Safeguarding Wireless Network with UAVs: A Physical Layer Security Perspective

Qingqing Wu, Weidong Mei, and Rui Zhang

Abstract

Integrating unmanned aerial vehicles (UAVs) into future wireless systems such as the fifth-generation cellular network is anticipated to bring significant benefits for both the UAV and telecommunication industries. Generally speaking, UAVs can be used as new aerial platforms in the cellular network to provide communication services for terrestrial users, or become new aerial users of the cellular network served by the terrestrial base stations. Due to their high altitude, UAVs usually have dominant line-of-sight channels with the ground nodes, which, however, pose new security challenges to future wireless networks with widely deployed UAVs. On one hand, UAV-ground communications are more prone than terrestrial communications to eavesdropping and jamming attacks by malicious nodes on the ground. On the other hand, compared to malicious ground nodes, malicious UAVs can launch more effective eavesdropping and jamming attacks to terrestrial communications. Motivated by the above, in this article, we aim to identify such new issues from a physical-layer security viewpoint and present novel solutions to tackle them efficiently. Numerical results are provided to validate their effectiveness, and promising directions for future research are also discussed.

Introduction

With flexible mobility and deployment, unmanned aerial vehicles (UAVs) or drones have found a plethora of new applications in recent years. Typical use cases of commercial UAVs include cargo delivery, surveillance and inspection, search and rescue, and aerial photography, among others. As projected by the Federal Aviation Administration (FAA), the UAV industry will generate more than US$82 billion for the U.S. economy alone and create more than 100,000 new jobs in the next decade. The prosperous global market of UAVs is also envisioned to bring new and valuable opportunities to the future wireless communication industry, such as the forthcoming fifth-generation (5G) cellular network. On one hand, to enable reliable communications for widely deployed UAVs in the future, a promising solution is to integrate UAVs into the future 5G cellular network as new aerial users served by terrestrial base stations (BSs). In fact, recent studies by the Third Generation Partnership Project (3GPP) have demonstrated the viability of supporting the basic communication requirements for UAVs with the existing cellular network [1]. On the other hand, with continuously miniaturized BSs/relays, it becomes more feasible to mount them on UAVs and make complementary aerial communication platforms in 5G cellular networks to provide or enhance the communication services for the terrestrial users [2].

However, the integration of UAVs into 5G also brings new challenges that need to be addressed. Compared to terrestrial wireless channels that in general suffer from severe path loss, shadowing, and multi-path fading, the high altitude of UAVs generally leads to more dominant line-of-sight (LoS) channels with the ground nodes. Although the strong LoS links can be exploited to improve the communication performance, they also cause severe interference to the terrestrial communications, and thus effective air-ground interference management techniques are needed [1]. Moreover, the unique LoS-dominant UAV-ground channel poses new security challenges to the future wireless network with various UAV applications, as shown in Fig. 1. Specifically, in Figs. 1a and 1b, the UAV is deployed as an aerial BS or relay that sends/forwards private messages to a legitimate ground node, respectively. However, the strong UAV-ground LoS links also enhance the reception quality of the terrestrial eavesdroppers. As a result, even a remote eavesdropper can take advantage of the LoS link to overhear the air-to-ground (A2G) communication clearly. Furthermore, in Fig. 1c and Fig. 1d, the UAV acts as a mobile hub to collect private data from terrestrial Internet of Things (IoT) devices such as sensors, or an aerial user that receives critical control signals from its serving ground BS. In such cases, a ground jammer can also exploit the strong ground-to-air (G2A) LoS links to launch more powerful jamming attacks to interfere with the UAV, thus significantly degrading its reception quality and even resulting in UAV communication failure. Therefore, compared to terrestrial communications, A2G and G2A communications are more susceptible to terrestrial eavesdropping and jamming, respectively. As such, how to effectively safeguard the legitimate UAV communications in the future wireless network is a new and challenging problem to resolve.

On the other hand, UAVs potentially may be a new security threat to the terrestrial cellular network if they are misused by unauthorized parties for malicious purposes. As shown in Fig. 2a, if the UAV is deployed as a malicious eavesdropper, it could more clearly overhear the terrestrial private communications between the ground BSs and their users even in a wide area as compared to the tra-

Digital Object Identifier:
10.1109/MWC.001.1900050

The authors are with the National University of Singapore.

1536-1284/19/$25.00 © 2019 IEEE

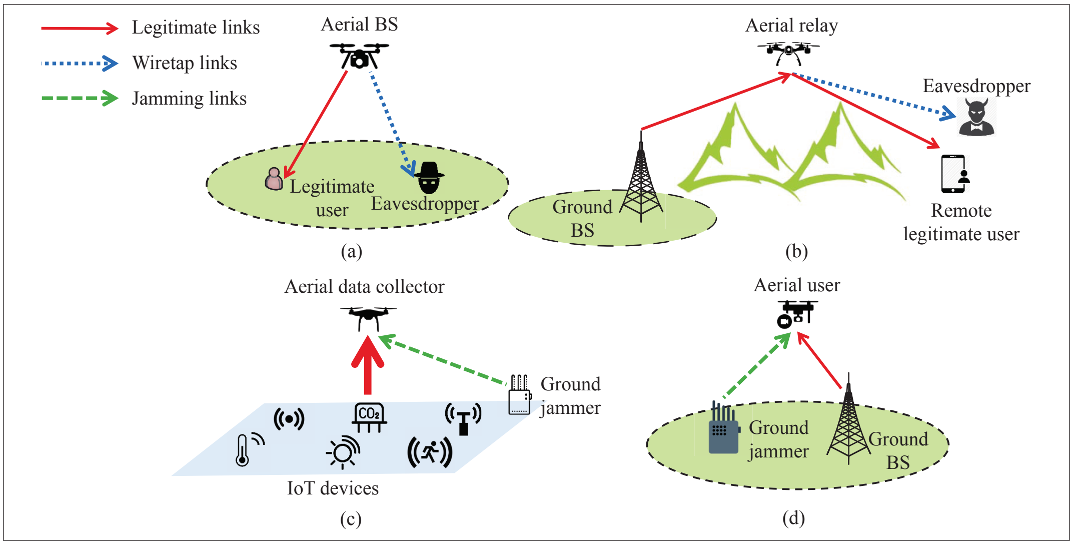


FIGURE 1. Eavesdropping and jamming attacks to legitimate UAV communications in a 5G wireless network.

