This is an electronic reprint of the original article.
This reprint may differ from the original in pagination and typographic detail.

Wang, Li; Chen, Yu; Wang, Pu; Yan, Zheng

Security Threats and Countermeasures of Unmanned Aerial Vehicle Communications

Published in:
IEEE Communications Standards Magazine

DOI:
[10.1109/MCOMSTD.0001.2000078](https://doi.org/10.1109/MCOMSTD.0001.2000078)

Published: 01/12/2021

Document Version
Peer reviewed version

Please cite the original version:
Wang, L., Chen, Y., Wang, P., & Yan, Z. (2021). Security Threats and Countermeasures of Unmanned Aerial Vehicle Communications. *IEEE Communications Standards Magazine*, 5(4), 41-47.
<https://doi.org/10.1109/MCOMSTD.0001.2000078>

Security Threats and Countermeasures of Unmanned Aerial Vehicle Communications

Li Wang, Yu Chen, Pu Wang, and Zheng Yan, *Senior Member, IEEE*

Abstract—Unmanned Aerial Vehicles (UAVs) have been widely applied in various fields, including but not limited to military, industry and agriculture. But UAVs also confront severe security threats, which retards its wide applications. Current research mainly focuses on the security of a single UAV system, while paying little attention to UAV related communications, especially in physical layer and network layer. Thus, it becomes necessary to summarize potential security threats and corresponding countermeasures. To this end, we study mainstream attacks on UAV communications in order to propose security requirements. Then, we present a comprehensive review on existing security countermeasures for enhancing UAV communication security in both physical layer and network layer. We conclude with open issues and future prospect of UAV security.

Index Terms—UAV, UAV security, UAV attacks, UAV security countermeasures.

I. INTRODUCTION

Unmanned aerial vehicles (UAVs), also known as drones, are becoming pervasive and have been employed in many military and civilian applications. UAVs can be operated either through remote control or via self-government. They have play a major and vital role in many military and civilian applications. Because of ease of deployment, high-maneuverability and mobility, UAVs have promoted their considerable use to perform various tasks, such as rescue, surveillance, search, aerial base station, and goods delivery. For example, Amazon, FedEx, and Walmart announced that they will utilize UAVs to deliver packages. During coronavirus pandemic, UAVs were used to measure body temperature, thus avoid the risk of viral infection. Moreover, UAV swarms have great potential to execute formidable tasks beyond the capability of a single UAV, e.g., investigation and message relay. In a UAV swarm, when one UAV becomes unavailable, other UAVs can quickly replace it, thus greatly ensuring reliability.

With the development of UAV applications, UAV-involved communications are becoming complicated and diverse. Traditional UAV communication architecture is usually composed of two parts: ground control station (GCS) and UAV. GCS controls UAV, and UAV feedbacks GCS commands. The two parts are connected through a communication link with

unlicensed spectrum (e.g., 2.4GHz) or Wi-Fi, which can only operate within a visual line-of-sight (LoS) range. To provide beyond LoS communications, cellular and satellite networks offer a promising solution for UAV communications. On the other hand, UAVs can provide cost-effective wireless communications in a variety of real-world scenarios. For example, UAVs can be utilized as a mobile platform for collecting data from ground sensors or as an aerial base station to offer wireless communications, a complement to the existing cellular networks, for users in case of emergency [1]. Compared to terrestrial wireless communications, UAV-based communications have many unique advantages, such as on-demand and swift deployment, high flexibility, and mobility, which bring promising gains for UAV applications.

Despite various applications enabled by UAVs, security threats on UAV communications increase rapidly. Due to security vulnerabilities exist in UAV protocols and standards, UAVs are vulnerable to various attacks, including eavesdropping attack, GPS spoofing attack, and denial-of-service (DoS) attack. For example, an RQ-170 Sentinel was hijacked by Iranian forces; a software called Skyjack can maliciously search and hijack civilian UAVs. The security issues of UAV communications become very severe nowadays, which brings big challenges to promote the widespread use of UAVs [2].

