UAV-enabled Friendly Jamming Scheme to Secure Industrial Internet of Things

Qubeijian Wang, Hong-Ning Dai, Hao Wang, Guangquan Xu, and Arun Kumar Sangaiah

Abstract: **Eavesdropping is a critical threat to the security of industrial Internet of things (IIoT) since many malicious attacks often follow eavesdropping activities. In this paper, we present an anti-eavesdropping scheme based on multiple unmanned aerial vehicles (UAVs) who emit jamming signals to disturb eavesdropping activities. We name such friendly UAV-enabled jamming scheme as Fri-UJ scheme. In particular, UAV-enabled jammers (UJs) emit artificial noise to mitigate the signal to interference plus noise ratio (SINR) at eavesdroppers consequently reducing the eavesdropping probability. In order to evaluate the performance of the proposed Fri-UJ scheme, we establish a theoretical framework to analyze both the local eavesdropping probability and the overall eavesdropping probability. Our analytical results show that the Fri-UJ scheme can significantly reduce the eavesdropping risk while having nearly no impact on legitimate communications. Meanwhile, the simulation results also agree with the analytical results, verifying the accuracy of the proposed model. The merits of Fri-UJ scheme include the deployment flexibility and no impact on legitimate communications.**

Index Terms: **Eavesdropping, Internet of things, jamming, security, unmanned aerial vehicles.**

I. INTRODUCTION

THE modern industry is experiencing a paradigm shift from computer-aided industry to "smart industry" [1]. During the evolution, industrial Internet of things (IIoT) plays a critical role of connecting the physical objects in industry environment into Internet with provision of various smart-decision services to users [2], [3]. Various devices in IIoT including sensors, actuators, IoT gateways, RFID tags, access points (APs) connect together via wireless or wired links.

The broadcast nature of wireless communications in IIoT leads to the vulnerability of information leakage. Conventional wireless networks such as wireless LAN typically exploit encryption protocols to protect confidential information. However, recent studies [4]–[8] show that wireless security protocols in IoT still contain a number of vulnerabilities. Recently, the work of [9] shows that machine learning (ML) based methods can extract confidential information via learning a large number of encrypted transmission messages. On the other hand, encryption schemes may not be applicable to IIoT scenarios where IoT devices have limited computational capability and battery storage.

In addition to security vulnerabilities, IIoT is also suffering from privacy exposure. For example, human behavior recognition based on radio frequency (RF) sensing has received extensive attention recently [10], [11]. The human action can be captured through analyzing the reflected RF signals from a human body. However, it is shown in recent work [12] that the human behavior information can easily leak out to malicious users. In this scenario, conventional encryption schemes cannot prevent the privacy exposure.

A. Motivation

Unlike conventional encryption approaches, friendly-jamming schemes are a promising solution to secure IIoT while causing no significant cost for computational-extensive tasks typically required by encryption approaches. The aim of the friendly jamming scheme is to reduce the probability of confidential information being wiretapped by eavesdroppers through mitigating the signal to interference plus noise ratio (SINR) at eavesdroppers.

Recently, unmanned aerial vehicles (UAVs) have also been applied in wireless communications to substitute some disrupted fixed transmitting nodes. For example, studies [13], [14] explore using UAVs to construct emergency communication networks. Meanwhile, drone small cells (DSCs) consisting of multiple UAVs called aerial base stations are used to support air communications [15]. Moreover, DSCs can also be used to support device-to-device (D2D) communications in [16]. Reference [17] shows that UAV-enabled base stations can be deployed in next-generation cellular networks. Furthermore, it is shown in [18] that a UAV can be used as a relay to support communications in mountainous terrain.

In this paper, we exploit UAVs as friendly jammers who emit artificial noise to disturb eavesdroppers from wiretapping confidential information. We name such UAV-enabled jammers as UJs. In each UJ, a directional antenna is mounted. The anti-eavesdropping scheme based on UAV-enabled jammers is named as Fri-UJ scheme. Fig. 1 shows an application example of Fri-UJ deployed in a factory. In the factory, industrial data has been collected by various IoT nodes through IoT gateways or APs. Meanwhile, an eavesdropper who is not permitted to enter the factory can wiretap the confidential industrial data in a wireless manner. When Fri-UJ scheme is deployed, a number of

Manuscript received February, 17, 2019.

This paper was supported by Macao Science and Technology Development Fund under Grant No. 0026/2018/A1, the State Key Development Program of China under Grant No. 2017YFE0111900, National Science Foundation of China under Grant No. 61572355, 61672170, U1736115. The authors would like to thank G. K.-T. Hon for his suggestions.

Q. Wang and H.-N. Dai are with the Faculty of Information Technology, Macau University of Science and Technology, Macau SAR, email: qubeijian.wang@gmail.com and hndai@ieee.org.

H. Wang is Department of Computer Science, Norwegian University of Science and Technology, Gjøvik, Norway, email: hawa@ntnu.no.

G. Xu is College of Intelligence and Computing, Tianjin University, Tianjin, China, email: losin@tju.edu.cn.

A. K. Sangaiah is School of Computing Science and Engineering, VIT University, Vellore, India, email: arunkumarsangaiah@gmail.com.

H.-N. Dai and H. Wang are the corresponding authors.

Digital Object Identifier: 10.1109/JCN.2019.000042

1229-2370/19/$10.00 © 2019 KICS

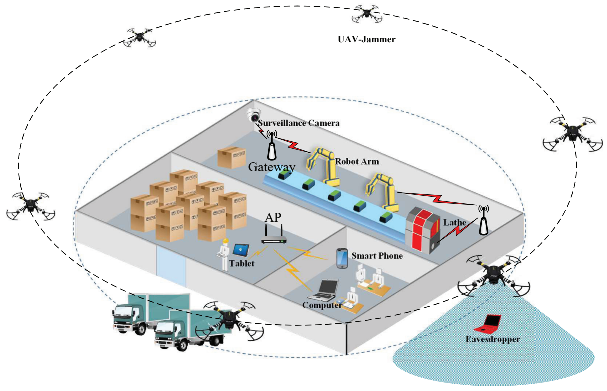


Fig. 1. Fri-UJ application scenario.

UJs flying over can emit artificial noise to disturb the eavesdropping activities consequently securing the communications in the factory.

B. Contributions

Comparing with prior friendly-jamming schemes, the Fri-UJ scheme has many advantages. First, the Fri-UJ does not affect legitimate communications owing to directional transmission of the artificial noise of UJs. Since the transmission direction of the artificial noise is towards to ground, there is almost no interference at legitimate users. Second, the Fri-UJ scheme is flexible to construct protection area thanks to the mobility of UAVs. After one protection task is completed, the UJs can move to another site to protect confidential communications. The flexible deployment of UJs can also reduce the constructing cost compared with fixed placements of jammers in prior friendly-jamming schemes.

The major research contributions of this paper can be summarized as follows.

- We propose Fri-UJ scheme to secure confidential communications in IIoT and prevent eavesdroppers from wiretapping.
- We establish an analytical framework to evaluate the effectiveness of Fri-UJ scheme. We consider both the local eavesdropping probability and the overall eavesdropping probability.
- We conduct extensive simulations to validate the effectiveness of our proposed model. The simulation results match the analytic results, indicating that our proposed model is accurate. Moreover, our results also show that Fri-UJ scheme can significantly decrease the eavesdropping risk compared with non-jamming scheme in which no UJs are deployed.

The rest of the paper is organized as follows: We summarize the related works in Section II. Section III then presents system model and Section IV gives the performance analysis of Fri-UJ scheme. We next present simulation results in Section V. Finally, the paper is concluded in Section VI.

