Physical Layer Security in UAV-based Networks

-Capstone Project-

Project Report

Didar Amangeldiyev

Nazarbayev University
Department of Electrical and Computer Engineering
School of Engineering and Digital Sciences

This project report was created on Overleaf editing platform using LaTeX. All the figures were drawn using draw.io online software tool.

NAZARBAYEV UNIVERSITY

Electrical and Computer Engineering
Nazarbayev University
http://www.nu.edu.kz

Title:
Physical Layer Security in UAV-based Networks

Project Period:
Fall Semester 2020

Participant(s):
Didar Amangeldiyev

Supervisor(s):
Dr. Galymzhan Nauryzbayev

Copies: 1

Page Numbers: 13

Date of Completion:
December 3, 2020

Abstract:

This Capstone Project is intended to design a security measure for unmanned aerial vehicle (UAV) based systems with a physical layer approach. During the project, two different methods will be introduced. The first technique considers a multiuser communications scenario where a terrestrial base station (BS) serves multiple authorized UAVs simultaneously. To improve the secrecy rates, which are compromised by the unauthorized UAVs present near the legitimate ones, we adopt the protected zone approach which ensures any unauthorized UAV is away by at least a certain distance from any legitimate UAV. The other one examines the scenario of transmission between the source and destination through UAVs. We propose UAV selection mechanism to choose the UAV with the best capability for transmitting data, while unselected UAVs will jam the eavesdropper to considerably improve the secrecy and performance of system.

Contents

Preface

The application of UAVs, an aircraft without a human pilot on board and a type of unmanned vehicle, is envisioned as one of the key technologies for next-generation wireless networks.Their extraordinary features, such as compactness, speed, embedded with the newest technologies, and most essential drivability without pilots, cause upsurge interest in both military and civil applications. In these latter days, with the UAV technology being thoroughly studied, I also intend to research this sphere extensively to leave my impact in the digital world. It is my passion to not only find out, but to develop tools to improve the security of UAV-based technologies for future generation.

Nazarbayev University, December 3, 2020

Didar Amangeldiyev
<didar,amangeldiyev@nu.edu.kz>

Chapter 1

Introduction

For unmanned aerial vehicle (UAV) enabled systems, we consider communication scenarios where at least one UAV is involved during its functioning [1]. Security aspect of UAV-based systems is one of the primary obstacles for the UAV technology, becoming a constituent element of wireless communication [2]. Since, it is crucial to protect classified information from unintended users in order to securely transmit a data without corrupting or eavesdropping it [3]. Extensive investigation on researches shows that physical layer security (PLS) is an effective security technique in UAV networks, which is more efficient than traditional encryption method [4]. According to [5], the optimization of UAV's trajectory and power has been regarded to maximize the average secrecy rate in the communication between a UAV above ground and a node on the ground in the presence of a potential ground-based eavesdropper. In [6], the physical layer feature associated with deep learning and artificial noise was applied to generate a secure real-time communication method for UAV networks. A source-based jamming (SBJ) scheme without any external jammers was exploited in [7] to examine the secrecy outage performance of transmissions between multiple UAVs which are operated in full-duplex mode. Corresponding to [8], the average secrecy capacity of UAV-to-UAV system was considered, where the legitimate UAV receiver and eavesdropper UAVs are spatially randomly located in the coverage of nearby space. The authors in [9] introduced the mobile relaying technique in the wire-tap channel to enhance PLS of UAV-based wireless networks by optimizing the transmission in four-node channel setup, where the objective was to maximize the secrecy rate of the network. According to [10], UAV equipped with an air-to-ground friendly jammer was examined, with the purpose of improving the PLS of wireless communications between the legitimate transmitter and receiver pair for unknown eavesdropper location.

