INL/CON-18-52261-Revision-0

Enhancing Physical Layer Security for NOMA Transmission in mmWave Drone Networks

Nadasanka Rupasinghe, Yanuz Yapici, Ismail Guvenc, Huaiyu Dai, Arupjyoti Bhuyan

December 2018

INL/CON-18-52261-Revision-0

Enhancing Physical Layer Security for NOMA Transmission in mmWave Drone Networks

Nadasanka Rupasinghe, Yanuz Yapici, Ismail Guvenc, Huaiyu Dai, Arupjyoti Bhuyan

December 2018

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Enhancing Physical Layer Security for NOMA Transmission in mmWave Drone Networks

Nadisanka Rupasinghe*, Yavuz Yapıcı*, İsmail Güvenç*, Huaiyu Dai*, Arupjyoti Bhuyan†
*Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC
†Idaho National Laboratory, Idaho Falls, ID
{rprupasi, yyapici, iguvenc, hdai}@ncsu.edu, arupjyoti.bhuyan@inl.gov

***Abstract*—Physical layer security (PLS) is critically important for emerging wireless communication networks to maintain the confidentiality of the information of legitimate users. In this paper, we investigate enhancing PLS in an unmanned aerial vehicle (UAV) based communication network where a UAV acting as an aerial base station (BS) provides coverage in a densely packed user area (such as a stadium or a concert area). In particular, non-orthogonal multiple access (NOMA) together with highly-directional multi-antenna transmission techniques in mmWave frequency bands are utilized for improving spectral efficiency. In order to achieve PLS against potential eavesdropper attacks, we introduce a protected zone around the user region. However, limited resource availability refrain protected zone being extended to cover the entire eavesdropper region. Hence, we propose an approach to optimize the protected zone shape (for fixed area) at each UAV-BS hovering altitude. The associated secrecy performance is evaluated considering the secrecy outage and sum secrecy rates. Numerical results reveal the importance of protected zone shape optimization at each altitude to maximize NOMA secrecy rates.**

***Index Terms*—5G, drone, HPPP, mmWave, non-orthogonal multiple access (NOMA), physical layer security (PLS), UAV.**

I. Introduction

The importance of deploying unmanned aerial vehicle (UAV) based communication networks during temporary events and after disasters to provide on-demand coverage and enhance capacity has recently been explored in some real word deployments and field trials [1], [2]. In order to reap maximum benefits from such networks, enhancing the spectral efficiency (SE) is essential. To that end, integrating non-orthogonal multiple access (NOMA) transmission to UAVs acting as aerial base stations (BSs) can be an effective solution [3], [4]. While enhancing the SE with NOMA, it is equally important to guarantee the confidentiality of communication going on between UAV-BS and legitimate users. Hence, introducing appropriate physical layer security (PLS) techniques to such networks become paramount importance.

A UAV based mobile cloud computing system is proposed in [5] where UAVs offer computation offloading opportunities to mobile stations (MS) with limited local processing capabilities. In that, just for offloading purposes between a UAV and the MSs, NOMA is proposed as one viable solution. In our earlier work [3], [4], NOMA transmission is introduced to UAVs acting as aerial BSs to provide coverage over a stadium or a concert scenario. In particular, leveraging multi-antenna techniques a UAV-BS generates directional beams, and multiple users are served within the same beam employing NOMA transmission. In [3], assuming the availability of user distance information, a beam scanning strategy is proposed to maximize NOMA sum rates whereas in [4] we study the performance of different feedback schemes for NOMA.

PLS in wireless communication networks has recently attracted significant attention [6]–[8]. One of the main objectives of the PLS is to increase the performance gap of the link quality between the legitimate user and that of the eavesdropper (Eve) by exploiting the physical properties of the wireless medium [9]. To enhance the PLS in wireless ad-hoc networks, artificial noise (AN) aided multi-antenna transmission strategy is proposed in [6]. In [7], a *protected zone* is defined surrounding the transmitter along with beamforming and AN transmission to enhance the PLS in a multi-input-single-output (MISO) communication system. Within the protected zone it is guaranteed that no Eve exists. Considering single antenna and multi-antenna scenarios, PLS with NOMA transmission in large-scale networks is investigated in [8]. In particular, for single antenna scenario Eve exclusion area is proposed while for multi-antenna scenario AN generation towards undesired directions is introduced to enhance PLS.

