Cyber Threats and Cybersecurity Reassessed in UAV-assisted Cyber Physical Systems

Majumder Haider
Department of Electrical Engineering & Computer Science
Howard University
Washington, DC, USA
majumder.haider@bison.howard.edu

Imtiaz Ahmed
Department of Electrical Engineering & Computer Science
Howard University
Washington, DC, USA
imtiaz.ahmed@howard.edu

Danda B. Rawat
Department of Electrical Engineering & Computer Science
Howard University
Washington, DC, USA
danda.rawat@howard.edu

***Abstract*—This study aims to perceive the potential security threats in unmanned aerial vehicles (UAVs) assisted communication networks and to determine the feasible and effective security solutions in order to ensure secured UAV assisted cyber physical system (CPS) (UAV-a-CPS). Fifth generation (5G) and beyond wireless technology is capable to provide support for a plethora of data hungry and time sensitive applications. UAV is one of the vital features of 5G and beyond cellular technology to be deployed in a wide gamut of applications. Since the application domain of UAV networks includes civilian, aviation, and military sectors, thus it can be a prime target to the hackers. This work emphasizes the security issues that require to be prioritized and addressed with appropriate security measures to make UAV-a-CPS secured and safe enough for commercial applications. Moreover, we provide several innovative, scalable, and insightful design considerations to encounter security threats inherent to UAV networks. It is shown that the multi-layer based adaptive security approaches would be beneficial to protect UAV-a-CPS from the potential and emerging security threats effectively. Finally, we provide probable futuristic research directions to add newer dimensions in these arena.**

***Keywords*—Unmanned aerial vehicles (UAVs), cybersecurity, cyber physical system (CPS), energy efficiency, 5G and beyond.**

I. Introduction

Unmanned aerial vehicles (UAVs) can also be named as flying ad-hoc wireless devices (FAWD) or drones are receiving noteworthy attention now-a-days due to have greater possibility of line of sight (LoS) links to the terrestrial users and flexible infrastructures with cost efficient implementation and greater mobility. The application field of FAWD is not limited to military and aviation sectors, it is gaining exponential growth in terms of civilian applications as well [1]. UAVs are capable to provide temporary cellular network coverage in areas, where fixed network infrastructure has been affected due to natural calamities. UAV-assisted ad-hoc wireless networks can be an alternative way acting as aerial base station to provide telecommunication network privileges to the remote places, where establishing fixed cellular infrastructure is expensive, inefficient, and not fruitful because of limited number of users. UAVs are also useful for emergency rescue operations, weather monitoring, industrial infrastructure monitoring, logistics, quick disaster management to the affected areas, and military surveillance and battle mission applications [1]–[3]. It is speculated by United States (US) federal aviation administration (FAA) that the demand of commercial UAVs implementation would be triple by 2023 [4]. Many countries are investing a large amount of money for the large scale commercial deployment of UAV because of its immense prospects. Despite of having rising potentials and versatile applications of UAV, several challenges exist in UAV-assisted networks such as route planning, security, privacy, collision avoidance, energy consumption, and delay optimization [5]–[7]. In order to bring out the full benefits of UAVs, it is imperative to address these challenges proactively and efficiently.

Cyber physical systems (CPSs) are a new breed of systems that combine computational and physical potentials to interact with humans through a variety of different controllable processes. UAVs would be an ideal CPS due to have three main parts of CPS like powerful computation unit, ad-hoc wireless communication systems, and adjustable control unit. The key benefits of deploying UAVs in CPS applications are their unconventional properties, such as mobility, easy deployment, adaptable altitude, tailored control, and excellent assessment of real-world functions at any time and at any location [8], [9]. Despite of offering wider promises as ideal CPS, UAV-assisted CPS (UAV-a-CPS) is easily vulnerable because of the unforeseen and unregulated settings, the open wireless communication channel, three dimensional placement, and the lack of appropriate security standards.

