Secure UAV Communication Networks over 5G

Bin Li, Zesong Fei, Yan Zhang, and Mohsen Guizani

Abstract

Wireless communications can leverage UAVs to provide ubiquitous connectivity to different device types. Recently, integrating UAVs into a macro cell network is drawing unprecedented interest for supplementing terrestrial cellular networks. Compared with communications with fixed infrastructure, a UAV has salient attributes, such as easy-to-deploy, higher capacity due to dominant LoS communication links, and additional design degree-of-freedom with the controlled mobility. While UAV communication offers numerous benefits, it also faces security challenges due to the broadcasting nature of the wireless medium. Thus, information security is one of the fundamental requirements. In this article, we first consider two application cases of UAVs (i.e., a UAV as a flying base station and a UAV as an aerial node) in conjunction with safeguarding the exchange of confidential messages. Then, we demonstrate physical layer security mechanisms via two case studies to ensure security, and numerically show superior performance gains. Finally, we shed light on new opportunities in the emerging network architecture that can serve as a guide for future research directions.

Introduction

As aerial communication platforms, unmanned aerial vehicles (UAVs) or drones have emerged as an innovative trend in providing ubiquitous connectivity from the sky, especially for temporary user equipments (UEs) or over disaster areas. Along with miniaturization and continuous cost reduction, low-altitude UAVs are in general more swift and flexible for deployment and reconfiguration due to fully controllable UAV mobility, and are likely to have strong short-distance Line-of-Sight (LoS) communication links with ground UEs [1, 2]. In this regard, a wide range of applications have become available, such as precision farming, infrastructure inspection, and monitoring of disaster areas. In addition, more projects on employing aerial platforms for broadband connectivity to remote parts have also been established, including the Google Loon Project [3] and Facebook Drone Project [4], to name two.

With the forthcoming 5G era, densely populated UEs are thirsty for broadband wireless communications, and network operators are expected to support diverse services with high wireless data demands such as multimedia streaming and video downloads [5, 6]. The unrelenting increase in mobile traffic volumes imposes an unacceptable burden on the operators in terms of increased capital expenditure and operating costs. An intuitive option to offload cellular traffic is to deploy small cell networks [7]. However, in unexpected or temporary events, the deployment of terrestrial infrastructures is challenging since mobile environments are sophisticated, volatile, and heterogeneous. One potential solution resorts to the usability of *aerial access points* for supporting massive dynamic connections. The success of UAV communications benefits from the portable transceiver functionality and advanced signal processing techniques that realize omnipresent coverage and establish wireless connections. Figure 1 depicts a UAV-assisted heterogeneous network architecture, aiming to construct a flexible network with improved agility and resilience.

Since the UAV-mounted network constitutes a dynamic and hierarchical network, it is challenging to provide security provisioning. This is because the transmit information of UAV communications is easily wiretapped by ground unauthorized parties, hereafter called the *eavesdroppers* [8, 9]. One of the common ways to protect the wireless communication against unauthorized access by eavesdroppers relies on upper-layer cryptographic mechanisms. Nonetheless, this is very hard to accomplish due to key management and the high computational complexity in the emerging network architecture. As a compelling remedy, physical-layer (PHY-layer) security leverages the intrinsic characteristics of wireless channels such as noise, interference, and fading, to degrade the received signal qualities at the malicious eavesdroppers, and realizes keyless secure transmission via signal design and signal processing methods.

In this article, we introduce PHY-layer security to UAV communication networks for surmounting the challenging information leakage problem due to potential eavesdropping. Such a UAV network aims to achieve secrecy communications in the exchange of information. We first lay out the system models of the envisioned networks facing security services. After that, two exemple case studies are provided to examine the secrecy performance by using PHY-layer security approaches. In the final two sections, we discuss open issues for future research efforts and conclude this article.

Security Service Scenarios Facing UAVs

Thanks to the versatility and high mobility of UAVs, low-altitude UAVs are extensively used in diverse fields for different applications and purposes. On one hand, UAVs are employed as

Bin Li is with Beijing Institute of Technology, and also with Nanjing University of Information Science and Technology; Zesong Fei (corresponding author) is with Beijing Institute of Technology; Yan Zhang is with the University of Oslo, and also with Simula Metropolitan Center for Digital Engineering; Mohsen Guizani is with Qatar University.