For A2G communications where UAVs transmit confidential messages to their ground nodes, the received signal strength is strong over a large area on the ground due to the LoS-dominant channels, which makes the prevention of terrestrial eavesdropping highly difficult. Nonetheless, by exploiting the high altitude of UAVs and their high mobility in the 3D space, secure A2G communication may still be achievable.

ditional terrestrial eavesdroppers, due to the more LoS-dominant G2A links. Moreover, the UAV may also be used as a malicious jammer to disrupt both the uplink and downlink terrestrial communications in the cellular network, as shown in Fig. 2b. Its strong A2G links thus impose more severe as well as more widely spread interference to legitimate ground communications than conventional terrestrial jammers with the same jamming signal power. In addition, the malicious UAVs can leverage their high mobility to flexibly change locations so that they can keep track of their moving targets over time and thus overhear/jam their communications more effectively. In light of the above, another challenging security problem arises: how to efficiently protect the terrestrial communications against the powerful UAV eavesdropping/jamming attacks.

Considering the above two new UAV security issues in future wireless networks, this article aims to identify their key challenges and discuss promising solutions to tackle them, mainly from a physical-layer (PHY) design perspective. Note that PHY security has been extensively studied in the literature to combat malicious eavesdropping and/or jamming attacks in terrestrial communication networks (e.g., [3, 4, references therein]). Typical anti-eavesdropping techniques include artificial noise (AN), cooperative jamming, transmit beamforming, and others [5]; while direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) are two commonly used anti-jamming techniques at PHY [6]. However, such techniques mainly consider terrestrial nodes as legitimate or malicious users in the network and thus may be ineffective in dealing with the new and more challenging LoS-induced security issues with UAVs. As such, it is necessary to revisit the conventional techniques for UAV security and devise new solutions to safeguard future wireless networks more effectively.

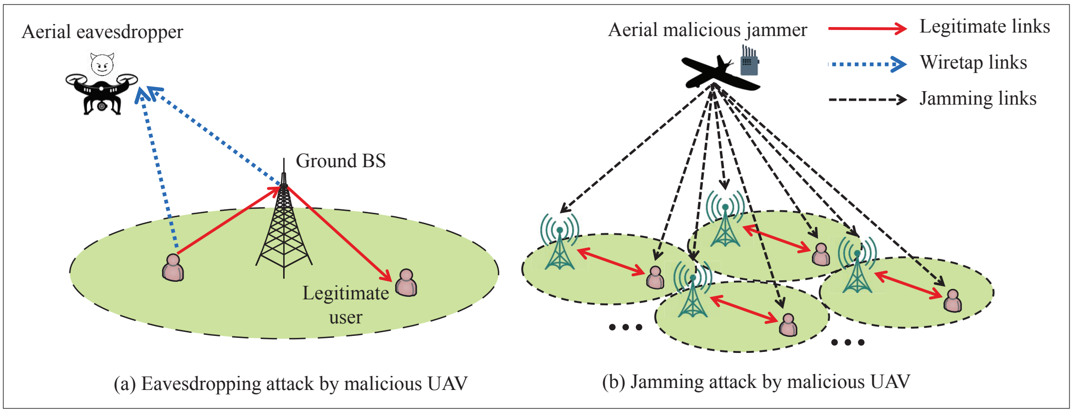
Securing Legitimate UAV Communications in Wireless Network

As compared to terrestrial communications, legitimate A2G/G2A communications are more susceptible to ground eavesdropping/jamming due to the LoS-dominant channels. In this section, we discuss promising countermeasures to improve UAV communication security and reliability.

Protecting A2G Communication from Terrestrial Eavesdropping

As shown in Figs. 1a and 1b, for A2G communications where UAVs transmit confidential messages to their ground nodes, the received signal strength is strong over a large area on the ground due to the LoS-dominant channels, which makes the prevention of terrestrial eavesdropping highly difficult. Nonetheless, by exploiting the high altitude of UAVs and their high mobility in the 3D space, secure A2G communication may still be achievable with the use of the following techniques.

