Friendly-Jamming: An Anti-Eavesdropping Scheme in Wireless Networks of Things

Xuran Li*, Hong-Ning Dai*, and Hao Wang†
*Macau University of Science and Technology, Macau SAR
lxrget@163.com; hndai@ieee.org
†Norwegian University of Science and Technology, Aalesund, Norway
hawa@ntnu.no

***Abstract*—In this paper, we propose a novel anti-eavesdropping scheme by introducing friendly jammers to a wireless network of things (WNoT). In particular, we establish a theoretical framework to evaluate the eavesdropping risk of WNoT with friendly jammers and the eavesdropping risk of WNoT without jammers. Our theoretical model takes into account various channel conditions such as the path loss and Rayleigh fading as well as the placement schemes of jammers. Our extensive numerical results show that using jammers in WNoT can effectively reduce the eavesdropping risk. Besides, our results also show that the eavesdropping risk heavily depends on both the channel conditions and the placements of jammers.**

I. Introduction

Internet of Things (IoT) has received extensive attention from both academia and industry recently. There are a variety of IoT applications including environmental monitoring with wireless sensor networks [1], smart homes [2], logistic management with Radio-Frequency Identifications (RFIDs) [3], e-health [4], etc. The main idea of IoT is to interconnect various *smart* objects (i.e., the things) together and form a network of smart objects. In order to connect diverse smart objects ranging from ultra-lower RFID tags to sensors, actuators, mobile phones, smart appliances and healthcare devices, a number of wireless communication technologies (such as ISO/IEC 18000 [3], IEEE 802.15.4 [5], Bluetooth [6]) have been proposed to interconnect the smart devices to form a Wireless Net of Things (WNoT).

WNoT is especially susceptible to *passive eavesdropping attacks* due to the broadcast nature of wireless medium. Encryption is one of the most commonly used techniques to protect the confidential communications from wiretapping in wireless networks. However, encryption schemes may not be feasible to WNoT due to the following reasons: (a) the inferior computational capability of smart objects, (b) the limited battery power of smart objects (e.g., the passive RFIDs can only harvest the energy from the readers) and (c) the difficulty of managing the widely distributed smart objects in centralized manner, which is often the necessity for most of the encryption algorithms [7], [8]. There are some alternative remedies including (i) light-weight encryption algorithms to encrypt the communications between the transmitter and the receiver by exploiting the inherent channel randomness [9]–[11] and (ii) mitigating eavesdropping possibility by using power control schemes [12]. However, the schemes are still impractical to be implemented in WNoT due to the power, cost, computational constraints of smart objects. For example, to implement light-weight encryption schemes at RFID tags will translate them into more expensive, power-consuming tags, which are essentially against to the initiative of RFID technologies [13].

The effect of eavesdropping attacks under different channel conditions on WNoT is investigated in [14], however, no protective scheme for WNoT is proposed. In this paper, we propose a Friendly-Jamming (Fri-Jam) Anti-Eavesdropping Scheme to prevent eavesdropping activities in WNoT. The main idea of Fri-Jam is to introduce a small number of *friendly jammers* in WNoT, which can emit artificial noise so that sufficient interference will be generated to prevent eavesdroppers from snooping confidential communications. One of benefits of Fri-Jam is that the introduction of friendly jammers will not lead to any modifications on smart objects in WNoT. Recently, [15], [16] 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 since eavesdroppers can appear at any location (even inside a building). Besides, Pro-Jam is mainly focused on the power assignment in a specific scenario. To the best of our knowledge, *there is no study on theoretical analysis on the eavesdropping risk of WNoT with friendly-jamming schemes.*

This paper concentrates on establishing a general analytical model to evaluate the performance of Fri-Jam schemes. The primary research contributions of our paper can be summarized as follows.

- In particular, we propose a general theoretical model to analyze the eavesdropping probability of WNoT with two kinds of Fri-Jam schemes: random placement of jammers (Fri-Jam-Ran scheme) and regular placement of jammers (Fri-Jam-Reg scheme).
- We compare the eavesdropping probability of WNoT without jammers with that with friendly jammers (Fri-Jam-Ran and Fri-Jam-Reg schemes). We find that *using friendly jammers in WNoT can effectively reduce the eavesdropping probability*.
- Our results also show that to place friendly jammers in WNoT appropriately will just slightly decrease the

transmission probability while the decrement on the transmission probability is less significant than the decrement on the eavesdropping probability.

The remaining paper is organized as follows. We first present the system model and the problem formulation in Section II. Section III then presents the main results. We next show numerical results in Section IV. Finally, the paper is concluded in Section V.

