Secrecy Rate Analysis of UAV-Enabled mmWave Networks Using Matérn Hardcore Point Processes

Yongxu Zhu, Gan Zheng, *Senior Member, IEEE* and Michael Fitch

***Abstract*—Communications aided by low-altitude unmanned aerial vehicles (UAVs) have emerged as an effective solution to provide large coverage and dynamic capacity for both military and civilian applications, especially in unexpected scenarios. However, because of their broad coverage, UAV communications are prone to passive eavesdropping attacks. This paper analyzes the secrecy performance of UAVs networks at the millimeter wave (mmWave) band and takes into account unique features of air-to-ground channels and practical constraints of UAV deployment. To be specific, it explores the 3D antenna gain in the air-to-ground links and uses the Matérn hardcore point process to guarantee the safety distance between the randomly deployed UAV base stations. In addition, we propose the transmit jamming strategy to improve the secrecy performance in which part of UAVs send jamming signals to confound the eavesdroppers. Simulation results verify our analysis and demonstrate the impact of different system parameters on the achievable secrecy rate. It is also revealed that optimizing the density of jamming UAVs will significantly improve security of UAV-enabled networks.**

***Index Terms*—Unmanned aerial vehicles, physical layer security, Matérn hardcore process, millimeter wave (mm-wave), 3D antenna pattern.**

I. Introduction

Wireless communications networks have experienced unprecedented data growth and the resulting need for high-speed ubiquitous and irregular access is beyond the capabilities of existing infrastructures [1]. Current terrestrial communication systems are rigidly planned based on the long-term traffic statistics, and cannot cope with the unexpected and temporary demands in festival events, search and rescue, etc. Recently low-altitude unmanned aerial vehicles (UAVs) flying at several hundred metres to a few kilometres have attracted growing interest in providing agile communications because of their mobility and elevated positions [2, 3]. Compared to the terrestrial systems, UAVs can overcome the propagation constraints due to terrain characteristics and augment the coverage area. UAV base stations (BSs) can also be rapidly deployed, thus address the capital expenditure and operating expenses issues in future networks, which cannot be handled alone by the current terrestrial systems.

Security is a major concern that hinders the wide deployment of UAV-enabled communication networks. Due to the inherent broadcasting nature of wireless communications and the broad coverage area, UAV-enabled communication networks – whether civil or military – are particularly prone to security threats. To guarantee perfect security, eavesdroppers need to be prevented from decoding any message intended to legitimate users. Existing security schemes are typically implemented at the higher layers based on the computational hardness via encryption schemes [4].

In contrast to the conventional cryptographic based methods, security has also been addressed using information-theoretic and signal processing approaches at the physical layer. There have been significant research efforts in ensuring secure wireless communications at the physical layer to prevent malicious eavesdroppers from decoding the message [5] [6]. In this regard, the secrecy rate, which can be transmitted both reliably and securely without any use of a formal crypto system, has been adopted as a useful performance metric to measure the system security against passive eavesdropping attacks. Secure connections from a typical multi-antenna transmitter to the multiple legitimate receivers have been studied in [7] over Rayleigh fading channels, where both the legitimate nodes and eavesdroppers' distributions are modelled as Poisson point processes (PPPs). Furthermore, the resource optimization problem for secure connections in multi-user dual-hop relay networks is proposed in [8]. The power minimization problem for a single antenna multicasting secrecy network is studied in [9].

There have been very few works that investigate the secrecy performance of UAV networks. The secrecy energy efficiency in UAV-enabled communication network is analyzed in Rayleigh fading channels where UAVs' distribution is modelled as a PPP [10]. In [11], UAVs are employed as mobile relays to maximize the secrecy rate in a four-node channel setup including a source, a destination, a buffer-aided mobile relay, and an eavesdropper, and it is shown that mobile relays can improve the secrecy performance compared to static relaying. However, existing works in physical layer security for UAV networks have not considered the unique air-to-ground channel characteristics and the 3D antenna gain, and often ignore the safety requirements on the UAV deployment.

This paper aims to analyze the secrecy performance of UAV-enabled millimeter wave (mmWave) networks taking into account the above mentioned factors. In the considered system, UAVs act as flying BSs serving legitimate ground receivers in the presence of ground eavesdroppers, and no terrestrial infrastructure is available. Below we first review the relevant

Manuscript received December 29, 2017; accepted February 1, 2018. This work was supported by the U.K. Engineering and Physical Sciences Research Council (EPSRC) under Grant EP/N007840/1. The editor coordinating the review of this manuscript and approving it for publication was Dr. Y. Wu. (*Corresponding author: Yongxu Zhu*).

Y. Zhu, G. Zheng are with the Department of Electrical and Manufacturing Engineering, Loughborough University, U.K. (Email: {y.zhu4,g.zheng}@lboro.ac.uk).

M. Fitch is with BT Research and Innovation, BT Adastral Park, IP5 3RE, U.K. (Email: michael.fitch@bt.com).

literature.

A. Related Works

1) UAV coverage: Coverage optimization and analysis is an important and universal issue for UAV communications, in applications such as UAV-enabled networks, information dissemination and data collection. Assuming deterministic UAV locations, the coverage radius has been derived as a function of the path loss in [12]. When there is no accurate information about UAVs' locations, it is reasonable to assume UAVs are randomly deployed and to employ stochastic geometry to analyze the coverage performance. In the literature, the UAVs' distribution is normally modelled as a PPP. An analytical expression for the coverage probability is provided in [13] as a function of the UAV parameters in a low-altitude urban environment, and the tradeoff between the UAV's density and height has also been studied. When there is a small number of UAVs deployed to cover a given area, the binomial point process is used to model the UAVs' spatial distribution in [14], where the overage probability for a Nakagami-m fading channel is derived.

2) UAV deployment: UAV deployment is a closely related issue to improve coverage, and presents unique challenges because it needs to jointly consider multiple systems parameters such as elevation angle, directional antennas and flight altitudes of the UAVs [3]. The coverage radius is maximized by optimizing the UAV altitude in the single-UAV deployment in [12], and it is extended to the deployment of two interfering UAVs to maximize the coverage area in [15]. UAV deployment may cause significant interference to ground terminals. It was noted in [16] that reducing the altitude difference between BS antennas and user equipment antennas is necessary to overcome the degradation in the area spectral efficiency in ultra-dense small-cell networks. Energy-efficient UAV-BSs deployment is studied in [17] that maximizes the number of covered users using the minimum transmit power. A novel UAV-satellite communication system has been investigated in [18], where the key challenge of unstable beam pointing is addressed.

3) 3D mmWave antennas: Because of the elevated positions, 3D mmWave antenna model is necessary for modelling UAV air-to-ground communications links, but this has only been studied in terrestrial networks. The impact of 3D BS antenna pattern on the heterogeneous cellular network is studied in [19], and it also discusses the antenna patterns in micro-cell BSs and pico-cell BSs, respectively. The 3D mmwave antenna gain pattern is derived in [20] which could be generalized to handle the 3D locations of the transmitters relative to the receiver and be applied to the UAV-ground mmWave communications.

4) Matérn Hardcore point process: Another unique feature of UAV deployment different from the terrestrial BS deployment is that UAVs need to maintain the minimum safety distance. The widely used PPP model [21] cannot satisfy this requirement. In the literature of spatial stochastic point processes, the Matérn Hardcore (MHC) point process is the most appropriate model to incorporate the UAV minimum separation distance requirement, in which points are forbidden to be closer to each other than a certain minimum distance [21]. Recently analysis of the repulsion between BSs in 2D terrestrial wireless networks has attracted much interest. An energy efficiency approach for the multi-user multi-antenna MHC wireless networks is proposed in [22], whilst the MHC point process is used to model the reject region with each BS in sub-6 GHz cellular networks in [23]. To the best of our knowledge, the MHC point process has not been used in modelling UAVs' spatial distribution.

5) Intentional jamming: Jamming or artificial noise is an effective way to enhance the secrecy rate by emitting radio interference to confuse the eavesdroppers [24, 25]. The transmit jamming can be introduced by either embedding it within the intended signals using multiple antennas at the transmitter [26], or sending it from a full-duplex receiver [27], or by employing external relay jammers [28–31]. However, it is unknown whether transmit jamming can bring any security benefit to UAV networks because not only using part of UAVs to send jamming signals will reduce the number of UAV BSs, but the quality of received signals at both the legitimate receivers and eavesdroppers will be degraded by jamming. Considering the jamming power constraint, a joint relay and jammer selection scheme is proposed in [32] to improve the physical-layer security of a wireless relay system with multiple jamming nodes and one relay node.

B. Contributions and Organization

In this paper, we use stochastic geometry to examine the secrecy performance of randomly deployed UAV-enabled multi-antenna mmWave communication networks in Nakagami-m fading channels considering both line-of-sight (LoS) and non-line-of-sight (NLoS) links, realistic 3D antenna gains, and UAV safety distances. We further propose the transmit jamming approach to improve the achievable secrecy rate. This is in stark contrast to existing work which considers Rayleigh fading [10], single antennas without fading [11], 2D mmWave antenna patterns [33] and no minimum distance between UAVs [34]. In addition, jamming has not been studied in UAV networks. The main contributions of this paper are summarized as follows.

- **Small-scale fading:** The mmWave links are modeled as Nakagami-m fading which is generic enough to incorporate both LoS and NLoS air-to-ground channels. This allows to characterize the dependence of the secrecy rate on key system parameters such as transmission power, densities of UAVs and eavesdroppers, number of antennas and flight altitudes.
- **3D beamforming:** We develop a realistic approach to model the 3D antenna beamforming gain in mmWave links considering the azimuth angle, as well as elevation and depression angles for UAVs and ground terminals respectively, which gives rise to characterize the connection ranges for the air-to-ground links. The results show that decreasing the antenna gain for the ground nodes will reduce the coverage range.
- **UAV minimum distance:** We use an MHC point process to model the UAVs' locations, such that UAVs' minimum

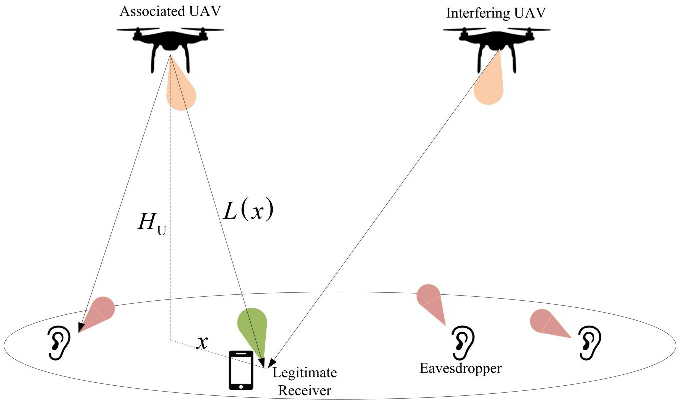


Fig. 1: Illustration of the system model.

safety distance can be guaranteed in the model and secrecy analysis. To the best of our knowledge, this is the first time the MHC point process is used in a 3D propagation model.

- **Transmit jamming:** We propose that part of UAVs can be used to transmit jamming signals to make eavesdropping harder. The results show that optimizing the jamming UAV density can indeed improve the secrecy rate compared to the no transmit jamming case.

The rest of this paper is organised as follows. Section II presents the UAV network model. Section III introduces the MHC point process and user association. The derivations for the secrecy rates with and without transmit jamming are given in Section IV and Section V, respectively. Numerical results and discussions are provided in Section VI, followed by concluding remarks in Section VII.

II. Network Model

We consider a downlink mmWave system in which UAVs serve as aerial BSs to provide wireless connectivity to legitimate ground receivers, in the presence of multiple eavesdroppers on the ground, as shown in Fig. 1. The locations of UAV-enabled BSs are modelled as an MHC point process $\Phi_{\mathtt{U}}$ with density $\lambda_{\mathtt{U}}$, and the eavesdroppers' distribution follows a PPP $\Phi_{\mathtt{E}}$ with density $\lambda_{\mathtt{E}}$, and we also assume that all UAV-enabled BSs are elevated at the same altitude $H_{\mathtt{U}} \gg 0$. For simplicity, the typical receiver is associated with the closest UAV BS. In the following, we will describe in detail the LoS probability, small scale fading, antenna gain and derive the signal-to-interference-plus-noise ratio (SINR) expressions for both the typical receiver and the eavesdroppers.

LoS probability: Due to the blockage effect in the air-to-ground links, we use the point process $\Phi_{\mathtt{U}}^{\mathrm{L}}$ to denote LoS UAV BSs, and $\Phi_{\mathtt{U}}^{\mathrm{N}} = \Phi_{\mathtt{U}}/\Phi_{\mathtt{U}}^{\mathrm{L}}$ to denote NLoS UAV BSs. Define $p_{\mathtt{U},\mathrm{L}}(\varphi)$ as the probability of the LoS link, where φ is the elevation angle from the UAV to the typical receiver. Because UAVs are deployed at the same altitude, we rewrite $p_{\mathtt{U},\mathrm{L}}(\varphi)$ as $p_{\mathtt{U},\mathrm{L}}(x)$, where x is the horizontal distance from the UAV BS to the typical receiver, and denote $p_{\mathtt{U},\mathrm{N}}(x) = 1 - p_{\mathtt{U},\mathrm{L}}(x)$ as the probability of the NLoS link.