In this work, two different system models will be presented to improve the secrecy rates of UAV enabled systems in terms of PLS. The first system model is

based on [11], where a swarm of authorized UAVs are simultaneously served by a terrestrial base station (BS). The scenario also includes a group of unauthorized UAVs, which are trying to eavesdrop the confidential information. In this model, to enhance the security of the system, we apply a protected zone approach, where each authorized UAV will start transmission only if no unauthorized UAVs are detected from a certain distance around the friendly UAV. For the second system model, we consider the scheme with a single source-destination pair without direct link. However, instead of using relay nodes as in [12], we will connect source-destination pair with authorized UAVs in the presence of a malicious attacker. To improve the secrecy rate of the system, we will select the best capable authorized UAV for the transmission, whereas other UAVs will act as a jammer to interrupt the eavesdropping of the attacker.

The next section of the paper will provide more detailed information about the proposed system models. Then, the numerical results for the system with protected zone approach will be analyzed and discussed. While, the performance of the other model will be further investigated in Capstone Project 2. At last, the conclusion will be made with final remarks.

Chapter 2

Methodology

2.1 Protect zone approach

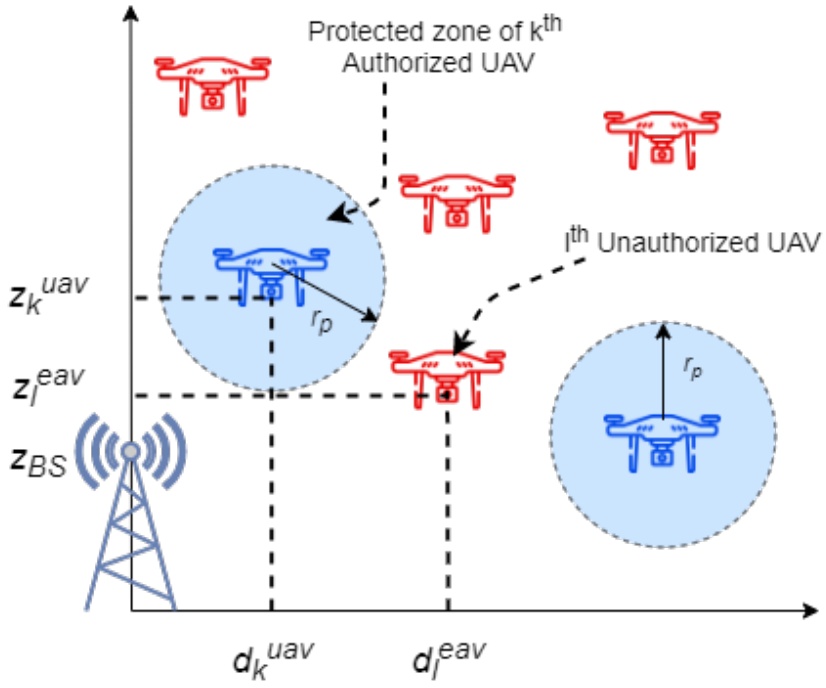

Figure 2.1: Illustrated system model of UAV swarm with protect zone approach

This communication environment involves K authorized single-antenna UAVs, where K_u out of them will serve terrestrial BS consisted from an array of M antennas. The scenario also includes malicious K_e unauthorized UAVs, which are trying to compromise the transmission between legitimate UAVs. As demonstrated

in Figure 2.1, all UAVs are randomly allocated in three-dimensional (3D) space, where the horizontal distance d_k^t and altitude z_k^t of kth UAV are uniformly distributed between $[d_{min}\ d_{max}]$ and $[z_{min}\ z_{max}]$ respectively. Whereas $t = \{uav, eav\}$ corresponds to authorized and unauthorized UAVs.

According to the system model to formulate the protected zone approach, at most K_u UAVs will be selected out of K authorized UAVs that follows the condition

$$(d_k^u - d_l^e)^2 + (z_k^u - z_l^e)^2 \geq r_p^2, \tag{2.1}$$

where (d_k^u, z_k^u) and (d_l^e, z_l^e) are coordinates of authorized UAV and the closest unauthorized UAV respectively, meanwhile r_p is the radius of the protected zone. In other words, we can state that, if every unauthorized UAVs are at least r_p distance from a certain authorized UAV, only then the given authorized UAV will be part of serving K_u UAVs.

