Covert Communication in UAV-Assisted Air-Ground Networks

Xu Jiang, *Member, IEEE*, Xinying Chen, *Graduate Student Member, IEEE*, Jie Tang, *Senior Member, IEEE*, Nan Zhao (Corresponding Author), *Senior Member, IEEE*, Xiu Yin Zhang, *Senior Member, IEEE*, Dusit Niyato, *Fellow, IEEE*, and Kai-Kit Wong, *Fellow, IEEE*

***Abstract*—Unmanned aerial vehicle (UAV) assisted communication is a promising technique for future wireless networks due to its characteristics of low cost and flexible deployment. However, the high possibility of line-of-sight (LoS) air-ground channels may result in a great risk of being attacked by malicious users. Especially compared to the encryption and physical layer security that prevent the eavesdropping, covert communication aims at hiding the existence of transmission, which is able to satisfy the more critical requirement of security. Thus, in this article, we focus on the covert communication issues of UAV-assisted wireless networks. First, the preliminaries of secure communications including encryption, physical layer security and covert communication are discussed. Then, current works and typical applications of UAV in covert communications are demonstrated. Furthermore, we propose two schemes to enhance the covertness of UAV-assisted networks for some typical scenarios. Specifically, to improve the covert rate in UAV-assisted data dissemination, an iterative algorithm is proposed to jointly optimize the time slot, transmit power and trajectory. For the covertness of ground-air communication, a friendly jammer is employed to confuse the wardens, where the location of jammer, the jamming power and the legitimate transmit power are jointly optimized. Numerical results are presented to validate the performance of these two proposed schemes. Finally, several challenges and promising directions are pointed out.**

***Index Terms*—Covert communication, resource allocation, unmanned aerial vehicle, wireless security.**

I. Introduction

Equipped with various small-size sensors and devices, unmanned aerial vehicles (UAVs) are able to perform a wide range of tasks in harsh environments including disaster rescue, surveillance, data gathering, and data relaying. Benefiting from the high altitude, UAVs can establish line-of-sight (LoS) wireless links for air-ground communications, which provide significant performance improvement over the conventional non-line-of-sight (NLoS) terrestrial communications [1]. With flexible deployment and high mobility, UAV-assisted air-ground networks can be deployed on-demand to provide wireless links for disconnected devices, especially in areas without communication infrastructures and in emergency situations. Thus, UAV-assisted wireless networks have aroused tremendous attentions in both industry and academia [2], [3].

By employing UAVs in wireless networks, the coverage and connectivity can be significantly improved. However, the utilization of UAVs brings new challenges for future networks. In particular, the high-quality LoS channels of air-ground communication lead to high possibility of being overheard or attacked due to the good received signal at the malicious adversaries. Since UAVs are frequently deployed to deliver sensitive information, the communication security of UAV-assisted wireless systems is of increasing concern. One of the commonly used techniques for secure transmission is upper-layer encryption. By sharing a secret key between two users, confidential information can be encrypted at the transmitter and decrypted at the receiver. Without the secret key, the illegitimate adversary needs near-infinite computational capacity to decrypt the confidential information. Another technique is the physical layer security. By leveraging the better legitimate channel over the eavesdropping channel, the eavesdropper cannot decode the received message.

However, encryption and physical layer security are not enough to guarantee the security. Once the communication behavior is observed by the adversary, the transmitted data becomes unreliable [4]. On one hand, the behavior of transmitting a signal can arouse suspicion. Thereby the radiation source may be located and physically attacked especially in military applications. On the other hand, the adversary is able to gather part of the confidential information from the received signal by side-channel analysis, even with well-designed encryption and physical layer security [5]. Therefore, the covert communication, also known as low probability of detection/intercept (LPD/LPI) communication, needs to be investigated to provide stealth communication links. Historically, spread spectrum techniques were used to realize covert communication in military applications. However, the covertness of spread spectrum has not been well analyzed. For the covertness analysis of wireless systems, the square root law was founded by Bash *et al.* in additive white Gaussian noise channel, i.e., $O(\sqrt{n})$ bits can be covertly transmitted over n channel uses

X. Jiang, X. Chen and N. Zhao (Corresponding Author) are with the School of Information and Communication Engineering, Dalian University of Technology, Dalian 116024, China, and also with Peng Cheng Laboratory, Shenzhen 518066, China. (e-mail: jiang_xu@dlut.edu.cn, cxy@mail.dlut.edu.cn, zhaonan@dlut.edu.cn).

J. Tang and X.-Y. Zhang are with the School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510641, China. (e-mail: eejtang@scut.edu.cn, zhangxiuyin@scut.edu.cn).

D. Niyato is with the School of Computer Science and Engineering, Nanyang Technological University, Singapore 639798. (e-mail: dniyato@ntu.edu.sg).

K.-K. Wong is with the Department of Electronic and Electrical Engineering, University College London, London WCIE 6BT, U.K. (e-mail: kai-kit.wong@ucl.ac.uk).

