The Full-Duplex Device-to-Device Security Communication Under the Coverage of Unmanned Aerial Vehicle

Qian Zeng [1] and Zhongshan Zhang[2]
[1] Beijing Engineering and Technology Center for Convergence Networks and Ubiquitous Services,
University of Science and Technology Beijing (USTB),
Beijing, China 100083
[2]The School of Communication and Electronics in Beijing Institute of Technology (BIT),
Beijing, China 100081
[e-mail: zengqian617@foxmail.com; zhangzs@bit.edu.cn]
*Corresponding author: Zhongshan Zhang

Received March 10, 2018; revised August 29, 2018; accepted November 12, 2018; published April 30, 2019

Abstract

Unmanned aerial vehicles (UAVs), acting as mobile base stations (BSs), can be deployed in the typical fifth-generation mobile communications (5G) scenarios for the purpose of substantially enhancing the radio coverage. Meanwhile, UAV aided underlay device-to-device (D2D) communication mode can be activated for further improving the capacity of the 5G networks. However, this UAV aided D2D communication system is more vulnerable to eavesdropping attacks, resulting in security risks. In this paper, the D2D receivers work in full-duplex (FD) mode, which improves the security of the network by enabling these legitimate users to receive their useful information and transmit jamming signal to the eavesdropper simultaneously (with the same frequency band). The security communication under the UAV coverage is evaluated, showing that the system's (security) capacity can be substantially improved by taking advantage of the flexible radio coverage of UAVs. Furthermore, the closed-form expressions for the coverage probabilities are derived, showing that the cellular users (CUs)' secure coverage probability in downlink transmission is mainly impacted by the following three factors: its communication area, the relative position with UAV, and its eavesdroppers. In addition, it is observed that the D2D users or DUs' secure coverage probability is relevant to state of the UAV. The system's secure capacity can be substantially improved by adaptively changing the UAV's position as well as coverage.

Keywords: Device-to-Device Communication, Security Communication, Unmanned Aerial Vehicle, Coverage Probability, Full-Duplex.

This work was supported by the key project of the National Natural Science Foundation of China (No. 61431001), the open research fund of National Mobile Communications Research Laboratory Southeast University (No.2017D02), Key Laboratory of Cognitive Radio and Information Processing, Ministry of Education (Guilin University of Electronic Technology), and the Foundation of Beijing Engineering and Technology Center for Convergence Networks and Ubiquitous Services, in part by the Foundation of Beijing Engineering and Technology Center for Convergence Networks and Ubiquitous Services.

http://doi.org/10.3837/tiis.2019.04.011 **ISSN : 1976-7277**

1. Introduction

Unmanned aerial vehicle (UAV), acting as the mobile base station (BS, for which we use “UAV” to stand for “UAV BS” for short hereinafter) with a flexible radio coverage, have attracted a wide attention and been already applied in a variant of practical scenarios such as emergency rescue and intelligent transportation. Especially in the typical fifth-generation mobile communications (5G) [1][2], UAV with other advance communication equipment will meet the processing and transmission demands with a number of transmit data.

Device-to-device (D2D) communication has also been widely regarded as a technology for 5G, which can provide the seamless coverage requirements for complementing and enhancing the conventional cellular systems, and has been widely investigated for substantially improving the data rate [3] and resource allocation [4] of the existing wireless networks. Besides the benefits of improving channel capacity and radio coverage, information security is also a critical issue in D2D communications. Thus, guaranteeing the security communication has been regarded as an essential study in D2D-aided networks [5]. Basically, solutions of the optimal joint power control for both the cellular users (CUs) and D2D users (DUs) can be proposed for optimizing the system’s secrecy rate [6]. However, the impact of only a cellular eavesdropper is considered in the above literature, without considering the impact of D2D eavesdroppers. In the underlay cellular networks, on the other hand, the eavesdropping behavior is always aimless, and there typically exist multiple eavesdroppers. In this case, a novel selective eavesdropping scenario must be considered to achieve the preset secrecy rate [7], in which scenario the eavesdroppers may arbitrarily choose one target (CU or DU) to overhear. Even that the eavesdroppers are sometimes capable of mitigating the interference via cooperation [8].

In light of the fact that the existed systems are usually operated at the half-duplex (HD) mode (e.g. either time division duplex (TDD) or frequency division duplex (FDD) mode is employed), their spectral efficiency is much lower than the full-duplex (FD) mode [9], which enables a concurrent transmission and reception at a single frequency band. However, the existence of self-interference (SI) always hinders the FD development, but the relative lower transmit power of D2D will allowing more easily SI cancellation. The FD-mode deployment in D2D communication has been studies for some time [10]. The throughput of FD-mode D2D network have been discussed in [11], and the effects of residual SI and spectral efficiency are analyzed in [12]. In FD-mode D2D security communication, the BS can allocate a fraction of the total transmitted signal as artificial noise (AN) to degrade the eavesdroppers’ channel, which can be employed for improving the security of the communications, but the FD-mode D2D only share the frequency band allocated to a CU by the BS [13]. In [14], the FD relay node receives the data and transmits jamming signals at the same time, which has the same data rate as the HD scheme but significant improving the secrecy performance, but it has not considered the D2D communication. Besides D2D nodes works in FD-mode, the BS also can work in FD-mode for a secure wireless system, which the secure transmission is ensured to all the users, and also meeting the QoS requirements of the users [15]. In [16], the FD-mode D2D receiver transmits the desired signal and forward the received interference simultaneously to the D2D receiving user to eliminate the interference from the BS, which do not consider the eavesdropper and the overall network performance. To the best of our knowledge, the FD-mode D2D security communication is still needs to be further researched.

In the typical 5G scenarios, UAV aided D2D communications may help to offer a ubiquitous radio coverage for many applications, such as vehicular connectivity [17], industrial automation, and urban communications, and so on [18]. For instance, the authors in [19] proposed a UAV aided D2D communication scene to extend the network coverage. By developing a UAV optimal position strategy, the authors in [19] can successfully maximizing the data rate of the network. Regarding D2D mode as an important option of communication means in cellular networks, the authors in [20] proposed a two-mode-selection scheme for UAV aided D2D networks to maximize the connectivity regions of each **U**AV. Furthermore, the authors in [21] proposed a mobile UAV-aided scheme (considering a disk-shaped covering area) for maximizing the cellular coverage in D2D-aided heterogeneous networks. Evidently, employing multiple UAVs may offer a reasonable way for furthermore improving the radio coverage. However, co-channel interference is also a problem for consider [22]. In UAV communication, it requires the operators to consider the radio channels' assignment due to the demand of inter-channel interference mitigation in the presence of a limited number of orthogonal channels [23].

As we know, as the D2D communication still suffers from a severe security problem, which also exists in UAV based systems. In addition, as the UAV moves, the coverage of D2D network can be changed accordingly. For the air-to-ground channel from UAV to the users on the ground, the users receiving signal will also suffer from different security issues. Hence, in D2D based security communication, the channels of both legitimate users and eavesdroppers will be impacted by the changing coverage and special channel, making the mobile UAV have an impact on the situation of D2D based security communication.

Meanwhile, although the FD-mode D2D communication was studied [10]-[16], the UAV coverage probability with security/coverage issues in FD-mode D2D networks has still been rarely studied. In this paper, we investigate the above-mentioned problem, with the contributions of this paper reflected as follows:

- This paper not only considers the UAV's radio coverage [21], but also investigates the network security issue by adaptively adjusting the UAV's position.
- The FD technology is employed in this paper to against the D2D eavesdropping. Unlike [15] in which the base station works in the FD mode, we allow the D2D (its receivers) to work in FD mode (e.g. like in [11]-[13], [16]) to prevent eavesdropping by transmitting jamming signals [14].
- The closed form expression of the security capacity under the UAV coverage in UAV-based BS is derived, showing that the UAV-based solution not only enhance the CUs communication security, but also increase DUs' capacity (thus increase the system's sum capacity).

The remainder of this paper is organized as follows. The system model is provided in Section 2, followed by closed-form expressions for security and coverage probability in Section 3. In Section 4, we analyze the performance of the proposed scheme. Finally, Section 5 concludes this paper.