Small scale fading: We use independent Nakagami-m fading for the LoS link and the NLoS link respectively. Nakagami-m fading covers a wide range of fading scenarios in realistic wireless applications via the m parameter, which includes the Rayleigh fading ($m = 1$) as a special case. The LoS link and the NLoS link have their own Nakagami fading parameters m_{L} and m_{N}, respectively[1].

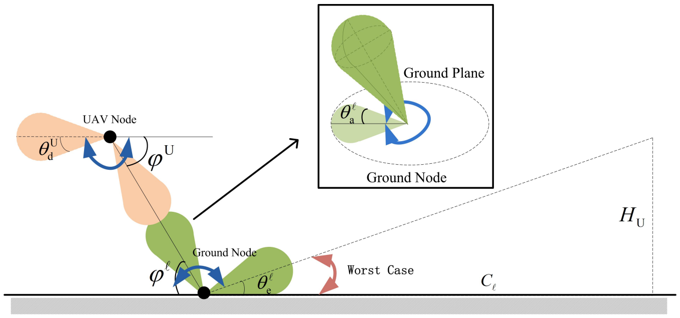


Fig. 2: Illustration of the antenna gain. As the figure shown, C_ℓ is the maximum connection distance range for the ground node (eavesdropper shown), the black double sided arrow denoted the uniform range for depression angle $\varphi^{\mathtt{U}}$ and elevation angle φ^{ℓ} range in $[-\pi, 0]$ and $[\frac{\theta_{\mathrm{e}}^{\ell}}{2}, \pi - \frac{\theta_{\mathrm{e}}^{\ell}}{2}]$ respectively. The sub figure shows the projection of 3D antenna beamforming, and the azimuth angle is uniform in the range of $[-\pi, \pi]$.

3D antenna gain: Suppose each UAV BS is equipped with $N_{\mathtt{U}}$ transmit antennas, and each ground receive terminal has N_{ℓ} receive antennas, where the index $\ell \in \{\mathtt{R}, \mathtt{E}\}$ denotes the typical receiver and the eavesdropper, respectively. Because of the UAVs' altitude, all antennas adopt a 3D sectorized model, and the gain pattern is given by $G(\theta_{\mathrm{a}}, \theta_{\mathrm{e/d}})$, where θ_a is the antenna 3-dB beamwidth for the azimuth orientation in the horizontal direction and $\theta_{\mathrm{e/d}}$ is the antenna 3-dB beamwidth for the elevation/depression angles in the ground/air node, with main-lobe antenna gain G_{M}, and side-lobe gain G_{m}.

The directional antenna gain and the associated probability can be approximated by the formulas below [20] for the UAV and the ground terminal (legitimate receiver or eavesdropper), respectively:

$$G_i^{\mathtt{U}} = \begin{cases} G_{\mathrm{M}}^{\mathtt{U}}, & \mathrm{P}_{\mathrm{M}}^{\mathtt{U}} = \dfrac{\theta_{\mathrm{a}}^{\mathtt{U}}}{2\pi} \cdot \dfrac{\theta_{\mathrm{d}}^{\mathtt{U}}}{\pi} \\ G_{\mathrm{m}}^{\mathtt{U}}, & \mathrm{P}_{\mathrm{m}}^{\mathtt{U}} = 1 - \dfrac{\theta_{\mathrm{a}}^{\mathtt{U}}}{2\pi} \cdot \dfrac{\theta_{\mathrm{d}}^{\mathtt{U}}}{\pi} \end{cases}, \tag{1}$$

and

$$G_j^{\ell} = \begin{cases} G_{\mathrm{M}}^{\ell}, & \mathrm{P}_{\mathrm{M}}^{\ell} = \dfrac{\theta_{\mathrm{a}}^{\ell}}{2\pi} \cdot \dfrac{\theta_{\mathrm{e}}^{\ell}}{\pi - \theta_{\mathrm{e}}^{\ell}} \\ G_{\mathrm{m}}^{\ell}, & \mathrm{P}_{\mathrm{m}}^{\ell} = 1 - \dfrac{\theta_{\mathrm{a}}^{\ell}}{2\pi} \cdot \dfrac{\theta_{\mathrm{e}}^{\ell}}{\pi - \theta_{\mathrm{e}}^{\ell}} \end{cases}. \tag{2}$$

Notice that $G_i^{\mathtt{U}}$ in (1) is the array gain at the UAV BS, where $i = \mathrm{M}$ denoted the main lobe directivity gain and $i = \mathrm{m}$ is the side-lobe gain. The azimuth angle $\psi^{\mathtt{U}}$ is uniform in the range of $[-\pi, \pi]$ and the depression angle $\varphi^{\mathtt{U}}$ for the UAV node is uniform in $[-\pi, 0]$ which is shown in Fig. 2. We have the corresponding probabilities $\mathrm{P}_{\mathrm{M}}^{\mathtt{U}}$ and $\mathrm{P}_{\mathrm{m}}^{\mathtt{U}}$ for the main-lobe and the side-lobe, respectively.

[1] We assume that both m_{L} and m_{N} are positive integers, and $m_{\mathrm{L}} \geq 2$ holds for the dominant LoS transmission in the LoS link.

Similarly, we have the array gain for the typical receiver and the eavesdropper in (2), where $j \in \{\mathrm{M}, \mathrm{m}\}$ denoted the main lobe directivity gain and the side-lobe gain respectively. Different from the UAV node, we have to take into account the worst case situation for the elevation angle at ground terminals as shown in Fig. 2 with red arrows. The azimuth angle of ground terminals is uniform in the range of $\varphi^{\ell} \in [\frac{\theta_{\mathtt{e}}^{\ell}}{2}, \pi - \frac{\theta_{\mathtt{e}}^{\ell}}{2}]$, so we only consider the case when $\varphi^{\ell} \geq \frac{\theta_{\mathtt{e}}^{\ell}}{2}$ or $\varphi^{\ell} \leq \pi - \frac{\theta_{\mathtt{e}}^{\ell}}{2}$ in order to have a reliable connection, which means $\frac{\theta_{\mathtt{e}}^{\ell}}{2}$ is the minimum elevation angle. This leads to the following results about the connection distance.

***Corollary** 1:* We define the maximum connection distances $C_{\mathtt{R}}$ and $C_{\mathtt{E}}$ as the maximum UAV coverage ranges in the horizontal direction for the typical receiver and the eavesdropper, respectively, and both of them are restricted by the elevation angle in the following way:

$$C_{\mathtt{R}} = \frac{H_{\mathtt{U}}}{\tan\left(\theta_{\mathtt{e}}^{\mathtt{R}}/2\right)}, \tag{3}$$

$$C_{\mathtt{E}} = \frac{H_{\mathtt{U}}}{\tan\left(\theta_{\mathtt{e}}^{\mathtt{E}}/2\right)}, \tag{4}$$

where $\varphi^{\mathtt{R}} = \theta_{\mathtt{e}}^{\mathtt{R}}/2$ and $\varphi^{\mathtt{E}} = \theta_{\mathtt{e}}^{\mathtt{E}}/2$ are the minimum elevation angles. Beyond these distances, no reliable connection can be established.

The SINR of the ground receiver: Based on the above assumptions on the UAV deployment, the air-to-ground channel model and the antenna gain, the signal-to-interference-plus-noise ratio (SINR) received from the associated UAV at the typical receiver can be expressed as

$$\mathrm{SINR}_{\mathtt{R}} = \frac{P_{\mathtt{U}} |h_o|^2 G_{\mathrm{M}}^{\mathtt{U}} G_{\mathrm{M}}^{\mathtt{R}} \mathrm{L}\left(|L_{\mathtt{R},o}|\right)}{\mathcal{I}_{\mathtt{R}} + \sigma^2}, \tag{5}$$

where the $P_{\mathtt{U}}$ is transmit power of the UAV BS. The path loss function is defined as $\mathrm{L}\left(|L_{\mathtt{R},o}(x)|\right) = \beta L_{\mathtt{R},o}(x)^{-\alpha_q}$, and $L_{\mathtt{R},o}(x) = \left(x^2 + {H_{\mathtt{U}}}^2\right)^{1/2}$ is the distance from the typical receiver to the associated UAV, x is the corresponding horizontal distance, β is the frequency dependent constant parameter and α_q is path loss exponent, where the sub-index $q = \mathrm{L}$ if it is associated with an LoS link, and $q = \mathrm{N}$ if it is associated with an NLoS link. The interference from both LoS and NLoS links is denoted as $\mathcal{I}_{\mathtt{R}} = \sum\limits_{l \in \Phi_{\mathtt{U}}/o} P_{\mathtt{U}} |h_l|^2 G_i^{\mathtt{U}} G_j^{\mathtt{R}} \mathrm{L}\left(|L_{\mathtt{R},l}|\right)$, and $|h_o|^2$ and $|h_l|^2$ are the normalized Gamma random variables, which correspond to independent Nakagami-m fading gain with the parameter m_q from distances $L_{\mathtt{R},o}(x)$ and $L_{\mathtt{R},l}(x)$, and σ^2 is the noise power.

SINR of the eavesdropper: We assume the worst case eavesdropping scenario, where all the eavesdroppers can cancel the interference from non-associated UAVs [35]. We also assume the legitimate receiver's channel and the eavesdropper's channel are independent of each other. Then the signal-to-noise ratio (SNR) in the worst case is written as

$$\mathrm{SNR}_{\mathtt{E}^*} = \max_{e \in \Phi_{\mathtt{E}}} \left\{ \frac{P_{\mathtt{U}} |h_e|^2 G_i^{\mathtt{U}} G_j^{\mathtt{E}} \mathrm{L}\left(|L_{e,o}|\right)}{\sigma_{\mathtt{E}}^2} \right\}, \tag{6}$$

where $L_{e,o}$ is the distance between the associated UAV BS and the eavesdropper where $e \in \Phi_{\mathtt{E}}$, $\sigma_{\mathtt{E}}^2$ is the noise power. $G_j^{\mathtt{E}}$ is the 3-D antenna gain seen from the eavesdropper.

III. Matérn Hardcore Based UAV Deployment

A unique feature of the UAV deployment is that the minimum safety distance needs to be guaranteed between UAVs and this section is devoted to model the UAVs distribution with this constraint based on the type-II MHC point process [21]. The MHC is a repulsion point process which mathematically represents the minimum distance ρ between all pairs of UAV nodes, where $\rho \ll H_{\mathtt{U}}$.

To model the MHC point process based UAV distribution $\Phi_{\mathtt{U}}$, we first generate the distribution where UAVs are deployed according to a PPP, which is denoted by $\Phi_{\mathtt{P}}$ with density $\lambda_{\mathtt{P}}$. Each point $d \in \Phi_{\mathtt{P}}$ then associates a mark $d \sim U[0, 1]$ independent of any other point, where $U[a, b]$ denotes the uniform distribution in $[a, b]$. At last, compare each two points, retain the point d only when d is the lowest mark compared to all points inside a circle centered at the point d with a radius ρ [23], as illustrated in Fig. 3.

Since the distribution of $\Phi_{\mathtt{U}}$ in the MHC point process is generated by a dependent thinning process of a stationary PPP $\Phi_{\mathtt{P}}$, we have the thinning probability $p_t = \frac{\lambda_{\mathtt{U}}}{\lambda_{\mathtt{P}}}$ where all the points in $\Phi_{\mathtt{P}}$ marked as a circle centred at each point with a radius ρ shown in Fig. 3. So we have the retaining probability p_t for an arbitrary access point d in $\Phi_{\mathtt{U}}$ as

$$p_t = \frac{\mathbb{P}(x < \rho)}{\lambda_{\mathtt{P}} \pi \rho^2} = \frac{1 - \exp(-\lambda_{\mathtt{P}} \pi \rho^2)}{\lambda_{\mathtt{P}} \pi \rho^2}. \tag{7}$$

Based on (7) and $p_t = \frac{\lambda_{\mathtt{U}}}{\lambda_{\mathtt{P}}}$, we can derive the first order product density of the MHC point process $\Phi_{\mathtt{U}}$ below:

$$\zeta^{(1)} = \lambda_{\mathtt{U}} = \frac{1 - \exp(-\lambda_{\mathtt{P}} \pi \rho^2)}{\pi \rho^2}. \tag{8}$$

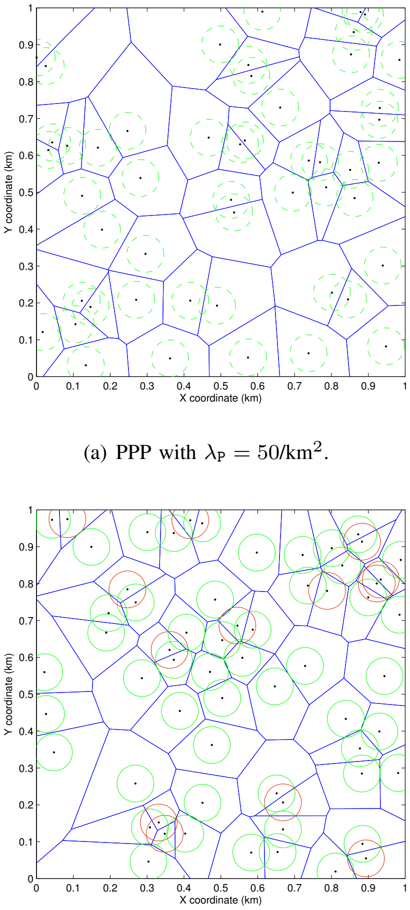
Given the density of the UAV BSs $\lambda_{\mathtt{U}}$, we can figure out the required density of the PPP $\lambda_{\mathtt{P}}$ as:

$$\lambda_{\mathtt{P}} = -\frac{\ln\left(1 - \lambda_{\mathtt{U}} \pi \rho^2\right)}{\pi \rho^2}. \tag{9}$$

From (9), it is clearly seen that $\lambda_{\mathtt{U}}$ is restricted and cannot be arbitrarily high. To be specific, $\lambda_{\mathtt{U}}$ should satisfy $\lambda_{\mathtt{U}} < \dfrac{1}{\pi \rho^2}$ to make the MHC based distribution feasible.