In this paper, we consider a similar scenario as in [3], [4], where a UAV-BS is employed to provide broadband connectivity over a densely packed user area in a stadium. NOMA along with multi-antenna transmission is then introduced to improve the SE. In particular, we consider there are Eves outside of the user area trying to breach communication going on between legitimate users and UAV-BS. In order to enhance the PLS of the UAV based communication network, we introduce a protected zone around the user area [7], [8]. However, due to physical constraints, protected zone may not be able to eliminate all the Eves distributed within the area. Hence, we propose an approach to optimize the protected zone shape based on UAV-BS hovering altitude such that the achievable NOMA sum secrecy rates are maximized.

II. System Model

A. Overview

We consider a mmWave-NOMA transmission scenario where a single UAV-BS equipped with an M element uniform linear array (ULA) is serving single-antenna users in the DL. We assume that all the users lie inside a specific *user region* as shown in Fig. 1. A 3-dimensional (3D) beam is generated by the UAV-BS which entirely covers the user region. We assume that there are K users in total, and the users can be represented by the set $\mathcal{N}_{\rm U} = \{1, 2, \dots K\}$. The user region

This research was supported in part by NSF under the grant CNS-1618692.

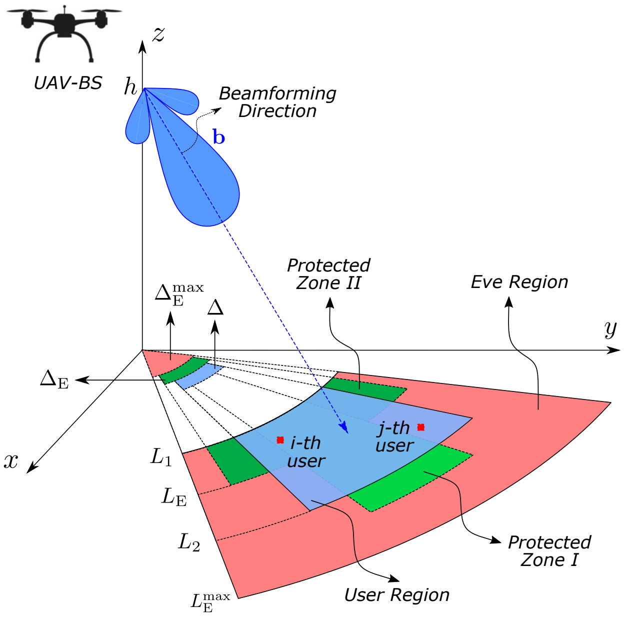


Fig. 1: System scenario where NOMA transmission serves multiple users simultaneously in a single DL beam.

is identified by an inner-radius L_1, an outer-radius L_2, and the angle Δ, which is the fixed angle within the projection of horizontal propagation pattern of UAV-BS on the xy-plane. Note that it is possible to reasonably model various different hot spot scenarios such as a stadium, concert hall, traffic jam, and urban canyon by modifying these control parameters.

We assume that although the user region is free from eavesdroppers, the surrounding region includes Eves trying to intercept the transmission between UAV-BS and the legitimate users. We designate the bounded region around the user region, which includes Eves as *Eve region*. Similar to the user region, we identify the Eve region by the same inner radius L_1, an outer radius $L_{\mathrm{E}}^{\max}$ (greater than L_2), and $\Delta_{\mathrm{E}}^{\max}$ (greater than Δ), as shown in Fig. 1. We assume K_{E} Eves in total, which are represented by the set $\mathcal{N}_{\mathrm{E}} = \{1, 2, \dots K_{\mathrm{E}}\}$. Note that horizontal footprint of the UAV-BS beam pattern covers the Eve region (so that any Eve has nonzero channel to UAV-BS), as well, but the coverage over Eve region might be provided by the side lobes depending on the specific radiation pattern.

B. Location Distribution and mmWave Channel Model

We assume that users and Eves are uniformly, randomly distributed within their specified regions following homogeneous Poisson point process (HPPP) with the densities λ and λ_{E}, respectively. The number of users (Eves) in the user (Eve) region is therefore Poisson distributed, i.e., $\mathrm{P}(k \text{ users in the user region}) = \frac{\mu^k e^{-\mu}}{k!}$ with $\mu = (L_2^2 - L_1^2)\frac{\Delta}{2}\lambda$.

We assume that all the users have line-of-sight (LoS) paths since i) UAV-BS is hovering at relatively high altitudes, and ii) LoS path is much stronger than non-LoS (NLoS) paths in mmWave frequency band [3], [10]. The channel $\mathbf{h}_k$ between the k-th user and the UAV-BS is therefore given as

$$\mathbf{h}_k = \sqrt{M}\frac{\alpha_k \mathbf{a}(\theta_k)}{\left[\mathrm{PL}\left(\sqrt{d_k^2 + h^2}\right)\right]^{1/2}}, \qquad (1)$$

where h, d_k, α_k and θ_k represent UAV-BS hovering altitude, horizontal distance between k-th user and UAV-BS, small scale fading gain (i.e., complex Gaussian with $\mathcal{CN}(0,1)$), and angle-of-departure (AoD), respectively. In addition, $\mathbf{a}(\theta_k)$ is the steering vector associated with AoD θ_k, and PL (x) represents the path loss (PL) over the distance x. Note that the channel between ℓ-th Eve in the Eve region (i.e., $\ell \in \mathcal{N}_{\mathrm{E}}$) and UAV-BS can also be given using (1).