This research was supported in part by the National Key R&D Program of China under Grant 2020YFB1807002, the China Postdoctoral Science Foundation under Grant 2020M680949, and the National Natural Science Foundation of China (NSFC) under Grant 61871065. *(Corresponding author: Nan Zhao.)*

TABLE I
COMPARISON OF THREE TYPICAL SECURE COMMUNICATION TECHNIQUES

Technique	Protocol layers	Purpose	Complexity	Limitation	Benefit from employing UAVs
Encryption	Mainly upper layers	Difficulty in unauthorized decryption	High	Key management	Barely no influence
Physical layer security	Physical layer	Degrade eavesdropping quality	Medium	CSI or partial CSI of eavesdropper	Differentiate legitimate and eavesdropping links
Covert communication	Physical layer	Avoid being detected	Low	Priori information of warden	Close to receivers, far from wardens

with arbitrarily small probability of being detected [6]. Since then, the covertness of wireless communications has attracted tremendous research attentions [7], [8].

Existing works have shown that covert communication can be achieved by exploiting interference or noise [8], [9]. However, employing UAV in wireless networks has brought new challenging issues to achieve covert communication. Specifically, the LoS air-ground channels may result in higher possibility of being detected by wardens [10]. Thus, the transmit power and altitude of UAVs need to be properly designed to maximize the covert rate [11]. In addition, exploiting the high mobility of UAV is an important aspect to enhance the covert communication quality [12]. Accordingly, achieving three-dimensional (3D) coverage, high energy efficiency and high reconfigurability in UAV covert communication systems are also challenging issues to be addressed.

Although a few works have been conducted to achieve covertness in UAV-assisted wireless networks [10]–[13], there still exist many challenging problems to be solved. Thus, in this article, we present two typical case studies to enhance the covertness of UAV-assisted networks. In the following sections, we first discuss the main secure communication techniques including encryption, physical layer security and covert communication. Then, we introduce several typical application scenarios of UAV-assisted covert networks. Furthermore, two case studies are carried out to improve the covertness of UAV-assisted networks. In the UAV-assisted multi-user data dissemination case, the time slot, transmit power and trajectory of the UAV are jointly optimized to maximize the covert rate. In the jamming-assisted ground-air communication case, the transmit power and location of the jammer, as well as the transmit power of the legitimate transmitter, are jointly optimized. Several research directions on UAV-assisted covert communications are finally discussed.

II. PRELIMINARIES OF SECURE COMMUNICATION IN UAV-AIDED WIRELESS NETWORKS

Due to the inherent broadcast and open nature, wireless communication faces more secure challenges than wired systems. During the past decades, various techniques for secure wireless communication have emerged. In this section, we discuss the most commonly investigated solutions to secure wireless communications and their applications for UAV-aided wireless networks, including encryption, physical layer security and covert communication.

A. Encryption

Encryption mainly happens in upper layers, including medium-access control (MAC) layer, network layer, transport layer, *etc*. For communication systems employing the encryption technique, the source data are encrypted with a secret key before transmission. The receiver can decrypt the received data with the same key. For the unauthenticated user, near-infinite computational capacity is needed for decryption when well-designed encryption is employed, and thus the data transmission security can be guaranteed accordingly. However, the encryption cannot always guarantee the security. For example, if the legitimate user does not have the secret key, a secret channel needs to be established to share it, which increases the risk of being overheard. Besides, non-computational methods such as side channel analysis can be employed by the adversary to gather confidential data without the secret key. In addition, the encrypted systems may be also threatened by brute-force methods such as quantum attack. Since the encryption is mainly utilized in upper layers, employing UAVs does not have much influence on the decryption performance of the adversaries, but have influence on the received quality.

B. Physical Layer Security

Physical layer security is able to guarantee the security at information-theoretic level in the presence of an eavesdropper. When the eavesdropper receives a degraded version of the legitimate signal, it may be completely confused about the confidential message, i.e., it is no better than receiving no signal at all. In physical layer security, the secrecy capacity can be expressed as $C = \max I(X;Y) - I(X;Z)$, where X is the channel input, Y and Z are the channel output at the legitimate receiver and the eavesdropper, respectively. This expression implies that physical layer security is a relative concept, i.e., the secrecy capacity is expressed by the difference of achievable rates between the legitimate link and the eavesdropping link. In conventional terrestrial wireless networks, physical layer security can be enhanced by proper power allocation or beamforming, usually with channel state information (CSI) or partial CSI of the eavesdropper.

For physical layer security in UAV-assisted wireless networks, more gains can be achieved by exploiting the characteristics of UAV. First, by choosing proper hovering position or flying with carefully designed trajectory, the distance of the legitimate link can be reduced and thus the probability of LoS channel can be enhanced. Then, the link distance of

TABLE II
CURRENT RESEARCH ON COVERT COMMUNICATION IN UAV-ASSISTED WIRELESS NETWORKS

Publication year	Reference number	Main feature	Role of UAVs
2020	[10]	Detecting UAV's transmission by a terrestrial warden	Transmitter
2019	[11]	Hiding UAV's transmission from a terrestrial warden	Transmitter
2019	[12]	Trajectory and power optimization for UAV's covert transmission	Transmitter
2020	[13]	Hiding terrestrial multi-hop transmission from an aerial warden	Warden
2020	[14]	Enhancing terrestrial covert communication by UAV-aided jamming	Jammer
2019	[15]	Collecting data and jamming the wardens by UAV	Jammer & Receiver

eavesdropping channel can be expanded and the probability of NLoS illegitimate transmission can be increased. In other words, with swiftly deployment and high mobility, the UAV is able to improve the difference between the legitimate channel and the eavesdropping channel, which results in a significant improvement of security.