Few existing works focus on the security of UAV systems although there are many studies on UAVs, such as communication techniques, network architectures and applications [1], [3]. Current works are mainly about a single UAV based system, lack investigation on the security threats of UAV swarms. Some existing works only address some specific aspects of UAV security, such as cyber threats and vulnerabilities of UAV autopilot [4] and routing [5]. It still lacks a comprehensive analysis of the UAV communication security by comprehensively considering its potential attacks. Through investigation, we found that attackers usually hack UAV communications from the perspective of network layer and physical layer. In order to reduce the occurrence of attacks, it is necessary to review the security of UAV communications, starting from potential attacks and threats to their countermeasures. To this end, this paper presents a systematic review of UAV communication security and prior art countermeasures by using a set of proposed security requirements as criteria to evaluate. Our review focuses on physical and network layers since they are highly related to UAV communications.

The remainder of this paper is organized as follows. We first summarize main security threats in UAV related communications in Section 2. Then, we propose secure communication requirements of UAV in Section 3, followed by security

L. Wang and P. Wang are with the State Key Lab of ISN, School of Cyber Engineering, Xidian University, Xi'an, 710071, China, e-mail: 1783364643@qq.com and wangpu03@gmail.com

Y. Chen is with the School of Information Systems and Technology at Lucas College and Graduate School of Business, San Jose State University, San Jose, CA 95192, USA, e-mail: yu.chen@sjsu.edu

Z. Yan (corresponding author) is with the State Key Lab of ISN, School of Cyber Engineering, Xidian University, Xi'an, 710071, China, and the Department of Communications and Networking, Aalto University, Espoo, 02180, Finland, e-mail: zheng.yan@aalto.fi; zyan@xidian.edu.cn

Fig. 1: De-authentication Attack

countermeasures in Section 4. Finally, we conclude with open issues and future research directions of UAV security.

II. SECURITY THREATS

Like other information transmission equipment, UAV also faces various security threats. From the perspective of attack types, potential attacks on UAV communications can be divided into network layer attacks and physical layer attacks.

A. Network Layer Attacks

Similar to other networked devices, UAVs face the same threats in the network layer, as shown in numerous prior work [3], [6]. The main three types of network layer attacks include flooding attack [3], de-authentication attack [6], and routing attack, as presented below.

1) *Flooding Attack*: The traditional flooding attack, also known as denial of service (DoS) attack, consumes a lot of system resources to make a networking service unavailable, so that legitimate users cannot use the service normally. As a networked device with limited computing resources and power energy [3], UAVs are especially vulnerable to the DoS attacks. As air equipment, the consequences of DoS attack on UAVs could be serious. For example, failing to receive GCS commands may make UAVs lose control in the air and exhaust battery power, leading to malignant events of falling injury. Some researchers used security tools to carry out a DoS attack on UAVs [3]. They sent a large number of data packets to a UAV to make it paralyzed, and eventually led to its crash.

2) *De-authentication Attack*: Most drones are equipped with Wi-Fi to communicate with GCS and receive commands from their users [3]. However, the Wi-Fi module based on 802.11 protocol is not really secure. Because its management frame is not encrypted, it is easy for attackers to forge it. Attackers can send a constructed de-authentication frame to GCS to disconnect it from the UAV [6]. As shown in Fig. 1, the attacker begins by sniffing and finding the MAC address of the UAV and its connected user. After that, the attacker sends a forged de-authentication frame packet to the user, forcing its communication link to the UAV interrupted. Then, the attacker can connect and control the UAV.

3) *Routing Attack*: Another attack mainly aims at multi-UAV networks or UAV swarms. Frequent replacement of nodes in UAV networks makes routing attack possible, similar

Fig. 2: Routing Attack

to wireless sensor networks. In this case, attackers could add UAV nodes controlled by themselves into a UAV network, pretending to be normal UAVs, or compromise UAVs in an existing UAV network to launch a routing attack. These malicious nodes are disguised as optimal routing nodes for the purpose of changing an entire routing table. Other nodes will then choose the malicious nodes to relay their packets. Routing attacks are severe in a multi-UAV network. They induce the entire network to malfunction by destroying its routing protocol. Common routing attacks include black hole attack, gray hole attack and wormhole attack [5], as presented below.

a) **Black hole attack**: A malicious node drops all control and data packets that are routed through it. Therefore, any packet routed through this intermediate malicious node will suffer from partial or total data loss. In multi-UAV networks, malicious UAVs discard all packets flowing through themselves, instead of forwarding them to the next hop (shown in Fig. 2). Consequently, some UAVs could fail to receive commands from GCS, and finally crash due to energy exhaustion. Moreover, the malicious node may analyze the contents of the packets and obtain confidential information before discarding the packets.