II. RELATED WORK

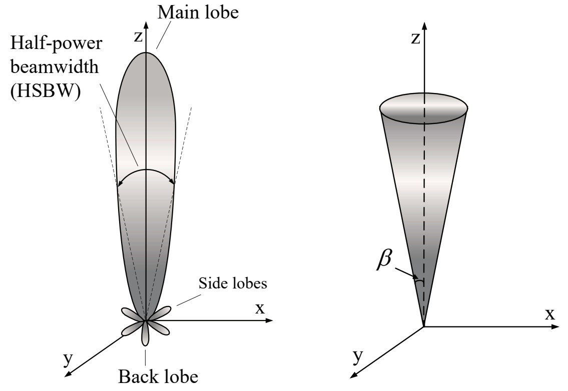
Security is a critical issue in IIoT. IIoT technology is enabling “smart industry” with communications, information sharing and data collection. During this procedure, ensuring data security and reliability is of great significance. There are different kinds of security problems in IIoT. We roughly categorize the security concerns of IIoT into internal and external issues.

The internal security problems in IIoT usually include authentication and authorization, lightweight cryptosystems and security protocols, and software vulnerability and backdoor analysis [19]–[21]. Efficient authentication and authorization can ensure the legitimate users to access the networks. However, the common agreements or standards are still vacant for authentication and authorization. New authentication and authorization mechanisms are continuously proposed (e.g., a lightweight authentication mechanism was proposed in [22]). Meanwhile, the limited computing capability restricts IIoT devices to enforce complex cryptosystems and security protocols. Thus, IIoT usually choose lightweight cryptosystems and security protocols, such as a lightweight certificateless signature scheme in [23]. Moreover, software vulnerability and backdoor analysis can also result in the malicious attacks of IIoT systems.

The external security problems in IIoT come from external threats, e.g., eavesdropping attacks, which are often the prerequisite for other malicious attacks. It is difficult to detect eavesdropping attacks in IIoT since eavesdroppers passively wiretap the confidential communications with concealment of their presence. The common technique to protect confidential communications is encryption. However, cryptosystems can only help hiding the meaning of information during transmissions, but not the existence of the information itself. In addition, even though cryptosystems increase the difficulty of understanding the true meaning of information for eavesdroppers, it is still possible for the eavesdroppers to access all the information as indicated in [24]. The reason may owe to the lightweight cryptosystems that have only been used in IIoT because of in sufficient computing capability IIoT devices.

Recently, the physical-layer countermeasures have been considered to confront eavesdropping activities in IIoT. The core idea of physical-layer countermeasures is to degrade the receiving signal at the eavesdroppers. There are two types of physical-layer countermeasures: power control and friendly jamming. One power control method was proposed to reduce the receiving power of malicious users by controlling transmission power appropriately [25]. However, it is shown in [26] that the power control scheme can also affect the legitimate communications. The friendly jamming schemes have attracted extensive attention recently [27]–[32]. Friendly jamming schemes aim at increasing the interference at malicious users [27], [33]. Most of friendly-jamming schemes assume to place single or multiple jammers who emit artificial noise to interfere with the wiretapping activities of eavesdroppers. However, they have the following limitations: 1) The fixed placement of jammers causes high construction cost; 2) the jamming signal can also affect legitimate communications (if jammers are not properly placed); 3) most of them can only be used for a specific application scenario (e.g., a warehouse).

In this paper, we propose Fri-UJ scheme to address the above concerns of current friendly-jamming schemes.



(a) (b)

Fig. 2. Antenna model: (a) Realistic antenna model and (b) sector antenna model.

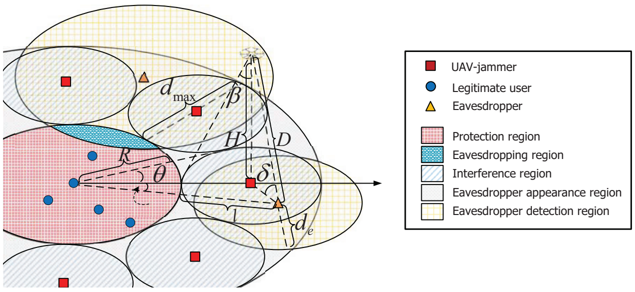


Fig. 3. Calculation details of Fri-UJ scheme.

Table 1. Definitions of regions.

Region name	Definition
Protection region	The region where the legitimate users appear
Eavesdropper appearance region	The region where the eavesdropper appear
Interference region	The region where can receive the artificial noise from UJs
Eavesdropper detection region	The region where the eavesdropper can wiretap legitimate communications
Eavesdropping region	The intersection of *eavesdropper detection region* and *protection region*

III. SYSTEM MODEL

In this section, we present directional antenna in Section III.A, network model in Section III.B, channel model in Section III.C and deployment of UJs in Section III.D.

A. Directional Antenna

A realistic directional antenna includes one main lobe with the highest antenna gain and a number of side lobes as well as back lobes with extremely low antenna gain, as shown in Fig. 2(a). However, it is complicated to conduct analysis based on realistic antenna models as indicated in [34]. Commonly, a sector antenna model is one of typical simplify antenna models [35]. Fig. 2(b) shows an example of sector antenna models, in which there is only one main beam with antenna gain g in the sector model. Generally, $g = 29000/\beta^2$, and β is a half of the antenna beamwidth.

B. Network Model

Fig. 3 shows an example of the network model of our Fri-UJ scheme. In particular, there is a *protection region* with radius R where the legitimate users are randomly distributed according to homogeneous poisson point process (HPPP) with the density of λ. We assume that eavesdroppers can only appear outside the protection region due to the access control (e.g., locking the door, building a fence around the protection region). A ring region surrounding the protection region is named as the *eavesdropper appearance region* where the eavesdropper has a chance to wiretap the legitimate communications. The distance between the eavesdropper and the boundary of the protection region is l.

In our Fri-UJ scheme, a number of UJs flying on the air emit the artificial noise from air to ground to disrupt the wiretapping activity. The region affected by the artificial noise emitted from UJs is named as the *interference region* which are essentially the circles projected on the ground, as shown in Fig. 3. From the perspective of an eavesdropper, there is a detection region in which the legitimate communication can be wiretapped. However, since the legitimate users only appear at the *protection region*, only the legitimate users within the intersection of *eavesdropper detection region* and *protection region* should be analyzed. We name such intersection of *eavesdropper detection region* and *protection region* as *eavesdropping region*. Table 1 summarizes the definitions of the above regions which will be used for the performance analysis of our Fri-UJ scheme.

C. Channel Model

In this paper, we consider two channel models: 1) Ground communication model; 2) air-to-ground communication model [35]–[37], which are introduced as follows.

We model the transmission between the legitimate users and the eavesdropper as the *ground communication*. We assume that the radio channel of the ground communication is mainly affected by Rayleigh fading and path loss. The transmitting power of legitimate user is P_t. Thus the received power is $P_t h d^{-\alpha}$ when the distance from the legitimate user to the eavesdropper is d. The random variable h follows an exponential distribution with mean value $1/\mu$ and α is the path loss factor.

