Covert Communication for Cellular and X2U-Enabled UAV Networks with Active and Passive Wardens

Bin Yang, Tarik Taleb, Guilin Chen and Shikai Shen

***Abstract*—Cellular and X2U-enabled UAV networks are a promising network paradigm to support constantly growing Internet of Things (IoT) applications in 5G and beyond wireless networks, wherein X2U includes the UAV-to-UAV (U2U) and ground IoT device-to-UAV (G2U) communications. However, such networks pose a significant challenge to secure wireless communications due to the open and broadcasting features of wireless channels. Covert communication is an attractive technique to hinder adversaries (i.e., wardens) from detecting the existence of data transmission for guaranteeing secure IoT communications. This article investigates the covert communication issue for a promising network scenario consisting of a BS, UAV swarm, multiple ground IoT devices and wardens. Especially, each UAV/ground IoT device can select cellular or X2U communication mode according to a flexible mode selection scheme which can cover the cellular network and ad hoc network as special cases by setting a bias factor. We design two types of wardens: active wardens who not only detect the legitimate transmission but also jet noise to interfere with legitimate signals, and passive wardens who only detect the legitimate transmission. Cooperative jamming technique is further employed to resist the attacks of wardens. Then, numerical results are provided to explore the effects of the flexible mode selection and the number of wardens on the covert performances like covert capacity and detection error probability. We finally present a vision for future research in the cellular and X2U-enabled UAV networks.**

***Index Terms*—UAV, Covert communication, mode selection, active and passive wardens, covert performance.**

I. Introduction

Unmanned aerial vehicle (UAV) networks, which bring many distinguishing characteristics such as high mobility, low cost and swift deployment, have been viewed as a key component of 5G and beyond wireless networks [1].Traditional UAV networks mainly perform simple point-to-point communications in a limited range over the unlicensed spectrum (e.g., ISM 2.4 GHZ), which are difficult to provide services with high data rates, reliability and security. Therefore, it will severely hinder large-scale deployment of such networks.

B. Yang is with the School of Computer and Information Engineering, Chuzhou University, Chuzhou, China, and is also with the School of Electrical Engineering, Aalto University, Espoo, Finland. E-mail: yangbinchi@gmail.com.

T. Taleb is with the School of Electrical Engineering, Aalto University, Finland, with the Information Technology and Electrical Engineering, Oulu University, Finland, and with the Department of Computer and Information Security, Sejong University, South Korea. E-mail: talebtarik@gmail.com.

G. Chen is with the School of Computer and Information Engineering, Chuzhou University, Chuzhou, China. E-mail: glchen@ah.edu.cn.

S. Shen is with the School of Information and Technology, Kunming University, Kunming, China. E-mail: kmssk2000@sina.com.

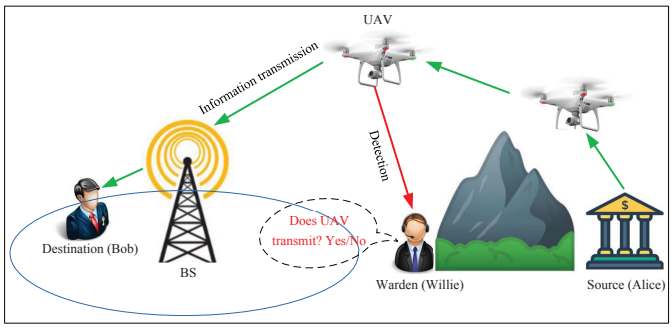


Fig. 1. An example of covert communication

Different from the networks, cellular and X2U-enabled UAV networks are an appealing network architecture for supporting a wide range of Internet of Things (IoT) applications such as air/water quality monitoring, target detection, video surveillance, precision agriculture, etc [2]. With the assistance of almost ubiquitous base stations (BSs) all over the world, people can remotely control UAVs and UAVs can also send their collected data to distant servers for further processing over the licensed spectrum. Furthermore, X2U communications enable nearby UAVs/ground IoT devices to directly communicate without passing by BSs, wherein X2U communications include the communication from a UAV to another one (i.e., U2U) and that from a ground IoT device to a UAV (i.e., G2U). Such direct communications can provide many benefits like high data rate, low delay, low energy consumption and mobile edge computing specially in disaster areas, emergency relief and battle fields without the support of BSs.

However, thanks to the open and broadcast nature of wireless channels, information transmissions suffer from serious security threats in the presence of adversaries. To guarantee secure communications, cryptography-based security techniques have been widely adopted. These techniques pose significant challenges of key management and high complex computation to the dramatic UAV networks with limited energy. Different from them, physical layer security (PLS) is to utilize the randomness characteristic of wireless channels to prevent transmitting information from being eavesdropped by adversaries. Using PLS technique, adversaries still have the ability to find the existence of wireless transmissions. However, many critical organizations (e.g., military and government) are highly desirable to prevent wireless transmissions from being

detected by enemies/illegal users.