b) **Gray hole attack**: A special type of the black hole attack. Instead of discarding all packets, the malicious node selectively drops or forwards packets, e.g., only forwarding control packets but discarding some data packets in multi-UAV networks (shown in Fig. 2). In this case, although a UAV can receive packets from its GCS, they could contain useless information. In a worse situation, the malicious UAV may forge some packets to cheat other UAVs and the GCS. Because the gray hole attack does not discard all packets, it is more difficult to be detected than the black hole attack.

c) **Wormhole attack**: By exploiting a pair of malicious nodes that have stronger communication ability than other nodes, they can form a short tunnel in a UAV network to attract more nodes to choose this communication tunnel. As shown in Fig. 2, the UAVs in A and B networks are attracted by the routing ability of malicious nodes to send packets to the two malicious UAVs first. Then, the two malicious nodes communicate with each other and selectively forward or even forge some messages to normal UAVs. Compared with the previous two routing attacks, the wormhole attack can receive messages from not only source addresses, but also destination

Fig. 3: Physical Layer Attacks

addresses, or forge data packets to obtain desired information.

B. Physical Layer Attacks

Physical layer attacks of UAVs refer to the attacks in wireless channels, it is also called physical link attack. According to the behavior of an adversary, physical layer attacks can be divided into two types: passive eavesdropping and active eavesdropping.

1) *Passive eavesdropping attack*: In the passive eavesdropping attack, a potential eavesdropper listens to a wireless channel and collects information. As shown in Fig. 3, the eavesdropper hides and has no other behaviors than silently collecting transmitted information. Passive eavesdropping does not affect legitimate users or UAVs to exchange messages, making it difficult for UAV operators to detect and accurately locate the eavesdropper [7].

2) *Active eavesdropping attack*: By contrast, the active eavesdropping attack is more dangerous than the passive one, which includes both eavesdropping and signal interference. As shown in Fig. 3, an active eavesdropper can use a jammer to maliciously send interference signals to legitimate channels. This technique will degrade a legitimate channel, which makes a legitimate receiver unable to receive packets, thus greatly affecting UAVs to execute tasks and transmit information. Furthermore, active eavesdroppers can move to an optimal eavesdropping location or use professional advanced wireless devices, such as full-duplex eavesdroppers, to receive wireless signals. The capability of attack can be enhanced by interacting with potential passive eavesdroppers [7], causing severe damage to legal UAV communications.

III. SECURITY REQUIREMENTS

In this section, we analyze the security requirements of UAV systems by considering their unique characteristics and security threats. We elaborate and present the following requirements: data confidentiality, access authentication, system availability, information integrity, and behavioral reliability. We further evaluate violation of these requirements in terms of each attack listed in Section II, shown in Table I.

a) **Data confidentiality**. UAVs inevitably need to transmit data in various scenarios, including military and civilian

contexts. Therefore, any unauthorized entities cannot gain the transmitted data information or directly decrypt the data in a transmission packet. In eavesdropping and gray hole attacks, attackers could get transmitted data silently. Thus, data confidentiality should be ensured to resist them.

b) **Access authentication**. It is essential to authenticate access in order to avoid the abuse of equipment by illegal users. Before operating a UAV, a user must provide a valid identity for re-authentication in time after disconnection. The de-authentication attack takes advantage of the authentication flaws in the Wi-Fi protocol to seize the control of UAV. Thereby, access authentication becomes critical to avoid malicious de-authentication attacks.

c) **System availability**. The UAV system should operate or collect data strictly complying with its legitimate user's command. The main purpose of some attacks is not to get the data transmitted by the UAV, but to hinder the normal operation of UAVs with a small overhead. For example, the flooding attack prevents UAVs from responding to the users' commands, and the black hole attack makes UAVs in multi-UAV networks unable to receive commands from GCS. These attacks make the UAV system unable to operate normally, and even UAV falling down. So, the availability of the UAV system should be guaranteed.

d) **Information integrity**. This refers to the integrity of data in UAV communications, especially for the commands used to control UAVs. The sensed data modified by attackers make UAV task incomplete with fake data, while modified control commands could directly result in failure of UAV operation. Obviously, information integrity is an essential system security requirement.

e) **Behavior reliability**. An attack usually makes UAVs behave abnormally. For example, attacking visual sensors and GPS sensors could cause the UAVs to drift or crash due to wrong images or geolocation information; flooding attacks can make the UAVs out of control. Therefore, we request the UAV to behave reliably without suffering from interruptions, wrongly sensed data, and intrusions.