The interference between the UJs and the eavesdropper is modeled as the *air-to-ground communication*. The air-to-ground communication is usually divided into light of sight (LoS) link and none light of sight (NLoS) link. We assume that the LoS link experiences path loss, and the NLoS link experiences path loss and Rayleigh fading [37]. The transmitting power of the UJs is P_j. The distance from the closest UJ to the eavesdropper is D. The random variable h_j follows an exponential distribution with mean value $1/\mu_j$ and α_j is the path loss factor. Thus, the received interference power of eavesdropper can be expressed as

$$I = \begin{cases} P_j g D^{-\alpha_j}, & \text{LoS link} \\ P_j g h_j D^{-\alpha_j}, & \text{NLoS link} \end{cases}, \tag{1}$$

We use signal-to-interference-noise-ratio (SINR) to evaluate the quality of the received signal. In particular, the SINR at the eavesdropper must be larger than SINR threshold T_e to guarantee that the eavesdropper can successfully wiretap the confidential information. In other words, we have the following expression,

$$\mathsf{SINR} = \frac{\mathsf{P_t h d^{-\alpha}}}{\sigma^2 + \mathsf{I_j}} \geq \mathsf{T_e}, \tag{2}$$

where σ^2 is the Gaussian noise power and I_j is the interference from the UJs.

D. Deployment of UJs

In our Fri-UJ scheme referring to Fig. 3, UJs are uniformly deployed around the boundary of the protection region and the total number of UJs is N. These UJs fly on the air with the same flight height H. The deployment of the UJs is highly related to the area of *eavesdropper appearance region*, as shown in Fig. 3. In our Fri-UJ scheme, the UJs need to cover *eavesdropper appearance region* as much as possible so as to reduce the eavesdropping risk. In an extreme case in which a legitimate user falls at the edge of the protection region and there is no external interference, the maximum eavesdropper detection distance is essentially the width of *eavesdropper appearance region* (i.e., a ring) denoted by $d_{\max}$ which can be calculated as follows,

$$d_{\max} = \mathbb{E}\left[\frac{P_t h}{\sigma^2 T_e}\right]^{1/\alpha} = \frac{1}{\alpha} \cdot \left[\frac{P_t}{\mu\sigma^2 T_e}\right]^{\frac{1}{\alpha}} \cdot \Gamma\Big(\frac{1}{\alpha}\Big), \tag{3}$$

where $\mathbb{E}(\cdot)$ denotes the expectation and $\Gamma(\cdot)$ denotes the standard gamma function.

The number of deployed UJs is highly related to the radius of the protection region R and the width of the *eavesdropper appearance region* $d_{\max}$. As shown in Fig. 3, the diameter of each interference region circle is equal to $d_{\max}$ so as to cover the maximum *eavesdropping appearance region.* According to the triangle relation shown in Fig. 3, $\theta = \arcsin\left(d_{\max}/(2R + d_{\max})\right)$. Meanwhile, each circle of *interference region* falls into the included angle of 2θ as shown in Fig. 3. Therefore, the number of UJs can be calculated as follows,

$$N = \left\lceil \frac{\pi}{\theta} \right\rceil = \left\lceil \frac{\pi}{\arcsin\left(\frac{d_{\max}}{2R+d_{\max}}\right)} \right\rceil. \tag{4}$$

The flight height of the UJs denoted by H is related to the width of the eavesdropper appearance region $d_{\max}$ and the half beamwidth of direction antenna β on UJ. According to the triangle relation as shown in Fig. 3, the flight height is expressed as follows,

$$H = \frac{d_{\max}}{2\tan\beta}. \tag{5}$$

IV. PERFORMANCE ANALYSIS

In this section, we evaluate the performance of the proposed Fri-UJ scheme in terms of eavesdropping risk. In particular, we first present the eavesdropping probability as the performance measure of eavesdropping risk in Section IV.A. We then analyze the eavesdropping probability of Fri-UJ scheme in Section IV.B. We next give a discussion on the impact of Fri-UJ scheme on legitimate communications in Section IV.C.

A. Eavesdropping Probability

Eavesdropping risk is of great importance to evaluate the security of wireless networks [38]. We exploit the *eavesdropping probability* to evaluate the eavesdropping risk in this paper. The eavesdropping probability is defined as the probability that at least one legitimate communication is wiretapped by the eavesdropper. In particular, we consider both the *local eavesdropping probability* and the *overall eavesdropping probability* (denoted by $\mathbb{P}_E$).

We first give the definition of *local eavesdropping probability* (denoted by $\mathbb{P}_e$) as follows.

Definition 1: The *local eavesdropping probability* is the probability that at least one legitimate communication is wiretapped by the eavesdropper (i.e., at least one legitimate user locates in the eavesdropper detection region).

The eavesdropper can successfully wiretap the legitimate communication if and only if at least one legitimate user falls in the eavesdropper detection region. On the other hand, the legitimate users can only appear in the protection region. Therefore, there are at least one legitimate users falling into the intersection of eavesdropper detection region and protection region. This intersection region is named as the eavesdropping region (as defined in Table 1). Since the legitimate users are randomly distributed according to HPPP with density of λ, the probability of k legitimate users being wiretapped is expressed as: $\mathbb{P}(x = k) = ((\lambda A)^k/k!)e^{-\lambda A}$. According to Definition 1, the local eavesdropping probability $\mathbb{P}_e$ is given by the following equation,

$$\mathbb{P}_e = 1 - \mathbb{P}(x = 0) = 1 - e^{-\lambda A}, \tag{6}$$

where A is the area of the eavesdropping region to be calculated in the next subsections.

The eavesdropper is randomly distributed in the eavesdropper appearance region. Each appearance of the eavesdropper results in the different value of local eavesdropping probability. In order to evaluate the overall performance of a jamming scheme, we consider the eavesdropping probability of all the possible appearance locations of eavesdroppers. In particular, we define the overall eavesdropping probability denoted by $\mathbb{P}_E$ as follows.

Definition 2: The *overall eavesdropping probability* is the probability that one legitimate communication is eavesdropped by the eavesdropper at every appearance location.

Essentially, the overall eavesdropping probability is the sum of the local eavesdropping probability when the eavesdropper appears in every location in the eavesdropper appearance region. Therefore, $\mathbb{P}_E$ is expressed as the following integration,

$$\begin{aligned}\mathbb{P}_E &= \frac{\int_0^{2\pi}\int_0^{d_{\max}} \mathbb{P}_e l \,\mathrm{d}l\,\mathrm{d}\theta}{\pi[(d_{\max}+R)^2 - R^2]} \\ &= \frac{\int_0^{2\pi}\int_0^{d_{\max}} (1 - e^{-\lambda A}) l \,\mathrm{d}l\,\mathrm{d}\theta}{\pi(d_{\max}^2 + 2d_{\max}R)}.\end{aligned} \tag{7}$$

B. Analysis of Eavesdropping Risk

In order to evaluate the performance of Fri-UJ scheme, we consider the eavesdropping probability of non-jamming scheme, in which no UJs are deployed. We give the analytical results of non-jamming scheme and Fri-UJ scheme in Subsection IV.B.1 and Subsection IV.B.2, respectively.

B.1 Analysis of Non-Jamming (NJ) Scheme

In this scheme, UJs are not used. Thus, the eavesdropper does not receive any extra interference from UJs. Thus, the radius of the eavesdropping detection region is also $d_{\max}$, as shown in Fig. 3.

We then have the following result for the local eavesdropper probability and the overall eavesdropping probability.