UAV 3D Beamforming: Different from the traditional 2D beamforming (e.g., via linear array) at ground BSs, which controls the beam pattern only in the azimuth plane, 3D beamforming (e.g., via planar array) is able to adjust the beam pattern in both elevation and azimuth planes with more refined beam resolution, which thus makes it appealing in 5G applications (e.g., spatial multiplexing for communicating with multiple users at different altitudes by exploiting their widely separated elevation angles with the serving BS). As such, it can be leveraged to null the legitimate user's signal in the directions of the eavesdroppers more effectively. Furthermore, the dominant LoS A2G channel also makes transmit beamforming more efficient as compared to that in terrestrial channels with more complicated multi-path effects due to the rich scattering environment. As shown in Fig. 3a, even equipped with 3D beamforming capability, a ground BS may lack sufficiently separated elevation angles with the legitimate user and the eavesdropper due to its low altitude above the ground; as a result, it cannot avoid information leakage if the two nodes are located in the same direction from it, even though they have different horizontal distances from it. In contrast, a UAV transmitter at a much higher altitude can still exploit the ground nodes' different elevation angles (θ_1 and θ_2) with it to cancel the legitimate user's signal at the eavesdropper by, for example, zero-forcing (ZF)-based precoding. Furthermore, In contrast to legitimate ground receivers in A2G communications, legitimate UAV receivers in G2A communications are exposed in the sky and thus more vulnerable to jamming attacks by ground adversary nodes that send AN signals to interfere with the UAV so as to reduce its receive signal-to-interference-plus-noise ratio (SINR) for decoding.



(a) Eavesdropping attack by malicious UAV

(b) Jamming attack by malicious UAV

FIGURE 2. Eavesdropping and jamming attacks to a terrestrial wireless network by malicious UAV nodes.

3D beamforming can be jointly employed with transmitting AN to jam or interfere with the ground eavesdroppers and thereby achieve better security [7]. This further enhances the robustness of 3D beamforming/jamming by the UAV.

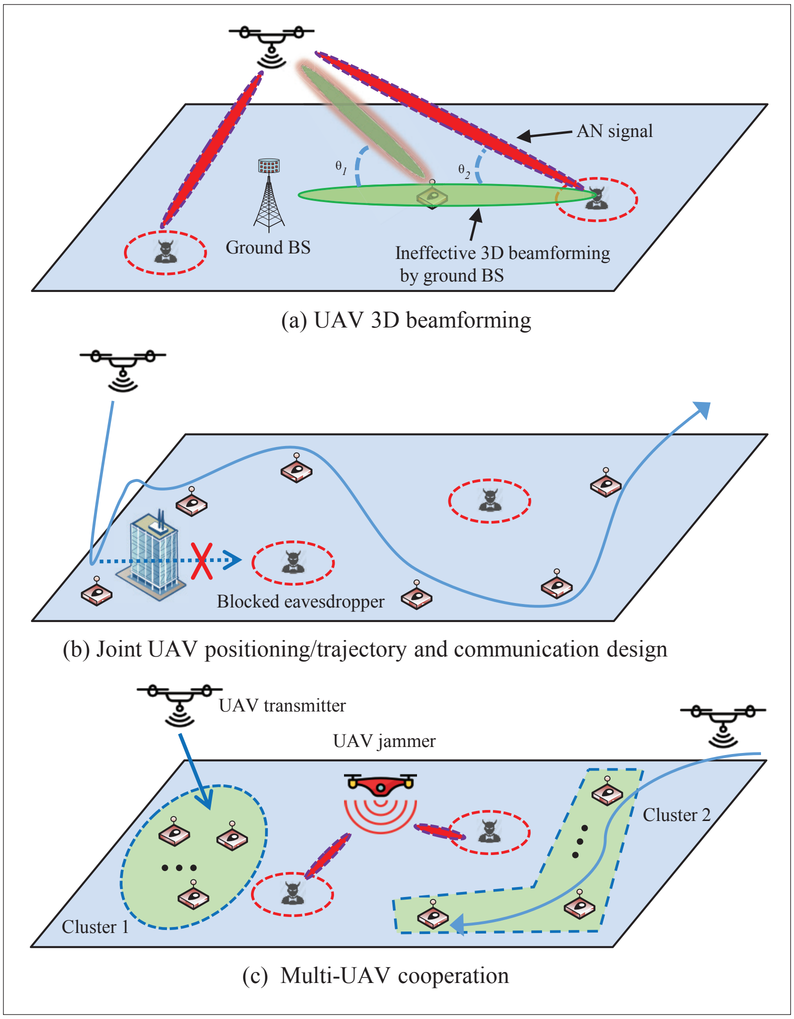
Joint UAV Positioning/Trajectory and Communication Design: As compared to terrestrial nodes, UAVs can be deployed more flexibly and move more freely in 3D space, which can be utilized to improve the communication throughput [8, 9] or secrecy rate [10] with the ground users. For example, a UAV transmitter at a given horizontal position can avoid signal blockage with legitimate users due to a high-rise building by increasing its altitude, or incur blockage and thus more propagation loss with the ground eavesdropper by lowering its altitude (Fig. 3b) so as to achieve better secrecy performance. On the other hand, for flying UAVs, a proper trajectory design of the UAV helps shorten its communication distances with legitimate users while enlarging the wiretap channel distances to alleviate the ground eavesdropping. Furthermore, communication scheduling and power control can be jointly designed with the UAV trajectory to achieve the optimum secrecy performance. For example, as shown in Fig. 3b, when a UAV has to fly over some eavesdroppers due to its mission requirement, the legitimate channel may not always be stronger than the wiretap channel along its trajectory. In this case, the UAV can increase its transmit power/rate when it flies closer to a legitimate user for communication while being further away from the eavesdroppers, and decrease transmit power/rate or even stop transmission otherwise. Finally, the UAV positioning/trajectory and communication co-design can be adaptive in real time to deal with moving eavesdroppers on the ground that intend to improve the eavesdropping performance and/or hide themselves from being exposed. It is worth pointing out that applying the UAV positioning/trajectory design to improve secrecy throughput generally leads to more UAV propulsion energy consumption as well as longer access delay, thus yielding fundamental trade-offs among them as characterized in [2].