Next we can derive the second order product density of the MHC point process $\Phi_{\mathtt{U}}$ [23] which is given by

$$\zeta^{(2)}(u) = \begin{cases} {\lambda_{\mathtt{U}}}^2 = \left(\dfrac{1 - \exp(-\lambda_{\mathtt{P}} \pi \rho^2)}{\pi \rho^2}\right)^2, 2\rho < u \\ \dfrac{2 V_\rho(u) \left(1 - e^{-\lambda_p \pi \rho^2}\right)}{\pi \rho^2 V_\rho(u) \left[V_\rho(u) - \pi \rho^2\right]} \\ -\dfrac{2\pi\rho^2 \left(1 - e^{-\lambda_{\mathtt{P}} V_\rho(u)}\right)}{\pi \rho^2 V_\rho(u) \left[V_\rho(u) - \pi \rho^2\right]}, \rho < u < 2\rho \\ 0, u < \rho \end{cases}, \tag{10}$$



(a) PPP with $\lambda_{\mathrm{P}} = 50/\mathrm{km}^2$.

(b) MHC point process with $\lambda_{\mathrm{U}} = 50/\mathrm{km}^2$, $\rho = 50\mathrm{m}$.

Fig. 3: A realization of the PPP and the MHC point process with the same density $\lambda_{\mathrm{P}} = \lambda_{\mathrm{U}} = 50/\mathrm{km}^2$. In Fig. 3(a), a dashed line circle around every point to help understand the intensity of each point in the PPP network. In Fig. 3(b), a node d is selected if it has the lowest mark compared to all points inside a circle centered at the point d with a radius ρ. In the figure, the central points of red circles need to be removed. We can see that both processes have the same density, but the MHC point process is more evenly distributed than the PPP.

where $V_\rho(u)$ in (10) denotes the area of the green union which is shown in Fig. 4 when two circles with the same radius ρ are separated by a distance u, which is given by

$$V_\rho(u) = \begin{cases} 2\pi\rho^2, u > 2\rho \\ 2\pi\rho^2 - 2\rho^2\cos^{-1}(\frac{u}{2\rho}) + u\sqrt{\rho^2 - \frac{u^2}{4}}, \rho < u \le 2\rho \\ 0, 0 < u \le \rho \end{cases} \cdot \tag{11}$$

For a stationary point process Φ_{U}, using Campbell's theorem [21, 36], we can deduce that the average number of interfering UAV BSs contained in the UAV distribution Φ_{U}, excluding the associated UAV at the origin 'o', is given by

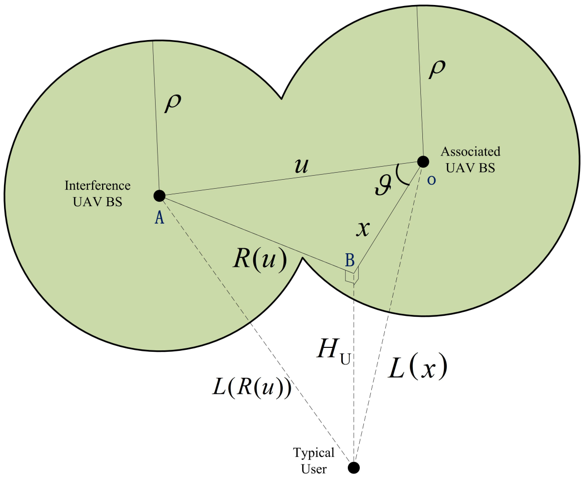


Fig. 4: Illustration of the repulsive point model. x is the horizontal distance between the associated UAV BS 'o' and the typical receiver, and point B is the projection of the typical receiver onto the UAV plane. Point A denotes an interference UAV. ϑ is the angle between $\angle$AoB', where u is the horizontal distance between the associated UAV BS and the interfering UAV BS. $R(u)$ denotes the horizontal distance between the typical receiver and the interfering UAV BS. The green region represents the area of union of two discs of radius ρ.

$$\mathbb{E}^{!o}\left[\sum_{z\in\Phi_{\mathrm{U}}} g(z)\right] = {\lambda_{\mathrm{U}}}^{-1}\int_{\mathbb{R}^2}\zeta^{(2)}(u)\, g(z)\, dz, \tag{12}$$

where $\mathbb{R}^2 \to [0,\infty]$ is a measurable integrable function, and $g(z)$ is the path loss function equation [37].

In addition, given that the distance between the typical receiver and the associated UAV is $L(x) = \sqrt{H_{\mathrm{U}}^2 + x^2}$ [2], the approximated user association probability density function (pdf) is given by [23]:

$$f_{|l_{\mathrm{R},o}|}(L(x)) = 2\pi\lambda_{\mathrm{U}} L(x)\exp(-\lambda_{\mathrm{U}}\pi L(x)^2). \tag{13}$$

Because all UAV-enabled BS are deployed at the same altitude H_{U} and $L(x) = \sqrt{H_{\mathrm{U}}^2 + x^2}$, we can simply transform the approximated user association pdf as follows:

$$f_{|l_{\mathrm{R},o}|}(x) = 2\pi\lambda_{\mathrm{U}} x\exp(-\pi\lambda_{\mathrm{U}} x^2). \tag{14}$$

IV. Secrecy Evaluation

In this section, we analyze the average achievable secrecy rate in the considered UAV-enabled mmWave networks. The average secrecy rate between the associated UAV BS and the typical receiver is defined as

$$R_{Sec} = [\ R_{\mathrm{R}} - R_{\mathrm{E}^*}]^+, \tag{15}$$

where $[x]^+ = \max\{x, 0\}$. The average rates of the typical receiver R_{R} and the most detrimental eavesdropper R_{E^*} are expressed as

$$R_{\mathrm{R}} = \mathbb{E}\left[\log_2(1 + \mathrm{SINR}_{\mathrm{R}})\right] = \frac{1}{\ln 2}\int_0^\infty \frac{\mathcal{P}_{\mathrm{cov,R}}(\gamma)}{1+\gamma} d\gamma, \tag{16}$$

[2] Since $H_{\mathrm{U}} \gg \rho$, we can easly derive that $L(x) \gg \rho$.

and

$$R_{\mathtt{E}^*} = \mathbb{E}\left[\log_2(1+\mathrm{SNR}_{\mathtt{E}^*})\right] = \frac{1}{\ln 2}\int_0^\infty \frac{1-\mathcal{F}_{\mathtt{E}^*}(\gamma)}{1+\gamma}d\gamma, \tag{17}$$

where $\mathcal{P}_{\mathrm{cov},\mathtt{R}}(\gamma)$ is the complementary cumulative distribution function (CCDF) of the average rate from the associated UAV to the typical receiver which is derived in (18) of Theorem 1, and $\mathcal{F}_{\mathtt{E}^*}(\gamma)$ is the cumulative distribution function (CDF) of the average rate of the most detrimental eavesdropper which is derived in Theorem 2, γ is the threshold ($\gamma > 0$).

***Theorem** 1:* The CCDF of $\mathrm{SINR}_\mathtt{R}$ at the typical receiver $\mathcal{P}_{\mathrm{cov},\mathtt{R}}$ is defined as the probability that the received $\mathrm{SINR}_\mathtt{R}$ is greater than the threshold γ, i.e.,

$$\begin{aligned}\mathcal{P}_{\mathrm{cov},\mathtt{R}}(\gamma) = &\int_0^{C_\mathtt{R}} \mathbb{P}^{\mathtt{R}}_{\mathrm{L}}(x,\gamma) f_{|l_{\mathtt{R},o}|}(x) p_{\mathtt{U},\mathrm{L}}(x)dx \\ &+ \int_0^{C_\mathtt{R}} \mathbb{P}^{\mathtt{R}}_{\mathrm{N}}(x,\gamma) f_{|l_{\mathtt{R},o}|}(x) p_{\mathtt{U},\mathrm{N}}(x)dx,\end{aligned} \tag{18}$$

where $\mathbb{P}^{\mathtt{R}}_{\mathrm{L}}(x,\gamma)$ and $\mathbb{P}^{\mathtt{R}}_{\mathrm{N}}(x,\gamma)$ are given in (19) and (20) below

$$\mathbb{P}^{\mathtt{R}}_{\mathrm{L}}(x,\gamma) \approx \sum_{n=1}^{m_\mathrm{L}} (-1)^{n+1} \left(\begin{array}{c} m_\mathrm{L} \\ n \end{array}\right) e^{-s_\mathrm{L}\sigma^2} e^{-\mathcal{A}_{\mathcal{I}_u}(s_\mathrm{L},\lambda_u,P_\mathtt{U})}, \tag{19}$$

$$\mathbb{P}^{\mathtt{R}}_{\mathrm{N}}(x,\gamma) \approx \sum_{n=1}^{m_\mathrm{N}} (-1)^{n+1} \left(\begin{array}{c} m_\mathrm{N} \\ n \end{array}\right) e^{-s_\mathrm{N}\sigma^2} e^{-\mathcal{A}_{\mathcal{I}_u}(s_\mathrm{N},\lambda_u,P_\mathtt{U})}, \tag{20}$$

in which $\mathcal{A}_{\mathcal{I}_u}(s_\mathrm{L},\lambda_u,P_\mathtt{U})$ is given in (23) shown at the top of the next page. $\overline{x}(\vartheta)$ used in (23) is the shortest distance from the interference UAV BS's to the associated UAV BS which is given by

$$\overline{x}(\vartheta) = 2x\left|\cos\vartheta\right|. \tag{21}$$

$\overline{C}_\mathtt{R}(\vartheta)$ in (23) denotes the upper limit integral of u and is given by

$$\overline{C}_\mathtt{R}(\vartheta) = C_\mathtt{R}\sin\left(\pi - \sin^{-1}\left(\tfrac{x\sin\vartheta}{C_\mathtt{R}}\right) - \vartheta\right)/\sin\vartheta, \tag{22}$$

where $C_\mathtt{R}$ is given in Corollary 1.

***Proof** 1:* Please see Appendix A.

With Theorem 1, we can evaluate the average achievable rate from the associated UAV to the typical receiver $R_\mathtt{R}$.

Next, we proceed to derive the CDF between the associated UAV and the most detrimental eavesdropper, which is summarized in the following theorem.

***Theorem** 2:* The CDF of the received SNR from the associated UAV BS at the most detrimental eavesdropper is derived as

$$\begin{aligned}&\mathcal{F}_{\mathtt{E}^*}(\gamma) = \exp\Bigg\{-2\pi\lambda_\mathtt{E} \times \\ &\left.\int_0^{C_\mathtt{E}} \left[\mathrm{T}_\mathrm{L}(\gamma,y)\,p_{\mathtt{U},\mathrm{L}}(y) + \mathrm{T}_\mathrm{N}(\gamma,y)\,p_{\mathtt{U},\mathrm{N}}(y)\right] ydy\right\},\end{aligned} \tag{26}$$

where

$$\mathrm{T}_q(\gamma,y) \approx \prod_{i,j\in\{\mathrm{M},\mathrm{m}\}} \mathrm{P}^{\mathtt{U}}_i \mathrm{P}^{\mathtt{E}}_j \sum_{n=1}^{m_q} (-1)^{n+1} \left(\begin{array}{c} m_q \\ n \end{array}\right) e^{-\frac{n\eta_q\gamma L(y)^{\alpha_q}\sigma^2}{P_\mathtt{U} G^\mathtt{U}_i G^\mathtt{E}_j \beta}}. \tag{27}$$

***Proof** 2:* The horizontal distance y denoted the distance between the associated UAV to the most detrimental eavesdropper. The rest proof is provided in Appendix B.

Substituting (18) and (26) into (16) and (17) respectively, we can obtain the desired average secrecy rate (15).