Digital Object Identifier:
10.1109/MWC.2019.1800458

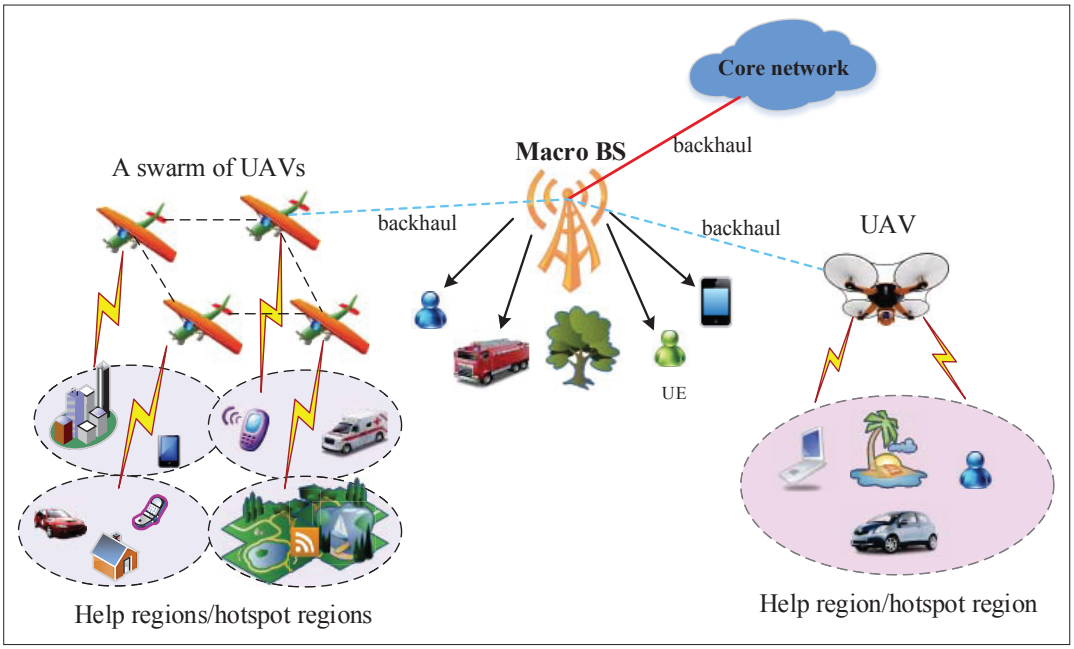

FIGURE 1. An exemplary scenario of UAV-based wireless networks, where each UAV is equipped with wireless transceivers allowing them to communicate with ground UEs and also with other UAVs. In particular, a swarm of UAVs construct a flying ad hoc network in which they establish UAV-to-UAV communication to determine the deployment results.

aerial communication platforms (e.g., fly base stations (BSs) or mobile relays) to provide/enhanced communication services to ground targets. On the other hand, UAVs can be used as aerial UEs (i.e., UAV-UEs) to enable a multitude of applications ranging from cargo delivery to surveillance. In summary, UAV communications have been an active area of research from two different perspectives:

- *Operator's perspective*: UAVs are appealing to reduce cellular traffic load providing low-cost solutions.
- *Mobile device's standpoint*: UAVs are also compelling to provide high data rates of the complementary networks.

In effect, UAVs construct highly dynamic network topologies and time-varying channel states. These can carry with them huge risks of privacy loss and security issues in the information exchange of UAVs and ground communication networks. Figure 2 shows a UAV network architecture substituting or assisting the terrestrial cellular networks in the presence of potential eavesdroppers. To take full advantage of the benefits of UAVs, the main objective is how to make this communication process as safe as possible. In this context, PHY-layer security approaches have been developed from the signal processing perspective which are attracting attention from research communities. Recently, various potential solutions have been proposed for the no-UAV networks to obtain a higher level of security in the physical layer, including multiple-antenna arrays, relay selection, and friendly jamming. In the following, we envision three typical UAV service scenarios facing malicious eavesdropping, for which the multiple antenna technique, relay selection, and friendly jamming are accordingly utilized to strengthen a secure transmission.

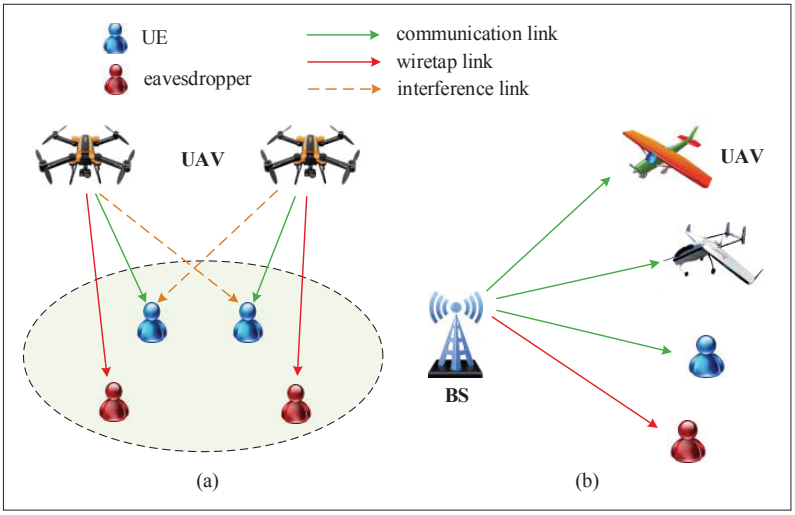

FIGURE 2. Illustration of two typical UAV network applications with security services (i.e., in the presence of ground eavesdroppers): a) UAVs as flying BSs; b) UAVs as aerial mobile UEs.