Security is a crucial aspect in any CPS, therefore, security issues in CPS need to be addressed with high priority to make

This research was funded in part by the US National Science Foundation under the grant number CNS/SaTC 2039583 and by the DoE/NNSA grant. However, any opinion, finding, and conclusions or recommendations expressed in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the funding agencies.

the system reliable and secured for commercial deployment [10], [11]. In present times, the researchers are focusing on the security issues of UAV-a-CPS with high importance and investigating feasible and efficient security solutions to protect the systems [1], [12], [13].

In this work, security issues, challenges and efficient protection initiatives have been revisited from UAV-a-CPS perspective. Potential and emerging security threats in different layers of UAV-a-CPS has been discussed in details. Moreover, we proposed combination of AI assisted layer-based adaptive security approaches that would be instrumental to guard the UAV-a-CPS in an effective manner.

Related works have been illustrated in section II. In section III, the architecture and characteristics of UAV-a-CPS have been described. Security and privacy concerns in UAV-a-CPS have been focused in section IV. In section V, potential cyber threats from UAV-a-CPS perspective have been articulated. Section VI briefly discusses the challenges when implementing new security solutions in UAV-a-CPS. The effective approaches to defend the security threats have been highlighted in section VII, and the insightful conclusions have been made in section VIII.

II. Related Work

Significant contributions have been made to identify the potential and emerging challenges in UAV-a-CPS underlining security and safety concerns [14]–[24]. In [14], [15], the authors highlighted the potentiality of existing communication technologies in order to fulfill the prospects of UAV assisted networks in civilian applications along with the enhancement of safety and scalable connectivity requirements. The authors also highlighted the security concerns from communication networks perspective in different data sharing stages such as UAV-to-UAV, UAV-to-cellular infrastructure and UAV-to-satellite networks. Moreover, the authors reviewed the threat mitigation techniques to protect confidentiality issues. In [16]–[24], the authors illustrated a comprehensive survey on security and privacy challenges and network vulnerabilities in UAV-a-CPS. Furthermore, the researchers recommended different measures and technologies to ensure safety and privacy in UAV-a-CPS. Theft and vandalism are considered as severe cyber threat in UAV-a-CPS in [21]. In [25], the authors emphasized on the secured UAV communications in 5G networks highlighting the impact of promising technologies such as multiple antenna and smart interference management that can reduce the eavesdropping cyber attack. The authors in [26], [27] discussed about a wide range of emerging applications of UAV-a-CPS and the challenges for commercial deployment.

In this review, we study the existing challenges of UAV-a-CPS underlining security vulnerability and safety issues and investigate how innovative and scalable technologies and approaches can be blended to provide efficient security solutions to secure UAV-a-CPS. We demonstrated that multi-layer based security techniques and adaptive approaches can actively protect UAV-a-CPS from potential cyber threats.

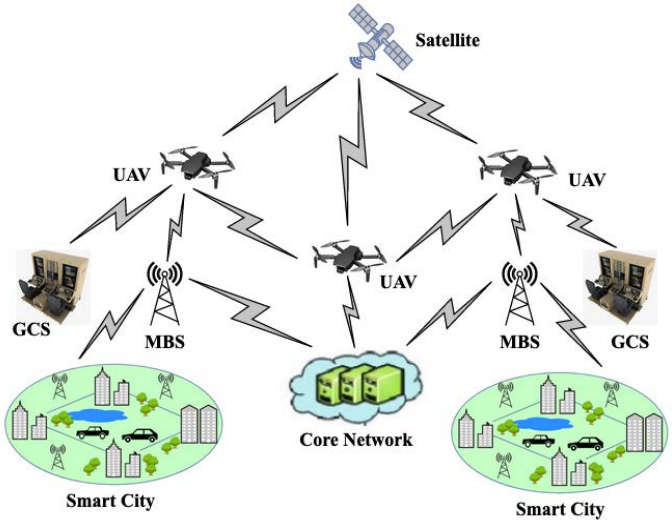

Fig. 1: Architecture of UAVs networks.