2. System Model

As illustrated in **Fig. 1**, a circular covering area with radius R_C is considered for each UAV, which acts as the mobile BS of the system of interest. The vertical position of the serving UAV in each area is denoted by o, with its floating height being h. Furthermore, both the downlink

CUs and underlay D2D transmitter are assumed to be located at (r,ϕ), where r and ϕ represent the radius and angle in a polar coordinates, respectively, with r' denoting the distance between o and the D2D receiver. In addition, the densities of CUs and DUs are assumed to be λ_c and λ_d, respectively, which follow homogeneous poisson point process (PPP) distribution Φ_c and Φ_d, respectively [26]. Note that in the proposed model the densities of eavesdroppers corresponding to each CU and DU can be represented as λ_{ec} and λ_{ed} , respectively. Apparently, both of the above-mentioned eavesdroppers follow homogeneous PPP distribution with $\lambda_c = \lambda_{ec}$ and $\lambda_d = \lambda_{ed}$, respectively. Without loss of generality, we assume that each CU has its own eavesdropper, while the D2D eavesdroppers must be associated with a D2D pair rather than a single DU. Meanwhile, we also assume that the distance between each pair of D2D peers is kept fixed in an isotropic direction [27], with d_{ec0}, d_{ed0} and d_0 representing the distance between CU and its eavesdropper, the distance between D2D pair and its eavesdropper, and the distance between the D2D pair transmitter and receiver. Finally, to prevent eavesdropping, we assume that the D2D receivers work in FD mode [1] to transmit jamming signal when they receiving the useful signals from their corresponding transmitters. We also assume that a perfect channel state information (CSI) is available in each node of interest[2].

2.1 The Channel Model of UAV-aided Networks

The proposed UAV-aided network has a typical three-dimensional (3D) architecture. In particular, when we consider the two-dimensional (2D) component of this network (i.e. on the ground), the channel attenuation between two nodes is typically assumed follow the Rayleigh distribution with unit average power, i.e. $g \sim \exp(1)$. Unlike the ground-based channels, the air-to-ground channel experiences both large-scale and small-scale fading, where we assume that the small-scale fading in the air-to-ground channel is identical to that in the ground channel [21], [30]. The received signal from the serving UAV can be expressed:

$$I_{U,i} = \begin{cases} P_{U,i} \left|X_{U,i}\right|^{-\alpha_u} g_{U,i}, & LoS \\ \eta P_{U,i} \left|X_{U,i}\right|^{-\alpha_u} g_{U,i}, & NLoS \end{cases} \tag{1}$$

- where i denotes the receiver, $\left|X_{U,i}\right| = \sqrt{h^2 + r^2}$, and the elevation angle is denoted by $\theta = (180/\pi)\arcsin\left(h/\left|X_u\right|\right)$. The probability of happening line-of-sight (LoS) propagation represented $P_L = 1/\left(1 + C\exp\left[-B\left(\theta - C\right)\right]\right)$, while the probability for appearing non-line-of-sight (NLoS) propagation is given by $P_{NL} = 1 - P_L$ [31], where η is the excessive attenuation factor for NLoS, and α_u denotes the path loss exponent, C

[1] In this paper, we assume that the self-interference in each FD device has already been suppressed to a tolerable level. The interested reader may refer to the existed literatures (e.g. [25]) for the detailed self-interference cancellation techniques.

[2] We may rely on some existing CSI estimation methods (e.g. [26]) for obtaining the CSI.

and B are parameters which depend on the environment (rural, urban, dense urban, or others).

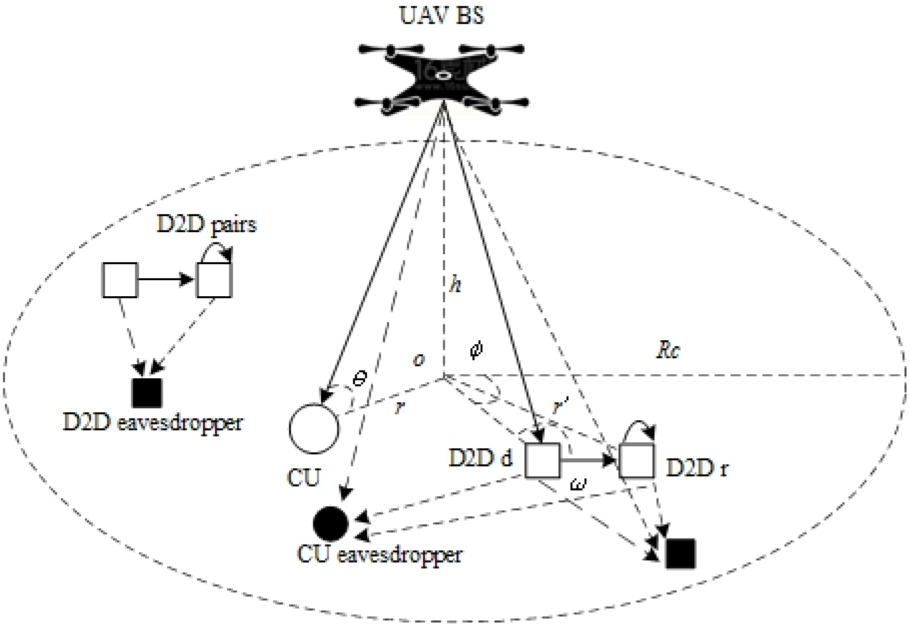


Fig. 1. UAV-aided D2D communications scenario, comprising downlink legitimate CUs, DUs and eavesdroppers.

2.2 The Received Signal-to-Interference-plus-Noise-Ratio

Following the above analysis, we list the expression of Signal-to-Interference-plus-Noise-Ratio (SINR) at different receiving terminals in the proposed UAV aided networks.

At the D2D receiver, the SINR can be expressed:

$$\gamma_d = \frac{P_d g_0 d_0^{-\alpha_d}}{I_d^d + I_d^r + I_{U,r} + I_{rr} + N} \tag{2}$$

where $I_d^d = \sum_{i\neq 0, i\in\Phi_d} P_d g_{di} d_{di}^{-\alpha_d}$ and $I_d^r = \sum_{i\neq 0, i\in\Phi_d} P_r g_{di'} d_{di'}^{-\alpha_d}$ denote the total interference from the neighboring D2D transmitters and receiver, respectively, $I_{U,r}$ is the interference induced by the serving UAV. Following (1), I_{rr} can be regarded as the residual noise after performing self-interference (SI) cancellation. As long as the SI can be cancelled to a tolerable level [28], we can readily use $I_{rr} = P_r g_{rr}$ to denote the residual SI. Furthermore, α_d is used to denote the path loss exponents, and N stands for the average power of additive noise.

The SINR for a D2D eavesdropper can thus be expressed:

$$\gamma_{ed} = \frac{P_d g_{ed0} d_{ed0}^{-\alpha_d}}{I_{ed}^d + I_{ed}^r + I_{U,ed} + N} \tag{3}$$

where $I_{ed}^{d} = \sum_{i \neq 0, i \in \Phi_d} P_d g_{edi} d_{edi}^{-\alpha_d}$ and $I_{ed}^{r} = \sum_{i \neq 0, i \in \Phi_d} P_d g_{edi'} d_{edi'}^{-\alpha_d}$ are the total interference from other D2D transmitters and receiver, respectively, and $I_{U,ed}$ denotes the interference from UAV, as given by (1).

Similarly, the SINR for a CU is given by:

$$\gamma_c = \frac{P_{U,c}}{I_c^d + I_c^r + N} \tag{4}$$

where $P_{U,c}$ is the received signal from UAV, as given (1), $I_c^d = \sum_{i \in \Phi_d} P_d g_{ci} d_{ci}^{-\alpha_d}$ and $I_c^r = \sum_{i \in \Phi_d} P_r g_{ci'} d_{ci'}^{-\alpha_d}$ denote the total interference from D2D transmitters and receiver, respectively.

Finally, the SINR for a CU eavesdropper is given by:

$$\gamma_{ec} = \frac{P_{U,ec}}{I_{ec}^d + I_{ec}^r + N} \tag{5}$$

where $P_{U,ec}$ is the received signal from UAV, as given by (1), $I_{ec}^d = \sum_{i \in \Phi_d} P_d g_{eci} d_{eci}^{-\alpha_d}$ and $I_{ec}^r = \sum_{i \in \Phi_d} P_r g_{eci'} d_{eci'}^{-\alpha_d}$ express the total interference from D2D transmitters and receiver, respectively.