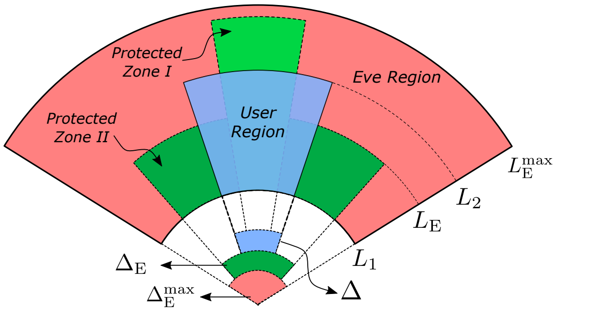


Fig. 2: Footprint of *protected zone* represented by angle-distance pair (Δ_{E}, L_{E}), which is free from any eavesdroppers.

C. Protected Zone Approach for Physical Layer Security

The overall transmission scheme between the UAV-BS and legitimate users presented in Fig. 1 is highly prone to the Eve attacks, and the PLS is accordingly impaired. In this study, we consider protected zone approach to enhance the secrecy rates of the network [7], [8]. In the proposed approach, an additional area (i.e., protected zone) around the user region (and inside the Eve region) has been cleared from Eves by means of some measures, as shown Fig. 2. This protected area is actually a fraction of the complete Eve region, and we denote this fraction by q with $q \leq 1$. Note that since clearing Eves in the protected zone requires certain resources being spent on the ground, our goal is to keep this area as small as possible. In addition, we consider to optimize the shape of the protected zone to enhance secrecy rates while keeping its area the same, which is the main problem we tackle in this study.

The protected zone can be represented by an angle-distance (radius) pair (Δ_{E}, L_{E}) with $\Delta_{\mathrm{E}}^{\min} \leq \Delta_{\mathrm{E}} \leq \Delta_{\mathrm{E}}^{\max}$ and $L_1 \leq L_{\mathrm{E}} \leq L_{\mathrm{E}}^{\max}$. Note that $\Delta_{\mathrm{E}}^{\min}$ is the minimum angle value which occurs when $L_{\mathrm{E}} = L_{\mathrm{E}}^{\max}$. We can therefore represent $\Delta_{\mathrm{E}}^{\min}$ as follows

$$\Delta_{\mathrm{E}}^{\min} = \frac{q\left[\left((L_{\mathrm{E}}^{\max})^2 - L_1^2\right)\Delta_{\mathrm{E}}^{\max} - (L_2^2 - L_1^2)\Delta\right]}{(L_{\mathrm{E}}^{\max})^2 - L_2^2}. \qquad (2)$$

As sketched in Fig. 2, it is possible to have different shapes for protected zone for a fixed q value. Note that whenever we have $\Delta_{\mathrm{E}} \leq \Delta$, L_{E} should be sufficiently greater than L_2 (e.g., "Protected Zone I" in Fig. 2) to have a nonzero protected zone. When $\Delta \leq \Delta_{\mathrm{E}} \leq \Delta_{\mathrm{E}}^{\max}$, L_{E} might however be smaller (e.g., "Protected Zone II" in Fig. 2) or greater than L_2 depending on the area of the user region and particular q choice. Specifically, L_{E} can be parametrically expressed as follows

$$L_{\mathrm{E}}^2 = L_2^2 + \frac{q}{\Delta_{\mathrm{E}}}\left[\left((L_{\mathrm{E}}^{\max})^2 - L_1^2\right)\Delta_{\mathrm{E}}^{\max} - (L_2^2 - L_1^2)\Delta\right], \qquad (3)$$

for $\Delta_{\mathrm{E}}^{\min} \leq \Delta_{\mathrm{E}} \leq \Delta$. Whenever we have $\Delta < \Delta_{\mathrm{E}} \leq \Delta_{\mathrm{E}}^{\max}$,

$$L_{\mathrm{E}}^2 = L_1^2 + \frac{q}{\Delta_{\mathrm{E}}}\left[\left((L_{\mathrm{E}}^{\max})^2 - L_1^2\right)\Delta_{\mathrm{E}}^{\max} + \frac{1-q}{q}(L_2^2 - L_1^2)\Delta\right], \qquad (4)$$

provided $L_{\mathrm{E}}^2 \geq L_2^2$, and L_{E} is otherwise expressed as

$$L_{\mathrm{E}}^2 = L_1^2 + \frac{q}{\Delta_{\mathrm{E}} - \Delta}\Big[\big((L_{\mathrm{E}}^{\max})^2 - L_1^2\big)\Delta_{\mathrm{E}}^{\max} - (L_2^2 - L_1^2)\Delta\Big]. \quad (5)$$

