathbb{P}_e(N_d = k) = \left(\frac{2}{\pi R^2}\right)^M \cdot \int_D^{D+2R} \exp(-\beta_p {l_0}^{\alpha}\sigma^2) l_0 Z(l_0)^{M-1} W'(l_0,k) \arccos\left[\frac{D}{l_0} + \frac{{l_0}^2 - D^2}{2l_0(R+D)}\right] dl_0. \tag{A7}$$

Then we derive $\mathbb{P}_E$ in the DJF scheme. When there are k jammers interfering with the eavesdropper via main lobes, according to Total Probability Theorem, we have the following expression,

$$\mathbb{P}_E = \sum_{x=0}^{k} \mathbb{P}(N_d = x) \cdot \mathbb{P}_E(N_d = x). \tag{A8}$$

However, the premise of $k > 1$ is that both the number of jammers and the distance D between eavesdropper and the communication area are large. Since this situation seldom exists in real communication environment, we simplify the expression of $\mathbb{P}_{\mathbb{E}}$ by considering only two scenarios: $k = 0$ and $k = 1$. When there is more than one jammer interfering with the eavesdropper via its main lobe, we assume there is one jammer interfering with the eavesdropper via its main lobe. Then we have the upper bound of $\mathbb{P}_E$ as follows,

$$\mathbb{P}_E \approx \mathbb{P}(N_d = 0) \cdot \mathbb{P}_E(N_d = 0) + \mathbb{P}(N_d = 1) \cdot \mathbb{P}_E(N_d = 1). \tag{A9}$$

Since our result of $\mathbb{P}_E$ is a upper bound, the effect of the DFJ scheme on the eavesdropper in reality will be more highlighted.

From the geometrical relationship as given in Figure 3, we have $\gamma = \omega - \arcsin(R \sin \omega / L)$. We denote $\gamma_0 = \frac{\theta_m}{2} - \arcsin\left(R \sin\left(\frac{\theta_m}{2}\right) / L\right)$. When $\gamma > \gamma_0$, we have $\omega > \frac{\theta_m}{2}$, which means the eavesdropper locates in area A_0 and no jammer interferes with the eavesdropper via its main lobe. Since the degree γ is uniformly distributed, the result in Equation (A9) becomes

$$\mathbb{P}_E = \frac{\varphi - \gamma_0}{\varphi} \cdot \left[1 - \left(1 - \mathbb{P}_e(N_d = 0)\right)^M\right] + \frac{\gamma_0}{\varphi} \cdot \left[1 - \left(1 - \mathbb{P}_e(N_d = 1)\right)^M\right], \tag{A10}$$

where $\mathbb{P}_e(N_d = 0)$ and $\mathbb{P}_e(N_d = 1)$ can be calculated from Equation (A7). □

References

1. Yang, G.; He, S.; Shi, Z.; Chen, J. Promoting Cooperation by the Social Incentive Mechanism in Mobile Crowdsensing. *IEEE Commun. Mag.* **2017**, *55*, 86–92.
2. Han, G.; Liu, L.; Chan, S.; Yu, R.; Yang, Y. HySense: A hybrid mobile crowdsensing framework for sensing opportunities compensation under dynamic coverage constraint. *IEEE Commun. Mag.* **2017**, *55*, 93–99.
3. Datta, S.K.; da Costa, R.P.F.; Bonnet, C.; Hrri, J. oneM2M Architecture Based Iot Framework for Mobile Crowd Sensing in Smart Cities. In Proceedings of the 2016 European Conference on Networks and Communications (EuCNC), Athens, Greece, 27–30 June 2016.
4. Pilloni, V. How Data Will Transform Industrial Processes: Crowdsensing, Crowdsourcing and Big Data as Pillars of Industry 4.0. *Future Intern.* **2018**, *10*, 24.
5. Shu, L.; Chen, Y.; Huo, Z.; Bergmann, N.; Wang, L. When Mobile Crowd Sensing Meets Traditional Industry. *IEEE Access* **2017**, *5*, 15300–15307.
6. Li, T.; Jung, T.; Qiu, Z.; Li, H.; Cao, L.; Wang, Y. Scalable Privacy-Preserving Participant Selection for Mobile Crowdsensing Systems: Participant Grouping and Secure Group Bidding. *IEEE Trans. Netw. Sci. Eng.* **2018**, doi:10.1109/TNSE.2018.2791948.
7. Ma, L.; Liu, X.; Pei, Q.; Xiang, Y. Privacy-Preserving Reputation Management for Edge Computing Enhanced Mobile Crowdsensing. *IEEE Trans. Serv. Comput.* **2018**, doi:10.1109/TSC.2018.2825986.
8. Choo, K.; Gritzalis, S.; Park, J.H. Cryptographic Solutions for Industrial Internet-of-Things: Research Challenges and Opportunities. *IEEE Trans. Ind. Inform.* **2018**, doi:10.1109/TII.2018.2841049.
9. Zhang, N.; Cheng, N.; Lu, N.; Zhang, X.; Mark, J.W.; Shen, X. Partner Selection and Incentive Mechanism for Physical Layer Security. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 4265–4276.
10. 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 15), Oakland, CA, USA, 4–6 May 2015.
11. Zou, Y.; Zhu, J.; Yang, L.; Liang, Y.; Yao, Y. Securing physical-layer communications for cognitive radio networks. *IEEE Commun. Mag.* **2015**, *53*, 48–54.
12. Wang, W.; Sun, Z.; Piao, S.; Zhu, B.; Ren, K. Wireless Physical-Layer Identification: Modeling and Validation. *IEEE Trans. Inform. Forensics Secur.* **2016**, *11*, 2091–2106.
13. Mucchi, L.; Ronga, L.; Zhou, X.; Huang, K.; Chen, Y.; Wang, R. A New Metric for Measuring the Security of an Environment: The Secrecy Pressure. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 3416–3430.

