Mode Selection and Cooperative Jamming for Covert Communication in D2D Underlaid UAV Networks

Bin Yang, Tarik Taleb, Yuanyuan Fan and Shikai Shen

Abstract

The integration of unmanned aerial vehicle (UAV) networks and device-to-device (D2D) communications is expected to provide ubiquitous connectivity and high-speed rates for sensitive information transmission in future wireless networks. However, the traditional cryptography and physical layer security techniques still cannot prevent adversaries from knowing the existence of information transmission such that they further launch attacks on transmitters and receivers. Covert communication can offer an even stronger level of security via hiding the information transmission process of wireless networks. In this article, we first integrate D2D communications into UAV networks, and then investigate the fundamental issues of mode selection and cooperative jamming for covert communication in such networks, aiming to provide a powerful security solution to support widespread security-sensitive applications of such networks. To this end, we propose two promising D2D underlaid UAV network architectures, whereby each UAV acts as either a flying BS or an aerial UE. Then, we propose a covert communication strategy by combining mode selection and cooperative jamming, where mode selection allows each user equipment to adaptively switch between half-duplex and full-duplex communication modes, and cooperative jamming means that idle D2D pairs inject interference to confuse adversaries. The goal of the proposed strategy is to enhance covert capacity performance (i.e., the maximum channel rate) while maintaining a high detection error probability at adversaries in the promising network architectures. Numerical results are presented to evaluate our strategy of mode selection and cooperative jamming, and to illustrate performance gains in terms of covert capacity and detection error probability in these two network architectures. Finally, a vision is discussed for our future research in D2D underlaid UAV networks.

Introduction

Unmanned aerial vehicles (UAVs), which can serve as flying base stations (BSs) and aerial user equipments (UEs) to provide reliable and low cost wireless communication services, have attracted significant attention in both academia and industry [1–4]. Recently, as a key communication technology, device-to-device (D2D) communication allows nearby UEs to directly communicate without passing by BS, opening up many new application opportunities for proximity and low latency services such as social networking, content sharing, and so on [5]. Specifically, it can offload traffic from UAVs in crowded areas (e.g., stadiums, concerts), extend the coverage region of UAVs in a large disaster area, and save their limited energy. By integrating D2D communications into UAV networks, the new D2D underlaid UAV networks are envisioned to provide ubiquitous connectivity and high-speed rates for supporting widespread applications in the fifth and beyond wireless networks. Noticeable examples of these applications are disaster relief, vehicle networking, and Internet of Things (IoT).

Unfortunately, the wireless channel characteristics of broadcast and openness pose unprecedented security and privacy threats when transmitting sensitive information, especially for financial and military data in the presence of adversaries. To protect the information transmission security, most commonly used security methods rely on upper-layer cryptographic techniques requiring high computational complexity, which may not be suitable for UAV networks due to a large amount of energy consumption. Meanwhile, these techniques may also be infeasible with the appearance of powerful computing devices. As an alternative, a physical layer security technique utilizes interference and noise of wireless channels to protect information transmission from being wiretapped by adversaries. However, adversaries can still detect the behavior of wireless communication such that they further launch an attack on the information source and destination. For instance, in a battlefield, soldiers hope to prevent adversaries from detecting their communication process with the military base to protect their location privacy.

Recently, a promising covert communication technology unitizes noise and interference of wireless channels to hide the information transmission process, which can provide stronger security protection for UAV networks. Figure 1 illustrates an example of a covert communication scenario, where a UAV transmitter (Alice) transmits information to an intended receiver (Bob) and Bob may inject interference to hide the transmission from an adversary (Willie). The existing works on covert communication mainly focus on the scenarios of wireless networks without the aid

Digital Object Identifier:
10.1109/MNET.011.2000100

Bin Yang is with Chuzhou University and Aalto University; Tarik Taleb is with Aalto University, Oulu University, and Sejong University; Yuanyuan Fan is with Chuzhou University; Shikai Shen is with Kunming University.

of UAV, D2D and ground BS under either half-duplex mode or full-duplex mode ("Related Works" below). To date, only a few works on covert communication consider either D2D communication or UAV networks under half-duplex mode [6–8]. In covert communication, half-duplex and full-duplex are two classic communication modes. Under full-duplex mode, each receiver can receive information from its transmitter and also simultaneously inject interference to confuse the watchful adversary over the same channel, which can increase the detection error probability at the watchful adversary. On the other hand, it can also decrease covert capacity (i.e., maximum channel rate) due to the effect of self-interference at the receiver. The half-duplex mode can overcome the effect of self-interference, but cannot ensure a high detection error probability at the watchful adversary. To satisfy the requirements of different applications in terms of covert capacity and detection error probability, it is critical to adaptively switch the communication modes for each receiver. As a result, two fundamental issues arise in UAV networks. One issue regards how to integrate D2D communications into UAV networks, and another is to design a mode selection method to adaptively switch between half-duplex and full-duplex modes for enhancing the covert capacity performance while keeping a high detection error probability at Willie.

To address these two issues, this article first proposes two promising D2D underlaid UAV network architectures, and then proposes a mode selection method allowing each UE to adaptively switch between these two communication modes in D2D underlaid UAV networks according to the requirements of different applications for covert capacity and detection error probability. However, if the receiver is far away from the watchful adversary, it has no ability to seriously interfere with the watchful adversary. Therefore, to provide a powerful security protection for information transmission, we further integrate cooperative jamming into the mode selection. With cooperative jamming, the idle D2D UEs, close to the transmitter, can be selected as friendly jammers to inject interference, aiming to confuse the watchful adversary far away from the receiver for guaranteeing covert communication from the transmitter to its receiver. Then, we provide numerical results to evaluate our strategy of mode selection and cooperative jamming and to illustrate the performance gains of covert capacity and detection error probability under these two network architectures, where UAVs serve as flying BSs and aerial UEs, respectively. Finally, we give a vision for future research in D2D underlaid UAV networks.