II. System Models

A. Fri-Jam Schemes

In this paper, we assume that the network is placed in a torus [17]. 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 [12], 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. In this paper, we consider two placement strategies of friendly jammers in WNoT: (i) Fri-Jam-Reg scheme, in which jammers are regularly placed at deterministic locations and (ii) Fri-Jam-Ran scheme, in which jammers are regularly placed at random locations. Specifically, in Fri-Jam-Ran scheme, friendly jammers are regularly placed in a grid manner. In Fri-Jam-Ran scheme, friendly jammers are randomly distributed according to homogeneous Poisson point process (PPP). We denote the conventional scheme without friendly jammers by Non-Jam scheme in order to compare with our proposed Fri-Jam schemes.

B. 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

$$\mathrm{SINR} = \frac{hr^{-\alpha}}{\sigma^2 + I_t + I_j}, \tag{1}$$

where σ^2 is the noise power, $I_t = \sum_{i \in \Phi / t_0} h_i R_i^{-\alpha}$ denotes the cumulative interference from all the legitimate users (except for the transmitter denoted by t_0), Φ denotes the set of legitimate users 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 derived in Section III.

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 $\mathrm{SINR} > T$, where T is the received power threshold that an eavesdropper can successfully decode the transmission.

C. 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.

In order to derive $P(E)$, we need to calculate the probability that one transmission has been eavesdropped, which is denoted by P_e. 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 $\mathrm{SINR} > \beta$ at the legitimate receiver, where β is the threshold value of the receiving power for a successful reception. Thus, we have $P(C) \triangleq P(\mathrm{SINR} > \beta)$. Following a similar approach to [18], we can obtain $P(C)$. Without the repetition, we omit the detailed derivations of $P(C)$ in this paper.

III. Analysis on Eavesdropping Probability

A. Analysis of Non-Jam Scheme

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

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

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

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

Proof: We denote the distance between the eavesdropper and its nearest transmitter by r. The probability density function (PDF) of r can be derived according to Poisson distribution of transmitters as the following steps.

Firstly, we have the probability that no transmitter 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

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

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

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

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

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

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

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

More specifically, we have

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

Substituting variable $\mu = (\frac{v}{rT^{1/\alpha}})^2$, we then have

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

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

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).

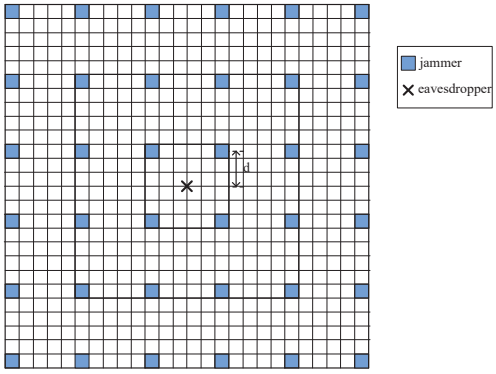


Fig. 1. Fri-Jam-Reg Scheme: every jammer is placed at a gray square. Note that we only show a part of the whole network.

B. Analysis of Fri-Jam Schemes

Recall that we consider two placement schemes of friendly jammers: Fri-Jam-Reg and Fri-Jam-Ran. Thus, we categorize our analysis into the following cases.

Case I: Fri-Jam-Reg Scheme

We first analyze the case of Fri-Jam-Reg, in which all the jammers are regularly placed in grid manner as shown in Fig. 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

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

Proof: 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 Fri-Jam-Reg scheme, the probability P_e that one transmission has been eavesdropped is

$$P_e = \int_{r>0} e^{-\mu Tr^{\alpha}(\sigma^2 + E_j) - \pi r^2 \lambda(\rho(T,\alpha)+1)} 2\pi\lambda r dr, \tag{9}$$

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

Proof: First, the SINR of the receiver 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

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

According to the channel model (given in Section II-B), we have

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

where $L(\mu T r^{\alpha}) = \exp(-\pi r^2 \lambda \rho(T,\alpha))$, $\rho(T,\alpha) = T^{-2/\alpha} \int_T^{\infty} \frac{1}{1+(\mu)^{\alpha/2}} d\mu$ and $E[I_j]$ is given by Eq. (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 IV will give the numerical results that will further confirm this observation.

Case II: Fri-Jam-Ran Scheme

We then analyze the case of Fri-Jam-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 PPP density of legitimate users by λ_1 and the PPP density of friendly jammers by λ_2. Based on the well-known stochastic geometric results [18], we can obtain Theorem 3 on the probability P_e that one transmission has been eavesdropped as follows.