IV. SECURITY COUNTERMEASURES

This section reviews the main security countermeasures of UAV systems, focusing on the network and physical layers. In Table 2, we summarize the reviewed security solutions by indicating their resisted attacks.

A. Security Solutions in Network Layer

1) *Wi-Fi security solutions*: Most UAVs apply Wi-Fi by using the preset WEP protocol, which does not require any password in communications [1]. To prevent malicious connections, the WPA protocol has been used instead, which requires identity verification using pre-shared keys, thus enhancing the security of UAVs. To prevent the de-authentication attacks, the 802.11w protocol was suggested, which encrypts the management frame. So the attacker cannot forge frame messages, thus the system availability of UAV is ensured. Moreover, a multi-layer security framework was proposed to secure communications of commercial UAVs using Wi-Fi and

TABLE I: Attacks and Violated Security Requirements

Types of attacks	Attack mechanisms	Violation of Security Requirements				
		Data confidentiality	Access authentication	System availability	Information integrity	Behavior reliability
Flooding attack [3]	Send a large number of packets to consume computing resources	No	No	Yes	No	Yes
De-authentication [6]	Send specific data frames to take over UAV Control	No	Yes	Yes	No	Yes
Black hole attack [5]	Change routing information and stop forwarding packets	No	No	Yes	No	Yes
Gray hole attack [5]	Change a routing table and selectively forward packets	No	Yes	Yes	Yes	Yes
Wormhole attack [5]	Change a routing table and build a malicious transport tunnel	No	Yes	Yes	Yes	Yes
Passive eavesdropping [7]	Silently listening to a link	Yes	No	No	No	No
Active eavesdropping [7]	Monitor a link and send interference	Yes	No	Yes	Yes	Yes

reduce the security risk of Zero-Day attacks, such as Address Resolution Protocol (ARP) Cache Poisoning attacks [1].

2) *Intrusion detection systems*: Intrusion detection system (IDS) is a security mechanism to identify malicious behaviors. By analyzing the routing behavior of UAV networks according to given rules, IDS is able to predict whether the UAV networks has been attacked [8]. Although not directly resisting attacks, IDS can be used to early detect attacks and minimize user loss in time. Because of the limitation of UAVs, the IDS for UAV systems should consider the following factors: energy economy, computation efficiency, lightweight, and real-time detection.

Sedjelmaci et al. [9] proposed mobile GCS to continuously provide a reliable connection to UAV. In this scheme, the data packet sent to the GCS by the UAV contains source address and destination address, next-hop information, etc. GCS checks the information to determine whether a relay node in a UAV swarm network forwards a data packet normally and calculates the number of dropped packets. GCS compares the calculated value with a previously defined threshold to decide malicious behaviors. In addition to finding malicious nodes that destroy routing, the mobile GCS can also collect a certain range of data packets, use a normal distribution method to evaluate the number of packets sent (NPS), check whether the NPS is in a normal range, and detect whether a drone is affected by a flooding attack. In particular, the authors combined rule-based detection and abnormal detection techniques to classify UAVs into normal, suspicious, abnormal, and malicious according to their behaviors. The IDS can effectively help the UAV users to detect possible attacks in different application scenarios by analyzing attacks according to their specific traffic. So IDS plays an important role in protecting UAV system availability and reliability.

3) *Authentication*: The main purpose of authentication is to verify the eligibility of data sources or a UAV to prevent attackers from faking packets or directly joining a drone swarm to destroy its network structure. This is especially important for protecting UAV swarms.

Regarding UAV communication protocols, the micro air vehicle link (MAVLink) protocol version 2.0 strengthens UAV

security with authentication. At the same time, timestamp and signature mechanism were added to ensure identity legality and prevent information from being tampered with [10]. Yoon et al. proposed a security authentication system to establish a secure channel between UAV and GCS for ensuring reliable data transmission. It also assures that users will not lose control of UAV after being attacked [11].

In addition to authenticating the UAV itself, authenticating transmitted data can also be used as a security measure. Because attackers may intercept a sensor's data and maliciously modify important data, Sun et al. designed an authentication watermark strategy by leveraging the characteristics of collected data to generate an authentication watermark and randomly insert it into the data [12]. The UAV can verify the integrity of the data to avoid data replay and tampering, so as to ensure information integrity. This countermeasure greatly improves the safety of UAV in the context of data collection.

