Introduction to Secure Computing Methods in Unmanned Aerial Vehicles

Soohyun Park†, Minjae Yoo†, Soyi Jung§, Minseok Choi‡, and Joongheon Kim†
†Department of Electrical and Computer Engineering, Korea University, Seoul, Republic of Korea
§School of Software, Hallym University, Chuncheon, Republic of Korea
‡Department of Electronic Engineering, Kyung Hee University, Yong-in, Republic of Korea
E-mails: soohyun828@korea.ac.kr, mj7015@korea.ac.kr,
sjung@hallym.ac.kr, choims@khu.ac.kr, joongheon@korea.ac.kr

***Abstract*—This paper reviews recent researches on security issues in unmanned aerial vehicles (UAVs)-based networks. We categorize the recent studies into secure communications and secure resource management in UAV-based networks, and provide the trends of state-of-the-art techniques. Lastly, future research directions on secure communication and computing for UAVs are summarized.**

I. Introduction

Nowadays, UAVs are utilized for various purposes, such as small mobile base stations (BSs), unmanned surveillance aircraft, and environmental observation equipment for smart urban or harbor environments. The recent developments of communication technology beyond 5G to 6G which is combined with edge computing technology enables high-speed computations and low-latency communication to support UAV-based networks. Furthermore, various types of UAVs have been produced, such as cluster UAVs, ultra-small UAVs, and drone-taxi [1]–[3]. In addition, multiple studies have been conducted to overcome the physical limitations of UAVs and to efficiently manage the limited resources of UAV networks according to the system's goal of use [4], [5].

In practical scenarios, UAVs construct networks with peripheral elements such as IoT devices, mobile devices, BSs, and virtual servers (e.g., cloud or edge server). As massive data traffic is generated in these UAV-to-everything networks, data loss or malicious attacks could be critical to not only driving control and data management of UAVs but also that of other components connected with UAVs. For this reason, research on network management and communication technology considering data privacy and security protection in UAV-based networks is attracting attention as an essential research subject and approaching from various perspectives. This paper classifies potential security issues in UAV-based networks and provides the trends of state-of-the-art techniques to address them. The rest of this paper is organized as follows. Sec. II overviews the data privacy issues of UAV-based networks and presents various research results for the security issues of UAV networks. Sec. III describes future research directions. Lastly, Sec. IV concludes this paper.

II. Security-Preserving Solutions for UAV Based Networks

UAVs are widely used in mobile networks and distributed systems due to their advantages such as low cost, high mobility, and scalability. However, there are practical limitations in UAV networks, e.g., limited battery, high uplink speed requirements for real-time video streaming, and we focus particularly on potential security threats in wireless data transmissions of UAVs. The potential security threats in UAV-based networks at the physical layer are subdivided into malware, malicious insider, service disruptment, man-in-the-middle, and sppofing, as shown in Fig. 1. This section introduces the latest studies dealing with these potential security threats by categorizing them into secure UAV communications and secure resource management.

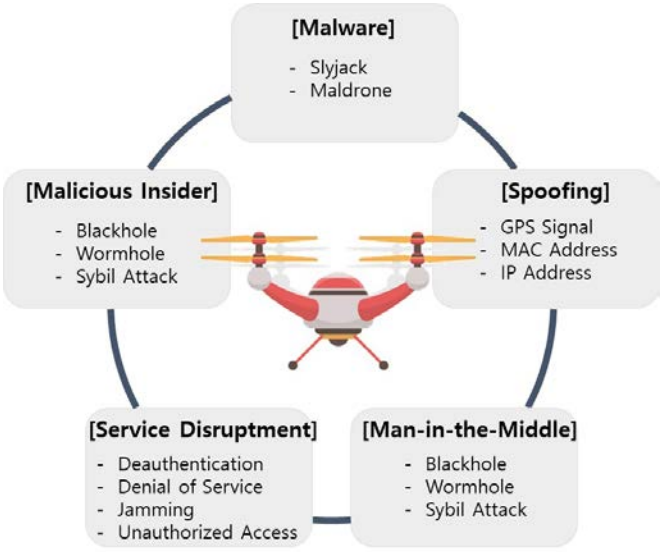

Fig. 1: Potential security threats in UAV networks

A. Secure UAV communications

In UAV networks, air-to-ground radio channels' broadcast and line-of-sight (LoS) characteristics can cause security vulnerabilities in data transmission. To improve the security