The channels between UAVs and BS are described in terms of line-of-sight (LoS)/non-LOS (NLoS) model [13], where the probability of having LoS and NLos links is equal to

$$P_{LoS}(\theta_k^t) = \frac{1}{1 + aexp(-b(\theta_k^t - a))}, \qquad P_{NLoS}(\theta_k^t) = 1 - P_{LoS}(\theta_k^t). \tag{2.2}$$

In (2.2), a, b parameters define the impact of the environment on the communication quality (e.g., suburban, urban, and dense urban [8]). Meanwhile, θ_k^t equivalent to elevation angle of kth UAV corresponding to the z_{BS}, the height of BS and can be expressed as the following:

$$\theta_k^t = arctan(\frac{z_k^t - z_{BS}}{d_k^t}), \tag{2.3}$$

where t equals to $\{uav, eav\}$.

Due to obstacles such as buildings, natural mountains, large-scale fading occurs in air-to-ground channels as a combination of path loss and shadowing. Thus, by assuming the coefficient of large-scale fading depends on LoS/NLoS conditions, we can express it in dB scale as

$$\beta_k^{t,s} = 10log\big((d_k^t)^2 + (z_k^t - z_{BS})^2\big) + 20log\left(\frac{4\pi f_c}{c}\right) + \eta^s, \tag{2.4}$$

where s represents $\{LoS, NLoS\}$ and η^s indicates the excess path loss that is happening due to the scattering of the obstacles in the transmission scenario. In the interim, f_c is the operating frequency and c is the speed of light.

On the other hand, small-scale fading is portrayed in the form of a spatially correlated Rician fading model. Eventually, the air-to-ground channel implicating both the large- and small-scale fading is represented as below

$$h_k^{t,s} = \sqrt{\beta_k^{t,s}}\left(\sqrt{\frac{\kappa}{1+\kappa}}\bar{h}_k^{t,s} + \sqrt{\frac{1}{1+\kappa}}(R_k^{t,s})^{\frac{1}{2}}\tilde{h}_k^{t,s}\right), \tag{2.5}$$

where κ is Rician K-factor, which is equal to power ratio between LoS and NLoS components, and $R_k^{t,s}$ displays the spatial correlation of the NLoS component. Furthermore, by assuming the structure of BS antenna in a uniform linear array (ULA) and the LoS component is using location of the UAV in 3D space as a basis, we can demonstrate the formulation for the deterministic LoS component $\bar{h}_k^{t,s}$ as

$$\bar{h}_k^{t,s} = [1 \quad e^{-j\pi\cos\theta_k} \quad ... \quad e^{-j\pi(M-1)\cos\theta_k}]. \tag{2.6}$$

In contrast, the deterministic NLoS component $\tilde{h}_k^{t,s}$ is equivalent to the complex standard normal distribution:

$$\tilde{h}_k^{t,s} \sim \mathcal{CN}(0_M, I_M). \tag{2.7}$$

By taking into consideration the probabilities of LoS/NLoS link, the composite channel can be expressed as follows

$$h_k^t = h_k^{t,LoS}P_{LoS}(\theta_k^t) + h_k^{t,NLoS}P_{NLoS}(\theta_k^t). \tag{2.8}$$