III. Secure NOMA for UAV-BS Downlink

In this section, we consider NOMA transmission in UAV-BS downlink (DL) to enhance the SE, and evaluate the associated secrecy rates in the presence of protected zone.

A. Secrecy Outage and Sum Secrecy Rates

We assume that UAV-BS generates a beam $\mathbf{b}$ where the respective projection in the azimuth domain is in the direction of $\overline{\theta}$ with $\overline{\theta} \in [0, 2\pi]$ [3]. Assuming critically spaced array, the effective channel gain of user $k \in \mathcal{N}_{\mathrm{U}}$ for beamforming direction $\overline{\theta}$ can be given using (1) as follows [3], [4]

$$|\mathbf{h}_k^{\mathrm{H}}\mathbf{b}|^2 \approx \frac{|\alpha_k|^2}{M \times \mathrm{PL}\left(\sqrt{d_k^2 + h^2}\right)} \left| \frac{\sin\left(\frac{\pi M(\overline{\theta} - \theta_k)}{2}\right)}{\sin\left(\frac{\pi(\overline{\theta} - \theta_k)}{2}\right)} \right|^2,$$

$$= \frac{|\alpha_k|^2}{\mathrm{PL}\left(\sqrt{d_k^2 + h^2}\right)} \mathrm{F}_M(\pi[\overline{\theta} - \theta_k]), \quad (6)$$

where $\mathrm{F}_M(\cdot)$ is the Fejér kernel. Similarly, the effective channel gain of the most detrimental Eve, g_{E} is given as,

$$g_{\mathrm{E}} = \max_{k_{\mathrm{E}} \in \mathcal{N}_{\mathrm{E}}} |\mathbf{h}_{k_{\mathrm{E}}}^{\mathrm{H}}\mathbf{b}|^2 \quad (7)$$

where $\mathbf{h}_{k_{\mathrm{E}}}$ is the channel gain of the k_{E}-th Eve.

When deriving secrecy rates in NOMA transmission, we assume that UAV-BS knows the effective channel gains of desired users while those of Eves are unknown. Without any loss of generality, we also assume that the users in set $\mathcal{N}_{\mathrm{U}}$ are already indexed from the best to the worst with respect to their effective channel gains as represented by (6). Defining β_k to be the power allocation coefficient of k-th user, we therefore have $\beta_1 \leq \ldots \leq \beta_K$ such that $\sum_{k=1}^{K} \beta_k^2 = 1$. The transmitted signal is generated by superposition coding as

$$\mathbf{x} = \sqrt{P_{\mathrm{Tx}}}\mathbf{b} \sum_{k=1}^{K} \beta_k s_k, \quad (8)$$

where P_{Tx} and s_k are the total DL transmit power and k-th user's message, respectively. The received signal at the k-th user is then given as

$$y_k = \mathbf{h}_k^{\mathrm{H}}\mathbf{x} + v_k = \sqrt{P_{\mathrm{Tx}}}\mathbf{h}_k^{\mathrm{H}}\mathbf{b} \sum_{k=1}^{K} \beta_k s_k + v_k, \quad (9)$$

where v_k is zero-mean complex Gaussian additive white noise with variance N_0.

With the received signal as in (9) in hand, each user first decodes messages of all weaker users (allocated with larger power) sequentially in the presence of stronger users' messages (allocated with smaller power). Those decoded messages are then subtracted from the received signal in (9), and each user decodes its own message treating the stronger users' messages as noise. This overall decoding process is known as successive interference cancellation (SIC), and k-th user decodes its own message after SIC with the following SINR:

$$\mathrm{SINR}_k = \frac{P_{\mathrm{Tx}}|\mathbf{h}_k^{\mathrm{H}}\mathbf{b}|^2\beta_k^2}{(1 - \delta_{k1})\, P_{\mathrm{Tx}} \sum\limits_{l=1}^{k-1} |\mathbf{h}_k^{\mathrm{H}}\mathbf{b}|^2\beta_l^2 + N_0}, \quad (10)$$

where δ_{k1} is the Kronecker delta function taking 1 if $k = 1$, and 0 otherwise. Assuming that Eves have powerful detection capability [6], [8], the most detrimental Eve decodes k-th user message with the SINR given as

$$\mathrm{SINR}_k^{\mathrm{E}} = \frac{P_{\mathrm{Tx}}\beta_k^2 g_{\mathrm{E}}}{(1 - \delta_{k1})\, P_{\mathrm{Tx}} \sum\limits_{l=1}^{k-1} \beta_l^2 g_{\mathrm{E}} + N_0^{\mathrm{E}}}, \quad (11)$$

where N_0^{E} is the associated noise variance.