Theorem 3: In Fri-Jam-Ran scheme, the probability P_e that one transmission has been eavesdropped is

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

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

Proof: According to the channel model defined in Section II-B, we have the

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

Following the similar analysis process to [18], we then have

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

Substituting $P[h > T r^{\alpha}(\sigma^2 + I_t + I_j)|r]$ in Eq. (10) by RHS of Eq. (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.

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

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

where P_e is given by Theorem 1, Theorem 2 and Theorem 3 in Non-Jam scheme, Fri-Jam-Reg scheme and Fri-Jam-Ran scheme, respectively. In next section, we will present numerical results of $P(E)$ based on the above schemes.

IV. Numerical Results

A. Comparisons of different schemes

In the first set of results, we compare the probability of eavesdropping attacks $P(E)$ of Fri-Jam-Ran scheme with that of Non-Jam scheme. Note that the larger node density λ_2 in Fri-Jam-Ran scheme and the smaller d in Fri-Jam-Reg scheme imply the higher cost (i.e., more jammers are deployed in the network). As shown in Fig. 2, the results of Non-Jam scheme are shown in a dash curve and the results of Fri-Jam-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 Fig. 2 that Non-Jam scheme always has higher values of $P(E)$ than Fri-Jam-Ran scheme, implying that *using friendly jammers in WNoT can effectively reduce the probability of eavesdropping attacks*.

It is also shown in Fig. 2 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 $T = 5\text{dB}$ (as shown in Fig. 2 (b)), P_E of Non-Jam scheme is 0.719 while P_E of Fri-Jam-Ran scheme is reduced to 0.393 with jammers density $\lambda_2 = 0.8$ and 0.211 with jammers density $\lambda_2 = 2.0$.

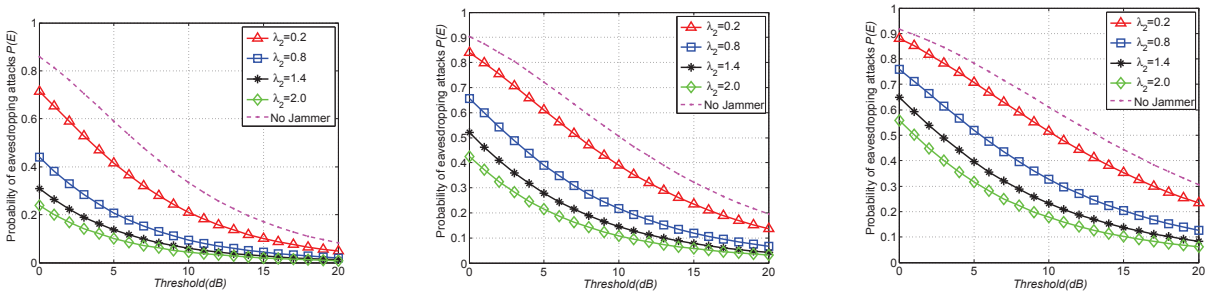
In the second set of results, we compare the probability of eavesdropping attacks $P(E)$ of Fri-Jam-Reg scheme with that of Non-Jam scheme. Fig. 3 shows the results, where a dash curve represents $P(E)$ of Non-Jam scheme and solid curves with markers depict the results of Fri-Jam-Reg scheme. Similar to Fig. 2, we find that using friendly jammers can always reduce the eavesdropping probability compared with the Non-Jam scheme. Moreover, it is shown in Fig. 3 that the probability of eavesdropping attacks $P(E)$ heavily depends on both the channel conditions and system parameter d. Specifically, it is shown in Fig. 3 (b) that the probability of eavesdropping attack P_E decreases with the decreased values of d. In fact, the d in Fri-Jam-Reg scheme plays a similar role to jammer density λ_2 in Fri-Jam-Ran scheme. In other words, decreasing d is equivalent to the effect of increasing jammer density λ_2. Take Fig. 3 (b) as an example again. When the threshold is $T = 5\text{dB}$ 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.