3. Security Communication Under the Coverage of UAV

Next let's obtain the system's (security) capacity under the coverage of UAV, which are very meaningful to the evaluation of the system's security performance. We first analyze the coverage and security probability for DUs, followed by obtaining the system's sum data rate. Finally, we analysis the benefit brought about by employing mobile UAV.

In the following, we denote the channel capacity of each user (either CU or D2D) by C_{user}, and the channel capacity of the eavesdropper by C_{eaves}. The average security capacity of each user can be defined:

$$C_s = C_{user} - C_{eaves} = \ln\left(\frac{1+\gamma_{user}}{1+\gamma_{eaves}}\right) \approx \ln\left(\frac{\gamma_{user}}{\gamma_{eaves}}\right) \tag{6}$$

Denoting the coverage threshold of the system by β, in the case of secure communication under the UAV coverage, the secure capacity of the UAV-aided system is given by:

$$C_{\text{cov}} = W \log_2(\beta) P\left(\frac{\gamma_{user}}{\gamma_{eaves}} \geq \beta\right) \tag{7}$$

where W denotes the system bandwidth.

3.1 Coverage and Security Probability for a DU

According to the above-mentioned analysis, from (2), (3) and (6), in the case of secure communication under the UAV, the coverage of a DU is expressed:

$$\begin{aligned} P_{\text{cov},d}\left(r,\omega,\beta\right) &= \mathbb{P}\left(\frac{\gamma_d}{\gamma_{ed}} \geq \beta\right) = P_{\text{cov},d}\left(r,\beta\right) \\ &= P_{Ld}\left(r\right)P_{Led}\left(r\right)\left(1+\frac{\Phi+P_U X_{U,r}\left(r\right)^{-\alpha_u}}{\Phi+P_U X_{U,ed}\left(r\right)^{-\alpha_u}}\Psi\beta\right)^{-1}+ \\ & P_{NLd}\left(r\right)P_{Led}\left(r\right)\left(1+\frac{\Phi+\eta P_U X_{U,r}\left(r\right)^{-\alpha_u}}{\Phi+P_U X_{U,ed}\left(r\right)^{-\alpha_u}}\Psi\beta\right)^{-1}+ \\ & P_{Ld}\left(r\right)P_{NLed}\left(r\right)\left(1+\frac{\Phi+P_U X_{U,r}\left(r\right)^{-\alpha_u}}{\Phi+\eta P_U X_{U,ed}\left(r\right)^{-\alpha_u}}\Psi\beta\right)^{-1}+ \\ & P_{NLd}\left(r\right)P_{NLed}\left(r\right)\left(1+\frac{\Phi+\eta P_U X_{U,r}\left(r\right)^{-\alpha_u}}{\Phi+\eta P_U X_{U,ed}\left(r\right)^{-\alpha_u}}\Psi\beta\right)^{-1} \end{aligned} \tag{8}$$

where $X_{U,r}\left(r\right)=\sqrt{r^2+d_0^2+h^2}$, $X_{U,ed}\left(r\right)=\sqrt{r^2+d_{ed0}^2+h^2}$, $P_{Ld}\left(r\right)$, $P_{Led}\left(r\right)$, $P_{NLd}\left(r\right)$ and $P_{NLed}\left(r\right)$ are from (1), which are the probability of LoS and NLoS propagation in DU and its eavesdropper in the radius *r*, $\Phi=\frac{-\alpha'\pi^2\lambda_d}{\sin\left(\pi\alpha'\right)}\left(P_d^{\alpha'}+P_r^{\alpha'}\right)+\sigma_{r,r}^2+\sigma_N^2$, $\Psi=\left(\frac{d_0}{d_{ed0}}\right)^{-\alpha_d}$, and $\alpha'=\frac{2}{\alpha}$.

Proof: See Appendix.

Without loss of generality, we consider a uniform distribution of DUs over the coverage area of a UAV, i.e. $f\left(r,\omega\right)=\frac{r}{\pi R_C^2}$, where $0\leq r\leq R_C$ and $0\leq\omega\leq 2\pi$. The average secure coverage probability for DUs can thus be given by:

$$\overline{P}_{\text{cov},d}\left(\beta\right)=\int_0^{R_C}P_{\text{cov},d}\left(r,\beta\right)f\left(r,\omega\right)drd\omega=\int_0^{R_C}P_{\text{cov},d}\left(r,\beta\right)\frac{2r}{R_C{}^2}dr \tag{9}$$

3.2 Coverage and Security Probabilities for CUs

From (4), (5) and (6), the coverage probability with security for a typical CU can be expressed:

$$\begin{aligned} P_{\text{cov},c}\left(r,\omega,\beta\right) &= \mathbb{P}\left(\frac{\gamma_c}{\gamma_{ec}}\geq\beta\right) \\ &= \mathbb{P}\left(\frac{P_{U,c}}{I_c^d+I_c^r+N}\frac{I_{ec}^d+I_{ec}^r+N}{P_{U,ec}}\geq\beta\right) \end{aligned} \tag{10}$$

assuming that $\mathbb{E}_{I_c^d,I_c^r}\left(I_c^d+I_c^r+N\right)=\mathbb{E}_{I_{ec}^d,I_{ec}^r}\left(I_{ec}^d+I_{ec}^r+N\right)$, according to appendix, (10) can be simplified as $\mathbb{P}\left[\frac{P_{U,c}}{\mathbb{E}_{I_c^d,I_c^r}\left(I_c^d+I_c^r+N\right)}\frac{\mathbb{E}_{I_{ec}^d,I_{ec}^r}\left(I_{ec}^d+I_{ec}^r+N\right)}{P_{U,ec}}\ge\beta\right]=P\left(\frac{P_{U,c}}{P_{U,ec}}\ge\beta\right)$, implying that

$$P\left(\frac{\left|X_{U,c}\right|^{-\alpha_u}g_c}{\left|X_{U,ec}\right|^{-\alpha_u}g_{ec}}\ge\beta\right)=\frac{1}{1+X\left(r\right)^{-\alpha_u}\beta} \tag{11}$$

where $X\left(r\right)=\frac{X_{U,ec}\left(r\right)}{X_{U,ec}\left(r\right)}=\sqrt{\frac{r^2+h^2}{r^2+d_{ec0}^2+h^2}}$. Consequently, the (secure) coverage of a typical CU can be expressed:

$$\begin{aligned}P_{\text{cov},c}\left(r,\beta\right)=&P_{Lc}\left(r\right)P_{Lec}\left(r\right)\frac{1}{1+X\left(r\right)^{-\alpha_u}\beta}+P_{NLc}\left(r\right)P_{Lec}\left(r\right)\frac{1}{1+\frac{1}{\eta}X\left(r\right)^{-\alpha_u}\beta}\\&+P_{Lc}\left(r\right)P_{NLec}\left(r\right)\frac{1}{1+\eta X\left(r\right)^{-\alpha_u}\beta}+P_{NLc}\left(r\right)P_{NLec}\left(r\right)\frac{1}{1+X\left(r\right)^{-\alpha_u}\beta}\end{aligned} \tag{12}$$

where $P_{Lc}\left(r\right)$, $P_{Lec}\left(r\right)$, $P_{NLc}\left(r\right)$and $P_{NLec}\left(r\right)$ are also from (1), which are the probability of LoS and NLoS propagation in DU and its eavesdropper in the radius *r*. Similar to (9), the average (secure) coverage probability of a typical CU over a UAV coverage is:

$$\overline{P}_{\text{cov},c}\left(\beta\right)=\int_0^{R_C}P_{\text{cov},c}\left(r,\beta\right)\frac{2r}{{R_C}^2}dr \tag{13}$$

3.3 System Sum-Rate Analysis

From (7), (9) and (13), the average achievable secure data rates for either the CUs and or the DUs can be expressed:

$$\begin{cases}\overline{C}_d=W\log_2\left(\beta\right)\overline{P}_{\text{cov},d}\left(\beta\right)\\\overline{C}_c=W\log_2\left(\beta\right)\overline{P}_{\text{cov},c}\left(\beta\right)\end{cases} \tag{14}$$

Hence, the sum data rate of the whole system is thus given by:

$$\overline{C}_{sum}=\pi R_C^2\left(\lambda_c\overline{C}_c+\lambda_d\overline{C}_d\right) \tag{15}$$

3.4 The Benefits Brought About by Employing Mobile UAV

Under the circular-shaped UAV secure coverage, the formula (9) and (13) have shown that the CU's secure coverage probability is a function of both h and R_C (but not of P_U). In this case, the mobile UAV is capable of both providing secure communication enhancement with variant h values and serving area after performing parameter adjustment. Here, we use the method of "stop points" [21], in which the UAV stops at each prescribed stop point and serves the present downlink users over a given radius. This approach adopts the disk covering method [32] for finding the minimum number of disks over circle R_C, followed by adjusting the height of UAV to ensure both the coverage and security in communications. The example of disk covering is illustrated in **Fig. 2**, in which the minimum number of stop points M for covering the area was illustrated in [21], [32]. We regard the requirement of coverage probability under the secure communication as the coverage probability that is not less than the threshold ε.