The 16th version (R16) of the 5th generation mobile networks (5G) has been completed. Compared with its previous version, R16 improves the part about vehicle to everything (V2X) and wireless location technology of V2X. For security, a V2X system uses public key infrastructure (PKI) based certificates to secure authentication and communication between devices. As a special vehicle, the safety standard of UAV will be provided in R17.

4) *Secure routing protocols*: Secure routing protocols are mainly used to protect the security of a UAV swarm network. Similar to a traditional computer network, the multi-UAV network is supported by routing protocols for forwarding data packets and transmitting commands. Secure routing protocols aim to resist attacks during routing and forwarding, such as black hole attack and wormhole attack. Existing UAV security routing protocols mainly identify a new UAV and check whether a node forwards data normally to ensure network stability. Maxa et al. [13] proposed a secure routing protocol that uses public key encryption and hash chains to perform signature operations and check the number of hops based on geographical leases in order to reduce the occurrence of wormhole attacks.

TABLE II: UAV Security Countermeasures

Security Requirements Security Solutions	Data confidentiality	Access authentication	System availability	Information integrity	Behavior reliability	Resisted attacks
802.11w protocol	-	✓	✓	-	-	De-authentication
IDS [9]	-	-	✓	-	✓	Flooding attack, Routing attack
Authentication [10]–[12]	-	✓	✓	✓	✓	Routing attack
Secure routing protocol [13]	-	✓	✓	-	✓	Routing attack
Signal power detection	-	-	✓	✓	-	Active eavesdropping
Joint trajectory and resource allocation [7]	✓	-	-	✓	-	Passive/active eavesdropping
Inject noise	✓	-	-	-	-	Passive/active eavesdropping
Coordinated Multiple Point Transmission	✓	-	-	✓	-	Passive/active eavesdropping
New radio technology (beamforming, mmWave) [14]	✓	-	-	✓	-	Passive/active eavesdropping

B. Security Solutions in Physical Layer

Different from network layer security, which focuses on encryption and authentication, physical layer security schemes focus on preventing information leakage and interference in the wireless channel, by exploiting power allocation, beamforming and artificially injecting [15].

1) *Signal power detection*: Signal power detection is mainly applied for identifying active eavesdropping attacks, in which attackers send interference signals and make the signal power received by a legitimate receiver higher than the normal. It can be used to detect attacks and help the UAV fly away from a maliciously monitored area, and then avoid the attacker's influence on its behavior. The key to this scheme is to set a proper power threshold. A low threshold could cause a false alarm, while a high threshold could make it difficult to identify an attack.

2) *Joint trajectory and resource allocation* : This method leverages UAV mobility and determines UAV flight path and transmission power based on the positions of an information receiver and an eavesdropper. In the joint design of UAV trajectory and resource allocation [7], when the UAV is close to the eavesdropper, it can reduce its transmission power or stop transmission to reduce the possibility of information leakage, and at the same time, move away from the eavesdropper at a full speed. On the contrary, when the UAV is close to the legitimate receiver, it will slow down and increase its transmission power to transmit confidential information.

3) *Noise injection*: Sometimes it is difficult to obtain the location of an eavesdropper. In this case, artificial noise can be injected into wireless signals to increase the security of information transmission. As shown in Fig. 3, artificial noise is transmitted to a zero space of a legal channel through the cooperation of multiple UAVs. Thus, possible information leakage is reduced by limiting the capacity of an eavesdropping channel without any effects on a legal channel. Since artificial noise consumes UAV energy and reduce the transmission power of effective information, it is necessary to optimize power distribution to improve energy utilization efficiency.

4) *Coordinated multiple point transmission*: In order to enhance the anti-jamming ability of a UAV network, cooperation between multiple UAVs can be used to enhance the security of the physical layer. As shown in Fig. 3, multiple UAVs can form a virtual antenna array to enhance the receiving ability of a legitimate UAV and reduce that of an eavesdropper. In addition, multiple UAVs can cooperate to optimize their trajectory and resource allocation, e.g., some UAVs responsible for interfering with eavesdroppers, and others for communicating with legitimate users on the ground safely.