UAVs as Flying BSs

In the wake of natural disasters (such as earthquakes, tsunamis or snow storms), the existing communication infrastructure may be damaged or even destroyed, and the required emergency data traffic leads to the congestion and overload of nearby macrocells. In such network breakdowns, a promising solution is to dynamically deploy low-altitude UAVs as flying BSs (i.e., UAV-BSs) to reinforce the communication infrastructure to compensate for cell overload or site outage, thereby forming an *aerial small cell*. In this case, wireless communications consisting of UAV-to-UE, UAV-to-ground control station, and UAV-to-UAV in an ad-hoc manner may happen.

Compared to the stationary ground BSs, UAV-

As the key enabler of Internet of Things (IoT), UAVs can naturally function as aerial mobile users, that is, UAV-UEs, coexisting with ground UEs as a part of network components, where cellular-connected UAV communication is able to provide seamless wireless communication for UAVs.

BSs can greatly boost wireless capacity and extend the coverage of wireless networks at temporary events or overloaded hotspot areas (such as sports competitions, parades and gatherings), since the LoS communication links can be established between UAVs and the served ground UEs. On the other hand, UAV-BSs form a moving aerial cell network to track the mobility patterns of ground UEs, which is more robust to decrease the intermittence of connectivity. Further, this can be extended to the deployment of multiple UAV-BSs to maximize the coverage area to serve a large group of ground UEs. A network comprising multiple UAV-BSs is fully autonomous. The coordination among UAV-BSs has opened a new paradigm for extending the viability of a single UAV from a standalone aerial platform to a network constituent of next-generation wireless networks.

In parallel with the widespread deployment of UAV-BS networks, there is an increasing concern about privacy issues. From the communication level, wireless security is a major problem where eavesdropping refers to intentionally listening to the privacy information emanating from a source, which directly threatens the wide deployment of UAV-BSs. As illustrated in Fig. 2a, a swarm of UAV-BSs are deployed in a large area to serve a collection of ground UEs in coexistence with multiple external eavesdroppers. Benefiting from the spatial degree-of-freedom of multiple-antenna technologies, it is in nature to configure multiple antennas in the UAV-BSs, which provides an opportunity for UAV-BSs to transmit airborne beamforming against eavesdropping. Note that multiple-antenna technology can be practically implemented at UAV systems by properly designing the antenna separation [10]. Existing works have shown that transmit beamforming designs for multiple-antenna transmitters can effectively improve the secrecy performance of wiretap channels. To better prevent information leakage, artificial noise can also be injected along with the source signal to dramatically impair the received Signal-to-Interference-plus-Noise Ratio (SINR) at the eavesdroppers.

UAVs as Aerial UEs

As the key enabler of Internet of Things (IoT), UAVs can naturally function as aerial mobile users, that is, UAV-UEs, coexisting with ground UEs as a part of network components, where *cellular-connected UAV communication* is able to provide seamless wireless communication for UAVs. This has been shown through field trials via taking advantage of WiFi and long term evolution technologies [11]. UAV-UEs usually have their own missions for a number of compelling IoT applications, especially in air cargo transport services (e.g., Amazon Prime Air and Google Wing Project). Compared to traditional ground-based package delivery, UAV delivery has distinct advantages:

- Speeds up over land transportation (such as using trucks or cars) since UAVs are not subjected to road traffic jams.
- Reduces resource usage in terms of manpower and energy.
- Can access hard-to-reach areas.

UAV delivery depends critically on having reliable and safe wireless connectivity between UAVs and ground BSs, particularly when the UAVs require beyond LoS control. Nevertheless, the ability of UAV-UEs to establish LoS connectivity to cellular BSs is tit-for-tat. On one hand, UAV-UEs enable high-speed data access as they can continuously fly in any direction. On the other hand, the deployment of UAV-UEs can lead to substantial interference to ground UEs when performing their missions. To this end, a widescale deployment of UAV-UEs is only possible if the interference management challenge is addressed. It is common knowledge that interference has a harmful impact on wireless networks. However, it was reported that interference can potentially be a valuable resource that can be harnessed to achieve wireless security, because interference from UAV-UEs can affect both legitimate ground UEs and eavesdroppers simultaneously. If carefully designed, it could be adapted to garner an enhanced secure transmission for legitimate receivers.