performance, a method is proposed to support legitimate data transmission through an area-based security measure called Intercept Probability Security Region (IPSR) which is based on Internet Protocol (IP) in applications that emit artificial noise [6]. An artificial neural network (ANN) is used for predicting future network changes and ensuring safe UAV operation by adaptively optimizing UAV controls and efficiently managing resources [7]. Also, the high mobility of UAVs is utilized to improve the fundamental confidentiality of UAV-to-ground communications while jointly optimizing trajectory and power controls [8]. Another study ensures stable wireless connectivity of cellular-connected UAV applications (e.g., delivery, taxi, VR application, traffic monitoring, accident investigation, and public safety) using deep learning and solves interference management and authentication problems [9].

In addition, there are several studies to deal with security issues related to abnormal intrusion detection, various security attacks, and authentication/access control in MEC systems using UAVs. To address security issues in edge server-connected networks, a new framework has been proposed that ensures the security of user identity authentication based on detection, defense, and authentication capabilities and allows timely security measures through effective early warning [10]. Also, when there are eavesdroppers and radio jamming attacks in UAV networks, collaborative remote jamming was proposed to efficiently identify and address attacks from a perspective of physical layer security [11].

B. *Secure resource management*

When UAVs have a role of mobile BSs, there could be resource sharing among UAVs through UAV swarm or multi-UAV system; therefore, some studies maximize the advantage of participating stakeholders to efficiently exchange costly resources (e.g., energy, data, money, etc.). There is a study that proposes a novel deep reinforcement learning model that includes Convolution Neural Turing Machines (ConvNTM). For all UAVs, it is possible to simultaneously make work decisions such as route and data collection or charging. This optimizes the cost of using resources [12]. Another solution is a hierarchical Stackelberg game framework for UAV access choice and BS bandwidth allocation [13]. In UAV and edge server-based environments, the problem of pricing resources and offloading risk-aware data can also be presented [14]. This problem is formulated as a distributed maximization problem of each user's expected prospect-theoretical utility function and is solved by switching to an uncooperative game between users. Another recent study uses the pricing Stackelberg game to formulate action utilities between UAVs, cluster headers, and BSs. The purpose of maximizing profits is achieved by optimizing the price of providing security as a service in the UAV cluster network [15].

Security resources can be deployed in the cloud or edge server, which can efficiently provide offloading and security services to UAVs with high bandwidth and low latency. Various studies have also been conducted to target managing security resources on the edge servers.

A new privacy security spectrum sharing mechanism based on blockchain technology between UAVs and terrestrial cellular networks solves security challenges in wireless transmission and jointly maximizes the benefits of mobile network operators (MNOs) and UAV operators [16].

Among the studies for security resource allocation present in edge servers, there is a study that assumes a software-defined air-ground integrated network consisting of UAVs, 5G BSs, and mobile edge computing (MEC) node groups [17]. In this work, the proposed solution jointly optimizes security and radio resource allocation in air-ground integrated networks (AGNs) based on software-defined networks (SDNs), while integrating cooperation and competition functions between UAVs and MEC nodes. In more detail, the authors introduce a non-cooperative game to model competition between UAVs in situations where security and radio resources are limited. The MEC nodes play a coalition game to share security and radio resources and build a coalition to improve profits. This solves limited resource sharing problems, reduces transmission delays in UAV-based networks, and smoothly responds to external attacks through optimized security resources [17].