In order to formulate the secrecy rate of the system, at first we assume kth authorized UAV will receive a signal with the magnitude

$$y_k = \underbrace{(h_k^{uav})^H w_k p_k s_k}_{desired\ signal} + \underbrace{\sum_{i\neq k}(h_i^{uav})^H w_i p_i s_i}_{multiuser\ interference} + n_k, \tag{2.9}$$

where the values of w, p, s, and n corresponds to the precoder, power allocation coefficient, unit-energy signal, and a circularly symmetric complex Gaussian observation noise with zero mean and N_0 variance respectively. Considering the aggregate channel matrix of the network is $H = [h_1\ h_2\ ...\ h_k]^H$, we could estimate the magnitude of w coefficient via this equation:

$$W = [w_1\ w_2\ ...\ w_k]^H = (HH^H + \frac{K_u}{SNR})^{-1}H, \tag{2.10}$$

where W is the aggregate precoder matrix. Meanwhile, to calculate the value of power allocation coefficient p, we can use transmit power P_{TX} which is equal to multiplication of transmit signal-to-noise ratio (SNR) and N_0 variance: $P_{TX} = N_0\,SNR$:

$$p_k = \sqrt{\frac{P_{TX}}{K_u}}||w_k||^{-1}. \tag{2.11}$$

Then, the instantaneous communication rate and signal-to-interference-plus-noise ratio (SINR) of kth authorized UAV are expressed as below

$$R_k^{uav} = log(1 + SINR_k^{uav}), \qquad SINR_k^{uav} = \frac{p_k^2 |(h_k^{uav})^H w_k|^2}{\sum_{i \neq k} p_i^2 |(h_i^{uav})^H w_i| + N_0}. \tag{2.12}$$

Likewise, the instantaneous communication rate and SINR of lth unauthorized UAV that aiming to compromise the kth authorized UAV equals to

$$R_{k \to l}^{eav} = log(1 + SINR_{k \to l}^{eav}), \qquad SINR_{k \to l}^{eav} = \frac{p_k^2 |(h_l^{eav})^H w_k|^2}{\sum_{i \neq k} p_i^2 |(h_l^{eav})^H w_i| + N_0}. \tag{2.13}$$

Finally, to compute the instantaneous secrecy rate, we can use the following equation:

$$R_k^{sec} = \left[R_k^{uav} \quad max\, R_{k \to l}^{eav} \right]^+, \tag{2.14}$$

where $[x]^+ = max\{0,\ x\}$. It is important to note that, to calculate the secrecy rate of each authorized UAV, we considered the worst possible conditions, therefore we selected the most detrimental unauthorized UAV for the formulation.