As illustrated in Fig. 2b, a cellular network serves both aerial UEs (i.e., UAV-UEs) and ground UEs with a potential eavesdropper that attempts to intercept the message intended for legitimate ground UEs. To increase secure transmission, a cost-effective strategy is to employ cooperation between the ground BS and UAVs, that is, part of the UAVs act as friendly jammers to weaken the quality of the wiretap channel and therefore improve the secrecy rate. Specifically, a UAV acting as a mobile jammer can dynamically adjust its own location as close as possible to ground eavesdroppers and jam them by emitting the interference signal; meanwhile, the characteristic of strong LoS link is a beneficial phenomenon with less impairment by terrestrial fading and shadowing. However, using the case of a UAV-jammer to defend against eavesdropping will face a number of new challenges, for instance, how to select the most favorable jamming UAV and how to efficiently optimize the jamming power and UAV location from the selected jamming UAV so as to maximize the interference to the eavesdroppers while having a minimal effect on the legitimate UEs.

State of the Art

Many efforts related to PHY-layer security in UAV communication networks are being carried out for improving secrecy performance. Specifically, the authors of [8] consider the issue of PHY-layer security in the presence of an eavesdropper deployed in a UAV communication system. By exploiting the mobility of the UAV, the secrecy rate of legitimate nodes is enhanced. The authors of [9] study the problem of secure transmission in a UAV-aided relaying network, where the trajectory and transmit power are jointly optimized to maximize the secrecy rate. The authors of [12] examine the secrecy performance of a randomly deployed UAV-enabled mmWave communication network over Nakagami-m fading channels. In [13], the concept of the intercept probability security region is proposed as a new security indicator when prior knowledge of the eavesdropper is unknown. The model of a dual-UAV-aided secure communication system is developed in [14], where one of the UAVs in the area adjusts its trajectory to jam multiple ground eavesdroppers to protect the communications of the desired nodes. Considering multiple UAV-eaves-

droppers in a UAV swarm communication system, [15] analyzed the secrecy outage performance and derived the exact expression of secrecy outage probability (SOP). However, we note that the secrecy energy efficiency (SEE) in the UAV communication system has not been explored, and limited research has been dedicated to the security enhancement methods.

To show the proclaimed prospects and benefits of PHY-layer techniques in securing UAV communication networks, in the following two sections two case studies will be presented and discussed with simulation results.

Case Study I: PHY-Layer Security in UAV-BS Networks

In this section, we consider a more general scenario where multiple UAV-BSs provide wireless access to a large number of ground UEs within the coverage area, while a group of eavesdroppers are trying to eavesdrop the information delivery from UAV-BSs to legitimate UEs, as shown in Fig. 2a. We assume each UAV is configured with N_t antennas, and the legitimate UEs and malicious eavesdroppers each have a single antenna. The location sets of UAV-BSs, legitimate UEs, and eavesdroppers are randomly dispersed following independent homogeneous Poisson point processes with densities λ_T, λ_u, and λ_e. Herein, we restrict attention to the rotary-wing UAVs within a limited height H that hover over the targeted area. We define the 3D Cartesian coordinates of the UAV j and UE i as $(x_j^{uav}, y_j^{uav}, H)$ and $(x_i, y_i, 0)$; the distance between UAV j and UE i is

$$d_{ij} = \sqrt{(x_j^{uav} - x_i)^2 + (y_j^{uav} - y_i)^2 + H^2}.$$

Without loss of generality, the UAV-BSs and ground UEs operate on the same frequency band, thus the co-channel interference to the ground UEs is triggered. Transmit beamforming is employed at the UAV-BSs to mitigate the resulting interference. Generally speaking, the flight duration and secrecy performance of a UAV-aided system are fundamentally limited by the on-board battery power, which is practically finite due to the UAV's size and weight constraints. The total energy of the UAV is mainly consumed by the wireless communication part, compared with the propulsion and computational energy. The energy of a UAV expended by communication includes two components, namely the hover and transition energies needed for its movement and the power consumed for the communication to deliver the data. In this sense, enhancing energy efficiency (EE) of the UAV communication for maximizing the information bits per unit of energy is of paramount importance. On the other hand, when the eavesdroppers have a better channel than the access threshold, the secrecy outage occurs without ensuring the security of these messages. Herein, SOP is defined as the probability that the perfect secrecy of the message cannot be guaranteed, is adopted as the performance measure of security.

For practical applications, the security and green requirements of UAV systems are two key primary indicators, which are in great demand. Motivated by this consideration, SEE is defined as the ratio of the achievable secrecy rate to the total power consumption of the UAV system (bits/Joule) to reflect the joint impact of security and EE. In particular, the SEE of this considered network is given by SEE = R_{sec}/P_{tot}, where R_{sec} represents the achieved average secrecy rate at a legitimate UE and P_{tot} denotes the total energy consumption of a UAV in each channel.