Remarkably, covert communication is an appealing technique to conceal the information transmission from watchful wardens, which provides strong security protection for various security-sensitive critical applications. As illustrated in Fig. 1, source Alice intends to covertly send important private information to a remote destination Bob with the help of UAVs and BS, while the warden Willie detects whether the UAV performs the operation of wireless transmission. Once Willie detects the existence of wireless transmission, Willie and his accomplices can further launch an attack on the UAV. Existing works on the studies of covert communication mainly consider the network scenario where all communication devices in these works are distributed on the ground without the assistance of UAV (see Related Works in Section II). So far, only very few works have devoted to exploring the covert communication issues in wireless networks with the support of one UAV [3], [4]. Notice that all previous works on the covert communications consider either a ground network scenario including a source-destination pair and a warden on the ground or a UAV-enabled network scenario including a UAV source, a ground destination and a warden. Meanwhile, the warden in these works can only passively detect the existence of wireless communications. Multiple wardens usually exist in a real environment, where each warden acts as not only a passive detector but also an active attacker who sends a jamming signal to prevent the legitimate information from being received by the destination. Besides, a UAV is more likely to perform a simple task due to a limited on-board sensors and energy. Recently, we study covert communication performance in a multiple UAVs-assisted network scenario, where each warden is only a passive detector [5].

Different from the above works, this article proposes a cellular and X2U-enabled UAV network scenario consisting of a UAV swarm, multiple ground IoT devices, passive wardens, active wardens and a BS, where the UAV swarm can work cooperatively to achieve a complex task, and the two types of wardens coexist in the network. Specially, each UAV/ground IoT device can select cellular or X2U communication mode based on a flexible mode selection scheme. Here, cellular mode includes the communications from ground IoT devices to BS (i.e.,G2B), and the ones from UAVs to BS (i.e.,U2B); X2U communication mode includes the communications from ground IoT devices to UAVs (i.e.,G2U), and the ones from UAVs to UAVs (i.e.,U2U). This scheme is general because it can cover the cellular network and ad hoc network as special cases by setting a bias factor.

The proposed network scenario is envisioned to play a significant role in IoT systems. For example, UAVs equipped with IoT devices need to send frequent measurements via U2U or U2B communication. In addition, UAVs also need to collect measurements from ground IoT devices via G2U or G2B communication. For the G2B communication, it can deplete the lifetime of the IoT devices quickly, mainly those being far away from the BS. We then consider each warden can serve as not only a passive one but also an active one jetting noise to interfere with legitimate signals based on a v-nearest neighbors based strategy, wherein if the number of legitimate receivers in a sphere centering on the location of warden is at least v, the warden serves as an active one; otherwise it is a passive one. Numerical results are provided to investigate the effects of the flexible mode selection and two types of wardens on the covert performances, i.e., covert capacity and detection error probability. Finally, some interesting research directions are presented in such networks. It is notable that there are three differences between this work and our previous work [5]. Firstly, our previous work only considers the passive wardens detecting the existence of wireless transmissions through their received signal. However, in reality, these wardens are also often active that can emit noise to interfere with the legitimate receivers. Thus, this work proposes a more general scenario in the presence of passive and active wardens. Secondly, this work proposes a more flexible mode selection scheme that can cover the received signal strength-based mode selection scheme in [5] as special case by setting a bias factor. Thirdly, this work proposes a promising cooperative jamming scheme, with which the friendly jammers emit artificial noise to confuse the detection of wardens and can reduce the interference with the legitimate receivers as much as possible simultaneously. However, under the cooperative jamming scheme in [5], the artificial noise can not only confuse the wardens but also hurt the legitimate receivers which may degrade the covert performance.

II. Related Works

This section reviews the related works for covert communication with/without the assistance of UAV.

A. Covert Communication without UAV

In a wireless network including ground devices, a source intends to covertly send information to its destination, while a warden tries to detect whether the transmission process occurs or not. The pioneering work in [6] presented a square root limit that the source can send information to its destination with low detection probability under Gaussian noise channels. Later, this result was proven to be suitable for various channels, such as multiple access channels, binary symmetric channels, discrete memoryless channels, etc [7].Recently, the work of [8] illustrated the random transmit power at a source can significantly enhance the covert capacity performance in comparison with the fixed transmit power in delay-intolerant networks, wherein the covert capacity represents the maximum rate at the source with which a warden cannot detect the transmission from the source to its destination.

For a two-hop relay wireless network, the authors in [9] considered a greedy relay to forward the information from source and also to transmit other information from itself at the same time, and then explored the detection error probability at a warden and the covert capacity from the relay to destination. The work of [10] focused on the study of covert communication in a multi-hop relay wireless network, wherein efficient algorithms are developed to find optimal paths for maximizing covert capacity and minimizing delay between source and destination.