2.2 UAV selection approach

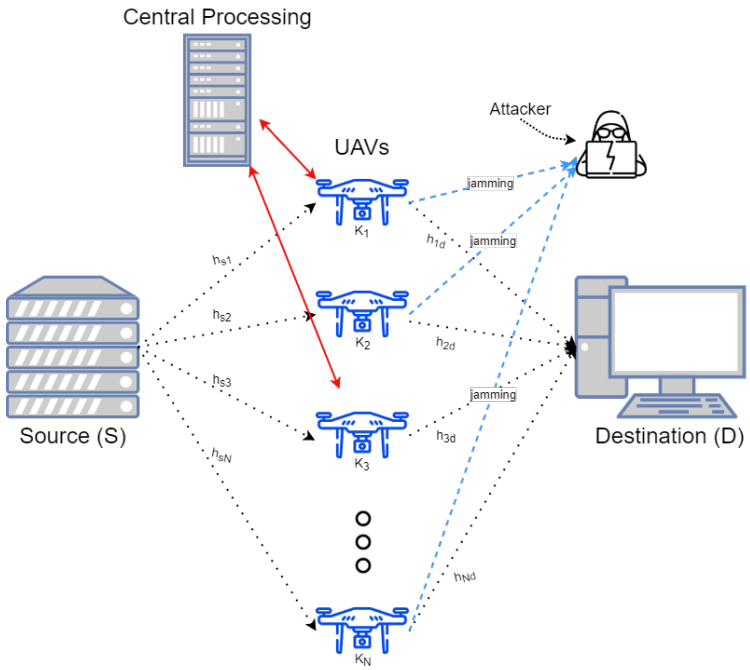

Figure 2.2: Illustrated system model of UAV network with UAV selection approach

This system model considers two-hop decode-and-forward (DF) wireless communication scenario, where the transmission of information between the source (S) node and the destination (D) node with no direct link commits by resorting to single UAV (K_{i*}) chosen from N available UAVs (FIgure 2.2). Where h_{si} and h_{id} represent source-to-UAV ($S \rightarrow K_i$) and UAV-to-destination ($K_i \rightarrow D$) links , while distance of $S \rightarrow K_i$ and $K_i \rightarrow D$ equals to d_{si} and d_{id}, respectively. In the meantime, the central processor will collect information about h_{si} links and then will choose an appropriate UAV for transmitting the data. In addition, the communication environment also includes a malicious eavesdropper, targeting to intercept the transmission. Therefore, to enhance security of the network, we can utilize UAVs except the selected one (K_{i*}) to jam the eavesdropper to deteriorate its connection quality.

Nevertheless, further research on the formulation, determining UAV selection algorithm, etc. will be conducted in Capstone Project 2.

Chapter 3

Results and Discussions

3.1 Results

In this section of the project, simulation results will be presented to demonstrate the performance of the protected zone approach. Simulation process will be based on extensive Monte Carlo simulation with 10^3 iterations. Note that we are considering a suburban environment for our communication scenario and the appropriate parameters will be based on [13]. Additionally, we assume no spatial correlation for the air-to-ground channels, thus $R_k^{t,s}$ will be equal to I_M. Other simulation parameters are displayed in the table below.

Table 3.1: Parameters for simulation

Parameters	Values
Number of authorized UAVs (K)	$10 - 150$
Number of unauthorized UAVs (K_e)	$10 - 150$
Number of actively serving authorized UAVs (K_u)	10
Number of transmit antennas (M)	64
Minimal and maximum horizontal distance of UAVs (d_{min}, d_{max})	(0, 100) m
Minimal and maximum altitude of UAVs (z_{min}, z_{max})	(10, 120) m
Height of BS (z_{BS})	25 m
Operating frequency (f_c)	4.2 GHz
Speed of light (c)	$3 * 10^8$ m/s
Rician K-Factor (κ)	10 dB
Environmental parameters (a, b)	(9.61, 0.28)
Excess path loss (η^{LoS}, η^{NLoS})	(1, 20) dB
SNR (SNR)	10 dB
Variance (N_0)	1

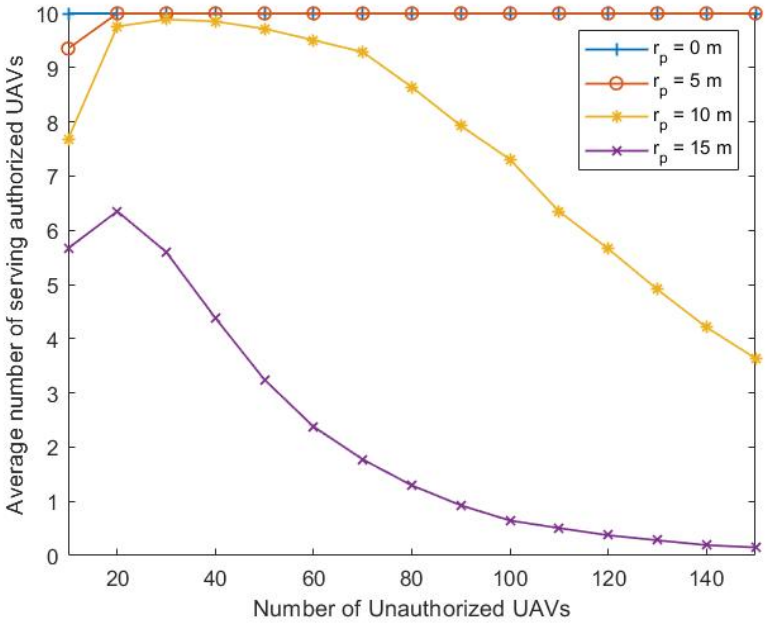

Figure 3.1: Average number of actively serving authorized UAVs versus total number of unauthorized UAVs (K_e)