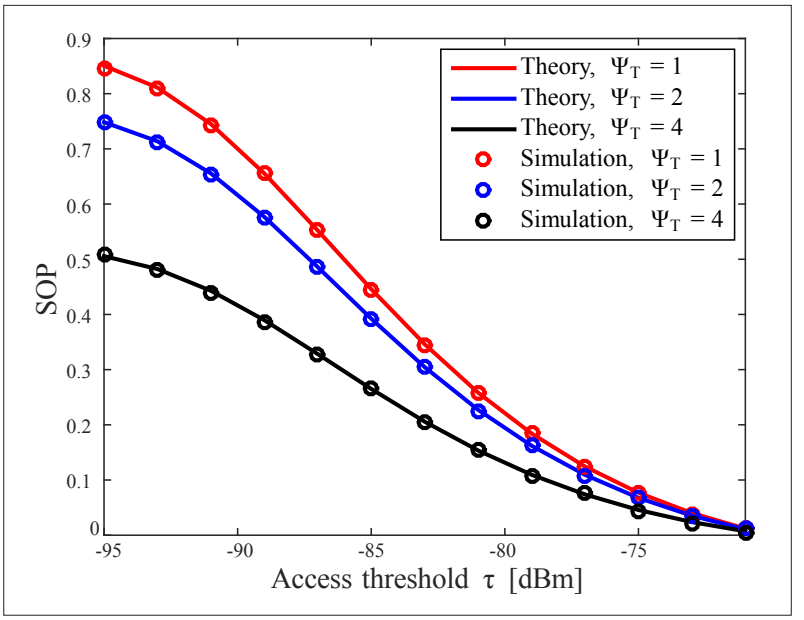

FIGURE 3. SOP versus τ.

Illustrative Results

In this subsection, numerical results are first provided to examine the SOP for a UAV-aided network, and the validity of the theoretical analysis is verified by the Monte Carlo simulation results. Then, the impact of parameters on the SEE is examined. The experimental setup is a dense urban environment, where $N_t = 4$, $\lambda_u = \lambda_e = 10^{-6}\text{m}^{-2}$, and flying altitude $H = 500$m. All UAV-BSs transmit at the same power value P_T for simplicity and the number of dispatched UAVs is Ψ_T. For a secure mobile association scheme, the served UAV-BS broadcasts data only when the truncated highest average received signal power at a legitimate UE is larger than a predetermined access threshold τ.

Figure 3 illustrates the SOP for different levels of Ψ_T with transmit power of UAV-BS $P_T = 5$dB. Intuitively, the simulation points are highly consistent with the theoretical curves, thereby demonstrating the correctness of our analysis. It is also observed that the SOP decreases with Ψ_T, which is mainly due to the fact that Ψ_T not only increases the interference received by eavesdroppers, but also increases the interference received by legitimate UEs. Furthermore, the SOP performance over different τ is also shown in Fig. 3. Obviously, the SOP degrades with increasing τ, which implies that the predetermined access threshold can affect the security. Figure 4 shows the set of achievable SEE for different values of τ and P_T. We note that the SEE is a function of τ and P_T, thus the optimal value of SEE can be obtained by properly designing them. In Fig. 4, the SEE reveals a maximum value for a given network with the optimal pair of $(\tau, P_T) = (-95\text{dBm}, 28\text{dBm})$, which is marked in this

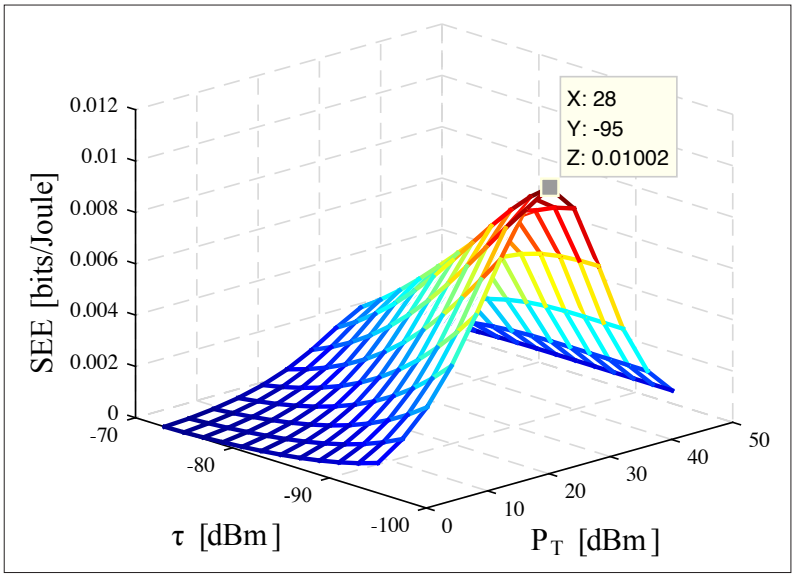

FIGURE 4. SEE versus τ and P_T.

figure. In this respect, we conclude that the network supported by the multiple-antenna UAV-BSs is the SEE-optimal architecture.