Theorem 1: The local eavesdropper probability $\mathbb{P}_e$ and the overall eavesdropping probability $\mathbb{P}_E$ for non-jamming scheme are shown as follows:

$$\begin{aligned}\mathbb{P}_e(\mathrm{NJ}) = 1 - \exp\Bigg\{ - \lambda\Bigg[\Bigg(\mathrm{R}^2 \arccos \frac{(\mathrm{R}+\mathrm{l})^2 - \mathrm{d}_{\max}^2 + \mathrm{R}^2}{\mathrm{R}} \\ - \frac{(R+l)^2 - d_{\max}^2 + R^2}{2(R+l)} \sqrt{\frac{4(R+l)^2R^2 - ((R+l)^2 - d_{\max}^2 + R^2)^2}{4(R+l)^2}}\Bigg) \\ + \Bigg(d_{\max}^2 \arccos \frac{(R+l)^2 + d_{\max}^2 - R^2}{2(R+l)d_{\max}} \\ - \frac{(R+l)^2 + d_{\max}^2 - R^2}{2(R+l)} \sqrt{\frac{d_{\max}^2(2R+2l+1) - (R+l)^2 - R^2}{2(R+l)}}\Bigg)\Bigg]\Bigg\},\end{aligned} \tag{8}$$

and

$$\mathbb{P}_E(\mathrm{NJ}) = \frac{2\int_0^{\mathrm{d}_{\max}} (1 - \mathrm{e}^{-\lambda \mathrm{A}_\mathrm{n}})\mathrm{l}\ \mathrm{dl}}{\mathrm{d}_{\max}^2 + 2\mathrm{d}_{\max}\mathrm{R}}. \tag{9}$$

Proof: The eavesdropping region is the intersection of the eavesdropping detection region and the protection region. As shown in Fig. 3, the area of the eavesdropping region is calculated as follows,

$$\begin{aligned}A_n =& \left(R^2 \arccos \frac{x}{R} - x\sqrt{R^2 - x^2}\right) \\ &+ \left(d_{\max}^2 \arccos \frac{L-x}{d_{\max}} - (L-x)\sqrt{d_{\max}^2 - (L-x)^2}\right),\end{aligned} \tag{10}$$

where $x = \frac{L^2 + d_{\max}^2 - R^2}{2L}$, and $L = R + l$.

According to the definition of local eavesdropping probability and (6), we have the above result in (1).

Similarly, according to the definition of overall eavesdropping probability and (7), we have the overall eavesdropping probability for non-jamming scheme as follows,

$$\begin{aligned}\mathbb{P}_E(\mathrm{NJ}) &= \frac{\int_0^{2\pi} \int_0^{d_{max}} \mathbb{P}_e(\mathrm{NJ})\mathrm{l}\ \mathrm{dl}\ \mathrm{d}\theta}{\pi(d_{\max}^2 + 2d_{\max})R} \\ &= \frac{\int_0^{d_{\max}} (1 - e^{-\lambda A_n})l\ \mathrm{dl}}{\frac{1}{2}(d_{\max}^2 + 2d_{\max}R)} \\ &= \frac{2\int_0^{d_{\max}} (1 - e^{-\lambda A_n})l\ \mathrm{dl}}{d_{\max}^2 + 2d_{\max}R}.\end{aligned} \tag{11}$$

■

B.2 Analysis of Fri-UJ Scheme

In the Fri-UJ scheme, the UJs are deployed one by one surrounding the protection region to cover the eavesdropper appearance region. However, there are still some small areas not covered by the emitted jamming signals of UJs as shown in Fig. 3. Therefore, we need to analyze the eavesdropping probability with consideration of both regions. We then have the following result for the local eavesdropper probability and the overall eavesdropping probability of Fri-UJ scheme.

Theorem 2: The local eavesdropper probability $\mathbb{P}_e$ and the overall eavesdropping probability $\mathbb{P}_E$ for Fri-UJ scheme are shown as follows:

$$\mathbb{P}_e(\mathrm{J}) = \begin{cases} \mathbb{P}_e^c(\mathrm{J}), & H \le D \le \sqrt{H^2 + \frac{d_{\max}}{2}^2} \\ \mathbb{P}_e(\mathrm{NJ}), & D > \sqrt{H^2 + \frac{d_{\max}}{2}^2} \end{cases}, \tag{12}$$

and

$$\mathbb{P}_E(\mathrm{J}) = \frac{\mathrm{N}\int_0^{\theta} \int_0^{\mathrm{d}_{\max}} \mathbb{P}_\mathrm{e}(\mathrm{J})\mathrm{l}\ \mathrm{dl}\ \mathrm{d}\theta}{\pi(\mathrm{d}_{\max}^2 + 2\mathrm{d}_{\max}\mathrm{R})}. \tag{13}$$

Proof: When we analyze the eavesdropping probability of our Fri-UJ schemes, there are two cases: 1) the eavesdropper falls inside the interference region, namely UJs-covered scheme and 2) the eavesdropper falls outside the interference region, namely UJs-Uncovered scheme. We then derive the local eavesdropping probability in both the two cases.

We first consider the location of the eavesdropper with the polar coordinate (L, ϕ), where the center of protection region is regarded as the origin point as shown in Fig. 3. We denote the angle between the x-axis and the line connecting the origin and the eavesdropper by ϕ. In particular, ϕ falls in the range of $[0, 2\pi]$. The local eavesdropping probability of UJs-Uncovered scheme is the same as that of non-jamming scheme in Section IV.B.1. Thus, we need to derive the local eavesdropping probability of UJs-covered scheme.

When the eavesdropper is in the interference region, the distance D between the nearest UJ and the eavesdropper is calculated by (as shown in Fig. 3),

$$D = [(R + r) - k\cos\phi]^2 + H^2. \tag{14}$$

Since there are LoS and NLoS interference links between a UJ and the eavesdropper, we need to calculate the probabilities of two different types of links. We first derive the probability of LoS link, which is expressed as follows [36],

$$\mathbb{P}_{\mathrm{LoS}} = a(\delta - 15^{\mathrm{o}})^b, \tag{15}$$

where a and b are constant values according to different environmental settings as shown in Table 2.

Then, the probability of NLoS link is $\mathbb{P}_{\mathrm{NLoS}} = 1 - \mathbb{P}_{\mathrm{LoS}}$.

The received interference at the eavesdropper from the closest UJ is I_j can be expressed as follows,

$$I_j = \mathbb{P}_{\mathrm{LoS}} P_j D^{-\alpha} + \mathbb{P}_{\mathrm{NLoS}} \frac{P_j D^{-\alpha}}{\mu_j}. \tag{16}$$

Therefore, the radius of eavesdropping region for UJs-covered scheme is given by,

$$d_e = \mathbb{E}\left[\frac{P_t h}{(I_j + \sigma^2)T_e}\right]^{\frac{1}{\alpha}} = \frac{1}{\alpha} \cdot \left[\frac{P_t}{\mu(I_j + \sigma^2)T_e}\right]^{\frac{1}{\alpha}} \cdot \Gamma\Big(\frac{1}{\alpha}\Big). \tag{17}$$

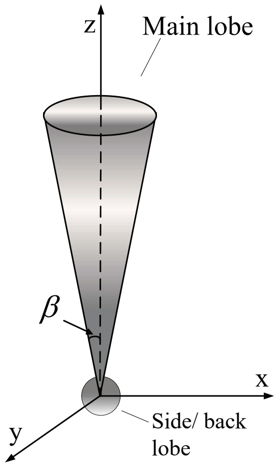


Fig. 4. Keyhole model.

Table 2. RF model parameters.