5) *New radio technologies*: Besides traditional security schemes mentioned above, new technologies also emerge to address existing security problems in the physical layer of UAV. For example, 3D beamforming can generate separate beams in 3D space to provide enhanced service coverage, increase system throughput, and secure data transmission by separating a legitimate receiver from an eavesdropper according to elevation and altitude difference of a target [14]. For another example, as a 5G core technology, millimeter wave was used to provide high-speed data transmission for UAV communications by applying its rich frequency band. Compared with ground communications, the UAV air application environment does not have too many signal scatterings caused by communication obstacles. Therefore, the special channel characteristics of millimeter wave can be used to achieve highly directional transmission and increase the difficulty of eavesdropping.

V. OPEN ISSUES AND FUTURE DIRECTIONS

By considering UAV security threats and reviewing state-of-art security countermeasures, we identify the following open issues and future research directions.

UAV security in the space-air-ground integrated network should be re-designed. Space-air-ground integrated network (SAGIN), as integration of satellite systems, UAV networks, and terrestrial communications, has been becoming an emerging architecture for various network services and applications. Because of integration of heterogeneous networks and dynamic network topology, it is necessary to reconsider UAV-involved communication security, such as authentication

and key agreement protocols between UAV and satellites or terrestrial nodes, and key management when UAVs handover from cellular base stations to satellites.

UAVs with new radio techniques is highly expected. To further enhance the physical layer security, some advanced radio techniques should be incorporated into UAV communications. Besides supporting high data rate and spectral efficiency, the applications of non-orthogonal multiple access (NOMA), multi-antenna, and millimeter wave can also enhance the secrecy of wireless channels in UAV-involved communications. Therefore, it is desired to investigate advanced technologies in terms of the physical layer security by exploiting the unique properties of UAVs (e.g., high mobility and positioning flexibility).

Privacy should be preserved in UAV enabled applications. UAVs are mainly applied to complete some specific tasks to satisfy people demands due to their autonomy and flexibility. In many UAV enabled applications, human-beings' personal data are necessarily needed in system operations, privacy protection becomes a crucial issue. Differential privacy and encryption methods are worth studying for privacy preservation in UAV systems. But the limited resources of UAVs should be seriously considered when exploring a privacy preservation scheme. Although encrypting data streams could be a solution, it undoubtedly increases transmission latency and energy consumption. Meanwhile, for some low sensitive data, such as aerial scenery video, users have no much privacy requirements. Thus, specific solutions should be investigated to fit into UAV scenarios. Equipment with special encryption hardware should be researched to improve encryption efficiency and allow users to personalize the protection of their personal data transmission.

Multi-layer and defense-in-depth security framework should be further developed. Defense-in-depth refers to a security approach in which a series of security mechanisms are layered throughout a UAV system. Based on the analysis of the existing security countermeasures, many techniques are only able to resist one type of attacks. Therefore, it becomes essential to design a multi-layer security framework that can protect UAV-involved communications by integrating multiple security countermeasures. For example, trajectory optimization can be combined with IDS. IDS can detect suspicious data streams for UAV to help it estimate the location of an attacker, so as to make UAV select a safe trajectory.

UAV-involved communication security standards should be formulated. At present, the industry still lacks uniform standards in terms of UAV communication security. Except for endless explorations of security technologies, formulating UAV communication security standards requests special efforts by considering many factors, such as wireless communication security, network security and data privacy. For the importance of privacy in UAV applications, data protection is better being included into the standards to make privacy preservation as a necessity.

VI. CONCLUSION

In this article, we reviewed the security threats and countermeasures of UAV communications. Driven by wide UAV

applications and its potential usages in many new fields, we summarized potential attacks on UAV communications in order to explore their security requirements. Through a comprehensive review of existing countermeasures against attacks in the physical and network layers, we indicated open issues and future research directions of UAV communication security.

ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation of China under Grants 62072351; in part by the Academy of Finland under Grant 308087 and Grant 335262; in part by the Shaanxi Innovation Team Project under Grant 2018TD-007; and in part by the 111 Project under Grant B16037, as well as Huawei Technologies Group Co., Ltd.