C. Covert Communication

Covert communication is an advanced level of security requirement. Not only the content of the confidential message cannot be decoded by the adversary, but also the existence of confidential wireless transmission should not be noticed. This is a critical requirement, since the existence of a wireless signal can be easily detected by a radiometer with energy detection. During the past decades, spread spectrum is the most widely used technique with low probability of detection. The spectrum of the original signal is spread into a signal with wide spectrum and low-power spectral density, which looks like white noise at the receiver side. Since spread spectrum techniques also have the advantage of resisting interference, it is commonly utilized in military communications.

However, there is barely no analytical study on the covertness of spread spectrum systems. We only know that the probability of being detected increases with the average transmit power. The famous square root law of covert communication was proposed in 2013 by Bash *et al.* [6], which revealed that no more than $O(\sqrt{n})$ bits can be covertly transmitted in AWGN channel over n channel uses. This implies zero covert communication since $\lim_{n\to\infty} \sqrt{n}/n = 0$. Besides the AWGN channel, the covert communications with friendly jamming, noise uncertainty, and in interference environment have aroused a lot of research attentions, and more gains can be achieved [8], [9].

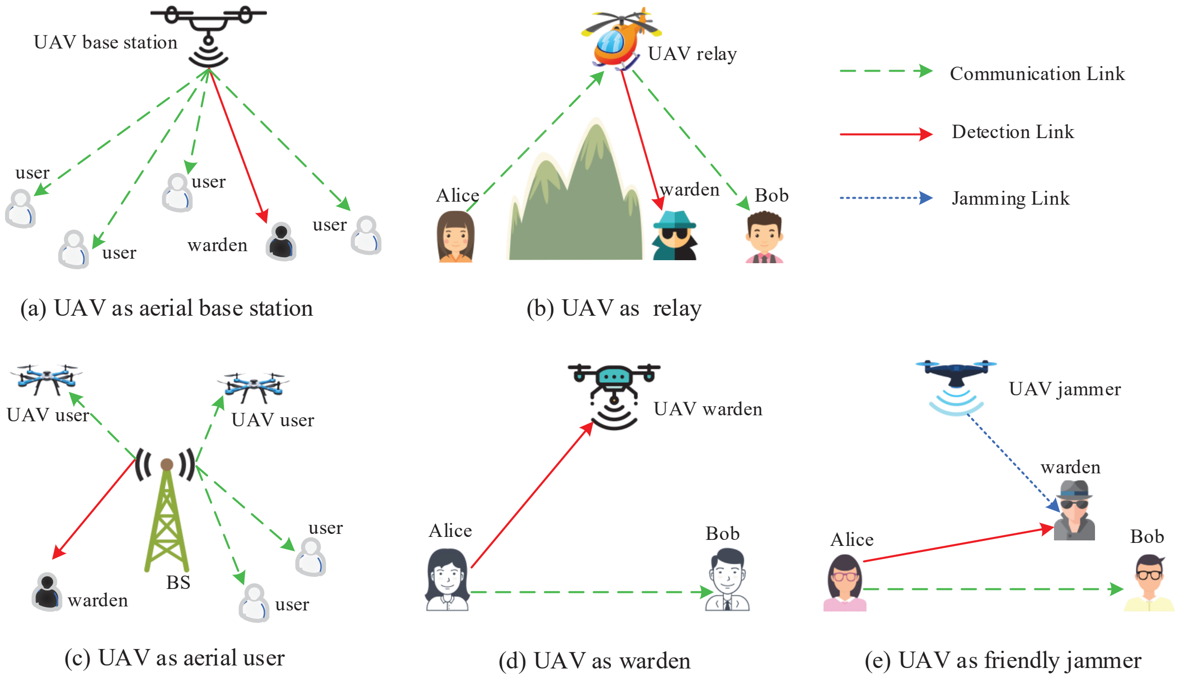
For UAV-assisted communication systems, the influence of employing UAV as a transmitter has two sides. On one hand, the mobility of UAV can be exploited to weaken the received signal at the warden. On the other hand, the high-quality LoS channels may increase the probability of being detected compared with conventional terrestrial NLoS channels. In addition, the UAV can also be employed as a receiver, which requires low transmit power due to the LoS environment. This is a favorable condition for covert communications. Other applications of UAV for covert communications include friendly jamming and working as a warden. By taking advantages of high altitude and flexible mobility, more gains can be achieved by UAVs comparing to conventional terrestrial devices.

In summary, a comparison of encryption, physical layer security and covert communication are listed in Table I. In practical wireless networks, the three above-mentioned techniques are not mutually exclusive. They can work jointly to enhance the security of wireless networks, especially in UAV-assisted networks.