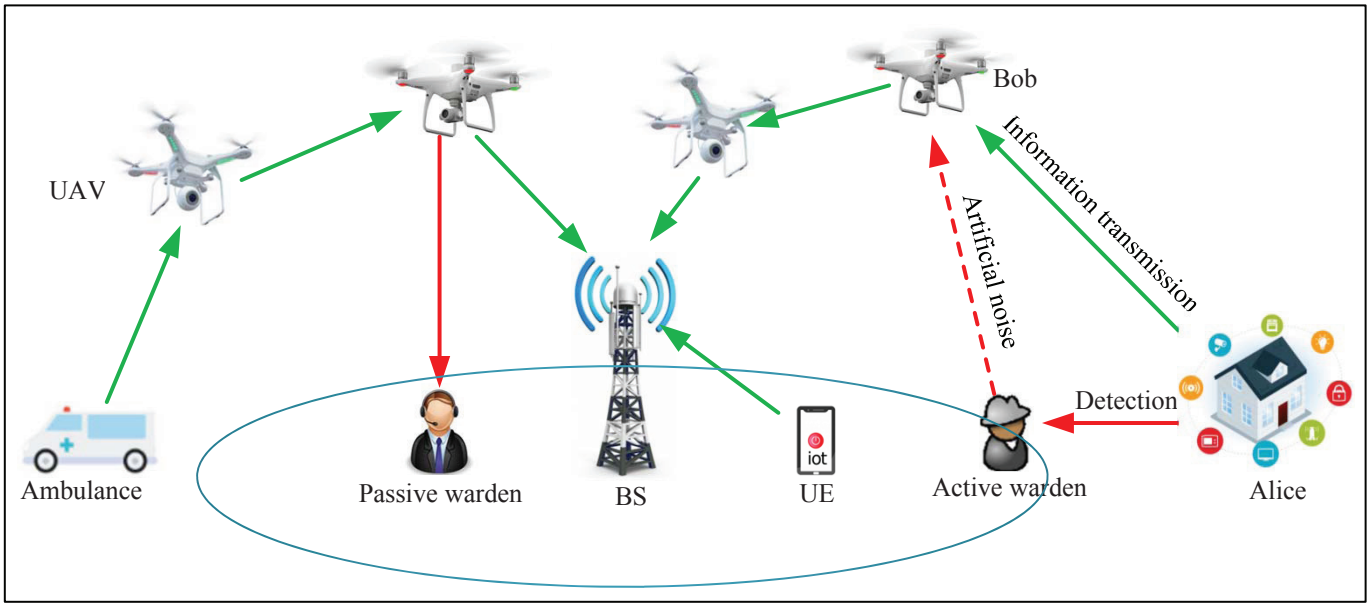


Fig. 2. An appealing network scenario facing the security threats from active and passive malicious wardens.

Cooperative jamming technique is also widely adopted to improve the covert capacity performance [11], [12], wherein a friendly jammer injected artificial noise to the wireless network aiming to confuse warden for guaranteeing covert communication from source to destination in [11], while the work in [12] deployed multiple friendly jammers against multiple malicious jammers in a wireless network. The authors in [13] proved that covert communication is achieved by using a full-duplex destination. Here, the destination not only receives information from source but also acts as a friendly jammer to inject noise to confuse a warden. Covert communication with delay-constraint was further investigated with the help of a full-duplex destination [14]. Specifically, the authors in [14] derived a covert condition with which a larger transmit power of artificial noise emitted by the destination always results in better covert communication performance. The authors in [15] focused on a two-hop full-duplex relay wireless network and illustrated that a positive covert capacity is achieved under an uncertain channel gain from a source to its destination.

B. Covert Communication with UAV

There are very few works concentrating on the covert communication study for UAV networks [3], [4]. The goal of [3] was to hide the information transmission from a UAV source to its destination for avoiding being detected by a warden. To this end, the work jointly optimized the UAV trajectory and transmit power for achieving the covert capacity maximization from the UAV to its destination with the constraints of transmission outage and covertness. The work in [4] considered a multi-hop wireless network including a source, a destination, multiple relays and a UAV warden, where the UAV warden tries to detect the information transmission and also eavesdrop the information. By solving a convex optimization problem, the detection error rate was obtained to measure the covert communication performance.

III. UAV Network Scenario

As shown in Fig. 2, we construct an appealing network scenario consisting of a swarm of UAVs, ground IoT devices (UEs), BS and malicious wardens, where each UAV serves as an aerial BS collecting data from ground UEs and also an aerial IoT device sending data to other UAVs or BS. It is notable that there are two types of UAVs, namely, rotary-wing and fixed ones currently, which are widely used in civilian and military fields. The main advantage of the rotary-wing UAVs are their high manoeuvrability. This enables them to hover in a stationary position, take off and land vertically, and also fly in any direction. They can be applied for monitoring traffic flow and fire as well as for providing local area communication services. Compared to the rotary-wing UAVs, the fixed-wing UAVs have the ability to fly in a large area. This enables them to survey oil pipelines and electricity pylons. However, they have less manoeuvrable and require a large distance for taking off and landing. The communication links of the network can be divided into X2U and cellular links. The X2U links include the U2U links from UAVs to UAVs and G2U links from ground UEs to UAVs, while the cellular links include the G2B links from ground UEs to BS and the U2B links from UAVs to BS. Besides, there exist interference links in the network from these transmitters reusing the same spectrum resources and these active wardens emitting artificial noise to interfere with the legitimate receivers. This network exhibits the following outstanding advantages.