Multi-UAV Cooperation: In practice, a single UAV only has limited communication and maneuvering capability and thus may not achieve the desired secure communication performance in some challenging scenarios (e.g., with multiple collusive eavesdroppers over a large area). This thus motivates the deployment of multiple collaborative UAVs to achieve more efficient secure communications [8, 11] For example, as shown in Fig. 3c, based on the locations of eavesdroppers, the ground users can be grouped into different clusters with each cluster served by a single UAV. As such, it may not be necessary for the UAV to fly over the eavesdroppers as in Fig. 3b, which thus helps reduce the information leakage. Alternatively, some UAVs may act as aerial jammers [11, 12], which are deployed above a group of nearby eavesdroppers to degrade their signal reception by sending AN signals [11, 12] This in turn provides higher flexibility for the deployment or trajectory design of other UAV transmitters to achieve better secrecy communication performance.

Securing G2A Communication against Terrestrial Jamming

In contrast to legitimate ground receivers in A2G communications, legitimate UAV receivers in G2A communications (Figs. 1c and 1d) are exposed in the sky and thus more vulnerable to jamming attacks by ground adversary nodes that send AN signals to interfere with the UAV so as to reduce its receive signal-to-interference-plus-noise ratio (SINR) for decoding. Although DSSS and FHSS are two widely applied anti-jamming techniques, they usually result in low spectrum efficiency and may not be sufficient to deal with the strong G2A jamming due to the LoS-dominant channel. Fortunately, the techniques discussed in the preceding subsection (e.g., 3D beamforming and UAV trajectory design) as well as device-to-device (D2D) communications can be applied to cope with the malicious jamming more effectively.

For example, the 3D receive beamforming at a legitimate UAV can provide higher spatial resolution than 2D beamforming and thus more efficiently cancel the interference from the ground jammers, as long as they are not so close to the legitimate ground transmitters that their elevation angles with the UAV can be resolved. In the case that the legitimate ground transmitter is a multi-antenna BS as shown in Fig. 1d, the 3D transmit and receive beamforming can be jointly employed at the BS and UAV to maximally improve the legitimate link SINR, which generally achieves higher spectrum efficiency than conventional DSSS and FHSS. Moreover, the 3D high mobility of UAV can be leveraged to optimize its position or trajectory by shortening/enlarging the distances from legitimate transmitters/malicious jammers. Finally, in the case where the UAV receiver needs to move away from the jammed area to avoid the strong interference, the D2D communications among the legitimate ground nodes (e.g., the ground sensors shown in Fig. 1c) can be exploited to forward the data of the ground nodes in the jammed area via a separate (unjammed) channel to other nodes that are sufficiently far away from the jammer but close to the UAV position/trajectory for more reliable uploading to the UAV.



(a) UAV 3D beamforming

(b) Joint UAV positioning/trajectory and communication design

(c) Multi-UAV cooperation

FIGURE 3. Approaches for safeguarding legitimate A2G communications against terrestrial eavesdropping.

Safeguarding Terrestrial Network against Malicious UAV Attacks

The LoS-dominant air-ground channels also make the terrestrial communications highly exposed to malicious UAVs. For example, a single UAV eavesdropper or jammer is capable of wiretapping or contaminating the transmissions within multiple cells. In addition, the flexible mobility and deployment of UAVs may be harnessed by malicious users to launch more aggressive attacks on terrestrial networks. It is therefore of paramount importance to develop advanced countermeasures for combating such attacks by malicious UAVs.

Anti-UAV Eavesdropping of Terrestrial Communication

As shown in Fig. 2a, thanks to the different altitudes of a legitimate ground receiver and a UAV eavesdropper, their well separated elevation angles can be exploited by the 3D transmit beamforming at a ground BS to achieve efficient signal nulling and hence secure communication in the downlink. However, for uplink transmissions where the legitimate ground users may not be equipped with a large number of antennas, combating malicious UAV eavesdropping becomes more challenging. To resolve this issue, we can apply two promising techniques based on different cooperation mechanisms in the terrestrial network, namely multihop D2D relaying and cooperative remote jamming, elaborated as follows.

Multihop D2D Relaying: Given the LoS advantage of G2A channels over terrestrial fading channels, the transmitted signal that needs to be received reliably at a ground receiver in terrestrial communication is more likely to be wiretapped by the UAV under the same link distance. To overcome this difficulty, one viable solution is to adopt multihop D2D relaying in the terrestrial network as shown in Fig. 4a, that is, utilizing nearby ground nodes as legitimate relays to help forward the confidential message from a source (legitimate ground node) to its destination (ground BS). By judiciously selecting the relay nodes (e.g., those with blocked LoS paths with the UAV) and designing their cooperative transmission (e.g., transmit power control and distributed space-time coding), the spatial/multi-path diversity gain can be reaped to significantly enhance the secrecy communication rate. However, on the other hand, an excessive number of hops may entail longer end-to-end delay as well as lower spectrum efficiency, and also increase the risk of being eavesdropped due to more exposure. As such, the number of hops, the transmit power in each hop, and the relay selection as well as the relay protocol need to be jointly designed to reconcile the above trade-off.

Cooperative Remote Jamming: Another effective means to prevent UAV eavesdropping is active jamming. However, its major weakness is that both the wiretap link and the legitimate link are degraded by the AN signal. To mitigate this adverse effect, a promising approach is employing terrestrial nodes (e.g., ground BSs) at favorable locations for cooperative *remote* jamming (e.g., those that are close to the UAV eavesdroppers but distant from the legitimate ground receivers of interest). As shown in Fig. 4b, a set of cooperative terrestrial BSs that are far away from the cell of the legitimate ground user but still have strong LoS channels with the UAV eavesdropper are selected as jammers. As such, the signal reception at the UAV eavesdropper is dramatically degraded, whereas only negligible interference is perceived at the legitimate ground receiver (serving BS) due to the more severe propagation loss and multi-path fading over terrestrial channels. In practice, depending on the traffic load of the terrestrial network, the jamming signals of the cooperative ground BSs can be either random message signals sent to their respective ground users or AN signals for dedicated jamming.