(a, b)	Frequency $700MHz$	Frequency $2000MHz$	Frequency $5800MHz$
Suburban	(0.77, 0.05)	(0.76, 0.06)	(0.75, 0.06)
Urban	(0.63, 0.09)	(0.6, 0.11)	(0.56, 0.13)
Dense urban	(0.37, 0.21)	(0.36 , 0.21)	(0.33, 0.23)
Highrise urban	(0.06, 0.58)	(0.05, 0.61)	(0.05, 0.64)

Similarly, we calculate the area of eavesdropping region for UJs-covered scheme by (10). The area of eavesdropping region for UJs-covered scheme A_j is expressed as follows,

$$\begin{aligned}A_j =&\Bigg(R^2 \arccos \frac{(R+l)^2 - d_e^2 + R^2}{R} \\ &- \frac{(R+l)^2 - d_e^2 + R^2}{2L} \sqrt{\frac{4(R+l)^2R^2 - ((R+l)^2 - d_e^2 + R^2)^2}{4(R+l)^2}} \Bigg) \\ &+ \Bigg(d_e^2 \arccos \frac{(R+l)^2 + d_e^2 - R^2}{2(R+l)d_e} \\ &- \frac{(R+l)^2 + d_e^2 - R^2}{2(R+l)} \sqrt{\frac{d_e^2(2R+2l+1) - (R+l)^2 - R^2}{2(R+l)}} \Bigg). \end{aligned} \tag{18}$$

After combining (6) and (18), the local eavesdropping probability of UJs-covered scheme is shown as,

$$\begin{aligned}\mathbb{P}_e^c(\mathrm{J}) = 1 - \exp&\Bigg\{ - \lambda \Bigg[\Bigg(\mathrm{R}^2 \arccos \frac{(\mathrm{R}+\mathrm{l})^2 - \mathrm{d}_\mathrm{e}^2 + \mathrm{R}^2}{\mathrm{R}} \\ &- \frac{(R+l)^2 - d_e^2 + R^2}{2(R+l)} \sqrt{\frac{4(R+l)^2R^2 - ((R+l)^2 - d_e^2 + R^2)^2}{4(R+l)^2}} \Bigg) \\ &+ \Bigg(d_e^2 \arccos \frac{(R+l)^2 + d_e^2 - R^2}{2(R+l)d_e} \\ &- \frac{(R+l)^2 + d_e^2 - R^2}{2(R+l)} \sqrt{\frac{d_e^2(2R+2l+1) - (R+l)^2 - R^2}{2(R+l)}} \Bigg) \Bigg] \Bigg\}, \end{aligned} \tag{19}$$

The eavesdropper suffers from the UJs' interference when the eavesdropper falls inside of the interference region. On the other hand, the eavesdropper is not interfered by UJs, when the eavesdropper falls outside the interference region. It means that the local eavesdropping probability of Fri-UJ scheme $\mathbb{P}_e(\mathrm{J})$ is either the local eavesdropping probability of non-jamming scheme or the local eavesdropping probability of UJs-covered scheme. Overall, when the UJs are used, the local eavesdropper probability is shown in (12).

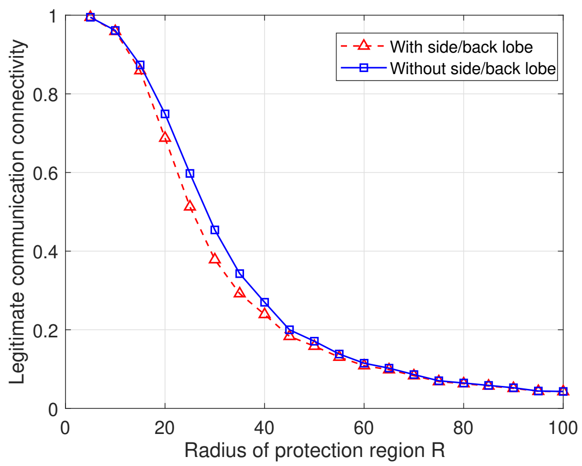


Fig. 5. Legitimate communication connectivity under Fri-UJ protection (path loss factor $\alpha = 3$, legitimate users density $\lambda = 0.2$).

After applying integration on (12) and (7), we have the overall eavesdropping probability of Fri-UJ scheme as given in (13). ■

B.3 Analysis of The Number of UAV-Jammers

In our Fri-UJ scheme, the deployment of UJs can significantly affect the performance (i.e., the eavesdropping risk). Generally, the more UJs, the lower eavesdropping probability achieves. However, it is not cost-efficient if a large number of UJs are deployed. On the other hand, the fewer UJs also result in the poor performance of Fri-UJ scheme. In our Fri-UJ scheme, we consider that the deployment of UJs follows a *non-overlapping-while-adjacent principle*. In particular, the projection of the interference caused by a UJ is a circle as shown in Fig. 3. We require that any two neighboring circles are adjacent and there is no overlapping between any two neighboring circles. In this setting, the maximum coverage can be achieved while the number of UJs is kept small enough.

In this setting, we observe that the number of UJs denoted by N is mainly affected by the radius of the protection region R. In particular, the larger value of R leads to the larger area of the protection region. Consequently, more UJs are needed to mitigate the eavesdropping risk when the area of the protection region is larger.

C. Impact on Legitimate Communication

Another concern with Fri-UJ scheme is the impact on legitimate communications. We observe that the Fri-UJ scheme has nearly no impact on the legitimate communications. This is mainly because the interference signal emitted by UJs is mainly concentrated on a certain direction (i.e., the circular projection on the ground) and there is almost no interference outside the projection area. It is true that there will be a little interference outside the projection area if we consider the side/back lobes of a directional antenna though the interference is much smaller than that inside the project area. Compared with other jamming schemes such as AE-shelter [31] using omni-directional antennas to emit the interference signals, our Fri-UJ scheme has much smaller impact on the legitimate communications.

We consider a more realistic antenna model named keyhole model with consideration of side/back lobes to investigate the impact of antenna models on legitimate communication. The keyhole model is shown in Fig. 4. Compared with the sector model, the keyhole model has two kinds of antenna gains including the gain of main lobe and the gain of side/back lobe. The antenna gain of main lobe is $29000/\beta^2$ as shown in Section III.A, and the gain of side/back lobe is approximated by the following equation as derived in our prior study [39],

$$g_s = \frac{2 - g(1-\cos\beta)}{1+\cos\beta}. \tag{20}$$

We exploit the *legitimate communication connectivity* to evaluate the impact on legitimate communications. In particular, we define the legitimate communication connectivity as the probability that two random legitimate users can successfully establish a data transmission link. The data transmission link is established when the SINR of a legitimate user (receiver) received signal is larger than a threshold T_u. In other words, the following inequality holds,

$$\mathsf{SINR_{user}} = \frac{\mathsf{P_t h d_u^{-\alpha}}}{\sigma^2 + \mathsf{I_s}} \geq \mathsf{T_u}, \tag{21}$$

where d_u is the distance between two legitimate users, and I_s is the cumulative interference from UJs.

It is worth mentioning that the cumulative interference I_s is the interference from side/back lobes of all UJs surrounding the protection region to the legitimate communication. After considering two types of links as shown in Section III.C, we have the cumulative interference I_s as given in the following equation,

$$I_s = \sum_{i=1}^{N} (\mathbb{P}_{\text{LoS}} P_j g_s D_i^{-\alpha} + \mathbb{P}_{\text{NLoS}} \frac{P_j g_s D_i^{-\alpha}}{\mu_j}), \tag{22}$$

where D_i is the distance from ith UJ to the legitimate user who receives the interference signal.

We next conduct simulations to evaluate the legitimate communication connectivity. We assume that the legitimate users are randomly distributed according to HPPP with the density of λ, and two users are randomly picked from all the legitimate users. Then, the legitimate communication connectivity of those two legitimate users is calculated according to the condition whether they can successfully establish a data transmission link. We then repeat the above procedure $10,000$ times and obtain the average legitimate communication connectivity.

Fig. 5 shows the legitimate communication connectivity versus the radius of protection region. In particular, the horizontal axis is the radius of protection region and the vertical axis is the legitimate communication connectivity as shown in Fig. 5. We observe that the legitimate communication connectivity always decreases with the increased radius of protection region. This is because the transmission distance is extended when the radius of protection region increases. As a result, the communication connectivity decreases.