III. TYPICAL APPLICATIONS OF UAV FOR COVERT COMMUNICATIONS

The above discussions have shown that the covertness of UAV-assisted networks can be enhanced by exploiting the mobility of UAV and the LoS air-ground channels. However, the UAV-assisted covert communication is still in its infancy stage, and the existing research works are listed in Table II. In [10], the beam sweeping based detection of a UAV's transmission by a terrestrial warden with multiple antennas was investigated, where the closed-form detection error probability and a low-complexity approximation were derived to reveal the performance. In [11], assuming that the warden locates at the projection of the UAV on the horizontal plane, the air-ground transmission quality under the covertness constraint was optimized. The covert rate of air-ground communication was enhanced by jointly optimizing the trajectory and transmit power in [12]. In [13], the covert throughput of terrestrial multi-hop communication was maximized with a UAV as an aerial warden. In [14], the covertness performance of terrestrial system with a UAV as a friendly jammer was analyzed in both the AWGN channel and Nakagami-m channel. In [15], a full-duplex UAV-enabled covert data collecting system was investigated by optimizing the trajectory and jamming power of UAV. Thus, with the high altitude and swift deployment, UAVs will have a lot of applications in future covert wireless networks. Fig. 1 shows several typical scenarios of UAV-assisted covert communications, which are introduced as follows.

- *UAV as aerial base station*: In harsh environments or in emergency situations, the UAV can be employed as an aerial base station (BS) to serve ground users. Through caching, the UAV is able to serve these users without backhaul links. In addition, the UAV-enabled base station can also provide edge computing service. However, the air-ground communications are vulnerable to malicious wardens. To avoid being detected by the warden and provide reliable transmission performance, the UAV can



(a) UAV as aerial base station

(b) UAV as relay

(c) UAV as aerial user

(d) UAV as warden

(e) UAV as friendly jammer

Fig. 1. Typical applications of UAVs in covert communication systems.

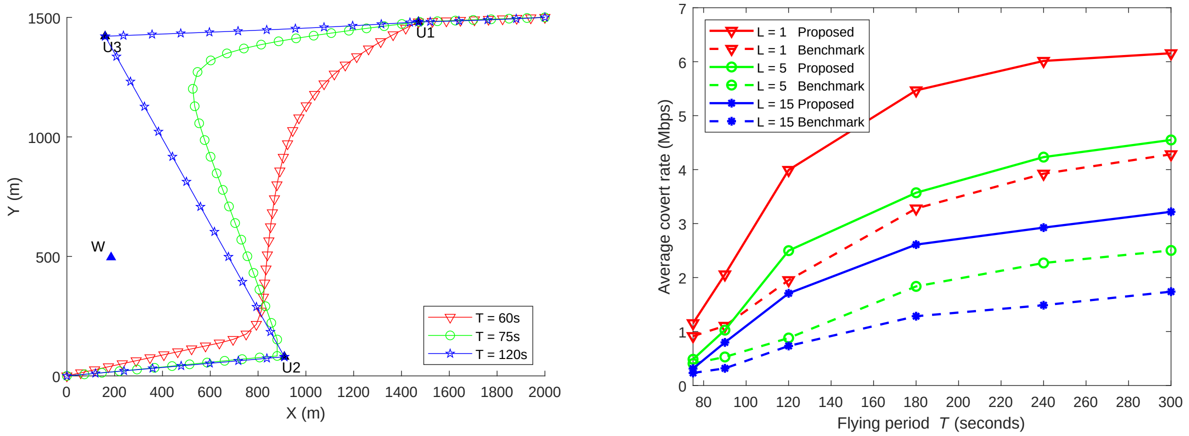
flexibly adjust its hovering position or trajectory, to fly away from the warden and close to the target user.

- *UAV as relay*: When there is no terrestrial communication infrastructure, e.g., the distance is too long, or the link is blocked, the UAV can be deployed as a mobile relay to connect two isolated terrestrial users. When relaying confidential messages, the transmission of UAV faces more secure threat due to the LoS air-ground links, especially in military applications. Thus, in the presence of a warden, the UAV should choose proper relay location to provide covert communication links.
- *UAV as aerial user*: When there exists communication infrastructure on the ground, the UAV can work as an aerial user to keep connected to the existing terrestrial network. When the UAV is executing confidential tasks, the covert ground-air communication is also a crucial issue. Proper UAV trajectory and communication optimization can enhance the covertness of this ground-air communication system. In addition, friendly jammers can also be deployed to enhance the covertness of ground-air communication.
- *UAV as warden*: UAV can be employed as an aerial warden to detect suspicious transmission on the ground. Since the UAV flies at high altitude, employing UAV as a warden can take advantage of LoS ground-air channels to achieve better detection performance. Furthermore, the high mobility enables UAV to fly towards the suspicious user to ensure short link distance. Therefore, the aerial warden can achieve better detection performance than conventional terrestrial wardens due to the high-quality received signal.
- *UAV as friendly jammer*: The excellent LoS channel and high mobility is also helpful for the UAV to disrupt malicious terrestrial wardens. However, the legitimate link may also be jammed because of the open nature of wireless communication. Under this scenario, the jamming location and power need to be carefully designed to enhance the covertness of legitimate communication without affecting the transmission quality.

Although the UAV-assisted covert communications face several challenges in various scenarios, only a few of them have been investigated in literature, as shown in Table II. In the following two sections, two typical case studies are presented to enhance the covertness of UAV-assisted communications, by optimizing the resource of UAV and by leveraging a friendly jammer, respectively.