Considering SINR in (10), the instantaneous rate at k-th user is given by $R_k^{\mathrm{NOMA}} = \log_2(1 + \mathrm{SINR}_k)$. Similarly, considering (11), the instantaneous rate at the most detrimental Eve for decoding the k-th user message is given as $R_{k,\mathrm{E}}^{\mathrm{NOMA}} = \log_2(1 + \mathrm{SINR}_k^{\mathrm{E}})$. The secrecy rate for k-th legitimate user can therefore be given as [8], [11]

$$C_k^{\mathrm{NOMA}} = \left[R_k^{\mathrm{NOMA}} - R_{k,\mathrm{E}}^{\mathrm{NOMA}}\right]^+, \quad (12)$$

where $[x]^+ = \max\{x, 0\}$. As (12) implies, the secrecy rates are always strictly positive [12].

Assuming that $\overline{R}_k$ denotes desired secrecy rate for the user $k \in \mathcal{N}_{\mathrm{U}}$, we define the secrecy outage event occurring whenever $C_k^{\mathrm{NOMA}} < \overline{R}_k$ with the respective secrecy outage probability $\mathrm{P}_k^{\mathrm{o}} = \mathrm{P}\{C_k^{\mathrm{NOMA}} < \overline{R}_k\}$. As a result, outage sum secrecy rate with NOMA transmission can be given as

$$R^{\mathrm{NOMA}} = \sum_{k=1}^{K} (1 - \mathrm{P}_k^o)\overline{R}_k. \quad (13)$$

For performance comparison, we also consider outage sum secrecy rate with OMA transmission.

B. Shape Optimization for Protected Zone

In this section, we discuss optimization of the protected zone shape to enhance the secrecy rates while keeping its area (i.e., q) the same. We note that any particular subregion within the Eve region does not equally impair the achievable secrecy rates even if the subregion areas are the same and the Eves are equally capable. This is basically due to the varying effective channel gain between UAV-BS and Eve with different subregions, which is a function of not only the distance but also the *relative angle* (i.e., angle offset from the beamforming direction) associated with each Eve.

Considering (12), the subregion involving the most detrimental Eve has the largest impact on the secrecy rates. Hence, instead of choosing the subregions arbitrarily to form the protected zone, it is more meaningful to include (i.e., *protect*) subregions which result in better effective channel gain for potential eavesdroppers, and hence is likely to involve the most detrimental Eve.

As we will show in Section IV-A, the location distribution of the most detrimental Eve depends also on the hovering altitude of UAV-BS. In particular, the most detrimental Eve is likely to be present in a subregion where $\Delta_{\mathrm{E}} \geq \Delta$ and $L_{\mathrm{E}} \leq L_2$, which is represented by "Protected Zone II" in Fig. 2, when the altitude is low. In contrast, the region including the most detrimental Eve becomes closer to "Protected Zone I" of Fig. 2 with $\Delta_{\mathrm{E}} \leq \Delta$ and $L_{\mathrm{E}} \geq L_2$ when the altitude is high. We therefore conclude that the shape of the protected zone should be optimized taking into account the UAV-BS hovering altitude. Hence, at a particular altitude and for a given q, the optimal shape of the protected zone can be identified as

$$\Delta_{\mathrm{E}}^{*},\, L_{\mathrm{E}}^{*} = \underset{\Delta_{\mathrm{E}},\, L_{\mathrm{E}}}{\operatorname{argmax}}\; R^{\mathrm{NOMA}} \tag{14}$$

$$\text{s.t. } \Delta_{\mathrm{E}}^{\min} \leq \Delta_{\mathrm{E}} \leq \Delta_{\mathrm{E}}^{\max},$$

$$L_{\mathrm{E}} \text{ is computed by (3)−(5),}$$

where R^{NOMA} is given in (13).