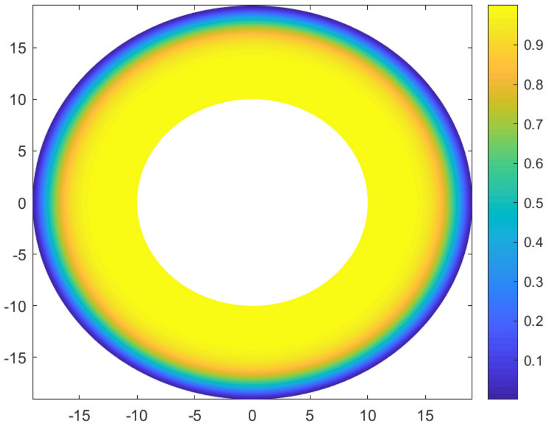


Fig. 6. Local eavesdropping probability $\mathbb{P}_e(\text{NJ})$ for non-jamming scheme (path loss factor $\alpha = 3$, legitimate users density $\lambda = 0.2$).

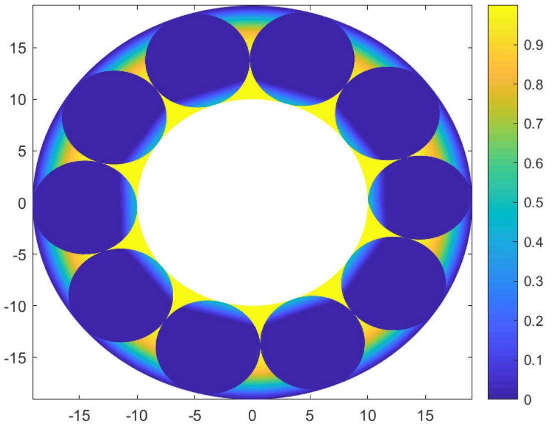


Fig. 7. Local eavesdropping probability $\mathbb{P}_e(\text{UJ})$ for Fri-UJ scheme (path loss factor $\alpha = 3$, legitimate users density $\lambda = 0.2$).

In addition, as shown in Fig. 5, the blue curve denotes the legitimate communication connectivity without consideration of side/back lobes, while the red curve is the legitimate communication connectivity with consideration of side/back lobe. Observing red curve and blue curve, we find that the red curve nearly matches the blue curve. It implies that Fri-UJ scheme barely affects the legitimate communication, when the side/back lobe is considered.

V. EMPIRICAL RESULTS

In this section, we conduct extensive simulations to evaluate the effectiveness of Fri-UJ scheme in terms of the eavesdropping probability. In Section V.A, we first analyze the local eavesdropping probability of Fri-UJ when the eavesdropper appears at different locations. In Section V.B, we then analyze the overall eavesdropping probability of Fri-UJ.

We consider the following common settings for simulations. The protection region is with radius $R = 10$ is in an suburban environment with $a = 0.77$ and $b = 0.05$. We assume the

Table 3. The levels of local eavesdropping probability.

Risk level	Color range	Local eavesdropping probability
safe	🟦	$\mathbb{P}_e = 0$
low risk	🟦	$0 < \mathbb{P}_e \leq 0.25$
medium risk	🟩	$0.25 < \mathbb{P}_e \leq 0.5$
high risk	🟧	$0.5 < \mathbb{P}_e \leq 0.75$
dangerous	🟨	$0.75 < \mathbb{P}_e \leq 1$

noise power is $\sigma^2 = 0.01$ and Rayleigh fading factor for ground communication is $\mu = 1$ and air-to-ground communication is $\mu_j = 1$. The SINR threshold value for the eavesdropper to decode information is $T_e = 1$. Only one eavesdropper randomly appears in eavesdropper appearance region to wiretap the confidential information.

A. The Local Eavesdropping Probability

We first analyze the local eavesdropping probability $\mathbb{P}_e$ for non-jamming scheme and Fri-UJ scheme. Figs. 6 and 7 show the local eavesdropping probability of non-jamming scheme and Fri-UJ scheme, respectively. To clearly compare results, we also define five levels of eavesdropping risk in the eavesdropping appearance region: safe, low risk, medium risk, high risk and dangerous. Table 3 shows the local eavesdropping probability for five levels of eavesdropping risk. The lightest yellow stands for $0.75 < \mathbb{P}_e \leq 1$ (i.e., dangerous) and the darkest blue stands for $\mathbb{P}_e = 0$ (i.e., safe). The color from yellow to blue in the eavesdropper appearance region implies the intensity of the local eavesdropping probability decreases.

Fig. 6 shows the result of the local eavesdropping probability $\mathbb{P}_e(\mathrm{NJ})$ for non-jamming scheme. It is shown in Fig. 6 that the local eavesdropping probability varies when the eavesdropper appears at different locations in the eavesdropper appearance region (i.e., a ring). In particular, the local eavesdropping probability $\mathbb{P}_e(\mathrm{NJ})$ decreases when eavesdropper moves far away from protection region. This is mainly due to the path loss of long distance.

The result of the local eavesdropping probability $\mathbb{P}_e(\mathrm{UJ})$ for Fri-UJ scheme is shown in Fig. 7. We observe that deploying UJs in protection region can greatly reduce the eavesdropping risk. In particular, the eavesdropping risk in most of protection region covered by UJs is either safe or low risk (i.e., dark blue) though the UJ-uncovered region is still dangerous.

Comparing Fig. 6 with Fig. 7 together, we find that the introduction of UJs can significantly reduce the local eavesdropping probability.

B. The Overall Eavesdropping Probability

We further investigate the effectiveness of Fri-UJ scheme for the whole network via evaluating the overall eavesdropping probability $\mathbb{P}_E$. In simulations, the density of legitimate users λ varies from 0. to 0.3.

Fig. 8 presents the simulation results of $\mathbb{P}_E$ of Fri-UJ scheme versus non-jamming scheme, in which red solid curves represent the results of Fri-UJ scheme and blue dash curves represent the results of non-jamming scheme; curves are analytical results and markers stand for the simulation results. Every simulation result is obtained via averaging over 10,000 simulations. It is shown in Fig. 8 that there is an excellent agreement between simulation results and analytical results, implying that our proposed analytical framework is quite accurate.

We observe that $\mathbb{P}_E$ of Fri-UJ scheme is always lower than that of non-jamming scheme in all the cases. It implies that Fri-UJ scheme can significantly reduce the eavesdropping risk. This is mainly because the deployment of UJs can significantly reduce the local eavesdropping probability at each location of eavesdropper appearance (as shown in Section V.A).

We then investigate the performance of Fri-UJ scheme under different channel conditions. In particular, we vary the path loss factor α from 3 to 5 and obtain results in Figs. 8(a), 8(b), and 8(c). It is shown in Figs. 8(a), 8(b), and 8(c) that the overall eavesdropping probability $\mathbb{P}_E$ of Fri-UJ scheme decreases when the path loss factor α increases, implying that the worse channel condition can significantly affect the eavesdropping probability. However, in every case, $\mathbb{P}_E$ of our Fri-UJ scheme is always lower than that of non-jamming scheme.

Meanwhile, we also find that adjusting the transmitter power of legitimate users P_t can also significantly affect the overall eavesdropper probability $\mathbb{P}_E$. For example, aligning Figs. 8(c) and 8(d) together, we find that $\mathbb{P}_E$ of both Fri-UJ scheme and non-jamming schemes increases when P_t increases from 1 to 3 when other factors (i.e., α, β, P_j) are fixed.

Moreover, we investigate the performance by adjusting the transmitting power of UJs P_j. In particular, comparing Fig. 8(d) with Fig. 8(e), we observe that $\mathbb{P}_E$ of Fri-UJ scheme increases while that of non-jamming scheme stays almost the same when P_j increases from 0.1 to 0.3. It implies that increasing the transmitting power of UJs can significantly reduce the eavesdropping risk due to the increased interference to the eavesdropper.