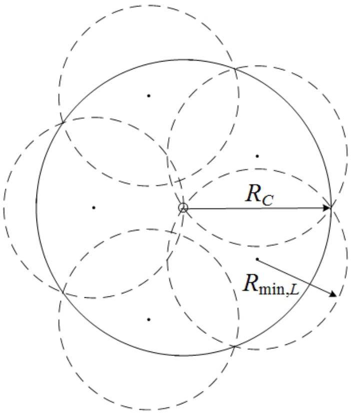


Fig. 2. Disks covering area of five small circles.

First, we compute the coverage radius of the UAV based on the minimum requirement for the DUs' coverage probability, which is supposed to be beyond ε:

$$r_C = \max\left\{R \mid \overline{P}_{\text{cov},c}\left(\beta\right) \geq \varepsilon, R_C, h\right\} = \overline{P}_{\text{cov},c}^{-1}\left(\beta, \varepsilon\right) \tag{16}$$

Note that only the users within the coverage of circle r_C are allowed to be activated in the proposed scheme. The minimum number of stop points for the full coverage is thus given by:

$$L = \min\left\{M\right\}, \quad R_{\min,L} \leq r_C \leq R_{\min,L-1} \tag{17}$$

provided that

$$\overline{P}_{\text{cov},c}\left(\beta, h, R_{\min,L}\right) \geq \varepsilon \tag{18}$$

is satisfied, where L denotes the minimum number of stop points, $R_{\min,L}$ is the radius corresponding to L smaller circles. After calculating $R_{\min,L}$, we may readily adjust h for optimizing the performance of the system. The optimal height of UAV can be calculated:

$$h_{opt} = \arg\min_{h}\left\{\overline{P}_{\text{cov},c}^{-1}\left(\beta, \varepsilon\right) = R_{\min,L} \mid h\right\} \tag{19}$$

4. Simulation Results and Analysis

In this section, let's first compare our analytical results with the numerical results, for which the simulation parameters are summarized in **Table 1**. (following [21], [25]).

The proposed scheme for HD mode and FD mode in simulation performance is shown in **Fig. 3**, which shows the coverage probability of CU and DU. As we can see, the result are very close, the reason is that as the DUs work in the underlay cellular networks, they would have been interfere with each other no matter the existence of eavesdroppers. So, when one of the DU in its pair works in FD mode, it not only interferes with its eavesdroppers, but also interfere themselves.

Table 1. Part of fundamental properties of self-organization network

Parameters	Values
D2D pair fix distance d_0	20m
The distance of D2D transmitter to its eavesdropper d_{ed}	25m
The distance of CU to its eavesdropper d_{ec}	30m
Path loss exponent α_d ; α_u	2.2; 3
Noise power σ_r^2	-120dBm
Residual SI after SI cancellation σ_{rr}^2	-100dBm
Parameters for dense urban environment B; C	0.136; 11.95
Excessive attenuation factor for NLoS η	20dB
Bandwidth W	$10^{-6}Hz$

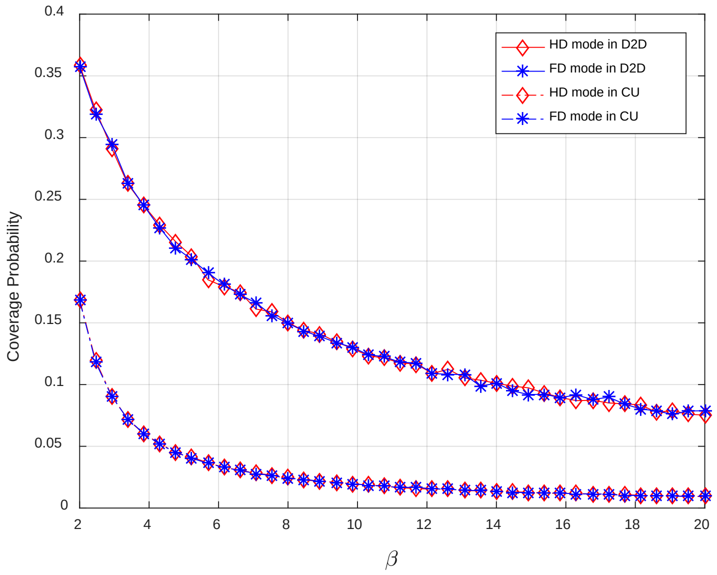


Fig. 3. The proposed scheme for HD mode and FD mode in simulation performance.

In **Fig. 4**, it gives out the secure coverage probabilities of both the DUs and CUs for variant thresholds, i.e. $\lambda_c = \lambda_d = 1\times10^{-4}m^2$, $P_d = P_r = 0.05W$, $P_U = 3W$, $h = 50m$, and $R_C = 300m$. It is shown that the analytical results for both users match the simulation results, especially with larger β values. Meanwhile, it also shows that the secure coverage probabilities for both users will decrease as β increases. Furthermore, from (9) and (13), it is shown that the CU's secure coverage probability is only relate to the relative position with UAV and their eavesdroppers, and the scope of communication area. While the secure coverage of DUs are affected by many parameters, as the impact of d_0, d_{ed} and d_{ec} are obvious, we will not analyze these parameters for simplify.

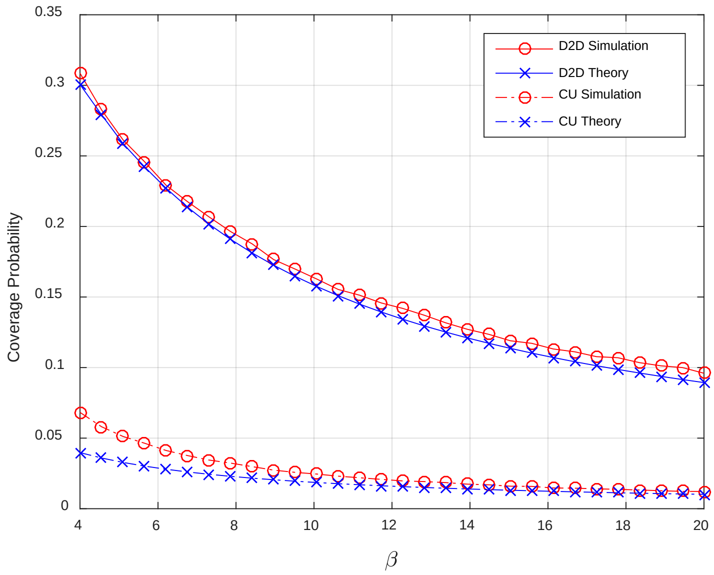


Fig. 4. Coverage probability vs. β of the proposed scheme.