IV. Numerical Results

In this section, we present numerical results to show the importance of shape optimization of the protected zone and its impact on the achievable sum secrecy rates with varying UAV-BS hovering altitudes. Considering Fig. 1, we assume that $L_2 = 100$ m, $L_1 = 25$ m, $L_{\mathrm{E}}^{\max} = 1.5L_2$ m, $\Delta = 0.02$ rad $(1.145°)$, $\Delta_{\mathrm{E}}^{\max} = 2\Delta$, $\bar{\theta} = 0°$, and $M = 100$. User distribution is based on HPPP with $\lambda = 1$, and user target secrecy rates are $\overline{R}_j = 4$ bits per channel use (BPCU) and $\overline{R}_i = 1$ BPCU, respectively. The power allocation ratios are $\beta_j^2 = 0.25$ and $\beta_i^2 = 0.75$ while $P_{\mathrm{Tx}} = 10$ dBm and $N_0 = -35$ dBm. We assume two user NOMA transmission with $j = 1$ and $i = 20$ after ordering users with respect to their effective channel gains. The path-loss model is assumed to be $\mathrm{PL}(\sqrt{d_k^2 + h^2}) = 1 + \left(\sqrt{d_k^2 + h^2}\right)^{\gamma}$ with $\gamma = 2$ [4], [10], and the UAV-BS altitude is $h \in [10, 150]$ m.

A. Location of the Most Detrimental Eavesdropper

We present the angle and distance distributions of the location of the most detrimental Eve in Fig. 3 and Fig. 4, respectively, for two different altitudes of $h = \{10, 100\}$ m, and HPPP densities of $\lambda_{\mathrm{E}} = \{0.1, 1\}$. In Fig. 3, we observe that the most detrimental Eve is very likely to have a relative angle which is greater than $\frac{\Delta}{2}$ at a lower altitude of $h = 10$ m. In particular, relative angle of the most detrimental Eve exceeds $\frac{\Delta}{2}$ all the time for $\lambda_{\mathrm{E}} = 1$ while it drops to approximately 70% of the time for $\lambda_{\mathrm{E}} = 0.1$. When the altitude becomes higher (i.e., $h = 100$ m), the relative angle of most detrimental Eve becomes smaller than $\frac{\Delta}{2}$. In Fig. 4, we observe that the PL distance of the most detrimental Eve is smaller (greater) than 100 m at lower (higher) altitudes, i.e., $h = 10$ m ($h = 100$ m). We therefore conclude that *the most detrimental Eve tends to have larger relative angles and smaller PL distances at lower altitudes in comparison to those at higher altitudes.*

B. Impact of the Protected Zone Shape on Secrecy Rates

In Fig. 5, we depict the sum secrecy rates along with the protected zone angle (i.e., Δ_{E}) at altitudes of $h = \{10, 100\}$ m assuming $q = 0.2$. We observe that while the secrecy rates get maximized at $\Delta_{\mathrm{E}} \approx 1.7°\,(> \Delta)$ for $h = 10$ m, the optimal angle turns out to be $\Delta_{\mathrm{E}} \approx 0.7°\,(< \Delta)$ at $h = 100$ m. This observation is consistent with the discussion in Section IV-A in the sense that the most detrimental Eve has a relative angle greater (smaller) than $\frac{\Delta}{2}$ at low (high) altitudes.

Similarly, Fig. 6 presents the secrecy rates along with the protected zone distance (i.e., L_{E}) for the same settings as of Fig. 5. We observe that while the optimal distance maximizing the secrecy rates is $L_{\mathrm{E}} \approx 110$ m at $h = 10$ m, it turns out to be $L_{\mathrm{E}} \approx 145$ m at $h = 100$ m. As before, this observation also nicely agrees with our discussions in Section IV-A regarding the distance distribution of the most detrimental Eve. This shows the importance of optimizing the protected zone shape at different hovering altitudes to maximize sum secrecy rates.

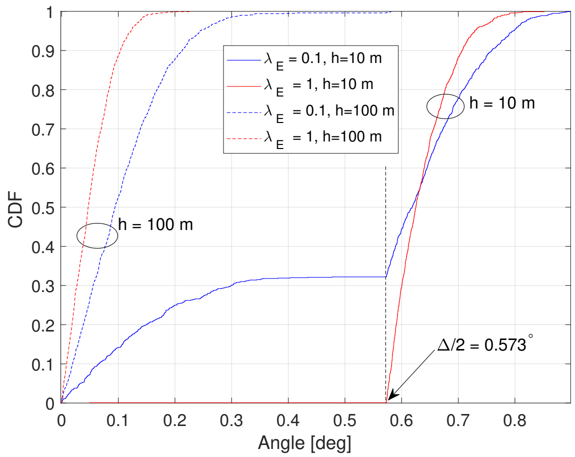


Fig. 3: Angle distribution of the most detrimental eavesdropper.