Related Works

We now introduce related works for covert communication with half-duplex mode, full-duplex mode and cooperative jamming.

Covert Communication with Half-Duplex Mode

Regarding a wireless network consisting of a transmitter (Alice), a receiver (Bob) and a watchful adversary (Willie), Alice wants to transmit information to Bob such that Willie does not know the transmission from Alice to Bob. Under the network scenario with half-duplex mode, the authors in [9] proposed a square root law with Gaussian noise channels for covert communication, which illustrates that $O(n)$ information bits can be transmitted reliably and covertly to Bob while Willie does not detect the transmission. This work was further extended to binary symmetric channels, multiple access channels, discrete memoryless channels, etc. [10, 11]. Multi-antenna covert communication in [12] was explored for a wireless network consisting of a multi-antenna transmitter and a single-antenna receiver against randomly distributed single antenna adversaries and interferers. Recently, the authors in [13] studied the effect of fixed and random transmit power on the covert performance in delay-intolerant wireless networks. The results showed that random transmit power could significantly increase the amount of information transmitted covertly. The covert communication was further investigated in a dense IoT network with an additive white Gaussian noise (AWGN) channel and terahertz (THz) channel, and the security of such networks can be enhanced from the physical layer via covert communication [14].

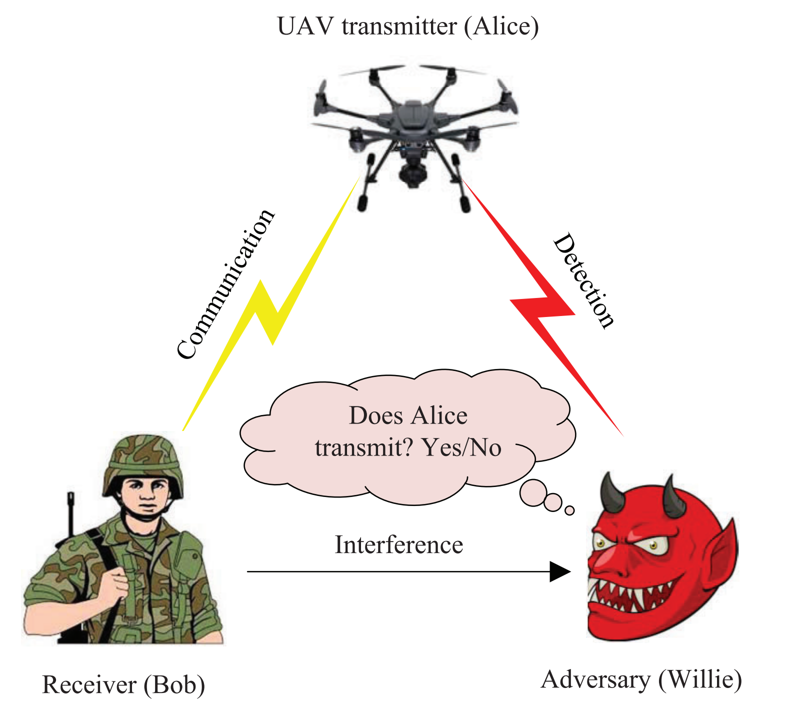

FIGURE 1. Illustration of covert communication scenario.

Consider relay assisted wireless networks, the work in [15] studied covert communication in two-hop relay wireless networks with Rayleigh fading channels. In [15], rate-control and power-control schemes were proposed for the relay to covertly transmit its information according to the performance metrics of detection error probability and covert capacity. The work in [16] considered a self-sustained relay and two energy harvesting schemes (i.e., time switching and power splitting) in a two-hop relay wireless network. A self-sustained relay, which could employ the two energy harvesting schemes to harvest energy from the source, used the harvested energy to forward the message from the source and meanwhile also tried to covertly send its own message. However, the source did not allow the relay to send its own

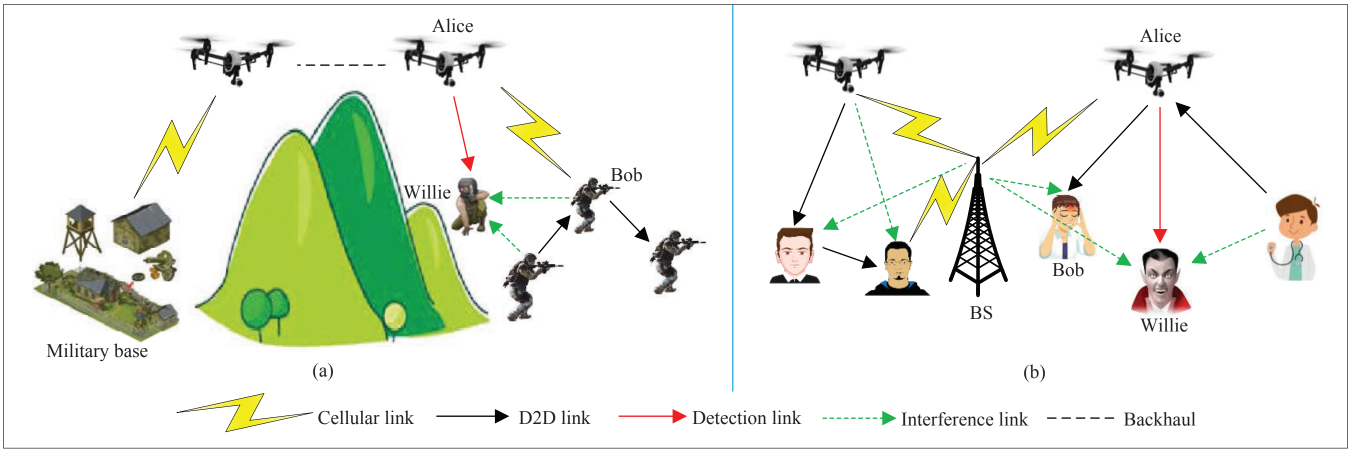

FIGURE 2. Illustration of two promising network architectures for covert communication in the presence of a watchful adversary Willie: a) UAVs as flying BSs; b) UAVs as aerial UEs.