III. Architecture and Characteristics of UAV Assisted Cyber Physical Systems

In this section, we described the general architecture of UAV networks along with the characteristics of UAV-a-CPS.

A. Architecture of UAVs Wireless Networks

UAVs are aircrafts or quadcopters that can fly without the need for a pilot on board. The exterior structure including interior design and control mechanism of UAVs can vary considering the varied application requirements and the condition of operational environments. The flight control unit, sensor payloads, wireless communications module, and a ground control station (GCS) build up the overall structure of unmanned aircraft systems. Fig. 1 depicts the general architecture of UAV driven wireless ad-hoc networks. UAV can be operated by on board electronic equipment or from the ground via remote control equipment with the aid of reliable and very high-speed wireless communication networks. The main part of the hardware section of the UAV is the flight control unit, which consists of powerful micro controller unit responsible for computation, control and data storage, and rechargeable batteries to supply the required energy for all operations. The sensor payloads equipped with different sensors, accelerometers, actuators, GPS module for position and navigation purposes, and high resolution cameras to collect images. The communication module includes very high-speed wireless interface and antennas to transmit and receive control signals and data. The ground control station comprised with a remote controller module to control UAVs and its activities, wireless communication module to maintain communication with UAVs and graphical user interface (GUI) integrated monitoring software to visualize the activities of UAVs. There are mainly two types of radio communications that occur in a typical UAV-assisted communication networks; UAV-to-UAV and the communication between UAV to any other objects denoted as UAV-to-X communications. Since UAV

is an unmanned aircraft, flight control, navigation, decision making, and data transmission and reception are controlled by the remote controller from the GCS. This leads UAV systems dependent on appropriate wireless networks. The 5G cellular networks can be truly heterogeneous, hence, the coordination of UAV systems with multiple technologies is a significant challenging task in order to ensure smooth wireless networking and uninterrupted services. The communication processes in UAV assisted systems can be affected due to irregular mobility of UAVs, interference in densed networks, and multipath fading effect in urban areas. Efficient interference management technique needs to be utilized to meet these challenges.

B. Characteristics of UAVs Cyber Physical Systems

CPS offers an embedded physical and cyber domain system, where three main operations of CPS named computation, communication, and control are achieved while serving the desired purposes. The national aeronautics and space administration (NASA) first advocated CPS in space explorations involving drones. Later, it is applied to military applications to lessen human injuries or even to save lives in battle mission, with a view to controlling weapons remotely without participating directly in the target spot. Now-a-days, the concept of UAV-a-CPS is widely deployed in industrial applications and many other areas of civilian applications [26].

It is anticipated from a typical CPS to conduct real-time and reliable monitoring and control of physical entities, as well as to improve the efficiency of resource management and performance optimization. In a similar way, the UAV integrated networks work by initializing data collection in terms of sensing physical parameters of interests, information exchange through wireless communication networks, decision making by the control unit through rigorous computation and programming, and finally the execution of the decision. Therefore, UAV-assisted system has all the required units of a typical CPS. An overview of UAV-a-CPS is shown in Fig. 2. Based on the structure of the CPS and the number of operating UAVs, UAV-a-CPS can be categorized in different ways. In multiple UAV-a-CPS the coordination among the components to ensure seamless operation and tasks management is a challenging task. Artificial intelligence (AI) driven approaches can shed light to address these challenges effectively. Moreover, machine learning based approach offers full scalability to optimize the UAVs route planning to avoid collision and interference issues and coordination among different units to improve the performance of UAV-a-CPS significantly.

IV. Security and Privacy Concerns in UAVs CPS

The secured UAV-a-CPS must ensure control and access of the system by authorized users only. This section illustrates the primary security and privacy concerns that need to be addressed properly in order to design a secured UAV-a-CPS.