Furthermore, there is a study considering the environment in which eavesdropping UAV exists, and its location is uncertain [18]. In this work, low complexity iterative algorithm is utilized to maximize the minimum security capacity under delay, minimum offloading, and total power constraints. The proposed algorithm can jointly optimize the UAV position, transmission power, UAV jamming power, offloading ratio, UAV computing capacity, and offloading association.

III. Potential Future Research Directions

To improve the security performance of UAV-to-everything networks, we can consider the following future research directions.

A. *Distributed AI for UAV environments*

Several studies have been conducted using federated learning (FL) and multi-agent deep reinforcement learning (MADRL) to effectively control UAV communications and resource management in a distributed mobile environment such as UAV-based networks in consideration of physical characteristics of UAVs [19]–[21]. It has already been proven that distributed artificial intelligence (AI) algorithms provide good performances in UAV environments such as UAV flight policy control, optimal power charging in multi-UAV environments, and communication resource allocation in UAV-based surveillance environments [1]–[5], [21]. Further researches on data privacy and security can be conducted in-depth through the pre-research technologies based on the distributed AI which is optimized for the physical limitations of UAV systems or UAV mobility and flexibility.

B. *Combination with digital twin technique*

It is expected to combine the UAV-based network with digital twin (DT), which can simulate real-world problems in

a virtual environment. DT allows real UAV-to-everything networks with heterogeneous network characteristics and physical limitations of UAVs (e.g., weight, hovering time, fuel limit, etc.) to be modeled on virtual environments. In this way, combined with DT, it is possible to predict the results of security enhancement techniques optimized for UAV systems. Moreover, in this process, data privacy issues arise from a data transmission perspective since data transfer between the real world and the virtual world is essential. Ensuring real-time and secure transmission and preventing malicious attacks and eavesdropping from outside in the process of delivering large amounts of data may attract attention as a new research subject.

C. Accessing through mmWave channel characteristics

Millimeter-wave (mmWave) channel is utilized for 6G communications to support high data transmission rates by supporting abundant frequency bands. Performances of UAV communications in mmWave bands, which finds potential eavesdroppers and resolves data privacy or security issues, are still strongly dependent on the availability of LOS channels. For this reason, considering mmWave channel characteristics to utilize the huge bandwidth is important to avoid potential eavesdropping and ensure the communication speed required by the UAV network.

IV. Conclusions

In this paper, various security issues in the UAV environment and related technology trends are investigated and classified. Security in the UAV environment has been mainly studied on the physical layer of communication, and there are several kinds of research applying economic theory, optimization theory, and AI. Through this research survey, we can predict future research trends on security issues in UAV environments. In addition, at the end of the paper, we propose research directions that can be extended through combination with various technologies.

Acknowledgment

This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2022-2017-0-01637) supervised by the IITP(Institute for Information & Communications Technology Planning & Evaluation). J. Kim is a corresponding author of this paper.

References

[1] W. J. Yun, S. Park, J. Kim, M. Shin, S. Jung, A. Mohaisen, and J.-H. Kim, "Cooperative multi-agent deep reinforcement learning for reliable surveillance via autonomous multi-uav control," *IEEE Transactions on Industrial Informatics*, pp. 1–1, March 2022.

[2] W. J. Yun, S. Jung, J. Kim, and J.-H. Kim, "Distributed deep reinforcement learning for autonomous aerial evtol mobility in drone taxi applications," *ICT Express*, vol. 7, no. 1, pp. 1–4, 2021.

[3] S. Park, W.-Y. Shin, M. Choi, and J. Kim, "Joint mobile charging and coverage-time extension for unmanned aerial vehicles," *IEEE Access*, vol. 9, pp. 94 053–94 063, June 2021.

[4] S. Jung, W. J. Yun, M. Shin, J. Kim, and J.-H. Kim, "Orchestrated scheduling and multi-agent deep reinforcement learning for cloud-assisted multi-UAV charging systems," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 5362–5377, June 2021.