message and thus detected whether the covert transmission happened or not. The analysis indicated that the detection error probability at the source is the same for the two energy harvesting schemes, and the increase in the energy cost of the relay's transmission is also the same when achieving the maximum covert capacity under both schemes. In [17], a muti-hop routing algorithm is used to improve covert performance in the presence of multiple collaborating Willies over additive white Gaussian noise. The results showed that when the distance between Alice and Bob is large, the proposed muti-hop routing algorithm can substantially enhance covert performance compared to one-hop covert communication.

Recently, some initial works have been dedicated to the study of covert communication in UAV networks and D2D communication. By combining UAV's trajectory and transmit power, the authors in [6] developed a joint optimal framework to maximize covert capacity performance in UAV networks. In [7], covert D2D communication was explored by joint optimization of the content delivery mode selection and resource management. Consider multi-hop relay wireless networks, the work in [8] optimized the transmit power at relays to maximize the covert capacity against UAV surveillance.

Covert Communication with Full-Duplex Mode

Consider a wireless network where transmitter Alice transmits information to a receiver Bob, whereas an adversary Willie tries to detect the transmission. In [18], the authors investigated the ability to achieve covert communication adopting a full-duplex receiver that emits artificial noise to confuse Willie to cause detection errors. Numerical results indicated the full-duplex mode can increase detection error probability at Willie and transmission power needs to be adjusted carefully, avoiding that the self-interference of the full-duplex receiver negatively affects covert communication. The authors in [19] examined delay-constrained covert communication using a full-duplex receiver. In [19], the receiver transmitting artificial noise with a fixed power can indeed enhance covert communication performance, because Willie cannot exactly learn its received power in a limited time period. The work in [20] showed that the source has a positive covert capacity with the help of a full-duplex relay in a two-hop relay wireless network, where it is uncertain to the channel gain between each transmitter and its receiver.

Covert Communication with Cooperative Jamming

The authors in [21] utilized a cooperative jamming technique to increase the interference that the adversary Willie experiences for achieving covert communication in a wireless network, where with the help of a friendly jammer, Alice can transmit $O(n)$ bits covertly and reliably to Bob without being detected by Willie. In [22], the authors focused on a network scenario where deploying multiple friendly jammers can emit noise to hide the transmission from Allice to Bob in the presence of multiple adversaries.

D2D Underlaid UAV Network Architectures

This section proposes two promising D2D underlaid UAV network architectures, where UAVs act as either flying BSs or aerial UEs.

UAVs Acting as Flying BSs

The network architecture consists of UAVs, ground UEs, and watchful adversaries. UAVs act as flying BSs; in other words, they perform operations similar to those of ground BSs while flying in the air. As shown in Fig. 2a, there are five types of communication links in such an architecture: cellular link between flying BS and UE; D2D link between D2D UEs; detection link between adversary and UE/flying BS; interference link between another transmitter and receiver; and backhaul between flying BSs. Compared to the traditional ground BS-based wireless networks, the new network architecture has many advantages:

- It can provide ubiquitous connectivity among users. Thanks to the flexible mobility and low cost of UAVs, it becomes fast and easy to deploy networks in areas outside the coverage of the cellular network (e.g., mountains, islands, disaster-affected areas, and military areas) for providing emergency communication services. Meanwhile, UEs can directly transmit messages to other UEs via D2D communications.
- It can also provide high-speed data rates, because there is very likely to be line-of-sight (LoS) links between UAVs and ground UEs and between proximity-based D2D pairs

while the LoS links suffer less path loss, shadowing and multi-path fading compared to the non-line-of-sight (NLoS) links.

Due to its distinctive advantages, the new network architecture has huge potential in civil and military applications. For example, in the civil field, the network architecture can ensure communications among users when the traditional cellular network is partially or fully damaged by natural disasters such as earthquakes, floods, and hurricanes. In the military field, troops in remote areas communicate with other troops or with their military base via such a network architecture.

However, the network architecture also faces significant security threats in the presence of malicious adversaries. Specifically, wireless LoS links are likely to be intentionally detected and listened to by some malicious adversaries. As shown in Fig. 2a, a flying BS Alice is performing a downlink transmission with a soldier Bob in a covert battlefield scenario. Once the adversary Willie detects the existence of the transmission, he can launch an attack on the flying BS Alice and soldier Bob, which seriously threatens the security of Alice and Bob. Remarkably, covert communication can guarantee that Willie cannot detect the transmission such that he does not launch an attack like eavesdropping, decoding and even destroying the transmitter. To ensure secure communication among UAVs and UEs, it is of paramount importance to explore covert communication methods in the network architecture.