A. Data Integrity

Data integrity signifies that data is not altered while in transit toward the intended users. Since, there is no on board

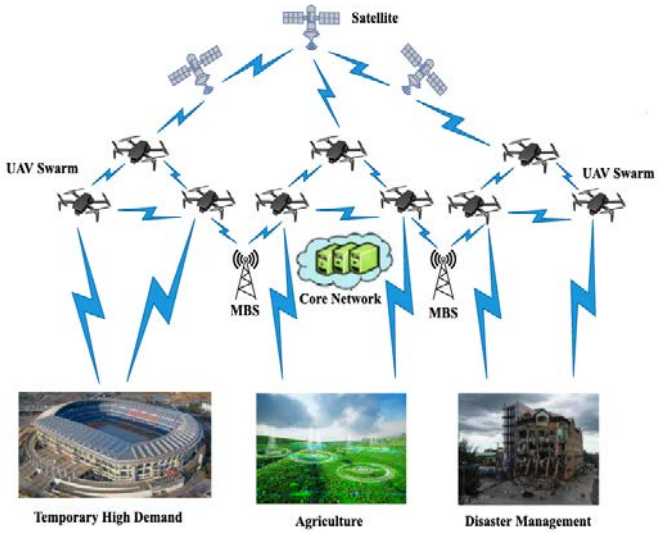

Fig. 2: UAV assisted cyber physical systems.

driver in UAVs, the whole operation is based on the data and control signal from the remote controller. Therefore, data integrity is crucial in UAV-a-CPS to perform designated tasks efficiently and safely. If data integrity is not ensured, then data manipulation through man-in-the-middle attack can confuse the UAVs and even can make the flight operation fall in vain. Data integrity has to be guaranteed in order to design secured UAV-a-CPS. To ensure data integrity, encrypted data sharing and strongly secured authentication mechanisms need to be deployed.

B. Data Confidentiality

Data privacy means data is not shared or made available to unauthorized and unintended users. The sensors incorporated in UAV networks collect plethora of confidential data that need to be protected in an appropriate manner. The cameras of UAVs take confidential targeted images while flying, which can include some undesired images as well. These undesired images can reveal the privacy of the people and valuable resources. The undesired images have to be protected or even be discarded in a secured way to certify confidentiality. In consequence, proper security mechanism is essential in UAV networks to handle targeted images in an organized way. Moreover, the security techniques need to guarantee that the undesired images are properly discarded and cannot be retrieved. Encrypted authentication and authorization, and highly secured device-to-device pairing and data sharing approaches can provide data confidentiality in UAV-a-CPS.

C. Authentication and Authorization

Proper authentication and authorization to access the systems and avail the expected services is vital in CPS. The ground control station primarily control and regulate the overall operation of UAVs remotely. It is imperative to guard any unauthorized access in the remote control system by implementing effective and encrypted security authorization

technique. Moreover, authorized users also need to be authenticated each time to certify the accountability and secured access in the control systems. Suitable virtual private network (VPN) technique should be implemented to promote secured authentication and authorization in UAV aided communication systems.

D. False Data Injection

False or unauthenticated data injection in UAV-a-CPS can ultimately ruin the performance of the systems and its impact on beneficiaries. When UAV-a-CPS are implemented for example in agriculture sector to predict authentic weather information, false data injection can provide wrong weather forecasts and ultimately mislead the farmers and entrepreneurs. Hence, it leads to undertake wrong decision and consequences severe financial loss. It is a rising threat in CPS and it should be addressed effectively in order to certify secured CPS.

E. Data Fabrication

Intended false representation of data while transmitting or receiving can severely hamper the flight operation of UAVs. Data fabrication can also mislead the ground controller to control the UAVs as expected, and it can deliver false information of several sensors status of UAVs to the controller by the hackers. Therefore, only authorized access and highly secured and encrypted data sharing strategy can lower the chances of data fabrication threats.

V. Potential Cyber Threats in UAVs CPS

The major potential and emerging cyber threats and its detrimental effects in UAV-a-CPS are articulated in this section.