14. 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.
15. Vilela, J.P.; Bloch, M.; Barros, J.; McLaughlin, S.W. Wireless Secrecy Regions with Friendly Jamming. *IEEE Trans. Inform. Forensics Secur.* **2011**, *6*, 256–266.
16. Hu, J.; Yan, S.; Shu, F.; Wang, J.; Li, J.; Zhang, Y. Artificial-Noise-Aided Secure Transmission with Directional Modulation Based on Random Frequency Diverse Arrays. *IEEE Access* **2017**, *5*, 1658–1667.
17. Zhang, X.; McKay, M.R.; Zhou, X.; Heath, R.W. Artificial-Noise-Aided Secure Multi-Antenna Transmission with Limited Feedback. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 2742–2754.
18. Zheng, T.X.; Wang, H.M. Optimal Power Allocation for Artificial Noise under Imperfect CSI Against Spatially Random Eavesdroppers. *IEEE Trans. Veh. Technol.* **2016**, *65*, 1658–1667.
19. Adams, M.; Bhargava, V.K. Using friendly jamming to improve route security and quality in ad hoc networks. In Proceedings of the 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE), Windsor, ON, Canada, 30 April–3 May 2017; pp. 1–6.
20. Dai, H.N.; Wang, Q.; Li, D.; Wong, R.C.W. On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas. *Int. J. Distrib. Sens. Netw.* **2013**, *9*, 760834.
21. Kim, M.; Hwang, E.; Kim, J. Analysis of eavesdropping attack in mmWave-based WPANs with directional antennas. *Wirel. Netw.* **2017**, *23*, 59–74.
22. MacDougall, J.A.; Buchholz, R.H. Cyclic Polygons with Rational Sides and Area. *J. Number Theory* **2008**, *128*, 17–48.
23. 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 ACM MOBIHOC, Hilton Head Island, SC, USA, 11–14 June 2012.
24. Singh, S.; Kulkarni, M.N.; Ghosh, A.; Andrews, J.G. Tractable Model for Rate in Self-Backhauled Millimeter Wave Cellular Networks. *IEEE J. Sel. Areas Commun.* **2015**, *33*, 2196–2211.
25. Wang, Q.; Dai, H.; Zheng, Z.; Imran, M.; Vasilakos, A. On Connectivity of Wireless Sensor Networks with Directional Antennas. *Sensors* **2017**, *17*, 134.
26. Mathai, A. *An Introduction to Geometrical Probability Distributional Aspects with Applications*; Gordon and Breach: Philadelphia, PA, USA, 1999.
27. Li, X.; Dai, H.N.; Wang, H.; Xiao, H. On Performance Analysis of Protective Jamming Schemes in Wireless Sensor Networks. *Sensors* **2016**, *16*, 1987.
28. Khalid, Z.; Durrani, S. Distance distributions in regular polygons. *IEEE Trans. Veh. Technol.* **2013**, *62*, 2363–2368.
29. Chen, L.; Wu, J.; Dai, H.N.; Huang, X. BRAINS: Joint Bandwidth-Relay Allocation in Multi-Homing Cooperative D2D Networks. *IEEE Trans. Veh. Technol.* **2018**, doi:10.1109/TVT.2018.2799970.
30. Berger, D.S.; Gringoli, F.; Facchi, N.; Martinovic, I.; Schmitt, J.B. Friendly jamming on access points: Analysis and real-world measurements. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 6189–6202.
31. Vo-Huu, T.D.; Vo-Huu, T.D.; Noubir, G. Interleaving Jamming in Wi-Fi Networks. In Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, Darmstadt, Germany, 18–20 July 2016.