Performing complex task: Most of existing UAV network scenario only consider one UAV, which is difficult for one UAV to perform complex task collecting and processing data from multiple types of sensors. This is because one UAV has limited capacity and energy such that it cannot carry multiple sensors to perform complex task. As an alternative, we consider a swarm of UAVs in the network to collaboratively perform complex

tasks, wherein different UAVs with on-board different sensors can cooperate with each other to collect data from different IoT devices and further conduct computing and analyzing.

Providing ubiquitous connectivity: Owing to the features of high mobility and low cost for UAVs, they can be fast and flexibly deployed to provide urgent network services in disaster areas where the infrastructures (e.g., BSs) may be damaged, or in the rural areas without the coverage of cellular networks. Specially, UAVs can act as aerial BSs to establish communication links with various ground IoT devices ubiquitously.

Implementing remote communication: Traditional UAV networks mainly operate over unlicensed spectrum band, which cannot provide high rate, long distance, reliable and secure communication services. In our concerned network, UAVs can reuse the licensed spectrum band of cellular networks and also utilize almost ubiquitous BSs to implement communication with remote targets. This will facilitate large-scale deployment and applications of UAV networks.

Acquiring high data rate: Since UAVs fly in the air, the line-of-sight (LoS) component probably dominates the G2U, U2U and U2B links. The LoS suffers from less negative impact from multi-path fading, shadowing and path loss in comparison with the non-line-of-sight (NLoS) links, which can provide communication services with high data rate.

Reducing energy consumption: U2U communications can reduce the energy consumption of UAVs. For instance, a UAV needs to transmit an identical message to others of the UAV swarm in a large range. Suppose that without the assistance of U2U communications among UAVs, the UAV must repeatedly transmit the message to different UAVs distributed on a larger range of geographical area. Both the UAV mobility and message retransmissions could quickly consume the precious energy resource of UAVs. To reduce the energy consumption of UAVs, U2U communications are a critical technique to achieve the message exchange among UAVs.

Thanks to these distinguished advantages, the concerned network has great potentials in civilian and military fields. For instance, in firefighting, human search and rescue operations, UAVs can use the on-board IoT devices to detect the existence of fire or human beings, and then send message to a remote control center with the assistance of BSs. G2U and U2U can also achieve the communications in the area affected by floods, earthquakes and hurricanes without the support of BSs.

However, wireless links have open and broadcast characteristics. Specifically, they are LoS links with high probability which are probably detected by some malicious wardens. Hence, the network faces significant security threats, which poses a serious challenge to large scale deployment of such network. As shown in Fig. 2, the network suffers from passive and active wardens. The former one represents that the warden only detects the wireless transmission while the latter one represents that the warden not only detects the wireless transmission but also emits artificial noise to confuse the legitimate receiver. To support the optimal design and deployment of such network, it is of fundamental importance to comprehensively understand the covert performance under the two types of wardens and also to develop a secure communication scheme against the attacks of wardens.

IV. Covert Communication

Covert communication aims at hiding wireless communication process and meanwhile the malicious wardens do not know the communication process or only know it with a low detection probability. Covert communication has exhibited great potentials in various security-sensitive applications. For example, the patients do not expect their information stored at medical IoT devices to be heard by others. In a military field, the communication process among the soldiers wishes to be covert against the detection from adversaries.

As illustrated in Fig. 2, a transmitter (e.g., Alice or Ambulance) intends to covertly transmit information to its receiver while an active/passive warden tries to decide whether the transmission occurs or not via detecting its received signal consisting of the signal from the transmitter (if any), the background noise and the total interference from other transmitters reusing the same spectrum resource with it. Specifically, the active warden can emit artificial noise to confuse the legitimate receiver.

To decide whether the transmitter is transmitting information, warden has to distinguish whether the received signal is from the transmitter (e.g., Alice or Ambulance) plus interference and background noise, or the interference and background noise according to null hypothesis (no covert communication) and alternative hypothesis (covert communication). Under the null hypothesis, the transmitter did not transmit covert information to the receiver, and the received signal at warden consists of background noise plus interference from other transmitters using the same channel with the transmitter. For the alternative hypothesis, the transmitter transmitted covert information, and thus the received signal at warden consists of the signal from the transmitter, interference and background noise. Warden utilizes its received signal to decide whether the transmitter executed a wireless communication in each time slot. To this end, warden conducts the following test: if the received signal at warden is stronger than a given detection threshold, warden judges that the alternative hypothesis is valid; otherwise the null hypothesis is valid.

In covert communication, the covert capacity and detection error probability are two fundamental performance metrics. The former one is used to measure the maximum data rate with which the transmitted information cannot be detected with a high probability, and the latter one is to measure the sum of the false alarm probability and missed detection probability. Here, the false alarm probability represents the probability that warden approves the alternative hypothesis, while the null hypothesis is valid actually. The missed detection probability represents the probability that warden approves the null hypothesis, while the alternative hypothesis is valid actually. A large covert capacity and a high detection error probability