A. Unauthorized Access

Unauthorized access in control system is considered as the main threats in UAV-a-CPS since this is the gateway to enter in the system. As there is no on-board controller in UAVs, any unauthorized access in the remote control system will gain the permission to control the overall UAV networks. After gaining unauthorized access in the control system, hacker can easily control the flight operation of UAV as per the hacker desire and even can hijack the UAV. The system loses its data integrity and confidentiality features through unauthorized access. It is worth mentioning that unauthorized or intruder access in the control system actually make the overall UAV system unsecured. Therefore, unauthenticated and unauthorized access has to be guarded effectively in order to keep UAV-a-CPS secured and protected.

B. GPS Spoofing and Jamming

UAV-a-CPS always maintain strong wireless communication with global positioning system (GPS) satellites and low altitude aerial repeaters to keep updated its location information in real time and other navigation purposes. GPS spoofing is a well-known example of false sensor data injection attacks. Because GPS signals are frequently unencrypted and unauthenticated, the attacker uses a spoofing attack on the GPS to modify the UAV's GPS receiver by mimicking the generated signal. As a result, the attacker gains complete control over the UAV. In [28], [29], the authors illustrated the damaging impact of GPS spoofing in UAV-a-CPS and how it causes the CPS unsecured. The drone can be forced to respond to false signals as a result of the GPS spoofing attack and it can completely disrupt its navigation system.

Besides GPS spoofing, GPS jamming is also a crucial threat, which is less difficult to implement than spoofing. Jamming occurs when an opponent sends out a distracting signal that hinders normal signals from being received and decoded, causing the UAV to become disoriented and disconnected from the GCS that leads to crash. The genuine or true position information of the drone must be maintained in order to maintain identity privacy. When a dispute arises, however, the proper authority can effectively race and arbitrate it. Necessary initiatives should be taken in order to prevent allowing unauthenticated drones to fly in the skies, and mutual authentication is required for secure communication to ensure that the identification of drones is not revealed.

C. False Sensor Data Injection

False sensor data injection target on-board sensors, accelerometers, and actuators that are dependent on sensing external environment conditions. The purpose of this cyber attack is to destabilize UAVs by compromising a collection of sensors and introducing falsified readings into the flight controller, hence jeopardizing the control system and the flight mission of the drones.

D. DoS Attack

Interception, spoofing, jamming, and denial of service (DoS) are examples of link attacks between UAVs and ground control station [24]. An attacker floods the link between UAVs and GCS with fake data packets to keep it busy while preventing it from receiving any useful data from UAVs. The hacker can easily do such activity if the communication link is not encrypted. In most cases, the attackers intercept real GCS communications, give the required instructions to the UAV, and then broadcast the expected responses to the GCS, like a man-in-the-middle assault.

E. Wireless Interface Attack

To maintain continuous contact with satellite repeaters, GCS, cellular base station, and other UAVs, typical UAVs utilize several wireless interfaces. Due to weak security features (WEP and WPA) of Wi-Fi access technology, the system is easily vulnerable. This level of sophistication, along with the physical and mechanical properties of UAVs, broadens the breadth of potential vulnerabilities and opens the door to a variety of attacks targeting UAV communication units.

Furthermore, automatic dependent surveillance-broadcast (ADS-B) plays a pivotal role as an aircraft operation monitoring system based on GPS for ground-to-air, and air-to-air data connection communications. Despite the fact that only a few UAVs are equipped with an ADS-B system, it must be an essential strategy for avoiding collisions with other

human and unmanned aircraft. UAVs equipped with ADS-B will automatically broadcast their location, altitude, speed, heading, identification number, and other data to other aircraft or ground stations within a certain range without the need for manual intervention while allowing the UAV operators to keep track of the aircraft's status by exchanging unencrypted and unauthenticated ADS-B signals [30]. Due to the inability to identify or validate the ADS-B warning, such signals can easily be jammed or replaced by fraudulent entities, putting UAVs in danger of crash.

F. Skyjack Attack

Skyjack is an emerging cyber threat in UAV-a-CPS that is capable to hijack nearby flying drones that are within the wireless perimeter of hacker drone [31]. First, the hacker drone finds medium access control (MAC) address of the neighbor drones within its Wi-Fi perimeter and then disconnects the victim drone from the control station. Then the controller of the hacker drone gains access to take the overall control of the victim drone.