REFERENCES

- [1] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. Garcia-Rodriguez, and J. Yuan, "Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3417–3442, 2019.
- [2] Y. Tan, J. Wang, J. Liu, and Y. Zhang, "Unmanned systems security: Models, challenges and future directions," *IEEE Network*, pp. 1–7, 2020.
- [3] H. Shakhathreh, A. H. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, N. S. Othman, A. Khreishah, and M. Guizani, "Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges," *IEEE Access*, vol. 7, pp. 48 572–48 634, 2019.
- [4] A. Kim, B. Wampler, J. Goppert, I. Hwang, and H. Aldridge, "Cyber attack vulnerabilities analysis for unmanned aerial vehicles," in *Infotech@Aerospace 2012*, 2012, p. 2438.
- [5] J.-A. Maxa, M.-S. B. Mahmoud, and N. Larrieu, "Survey on UAANET routing protocols and network security challenges," *Ad Hoc & Sensor Wireless Networks*, 2017.
- [6] D. He, S. Chan, and M. Guizani, "Communication security of unmanned aerial vehicles," *IEEE Wireless Communications*, vol. PP, no. 99, pp. 2–7, 2016.
- [7] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong, "Physical layer security in UAV systems: Challenges and opportunities," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 40–47, 2019.
- [8] G. Choudhary, V. Sharma, I. You, K. Yim, R. Chen, and J.-H. Cho, "Intrusion detection systems for networked unmanned aerial vehicles: a survey," in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, 2018, pp. 560–565.
- [9] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1594–1606, 2017.
- [10] A. Koubaa, A. Allouch, M. Alajlan, Y. Javed, A. Belghith, and M. Khalgui, "Micro air vehicle link (mavlink) in a nutshell: A survey," *IEEE Access*, vol. 7, pp. 87 658–87 680, 2019.
- [11] K. Yoon, D. Park, Y. Yim, K. Kim, S. K. Yang, and M. Robinson, "Security authentication system using encrypted channel on UAV network," in *Robotic Computing (IRC), IEEE International Conference on*. IEEE, Conference Proceedings, pp. 393–398.
- [12] J. Sun, W. Wang, L. Kou, Y. Lin, L. Zhang, Q. Da, and L. Chen, "A data authentication scheme for UAV ad hoc network communication," *The Journal of Supercomputing*, vol. 76, no. 6, pp. 4041–4056, 2020.
- [13] J.-A. Maxa, M. S. B. Mahmoud, and N. Larrieu, "Extended verification of secure UAANET routing protocol," in *2016 IEEE/AIAA 35th Digital Avionics Systems Conference (DASC)*, 2016, pp. 1–16.
- [14] Y. Zeng, J. Lyu, and R. Zhang, "Cellular-connected uav: Potential, challenges, and promising technologies," *IEEE Wireless Communications*, vol. 26, no. 1, pp. 120–127, 2018.
- [15] X. Chen, D. Li, Z. Yang, Y. Chen, N. Zhao, Z. Ding, and F. R. Yu, "Securing aerial-ground transmission for NOMA-UAV networks," *IEEE Network*, pp. 1–7, 2020.

Li Wang graduated from the Henan Agricultural University in 2015. He is currently pursuing the master degree in the Xidian University, Xi'an, China. His research interests are in UAV network security.

Yu Chen is an assistant professor in the School of Information Systems and Technology and the Lucas College of Business at San Jose State University. Prior to that, she was a postdoctoral researcher at University of California, Irvine. Dr. Chen received her PhD from Swiss Federal Institute of Technology at Lausanne, Master's degrees from both Aalto University and Northwestern University of Science and Technology, and Bachelor's degree from Huazhong University of Science and Technology.

Pu Wang (wangpu@stu.xidian.edu.cn) received his B.S. degree in telecommunications engineering from the Xidian University, Xi'an, China in 2014. Currently, he is working towards a Ph.D. in cyber security at the Xidian University, China. His research interests are in UAV network security, backscatter communication, wireless information and power transfer, and physical layer security.

Zheng Yan is currently a Professor in the School of Cyber Engineering, Xidian University, China and a Visiting Professor and Finnish Academy Research Fellow at the Aalto University, Finland. Her research interests are in trust, security, privacy, and data analytics. Dr. Yan is an area editor or an associate Editor of Information Fusion, Information Sciences, IEEE Network Magazine, IEEE Access and Journal of Network and Computer Applications. She served as a General Chair or Program Chair for numerous international conferences, including IEEE TrustCom 2015 and IFIP Networking 2021. She is a Founding Steering Committee Co-Chair of IEEE Blockchain conference.