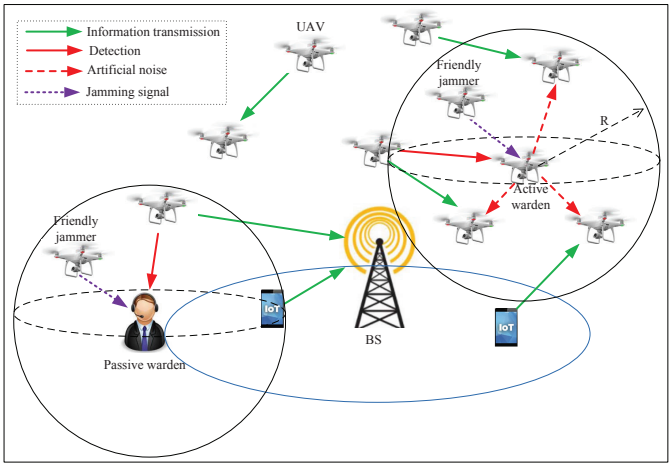


Fig. 3. An illustration of security attack and cooperative jamming

are expected in our concerned networks. To evaluate both the covertness and reliability in the UAV network, we explore the covert capacity performance with a constraint of high detection error probability.

V. Mode Selection, Security Attack and Cooperative Jamming

This section introduces communication mode selection scheme, security attack method and cooperative jamming technique for covert communication.

A. Mode Selection

Each UAV/ground UE transmitter individually decides its communication mode according to a flexible mode selection scheme. Under the mode selection scheme, if the product of a bias factor and the received signal strength (RSS) at the BS is not less than the RSS at the nearest UAV receiver, the transmitter selects the cellular communication mode to connect to the BS; otherwise it selects the X2U communication mode to connect to the nearest UAV receiver. Here, the cellular communications include G2B and U2B communications, and the X2U communications include G2U and U2U communications. The bias factor is a real number with no less than 0.

The promising features of such mode selection scheme are two fold. On one hand, the bias factor can be flexibly set according to different application requirements. For instance, when a cellular network encounters severe congestion, a relatively large bias factor is set to offload the data traffic of the cellular network via X2U communications. On the other hand, the mode selection scheme can enable a unified method to analyze the performances of UAV networks. Specially, when the bias factor tends to infinity, all ground UEs and UAVs connect to the BS, and the network then becomes a cellular network with only cellular communication mode; while the bias factor tends to zero, all ground UEs and UAVs connect to their nearest UAVs, and the network corresponds to an ad hoc network with only X2U communication mode. Thus, by varying the bias factor from zero to a very large value, we can explore the full covert performance range as the network accordingly evolves from ad hoc network towards cellular network.

TABLE I
Simulation Parameters

Parameters	Values
Network area S	3.6×10^5 m^2
Total system bandwidth W	2 GHz
Density of UAV transmitters λ_{TUAV}	10^{-4} UAVs/m^2
Density of UAV receivers λ_{RUAV}	2×10^{-4} UAVs/m^2
Density of Wardens λ_{warden}	5×10^{-5} wardens/m^2
Highest hovering altitude of the UAVs H	300 m
Sphere radius R	80 m
Number of the nearest UAV receivers v	5 UAVs
Cooperative Jamming parameter r	80 m
Cooperative Jamming parameter k	3 wardens
Cooperative Jamming parameter l	1 UAV
Received signal threshold θ	-120 dBm
Transmit power of UAV transmitters/active wardens P	200 mW
Noise variance σ^2	-150 dBm
Bias factor f	1
Path loss exponent α	2 for the X2U links, and 4 for the G2B links

B. Security Attack

We propose a security attack scheme, in which each warden can flexibly switch its role between passive warden and active one. In this scheme, passive wardens aims to detect the wireless transmission while do not degrade the quality of legitimate channel. Different from the passive wardens, the active ones behave more dangerously. This is because the active wardens can not only detect the wireless transmission, but also emit noise to attack the legitimate channel for degrading the channel quality simultaneously.

Each warden uses a v-nearest neighbors (vNN) method to switch its role. Under the vNN method, if there exist at least v UAV receivers in a sphere with radius R centered on the warden, the warden selects the active role to detect the wireless transmission and simultaneously emits noise to its nearest v UAV receivers. Fig. 3 provides an example of role switch with two wardens. When $v = 3$, one warden switches to the active role that detects one wireless transmission and simultaneously emits noise to its nearest 3 UAV receivers, while another one switches to the passive role that only detects the wireless transmission from a UAV. Note that because one transmission from the active warden can affect at least v UAV receivers under the vNN method, it can greatly enhance the attack ability of each active warden, and also significantly reduce the energy consumption of the warden.

C. Cooperative Jamming

Cooperative jamming is a promising security technique, with which friendly jammers transmit jamming signal to