UAVs Acting as Aerial UEs

The network architecture consists of ground BSs, UAVs, ground UEs, and watchful adversaries. In this network architecture, UAVs are mere UEs, capable of flying in the air. As shown in Fig. 2b, in this network architecture, each UE can select to communicate with either its nearby UE or BS. The network architecture is expected to be widely used in IoT. This is because it can provide ubiquitous connectivity due to its distinctive features of flexible mobility and on-demand deployment. It also has great potential in firefighting operations and human search and rescue operations, whereby aerial UEs (i.e., UAVs) carrying some IoT devices can sense the presence of fire and/or human beings, and accordingly notify a ground control center. Specifically, with the help of almost ubiquitous cellular BSs worldwide, UAVs can communicate with remote users who are even distributed around the world, which will open up many new opportunities for UAVs in future applications.

D2D communication can also significantly improve the network performance in the architecture. For example, aerial UEs need to send the same information to a large number of ground UEs in a large area. Without the help of D2D communications among ground UEs, UAVs have to repeatedly send the same information to different ground UEs dispersed over a large geographic area. Both the physical mobility of UAVs and multiple retransmissions of messages would drain the limited energy of UAVs. To save the energy of UAVs, a promising method is to unitize D2D communication techniques for information exchange among ground UEs.

However, due to the broadcast feature of wireless links, the network architecture faces serious security threats, which may prevent it from being deployed on a large scale in the future. As shown in Fig. 2b, an adversary Willie can detect not only the transmissions between D2D UEs but also the transmissions between UEs and BS. To provide strong security protection for the transmission links, it is critical to ensure the covert communication in the network architecture.

Covert Communication

The goal of covert communication is to provide a covert wireless transmission between users while maintaining a low detection probability at a watchful adversary for supporting a wide range of security-sensitive applications, such as location tracking in vehicular networks, covert military commutations and IoT.

As shown in Fig. 2, we consider two promising D2D underlaid UAV network architectures, where UAVs serve as flying BSs and aerial UEs to conduct the similar operations of ground BSs and UEs, respectively. In Fig. 2, a UAV transmitter Alice transmits information to its intended receiver Bob while a watchful adversary Willie tries to decide whether Alice is transmitting or not. Suppose that Alice transmits n symbols to Bob, Willie will detect a symbol vector with length n, each element of which is the sum of the received signal from Alice, the background noise and the aggregate interference that Willie experiences.

To determine whether or not Alice is transmitting, Willie attempts to decide whether its received signal is interference and background noise or signal from Alice plus interference and background noise. In other words, Willie needs to distinguish the following two hypotheses: null hypothesis and alternative hypothesis. The null hypothesis represents that Alice did not transmit, and thus the received signal of Willie is the sum of interference from other transmitters and the background noise he experiences, while the alternative hypothesis represents that Alice transmitted information to Bob, and thus its received signal is the signal from Alice plus the sum of the interference from other transmitters and the background noise.

Based on Willie's received signal vector, it has to make a decision whether Alice did a transmission in each slot. A radiometer is used by Willie as its detector. Willie first needs to determine a sampling value of Willie's received signal, and then performs the following test: if the sampling value is larger than a detection threshold of Willie, Willie makes a decision in favor of alternative hypothesis; otherwise, it is in favor of null hypothesis.

We now introduce detection error probability at Willie as a measure of covertness. First, we define two probabilities of false alarm and missed detection. The probability of false alarm is defined as the probability that when null hypothesis is true, Willie is in favor of alternative hypothesis. Similarly, the probability of missed detection is the probability that when alternative hypothesis is true, Willie is in favor of null hypothesis. Both the priori probabilities of null and alternative hypotheses equal 0.5, which implies that Willie randomly guesses the transmission state of Alice. Then, the detection error probability at Willie equals 0.5 multiplied by the sum of these two probabilities of false alarm and missed detection.

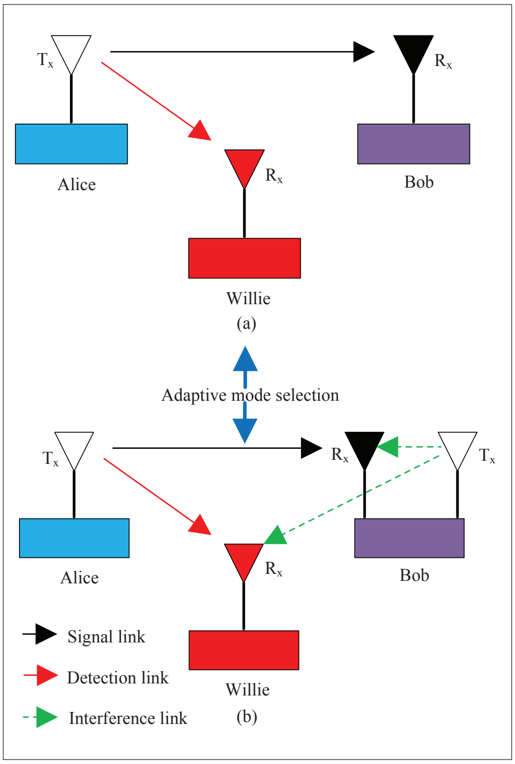

FIGURE 3. Communication mode selection: a) half-duplex mode; b) full-duplex mode.