Anti-UAV Jamming to Terrestrial Communication

The jamming attack by malicious UAVs is another challenging issue for safeguarding terrestrial communications against their strong LoS jamming.

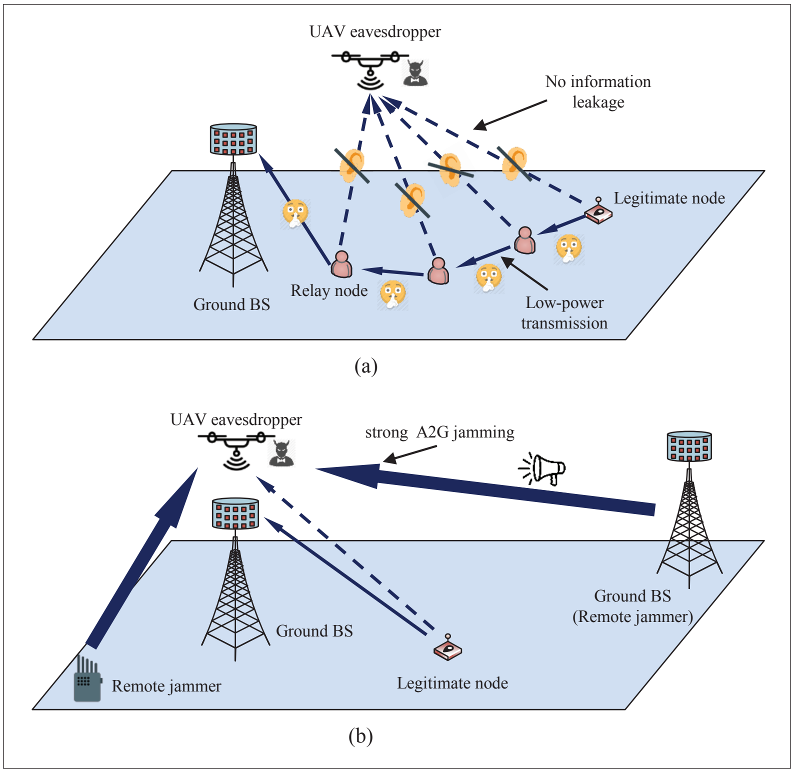


FIGURE 4. Approaches for safeguarding terrestrial communications against UAV eavesdropping: a) multihop D2D relaying; b) cooperative remote jamming.

However, it can be potentially tackled by applying techniques such as 3D beamforming, cooperative jamming signal cancellation, and D2D communications. For example, for uplink transmissions (Fig. 4b), the receive 3D beamforming can be applied at ground BSs to mitigate the UAV jamming signals efficiently. Furthermore, a neighboring idle BS that receives the jamming signal can also forward it via the high-speed backhaul link to the serving BS for cooperative jamming signal cancellation. However, for downlink transmissions with single-antenna legitimate receivers (e.g., sensors), the above approaches become infeasible, and anti-UAV jamming becomes more challenging. One possible solution for this scenario is again exploiting the potential cooperative D2D communication of the ground nodes and their probabilistic LoS channels with the UAV jammer, where the terrestrial message is first sent to a ground node that is near the legitimate user and also has a blocked LoS link with the UAV jammer for reliably decoding the message and then forwarding it to the legitimate user over an unjammed channel via D2D communication.

Numerical Results and Discussion

Numerical results are provided in this section to demonstrate the effectiveness of some of the techniques discussed in the previous two sections, respectively.

UAV-Assisted Jamming

First, we show the performance of the UAV positioning design with cooperative jamming against terrestrial eavesdropping. As shown in Fig. 5a, we consider that a ground eavesdropper intends to wiretap the A2G communication from a UAV-BS to a ground user. To improve the secrecy rate, a cooperative UAV-jammer is deployed right above the eavesdropper with the fixed jamming power given by $P_J = 5$ dBm. The two UAVs are deployed at the altitude of 200 m such that the A2G links approximately follow the free-space path loss model [8]. The reference signal-to-noise ratio (SNR) at the distance of 1 m is set as 80 dB. For comparison, we consider the following three schemes:

1. Optimized UAV-BS location with jammer
2. Optimized UAV-BS location without jammer
3. UAV-BS location fixed at (0, 200) m without jammer (i.e., right above the legitimate user)

The optimal UAV-BS locations in 1 and 2 are obtained by 1D search. In Fig. 5b, we plot the achievable secrecy rates in bits per second per Hertz by different schemes vs. the UAV-BS transmit power, P_U. First, it is observed that compared to hovering at the fixed location, optimizing the UAV-BS locations achieves significant secrecy rate gains, even without the helping UAV-jammer. This is because the UAV-BS can enlarge the difference in the receive SNRs of the legitimate user and the eavesdropper by properly positioning itself away from both of them, hovering at the left side of (0, 200). Second, one can observe that for the low UAV-BS transmit power, deploying the UAV-jammer with fixed jamming power degrades the secrecy rate, while for the high UAV-BS transmit power, the secrecy rate is substantially improved as compared to the other two schemes. This is expected as in the former case, the eavesdropping rate is quite small, and hence deploying a dedicated jammer has a more detrimental effect on the legitimate receiver than the eavesdropper. In the latter case, where the eavesdropping rate becomes high, deploying the UAV-jammer in the eavesdropper's vicinity can effectively disrupt its signal reception. Meanwhile, such a cooperative UAV-jammer also enables the UAV-BS to move closer to the user for improving the secrecy rate. For example, when $P_U = 15$ dBm, the optimized locations of the UAV-BS without and with the UAV-jammer are (–100, 200) m and (–89.5, 200) m, respectively. It is worth pointing out that instead of fixing the UAV-jammer's power and location in this example, we can optimize them along with the UAV-BS's location so that the secrecy rate with the UAV-jammer is always better than that without using it [10–12].