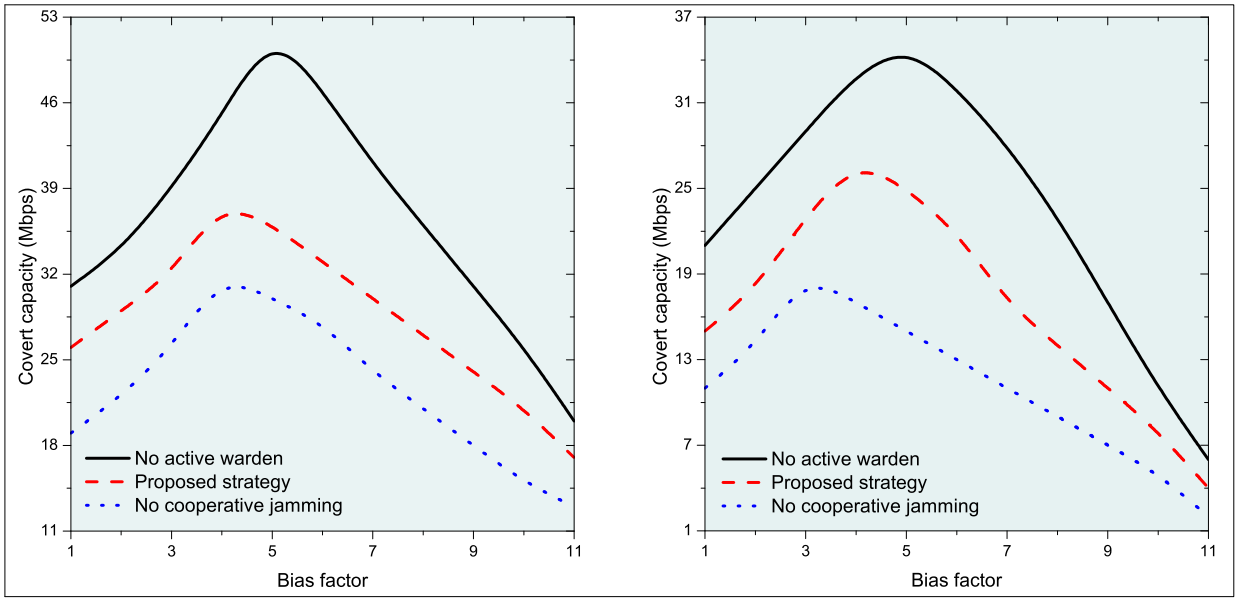


Fig. 4. Covert capacity versus bias factor under different types of links: a) X2U link; b) X2B link.

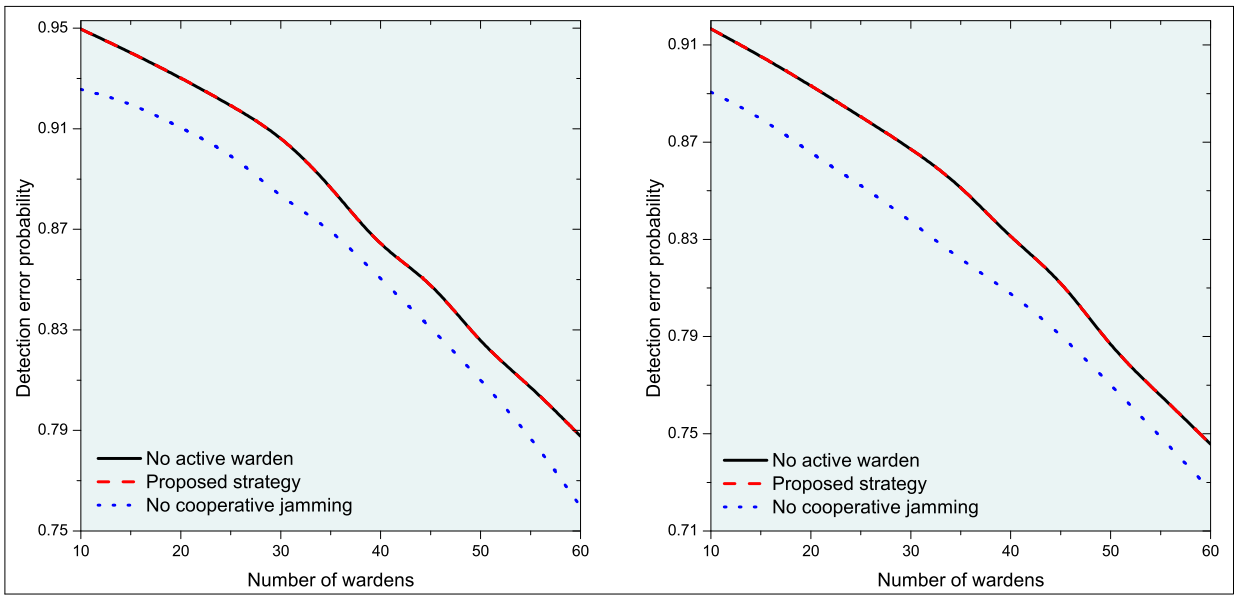


Fig. 5. Detection error probability versus the number of wardens under different types of links: a) X2U link; b) X2B link.

confuse the warden for guaranteeing the covert information transmission. The friendly jammers can be selected based on the following process at each time slot. For the UAV/ground UE transmitter, if the signal-to-interference-plus-noise ratio (SINR) at its receiver is less than a given threshold , the receiver cannot successfully decode the information. Accordingly, the transmitter is a potential jammer. If there exist at least k wardens and at most l legitimate receiving UAVs in a sphere with radius r centered on the transmitter, the potential jammer becomes a jammer to transmit jamming signal to interfere with the k wardens, and meanwhile to mitigate the negative impact of interference on the legitimate receiving UAVs as much as possible.