Case Study II: PHY-Layer Security in UAV-Relay Networks

In practical communication networks, the radio paths between the remote ground UEs and the ground BS are often obstructed. To cope with this urgent situation, the controllable UAVs are utilized to relay the data of the ground BS to the destination UEs, whereas the data information may be leaked to the malicious eavesdroppers during the transmission. Typically, UAV-relays can adopt the amplify-and-forward (AF) protocol for transmission. In a cooperative dual-hop network, an opportunistic relay selection technique has been shown as a simple and effective method to enhance the secrecy performance due to the increased diversity gain.

Artificial Noise-Aided UAV-Relay Scheme

We focus on a configuration where a ground source node communicates with the legitimate destination nodes, assisted by multiple rotary-wing UAV-relays operating in a half-duplex mode. The relaying signals may be overheard by K independent eavesdroppers. The direct links are unavailable between source node and destination nodes due to the severe blockage or far distance, and the source-relay selection strategy with anti-eavesdropping capabilities is considered in this cooperative dual-hop network. Specifically, the source node transmits its information to UAV-relays in the first phase; the UAV-relay R_j is selected among available relays and then delivers the source signal to destination nodes in the second phase in an AF manner. On this basis, each destination node receives the transmitted signal by the best relay path in the second phase, that is, the received signal with the highest instantaneous SINR at each destination node is selected.

For the purpose of exposition, we assume that the source node, each destination node and the eavesdropper are equipped with a single antenna having limited signal processing capabilities and low-power budgets. By contrast, the j-th UAV-relay R_j is equipped with N_t antennas, the channels between source node and R_j as well as between R_j and destination node are dominated by the LoS links. We model the movement state of the target UAV-relay with a general linear time invariant model due to the continuous navigation, which moves at a constant altitude and is calculated as

$$x(t+1) = \mathbf{A}x(t) + \mathbf{n}(t),$$

where $x(t)$ is the state vector of the target UAV movement process at time slot t, which can be determined by the location, speed, and acceleration of the target UAV in Cartesian coordinates. $\mathbf{A}$ denotes the state transition matrix of the target that explains how the current state of the system influences the next step state, and $\mathbf{n}(t)$ stands for the target UAV movement process noise.

To further counteract the eavesdropping attack, we will present an achievable scheme for the eavesdroppers' channel, whose key idea is to inject artificial noise at Rj for deteriorating the received SINRs of the eavesdroppers. To analyze the effectiveness of artificial noise on security, we focus on the secrecy rate, which is defined as the difference between the main and the maximum eavesdropper's channel capacities, that is, $R_{sec} = (1/2)[C_d - \max_{k\in\mathcal{K}} C_{e,k}]^+$, where the factor 1/2 accounts for the fact that a pair of orthogonal time slots are required for the whole transmission in a two-hop AF transmission, C_d and $C_{e,k}$ correspond to the information capacities at destination node and the k-th eavesdropper.

Illustrative Results

In this subsection, we provide simulation results for evaluating the secrecy performance of the proposed design scheme in a UAV-aided relaying network. We consider the scenario that the number of antennas at the UAV is set to $N_t = 6$ and the other communication nodes have a single antenna. In the experimental setup, the air-to-ground channel model follows path loss and small-scale fast fading effects. The UAV-relays fly at a fixed altitude $H = 150$m above ground. We set the transmit power of the source node at 10dB, the path loss coefficient of LoS at 1dB, the path loss coefficient of NLoS at 10dB, and the carrier frequency at 2GHz. For the purpose of comparison, we consider three schemes as the benchmarks, that is, without artificial noise scheme (denoted as "w/o AN"), isotropic artificial noise scheme (denoted as "Isotropic AN"), and traditional ground-relay scheme.

Figure 5 examines the secrecy rate of different schemes versus the number of Eves (i.e., K). As shown in this figure, one can observe that the secrecy rate decreases with K, which is caused by the increasing diversity gain for the information eavesdropping with more eavesdroppers, leading to a poorer secrecy performance. Compared to the "w/o AN" and "Isotropic AN" schemes, a considerable gain is observed for the UAV-relay network with optimized artificial noise. In other words, the optimally designed jamming signal can make the legitimate network much more secure. In addition, the proposed scheme performs better

than the static ground-relay scheme in terms of improving the secrecy rate, because the UAV-relay offers a new degree-of-freedom for a secure performance enhancement via intelligent trajectory design.

Future Research Directions

The research on UAV-aided communications is still in its infancy. A UAV, as a flying platform, could further contribute to different services for diverse user devices. We point out several open security issues as further research directions.