VI. Challenges in Protecting UAV-a-CPS

This section highlights the major challenges that need to be addressed while implementing new prospective techniques to make UAV-a-CPS more secured and safe.

A. Energy Efficiency

UAVs are battery powered digital electronic device that can perform the desired flight mission with limited energy storage. Therefore, any new initiatives to ensure improved security features must be energy efficient. Otherwise, new security technique may not be a feasible solution in UAV-a-CPS considering the energy constraint. Appropriate optimization techniques can be reevaluated parallel to the security initiatives in order to provide secured energy efficient communications in UAV-a-CPS.

B. Latency Awareness

Low latency communication is one of the generic features under ultra reliable low latency communication (URLLC) in 5G and beyond wireless networks. To ensure security in UAV-a-CPS, new security approaches should not increase transmission latency in UAV communication networks. Security initiatives that increase latency can make the UAV-a-CPS inappropriate for several time sensitive applications.

C. Complexity Reduction

The skyrocketing demands of data greedy applications of UAV assisted communication systems make the architecture of the network much complicated. Due to the limited battery energy and computational processing ability, the complexity of the structure of UAV should not be increased while offering intensive amenities, additional services and security benefits. Smart computational offloading can be an effective approach to reduce computational complexity at the end of UAVs. Since UAVs are battery powered digital electronic devices, thus energy storage has to be efficiently managed to complete the desired mission. Tasks offloading concept [6] either on ground or air in UAV networks can assist to provide desired services while reducing the computational burden in UAV intelligently. It is important to keep in mind that new security techniques also need to be optimized in such a way that it would be compatible without increasing the computational and circuital complexity in UAV-a-CPS.

VII. Cybersecurity Approaches in UAV-a-CPS

In order to secure the UAV-a-CPS, there is no alternative of standardizing wireless security protocols solely for UAV communication networks. We propose a blend of emerging security techniques in Table I to protect UAV-a-CPS from potential cyber threats while keeping the security challenges in mind.

TABLE I: Proposed security approaches

Proposed Security Initiatives	**Features**	**Benefits Over Existing Approaches**
No-trust authentication	Identity-centric approach that combines runtime authorization choices with classic defense-in-depth security concepts [32]. This protocol will be coordinated at the ground station and will ensure that no illegal UAVs stay inside the designated aerial network.	This technique will assist the aerial system to significantly limit the chances of an external attacker gaining unauthorized access to the network as well as the risk of lateral movement in the event of a security breach instead of existing perimeter-based implicit trust method.
Lightweight cryptographic protocols	A lightweight mutual authentication protocol can provide energy-efficient and secure communications among drones and ground stations effectively by integrating advanced encryption standard (AES) to encrypt information of the transceiver [33].	Energy-efficient and low-consumption of computational resources will be emerged while rendering secured communications compared to current cryptographic encryption protocols that offer basic security services while consuming high energy and computational resources.
AI assisted jam-resilient aerial waveform design	The low probability interception and detection (LPID) property of a transmit signal makes it difficult for an adversarial transceiver to discover and extract relevant information from its broadcasts [34].	Conventional methods, such as spread-spectrum-based jam-resistant signaling techniques have the potential to be readily predictable while compromising the system's security. In contrast, an autoencoder based approach to generate transmit waveforms from ground station to drones and vice-versa yields promising outcomes to encounter potential jamming signals.
AI driven blockchain	AI driven blockchain-based security mechanism is efficient to ensure data integrity and confidentiality through offering transparency [35] in UAV-a-CPS.	Its scalable and adaptive layer-based natures can yield robust security in UAV-a-CPS rather than ordinary security mechanisms.