Cooperative Remote Jamming

Next, we evaluate the performance of the cooperative remote jamming technique for protecting the terrestrial communication from the UAV eavesdropping. As shown in Fig. 6a, we consider a cellular network where a UAV eavesdropper aims to overhear the downlink communication in a specific cell. To combat the UAV's strong LoS eavesdropping link, multiple remote BSs send independent jamming signals to the UAV eavesdropper. In Fig. 6b, we plot the secrecy rate of the legitimate communication vs. the number of cooperative BSs with different BS transmit power, denoted as P_T. The cell radius is assumed to be 800 m. The UAV altitude is set to be 200 m, and the horizontal distance between the UAV and the legitimate BS transmitter is set to be 1000 m. The location of the legitimate receiver is randomly generated in the cell of the serving BS. The ground user and the UAV are

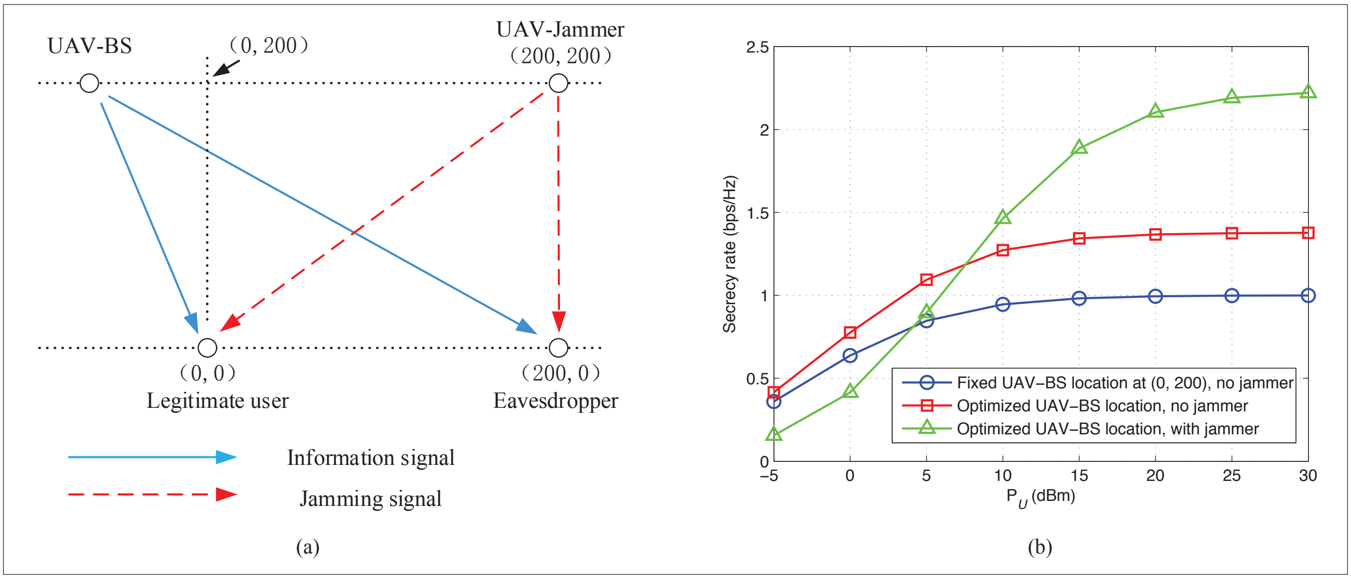


FIGURE 5. Secrecy rate performance with UAV-assisted jamming: a) simulation setup; b) secrecy rate vs. UAV transmit power.