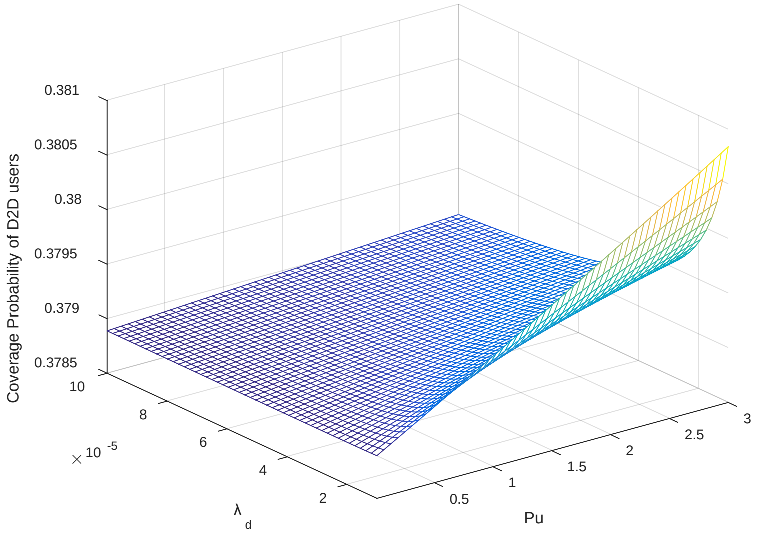


Fig. 5. Coverage probability for DUs vs. P_U and λ_d of the proposed scheme.

In **Fig. 5**, it evaluates the impact of both P_U and λ_d on DUs. To guarantee a security communication, the coverage probability of DUs is a monotonically increasing function of P_U, implying that the UAV is capable of producing interference to D2D eavesdroppers, thus improving the system's secure capacity.

In **Fig. 6**, we evaluate the coverage probability of DUs under variant P_d and P_r. It is worth noting that the coverage probability will be inversely proportional to the transmit power (as the latter produces interference to the users), so decreasing DUs' transmit power will not only increase their energy efficiency, but also increase their coverage probability.

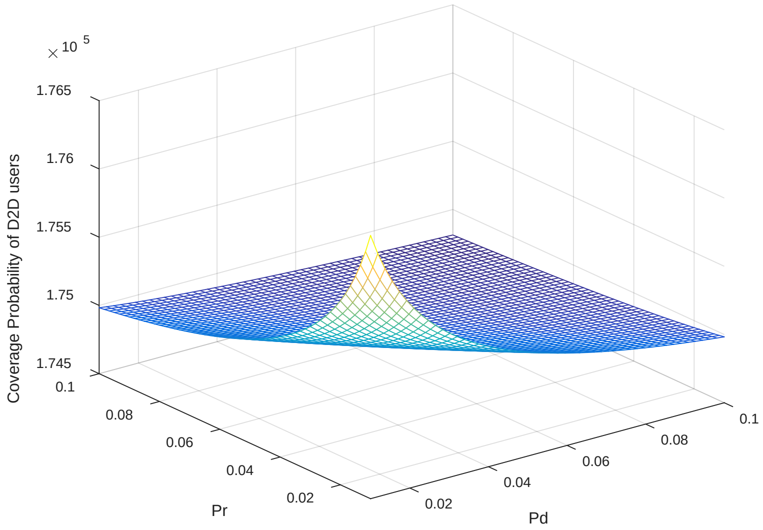


Fig. 6. Coverage probability for DUs vs. P_d and P_r of the proposed scheme.

In **Fig. 7** and **Fig. 8**, the impacts of R_C and h on CUs and DUs' coverage probability are evaluated. In particular, in **Fig. 7**, smaller communication area implies a higher CUs' coverage probability, while a lower altitude of UAV makes it decreased. In **Fig. 8**, on the other hand, it is shown that the DUs' coverage probability increases as h decreases, similar to **Fig. 5**. When the communication area becomes larger, the coverage probability will be a monotonically decreasing function of the area with an increasing logarithmic function with small range.

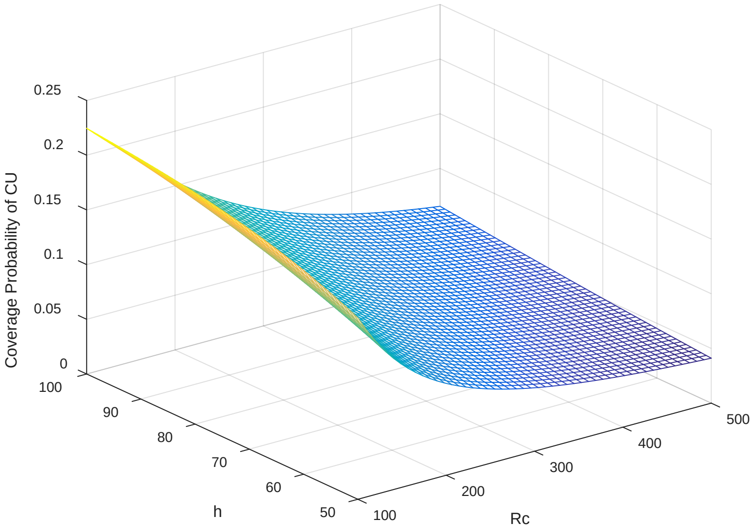


Fig. 7. Coverage probability for CUs vs. h and R_C of the proposed scheme.

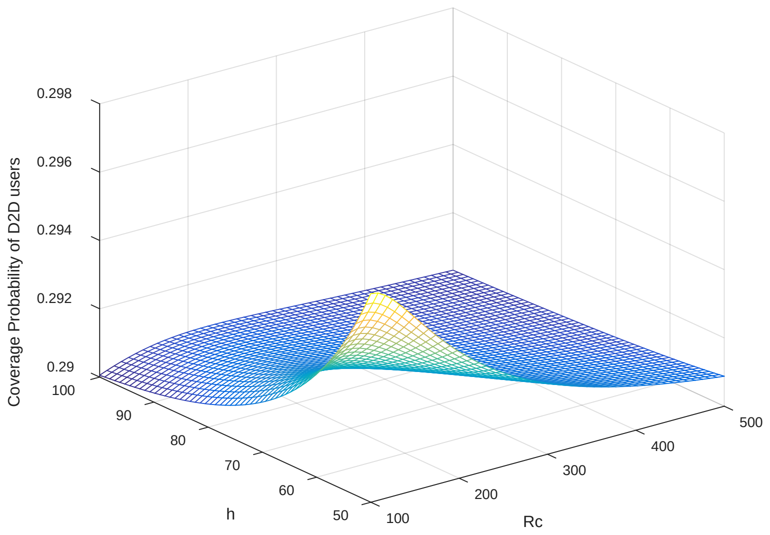


Fig. 8. Coverage probability for DUs vs. *h* and R_C of the proposed scheme.

Fig. 9 and **Fig. 10** are show separately the stop points and average sum capacity changes in secure communication under the coverage of a mobile UAV and a static UAV with $\varepsilon = 0.15$, at this time, $\lambda_c = 1\times10^{-4}m^2$, $\lambda_d = 0.5\times10^{-4}m^2$, $d_0 = 30m$. The results in the two figures with the same color correspond to the same simulation parameters. From **Fig. 9**, when $h = 100m$, the changes of stop points are the same (black, green and red curves), when *h* decrease to 80, the number of stop points increased (blue curves), that is the length of *h* affects the change of stop points. And corresponds to **Fig. 10**, the sum capacity increased (black and blue curves), at the time, the users' densities are the same. Meanwhile, it can be seen from **Fig. 7** and **Fig. 8** that the influence of *h* on D2D user and DU are opposite, that is lower *h* increase D2D users' capacity and decrease CUs', but the sum system capacity is increasing. At the same time, when D2D users' density or CUs' is half of each other (green or magenta curve), the sum capacity in the system is lower than before. Therefore, to improve the sum capacity of the system, the density of D2D users' and CUs' should be equal and *h* should reduce.

Fig. 9 and **Fig. 10** are show separately the stop points and average sum capacity changes in secure communication under the coverage of a mobile UAV and a static UAV with $\varepsilon = 0.15$, at this time, $\lambda_c = 1\times10^{-4}m^2$, $\lambda_d = 0.5\times10^{-4}m^2$, $d_0 = 30m$. The results in the two figures with the same color correspond to the same simulation parameters. From **Fig. 9**, when $h = 100m$, the changes of stop points are the same (black, green and red curves), when *h* decrease to 80, the number of stop points increased (blue curves), that is the length of *h* affects the change of stop points. And corresponds to **Fig. 10**, the sum capacity increased (black and blue curves), at the time, the users' densities are the same. Meanwhile, it can be seen from **Fig. 7** and **Fig. 8** that the influence of *h* on D2D user and DU are opposite, that is lower *h* increase D2D users' capacity and decrease CUs', but the sum system capacity is increasing. At the same time, when D2D users' density or CUs' is half of each other (green or magenta curve), the sum capacity in the system is lower than before. Therefore, to improve the sum capacity of the system, the density of D2D users' and CUs' should be equal and *h* should reduce.