The proposed security initiatives can outweigh the existing security mechanisms efficiently. The multi-layer and adaptive

functionalities of the proposed security approaches offer applications specific customized features to contribute appropriate shield against potential cyber threats in UAV-a-CPS. The proposed security techniques with the aid of AI can offer robust security to ensure effective protection in UAV-a-CPS considering the constraints.

VIII. Conclusion

This paper reassessed potential and emerging cyber threats and proposed suitable cybersecurity approaches in UAV-a-CPS. Complicated security mechanisms cannot be suitable for deployment in UAV-a-CPS due to its limited computational processing ability and energy constraint. UAV-a-CPS has a plethora of sophisticated applications in military and civilian sectors. Due to weak security system, the UAV-a-CPS is still vulnerable to cyber attacks, which hinders massive commercial deployment. In summary, it can be stated that the proposed multi-layer and applications oriented adaptive security techniques can secure UAV-a-CPS while meeting up the existing security challenges. In near future, AI-based security initiatives will be explored extensively to provide advanced security solutions against emerging cyber threats in UAV-a-CPS to fulfill the rising expectations of beyond 5G networks.

References

[1] H. Sedjelmaci, S. M. Senouci and N. Ansari, "A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1594-1606, Sept. 2018.

[2] H. Shakhatreh et al., "Unmanned Aerial Vehicles (UAVs): A Survey on Civil Applications and Key Research Challenges," in *IEEE Access*, vol. 7, pp. 48572-48634, 2019.

[3] N. H. Motlagh, M. Bagaa and T. Taleb, "UAV-Based IoT Platform: A Crowd Surveillance Use Case," in *IEEE Communications Magazine*, vol. 55, no. 2, pp. 128-134, February 2017.

[4] Federal Aviation Administration, "FAA National Forecast FY 2019-2039 Full Forecast Document and Tables," *Tech. Rep*. [Online] Available: https://www.faa.gov/data˙research/aviation/aerospace˙forecasts/media/fy 2019-39˙faa˙aerospace˙forecast.pdf

[5] T. Zahariadis, A. Voulkidis, P. Karkazis and P. Trakadas, "Preventive maintenance of critical infrastructures using 5G networks & drones," *2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, 2017, pp. 1-4.

[6] A. A. Ashraf Ateya, A. Muthanna, R. Kirichek, M. Hammoudeh and A. Koucheryavy, "Energy- and Latency-Aware Hybrid Offloading Algorithm for UAVs," in *IEEE Access*, vol. 7, pp. 37587-37600, 2019.

[7] Y. Zeng, J. Lyu and R. Zhang, "Cellular-Connected UAV: Potential, Challenges, and Promising Technologies," in *IEEE Wireless Communications*, vol. 26, no. 1, pp. 120-127, February 2019.

[8] HR. Shakeri et al., "Design Challenges of Multi-UAV Systems in Cyber-Physical Applications: A Comprehensive Survey and Future Directions," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3340-3385, Fourthquarter 2019.

[9] H. Wang, H. Zhao, J. Zhang, D. Ma, J. Li and J. Wei, "Survey on Unmanned Aerial Vehicle Networks: A Cyber Physical System Perspective," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1027-1070, Secondquarter 2020.

[10] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security-a survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017.

[11] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, "Security and privacy in cyber-physical systems: A survey of surveys," *IEEE Design & Test*, vol. 34, no. 4, pp. 7–17, Aug. 2017.

[12] G. Panice et al., "A SVM-based detection approach for GPS spoofing attacks to UAV," *2017 23rd International Conference on Automation and Computing (ICAC)*, pp. 1-11, 2017.

[13] L. Petnga and H. Xu, "Security of unmanned aerial vehicles: Dynamic state estimation under cyber-physical attacks," *2016 International Conference on Unmanned Aircraft Systems (ICUAS)*, pp. 811-819, 2016.

[14] S. Hayat, E. Yanmaz and R. Muzaffar, "Survey on Unmanned Aerial Vehicle Networks for Civil Applications: A Communications Viewpoint," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 4, pp. 2624-2661, Fourthquarter 2016.