V. Transmit Jamming-aided UAV networks

Transmit jamming is an effective measure to degrade the quality of eavesdroppers' received signals. However, it is an unproven idea to enhance the UAV communication security. In this section, we propose the concept of UAV transmit jamming and analyze its performance. To be specific, part of the UAVs in $\Phi^\mathrm{J}_\mathtt{U} \subseteq \Phi_\mathtt{U}$ with density $\varepsilon\lambda_\mathtt{U}$ will only transmit jamming signals to confound eavesdroppers, and the rest UAVs in $\Phi^\mathrm{S}_\mathtt{U} \subseteq \Phi_\mathtt{U}$ with density $(1-\varepsilon)\lambda_\mathtt{U}$ are used to support information transmission. $0 \le \varepsilon \le 1$ is the jamming factor.

With transmit jamming, the SINR at the typical receiver becomes

$$\mathrm{SINR}^{(\mathrm{J})}_\mathtt{R} = \frac{P_\mathtt{U}|h_o|^2 G^\mathtt{U}_\mathrm{M} G^\mathtt{R}_\mathrm{M} \mathrm{L}\left(|L_{\mathtt{R},o}|\right)}{\mathcal{I}^{(S)}_\mathtt{R} + \mathcal{I}^{(J)}_\mathtt{R} + \sigma^2}, \tag{28}$$

where $\mathcal{I}^{(S)}_\mathtt{R} = \sum\limits_{l\in\Phi^S_\mathtt{U}\backslash o} P_\mathtt{U}|h_l|^2 G^\mathtt{U}_i G^\mathtt{R}_j \mathrm{L}\left(|L_{\mathtt{R},l}|\right)$ is the interference from those UAVs in $\Phi^S_\mathtt{U}$ which transmit signal to other ground receivers excluding the associated UAV BS at 'o', and $\mathcal{I}^{(J)}_\mathtt{R} = \sum\limits_{k\in\Phi^J_\mathtt{U}} P_\mathtt{U}|h_k|^2 G^\mathtt{U}_{i'} G^\mathtt{R}_j \mathrm{L}\left(|L_{\mathtt{R},k}|\right)$ is the jamming signals sent from jamming UAVs in $\Phi^J_\mathtt{U}$. $G_{i'}$ denote the antenna gains from the jamming UAVs. Notice that in transmit jamming-aided UAV networks, the density of UAVs that a typical receiver can be associated to is reduced to $(1-\varepsilon)\lambda_\mathtt{U}$, so the approximated MHC distribution is derived as follows:

$$f^{(J)}_{|l_{\mathtt{R},o}|}(x) = 2\pi(1-\varepsilon)\lambda_\mathtt{U} x\exp(-\pi(1-\varepsilon)\lambda_\mathtt{U} x^2). \tag{29}$$

The SINR at the most detrimental eavesdropper is given by

$$\mathrm{SINR}^{(J)}_{\mathtt{E}^*} = \max_{e\in\Phi_\mathtt{E}}\left\{\frac{P_\mathtt{U}|h_e|^2 G^\mathtt{U}_i G^\mathtt{E}_j \mathrm{L}\left(|L_{o,e}|\right)}{\mathcal{I}^{(J)}_\mathtt{E} + \sigma^2_\mathtt{E}}\right\}, \tag{30}$$

where $\mathcal{I}^{(J)}_\mathtt{E} = \sum\limits_{k\in\Phi^J_\mathtt{U}} \eta P_\mathtt{U}|h_k|^2 G^\mathtt{U}_{i'} G^\mathtt{E}_j \mathrm{L}\left(|L_{e,k}|\right)$ is the jamming signal from the jamming UAVs.

According to (15), the average achievable secrecy rate for the jamming-aided UAV transmission now becomes

$$R^{(\mathrm{J})}_{Sec} = \left[\, R^{(J)}_\mathtt{R} - R^{(J)}_{\mathtt{E}^*} \right]^+, \tag{31}$$

where the expressions of $R^{(J)}_\mathtt{R}$ and can be found in (16) and (17), by replacing $\mathcal{P}_{\mathrm{cov},\mathtt{R}}(\gamma)$ by $\mathcal{P}^{(J)}_{\mathrm{cov},\mathtt{R}}(\gamma)$ and $\mathcal{F}_{\mathtt{E}^*}(\gamma)$ by $\mathcal{F}^{(J)}_{\mathtt{E}^*}(\gamma)$, where $\mathcal{P}^{(J)}_{\mathrm{cov},\mathtt{R}}(\gamma)$ is the CCDF of (32) in Theorem 3, and $\mathcal{F}^{(J)}_{\mathtt{E}^*}(\gamma)$ is the CDF from (36) in Theorem 4 below, respectively.

***Theorem** 3:* The CCDF of $\mathrm{SINR}^{(\mathrm{J})}_\mathtt{R}$ in jamming-aided networks can be obtained as

$$\begin{aligned}\mathcal{P}^{(J)}_{\mathrm{cov},\mathtt{R}}(\gamma) = &\int_0^{C_\mathtt{E}} \mathbb{P}^{\mathrm{U},(J)}_{\mathrm{L}}(x,\gamma) f^{(J)}_{|l_{\mathtt{R},o}|}(x) p_{\mathtt{U},\mathrm{L}}(x)dx \\ &+ \int_0^{C_\mathtt{E}} \mathbb{P}^{\mathrm{U},(J)}_{\mathrm{N}}(x,\gamma) f^{(J)}_{|l_{\mathtt{R},o}|}(x) p_{\mathtt{U},\mathrm{N}}(x)dx,\end{aligned} \tag{32}$$

$$
\begin{aligned}
&\mathcal{A}^{q}_{\mathcal{I}_u}\left(\lambda_u, P_{\mathtt{U}}\right) \approx \sum_{i,j\in\{\mathrm{M,m}\}} \mathrm{P}^{\mathtt{U}}_i \mathrm{P}^{\mathtt{R}}_j \\
&\Bigg\{ {\lambda_u}^{-1} \int_0^{2\pi} \int_{\max[\rho,\bar{x}(\vartheta)]}^{\min\left[\max[2\rho,\bar{x}(\vartheta)],\bar{C}_{\mathtt{R}}(\vartheta)\right]} \left[\Omega^{q}_{\mathrm{L}}\left(u,\vartheta,G^{\mathtt{U}}_i G^{\mathtt{R}}_j\right) p_{\mathtt{U},\mathrm{L}}(u) + \Omega^{q}_{\mathrm{N}}\left(u,\vartheta,G^{\mathtt{U}}_i G^{\mathtt{R}}_j\right) p_{\mathtt{U},\mathrm{N}}(u)\right] u\zeta^{(2)}\left(u\right) du d\vartheta \qquad (23) \\
&+ \lambda_u \int_0^{2\pi} \int_{\max[2\rho,\bar{x}(\vartheta)]}^{\bar{C}_{\mathtt{R}}(\vartheta)} \left[\Omega^{q}_{\mathrm{L}}\left(u,\vartheta,G^{\mathtt{U}}_i G^{\mathtt{R}}_j\right) p_{\mathtt{U},\mathrm{L}}(u) + \Omega^{q}_{\mathrm{N}}\left(u,\vartheta,G^{\mathtt{U}}_i G^{\mathtt{R}}_j\right) p_{\mathtt{U},\mathrm{N}}(u)\right] u du d\vartheta \Bigg\},
\end{aligned}
$$

where

$$
\Omega^{q}_{\mathrm{L}}\left(u,\vartheta,G^{\mathtt{U}}_i G^{\mathtt{R}}_j\right) = 1 - \left(1 + \frac{n\eta_q\gamma\left(x^2+H^2_{\mathtt{U}}\right)^{\alpha_q/2} G^{\mathtt{U}}_i G^{\mathtt{R}}_j}{\left(x^2+u^2-2xu\cos\vartheta+H^2_{\mathtt{U}}\right)^{\alpha_{\mathrm{L}}/2} G^{\mathtt{U}}_{\mathrm{M}} G^{\mathtt{R}}_{\mathrm{M}} m_{\mathrm{L}}}\right)^{-m_{\mathrm{L}}}, \qquad (24)
$$

$$
\Omega^{q}_{\mathrm{L}}\left(u,\vartheta,G^{\mathtt{U}}_i G^{\mathtt{R}}_j\right) = 1 - \left(1 + \frac{n\eta_q\gamma\left(x^2+H^2_{\mathtt{U}}\right)^{\alpha_q/2} G^{\mathtt{U}}_i G^{\mathtt{R}}_j}{\left(x^2+u^2-2xu\cos\vartheta+H^2_{\mathtt{U}}\right)^{\alpha_{\mathrm{N}}/2} G^{\mathtt{U}}_{\mathrm{M}} G^{\mathtt{R}}_{\mathrm{M}} m_{\mathrm{N}}}\right)^{-m_{\mathrm{N}}}. \qquad (25)
$$

TABLE I: 3D UPA Antenna Pattern [20].

Number of antenna elements	$N_\ell = 4, 16$
Half-power Beamwidth ($\theta_{\mathrm{a}} = \theta_{\mathrm{e}} = \theta_{\mathrm{d}}$)	$\frac{\sqrt{3}}{\sqrt{N_\ell}}$
Main-lobe gain (G_{M})	N_ℓ
Side-lobe gain (G_{m})	$\frac{\sqrt{N_\ell} - \frac{\sqrt{3}}{2\pi} N_\ell \sin(3\pi/2\sqrt{N_\ell})}{\sqrt{N_\ell} - \frac{\sqrt{3}}{2\pi} \sin(3\pi/2\sqrt{N_\ell})}$

where $\mathbb{P}^{\mathrm{U},(J)}_{\mathrm{L}}(x,\gamma)$ and $\mathbb{P}^{\mathrm{U},(J)}_{\mathrm{N}}(x,\gamma)$ are given in (33) and (34), respectively, at the top of the next page.

Proof 3: It can be proved by following a similar approach in Theorem 1.

Theorem 4: The CDF of $\mathrm{SINR}^{(\mathrm{J})}_{\mathtt{E}^*}$ in jamming-aided UAV networks can be obtained as

$$
\begin{aligned}
&\mathcal{F}^{(\mathrm{J})}_{\mathtt{E}^*}(\gamma) = \exp\Big\{-2\pi\lambda_{\mathtt{E}} \\
&\int_0^{C_{\mathtt{E}}} \left[\mathrm{W}_{\mathrm{L}}\left(\gamma,y\right) p_{\mathtt{U},\mathrm{L}}(y) + \mathrm{W}_{\mathrm{N}}\left(\gamma,y\right) p_{\mathtt{U},\mathrm{N}}(y)\right] y dy\Big\}, \qquad (36)
\end{aligned}
$$

where $C_{\mathtt{E}}$ in (36) is given by (4), $\overline{C}_{\mathtt{E}}(\vartheta_{\mathtt{E}})$ in (38) denotes the upper limit of the integral of u, and is expressed as

$$
\overline{C}_{\mathtt{E}}(\vartheta_{\mathtt{E}}) = C_{\mathtt{E}} \sin\left(\pi - \sin^{-1}\left(\tfrac{y\sin\vartheta_{\mathtt{E}}}{C_{\mathtt{E}}}\right) - \vartheta_{\mathtt{E}}\right) / \sin\vartheta_{\mathtt{E}}, \qquad (37)
$$

where $C_{\mathtt{E}}$ is given in Corollary 1 and $\mathrm{W}_q(\gamma,y)$ is given in (38) at the top of this page.

Proof 4: Please see Appendix C.

VI. Numerical Results and Discussions

In this section, we provide numerical results for the average achievable secrecy rate in the UAV-enabled mmWave networks. We assume that the uniform planar array (UPA) is used and modeled as a sectorized pattern, and the associated parameters are shown in Table I. Notice that the 3-dB beamwidth and the number of antennas have an inverse relationship. We assume that the LoS connection probability is given by [12]

$$
p_{\mathtt{U},\mathrm{L}}(x) = \frac{1}{1 + a\exp\left(-b\left[\arctan\left(\frac{H_{\mathtt{U}}}{x}\right) - a\right]\right)}, \qquad (41)
$$

TABLE II: Parameter Values.

Parameters	Values
Number of Antenna (N_ℓ)	4,16
Safety distance (ρ)	10 m
Nakagami parameter for LoS link (m_{L})	3
Nakagami parameter for NLoS link (m_{N})	2
Altitude of UAV ($H_{\mathtt{U}}$)	200m
Constant values in the Urban Environment (a, b)	9.6, 0.28
Transmit power of UAV nodes $P_{\mathtt{U}}$	20 dBm
Path loss exponents at f_c=28 GHz [38]	α_{L}=2,α_{N}=3
Available bandwidth (BW)	1 GHz
Noise figure Nf	10 dB
Noise power ($\sigma_o^2 = \sigma_{\mathtt{E}}^2$)	$-170 + 10\log_{10}(\mathrm{BW})$ +Nf dBm

where $\varphi^{\ell} = \arctan\left(\frac{H_{\mathtt{U}}}{x}\right)$ is elevation angle, and a and b are constant values which depend on the environment (rural, urban, dense urban, etc.). Other system parameters are given in Table II, unless otherwise specified.