The “disk coverage” solutions can enhance the system capacity even in the presence of eavesdropping. At the same time, from Section 3.4, the “disk coverage” solution is capable of keeping the CUs coverage at a constant value while do not decrease with R_C, so that the performance improvement in terms of sum capacity actually comes from the contribution of D2D users. Consequently, the mobile UAV solution not only enhances the system’s security, but also increases the sum capacity.

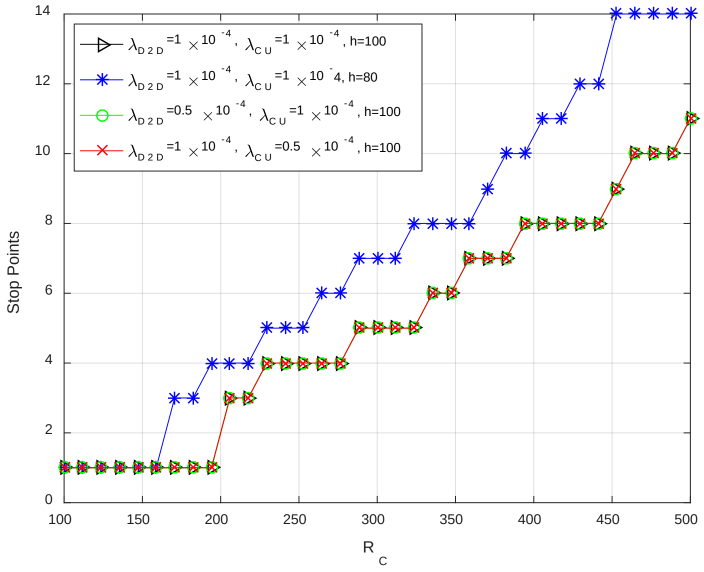


Fig. 9. The stop points change under the coverage of mobile UAV-based BS.

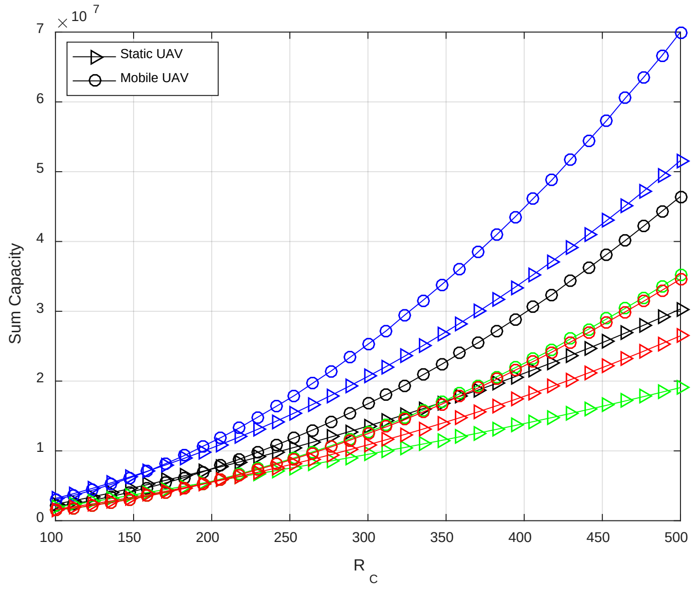


Fig. 10. The average sum capacity of the proposed scheme.

5. Conclusion

In this paper, we consider the security problem of UAV coverage FD D2D network, and obtain the expressions of system capacity under the UAV coverage. In the situation, both CUs and DUs assumed to suffer from eavesdropping. To guarantee a secure communication, an FD mode D2D receiver employed for transmitting jamming signal to its eavesdropper. Furthermore, the expressions show that the secure coverage probability in CUs is a function of the relative position of UAV, and a larger received power from UAV implies a higher secure coverage probability in DUs.

Appendix

The probability $P_{\text{cov},d}\left(r,\omega,\beta\right)$ can be calculated:

$$\begin{aligned}
P_{\text{cov},d}\left(r,\omega,\beta\right) &= \mathbb{P}\left(\frac{\gamma_d}{\gamma_{ed}} \geq \beta\right) \\
&= \mathbb{P}\left(\frac{P_d g_0 d_0^{-\alpha_d}}{I_d^d + I_d^r + I_{U,r} + I_{rr} + N} \frac{I_{ed}^d + I_{ed}^r + I_{U,ed} + N}{P_d g_{ed0} d_{ed0}^{-\alpha_d}} \geq \beta\right) \\
&= P\left[\frac{\mathbb{E}_{I_{ed}^d, I_{ed}^r, I_{U,ed}}\left(I_{ed}^d + I_{ed}^r + I_{U,ed} + N\right)}{\mathbb{E}_{I_d^d, I_d^r, I_{U,r}}\left(I_d^d + I_d^r + I_{U,r} + I_{rr} + N\right)}\left(\frac{d_0}{d_{ed0}}\right)^{-\alpha_d} \frac{g_0}{g_{ed0}} \geq \beta\right] \\
&= \frac{1}{1 + \frac{\mathbb{E}_{I_d^d, I_d^r, I_{U,r}}\left(I_d^d + I_d^r + I_{U,r} + I_{rr} + N\right)}{\mathbb{E}_{I_{ed}^d, I_{ed}^r, I_{U,ed}}\left(I_{ed}^d + I_{ed}^r + I_{U,ed} + N\right)}\left(\frac{d_0}{d_{ed0}}\right)^{-\alpha_d} \beta}
\end{aligned} \tag{20}$$

Following the PPP distribution, the interference imposed on the D2D receivers due to the neighboring users is independent of their locations. The expectations of the interference can be calculated:

$$\begin{aligned}
&\mathbb{E}_{I_d^d, I_d^r, I_{U,r}}\left(I_d^d + I_d^r + I_{U,r} + I_{rr} + N\right) \\
&= \mathbb{E}_{d_{di}}\left(I_d^d\right) + \mathbb{E}_{d_{di}'}\left(I_d^r\right) + \mathbb{E}\left(I_{U,r}\right) + I_{rr} + N
\end{aligned} \tag{21}$$

and

$$\begin{aligned}
&\mathbb{E}_{I_{ed}^d, I_{ed}^r, I_{U,ed}}\left(I_{ed}^d + I_{ed}^r + I_{U,ed} + N\right) \\
&= \mathbb{E}_{d_{edi}}\left(I_{ed}^d\right) + \mathbb{E}_{d_{edi}'}\left(I_{ed}^r\right) + \mathbb{E}\left(I_{U,ed}\right) + N
\end{aligned} \tag{22}$$

The first part of (21) is given by:

$$\mathbb{E}_{d_{di}}\left(I_d^d\right) = \mathbb{E}_{I_d^d}\left(\sum_{i \neq 0} P_d g_{di} d_{di}^{-\alpha_d}\right) = \mathbb{E}_{d_{di}}\left\{\ln\left[\exp\left(\sum_{i \neq 0} P_d g_{di} d_{di}^{-\alpha_d}\right)\right]\right\} \tag{23}$$

For an exponential function, we can calculate its mean value:

$$\begin{aligned} &\mathbb{E}_{d_{di}}\left[\exp\left(\sum_{i\neq 0} P_d g_{di} d_{di}^{-\alpha_d}\right)\right] = \mathbb{E}_{d_{di}}\left[\prod_{i\neq 0}\exp\left(P_d g_{di} d_{di}^{-\alpha_d}\right)\right] \\ &= \mathbb{E}_{d_{di}}\left[\prod_{i\neq 0}\int_0^\infty e^{P_d d_{di}^{-\alpha_d} x} e^{-x} dx\right] = \mathbb{E}_{d_{di}}\left[\prod_{i\neq 0}\frac{1}{1-P_d d_{di}^{-\alpha_d}}\right] \\ &\overset{(a)}{=} \exp\left[-\lambda_d \int_0^\infty \left(1-\frac{1}{1-P_d d_{di}^{-\alpha_d}}\right) 2\pi x dx\right] \\ &= \exp\left[\frac{-\alpha'\pi^2\lambda_d \left(P_d\right)^{\alpha'}}{\sin\left(\pi\alpha'\right)}\right] \end{aligned} \tag{24}$$

where $\alpha' = \frac{2}{\alpha}$, and step (a) follows [33]. Taking the result into Logarithmic function, (23) becomes:

$$\mathbb{E}_{d_{di}}\left(I_d^d\right) = \frac{-\alpha'\pi^2\lambda_d P_d^{\alpha'}}{\sin\left(\pi\alpha'\right)} \tag{25}$$