[15] F. Noor, M. A. Khan, A. Al-Zahrani, I. Ullah, and K. A. Al-Dhlan, "A review on communications perspective of flying AD-HOC networks: Key enabling wireless technologies, applications, challenges and open research topics," *Drones*, vol. 4, no. 4, pp. 1–14, 2020.

[16] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet of Things*, vol. 11, p. 100218, 2020.

[17] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," *ACM Transactions on Cyber-Physical Systems*, vol. 1, no. 2, pp. 1–25, 2017.

[18] C. G. L. Krishna and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," *2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*, pp. 194-199, 2017.

[19] A. I. Hentati and L. C. Fourati, "Comprehensive survey of UAVs communication networks," *Computer Standards and Interfaces*, vol. 72, no. September 2019, p. 103451, 2020.

[20] Zhi, Z. Fu, X. Sun, and J. Yu, "Security and Privacy Issues of UAV: A Survey," *Mobile Networks and Applications*, vol. 25, no. 1, pp. 95–101, 2020.

[21] M. Yahuza et al., "Internet of Drones Security and Privacy Issues: Taxonomy and Open Challenges," in *IEEE Access*, vol. 9, pp. 57243-57270, 2021.

[22] F. Syed, S. K. Gupta, S. Hamood Alsamhi, M. Rashid, and X. Liu, "A survey on recent optimal techniques for securing unmanned aerial vehicles applications," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 7, 2021.

[23] B. Nassi, R. Bitton, R. Masuoka, A. Shabtai, and Y. Elovici, "SoK: Security and Privacy in the Age of Commercial Drones," *2021 IEEE Symposium on Security and Privacy (SP)*, no. Section IV, pp. 73–90, 2021.

[24] A. Shafique, A. Mehmood, and M. Elhadef, "Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles," *IEEE Access*, vol. 9, pp. 46927–46948, 2021.

[25] B. Li, Z. Fei, Y. Zhang and M. Guizani, "Secure UAV Communication Networks over 5G," in *IEEE Wireless Communications*, vol. 26, no. 5, pp. 114-120, October 2019.

[26] Y. Lu, "Cyber physical system (CPS)-based industry 4.0: A survey," *Journal of Industrial Integration and Management*, vol. 02, no. 03, p. 1750014, Nov. 2017.

[27] Anousheh Gholami, Usman A. Fiaz and John S. Baras, "Drone-Assisted Communications for Remote Areas and Disaster Relief," 2019. [Online] Available: https://arxiv.org/abs/1909.02150

[28] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[29] S.-H. Seo, B.-H. Lee, S.-H. Im, and G.-I. Jee, "Effect of Spoofing on Unmanned Aerial Vehicle using Counterfeited GPS Signal," *Journal of Positioning, Navigation, and Timing*, vol. 4, no. 2, pp. 57–65, 2015.

[30] H. Yang, M. Yao, Z. Xu and B. Liu, "LHCSAS: A Lightweight and Highly-Compatible Solution for ADS-B Security," *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, 2017, pp. 1-7.

[31] Samy Kamkar, "Skyjack Drone Hacking," [Online] Available: http://www.samy.pl/skyjack/

[32] Kerman, A., Borchert, O., Rose, S., and Tan, A., "Implementing a zero trust architecture," *National Institute of Standards and Technology (NIST)*, 2020.

[33] C. Pu, A. Wall, K. -K. R. Choo, I. Ahmed and S. Lim, "A Lightweight and Privacy-Preserving Mutual Authentication and Key Agreement Protocol for Internet of Drones Environment," in *IEEE Internet of Things Journal*, early access, doi: 10.1109/JIOT.2022.3163367.

[34] G. Kaddoum, "Wireless Chaos-Based Communication Systems: A Comprehensive Survey," in *IEEE Access*, vol. 4, pp. 2621-2648, 2016.

[35] M. Singh, G. S. Aujla and R. S. Bali, "A Deep Learning-Based Blockchain Mechanism for Secure Internet of Drones Environment," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4404-4413, July 2021.