B. 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.

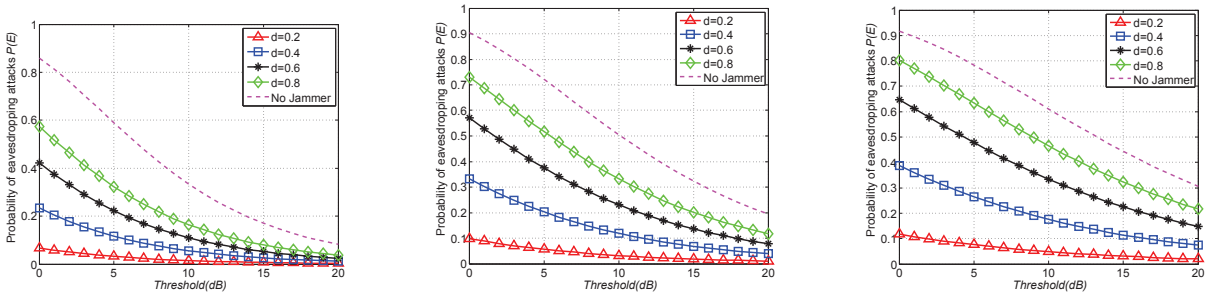
Definition 4: Eavesdropping deviation $\mathcal{D}_E$ is equal to the difference between the eavesdropping probability $P(E)$ without jammers and the eavesdropping probability $P(E)$ with jammers.

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.



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

Fig. 2. Probability of eavesdropping attacks $P(E)$ with Fri-Jam-Ran scheme (PPP) versus Non-Jam scheme when $\alpha = 3, 4, 5$ with SINR threshold T ranging from 0 dB to 20 dB.



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

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

We then derive the eavesdropping deviation $\mathcal{D}_E$ and the transmission deviation $\mathcal{D}_C$ in the first case of comparing Fri-Jam-Ran scheme with Non-Jam scheme. In particular, we have $\mathcal{D}_E(\text{Ran}) = P_{\text{Non-Jam}}(E) - P_{\text{Fri-Jan-Ran}}(E)$, where $P_{\text{Non-Jam}}(E)$ denotes the eavesdropping probability of Non-Jam scheme and $P_{\text{Fri-Jan-Ran}}(E)$ denotes the eavesdropping probability of Fri-Jam-Ran scheme. Besides, we have $\mathcal{D}_C(\text{Ran}) = P_{\text{Non-Jam}}(C) - P_{\text{Fri-Jan-Ran}}(C)$, where $P_{\text{Non-Jam}}(C)$ denotes the transmission probability of Non-Jam scheme and $P_{\text{Fri-Jan-Ran}}(C)$ denotes the transmission probability of Fri-Jam-Ran scheme. Note that $P(C)$ can be calculated by [18] and we omit the detailed derivations in this paper.

Table I shows the comparison results. As shown in Table I, the eavesdropping deviation is much larger than the transmission deviation at the same network settings, implying that *using jammers in WNoT will not significantly affect the legitimate communications* compared with the reductions on the eavesdropping probability. For example, when $\lambda_2 = 2.0$, $\mathcal{D}_E = 0.5178$, implying that there is nearly 52% reduction on the eavesdropping probability while there is less than 10% reduction on the transmission probability (i.e., $\mathcal{D}_C = 0.0963$).

Similarly, we derive derive the eavesdropping deviation $\mathcal{D}_E$ and the transmission deviation $\mathcal{D}_C$ in the second case of comparing Fri-Jam-Reg scheme with Non-Jam scheme. Table II shows the comparison results. It is shown in Table II that Fri-Jam-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 67% while the reduction of $P(C)$ is only 11% when $d = 0.2$).

TABLE I
EAVESDROPPING DEVIATION AND TRANSMISSION DEVIATION OF COMPARING FRI-JAM-RAN SCHEME WITH NON-JAM SCHEME WHEN $T = 10$dB AND $\alpha = 4$.

Density λ_2	Eavesdropping deviation $\mathcal{D}_E(\text{Ran})$	Transmission deviation $\mathcal{D}_C(\text{Ran})$
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 II
EAVESDROPPING DEVIATION AND TRANSMISSION DEVIATION OF COMPARING FRI-JAM-REG SCHEME WITH NON-JAM SCHEME WHEN $T = 10$dB AND $\alpha = 4$.

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

V. CONCLUSION

In this paper, a novel anti-eavesdropping scheme has been proposed to mitigate the eavesdropping attacks in Wireless Network of Things (WNoT). In particular, we analyze the eavesdropping probability with consideration of various channel conditions (such as Rayleigh fading and the path loss effect) and the placement of friendly jammers (such as regular

placement of jammers and random placement of jammers). One of our major findings is that to introduce friendly jammers in WNoT can significantly reduce the eavesdropping probability without the significant influence on the legitimate communications. One of the future directions is to improve our friendly-jamming schemes so that the eavesdropping probability can be further reduced while maintaining the lowest influence on the legitimate communications. This goal can be achieved by controlling power [12] or placing jammers at the specific locations (such as the network boundary) [15].

ACKNOWLEDGEMENT

The work described in this paper was partially supported by Macao Science and Technology Development Fund under Grant No. 096/2013/A3. The authors would like to thank Gordon K.-T. Hon for his constructive comments.