Fig. 5 shows the effects of the UAV transmit power on the average achievable rates. The analytical curves are obtained from (16) and (17) respectively, which are validated by the Monte Carlo simulation marked by '+'. The numbers of $N_{\mathtt{R}}$ and $N_{\mathtt{E}}$ are shown in the figure. Note that although the individual receivers and eavesdroppers' rates increase with the UAV transmit power, we observe that there exists an optimal transmit power value for maximizing the average achievable secrecy rate when the typical receiver is equipped with $N_{\mathtt{R}} = 16$ antennas.

Fig. 6 shows the effects of the UAV transmit power on the average secrecy rate. We observe that when the antenna number of eavesdroppers $N_{\mathtt{E}}$ is reduced from 16 to 4, or the antenna number of the legitimate ground receiver $N_{\mathtt{R}}$ increases from 4 to 16, the secrecy rate improves dramatically. This is because the 3-dB beamwidths in the azimuth and elevation directions are inversely proportional to $\sqrt{N_{\mathtt{R}}}$ and $\sqrt{N_{\mathtt{E}}}$ [3], therefore less antennas will result in smaller coverage range for receivers.

[3] Note that we have assumed the UPA for each mmWave node.

$$\mathbb{P}_{\mathrm{L}}^{\mathrm{U},(J)}(x,\gamma) \approx \sum_{n=1}^{m_{\mathrm{L}}} (-1)^{n+1} \left(\begin{array}{c} m_{\mathrm{L}} \\ n \end{array} \right) e^{-s_{\mathrm{L}}\sigma^2} e^{-\mathcal{A}_{\mathcal{I}_{\mathtt{U}}}^{\mathrm{L}}((1-\varepsilon)\lambda_{\mathtt{U}},P_{\mathtt{U}})} e^{-\mathcal{B}_{\mathcal{I}_{\mathtt{U}}}^{\mathrm{L}}(\varepsilon\lambda_{\mathtt{U}},P_{\mathtt{U}})}, \tag{33}$$

$$\mathbb{P}_{\mathrm{N}}^{\mathrm{U},(J)}(x,\gamma) \approx \sum_{n=1}^{m_{\mathrm{N}}} (-1)^{n+1} \left(\begin{array}{c} m_{\mathrm{N}} \\ n \end{array} \right) e^{-s_{\mathrm{N}}\sigma^2} e^{-\mathcal{A}_{\mathcal{I}_{\mathtt{U}}}^{\mathrm{N}}((1-\varepsilon)\lambda_{\mathtt{U}},P_{\mathtt{U}})} e^{-\mathcal{B}_{\mathcal{I}_{\mathtt{U}}}^{\mathrm{N}}(\varepsilon\lambda_{\mathtt{U}},P_{\mathtt{U}})}, \tag{34}$$

$$\begin{aligned} &\mathcal{B}_{\mathcal{I}_u}^{q}\left(\varepsilon\lambda_u, P_{\mathtt{U}}\right) \approx \sum_{i,j\in\{\mathrm{M,m}\}} \mathrm{P}_{i'}^{\mathtt{U}}\mathrm{P}_{j}^{\mathtt{R}} \times \\ &\Bigg\{ \left[\varepsilon\lambda_{\mathtt{U}}\right]^{-1} \int_0^{2\pi} \int_{\rho}^{\min\left[2\rho,\bar{C}_{\mathtt{R}}(\vartheta)\right]} \left[\Omega_{\mathrm{L}}^{q}\left(u,P_{\mathtt{U}},G_{i'}^{\mathtt{U}}G_{j}^{\mathtt{R}}\right)p_{\mathtt{U},\mathrm{L}}(u) + \Omega_{\mathrm{N}}^{q}\left(u,P_{\mathtt{U}},G_{i'}^{\mathtt{U}}G_{j}^{\mathtt{R}}\right)p_{\mathtt{U},\mathrm{N}}(u)\right] u\zeta^{(2)}(u)\,dud\vartheta \\ &+ \varepsilon\lambda_{\mathtt{U}} \int_0^{2\pi} \int_{2\rho}^{\bar{C}_{\mathtt{R}}(\vartheta)} \left[\Omega_{\mathrm{L}}^{q}\left(u,P_{\mathtt{U}},G_{i'}^{\mathtt{U}}G_{j}^{\mathtt{R}}\right)p_{\mathtt{U},\mathrm{L}}(u) + \Omega_{\mathrm{N}}^{q}\left(u,P_{\mathtt{U}},G_{i'}^{\mathtt{U}}G_{j}^{\mathtt{R}}\right)p_{\mathtt{U},\mathrm{N}}(u)\right] ududv\vartheta \Bigg\}. \end{aligned} \tag{35}$$

$$\begin{aligned} &\mathrm{W}_q\left(\gamma,y\right) \approx \sum_{n=1}^{m_q} (-1)^{n+1} \left(\begin{array}{c} m_q \\ n \end{array} \right) \prod\nolimits_{i,i',j\in\{\mathrm{M,m}\}} \mathrm{P}_{i}^{\mathtt{U}}\mathrm{P}_{i'}^{\mathtt{U}}\mathrm{P}_{j}^{\mathtt{R}} \exp\Bigg\{ -\frac{n\eta_q\gamma L(y)^{\alpha_q}}{P_{\mathtt{U}}G_i^{\mathtt{U}}G_j^{\mathtt{R}}\beta}\sigma^2 - \left[\varepsilon\lambda_{\mathtt{U}}\right]^{-1} \\ &\times \int_0^{2\pi} \int_{\rho}^{\min\left[2\rho,\bar{C}_{\mathtt{E}}(\vartheta_{\mathtt{E}})\right]} \left(\Omega_{\mathrm{L}}^{q,(\mathrm{J})}\left(u,\vartheta_{\mathtt{E}},G_i^{\mathtt{U}},G_{i'}^{\mathtt{U}}\right)p_{\mathtt{U},\mathrm{L}}(u) + \Omega_{\mathrm{N}}^{q,(\mathrm{J})}\left(u,\vartheta_{\mathtt{E}},G_i^{\mathtt{U}},G_{i'}^{\mathtt{U}}\right)p_{\mathtt{U},\mathrm{N}}(u)\right) u\zeta^{(2)}(u)\,dud\vartheta_{\mathtt{E}} \\ &- \varepsilon\lambda_{\mathtt{U}} \int_0^{2\pi} \int_{2\rho}^{\bar{C}_{\mathtt{E}}(\vartheta_{\mathtt{E}})} \left(\Omega_{\mathrm{L}}^{q,(\mathrm{J})}\left(u,\vartheta_{\mathtt{E}},G_i^{\mathtt{U}},G_{i'}^{\mathtt{U}}\right)p_{\mathtt{U},\mathrm{L}}(u) + \Omega_{\mathrm{N}}^{q,(\mathrm{J})}\left(u,\vartheta_{\mathtt{E}},G_i^{\mathtt{U}},G_{i'}^{\mathtt{U}}\right)p_{\mathtt{U},\mathrm{N}}(u)\right) ududv\vartheta_{\mathtt{E}} \Bigg\} \end{aligned} \tag{38}$$

where

$$\Omega_{\mathrm{L}}^{q,(\mathrm{J})}\left(u,\vartheta_{\mathtt{E}},G_i^{\mathtt{U}},G_{i'}^{\mathtt{U}}\right) = 1 - \left(1 + \frac{n\eta_q\gamma\left(y^2+H_{\mathtt{U}}^2\right)^{\alpha_q/2}G_{i'}^{\mathtt{U}}}{\left(y^2+u^2-2yu\cos\vartheta_{\mathtt{E}}+H_{\mathtt{U}}^2\right)^{\alpha_{\mathrm{L}}/2}G_i^{\mathtt{U}}m_{\mathrm{L}}}\right)^{-m_{\mathrm{L}}}, \tag{39}$$

$$\Omega_{\mathrm{N}}^{q,(\mathrm{J})}\left(u,\vartheta_{\mathtt{E}},G_i^{\mathtt{U}},G_{i'}^{\mathtt{U}}\right) = 1 - \left(1 + \frac{n\eta_q\gamma\left(y^2+H_{\mathtt{U}}^2\right)^{\alpha_q/2}G_{i'}^{\mathtt{U}}}{\left(y^2+u^2-2yu\cos\vartheta_{\mathtt{E}}+H_{\mathtt{U}}^2\right)^{\alpha_{\mathrm{L}}/2}G_i^{\mathtt{U}}m_{\mathrm{N}}}\right)^{-m_{\mathrm{N}}}. \tag{40}$$

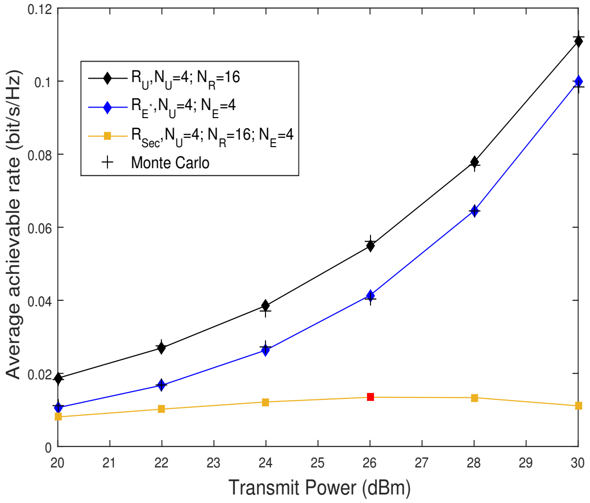


Fig. 5: The effects of the UAV transmit power on the average rates, with $\lambda_{\mathtt{U}} = 100/\mathrm{km}^2$, $\lambda_{\mathtt{E}} = 300/\mathrm{km}^2$, $H_{\mathtt{U}} = 300\mathrm{m}$,$\rho = 10\mathrm{m}$.

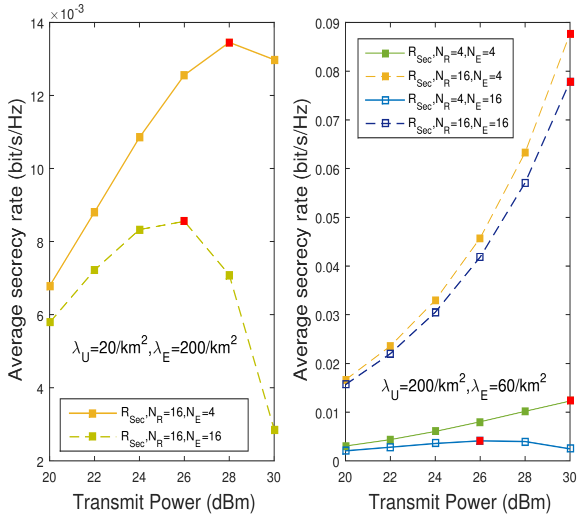


Fig. 6: The effects of the UAV transmit power on the average secrecy rates, $H_{\mathtt{U}} = 200\mathrm{m}$, and $\rho = 10\mathrm{m}$.

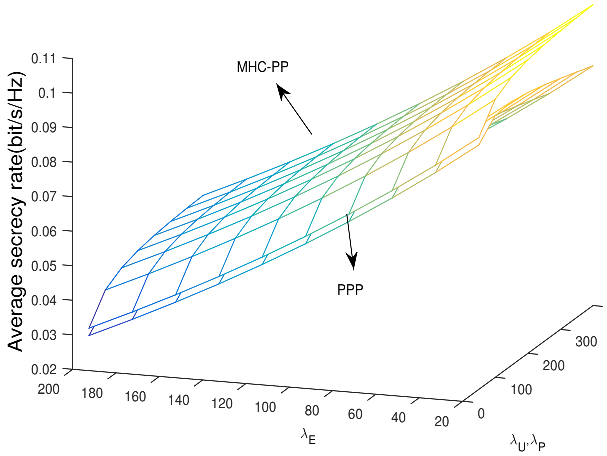


Fig. 7: The effects of the UAV density on the average secrecy rates, with $P_{\mathrm{U}} = 30$ dBm and $N_{\mathrm{R}} = 16$, $N_{\mathrm{E}} = 16$, $\rho = 10$ m.

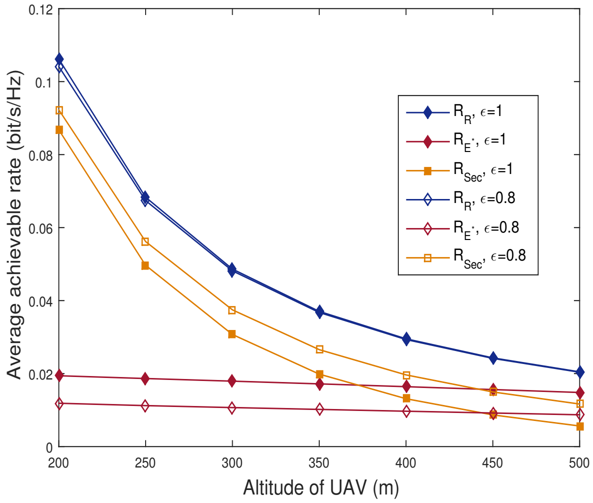


Fig. 8: The effects of the UAV altitude on the average rates, with $P_{\mathrm{U}} = 30$ dBm, $\lambda_{\mathrm{U}} = 100/\mathrm{km}^2$, $\lambda_{\mathrm{E}} = 40/\mathrm{km}^2$, and $N_{\mathrm{R}} = 16$.