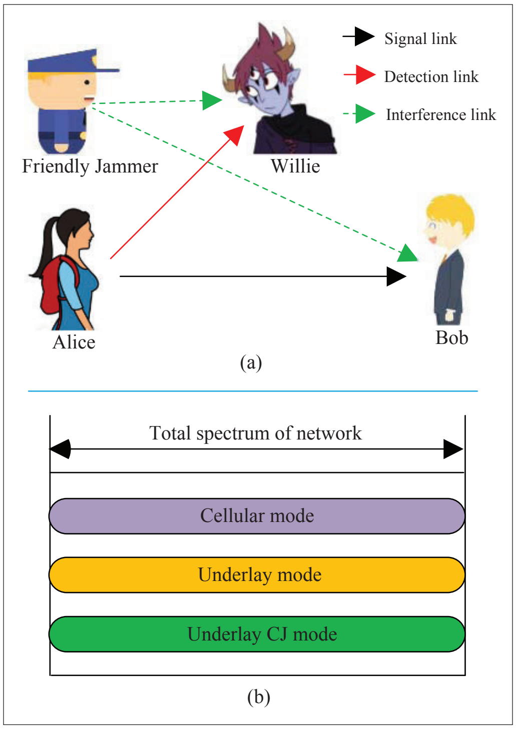

FIGURE 4. Cooperative jamming: a) cooperative jamming technique; b) cooperative jamming based spectrum reuse.

In covert communication, we hope Willie has a high detection error probability. To evaluate both covertness and reliability in D2D underlaid UAV networks, we study covert capacity performance subject to a high detection error probability constraint. The covert capacity is defined as the maximum achievable channel rate, which can be determined according to Shannon's Theorem. Moreover, we also study detection error probability performance with a requirement of covert capacity no less than a given value.

Mode Selection and Cooperative Jamming Strategy

In this section, we introduce a new strategy of covert communication by combining mode selection and a cooperative jamming technique.

Adaptive Mode Selection

Half-duplex and full-duplex are two prevalent communication modes. As shown in Fig. 3, the receiver Bob using half-duplex mode only receives information from Alice, while using full-duplex mode not only receives information but also transmits over the same channel at the same slot. It is notable that a full-duplex Bob can transmit artificial noise to deliberately confuse Willie for increasing his detection error probability. Meanwhile, full-duplex mode can also improve spectrum efficiency. On the other hand, it may cause self-interference at Bob, reducing covert capacity, while half-duplex mode can overcome the effect of self-interference at Bob for enhancing covert capacity performance. The existing works on covert communication mainly consider these two modes separately.

To improve covert performance in D2D underlaid UAV networks, we propose an adaptive mode selection method. Here, we consider an ideal situation whereby the receiver Bob knows the detection error probability at the watchful adversary Willie. Regarding the mode selection, given an accepted high detection error probability, if the covert capacity under the half-duplex mode is larger than that under the full-duplex mode, Bob adaptively switches to the half-duplex mode; otherwise, it turns to the full-duplex mode. On the other hand, given a covert capacity, if the detection error probability under half-duplex mode is larger than that under full-duplex mode, Bob switches to the half-duplex mode; otherwise, it turns to the full-duplex mode.

Notice that in practice, the detection error probability at Willie is unknown to Bob. To enable the receiver to adaptively switch between the full-duplex and half-duplex modes, we first conduct sufficient independent statistic experiments and then construct a decision rule at Bob. With the decision rule, once the covert capacity or detection error probability is lower than a predetermined threshold, Bob determines to switch the modes.

Cooperative Jamming

In the cooperative jamming (CJ) technique, friendly jammers can transmit jamming signal to interfere with watchful adversary Willie such that Alice can covertly transmit information to Bob, as shown in Fig. 4a. Additionally, in D2D communication, cellular and underlay modes are two basic spectrum reuse modes, as shown in Fig. 4b. The former one represents cellular UEs using the spectrum of a cellular network to communicate with BSs, while in the latter one D2D UEs reuse the spectrum of cellular UEs to directly communicate with each other.

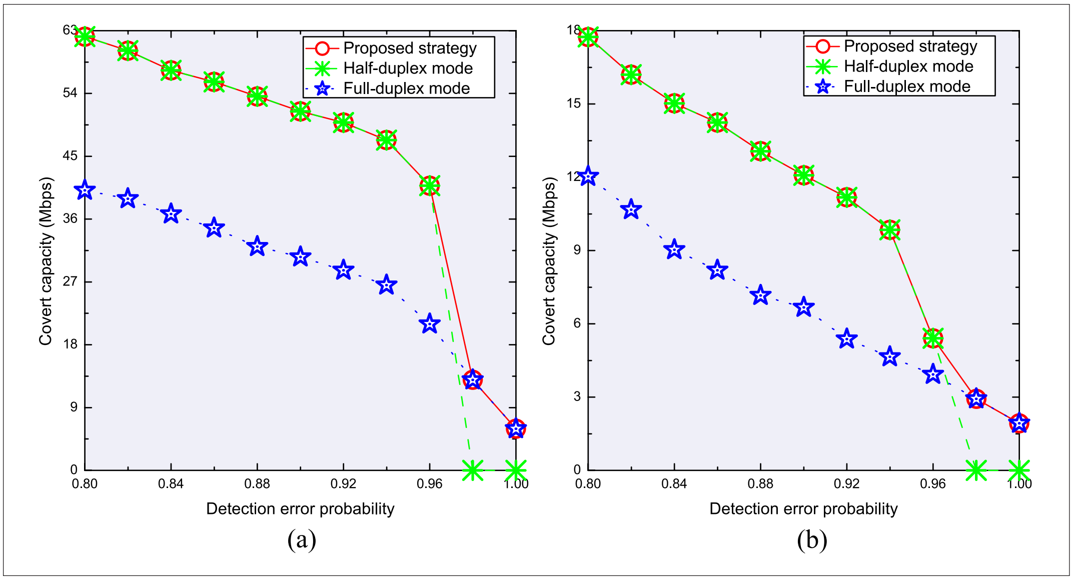

FIGURE 5. Covert capacity in the scenario with UAVs as flying BSs: a) covert capacity of D2D link; b) covert capacity of cellular link.