IV. UAV-Assisted Multi-User Data Dissemination

One typical application of UAV-assisted covert communication is data dissemination in harsh environments, as shown in Fig. 1(a). In some critical scenarios such as military applications, the employment of UAV is useful to reduce pilot losses. In this case, the UAV's transmitted signal can be hidden in the background noise. To avoid being detected by the adversary, radio resource and UAV's hovering position/trajectory need to be carefully designed. To evaluate the covertness, the total detection error probability ξ is commonly used as the performance metric, which can be given by $\xi = P_{fa} + P_{md}$, where P_{fa} is the false alarm probability and P_{md} is the miss detection probability. When $\xi \geq 1 - \epsilon$ for any $\epsilon > 0$, we can conclude that covert communication can be achieved. It is worth noting that this covertness metric implies that the



(a) Optimized trajectories with different values of flying period T.

(b) Optimized average covert rate with different values of flying period T and number of observations L.

Fig. 2. Optimized trajectory and covert rate for the UAV-assisted multi-user data dissemination scheme.

warden assumes equal probability that the UAV is transmitting or not.

A. Problem Formulation

Consider the scenario that the UAV serves K ground users in a time division multiple access manner, and the time slots can be allocated to the user when the UAV flies close to it. This joint design of time slot and trajectory can obtain more gain than conventional terrestrial systems with fixed node positions. In addition, with carefully optimized transmit power for each location of UAV, the transmission rate can be maximized under the covertness constraint. Therefore, we propose a joint time slot, transmit power and trajectory optimization approach to maximize the average communication rate under the covertness constraint, which is termed as the covert rate.

To avoid obstacles and provide LoS links, the UAV is assumed to fly at a high altitude. On the other hand, to reduce the air-ground distance, it is favorable for the UAV to fly at a low altitude. Therefore, the altitude of UAV has a tradeoff between the LoS probability and link distance, which needs to be carefully chosen.

For tractability of analysis, the flying period of the UAV is equally divided into multiple time slots. It is assumed that the warden can have L observations in each time slot, where L is a limited positive integer. We also assume that the UAV does not know the exact position of the warden, i.e., the position of the warden satisfies $(x_w - x_e)^2 + (y_w - y_e)^2 \leq r^2$, where (x_w, y_w) is the horizontal coordinate of the warden, (x_e, y_e) is the estimated location, and r is the radius of the maximum estimation error. Therefore, we consider the robust covert UAV-assisted data dissemination under the worst-case of the warden's location uncertainty.

First, the detection performance of the warden is analyzed. Since the warden has no prior information of the UAV's transmission, energy detection is employed. For ease of analysis, the covertness constraint is transformed into the constraint on the received power at the warden. Then, the worst-case covertness constraint under the location uncertainty of warden is approximated into a more tractable form. Specifically, since the location uncertainty and the worst-case covertness constraint are both quadratic, they can be transformed into semi-definite constraints approximately. Finally, the time slot allocation can be relaxed in to a convex one, the power allocation is convex, and the trajectory optimization problem can be solved by semi-definite programming. Based on the above, an efficient block coordinate descent based algorithm is developed to optimize the time slot, transmit power and trajectory iteratively. Thus, the robust covert communication for UAV-assisted multi-user data dissemination can be achieved.

B. Simulation Results

Simulation results are presented to demonstrate the effectiveness of the proposed joint optimization algorithm. Consider 3 ground users and one warden that locate in a rectangular area shown in Fig. 2(a). The initial and final locations of UAV are $(0, 0, H)$ and $(2000, 1500, H)$ in meters, respectively. The UAV flies at a fixed altitude $H = 100$ m with the maximum speed of 50 m/s. The tolerance of being detected is $\epsilon = 0.05$. The radius of the warden's location uncertainty is $r = 50$ m.

In Fig. 2(a), when $L = 5$, three trajectories under different flying period of UAV T are presented. It can be seen that as T increases, the UAV has more freedom to fly close to the target user to obtain better air-ground channels. We can also see that the UAV tries to fly away from the warden to avoid being detected in each trajectory. In Fig. 2(b), the average covert rate versus different values of T is demonstrated with $L = 1, 5$ and 15. A benchmark scheme is given, where the time and trajectory are optimized without considering the warden according to [2], with the maximum transmit power satisfying the covertness constraint. It is shown that the proposed scheme outperforms the benchmark for each value of T and L. Since when T is larger, the UAV has more freedom to design its trajectory, we can see that higher covert rate can be achieved with larger T. In addition, when L increases, the average covert rate decreases. This is because more information can be

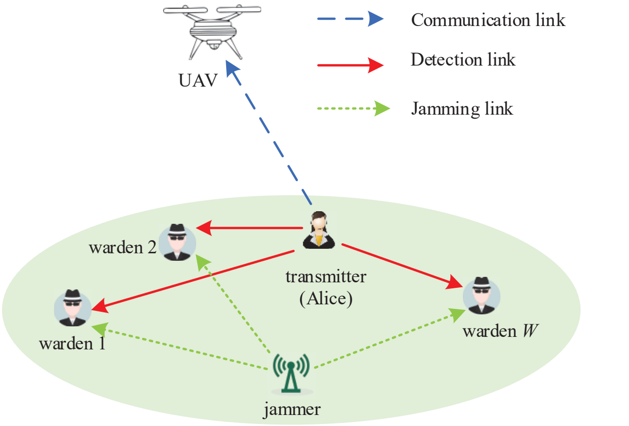


Fig. 3. Ground-air covert communication with multiple wardens and a friendly multi-antenna jammer.

gathered with more observations, and the warden can achieve better detection performance accordingly.