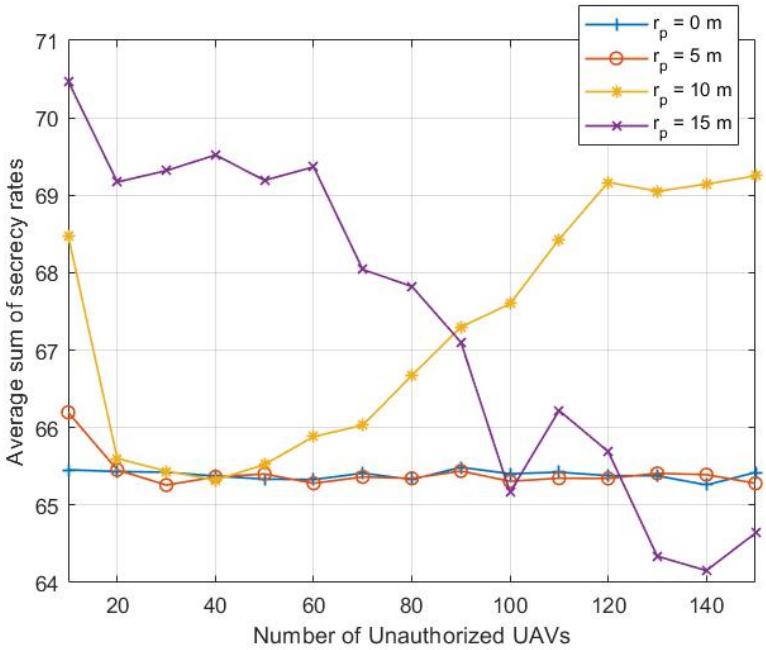

Figure 3.2: Average sum of secrecy rates versus total number of unauthorized UAVs (K_e)

3.2 Discussions

In order to estimate the impact of the technique, we considered $r_p \in \{0, 5, 10, 15\}$ m for the values of protected zone radius, where $r_p = 0$ m corresponds to the scenario without protected zone approach.

By observing Figure 3.1, it is possible to identify the average number of authorized UAVs (K_u) that are participating in multi-user transmission depending on r_p. The magnitude of K_u is around 10 when $r_p \in \{0, 5\}$ m, which is significantly larger if we compare to K_u of $r_p \in \{10, 15\}$ m. Since by increasing r_p, we are decreasing the area of location, where the authorized UAV is capable to be involved in multiuser transmission. Especially, in the scenario, when we have $K_e = 150$ unauthorized UAVs and $r_p = 15$ m, it is extremely hard to find the spot where the authorized UAV satisfies the condition in (2.1). Therefore, we have almost no actively serving authorized UAV for this scenario.

Meanwhile, Figure 3.2 depicts dependency of the average sum secrecy rate of the system model on K_e. We detect the monotonic behavior of secrecy rate for $r_p \in \{0, 5\}$ m, which can be explained by the same behavior of K_u in Figure 3.1. Whereas, the sum secrecy rate for $r_p = 10$ m always reveals better performance than the sum secrecy rate for $r_p \in \{0, 5\}$ m. However, the peak sum of secrecy rates is demonstrated when r_p is equal to 15 m, and only if we consider less than 80 unauthorized UAVs for testing. In the opposite case, the sum of secrecy rates is sharply declining, thus $r_p = 10$ m will be a more superior alternative for the $K_e > 80$ range according to Figure 3.2.

Note that a higher secrecy rate defines a more safeguarded communication system from eavesdroppers. Thereby, the simulation results indicate enhanced security of the system compared to the model without protected zone. Certainly, applying any value for r_p does not denote an improvement of secrecy level. For instance, Figure 3.2 clearly displays $r_p = 5$ m as a bad example for the implementation of the protected zone approach. Hence, it is crucial to find the ideal value for r_p by judging the specific parameters of the communication scenario to reach the most optimal secrecy rate.