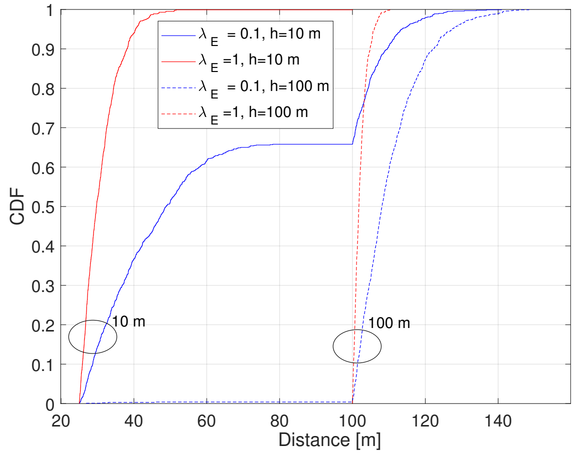


Fig. 4: Distance distribution of the most detrimental eavesdropper.

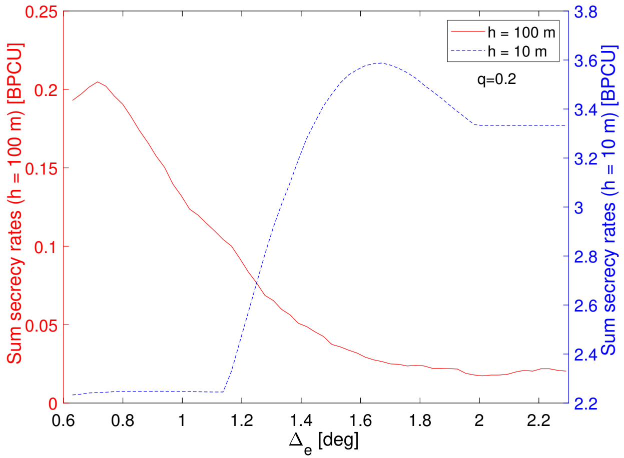


Fig. 5: Sum secrecy rates of NOMA along with the protected zone angle (i.e., Δ_{E}) for $h = \{10, 100\}$ m, $q = 0.2$, and $\lambda_{\mathrm{E}} = 0.1$.

C. Secrecy Rates Variation with Altitude

In Fig. 7, we present sum secrecy rates of NOMA and OMA transmission along with varying altitude of $h \in [10, 150]$ m and for different protected zone sizes (i.e., $q \in \{0, 0.2, 0.5\}$).

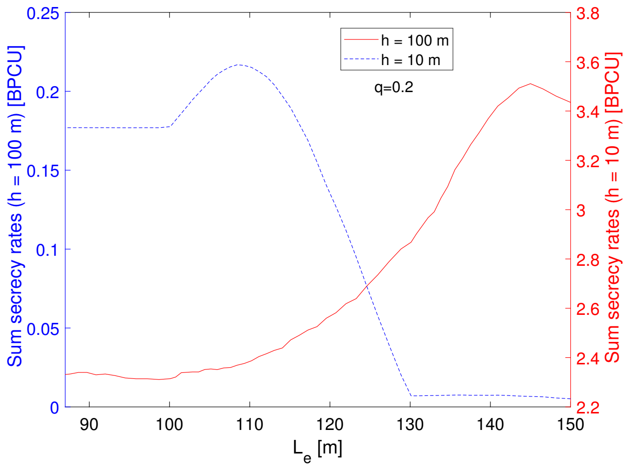


Fig. 6: Sum secrecy rates of NOMA along with the protected zone distance (i.e., L_{E}) for $h = \{10, 100\}$ m, $q = 0.2$, and $\lambda_{\mathrm{E}} = 0.1$.

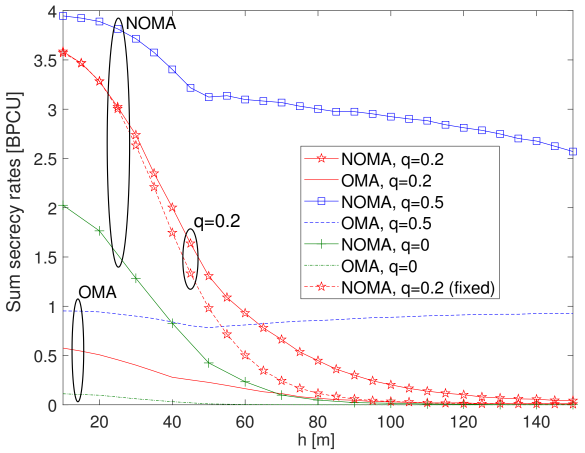
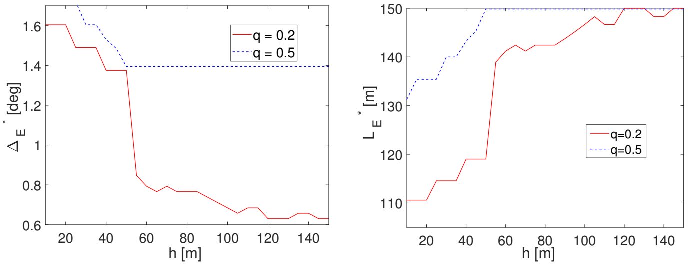


Fig. 7: Sum secrecy rates for NOMA and OMA along with UAV-BS hovering altitude, where $q \in \{0, 0.2, 0.5\}$, and $\lambda_{\mathrm{E}} = 0.1$.