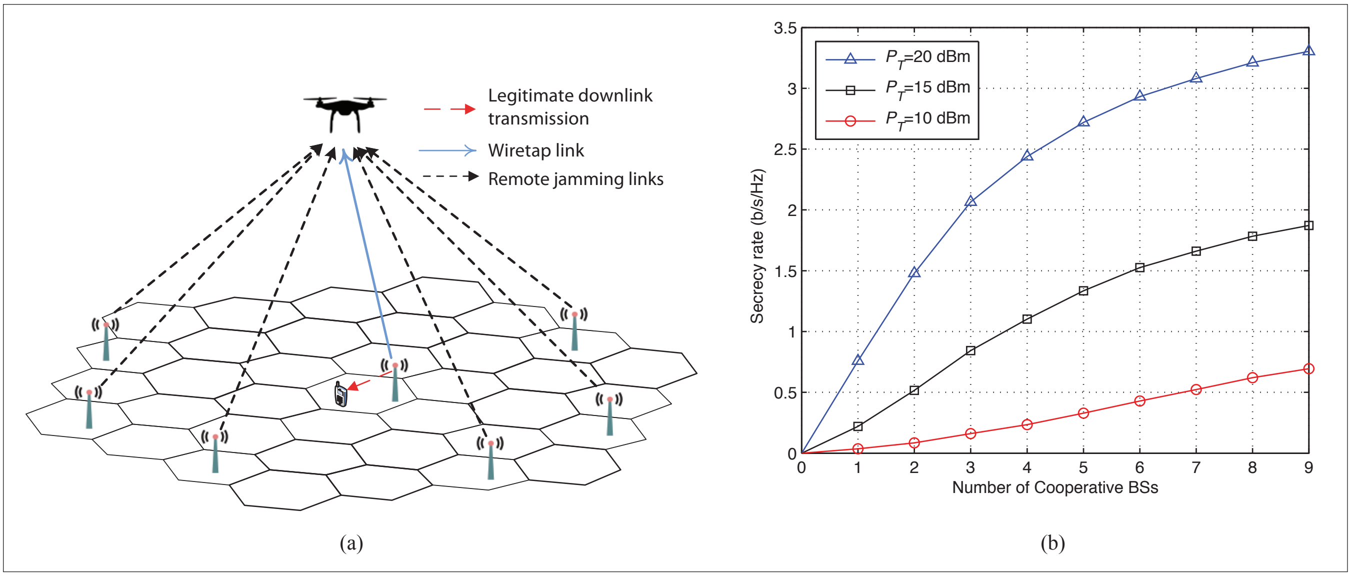


FIGURE 6. Secrecy rate performance with remote jamming: a) cellular network setup; b) secrecy rate vs. number of cooperative BSs.

assumed to be equipped with an isotropic antenna, while each BS employs a fixed antenna pattern with 10° downtilt angle [1]. For terrestrial channels, the path loss and shadowing are modeled based on a 3GPP Technical Report,[1] and the small-scale fading is modeled as Rayleigh fading. From Fig. 6b, it is observed that the secrecy rate is approximately zero when there are no cooperative jamming BSs, regardless of the BS's transmit power. This is because the G2A eavesdropping channel with dominant LoS is much better than the terrestrial fading channel of the legitimate link, thus leading to virtually zero secrecy rate. However, the secrecy rate is observed to increase rapidly as the number of cooperative BSs increases. This is expected since the UAV eavesdropper suffers from more interference from the increasing number of jamming BSs, which only cause negligible interference to the legitimate receiver due to the more severe path loss and multi-path fading over the terrestrial channels. Furthermore, it is observed that increasing P_T further improves the secrecy rate, despite the fact that the achievable rates of both the legitimate link and the UAV eavesdropping link increase with P_T. The reason lies in the former increasing much faster than the latter, which is severely limited by the increasing G2A interference with higher P_T.

Conclusions and Future Work

In this article, we focus on addressing two new and challenging security issues arising from the LoS-dominant UAV-ground channels in future wireless networks from a PHY design perspective. We present promising approaches and techniques to achieve secure UAV-ground communications in the presence of terrestrial eavesdroppers/jammers, as well as secure terrestrial communications against malicious eavesdropping/jamming attacks by UAVs. In practice, the use of such techniques needs to take into account issues such as implementation cost, prior knowledge of terrestrial node channel/location, and communication overhead. For example, although multi-UAV cooperation is expected to achieve better performance, it also requires the coordination of UAVs with increased signaling overhead. In addition, effective 3D beam-

[1] See http://www.3gpp.org/DynaReport/38901.htm for more details.

In future wireless networks, legitimate aerial and terrestrial communications both need to be protected against sophisticated attacks that may involve collusive eavesdroppers and jammers on the ground as well as over the air. As such, the presented approaches in this article need to be further investigated to address more challenging scenarios in practice.

forming requires a large number of antennas to be equipped at the UAV, while harnessing the UAV's high mobility generally leads to more propulsion energy consumption. In future wireless networks, legitimate aerial and terrestrial communications both need to be protected against sophisticated attacks that may involve collusive eavesdroppers and jammers on the ground as well as over the air. As such, the presented approaches in this article need to be further investigated to address more challenging scenarios in practice. Besides the PHY security issues discussed in this article, there are other related problems that need to be addressed, as listed below to motivate future work:

PHY security among UAVs: The presence of coexisting legitimate and malicious UAVs may pose several new challenges. For example, malicious UAVs may launch even more powerful attacks on legitimate UAVs over the more favorable air-to-air channels, as compared to the A2G/G2A channels considered in this article. In addition, malicious UAVs can also keep track of the movement of legitimate UAVs to maintain short distances with them so as to launch eavesdropping/jamming attacks more effectively as compared to their terrestrial counterparts.

UAV-assisted terrestrial adversary detection: With the rapid advances of high-definition optical cameras, it would be an appealing solution to deploy them on UAVs for detecting, identifying, and tracking malicious nodes on the ground. In addition, thanks to the high altitude and favorable LoS-dominant link, the UAV generally has stronger spectrum sensing ability than conventional terrestrial nodes. Thus, the UAV can also help achieve more accurate terrestrial jamming detection.

Malicious UAV detection: When there are malicious UAVs, it is imperative to detect their presence and also track their moving locations. For active UAVs such as UAV jammers, they can be detected/localized by using conventional signal sensing and ranging techniques. For passive UAVs such as UAV eavesdroppers, more sophisticated detection methods are generally required, such as radar and computer-vision-based methods [13].

UAV spoofing: In addition to the eavesdropping and jamming attacks, legitimate UAV communications may suffer from a more advanced spoofing attack such as GPS spoofing [14] where the ground adversary aims to deceive the UAV's navigation system by sending counterfeit GPS signals.

UAV-aided wireless surveillance and intervention: By exploiting its high mobility and LoS channel with the ground, a UAV can act as a legitimate eavesdropper or jammer for realizing the surveillance of suspicious communications or intervention of malicious communications on the ground, respectively [15]. In contrast to the techniques presented in this article to defend against UAV eavesdropping and jamming, the objective is reversed in this case to design efficient eavesdropping and jamming schemes for legitimate UAVs.