Fig. 7 shows the effects of the UAV densities on the average secrecy rate. It can be observed that there exists an optimal density of UAVs to maximize the average secrecy rate in the PPP model, and when λ_{P} is higher than $150/\mathrm{km}^2$, the average secrecy rate starts to decrease. That is because as the density of UAVs increase, the MHC point process is more evenly distributed than the PPP. The minimum distance helps limit the effect of interference, which could avoid some concentrated interference around serving UAV-enabled BS, so the average secrecy rate can keep increasing. However, in the PPP model, as the density of UAVs increases, it will help the typical user connect to the nearest UAV-enabled BS first but then the performance will be limited by the interference.

Fig. 8 shows the effects of the UAV altitudes on the average rates. It's seen that high altitudes will dramatically reduce the achievable rate of the typical user but only slightly degrade the most aggressive eavesdropper's rate. That is because as the altitude of the UAV BS increases, the received signal at the typical receiver will be much weaker but the signal received at the eavesdropper is not affected much because their antenna gains are low in mmWave links.

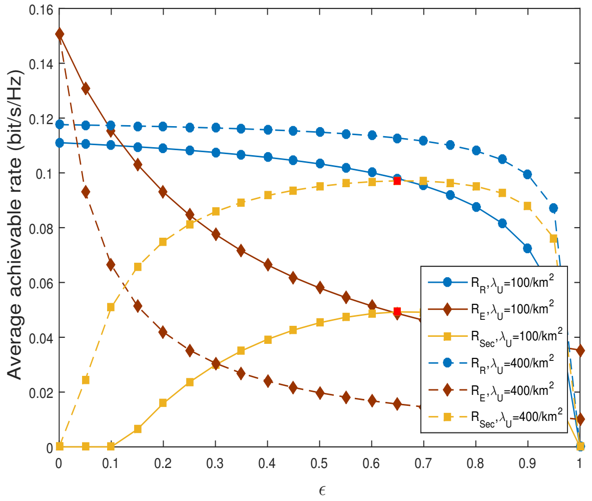


Fig. 9: The effects of the UAV jamming factor on the average rate, with $P_{\mathrm{U}} = 30$ dBm, $N_{\mathrm{U}} = 4$, $N_{\mathrm{R}} = 16$, $N_{\mathrm{E}} = 4$ and $\lambda_{\mathrm{E}} = 600/\mathrm{km}^2$.

Fig. 9 shows the impact of the jamming factor ε (i.e., the percentage of UAVs that transmit jamming signals) on the average achievable rates when the eavesdroppers' density is $\lambda_{\mathrm{E}} = 600/\mathrm{km}^2$. It is easy to see that as the density of jamming UAVs increases, both the typical receiver and the eavesdropper's rates will be reduced due to the increased interference. However, the secrecy rate is not changing monotonically, but there is an optimal ε to maximize the average achievable secrecy rate which is marked with red squares. In the simulated system, using 70% UAVs to transmit jamming signals leads to near optimal secrecy rate. That can be explained by the fact using appropriate amount of UAVs to send the jamming signals will reduce the eavesdropper's rate more than the typical receiver's rate.

Fig. 10 shows the impact of the minimum distance of ρ on the average secrecy rate without jamming signals. We assume each curve has the same initial PPP density λ_{P}. It is observed that as the minimum distance ρ increases, the MHC point process tend to be thinner and less UAVs will be deployed, therefore the secrecy rate will decrease as well.

VII. Conclusion

This paper analyzed the secrecy performance of 3D UAV-enabled mmWave networks taking into account practical propagation characteristics and system deployment constraints. A tractable approach was developed to evaluate the 3D antenna gain of the air-to-ground links. The MHC point process has been employed to guarantee the safety distance between the randomly deployed UAV BSs. Furthermore, we proposed

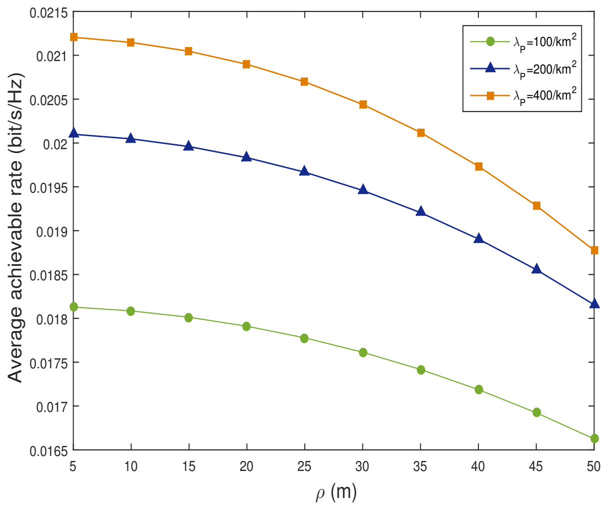


Fig. 10: The effects of the UAV safety distance on the average secrecy rates, with $P_{\mathtt{U}} = 25$ dBm, $N_{\mathtt{U}} = 4$, $N_{\mathtt{R}} = 16$, $N_{\mathtt{E}} = 4$, $\lambda_{\mathtt{E}} = 200/\text{km}^2$ and $\varepsilon = 0$.

to use part of UAVs to transmit jamming signals to the eavesdroppers and characterized the improved secrecy performance. Simulation results demonstrate the impact of system parameters on the secrecy rate. Our analysis also shows that optimizing the jamming factor of the UAV network will indeed improve the secrecy rate. This paper focuses on the fixed ground user scenario. As an important future direction, UAV trajectory optimization to track mobility users [39] is worth further study.

Appendix A: Proof of Theorem 1

Based on the fact that the typical receiver is associated with different types (LoS or NLoS) of UAV-enabled BSs $\Phi_{\mathtt{U}}^{\mathrm{L}}$ or $\Phi_{\mathtt{U}}^{\mathrm{N}}$ with probability $p_{\mathtt{U},\mathrm{L}}$ or $p_{\mathtt{U},\mathrm{N}}$, the conditional coverage probability can be derived as

$$\begin{aligned}
&\mathcal{P}_{\mathrm{cov},\mathtt{R}}(\gamma) = \int_0^{C_{\mathtt{R}}} \mathbb{P}\left[\mathrm{SINR}_{\mathtt{R}} > \gamma\right] f_{|l_{\mathtt{R},o}|}(x)dx \\
&= \int_0^{C_{\mathtt{R}}} \underbrace{\mathbb{P}\left[\frac{P_t G_{\mathrm{M}}^{\mathtt{U}} G_{\mathrm{M}}^{\mathtt{R}} |h_o|^2 \beta L(x)^{-\alpha_{\mathrm{L}}}}{\mathcal{I}_{\mathtt{R}}^{\mathrm{L}} + \mathcal{I}_{\mathtt{R}}^{\mathrm{N}} + \sigma^2} > \gamma\right]}_{\mathbb{P}_{\mathrm{L}}^{\mathtt{R}}(x,\gamma)} f_{|l_{\mathtt{R},o}|}(x) p_{\mathtt{U},\mathrm{L}}(x)dx \\
&+ \int_0^{C_{\mathtt{R}}} \underbrace{\mathbb{P}\left[\frac{P_t G_{\mathrm{M}}^{\mathtt{U}} G_{\mathrm{M}}^{\mathtt{R}} |h_o|^2 \beta L(x)^{-\alpha_{\mathrm{N}}}}{\mathcal{I}_{\mathtt{R}}^{\mathrm{L}} + \mathcal{I}_{\mathtt{R}}^{\mathrm{N}} + \sigma^2} > \gamma\right]}_{\mathbb{P}_{\mathrm{N}}^{\mathtt{R}}(x,\gamma)} f_{|l_{\mathtt{R},o}|}(x) p_{\mathtt{U},\mathrm{N}}(x)dx,
\end{aligned} \tag{A.1}$$

where $L(x) = \sqrt{x^2 + {H_{\mathtt{U}}}^2}$ is the distance from the associated UAV-enabled BS to the typical receiver, and x is the corresponding horizontal distance. Note that $|h_o|^2$ is a normalized gamma random variable with the parameter m_q. $f_{|\mathtt{R},o|}(x)$ is given by (14). Then, we have the following approximation of the coverage probability with given distance x for the LoS link:

$$\begin{aligned}
&\mathbb{P}_{\mathrm{L}}^{\mathtt{R}}(x,\gamma) = \mathbb{P}\left[h_o > \frac{\gamma L(x)^{\alpha_{\mathrm{L}}}}{P_{\mathtt{U}} G_{\mathrm{M}}^{\mathtt{U}} G_{\mathrm{M}}^{\mathtt{R}} \beta}\left(\mathcal{I}_{\mathtt{R}}^{\mathrm{L}} + \mathcal{I}_{\mathtt{R}}^{\mathrm{N}} + \sigma^2\right)\right] \\
&\overset{(a)}{\approx} 1 - \mathbb{E}_{\Phi_{\mathtt{U}}}\left[\left(1 - e^{-\frac{\eta_{\mathrm{L}} \gamma L(x)^{\alpha_{\mathrm{L}}}}{P_{\mathtt{U}} G_{\mathrm{M}}^{\mathtt{U}} G_{\mathrm{M}}^{\mathtt{R}} \beta}\left(\mathcal{I}_{\mathtt{R}}^{\mathrm{L}} + \mathcal{I}_{\mathtt{R}}^{\mathrm{N}} + \sigma^2\right)}\right)^{m_{\mathrm{L}}}\right] \\
&= \sum_{n=1}^{m_{\mathrm{L}}} (-1)^{n+1} \begin{pmatrix} m_{\mathrm{L}} \\ n \end{pmatrix} \mathbb{E}\left[e^{-\frac{n \eta_{\mathrm{L}} \gamma L(x)^{\alpha_{\mathrm{L}}}}{P_{\mathtt{U}} G_{\mathrm{M}}^{\mathtt{U}} G_{\mathrm{M}}^{\mathtt{R}} \beta}\left(\mathcal{I}_{\mathtt{R}}^{\mathrm{L}} + \mathcal{I}_{\mathtt{R}}^{\mathrm{N}} + \sigma^2\right)}\right] \\
&= \sum_{n=1}^{m_{\mathrm{L}}} (-1)^{n+1} \begin{pmatrix} m_{\mathrm{L}} \\ n \end{pmatrix} e^{-s_{\mathrm{L}} \sigma^2} \mathcal{L}_{\mathcal{I}_{\mathtt{R}}^{\mathrm{L}}}\left(s_{\mathrm{L}}\right) \mathcal{L}_{\mathcal{I}_{\mathtt{R}}^{\mathrm{N}}}\left(s_{\mathrm{L}}\right),
\end{aligned} \tag{A.2}$$

and the coverage rate for the NLoS link can be computed as

$$\begin{aligned}
&\mathbb{P}_{\mathrm{N}}^{\mathtt{R}}(x,\gamma) = \mathbb{P}\left[h_o > \frac{\gamma L(x)^{\alpha_{\mathrm{N}}}}{P_{\mathtt{U}} G_{\mathrm{M}}^{\mathtt{U}} G_{\mathrm{M}}^{\mathtt{R}} \beta}\left(\mathcal{I}_{\mathtt{R}}^{\mathrm{L}} + \mathcal{I}_{\mathtt{R}}^{\mathrm{N}} + \sigma^2\right)\right] \\
&\approx \sum_{n=1}^{m_{\mathrm{N}}} (-1)^{n+1} \begin{pmatrix} m_{\mathrm{N}} \\ n \end{pmatrix} e^{-s_{\mathrm{N}} \sigma^2} \mathcal{L}_{\mathcal{I}_{\mathtt{R}}^{\mathrm{L}}}\left(s_{\mathrm{N}}\right) \mathcal{L}_{\mathcal{I}_{\mathtt{R}}^{\mathrm{N}}}\left(s_{\mathrm{N}}\right),
\end{aligned} \tag{A.3}$$

where $\eta_{\mathrm{L}} = m_{\mathrm{L}}(m_{\mathrm{L}}!)^{-\frac{1}{m_{\mathrm{L}}}}$, $\eta_{\mathrm{N}} = m_{\mathrm{N}}(m_{\mathrm{N}}!)^{-\frac{1}{m_{\mathrm{N}}}}$, and we have used the assumption that m_{L} and m_{N} are integers, and $\Phi_{\mathtt{U}}^{\mathrm{L}}$ and $\Phi_{\mathtt{U}}^{\mathrm{N}}$ are independent. (a) comes from Appendix A of [33] . We assume $s_q(x) = \frac{n \eta_q \gamma L(x)^{\alpha_q}}{P_{\mathtt{U}} G_{\mathrm{M}}^{\mathtt{U}} G_{\mathrm{M}}^{\mathtt{R}} \beta}$. By applying the stochastic geometry, the LoS interference $\mathbb{E}_{\Phi_{\mathtt{U}}^{\mathrm{L}} \backslash o}$ can be derived as