Chapter 4

Conclusion

This project is intended to design a system model of UAV-based wireless network with corresponding PLS communication techniques to improve the security of system. Throughout the project, two different techniques with system models have been presented. The first method with protected zone approach displayed good results with enhanced secrecy rates, but with the remark of choosing the appropriate radius of the protected zone. The second technique was based on UAV selection approach. Further investigation of the formulation and integration of the two techniques together will be examined in Capstone Project 2.

Bibliography

[1] J. Hamamreh, “Physical Layer Security Against Eavesdropping in The Internet of Drones (IoD) Based Communication Systems”, *figshare*, April 2019, doi:10.6084/m9.figshare.8362385.v1.

[2] H. Wang, X. Zhang and J. Jiang, "UAV-Involved Wireless Physical-Layer Secure Communications: Overview and Research Directions", in *IEEE Wireless Communications*, vol. 26, no. 5, pp. 32-39, October 2019, doi:10.1109/MWC.001.1900045.

[3] Q. Wu, W. Mei, and R. Zhang, “Safeguarding Wireless Network with UAVs: A Physical Layer Security Perspective”, *arXiv e-prints*, 2019, arXiv:1902.02472.

[4] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu and Z. Zhong, "Physical Layer Security in UAV Systems: Challenges and Opportunities", in *IEEE Wireless Communications*, vol. 26, no. 5, pp. 40-47, October 2019, doi:10.1109/MWC.001.1900028.

[5] G. Zhang, Q. Wu, M. Cui and R. Zhang, "Securing UAV Communications via Joint Trajectory and Power Control", in *IEEE Transactions on Wireless Communications*, vol. 18, no. 2, pp. 1376-1389, Feb. 2019, doi:10.1109/TWC.2019.2892461.

[6] B. Khadem and S. Mohebalizadeh, “Efficient UAV Physical Layer Security based on Deep Learning and Artificial Noise”, *arXiv e-prints*, 2020, arXiv:2004.01343.

[7] T. Nuradha, K. Hemachandra, T. Samarasinghe, and S. Atapattu, “Physical-Layer Security for Untrusted UAV-Assisted Full-Duplex Wireless Networks”, *arXiv e-prints*, 2019, arXiv:1909.06600.

[8] J. Ye, C. Zhang, H. Lei, G. Pan and Z. Ding, "Secure UAV-to-UAV Systems With Spatially Random UAVs", in *IEEE Wireless Communications Letters*, vol. 8, no. 2, pp. 564-567, April 2019, doi:10.1109/LWC.2018.2879842.

[9] N. Rupasinghe, Y. Yapıcı, İ. Güvenç, H. Dai and A. Bhuyan, "Enhancing Physical Layer Security for NOMA Transmission in mmWave Drone Networks",

2018 52nd Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, USA, 2018, pp. 729-733, doi:10.1109/ACSSC.2018.8645326.

[10] Y. Zhou et al., "Improving Physical Layer Security via a UAV Friendly Jammer for Unknown Eavesdropper Location," in *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 11280-11284, Nov. 2018, doi:10.1109/TVT.2018.2868944.

[11] Y. Yapici, İ. Güvenç, H. Dai and A. Bhuyan, "Physical Layer Security for UAV Swarm Communications via Protected Zone", *2019 Resilience Week (RWS)*, San Antonio, TX, USA, 2019, pp. 174-177, doi:10.1109/RWS47064.2019.8971823.

[12] M. Majid Butt, G. Nauryzbayev, and N. Marchetti, "On Maximizing Information Reliability in Wireless Powered Cooperative Networks", *arXiv e-prints*, 2020, arXiv:2002.11110.

[13] A. Al-Hourani, S. Kandeepan and S. Lardner, "Optimal LAP Altitude for Maximum Coverage", in *IEEE Wireless Communications Letters*, vol. 3, no. 6, pp. 569-572, Dec. 2014, doi:10.1109/LWC.2014.2342736.