Furthermore, we also evaluate the impact of directional antennas of UJs on the performance. In particular, we investigate the overall eavesdropping probability via varying β from 45° to 60° while fixing other parameters. In contrast to Fig. 8(e), increasing the beam-width also results in the decreased overall eavesdropping probability as shown in Fig. 8(f).

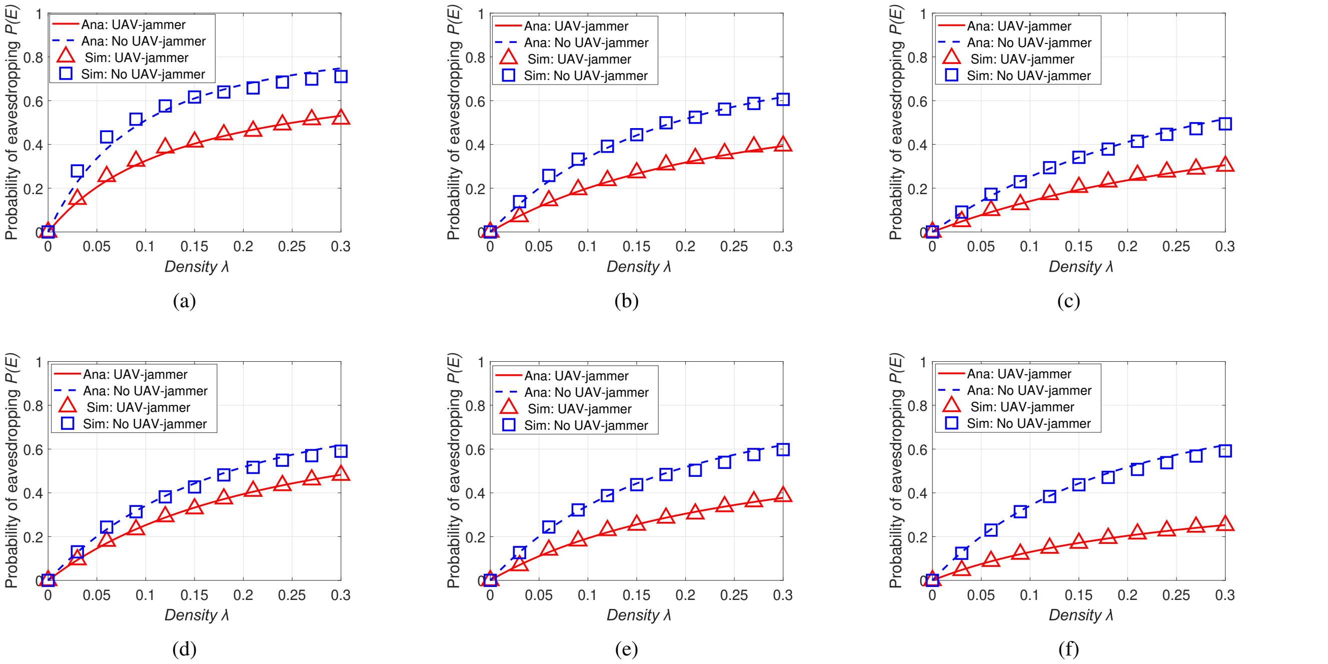
VI. CONCLUSION

In this paper, we present an anti-eavesdropping scheme based on UAV jammers who emit artificial noise to disturb eavesdroppers from wiretapping confidential information. We evaluate the effectiveness of the Fri-UJ scheme via analyzing the local eavesdropping probability and the overall eavesdropping probability. We conduct extensive simulations to verify the proposed model. Simulation results agree with analytical results implying the accuracy of the proposed model. Our results also show the Fri-UJ scheme can effectively mitigate the eavesdropping probability. Compared with prior friendly-jamming scheme, Fri-UJ scheme has the deployment flexibility and nearly no impact on legitimate communications.

REFERENCES

[1] T. Qiu *et al.*, "Sigmm: A novel machine learning algorithm for spammer identification in industrial mobile cloud computing," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 2349–2359, Apr. 2019.

[2] T. Qiu, X. Wang, C. Chen, M. Atiquzzaman, and L. Liu, "Tmed: A spider-web-like transmission mechanism for emergency data in vehicular ad hoc



(a) (b) (c)

(d) (e) (f)

Fig. 8. Overall eavesdropping probability $\mathbb{P}_E$ with the density of legitimate users λ varies from 0 to 0.3: (a) $P_t = 1$, $P_j = 0.1$, $\beta = 45^o$, $\alpha = 3$, (b) $P_t = 1$, $P_j = 0.1$, $\beta = 45^o$, $\alpha = 4$, (c) $P_t = 1$, $P_j = 0.1$, $\beta = 45^o$, $\alpha = 5$, (d) $P_t = 3$, $P_j = 0.1$, $\beta = 45^o$, $\alpha = 5$, (e) $P_t = 3$, $P_j = 0.3$, $\beta = 45^o$, $\alpha = 5$, and (f) $P_t = 3$, $P_j = 0.3$, $\beta = 60^o$, $\alpha = 5$.

networks," *IEEE Trans. Veh. Commun.*, vol. 67, no. 9, pp. 8682–8694, Sept. 2018.

[3] T. Qiu, R. Qiao, and D. O. Wu, "Eabs: An event-aware backpressure scheduling scheme for emergency Internet of things," *IEEE Trans. Mobile Comput.*, vol. 17, no. 1, pp. 72–84, Jan. 2018.

[4] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in wpa2," in *Proc. ACM SIGSAC*, Oct. 2017, pp. 1313–1328.

[5] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[6] S. Alblwi and K. Shujaee, "A survey on wireless security protocol wpa2," in *Proc. SAM*, Oct. 2017, pp. 12–17.

[7] G. Xu *et al.*, "CSP-E^2: An abuse-free contract signing protocol with low-storage TTP for energy-efficient electronic transactions ecosystems," *Information Sciences*, vol. 476, pp. 505–515, 2019.

[8] X. Zeng, G. Xu, X. Zheng, Y. Xiang, and W. Zhou, "E-aua: An efficient anonymous user authentication protocol for mobile iot," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1506–1519, Apr. 2019.

[9] T. Gabel, A. Tharwat, and E. Godehardt, "Eavesdropping opponent agent communication using deep learning," in *Proc. MATES*, Springer, 2017, pp. 205–222.

[10] F. Adib, C.-Y. Hsu, H. Mao, D. Katabi, and F. Durand, "Capturing the human figure through a wall," *ACM Trans. Graphics*, vol. 34, no. 6, p. 219, 2015.

[11] S. Yousefi, H. Narui, S. Dayal, S. Ermon, and S. Valaee, "A survey on behavior recognition using wifi channel state information," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 98–104, 2017.

[12] Y. Yao *et al.*, "Aegis: An interference-negligible rf sensing shield," in *Proc. IEEE INFOCOM*, June 2018, pp. 1718–1726.

[13] G. Tuna, T. V. Mumcu, and K. Gulez, "Design strategies of unmanned aerial vehicle-aided communication for disaster recovery," in *Proc. IEEE HONET*, Dec. 2012, pp. 115–119.

[14] G. Tuna, B. Nefzi, and G. Conte, "Unmanned aerial vehicle-aided communications system for disaster recovery," *J. Netw. Comput. Applicat.*, vol. 41, pp. 27–36, 2014.

[15] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Drone small cells in the clouds: Design, deployment and performance analysis," in *Proc. IEEE GLOBECOM*, Dec. 2015, pp. 1–6.

[16] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Unmanned aerial vehicle with underlaid device-to-device communications: Performance and tradeoffs," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 3949–3963, 2016.