VI. Numerical Results

This section provides simulation results to explore the effects of the bias factor associated with the flexible mode selection and the number of wardens on the covert performances, i.e., covert capacity and detection error probability.

A. Parameter Settings

In this article, we focus on an uplink transmission scenario, where the UAV transmitters, UAV receivers, ground UEs and wardens are distributed in a three dimensional space based on homogeneous Poisson point process (PPPs) with densities $TUAV$, $RUAV$, UE and $warden$. We use PPP only to illustrate the covert performances under our proposed novel network scenario and three schemes (i.e., mode selection,

security attack and cooperative jamming). Note that our proposed network scenario and schemes can also be applied to the situation that the distributions of the UAVs, UEs and wardens are in an aggregated and non-Poisson manner. The highest hovering altitude of the UAVs is H m. The BS is located at the original point. We consider the total spectrum bandwidth W GHz is evenly divided into N spectrum blocks. Here, N is set as the number of cellular UAV transmitters and ground UEs. An orthogonal spectrum sharing scheme is adopted for spectrum block allocation, under which each cellular UAV transmitter/ground UE is assigned an orthogonal spectrum block. Thus, there does not exist interference among cellular UAVs/ground UEs. Each U2U transmitter/ground UE randomly reuses a spectrum block with a cellular UAV transmitter/ground UE, which incurs the interference among the U2U transmitters/ground UEs reusing the same spectrum block.

We conduct simulation study under the following three strategies: (1) our proposed strategy including mode selection, security attack and cooperative jamming, (2) no active warden equivalent to our proposed strategy without active wardens, and (3) no cooperative jamming equivalent to our proposed strategy without cooperative jamming. In this simulation, the parameter settings for the concerned cellular and X2U-enabled UAV networks are summarized in table I unless otherwise specified. We use Ralyleigh fading to depict both small scale and large scale fading of the G2B links, and use Rician fading to depict the fading of the U2U links.

B. Covert Capacity

To explore the effect of the bias factor on the covert capacity under these three strategies, Fig. 4 shows how the covert capacity varies with the bias factor subject to a constraint of detection error probability no less than 0.92. We can see from Fig. 4 that as the bias factor increases, the covert capacities of X2U and X2B links first increase and then decrease under each strategy. This can be explained as follows. As the bias factor increases, more UAVs and ground UEs select X2B mode to communicate with the BS. Since each cellular UAV/ground UE is assigned an orthogonal channel, it can reduce the interference among all UAVs and ground UEs resulting in the increase of covert capacity in the network. On the other hand, it can also reduce the spectrum bandwidth of each orthogonal channel, and thus this will result in the decrease of covert capacity. As the bias factor is relative small, the former positive effect on the covert capacity is higher than the latter negative effect, and thus the covert capacity increases with the increase of the bias factor under each type of link, while as the bias factor further increases, the latter negative effect is higher than the former positive effect, and thus the covert capacity decreases.

Another observation from Fig. 4 illustrates that for each setting of bias factor, the covert capacity under our proposed strategy is lower than that under no active warden, but it is higher than that under no cooperative jamming. This is because under our proposed strategy, the active wardens can send noise to interfere with legitimate receivers leading to the decrease of the covert capacity, while the cooperative jamming can improve the covert capacity via sending jamming signal to confuse the wardens. Therefore, the covert capacity under no active warden is the largest one, and that under no cooperative jamming is the smallest one.

C. Detection Error Probability

We proceed to investigate the effect of the number of wardens on the detection error probability under the three strategies. Fig. 5 shows how the number of wardens affect the detection error probability subject to a constraint of covert capacity no less than 9 Mbps. We can see from Fig. 5 that as the number of wardens increases, the detection error probabilities of X2U and X2B links decrease. This is because more wardens are distributed around the legitimate transmitters, so that they can more easily detect the legitimate wireless transmission process, leading to the decrease of the detection error probabilities.

We further observe from Fig. 5 that the detection error probability under no active warden well matches with that under our proposed strategy. This is due to the following reasons. We assume the self-interference at active wardens caused by noise emission is cancelled by using interference cancellation techniques, such as absorptive shielding and adaptive filter, which leads to the same detection error probability under the two strategies. Another careful observation from Fig. 5 illustrates that the detection error probability under no cooperative jamming is smaller than that under the other two strategies for each fixed setting of number of wardens. It is because no transmitter sends jamming signal to confuse wardens, which leads to the decrease of detection error probability without cooperative jamming.

VII. Conclusions and Future Research Directions

This article constructed an appealing network scenario consisting of a swarm of UAVs, ground IoT devices, BS and malicious wardens. In such network scenario, we first proposed a flexible mode selection scheme, then we designed two types of wardens, i.e., passive and active wardens. A cooperative jamming scheme was further proposed against the attack of wardens. Numerical results illustrate that the active wardens pose more passive effects to the covert capacity compared to the passive wardens, while the cooperative jamming can increase detection error probability at wardens.

Some interesting future research is summarized as follows.