Cyber-Physical Security: The UAV system may face wiretap as well as malicious attacks due to the open links and dynamic topologies that blanket out a mission-critical area by intentional jamming/disruption. In practice, the UAV system is more vulnerable to control signal spoofing attacks by transmitting false signals or even to be taken control by adversaries through successfully launching cyber attacks. This is a tremendous threat to the safety of UAV systems. To avoid malicious modification, there is a need for a more in-depth study of the security issues across all the protocol layers.

Secure UAV-to-UAV Communications: For a significantly wide area, a swarm of UAVs construct a multi-hop network to provide communication services to ground UEs, each of which has a trajectory. However, due to the high-speed mobility and the need to maintain close communication links with ground UEs, the link connection with the neighboring UAVs is disconnected frequently. Therefore, new unmanned aircraft traffic management systems may be necessary to control the flight of the UAVs for cooperative path planning and collision avoidance of multiple UAVs. Besides, the security of UAV-to-UAV systems is more complicated as opposed to UAV-to-ground systems, since the receivers (i.e., legitimate UAVs) or eavesdroppers (i.e., illegitimate UAVs) operate in all directions of 3D space.

Aerial Blockchain: With the widespread adoption of UAVs in IoT for performing commissions, the data integrity between UAVs and GCS during data collection, as well as the communication security during data transmission, are critical concerns. To prevent privacy leakage of UAV communication and ensure the integrity of collected data from UAVs, blockchain technology, as a decentralized solution, is expected to be a new paradigm to securely and adaptively maintain the privacy preferences for blockchain-based UAV systems, which is called "UAVChain."

Conclusions

This article introduced PHY-layer security into UAV communication networks, which has become an important concept that leveraged the physical characteristics of wireless channels to achieve secure transmissions. Two typical applications of UAVs were presented where PHY-layer security played a crucial role. Furthermore, PHY-layer security schemes in both the UAV-BS network and the UAV-relay network were studied. Illustrative results indicated that the secrecy performance of the proposed schemes can be substantially improved in terms of SEE and secrecy rate. Finally, we shed light on the open issues that need further research efforts.

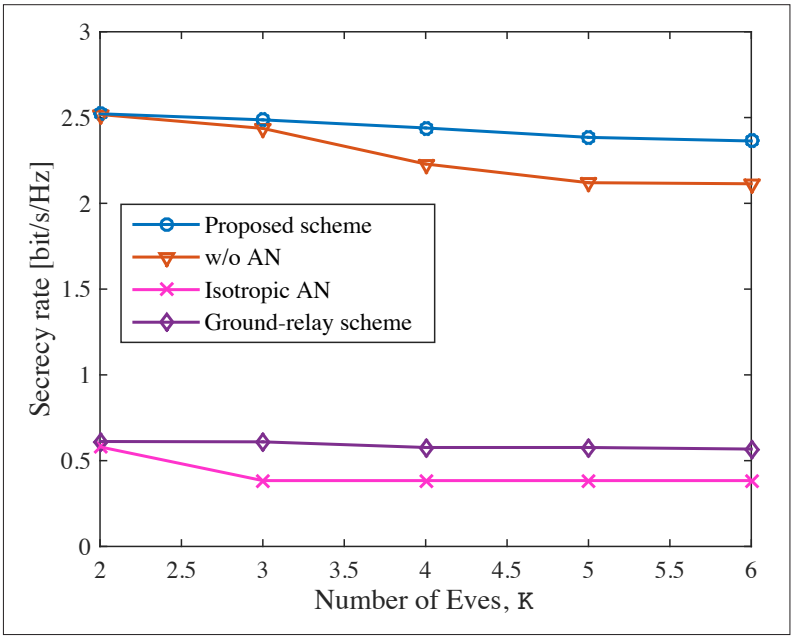

FIGURE 5. Secrecy rate versus number of Eves with P_{th} = 10 dB.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China under Grant 61871032; in part by the Beijing Natural Science Foundation under Grant L182038; in part by the Chinese Ministry of Education-China Mobile Communication Corporation Research Fund under Grant MCM20170101; and in part by the scholarship from the China Scholarship Council [2017] 3019. This work has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Sklodowska-Curie grant agreement No 824019 and "Supported by Sichuan Science and Technology Program"(2019YFH0033).