Based on the spectrum reuse modes, a new underlay CJ mode is proposed to further enhance covert performance of D2D underlaid UAV networks as shown in Fig. 4b. With the new underlay CJ mode, idle D2D UEs, which do not transmit information in some slot, transmit jamming signal to confuse adversaries achieving covert transmissions from other D2D and cellular UEs using the same spectrum with them. As shown in Fig. 4a, an idle D2D UE can serve as a friendly jammer if the signal-to-interference-plus-noise ratio (SINR) of jamming signal at the adversary Willie is larger than that at the receiver Bob, since the jamming signal has more effects on Willie than Bob.

Illustrative Results

In this section, we present numerical results to evaluate the covert communication performance of our proposed strategy in terms of covert capacity and detection error probability.

As shown in Fig. 2, we focus on the two D2D underlaid UAV network architectures, where UAVs act as flying BSs and aerial UEs, respectively. The former one in Fig. 2a shows that flying BSs can extend the communication distance of ground UEs and the nearby UEs can also perform direct D2D communication which helps ease the traffic of flying BSs. On the other hand, UAVs as flying BSs can reduce the traffic of ground BSs and extend their coverage through D2D communications. In these two network architectures, both D2D and cellular communications encounter the threats of detection from watchful adversaries Willies.

In this article, UAVs, UEs, ground BSs and Willies are distributed in a three dimensional space following homogeneous Poisson point processes with densities λ_A, λ_U, λ_B and λ_W. Each UE selects one of D2D and cellular communications according to the following received signal strength (RSS) based scheme: if the RSS at its closest (flying) BS is larger than that at its closest (aerial) UE, it selects cellular communication with the (flying) BS; otherwise, it selects D2D communication with the (aerial) UE. In a slot, if the RSS at the D2D receiver is smaller than a threshold θ, the corresponding D2D transmitter keeps silent (called idle D2D UEs). Each cellular UE is assigned an orthogonal and equal-sized spectrum which means that there is no interference among cellular UEs in the same cell. The total spectrum width of the network is denoted by *W* GHZ. Here, we focus on the case of one uplink channel being shared by one cellular UE and D2D UEs, and the rotary-wing UAVs hovering over the targeted area with altitude *H*.

UAVs as Flying BSs

A simulation study is presented to evaluate our proposed strategy according to covert capacity performance subject to detection error probability at Willies in the scenario of UAVs as flying BSs in Fig. 2a. We also compare the performance with half-duplex and full-duplex modes, respectively. We consider the network scenario with the following settings: total spectrum width of network W = 2 GHz, $\lambda_A = 10^{-4}$ UAVs/m^2, λ_U = 0.02 UEs/m^2, λ_W = 0.01 UEs/m^2, transmit power of transmitter UE P_U = 200 mW, transmit power of receiver UE P_R = 200 mW under full-duplex, flying altitude H = 300 m, the distance between two antennas equipped in each UE *dst* = 0.1 m under full-duplex, the received signal threshold $\theta = -120$ dBm, noise variance $\sigma^2 = -150$ dBm, and path loss exponents $\alpha = 2$ for the channel from ground to air, and $\alpha = 4$ for that from ground to ground. Rayleigh fading is employed to characterize both small scale and large scale fading for the channels between ground UEs, while Rician fading is used to depict the line-of-sight (LOS) channels from ground to air [23].

Figure 5 summarizes covert capacity results of D2D and cellular links with the constraint of detection error probability under our proposed strategy and the strategies under half-duplex and full-duplex modes. For each value (x, y) in Fig. 5, it represents that with the requirement of detection error probability not less than x, the covert capacity equals y. We can see from Fig. 5 that both covert capacities of D2D and cellular links

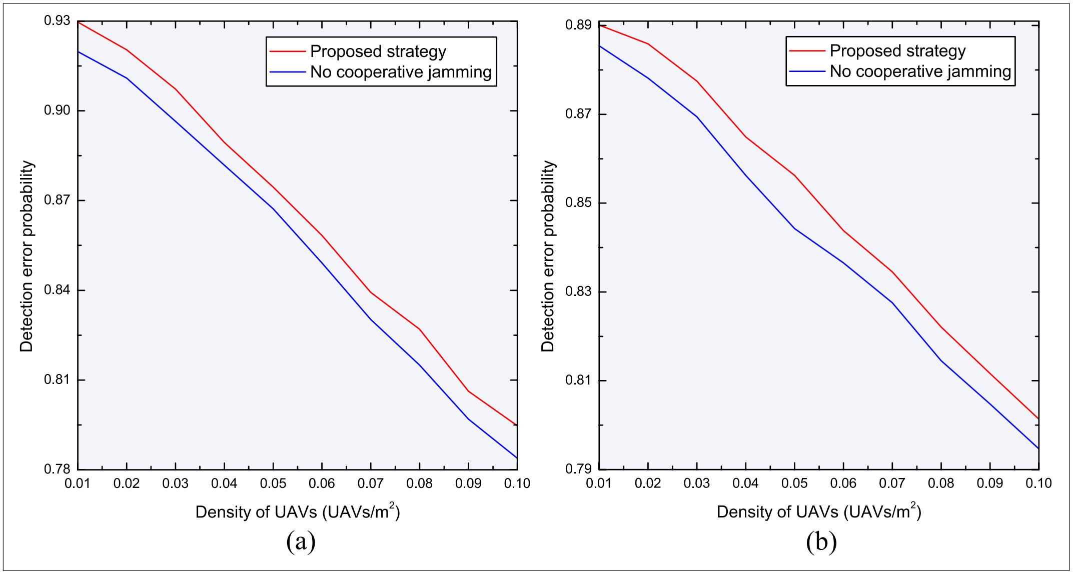

FIGURE 6. Detection error probability in the scenario with UAVs as aerial UEs: a) detection error probability of D2D link; b) detection error probability of cellular link.

reduce as detection error probability increases. This is because a larger detection error probability means that Willies receive more interference and noise; meanwhile, the receivers of D2D and cellular links are also deeply affected by interference and noise leading to the decreasing of covert capacity. We notice that our proposed strategy can adaptively switch between half-duplex and full-duplex modes in terms of the maximum covert capacity.