$$\begin{aligned}
&\mathcal{L}_{\mathcal{I}_{\mathtt{R}}^{\mathrm{L}}}\left(s_q\right) = \mathbb{E}_{\Phi_{\mathtt{U}}^{\mathrm{L}} \backslash o}\left[e^{-s_q \mathcal{I}_{\mathtt{R}}^{\mathrm{L}}}\right] \\
&= \mathbb{E}\left\{\exp\left(-s_q \sum_{l \in \Phi_{\mathtt{U}}^{\mathrm{L}} \backslash o} \sum_{i,j \in \{\mathrm{M},\mathrm{m}\}} \mathrm{P}_i^{\mathtt{U}} \mathrm{P}_j^{\mathtt{R}} \, \frac{P_{\mathtt{U}} |h_l|^2 G_i^{\mathtt{U}} G_j^{\mathtt{R}} \beta}{L(u)^{\alpha_{\mathrm{L}}}}\right)\right\} \\
&\overset{(b)}{=} \prod_{i,j \in \{\mathrm{M},\mathrm{m}\}} \mathrm{P}_i^{\mathtt{U}} \mathrm{P}_j^{\mathtt{R}} \exp\left\{-{\lambda_{\mathtt{U}}}^{-1} \times\right. \\
&\left\{\int_0^{2\pi} \int_{u_{\min}^{(1)}(\vartheta)}^{u_{\max}^{(1)}(\vartheta)} \Omega_{\mathrm{L}}^q\left(u, P_{\mathtt{U}}, G_i^{\mathtt{U}} G_j^{\mathtt{R}}\right) u p_{\mathtt{U},\mathrm{L}}(R(u)) \zeta^{(2)}(u) \, du d\vartheta\right. \\
&\left.\left. + \int_0^{2\pi} \int_{u_{\min}^{(2)}(\vartheta)}^{u_{\max}^{(2)}(\vartheta)} \Omega_{\mathrm{L}}^q\left(u, P_{\mathtt{U}}, G_i^{\mathtt{U}} G_j^{\mathtt{R}}\right) u p_{\mathtt{U},\mathrm{L}}(R(u)) \lambda_{\mathtt{U}}^2 du d\vartheta\right\}\right\},
\end{aligned} \tag{A.4}$$

where (b) comes from the Laplace function of the MHC point process with $\Phi_{\mathtt{U}}^{\mathrm{L}}$, and notice that $|h_l|^2$ is a normalized gamma random variable with the parameter m_{L} for the small scale fading. Fig. 11 shows the interference range, u is the integral variable from the original point 'o' to 'l' which denotes the distance from the associated UAV BS to the interference UAV. $\Omega_{\mathrm{L}}^q\left(u, P_{\mathtt{U}}, G_i^{\mathtt{U}} G_j^{\mathtt{R}}\right)$ is given as follows,

$$\Omega_{\mathrm{L}}^q\left(u, P_{\mathtt{U}}, G_i^{\mathtt{U}} G_j^{\mathtt{R}}\right) = 1 - \left(1 + \frac{n \eta_q \gamma L(x)^{\alpha_q} G_i^{\mathtt{U}} G_j^{\mathtt{R}}}{L(R(u))^{\alpha_{\mathrm{L}}} G_{\mathrm{M}}^{\mathtt{U}} G_{\mathrm{M}}^{\mathtt{R}} m_{\mathrm{L}}}\right)^{-m_{\mathrm{L}}}, \tag{A.5}$$

where $R(u)$ is given as $R(u) = \sqrt{x^2 + u^2 - 2xu\cos\vartheta}$. Based on $R(u)$, we can write down the distance $L(R(u))$ from the associated UAV BS to the typical receiver as

$$L(R(u)) = \sqrt{x^2 + u^2 - 2xu\cos\vartheta + H_{\mathtt{U}}^2}. \tag{A.6}$$

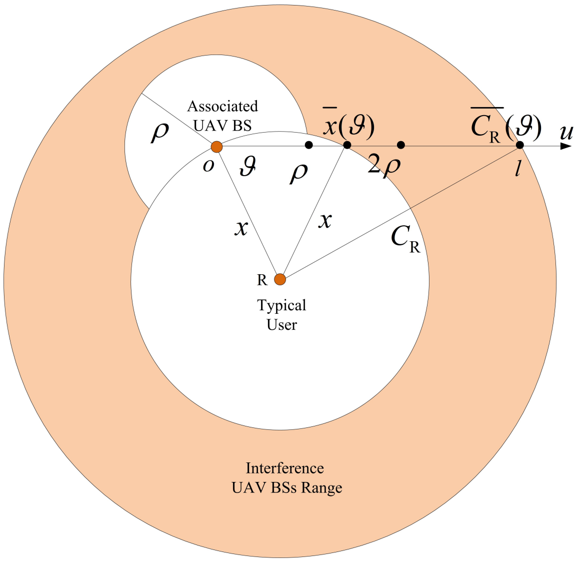

ρ
Associated UAV BS
$\overline{x}(\vartheta)$
$\overline{C}_R(\vartheta)$
u
o
ϑ
ρ
2ρ
l
x
x
C_R
R
Typical User
Interference UAV BSs Range

Fig. 11: Diagram of the MHC point process interference distance.

From trigonometry in Fig. 11, we can see that the lower integral limit of u for the horizontal distance from the typical user to interference UAV BS is equal to x since the closest interference UAV BS is at least at a distance $\overline{x}(\vartheta)$ on the projection plane, which is given by

$$\overline{x}(\vartheta) = 2x\left|\cos\vartheta\right|. \tag{A.7}$$

Similarly, we denote the upper integral limit of u to the UAV maximum connection distance, which is given by

$$\overline{C}_{\mathtt{R}}(\vartheta) = C_{\mathtt{R}}\sin\left(\pi - \sin^{-1}(\tfrac{x\sin\vartheta}{C_{\mathtt{R}}}) - \vartheta\right)/\sin\vartheta. \tag{A.8}$$

Based on the above results, the integral limits for $\rho < u < 2\rho$ in (10) are given by

$$\begin{cases} u_{\max}^{(1)}(\vartheta) = \min\left[\max\left[2\rho, \overline{x}(\vartheta)\right], \overline{C}_{\mathtt{R}}(\vartheta)\right] \\ u_{\min}^{(1)}(\vartheta) = \max\left[\rho, \overline{x}(\vartheta)\right] \end{cases}, \tag{A.9}$$

and when $u \geq 2\rho$ in (10), the integral limits are given by[4]

$$\begin{cases} u_{\max}^{(2)}(\vartheta) = \overline{C}_{\mathtt{R}}(\vartheta) \\ u_{\min}^{(2)}(\vartheta) = \max\left[2\rho, \overline{x}(\vartheta)\right] \end{cases}. \tag{A.10}$$

Finally, we have $\zeta^{(2)}(u) = 0$ when $u < \rho$.

Using a similar approach in (A.4), we derive the interference coming from NLoS links as follows

$$\mathcal{L}_{\mathcal{I}_{\mathtt{R}}^{\mathrm{N}}}\left(s_q\right) = \mathbb{E}_{\Phi_{\mathtt{U}}^{\mathrm{L}}\backslash o}\left[e^{-s_q\mathcal{I}_{\mathtt{U}}^{\mathrm{N}}}\right] = \prod_{i,j\in\{\mathrm{M,m}\}} \mathrm{P}_i^{\mathtt{U}}\mathrm{P}_j^{\mathtt{R}} \exp\left\{-\lambda_{\mathtt{U}}{}^{-1}\times\right.$$
$$\left\{\int_0^{2\pi}\int_{u_{\min}^{(1)}(\vartheta)}^{u_{\max}^{(1)}(\vartheta)} \Omega_{\mathrm{N}}^{q}\left(u, P_{\mathtt{U}}, G_i^{\mathtt{U}}G_j^{\mathtt{R}}\right) u p_{\mathtt{U},\mathrm{N}}(R(u))\zeta^{(2)}\left(u\right) du d\vartheta\right.,$$
$$\left. + \int_0^{2\pi}\int_{u_{\min}^{(2)}(\vartheta)}^{u_{\max}^{(2)}(\vartheta)} \Omega_{\mathrm{N}}^{q}\left(u, P_{\mathtt{U}}, G_i^{\mathtt{U}}G_j^{\mathtt{R}}\right) u p_{\mathtt{U},\mathrm{N}}(R(u))\lambda_{\mathtt{U}}^{2} du d\vartheta\right\}\Big\} \tag{A.11}$$

and $\Omega_{\mathrm{N}}^{q}\left(u, P_{\mathtt{U}}, G_i^{\mathtt{U}}G_j^{\mathtt{R}}\right)$ is given by

$$\Omega_{\mathrm{N}}^{q}\left(u, P_{\mathtt{U}}, G_i^{\mathtt{U}}G_j^{\mathtt{R}}\right) = 1 - \left(1 + \frac{n\eta_q\gamma L(x)^{\alpha_q}G_i^{\mathtt{U}}G_j^{\mathtt{R}}}{L(R(u))^{\alpha_{\mathrm{L}}}G_{\mathrm{M}}^{\mathtt{U}}G_{\mathrm{M}}^{\mathtt{R}}m_{\mathrm{N}}}\right)^{-m_{\mathrm{N}}}. \tag{A.12}$$

After that, we can obtain the CDF of the SINR in (18), and this completes the proof.

Appendix B: Proof of Theorem 2

Define $\mathcal{F}_{\mathtt{E}^*}(\cdot)$ as the CDF of the SNR of the most detrimental eavesdropper, which can be written as

$$\begin{aligned} \mathcal{F}_{\mathtt{E}^*}(\gamma) &= \mathbb{P}\left(\mathrm{SNR}_{\mathtt{E}^*} < \gamma\right) \\ &= \mathbb{P}\left(\max\left\{\mathrm{SNR}_{\mathtt{E}^*}^{\mathrm{L}}, \mathrm{SNR}_{\mathtt{E}^*}^{\mathrm{N}}\right\} < \gamma\right). \end{aligned} \tag{B.1}$$

By using the thinning theorem in the point process, we divide the eavesdroppers into the LoS point process $\Phi_{\mathtt{E}}^{\mathrm{L}}$ with density $\lambda_{\mathtt{E}}p_{\mathtt{U},\mathrm{L}}(r)$ and the NLoS point process $\Phi_{\mathtt{E}}^{\mathrm{N}}$ with density $\lambda_{\mathtt{E}}p_{\mathtt{U},\mathrm{N}}(r)$, respectively. Different from the UAVs, eavesdroppers do not have safety distance between each other. Accordingly, we express (B.1) as

$$\mathcal{F}_{\mathtt{E}^*}(\gamma) = \mathbb{P}\left(\mathrm{SNR}_{\mathtt{E}^*}^{\mathrm{L}} < \gamma\right)\cdot\mathbb{P}\left(\mathrm{SNR}_{\mathtt{E}^*}^{\mathrm{N}} < \gamma\right). \tag{B.2}$$

$\Pr\left(\mathrm{SNR}_{\mathtt{E}^*}^{\mathrm{L}} < \gamma\right)$ is derived as

$$\begin{aligned} \mathbb{P}\left(\mathrm{SNR}_{\mathtt{E}^*}^{\mathrm{L}} < \gamma\right) &= \mathbb{E}\left[\prod_{e\in\Phi_{\mathtt{E}}^{\mathrm{L}}} \Pr\left(\frac{P_{\mathtt{U}}|h_e|^2G_i^{\mathtt{U}}G_i^{\mathtt{R}}\beta}{L(y)^{\alpha_{\mathrm{L}}}\sigma^2} < \gamma\right)\right] \\ &= \exp\left\{-2\pi\lambda_{\mathtt{E}}\int_{H_{\mathtt{U}}}^{\sqrt{C_{\mathtt{E}}^2+H_{\mathtt{U}}^2}} \underbrace{\left(1 - \Pr\left(\frac{P_{\mathtt{U}}h_eG_i^{\mathtt{U}}G_i^{\mathtt{E}}\beta}{L^{\alpha_{\mathrm{L}}}\sigma^2} < \gamma\right)\right)}_{\mathrm{T_L}(L(y),\gamma)}\right. \\ &\qquad \left.\times\, p_{\mathtt{U},\mathrm{L}}(\sqrt{L^2 - H_{\mathtt{U}}^2})LdL\right\} \\ &= \exp\left\{-2\pi\lambda_{\mathtt{E}}\int_0^{C_{\mathtt{E}}} \mathrm{T_L}\left(y,\gamma\right)p_{\mathtt{U},\mathrm{L}}(y)ydy\right\}, \end{aligned} \tag{B.3}$$

where $\left|h_e\right|^2$ in (B.3) is a normalized gamma random variable with the parameter m_{L}. Similarly, we derive $\Pr\left(\mathrm{SNR}_{\mathtt{E}^*}^{\mathrm{N}} < \gamma\right)$ below:

$$\begin{aligned} \mathbb{P}\left(\mathrm{SNR}_{\mathtt{E}^*}^{\mathrm{N}} < \gamma\right) &= \mathbb{E}\left[\prod_{e\in\Phi_{\mathtt{E}}^{\mathrm{N}}} \Pr\left(\frac{P_{\mathtt{U}}|h_e|^2G_i^{\mathtt{U}}G_i^{\mathtt{E}}\beta}{L(y)^{\alpha_{\mathrm{N}}}\sigma^2} < \gamma\right)\right] \\ &= \exp\left\{-2\pi\lambda_{\mathtt{E}}\int_0^{C_{\mathtt{E}}} \mathrm{T_N}\left(y,\gamma\right)p_{\mathtt{U},\mathrm{N}}(y)ydy\right\}, \end{aligned} \tag{B.4}$$

where $\left|h_e\right|^2$ in (B.4) is a normalized gamma random variable with the parameter m_{N}. $\mathrm{T}_q, q\in\{L,N\}$ in (B.3) and (B.4) is obtained using (B.5) below based on the law of the total probability:

$$\mathrm{T}_q\left(y,\gamma\right) = \prod_{i,j\in\{\mathrm{M,m}\}} \mathrm{P}_i^{\mathtt{U}}\mathrm{P}_j^{\mathtt{E}} \Pr\left(h_e > \frac{\gamma L(y)^{\alpha_q}}{P_{\mathtt{U}}G_i^{\mathtt{U}}G_j^{\mathtt{E}}\beta}\sigma^2\right). \tag{B.5}$$

Substituting (B.3) and (B.4) into (B.2), we can derive (26) and this completes the proof.