[5] M. Shin, J. Kim, and M. Levorato, "Auction-based charging scheduling with deep learning framework for multi-drone networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, pp. 4235–4248, May 2019.

[6] Y. Zhou, P. L. Yeoh, H. Chen, Y. Li, R. Schober, L. Zhuo, and B. Vucetic, "Improving physical layer security via a uav friendly jammer for unknown eavesdropper location," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 11 280–11 284, September 2018.

[7] R. Han, L. Bai, J. Liu, J. Choi, and Y.-C. Liang, "A secure structure for uav-aided iot networks: Space-time key," *IEEE Wireless Communications*, vol. 28, no. 5, pp. 96–101, November 2021.

[8] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing uav communications via joint trajectory and power control," *IEEE Transactions on Wireless Communications*, vol. 18, no. 2, pp. 1376–1389, October 2019.

[9] U. Challita, A. Ferdowsi, M. Chen, and W. Saad, "Machine learning for wireless connectivity and security of cellular-connected uavs," *IEEE Wireless Communications*, vol. 26, no. 1, pp. 28–35, February 2019.

[10] A. Yao, F. Jiang, X. Li, C. Dong, J. Xu, Y. Xu, G. Li, and X. Liu, "A novel security framework for edge computing based uav delivery system," in *Proc. of the International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Shenyang, China, October 2021, pp. 1031–1038.

[11] Q. Wu, W. Mei, and R. Zhang, "Safeguarding wireless network with uavs: A physical layer security perspective," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 12–18, October 2019.

[12] C. H. Liu, C. Piao, and J. Tang, "Energy-efficient uav crowdsensing with multiple charging stations by deep learning," in *Proc. of the IEEE International Conference on Computer Communications (INFOCOM)*, ON, Canada, August 2020, pp. 199–208.

[13] S. Yan, M. Peng, and X. Cao, "A game theory approach for joint access selection and resource allocation in uav assisted iot communication networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1663–1674, April 2019.

[14] P. A. Apostolopoulos, G. Fragkos, E. E. Tsiropoulou, and S. Papavassiliou, "Data offloading in uav-assisted multi-access edge computing systems under resource uncertainty," *IEEE Transactions on Mobile Computing*, pp. 1–1, April 2021.

[15] G. Bansal, V. Chamola, B. Sikdar, and F. R. Yu, "Uav secaas: Game-theoretic formulation for security as a service in uav swarms," *IEEE Systems Journal*, pp. 1–10, April 2021.

[16] J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, "Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operator's perspective," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 451–466, January 2020.

[17] Y. Wang, Z. Su, N. Zhang, A. Benslimane, R. Li, and Y. Wang, "Security-aware resource sharing in software defined air-ground integrated networks: A game approach," in *Proc. of the IEEE Global Communications Conference (GLOBECOM)*, Taipei, Taiwan, December 2020, pp. 01–06.

[18] Y. Zhou, C. Pan, P. L. Yeoh, K. Wang, M. Elkashlan, B. Vucetic, and Y. Li, "Secure communications for uav-enabled mobile edge computing systems," *IEEE Transactions on Communications*, vol. 68, no. 1, pp. 376–388, January 2020.

[19] H. Lee and J. Kim, "Trends in blockchain and federated learning for data sharing in distributed platforms," in *Proc. of the International Conference on Ubiquitous and Future Networks (ICUFN)*, Jeju, Korea, August 2021, pp. 430–433.

[20] S. Park, Y. Kang, J. Park, and J. Kim, "Self-controllable super-resolution deep learning framework for surveillance drones in security applications," *EAI Endorsed Transactions on Security and Safety*, vol. 7, no. 23, June 2020.

[21] W. J. Yun, D. Kwon, M. Choi, J. Kim, G. Caire, and A. F. Molisch, "Quality-aware deep reinforcement learning for streaming in infrastructure-assisted connected vehicles," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 2, pp. 2002–2017, Febuary 2022.