References

[1] M. Mozaffari *et al.*, "Mobile Unmanned Aerial Vehicles (UAVs) for Energy-Efficient Internet of Things Communications," *IEEE Trans. Wireless Commun.*, vol. 16, no. 11, Nov. 2017, pp. 7574–89.
[2] M. Bouaziz, A. Rachedi, and A. Belghith, "EKF-MRPL: Advanced Mobility Support Routing Protocol for Internet of Mobile Things: Movement Prediction Approach," *Future Generation Computer Systems*, vol. 93, Apr. 2019, pp. 822–32.
[3] "Project Loon," available: https://www.google.com/loon.
[4] M. Zuckerberg, "Connecting the World from the Sky," Facebook, Cambridge, MA, USA, Tech. Rep., 2014.
[5] A. A. Khan, M. H. Rehmani, and A. Rachedi, "Cognitive-Radio-Based Internet of Things: Applications, Architectures, Spectrum Related Functionalities, and Future Research Directions," *IEEE Wireless Commun.*, vol. 24, no. 3, June 2017, pp. 17–25.
[6] D. Bendouda, A. Rachedi, and H. Haffaf, "Programmable Architecture Based on Software Defined Network for Internet of Things: Connected Dominated Sets Approach," *Future Generation Computer Systems*, vol. 80, Mar. 2018, pp. 188–97.
[7] C.-C. Lin, D.-J. Deng, and S.-Y. Jhong, "Energy-Efficient Placement and Sleep Control of Relay Nodes in Heterogeneous Small Cell Networks," *Wireless Networks*, vol. 23, no. 2, Feb. 2017, pp. 593–608.
[8] G. Zhang *et al.*, "Securing UAV Communications via Trajectory Optimization," *Proc. IEEE GLOBECOM*, Singapore, 2017, pp. 1–6.
[9] Q. Wang *et al.*, "Joint Power and Trajectory Design for Physical-Layer Secrecy in the UAV-Aided Mobile Relaying System," *IEEE Access*, vol. 6, 2018, pp. 62 849–55.

[10] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless Communications with Unmanned Aerial Vehicles: Opportunities and Challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, May 2016, pp. 36–42.
[11] B. V. D. Bergh, A. Chiumento, and S. Pollin, "LTE in the Sky: Trading Off Propagation Benefits with Interference Costs for Aerial Nodes," *IEEE Commun. Mag.*, vol. 54, no. 5, May 2016, pp. 44–50.
[12] Y. Zhu, G. Zheng, and M. Fitch, "Secrecy Rate Analysis of UAV-Enabled mmWave Networks Using Matérn Hardcore Point Processes," *IEEE JSAC*, vol. 36, no. 7, Jul. 2018, pp. 1397–1409.
[13] Y. Zhou *et al.*, "Improving Physical Layer Security via a UAV Friendly Jammer for Unknown Eavesdropper Location," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, Nov. 2018, pp. 11 280–84.
[14] Y. Cai *et al.*, "Dual-UAV Enabled Secure Communications: Joint Trajectory Design and User Scheduling," *IEEE JSAC*, vol. 36, no. 9, Sept. 2018, pp. 1972–85.
[15] H. Liu, S.-J. Yoo, and K. S. Kwak, "Opportunistic Relaying for Low-Altitude UAV Swarm Secure Communications with Multiple Eavesdroppers," *J. Communications and Networks*, vol. 20, no. 5, Oct. 2018, pp. 496–508.

Biographies

Bin Li (libin_sun@bit.edu.cn) is currently pursuing the Ph.D. degree at the School of Information and Electronics, Beijing Institute of Technology, Beijing, China. From 2013 to 2014, he was a research assistant at Hong Kong Polytechnic University, Hong Kong. From 2017 to 2018, he was a visiting student at the University of Oslo, Norway. In 2019, he is an associate professor with the School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, China. His research interests include physical-layer security, wireless cooperative networks, and UAV communications.

Zesong Fei [M'07, SM'16] (feizesong@bit.edu.cn) received the B.Eng. degree in electronic engineering from the Beijing Institute of Technology (BIT), China, in 1999, and the Ph.D. degree in electronic engineering from BIT, China, in 2004. He is currently a professor with the Research Institute of Communication Technology (RICT) of BIT. His main research interests include error control coding, physical-layer security, cooperative communications and networking, and quality of experience. He is a senior member of the Chinese Institute of Electronics and China Institute of Communications.

Yan Zhang [M'05, SM'10] (yanzhang@ieee.org) is a full professor at the University of Oslo. He is an editor of several IEEE publications, including *IEEE Communications Magazine*, *IEEE Network*, *IEEE Transactions on Green Communications and Networking*, *IEEE Communications Surveys & Tutorials*, and the *IEEE Internet of Things Journal*. His current research interests include next generation wireless networks leading to 5G and cyber physical systems. He is an IEEE VTS Distinguished Lecturer and a Fellow of IET. He received the "Highly Cited Researcher" award (Web of Science top 1 percent most cited worldwide) according to Clarivate Analytics.

Mohsen Guizani [S'85, M'89, SM'99, F'09] (mguizani@ieee.org) received the B.S. (with distinction) and M.S. degrees in electrical engineering, and the M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He is currently a professor with the Computer Science and Engineering Department at Qatar University, Qatar. He is an IEEE Fellow and a Senior Member of ACM.