[4] Note that we ignore the worst case scenario where $\rho > \overline{C}_{\mathtt{R}}(\vartheta)$ and assume that $\overline{C}_{\mathtt{R}}(\vartheta)$ is always greater than 2ρ.

Appendix C: Proof of Theorem 4

It can be proved by following a similar approach shown in Appendix B for **Theorem 2**, where $\mathrm{W}_q(\gamma, y)$ is given by

$$\begin{aligned} &\mathrm{W}_q(\gamma, y) = \Pr\left(h_e > \frac{\gamma L(y)^{\alpha_q}}{P_{\mathtt{U}}\beta} \left(\sigma^2 + I_{\mathtt{E}}^{(J)} \right) \right) \\ &\approx \sum_{n=1}^{m_q} (-1)^{n+1} \left(\begin{array}{c} m_q \\ n \end{array} \right) \prod_{i,i',j \in \{\mathrm{M},\mathrm{m}\}} \mathrm{P}_i^{\mathtt{U}} \mathrm{P}_{i'}^{\mathtt{U}} \mathrm{P}_j^{\mathtt{E}} \times \\ &\left\{ e^{-\frac{n\eta_q \gamma L(y)^{\alpha_q}}{P_{\mathtt{U}} G_i^{\mathtt{U}} G_j^{\mathtt{E}} \beta}} \mathcal{L}_{I_{\mathtt{E}}^{(J)}} \left(\frac{n\eta_q \gamma L(y)^{\alpha_q}}{P_{\mathtt{U}} G_i^{\mathtt{U}} G_j^{\mathtt{E}} \beta} \right) \right\}. \end{aligned} \quad \text{(C.1)}$$

$\mathcal{L}_{I_{\mathtt{E}}^{(J)}}(\cdot) = \mathcal{L}_{I_{\mathtt{E}}^{\mathrm{L},(J)}}(\cdot) \cdot \mathcal{L}_{I_{\mathtt{E}}^{\mathrm{N},(J)}}(\cdot)$ is obtained by the basic principle of the MHC point process with LoS jamming UAVs with the density $\varepsilon\lambda_{\mathtt{U}}$, for LoS link with $\varepsilon\lambda_{\mathtt{U}} p_{\mathtt{U},\mathrm{L}}(u)$ and NLoS jamming UAVs with the density $\varepsilon\lambda_{\mathtt{U}} p_{\mathtt{U},\mathrm{N}}(u)$, respectively. The proof of $\mathcal{L}_{I_{\mathtt{E}}^{\mathrm{L},(J)}}$ and $\mathcal{L}_{I_{\mathtt{E}}^{\mathrm{N},(J)}}$ are similar to (A.4) in Appendix A.

References

[1] Cisco, "Cisco visual networking index: Global mobile data traffic forecast update: 2016–2021 white paper," Feb. 2017.

[2] 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.

[3] J. Wang, C. Jiang, Z. Han, Y. Ren, R. G. Maunder, and L. Hanzo, "Cooperative distributed unmanned aerial vehicular networks: Small and mini drones," *IEEE Veh. Technol. Mag.*, pp. 1–18, Dec. 2016.

[4] M. Strohmeier, V. Lenders, and I. Martinovic, "On the security of the automatic dependent surveillance-broadcast protocol," *IEEE Commun. Surveys Tuts*, vol. 17, no. 2, pp. 1066–1087, Secondquarter 2015.

[5] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: State of the art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015.

[6] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[7] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425–430, Feb. 2011.

[8] W. Aman, G. A. S. Sidhu, T. Jabeen, F. Gao, and S. Jin, "Enhancing physical layer security in dual-hop multiuser transmission," in *Proc., IEEE Wireless Commun. and Netw. Conf. (WCNC)*, Doha, Qatar, Sep. 2016, pp. 1–6.

[9] K. Cumanan, Z. Ding, M. Xu, and H. V. Poor, "Secrecy rate optimization for secure multicast communications," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1417–1432, Aug. 2016.

[10] X. Qi, B. Li, Z. Chu, K. Huang, and H. Chen, "Secrecy energy efficiency performance of UAV-enabled communication networks," *arXiv preprint arXiv:1704.01883*, 2017.

[11] Q. Wang, Z. Chen, W. Mei, and J. Fang, "Improving physical layer security using UAV-enabled mobile relaying," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 310–313, Jun. 2017.

[12] A. Al-Hourani, S. Kandeepan, and S. Lardner, "Optimal LAP altitude for maximum coverage," *IEEE Wireless Commun. Lett.*, vol. 3, no. 6, pp. 569–572, Dec. 2014.

[13] B. Galkin, J. Kibiłda, and L. A. DaSilva, "Coverage analysis for low-altitude UAV networks in urban environments," *arXiv preprint arXiv:1704.06214*, 2017.

[14] V. V. Chetlur and H. S. Dhillon, "Downlink coverage analysis for a finite 3D wireless network of unmanned aerial vehicles," *IEEE Trans. Commun.*, vol. 65, no. 10, pp. 4543–4558, Jul. 2017.

[15] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Drone small cells in the clouds: Design, deployment and performance analysis," in *Proc., IEEE Global Commun. Conf. (GLOBECOM)*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[16] M. Ding and D. L. Pérez, "Please lower small cell antenna heights in 5g," in *Proc., IEEE Global Commun. Conf. Commun. (GLOBECOM)*. Washington, DC, USA: IEEE, Dec. 2016, pp. 1–6.

[17] M. Alzenad, A. El-Keyi, F. Lagum, and H. Yanikomeroglu, "3-D placement of an unmanned aerial vehicle base station (UAV-BS) for energy-efficient maximal coverage," *IEEE Wireless Commun. Lett.*, vol. 6, no. 4, pp. 434–437, Aug. 2017.

[18] J. Zhao, F. Gao, Q. Wu, S. Jin, Y. Wu, and W. Jia, "Beam tracking for uav mounted satcom on-the-move with massive antenna array," *arXiv preprint arXiv:1709.07989*, 2017.

[19] X. Li, T. Bai, and R. W. Heath, "Impact of 3d base station antenna in random heterogeneous cellular networks," in *Proc., IEEE Wireless Commun. and Netw. Conf. (WCNC)*. Istanbul, Turkey: IEEE, Apr. 2014, pp. 2254–2259.

[20] K. Venugopal, M. C. Valenti, and R. W. Heath, "Device-to-device millimeter wave communications: Interference, coverage, rate, and finite topologies," *IEEE Trans. Wireless Commun.*, vol. 15, no. 9, pp. 6175–6188, Sep. 2016.

[21] M. Haenggi, *Stochastic geometry for wireless networks*. Cambridge University Press, 2012.

[22] X. Ge, B. Du, Q. Li, and D. S. Michalopoulos, "Energy efficiency of multiuser multiantenna random cellular networks with minimum distance constraints," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1696–1708, Feb. 2017.

[23] A. M. Ibrahim, T. ElBatt, and A. El-Keyi, "Coverage probability analysis for wireless networks using repulsive point processes," in *Proc., IEEE Personal Indoor and Mobi. Radio Commun. (PIMRC)*. London, UK: IEEE, 2013, pp. 1002–1007.

[24] Y. Zou, J. Zhu, L. Yang, Y.-C. Liang, and Y.-D. Yao, "Securing physical-layer communications for cognitive radio networks," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 48–54, Sep. 2015.

[25] K. Cumanan, H. Xing, P. Xu, G. Zheng, X. Dai, A. Nallanathan, Z. Ding, and G. K. Karagiannidis, "Physical layer security jamming: Theoretical limits and practical designs in wireless networks," *IEEE Access*, vol. 5, pp. 3603–3611, Dec. 2016.

[26] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, Jun. 2008.

[27] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct 2013.

[28] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, Oct. 2009.

[29] Y. Deng, L. Wang, S. A. R. Zaidi, J. Yuan, and M. Elkashlan, "Artificial-noise aided secure transmission in large scale spectrum sharing networks," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 2116–2129, May 2016.

[30] K. Cumanan, G. C. Alexandropoulos, Z. Ding, and G. K. Karagiannidis, "Secure communications with cooperative jamming: Optimal power allocation and secrecy outage analysis," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7495–7505, Aug 2017.

[31] Y. Zou and J. Zhu, "Intercept probability analysis of joint user-jammer selection against eavesdropping," in *Proc., IEEE Global Commun. Conf. Commun. (GLOBECOM)*. Washington, DC, USA: IEEE, Dec. 2016, pp. 1–6.

[32] H. Guo, Z. Yang, L. Zhang, J. Zhu, and Y. Zou, "Power-constrained secrecy rate maximization for joint relay and jammer selection assisted wireless networks," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2180–2193, May 2017.

[33] T. Bai and R. W. Heath, "Coverage and rate analysis for millimeter-wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 1100–1114, Feb. 2015.

[34] O. Bouachir, A. Abrassart, F. Garcia, and N. Larrieu, "A mobility model for UAV ad hoc network," in *Proc., IEEE Intl. Conf. on Unmanned Aircraft Systems (ICUAS)*. Orlando, FL, USA: IEEE, 2014, pp. 383–388.

[35] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006–2021, Apr. 2014.

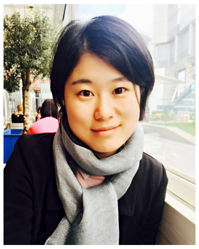
[36] F. Baccelli, B. Błaszczyszyn *et al.*, "Stochastic geometry and wireless networks: Volume II Applications," *Foundations and Trends® in Networking*, vol. 4, no. 1–2, pp. 1–312, Jan. 2010.

[37] M. Haenggi, "Mean interference in hard-core wireless networks," *IEEE Commun. Lett.*, vol. 15, no. 8, pp. 792–794, Aug. 2011.

[38] T. S. Rappaport, E. Ben-Dor, J. N. Murdock, and Y. Qiao, "38 GHz and 60 GHz angle-dependent propagation for cellular & peer-to-peer

wireless communications," in *Proc., IEEE Int. Conf. Commun. (ICC)*, Ottawa, Canada, Nov. 2012, pp. 4568–4573.

[39] H. Oh, H.-S. Shin, S. Kim, P. Ladosz, and W.-H. Chen, "Communication-aware convoy following guidance for uavs in a complex urban environment," in *Control and Automation (MED), 24th Mediterranean Conference on*. Athens, Greece: IEEE, 2016, pp. 1230–1235.



Yongxu Zhu is research associate at Loughborough University now. She received the M.S. degree from the Beijing University of Posts and Telecommunications and Dublin City Univeristy, in 2012 and 2013, and the Ph.D degree in Electrical Engineering from University College London in 2017. Her research interests are in the areas of energy harvesting wireless communications, wireless edge caching, millimeter-wave communications, heterogeneous cellular networks, Massive MIMO, physical-layer security.

Gan Zheng (S'05-M'09-SM'12) received the BEng and the MEng from Tianjin University, Tianjin, China, in 2002 and 2004, respectively, both in Electronic and Information Engineering, and the PhD degree in Electrical and Electronic Engineering from The University of Hong Kong in 2008. He is currently a Senior Lecturer in the Wolfson School of Mechanical, Electrical and Manufacturing Engineering, Loughborough University, UK. His research interests include edge caching, full-duplex radio, wireless power transfer, cooperative communications, cognitive radio and physical-layer security. He is the first recipient for the 2013 IEEE Signal Processing Letters Best Paper Award, and he also received 2015 GLOBECOM Best Paper Award. He currently serves as an Associate Editor for IEEE Communications Letters.

Michael Fitch works in BT Research and Innovation, providing technical leadership to a small research team specialising in physical and systems aspects of wireless communications. He is currently working on a number of projects on emerging wireless technologies such as small cells, radio resource management and 5G. In addition he provides engineering consultancy to other parts of BT on LTE, WiFi and other wireless topics. Previous experience is with modelling, trials and deployments of Satellite, WiMAX, 3G and LTE systems. Michael has a first degree in maths and physics, a PhD in satellite communications and he is a member of the IET.