For a nonzero protected zone (i.e., $q \neq 0$), considering shape optimization as discussed in Section III-B, sum secrecy rates are identified. In addition, Fig. 7 also captures sum secrecy rate variation with $q = 0.2$ for a fixed shape (optimal shape at $h = 10$ m). As can be observed, the fixed protected zone shape yields sum secrecy rates comparable to that of optimized protected zone shape only around $h = 10$ m and performs worse at all the other altitudes. Further, we observe that the secrecy rates improve if large portion of the Eve region can be covered by the protected zone (i.e., q increases). Based on the target sum secrecy rate and the operational altitude, the smallest q can also be determined. By this way, the desired secrecy rates can be achieved optimally by designating less area as the protected zone which would relieve the burden of clearing any unnecessary region free from Eves. Note also that the secrecy rates associated with NOMA is much larger than those of OMA especially at lower altitudes.

In Fig. 8, variation of the optimal shape of the protected zone is captured for $q = 0.2, 0.5$. In particular, Fig. 8a shows the optimal angle, Δ_{E}^* variation whereas Fig. 8b depicts optimal distance L_{E}^* variation with UAV-BS hovering altitude. As can be observed from Fig. 8, Δ_{E}^* decreases with altitude (see Fig. 8a) while L_{E}^* increases with altitude (see Fig. 8b). This observation aligns nicely with the discussion in Section IV-A which tells us that at lower altitudes the most detrimental Eve tends to have a larger relative angle and smaller distance whereas at higher altitudes this is vice versa.



(a) Optimal angle, Δ_{E}^*.

(b) Optimal distance, L_{E}^*.

Fig. 8: Δ_{E}^* and L_{E}^* variation with varying UAV-BS hovering altitudes, Here $q = 0.2, 0.5$.

V. Concluding Remarks

In this paper, we investigate the secrecy rates of UAV based mmWave communication network considering NOMA transmission. In particular, we consider *protected zone* approach to enhance the secrecy rates. Towards this end, we first investigate the distribution of the location of the most detrimental Eve which impairs secrecy rates the most. We then consider the protected zone which is free from any Eve, and the associated optimal shape of it to enhance the secrecy performance. We show that the optimal shape of the protected zone should cover the most detrimental Eve. In addition, we also show that the optimal shape highly relies on the UAV-BS hovering altitude such that the protected zone should be wider (narrower) in angle and shorter (longer) in distance at lower (higher) altitudes.

References

[1] AT&T, "Flying COW connects Puerto Rico," Nov. 2017. [Online]. Available: http://about.att.com/inside_connections_blog/flying_cow_puertori

[2] BBC, "Drones to the rescue," May 2018. [Online]. Available: http://www.bbc.com/news/business-43906846

[3] N. Rupasinghe, Y. Yapici, I. Guvenc, and Y. Kakishima, "Non-orthogonal multiple access for mmWave drone networks with limited feedback," *IEEE Trans. Commun.*, pp. 1–1, 2018.

[4] ——, "Comparison of limited feedback schemes for noma transmission in mmwave drone networks," in *IEEE Int. Workshop on Sig. Process. Adv. in Wireless Commun. (SPAWC)*, June 2018, pp. 1–5.

[5] S. Jeong, O. Simeone, and J. Kang, "Mobile edge computing via a UAV-Mounted Cloudlet: Optimization of bit allocation and path planning," *IEEE Trans. Vehic. Technol.*, vol. PP, no. 99, pp. 1–1, 2017.

[6] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1802–1814, Nov. 2013.

[7] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "Phy layer security based on protected zone and artificial noise," *IEEE Sig. Process. Lett.*, vol. 20, no. 5, pp. 487–490, May 2013.

[8] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.

[9] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts*, pp. 1–1, 2018.

[10] Z. Ding, P. Fan, and H. V. Poor, "Random beamforming in millimeter-wave NOMA networks," *IEEE Access*, no. 99, pp. 1–1, 2017.

[11] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[12] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of tas/mrc with antenna correlation," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 254–259, Jan. 2013.