As shown in Fig. 5, as detection error probability increases, the covert capacity under half-duplex mode is first larger than that under full-duplex mode, and then the former one is smaller than the latter one. This can be explained as follows: the negative effect of self-interference under full-duplex mode leads to a smaller covert capacity, while as detection error probability continues to increase, the covert capacity under half-duplex mode first reduces to zero compared to full-duplex mode since Willies receive more interference under full-duplex mode such that the decreasing rate of detection error probability is slower than that under half-duplex model.

UAVs as Aerial UEs

We proceed to illustrate our simulation results in the scenario with UAVs as aerial UEs. For the parameter settings: W = 2 GHz, $\lambda_B = 10^{-4}$ BSs/m^2, λ_U = 0.02 UEs/m^2, λ_W = 0.02 UEs/m^2, P_U = 200 mW, P_R = 200 mW, H = 300 m, dst = 0.1 m, θ = –120 dBm, σ^2 = –150 dBm, and path loss exponents α = 2 for the channel from ground to air, and α = 4 for that from ground to ground. Under our proposed strategy and that without cooperative jamming, we summarize in Fig. 6 that the effect of the number of UAVs on the detection error probabilities of D2D and cellular links with requirements of covert capacity no less than 10 Mb/s for D2D link and 4 Mb/s for cellular link. We can see from Fig. 6 that both the detection error probabilities of D2D and cellular links decrease as the number of UAVs increases. This is because as the number of UAVs becomes larger, adversaries Willies are closer to their detecting transmitters, which leads to increasing of probabilities that these transmissions are detected by them, and thus the detection error probabilities decrease.

A further observation from Fig. 6 illustrates that detection error probabilities of D2D and cellular links under our proposed strategy are higher than those under that without cooperative jamming. This is due to the fact that Willies can receive more interference under our proposed strategy with cooperative jamming, leading to increasing of detection error probability compared to that under no cooperative jamming strategy.

Future Research Directions

Active Adversaries' Attacks: In D2D underlaid UAV networks, Alice transmits information in the presence of passive adversaries only detecting the transmission as well as active ones launching a jamming attack or more advanced spoofing attacks, which will seriously threaten future deployment of such networks. Therefore, new research is needed to explore the covert communication with multiple active adversaries' attacks.

Adaptive Mode Selection for Multi-Hop Covert Communication: If the distance between Alice and Bob is large, Alice needs to increase its transmit power to communicate with Bob, leading to the increasing of probability that wireless communication is detected by adversaries. With the help of relay nodes, the information from Alice experiences multi-hop to reach Bob, which reduces the transmit power of each node. An interesting research direction is to design an adaptive strategy of mode selection between half-duplex and full-duplex modes in multi-hop routing D2D underlaid UAV networks.

Millimeter Wave Covert Communication: Millimeter wave, which can provide rich available spectrum and proximity-based high speed information transmission, has been identified as a key technology in future wireless networks. Although millimeter wave wireless networks with directional antennas can enhance security performance, adversaries still probably detect communication processes of such networks when they reside in the signal beam. Millimeter wave covert communication needs to be further studied in D2D underlaid UAV networks and other types of wireless networks.

Performance Studies of D2D Underlaid UAV Networks: Such networks have significant potential to improve the performance in terms of channel rate, sum rate, max-min rate, coverage and energy efficiency. One interesting direction is how to optimize various parameters (e.g., UAV trajectory, UAV altitude, power and channel allocations for UAVs and UEs, and so on) to maximize the fundamental performance for satisfying various application requirements.

Conclusions

This article first proposed two promising D2D underlaid UAV network architectures, and then proposed an adaptive mode selection and cooperative jamming strategy for enhancing covert communication performance in terms of covert capacity and detection error probability in such network architectures. We further evaluated our proposed strategy under the two network architectures. Numerical results are provided to illustrate that our proposed strategy can significantly improve covert communication performance in D2D underlaid UAV networks compared to those under half-duplex mode, full-duplex mode and no cooperative jamming. It is also demonstrated that our research can provide a comprehensive covert communication solution for supporting various security-sensitive applications. Finally, we presented a vision for future research.

Acknowledgment

This work was supported by the European Union's Horizon 2020 Research and Innovation Program through the 5G!Drones Project under Grant No. 857031; by the Academy of Finland 6Genesis project under Grant No. 318927; by the Academy of Finland CSN project under Grant No. 311654; by the NSFC under Grant No. 61962033; by the Anhui Province project under Grant No. 1808085MF165, gxgwfx2019060, KJ2019A0643, 2020LCX020 and gxyq2020056; by the Yunnan Province project under Grant No.2018FH001-010; and by the CHZU project under Grant No. 2020qd16 and zrjz2019011.

References

[1] H. Hellaoui *et al.*, "Aerial Control System for Spectrum Efficiency in UAV-to-Cellular Communications," *IEEE Commun. Mag.*, vol. 56, no. 10, Oct. 2018, pp. 108–13.

[2] B. Yang *et al.*, "Performance, Fairness and Tradeoff in UAV Swarm Underlaid mmWave Cellular Networks with Directional Antennas," *IEEE Trans. Wireless Commun.*, 2020; available: https://doi.org/10.1109/TWC.2020.3041800.