Machine learning (ML)-based covert communication: The existing works on covert communication need to exchange massive channel state information (CSI) among users. This will result in high energy consumption, specially for these UAVs with limited energy. ML is a promising method that can utilize historical information to unveil the hidden patterns, which significantly reduces the system overhead. Therefore, ML-based covert communication is an important research direction in UAV networks.

Multi-hop covert communication with advanced active wardens: When a source is far away from its destination, the source needs to employ high power to send information

to the destination, which probably be detected by wardens. With the assistance of relays, each node can use low power to send information. However, the wireless transmission may encounter more advanced active wardens that can launch spoofing attacks. For instance, in the UAV navigation system, spoofed GPS signals will cause the UAV to deviate from the correct trajectory. Therefore, a new research is deserved to investigate multi-hop covert communication with advance active wardens in UAV networks.

Covert performance modeling of cellular-enabled UAV networks: Cellular-enabled UAV networks are envisioned to be network paradigm in 5G and beyond wireless networks. Covert performance is of fundamental importance to measure quality of service (QoS) of the networks. One interesting direction is how to theoretically model the covert performance via optimizing various system parameters such as UAV trajectory, UAV altitude, transmit power and channel allocation.

VIII. Acknowledgment

This work was supported by the Academy of Finland Projects: 6Genesis under Grant No. 318927 and IDEA-MILL under Grant No. 335936; the NSF of China under Grant No. 61962033; the Anhui Province project under Grant No. 1808085MF165; the Yunnan Province project under Grant No. 2018FH001-010; and the Chuzhou University projects under Grant No. zrjz2017003, zrjz2019011, and 2020qd16.

References

[1] Z. Chen, K. Chi, K. Zheng, G. Dai, and Q. Shao, "Minimization of transmission completion time in UAV-enabled wireless powered communication networks," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 1245–1259, Feb. 2020.

[2] B. Yang, T. Taleb, Z. Wu, and L. Ma, "Spectrum sharing for secrecy performance enhancement in D2D-enabled UAV networks," *IEEE Network*, vol. 34, no. 6, pp. 156–163, Nov./Dec. 2020.

[3] X. Zhou, S. Yan, J. Hu, and *et al*, "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.

[4] H. Wang and Y. Zhang and 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.

[5] B. Yang, T. Taleb, Y. Fan, and S. Shen, "Mode selection and cooperative jamming for covert communication in D2D underlaid UAV networks," *IEEE Network*, vol. 35, no. 2, pp. 104–111, Feb. 2021.

[6] 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, pp. 1921–1930, Sept. 2013.

[7] 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, pp. 3493–3503, Jun. 2016.

[8] S. Yan and B. He and X. Zhou and Y. Cong and A. L. Swindlehurst, "Delay-intolerant covert communications with either fixed or random transmit power," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 1, pp. 129–140, Jan. 2019.

[9] J. Hu, S. Yan, X. Zhou, and *et al*, "Covert communication achieved by a greedy relay in wireless networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, pp. 4766–4779, Jun. 2018.

[10] A. Sheikholeslami, M. Ghaderi, D. Towsley, and *et al*, "Multi-hop routing in covert wireless networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 3656–3669, Jun. 2018.

[11] T. V. Sobers, B. A. Bash, S. Guha, and *et al*, "Covert communication in the presence of an uninformed jammer," *IEEE Trans. Wireless Commun.*, vol. 16, no. 9, pp. 6193–6206, Sep. 2017.

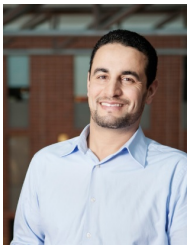
[12] R. Soltani, D. Goeckel, D. Towsley, and *et al*, "Covert wireless communication with artificial noise generation," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7252–7267, Nov. 2018.

[13] K. Shahzad, X. Zhou, S. Yan, J. Hu, and *et al*, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8517–8530, Dec. 2018.

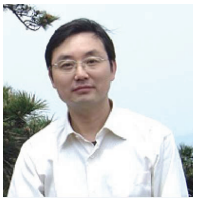
[14] F. Shu, T. Xu, J. Hu, and S. Yan, "Delay-constrained covert communications with a full-duplex receiver," *IEEE Wireless Commun. Lett.*, vol. 8, no. 3, pp. 813–816, Jun. 2019.

[15] J. Wang and W. Tang and Q. Zhu and X. Li and H. Rao and S. Li, "Covert communication with the help of relay and channel uncertainty," *IEEE Wirel. Commun. Lett.*, vol. 8, no. 1, pp. 317–320, Feb. 2019.

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 senior researcher with the MOSAIC Lab, 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 Information Technology and Electrical Engineering, Oulu University, Finland. He is the founder and the Director of the MOSA!C Lab. He is the Guest Editor-in-Chief for the IEEE JSAC series on network softwarization and enablers.



Guilin Chen received the B.S. degree from Anhui Normal University, China, in 1985, and the M.S. degree from the Hefei University of Technology, in 2007. He is currently a professor with the School of Computer and Information Engineering, Chuzhou University, Chuzhou, Anhui, China. His current research interests include cloud computing, wireless networks, healthcare, and the Internet of Things.

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 of Kunming University, China. His research interests include wireless sensor networks, cyber security and Internet of Things.