V. Jamming-Assisted UAV Covert Communication

When the UAV works as an aerial receiver, the ground-air communication may be monitored by one or more wardens on the ground. Considering the covert ground-air communication when there exist multiple wardens, a friendly jammer can be utilized to further interfere the detection of the wardens. To achieve covert UAV communication, the location of jammer, the jamming power and the legitimate transmit power need to be carefully designed.

A. Problem Formulation

Consider the communication system shown in Fig. 3, where a ground user Alice with M antennas performs transmission to a UAV in the air, and W malicious wardens on the ground are detecting the transmission of the ground Alice. A friendly jammer with N antennas is employed to enhance the covertness of such a ground-air communication. In this case, we assume that each warden keeps listening and has infinite number of observations.

First, the global detection performance at the wardens is analyzed. Since the W wardens detect the transmission of Alice independently, the global detection outage probability is the expectation of the multiplication of all the wardens' detection outage probability. This implies that when there are more wardens, the detection outage probability decreases. Besides, although the number of antennas at Alice and jammer has no influence on wardens' detection performance, employing multiple antennas is helpful to eliminate the jamming signal at the UAV by zero-forcing.

Based on the detection performance of wardens, the covert rate can be maximized by optimizing the location and transmit power of the jammer, as well as the transmit power of Alice accordingly. It can be seen that the global detection outage probability increases with the jamming power. Since the jamming signal can be cancelled at the UAV via zero-forcing, only the wardens are influenced by the jammer. Thus, the jamming power should be as high as possible to enhance the covertness. To weaken all the wardens' detection performance by jamming, we find that the optimal jamming location is at the geometric center of wardens. For the UAV, the optimal hovering location is above the geometric center of wardens. Since the detection outage probability decreases with higher transmit power of Alice, the transmit power should be maximized to achieve maximum covert rate with the covertness constraint satisfied.

B. Simulation Results

Simulation results are carried out to evaluate the proposed scheme. The path-loss exponent of the ground-air channel and terrestrial channels are 2 and 3, respectively. The altitude of UAV is 100m.

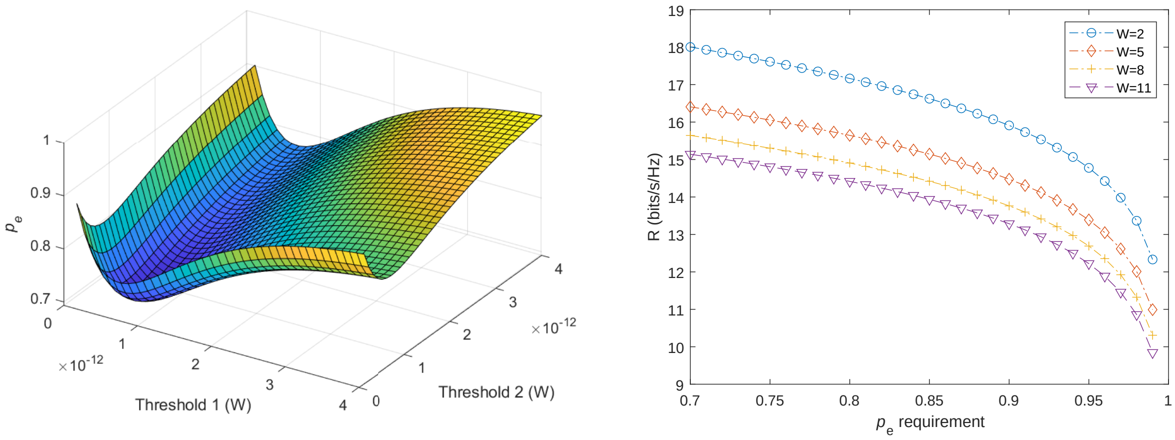
Fig. 4(a) demonstrates the detection outage probability with different detection thresholds for two of the wardens. The transmitter Alice has 10 antennas and its transmit power is 10 mW. The jammer has 8 antennas and its transmit power is 30 mW. It can be seen that the detection outage probability varies dynamically with the detection thresholds, and there exists a set of optimal thresholds for the wardens. It can be also observed that each warden has its own optimal detection threshold, which can be obtained in the closed-form expression.

Fig. 4(b) provides the curves of the maximized covert rate, where Alice has 10 antennas and the jammer has 8 antennas. The jammer locates at its optimal location and the jamming power is 1 W. The results with different number of wardens $W = 2$, 5, 8 and 11 are shown. It can be concluded that the maximized covert rate decreases when the requirement of detection outage probability increases. In addition, it can be also concluded that when there exist more wardens, it becomes more difficult to hold high transmission rate and guarantee the covertness simultaneously.

VI. Challenges and Future Directions

Although some of the issues in covert UAV-assisted wireless networks have been addressed above, there still remain some challenges to be solved as follows.