[17] R. I. Bor-Yaliniz, A. El-Keyi, and H. Yanikomeroglu, "Efficient 3-d placement of an aerial base station in next generation cellular networks," in *Proc. IEEE ICC*, May 2016, pp. 1–5.

[18] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: opportunities and challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 36–42, May 2016.

[19] Z.-K. Zhang *et al.*, "Iot security: Ongoing challenges and research opportunities," in *Proc. IEEE SOCA*, Nov. 2014, pp. 230–234.

[20] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," in *Proc. IEEE ICITST*, Dec. 2015, pp. 336–341.

[21] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," *Future Generation Comput. Syst.*, vol. 82, pp. 395–411, 2018.

[22] A. Esfahani *et al.*, "A lightweight authentication mechanism for M2M communications in industrial IoT environment," *IEEE Internet Things J.*, 2017.

[23] A. Karati, S. H. Islam, and M. Karuppiah, "Provably secure and lightweight certificateless signature scheme for IIoT environments," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3701–3711, 2018.

[24] X. Li, H.-N. Dai, H. Wang, and H. Xiao, "On performance analysis of protective jamming schemes in wireless sensor networks," *Sensors*, vol. 16, no. 12, p. 1987, 2016.

[25] J.-C. Kao and R. Marculescu, "Minimizing eavesdropping risk by transmission power control in multihop wireless networks," *IEEE Trans. Comput.*, vol. 56, no. 8, pp. 1009–1023, 2007.

[26] S. Bashar and Z. Ding, "Optimum power allocation against information leakage in wireless network," in *Proc. IEEE GLOBECOM*, Dec. 2009, pp. 1–6.

[27] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 256–266, 2011.

[28] S. Sankararaman *et al.*, "Optimization schemes for protective jamming," *Mobile Netw. Applicat.*, vol. 19, no. 1, pp. 45–60, 2014.

[29] Y. S. Kim, P. Tague, H. Lee, and H. Kim, "A jamming approach to enhance enterprise Wi-Fi secrecy through spatial access control," *Wireless Netw.*, vol. 21, no. 8, pp. 2631–2647, 2015.

[30] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Friendly jamming for wireless secrecy," in *Proc. IEEE ICC*, May 2010, pp. 1–6.

[31] X. Li, H.-N. Dai, Q. Wang, and A. V. Vasilakos, "Ae-shelter: An novel anti-eavesdropping scheme in wireless networks," in *Proc. IEEE ICC*, May 2017, pp. 1–6.

[32] J. Yang, I.-M. Kim, and D. I. Kim, “Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers,” *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2840–2852, 2013.

[33] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, 2008.

[34] Q. Wang, H.-N. Dai, O. Georgiou, Z. Shi, and W. Zhang, “Connectivity of underlay cognitive radio networks with directional antennas,” *IEEE Trans. Veh. Commun.*, vol. 67, no. 8, pp. 7003–7017, 2018.

[35] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, “Efficient deployment of multiple unmanned aerial vehicles for optimal wireless coverage,” *IEEE Commun. Lett.*, vol. 20, no. 8, pp. 1647–1650, 2016.

[36] A. Al-Hourani, S. Kandeepan, and A. Jamalipour, “Modeling air-to-ground path loss for low altitude platforms in urban environments,” in *Proc. IEEE GLOBECOM*, Dec. 2014, pp. 2898–2904.

[37] J. Holis and P. Pechac, “Elevation dependent shadowing model for mobile communications via high altitude platforms in built-up areas,” *IEEE Trans. Antennas Propag.*, vol. 56, no. 4, pp. 1078–1084, 2008.

[38] X. Li, Q. Wang, H.-N. Dai, and H. Wang, “A novel friendly jamming scheme in industrial crowdsensing networks against eavesdropping attack,” *Sensors*, vol. 18, no. 6, 2018.

[39] Q. Wang, H.-N. Dai, Z. Zheng, M. Imran, and A. Vasilakos, “On connectivity of wireless sensor networks with directional antennas,” *Sensors*, vol. 17, no. 1, p. 134, 2017.

Qubeijian Wang received the B.E. degree in Electrical Engineering from Xi’an Jiao-Tong Liverpool University, China and University of Liverpool, UK in 2015, and M.E. degree in Telecommunications from University of Melbourne, Australia in 2017. He is currently pursuing the Ph.D. degree in Communication Engineering at Macau University of Science and Technology. His research interests include UAV-aided communication, physical-layer security and network performance analysis.

Hong-Ning Dai is an Associate Professor in Faculty of Information Technology at Macau University of Science and Technology. He obtained the Ph.D. degree in Computer Science and Engineering from Department of Computer Science and Engineering at the Chinese University of Hong Kong. His research interests include Internet of Things, Big Data Analytics and Blockchains. He has published more than 90 peer-reviewed papers in top-tier journals and conferences, including ACM Computing Surveys, IEEE Transactions on Industrial Informatics, IEEE Transactions on Vehicular Technology, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Computational Social Systems, ACM/Springer Wireless Networks, IEEE INFOCOM, etc. He has 1 ESI highly-cited paper awarded by Clarivate Analytics. He is also the holder of 1 U.S. patent. Due to his outstanding research performance, he was awarded with BOC Excellent Research Award of Macau University of Science and Technology in 2015. He has served as an Associate Editor for IEEE Access and Guest Editors of IEEE Transactions on Industrial Informatics. He is a Senior Member of IEEE and a Professional Member of ACM.

Hao Wang received the B.Eng. and Ph.D. degrees in Computer Science and Engineering from the South China University of Technology, Guangzhou, China, in 2006. He is currently an Associate Professor with the Norwegian University of Science and Technology, Gjøvik, Norway. He has authored or co-authored 80+ papers in reputable international journals and conferences. His current research interests include big data analytics, industrial Internet of things, high performance computing, safety-critical systems, and communication security. He is a Member of the IEEE IES Technical Committee on Industrial Informatics. He served as a TPC Co-Chair for the IEEE DataCom 2015, IEEE CIT 2017, and ES 2017. He served as a Reviewer for journals such as the IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE TRANSACTIONS ON BIG DATA, the IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING, the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, the IEEE INTERNET OF THINGS JOURNAL, and ACM Transactions on Multimedia Computing, Communications, and Applications.

Guangquan Xu is a Ph.D. and Full Professor at the Tianjin Key Laboratory of Advanced Networking (TANK), College of Intelligence and Computing, Tianjin University, China. He received his Ph.D. degree from Tianjin University in March 2008. He is a Member of the CCF and IEEE. His research interests include cyber security and trust management.

Arun Kumar Sangaiah (M’09) received the Master of Engineering degree from Anna University, Chennai, India, in 2007, and the Ph.D. from the Vellore Institute of Technology, Vellore, India, in 2014. He is currently an Associate Professor with the School of Computing Science and Engineering, Vellore Institute of Technology. He has authored or coauthored more than 250 scientific papers in high-standard Science Citation Index (SCI) journals, such as the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE COMMUNICATION MAGAZINE, IEEE SYSTEMS, the IEEE INTERNET OF THINGS, the IEEE TRANSACTIONS ON SERVICES COMPUTING, and the IEEE ETC. In addition, he has authored/edited more than eight books (Elsevier, Springer, Wiley, Taylor, and Francis) and 50 journal special issues in the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE COMMUNICATION MAGAZINE, the IEEE INTERNET OF THINGS, the IEEE CONSUMER ELECTRONIC MAGAZINE, etc. He holds one Indian patent in the area of computational intelligence. He is an Editorial Board Member/Associate Editor for various international SCI journals. His research interests include software engineering, Internet of Things, computational intelligence, wireless networks.