From (24), the second item of (21) becomes:

$$\mathbb{E}_{d_{di}'}\left(I_d^r\right) = \frac{-\alpha'\pi^2\lambda_d P_r^{\alpha'}}{\sin\left(\pi\alpha'\right)} \tag{26}$$

Assume that the D2D receiver is located inside the circle with radius d_0 in its transmitter, we have: $\mathbb{E}\left(r'\right)^2 = \frac{1}{\pi}\int_0^\pi \left(r^2 + d_0^2 - 2rd_0\cos(\omega)\right) d\omega = r^2 + d_0^2$. Therefore, the average distance between UAV and D2D receiver is $X_{U,r}\left(r\right)^2 = \mathbb{E}\left(r'\right)^2 + h^2 = r^2 + d_0^2 + h^2$. Furthermore, the third item of (21) can be calculated:

$$\mathbb{E}\left[I_{U,r}\left(r\right)\right] = \begin{cases} P_U X_{U,r}\left(r\right)^{-\alpha_u}\int_0^\infty xe^{-x}dx & \\ = P_U X_{U,r}\left(r\right)^{-\alpha_u}, & LoS \\ \eta P_U X_{U,r}\left(r\right)^{-\alpha_u}\int_0^\infty xe^{-x}dx & \\ = \eta P_U X_{U,r}\left(r\right)^{-\alpha_u}, & NLoS \end{cases} \tag{27}$$

Hence, (21) can be rewritten:

$$\begin{aligned} &\mathbb{E}_{I_d^d, I_d^r, I_{U,r}}\left(I_d^d + I_d^r + I_{U,r} + I_{rr} + N\right) \\ &= \frac{-\alpha'\pi^2\lambda_d}{\sin\left(\pi\alpha'\right)}\left(P_d^{\alpha'} + P_r^{\alpha'}\right) + \mathbb{E}\left[I_{U,r}\left(r\right)\right] + \sigma_{r,r}^2 + \sigma_N^2 \end{aligned} \tag{28}$$

According to the previous equation, the interference (22) becomes:

$$\begin{aligned} &\mathbb{E}_{I_{ed}^d, I_{ed}^r, I_{U,ed}}\left(I_{ed}^d + I_{ed}^r + I_{U,ed} + N\right) \\ &= \frac{-\alpha'\pi^2\lambda_d}{\sin\left(\pi\alpha'\right)}\left(P_d^{\alpha'} + P_r^{\alpha'}\right) + \mathbb{E}\left[I_{U,ed}\left(r\right)\right] + \sigma_N^2 \end{aligned} \tag{29}$$

where $\mathbb{E}_{d_{edi}}\left(I_{ed}^{d}\right)=\frac{-\alpha'\pi^{2}\lambda_{d}P_{d}^{\alpha'}}{\sin\left(\pi\alpha'\right)}$, $\mathbb{E}_{d_{edi}'}\left(I_{ed}^{r}\right)=\frac{-\alpha'\pi^{2}\lambda_{d}P_{r}^{\alpha'}}{\sin\left(\pi\alpha'\right)}$,

$\mathbb{E}\left[I_{U,ed}\left(r\right)\right]=\begin{cases} P_{U}X_{U,ed}\left(r\right)^{-\alpha_{u}}, & LoS \\ \eta P_{U}X_{U,ed}\left(r\right)^{-\alpha_{u}}, & NLoS \end{cases}$, and $X_{U,ed}\left(r\right)^{2}=r^{2}+d_{ed0}^{2}+h^{2}$.

Therefore, in the case of secure communication, the coverage of a single DU can be given by:

$$\begin{aligned}
P_{\mathrm{cov},d}\left(r,\omega,\beta\right)&=\mathbb{P}\left(\frac{\gamma_{d}}{\gamma_{ed}}\geq\beta\right)=P_{\mathrm{cov},d}\left(r,\beta\right)\\
&=P_{Ld}\left(r\right)P_{Led}\left(r\right)\left(1+\frac{\Phi+P_{U}X_{U,r}\left(r\right)^{-\alpha_{u}}}{\Phi+P_{U}X_{U,ed}\left(r\right)^{-\alpha_{u}}}\Psi\beta\right)^{-1}+\\
&P_{NLd}\left(r\right)P_{Led}\left(r\right)\left(1+\frac{\Phi+\eta P_{U}X_{U,r}\left(r\right)^{-\alpha_{u}}}{\Phi+P_{U}X_{U,ed}\left(r\right)^{-\alpha_{u}}}\Psi\beta\right)^{-1}+\\
&P_{Ld}\left(r\right)P_{NLed}\left(r\right)\left(1+\frac{\Phi+P_{U}X_{U,r}\left(r\right)^{-\alpha_{u}}}{\Phi+\eta P_{U}X_{U,ed}\left(r\right)^{-\alpha_{u}}}\Psi\beta\right)^{-1}+\\
&P_{NLd}\left(r\right)P_{NLed}\left(r\right)\left(1+\frac{\Phi+\eta P_{U}X_{U,r}\left(r\right)^{-\alpha_{u}}}{\Phi+\eta P_{U}X_{U,ed}\left(r\right)^{-\alpha_{u}}}\Psi\beta\right)^{-1}
\end{aligned}\tag{30}$$

where $X_{U,r}\left(r\right)=\sqrt{r^{2}+d_{0}^{2}+h^{2}}$, $X_{U,ed}\left(r\right)=\sqrt{r^{2}+d_{ed0}^{2}+h^{2}}$, $P_{Ld}\left(r\right)$, $P_{Led}\left(r\right)$, $P_{NLd}\left(r\right)$ and $P_{NLed}\left(r\right)$ are from (1), which are the probability of LoS and NLoS propagation in DU and its eavesdropper in the radius r, $\Phi=\frac{-\alpha'\pi^{2}\lambda_{d}}{\sin\left(\pi\alpha'\right)}\left(P_{d}^{\alpha'}+P_{r}^{\alpha'}\right)+\sigma_{r,r}^{2}+\sigma_{N}^{2}$,

$\Psi=\left(\frac{d_{0}}{d_{ed0}}\right)^{-\alpha_{d}}$, and $\alpha'=\frac{2}{\alpha}$.

References

[1] X. Ge, S. Tu, G. Mao, et al., "5G Ultra-Dense Cellular Networks," *IEEE Wireless Communications*, Vol. 23, No. 1, pp.72-79, 2016. Article (CrossRef Link).

[2] J. An, K. Yang, J. Wu, N. Ye, S. Guo, and Z. Liao, "Achieve sustainable ultra-dense heterogeneous networks for 5G," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 84-90, Dec. 2017. Article (CrossRef Link).

[3] J. Sun, T. Liu, X. Wang, C. Xing, H. Xiao, A. V. Vasilakos, and Z. Zhang, "Optimal mode selection with uplink data rate maximization for D2D-aided underlaying cellular networks," *IEEE Access*, vol. 4, pp. 8844-8856, 2016. Article (CrossRef Link).

[4] J. Sun, Z. Zhang, H. Xiao, C. Xing, "Uplink interference coordination management with power control for D2D underlaying cellular networks: modeling, algorithms and analysis," *IEEE Transactions on Vehicular Technology*, vol.67, no. 9, pp. 8582-8594, 2018. Article (CrossRef Link).

[5] P. Gandotra, R. K. Jha, and S. Jain, "A survey on device-to-device (D2D) communication: architecture and security issues," *Journal of Network and Computer Applications*, vol. 78, pp. 9-29, 2017. Article (CrossRef Link).

[6] J. Wang, Q. Tang, C. Yang, R. Schober, and J. Li, "Security enhancement via Device-to-device communication in cellular networks," *IEEE Signal Processing Letters*, vol. 23, no. 11, pp. 1622-1626, 2016. Article (CrossRef Link).