[3] N. H. Motlagh, M. Bagaa, and T. Taleb, "Energy and Delay Aware Task Assignment Mechanism for UAV-Based IoT Platform," *IEEE Internet Things J.*, vol. 6, no. 4, Aug. 2019, pp. 6523–36.

[4] N. H. Motlagh, T. Taleb, and O. Arouk, "Low-Altitude Unmanned Aerial Vehicles-Based Internet of Things Services: Comprehensive Survey and Future Perspectives," *IEEE Internet of Things J.*, vol. 3, no. 6, Dec. 2016, pp. 899–922.

[5] B. Yang *et al.*, "Spectrum Sharing for Secrecy Performance Enhancement in D2D-Enabled UAV Networks," *IEEE Network*, vol. 34, no. 6, Nov./Dec. 2020, pp. 156–63.

[6] X. Zhou *et al.*, "Joint Optimization of a UAV's Trajectory and Transmit Power for Covert Communications," *IEEE Trans. Signal Process.*, vol. 67, no. 16, Aug. 2019, pp. 4276–90.

[7] C. Wan *et al.*, "Trust Evaluation and Covert Communication-Based Secure Content Delivery for D2D Networks: A Hierarchical Matching Approach," *IEEE Access*, vol. 7, Sep. 2019, pp. 134 838–53.

[8] H. Wang *et al.*, "Secrecy and Covert Communications against UAV Surveillance via Multi-Hop Networks," *IEEE Trans. Commun.*, vol. 68, no. 1, Jan. 2020, pp. 389–401.

[9] B. Bash, D. Goeckel, and D. Towsley, "Limits of Reliable Communication with Low Probability of Detection on AWGN Channels," *IEEE JSAC*, vol. 31, no. 9, Sept. 2013, pp. 1921–30.

[10] M. R. Bloch, "Covert Communication over Noisy Channels: A Resolvability Perspective," *IEEE Trans. Inf. Theory,* vol. 62, no. 5, May 2016, pp. 2334–54.

[11] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental Limits of Communication with Low Probability of Detection," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, June 2016, pp. 3493–3503.

[12] T. X. Zheng *et al.*, "Multi-Antenna Covert Communications in Random Wireless Networks," *IEEE Trans. Wireless Commun.*, vol. 18, no. 3, Mar. 2019, pp. 1974–87.

[13] S. Yan *et al.*, "Delay-Intolerant Covert Communications with Either Fixed or Random Transmit Power," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 1, Jan. 2019, pp. 129–40.

[14] Z. Liu *et al.*, "Covert Wireless Communication in IoT Network: From AWGN Channel to THz Band," *IEEE Internet Things J.*, vol. 7, no. 4, Apr. 2020, pp. 3378–88.

[15] J. Hu *et al.*, "Covert Communication Achieved by a Greedy Relay in Wireless Networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, Jun. 2018, pp. 4766–79.

[16] J. Hu *et al.*, "Covert Transmission with a Self-Sustained Relay," *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, Aug. 2019, pp. 4089–4102.

[17] A. Sheikholeslami *et al.*, "Multi-Hop Routing in Covert Wireless Networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, June 2018, pp. 3656–69.

[18] K. Shahzad *et al.*, "Achieving Covert Wireless Communications Using a Full-Duplex Receiver," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, Dec. 2018, pp. 8517–30.

[19] F. Shu *et al.*, "Delay-Constrained Covert Communications with a Full-Duplex Receiver," *IEEE Wireless Commun. Lett.*, vol. 8, no. 3, Jun. 2019, pp. 813–16.

[20] J. Wang *et al.*, "Covert Communication with the Help of Relay and Channel Uncertainty," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, Feb. 2019, pp. 317–20.

[21] T. V. Sobers *et al.*, "Covert Communication in the Presence of an Uninformed Jammer," *IEEE Trans. Wireless Commun.*, vol. 16, no. 9, Sep. 2017, pp. 6193–6206.

[22] R. Soltani *et al.*, "Covert Wireless Communication with Artificial Noise Generation," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, Nov. 2018, pp. 7252–67.

[23] M. Z. Win *et al.*, "A Mathematical Theory of Network Interference and Its Applications," *Proc. IEEE*, vol. 97, no. 2, Feb. 2009, pp. 205–30.

Biographies

Bin Yang received the Ph.D. degree in systems information science from Future University Hakodate, Japan in 2015. He is a professor with the School of Computer and Information Engineering, Chuzhou University, China, and is also a research fellow with the School of Electrical Engineering, Aalto University, Finland. His research interests include unmanned aerial vehicle networks, cyber security and Internet of Things.

Tarik Taleb received the B.E. degree (with distinction) in information engineering in 2001, and the M.Sc. and Ph.D. degrees in information sciences from Tohoku University, Sendai, Japan, in 2003 and 2005, respectively. He is currently a professor with the School of Electrical Engineering, Aalto University, Espoo, Finland. He is the founder and Director of the MOSA!C Lab.

Yuanyuan Fan received the B.S. degree from Huaibei Normal University, China, in 2004, and the M.S. degree from the Huazhong University of Science and Technology, China, in 2007. She is currently an associate professor with the School of Mathematics and Finance, Chuzhou University, China. Her research interests include wireless networks, applied probability, and cyber security.

Shikai Shen received the B.S. and M.S. Degrees from Yunnan Normal University in 1984 and from Yunnan University in 2003, respectively. He is currently a professor at Kunming University, China. His research interests include wireless sensor networks, cyber security and Internet of Things.