References

[1] Y. Zeng, Q. Wu, and R. Zhang, "Accessing from the Sky: A Tutorial on UAV Communications for 5G and Beyond," *Proc. IEEE*, 2019, submitted; https://arxiv.org/abs/1903.05289.

[2] Q. Wu, L. Liu, and R. Zhang, "Fundamental Trade-offs in Communication and Trajectory Design for UAV-Enabled Wireless Network," *IEEE Wireless Commun.*, vol. 26, no. 1, Feb. 2019, pp. 36–44.

[3] N. Yang *et al.*, "Safeguarding 5G Wireless Communication Networks Using Physical Layer Security," *IEEE Commun. Mag.*, vol. 53, no. 4, Apr. 2015, pp. 20–27.

[4] F. Jameel *et al.*, "A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security," *IEEE Commun. Surveys & Tutorials*, vol. 21, no. 3, 3rd qtr. 2019, pp. 2734–71.

[5] A. Mukherjee *et al.*, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 3, 3rd qtr. 2014, pp. 1550–73.

[6] A. Mpitziopoulos *et al.*, "A Survey on Jamming Attacks and Countermeasures in WSNs," *IEEE Commun. Surveys & Tutorials*, vol. 11, no. 4, 4th qtr. 2009.

[7] Y. Wu *et al.*, "Secure Massive MIMO Transmission with an Active Eavesdropper," *IEEE Trans. Info. Theory*, vol. 62, no. 7, July 2016, pp. 3880–900.

[8] Q. Wu, Y. Zeng, and R. Zhang, "Joint Trajectory and Communication Design for Multi-UAV Enabled Wireless Networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, Mar. 2018, pp. 2109–21.

[9] Y. Zeng, R. Zhang, and T. J. Lim, "Throughput Maximization for UAV-Enabled Mobile Relaying Systems," *IEEE Trans. Commun.*, vol. 64, no. 12, Dec. 2016, pp. 4983–96.

[10] G. Zhang *et al.*, "Securing UAV Communications Via Joint Trajectory and Power Control," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, Feb. 2019, pp. 1376–89.

[11] C. Zhong, J. Yao, and J. Xu, "Secure UAV Communication with Cooperative Jamming and Trajectory Control," *IEEE Commun. Lett.*, vol. 23, no. 2, Feb. 2019, pp. 286–89.

[12] A. Li, Q. Wu, and R. Zhang, "UAV-Enabled Cooperative Jamming for Improving Secrecy of Ground Wiretap Channel," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, Feb. 2019, pp. 181–84.

[13] I. Güvenc *et al.*, "Detection, Localization, and Tracking of Unauthorized UAS and Jammers," *Proc. IEEE/AIAA 36th Digital Avionics Systems Conf.*, St. Petersburg, FL, 2017, pp. 1–10.

[14] A. J. Kerns *et al.*, "Unmanned Aircraft Capture and Control via GPS Spoofing," *J. Field Robotics*, vol. 31, no. 4, Apr. 2014, pp. 617–36.

[15] J. Xu, L. Duan, and R. Zhang, "Surveillance and Intervention of Infrastructure-Free Mobile Communications: A New Wireless Security Paradigm," *IEEE Wireless Commun.*, vol. 24, no. 4, Aug. 2017, pp. 152–59.

Biographies

Qingqing Wu (elewuqq@nus.edu.sg) received his B.Eng. and Ph.D. degrees in electronic engineering from South China University of Technology and Shanghai Jiao Tong University (SJTU) in 2012 and 2016, respectively. He is currently a research fellow in the Department of Electrical and Computer Engineering at National University of Singapore (NUS). His current research interests include intelligent reflecting surface (IRS), unmanned aerial vehicle (UAV) communications, and MIMO transceiver design. He was the recipient of the Outstanding Ph.D. Thesis Funding in SJTU in 2016 and the Best Ph.D. Thesis Award of China Institute of Communications in 2017. He received the IEEE WCSP Best Paper Award in 2015. He is now an Editor of *IEEE Communications Letters* and the Workshop Co-Chair for the ICC 2019 Workshop on UAV Communications.

Weidong Mei (wmei@u.nus.edu) received his B.Eng. degree in communication engineering and M.Eng. degree in communication and information systems from the University of Electronic Science and Technology of China, Chengdu, in 2014 and 2017, respectively. Currently, he is pursuing a Ph.D. degree with the NUS Graduate School for Integrative Sciences and Engineering under the NGS scholarship. His research interests include wireless drone communications, physical-layer security, and convex optimization techniques. He received the Outstanding Master's Thesis Award from the Chinese Institute of Electronics in 2017.

Rui Zhang (F'17) (elezhang@nus.edu.sg) received his Ph.D. degree from the Electrical Engineering Department of Stanford University in 2007 and is now a Dean's Chair Associate Professor in the Electrical and Computer Engineering Department of NUS. He has been listed as a Highly Cited Researcher by Thomson Reuters since 2015. His research interests include wireless communication and wireless power transfer. He was the co-recipient of the IEEE Marconi Prize Paper Award in Wireless Communications, the IEEE Signal Processing Society Best Paper Award, the IEEE Communications Society Heinrich Hertz Prize Paper Award, and the IEEE Signal Processing Society Donald G. Fink Overview Paper Award, among others. He is now an Editor for *IEEE Transactions on Communications* and a member of the Steering Committee of *IEEE Wireless Communications Letters*.