[7] W. Mei, Z. Chen, J. Fang, and B. Fu, "Secure D2D-enabled cellular communication against selective eavesdropping," in *Proc. of IEEE International Conference on Communications (ICC)*, pp. 1-7, 2017. Article (CrossRef Link).

[8] B. Zhong, Z. Zhang, "Secure full-duplex two-way relaying networks with optimal relay selection," *IEEE Communications Letters*, vol. 21, no. 5, pp. 1123-1126, 2017. Article (CrossRef Link).

[9] B. Zhong, Z. Zhang, "Opportunistic two-way full-duplex relay selection in underlay cognitive networks," *IEEE System Journal*, vol. 12, no. 1, pp. 725-734, 2018. Article (CrossRef Link).

[10] K. S. Ali, H. ElSawy, and M.-S. Alouini, "Modeling cellular networks with full-duplex D2D communication: A stochastic geometry approach," *IEEE Transactions on Communications*, vol. 64, no. 10, pp. 4409-4424, 2016. Article (CrossRef Link).

[11] X. Chai, T. Liu, C. Xing, H. Xiao, and Z. Zhang, "Throughput improvement in cellular networks via full-duplex based device-to-device communications," *IEEE Access*, vol. 4, pp. 7645-7657, 2016. Article (CrossRef Link).

[12] H. Bagheri, F. A. M. Bonomi, and M. Katz, "Spectral efficiency and throughput enhancement by full-duplex D2D communication in mobile clouds," in *Proc. of 21th European Wireless Conference. VDE*, pp. 1-6, 2015. Article (CrossRef Link).

[13] M. R. Khandaker, C. Masouros, and K.-K. Wong, "Secure full-duplex Device-to-device communication," in *Proc. of IEEE Globecom Workshops*, pp. 1-6, 2017. Article (CrossRef Link).

[14] G. Chen, G. Yu, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 574-583, 2015. Article (CrossRef Link).

[15] Y. Sun, D. W. K. Ng, J. Zhu, and R. Schober, "Multi-objective optimization for robust power efficient and secure full duplex wireless communication systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 8, pp. 5511-5526, 2016. Article (CrossRef Link).

[16] S. Han, P. Chen, and C. Yang, "Full duplex assisted interference suppression for underlay device-to-device communications," in *Proc. of IEEE Globecom Workshops*, pp. 851-856, 2014. Article (CrossRef Link).

[17] X. Ge, Z Li, S. Li. "5G software defined vehicular networks," *IEEE Communications Magazine*, vol. 55, no. 7, pp. 87-93, 2017. Article (CrossRef Link).

[18] A. Orsino, A. Ometov, G. Fodor, D. Moltchanov, L. Militano, S. Andreev, O. N. Yilmaz, T. Tirronen, J. Torsner, G. Araniti, et al., "Effects of heterogeneous mobility on D2D-and drone-assisted mission-critical MTC in 5G," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 79-87, 2017. Article (CrossRef Link).

[19] X. Li, D. Guo, H. Yin, and G. Wei, "Drone-assisted public safety wireless broadband network," in *Proc. of IEEE Wireless Communications and Networking Conference Workshops* (WCNCW), pp. 323-328, 2015. Article (CrossRef Link).

[20] A. Omri, M. O. Hasna, and M. Z. Shakir, "Mode selection schemes for D2D enabled aerial networks," *arXiv preprint arXiv:1711.02220*, pp.1-4, 2017. Article (CrossRef Link).

[21] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Unmanned aerial vehicle with underlaid device-to-device communications: Performance and tradeoffs," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 3949-3963, 2016. Article (CrossRef Link).

[22] X. Ge, K. Huang, C. X. Wang, et al. "Capacity analysis of a multi-cell multi-antenna cooperative cellular network with co-channel interference," *IEEE Transactions on Wireless Communications*, vol. 10, no. 10, pp. 3298-3309, 2011. Article (CrossRef Link).

[23] F. Tang, Z. M. Fadlullah, N. Kato, F. One, and R. Miura, “AC-POCA: Anti-coordination game based partially overlapping channels assignment in combined UAV and D2D-Based networks,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 2, pp. 1672-1683, 2018. Article (CrossRef Link).

[24] Y. Chang, H. Chen, and F. Zhao, “Energy efficiency maximization of full-duplex two-way relay-assisted device-to-device communications underlaying cellular networks,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, no. 1, 2016. Article (CrossRef Link).

[25] B. Zhong, J. Zhang, Q. Zeng, and X. Dai, “Coverage probability analysis for full-duplex relay aided device-to-device communications networks,” *China Communications*, vol. 13, no. 11, pp. 60-67, 2016. Article (CrossRef Link).

[26] M. Haenggi, “Stochastic geometry for wireless networks,” *Cambridge University Press*, 2012. Article (CrossRef Link).

[27] N. Lee, X. Lin, J. G. Andrews, and R. W. Heath, “Power control for D2D underlaid cellular networks: modeling, algorithms, and analysis,” *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 1, pp. 1-13, 2015. Article (CrossRef Link).

[28] Z. Zhang, K. Long, A. V. Vasilakos, and L. Hanzo, “Full-duplex wireless communications: challenges, solutions and future research directions,” *IEEE Proceedings*, vol. 104, no. 7, pp. 1369-1409, 2016. Article (CrossRef Link).

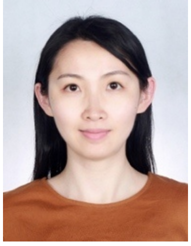
[29] H. Cui, M. Ma, L. Song, and B. Jiao, “Relay selection for two-way full duplex relay networks with amplify-and-forward protocol,” *IEEE Transactions on Wireless Communications*, vol. 13, no. 7, pp. 3768-3777, 2014. Article (CrossRef Link).

[30] X. Qi, B. Li, Z. Chu, K. Huang, and H. Chen, “Secrecy energy efficiency performance in communication networks with mobile sinks,” *Physical Communications*, vol. 32, pp. 41-49, 2019. Article (CrossRef Link).

[31] A. Al-Hourani, S. Kandeepan, and S. Lardner, “Optimal lap altitude for maximum coverage,” *IEEE Wireless Communications Letters*, vol. 3, no. 6, pp. 569-572, 2014. Article (CrossRef Link).

[32] R. Kershner, “The number of circles covering a set,” *American Journal of mathematics*, vol. 61, no. 3, pp. 665-671, 1939. Article (CrossRef Link).

[33] D. Stoyan, S. N. Chiu, W. S. Kendall, et al., “Stochastic geometry and its applications,” *Journal of the Royal Statistical Society*, vol. 151, no. 1, pp. 239-240, 1988. Article (CrossRef Link).



Qian Zeng, received her B.S. degree in Guangxi Normal University, Guangxi, China in 2008, the M.S. degree in Guilin University of Electronic Technology, Guilin, China in 2015. She is currently working toward the D.S. degree in University of Science and Technology Beiing (USTB), Beiing, China. Her current research interests include Unmanned Aerial Vehicles (UAVs) aided communication system, D2D communication system and cooperative communications. Email: zengqian617@foxmail.com.

Zhongshan Zhang, received the B.E. and M.S. degrees in computer science from the Beijing University of Posts and Telecommunications (BUPT) in 1998 and 2001, respectively, and received Ph.D. degree in electrical engineering in 2004 from BUPT. From Aug. 2004 he joined DoCoMo Beijing Laboratories as an associate researcher, and was promoted to be a researcher in Dec. 2005. From Feb. 2006, he joined University of Alberta, Edmonton, AB, Canada, as a postdoctoral fellow. From Apr. 2009, he joined the Department of Research and Innovation (R&I), Alcatel-Lucent, Shanghai, as a Research Scientist. From Aug. 2010 to Jul. 2011, he worked in NEC China Laboratories, as a Senior Researcher. He served or is serving as a Guest Editor and/or an editor for several technical journals, such as the IEEE Communications Magazine and KSII Transaction on Internet and Information System. He is currently a professor of the School of Communication and Electronics in Beijing Institute of Technology (BIT). His main research interests include statistical signal processing, self-organized networking, cognitive radio, and cooperative communications. Email: zhangzs@bit.edu.cn.