APPENDIX A

Proof of Lemma 1

We consider a coordinate system that is centered at the eavesdropper as shown in Fig. 1. Since jammers are placed in a grid, each friendly jammer is $2d$ away from its nearest neighbor in the same axis. From the channel model defined in Section II-B, 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,

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

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

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

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

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

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

$$\begin{aligned} I_j(n-1) \;=\; & 4\Bigg\{2\cdot\Bigg[\Big(d\cdot\sqrt{1+(2n-3)^2}\Big)^{-\alpha} + \\ & \Big(d\cdot\sqrt{9+(2n-3)^2}\Big)^{-\alpha} + \cdots + \\ & \Big(d\cdot\sqrt{(2n-5)^2+(2n-3)^2}\Big)^{-\alpha}\Bigg] + \\ & \Big(d\cdot\sqrt{2(2n-3)^2}\Big)^{-\alpha}\Bigg\}. \end{aligned} \tag{12}$$

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

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

Summarizing them all, we then have

$$\begin{aligned} I_j(n) \;=\; & 4\Big\{2\cdot\sum_{k=1}^{n}\Big(d\cdot\sqrt{(2k-3)^2+(2k-1)^2}\Big)^{-\alpha} \\ & +\Big(d\cdot\sqrt{2(2k-1)^2}\Big)^{-\alpha}\Big\}. \end{aligned} \tag{13}$$

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. □

REFERENCES

[1] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292 – 2330, 2008.

[2] C. Dixon, R. Mahajan, S. Agarwal, A. Brush, B. Lee, S. Saroiu, and P. Bahl, "An operating system for the home," in *NSDI*. USENIX, April 2012.

[3] "ISO/IEC 18000," 2013. [Online]. Available: http://en.wikipedia.org/wiki/ISO/IEC_18000

[4] K. Habib, A. Torjusen, and W. Leister, "Security Analysis of a Patient Monitoring System for the Internet of Things in eHealth," in *The Seventh International Conference on eHealth, Telemedicine, and Social Medicine (eTELEMED)*, 2015.

[5] "IEEE 802.15.4," 2011. [Online]. Available: http://standards.ieee.org/getieee802/download/802.15.4-2011.pdf

[6] "Bluetooth Core Specification 4.2," 2014. [Online]. Available: http://www.bluetooth.org/

[7] D. Wagner, B. Schneier, and J. Kelsey, "Cryptanalysis of the cellular message encryption algorithm," in *Advances in Cryptology–CRYPTO '97*, 1997.

[8] "IEEE 802.11i-2004." [Online]. Available: http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[9] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel," in *Proceedings of ACM MobiCom*, 2008.

[10] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Communications*, vol. 18, no. 4, pp. 6–12, 2011.

[11] M. Zafer, D. Agrawal, and M. Srivatsa, "Limitations of Generating a Secret Key Using Wireless Fading Under Active Adversary," *IEEE/ACM Transactions on Networking*, vol. 20, no. 5, pp. 1440–1451, 2012.

[12] J.-C. Kao and R. Marculescu, "Minimizing Eavesdropping Risk by Transmission Power Control in Multihop Wireless Networks," *IEEE Transactions on Computers*, vol. 56, pp. 1009 – 1023, 2007.

[13] H. Hassanieh, J. Wang, D. Katabi, and T. Kohno, "Securing rfids by randomizing the modulation and channel," in *12th USENIX Symposium on Networked Systems Design and Implementation (NSDI 15)*, May 2015.

[14] X. Li, H. Wang, H.-N. Dai, Y. Wang, and Q. Zhao, "An Analytical Study on Eavesdropping Attacks in Wireless Nets of Things," *Mobile Information Systems*, vol. 2016, 2016.

[15] S. Sankararaman, K. Abu-Affash, A. Efrat, S. D. Eriksson-Bique, V. Polishchuk, S. Ramasubramanian, and M. Segal, "Optimization schemes for protective jamming," in *Proceedings of ACM MOBIHOC*, 2012.

[16] Y. S. Kim, P. Tague, H. Lee, and H. Kim, "A jamming approach to enhance enterprise wi-fi secrecy through spatial access control," *Wirel. Netw.*, pp. 2631–2647, Nov. 2015.

[17] A. E. Gamal, J. Mammen, B. Prabhakar, and D. Shah, "Optimal throughput-delay scaling in wireless networks-part I: The fluid model," *IEEE Transactions on Information Theory*, vol. 52, no. 6, pp. 2568–2592, 2006.

[18] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Transactions on Communications*, pp. 3122 – 3134, Nov. 2011.