- *Interference-aware UAV covert communication*: Present works on covert UAV-assisted networks mainly consider the influence of noise. However, future wireless networks are expected to be more dynamic and heterogeneous. Users in the network experience not only noise, but also the aggregated interference from other sources. For UAV-assisted systems, the LoS-dominant wireless channels lead to higher received power of interference, which becomes a critical issue in future networks. Although suffering from the interference, it has been shown that interference may be beneficial for covertness communication [8]. The UAV covert communication in such an interference-limited environment has not been well investigated.
- *3D UAV deployment for covert communication*: Benefiting from the characteristics of flexible deployment, UAV can fly close to legitimate nodes to achieve LoS channels



(a) Global detection outage probability when two of the wardens adopt different detection thresholds.

(b) Maximized rate R under different detection outage probability requirements p_e and number of wardens W.

Fig. 4. Detection outage probability and covert rate for the jamming-assisted UAV covert communication scheme.

and short distance, which results in better channel gain. The UAV can also fly away from the warden to degrade the detection channel, which is helpful to decrease the probability of detection. However, the existing literature mainly considers the deployment of UAV in a two-dimensional (2D) horizontal plane. The altitude of UAV also has a significant influence on the covert communication performance. Thus, more efforts should be focused on the 3D deployment and trajectory design of UAV to achieve covert communication.

- *Energy-efficient UAV covert communication*: UAVs are usually equipped with limited batteries, which have to provide energy for propulsion and communication simultaneously. Thus, the energy-efficient covert communication is a challenging issue. On one hand, to save energy for communication, the UAV needs to exploit its flexible mobility to achieve better channel for covert communication. On the other hand, UAV's trajectory needs to be carefully designed to save energy for propulsion. In addition, the fixed-wing UAV may be more energy-efficient for propulsion than the rotary-wing UAV, but cannot hover at a fixed location. Thus, different UAVs should be carefully utilized based on specific requirements.
- *UAV covert communication in NLoS environment*: Since the UAV flies in the air, it is reasonable to have LoS links for the air-ground communications. However, when the UAV performs the transmission in NLoS environments, it will become more complicated. Thus, the detection performance of the warden will be degraded, and the communication quality of the legitimate link may be also impaired. The influence of small-scale fading, as well as the shadow effect on the performance of the UAV-assisted covert wireless networks, has not been fully investigated yet, which still remains as an open problem.
- *UAV covert communication with imperfect CSI*: Previous works mainly consider the covert communication of UAV-assisted networks with perfect CSI. In practice, it is difficult to obtain the CSI at the transmitter. When the CSI is estimated at the receiver, additional feedback link is required to send it back to the transmitter. Furthermore, since the warden is a malicious node, the CSI of the detection channel is more difficult to estimate. In some cases, the legitimate network can only obtain partial information of the warden. Thus, the covert UAV communication with imperfect CSI, especially with imperfect CSI of the detection channel, is still a challenge.

VII. Conclusion

Covertness is a higher level of secure requirement for wireless communication than conventional encryption and physical layer security. In this article, we first introduce the basics of encryption, physical layer security and covert communication. Then, the covert communication of UAV-assisted networks are investigated, with several typical applications of UAV in covert communication discussed. In addition, two typical schemes for UAV-assisted covert networks are proposed, i.e., UAV-assisted multi-user covert data dissemination and jamming-assisted ground-air covert communication with multiple wardens. The solutions and simulation results of these two case studies are presented. Finally, several challenging problems and directions are also pointed out for UAV-assisted covert networks.

References

[1] N. Zhao, W. Lu, M. Sheng, Y. Chen, J. Tang, F. R. Yu, and K. Wong, "UAV-assisted emergency networks in disasters," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 45–51, Feb. 2019.

[2] Y. Zeng, Q. Wu, and R. Zhang, "Accessing from the sky: A tutorial on UAV communications for 5G and beyond," *Proc. IEEE*, vol. 107, no. 12, pp. 2327–2375, Dec. 2019.

[3] H. Wu, X. Tao, N. Zhang, and X. Shen, "Cooperative UAV cluster-assisted terrestrial cellular networks for ubiquitous coverage," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 9, pp. 2045–2058, Sept. 2018.

[4] L. Zhou, D. Wu, X. Wei, and Z. Dong, "Seeing isn't believing: QoE evaluation for privacy-aware users," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 7, pp. 1656–1665, July 2019.

[5] Y. Xun, J. Liu, and Y. Zhang, "Side-channel analysis for intelligent and connected vehicle security: A new perspective," *IEEE Netw.*, vol. 34, no. 2, pp. 150–157, Mar. 2020.

[6] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1921–1930, Sept. 2013.

[7] S. Yan, X. Zhou, J. Hu, and S. V. Hanly, "Low probability of detection communication: Opportunities and challenges," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 19–25, Oct. 2019.

[8] Z. Liu, J. Liu, Y. Zeng, and J. Ma, "Covert wireless communications in IoT systems: Hiding information in interference," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 46–52, Dec. 2018.

[9] B. He, S. Yan, X. Zhou, and V. K. N. Lau, "On covert communication with noise uncertainty," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 941–944, Apr. 2017.

[10] J. Hu, Y. Wu, R. Chen, F. Shu, and J. Wang, "Optimal detection of UAV's transmission with beam sweeping in covert wireless networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 1080–1085, Jan. 2020.

[11] S. Yan, S. V. Hanly, I. B. Collings, and D. L. Goeckel, "Hiding unmanned aerial vehicles for wireless transmissions by covert communications," in *Proc. IEEE ICC*, Shanghai, China, Jul. 2019, pp. 1–6.

[12] X. Zhou, S. Yan, J. Hu, J. Sun, J. Li, and F. Shu, "Joint optimization of a UAV's trajectory and transmit power for covert communications," *IEEE Trans. Signal Process.*, vol. 67, no. 16, pp. 4276–4290, Aug. 2019.

[13] H. Wang, Y. Zhang, X. Zhang, and Z. Li, "Secrecy and covert communications against UAV surveillance via multi-hop networks," *IEEE Trans. Commun.*, vol. 68, no. 1, pp. 389–401, Jan. 2020.

[14] W. Liang, J. Shi, Z. Tie, and F. Yang, "Performance analysis for UAV-jammer aided covert communication," *IEEE Access*, vol. 8, pp. 111 394–111 400, Jun. 2020.

[15] X. Zhou, S. Yan, F. Shu, R. Chen, and J. Li, "Covert wireless data collection based on unmanned aerial vehicles," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Waikoloa, HI, USA, Mar. 2019, pp. 1–6.

Biographies

Xu Jiang [M] (jiang_xu@dlut.edu.cn) received the B.Eng. degree in electronics and information engineering, the M.Sc., and Ph.D. degrees in information and communication engineering, from Harbin Institute of Technology in 2012, 2015 and 2020, respectively. He is currently a postdoctoral researcher with Dalian University of Technology, China. His research interests include UAV communications, covert communications, and physical-layer security.

Xinying Chen [GSM] (cxy@mail.dlut.edu.cn) received her B.Eng. degree in electronic information engineering from Dalian University of Technology in 2015 and M.Sc. degree in communication engineering from Beijing University of Posts and Telecommunications in 2018. She is currently pursuing the Ph.D. degree in information and telecommunication with Dalian University of Technology, China. Her research interests include covert communications, physical-layer security in NOMA, SDWN routing.

Jie Tang [SM] (eejtang@scut.edu.cn) received the B.Eng. degree in Information Engineering from the South China University of Technology, Guangzhou, China, in 2008, the M.Sc. degree in Communication Systems and Signal Processing from the University of Bristol, UK, in 2009, and the Ph.D. degree from Loughborough University, Leicestershire, UK, in 2012. From 2013 to 2015, he was a research associate at the School of Electrical and Electronic Engineering, University of Manchester, UK. He is currently a full professor at the School of Electronic and Information Engineering, South China University of Technology, China. He is currently serving as an Editor for IEEE Systems Journal and IEEE Wireless Communications Letters.

Nan Zhao [SM] (zhaonan@dlut.edu.cn) is a Professor at Dalian University of Technology, China. He received the Ph.D. degree in information and communication engineering in 2011, from Harbin Institute of Technology, Harbin, China. He received the IEEE Communications Society Asia Pacific Board Outstanding Young Researcher Award in 2018. He is an Editor for IEEE Wireless Communications (magazine) and IEEE Wireless Communications Letters.

Xiu Yin Zhang [SM] (zhangxiuyin@scut.edu.cn) received the PhD degree in electronic engineering from City University of Hong Kong, China, in 2009. He joined South China University of Technology in 2010, where he is currently a full professor and vice dean with the School of Electronic and Information Engineering. He has authored or coauthored more than 150 internationally referred journal papers (including more than 90 IEEE Transactions) and 80 conference papers. His research interests include antennas and arrays, MMIC, RF components and sub-systems, wireless sensing and communications. He is an Associate Editor for IEEE AWPL, APM, OJAP and Access.

Dusit Niyato [F] (dniyato@ntu.edu.sg) is currently a professor in the School of Computer Science and Engineering, at Nanyang Technological University, Singapore. He received B.Eng. from King Mongkuts Institute of Technology Ladkrabang (KMITL), Thailand in 1999 and Ph.D. in Electrical and Computer Engineering from the University of Manitoba, Canada in 2008. His research interests are in the areas of Internet of Things (IoT), machine learning, and incentive mechanism design.

Kai-Kit Wong [F] (kai-kit.wong@ucl.ac.uk) received the BEng, the MPhil, and the PhD degrees, all in Electrical and Electronic Engineering, from the Hong Kong University of Science and Technology, Hong Kong, in 1996, 1998, and 2001, respectively. After graduation, he took up academic and research positions at the University of Hong Kong, Lucent Technologies, Bell-Labs, Holmdel, the Smart Antennas Research Group of Stanford University, and the University of Hull, UK. He is Chair in Wireless Communications at the Department of Electronic and Electrical Engineering, University College London, UK. His current research centers around 5G and beyond mobile communications. He is a co-recipient of the 2013 IEEE Signal Processing Letters Best Paper Award and the 2000 IEEE VTS Japan Chapter Award at the IEEE Vehicular Technology Conference in Japan in 2000, and a few other international best paper awards. He is Fellow of IEEE and IET and is also on the editorial board of several international journals. He is the Editor-in-Chief for IEEE Wireless Communications Letters since 2020.