2020 IEEE 23rd International Multitopic Conference (INMIC) | 978-1-7281-9893-4/20/$31.00 ©2020 IEEE | DOI: 10.1109/INMIC50486.2020.9318207

Unmaned Aerial Vehicles Threats and Defence Solutions

Ameer Hamza
Department of Information Technology
Khwaja Fareed UEIT
Rahim Yar Khan, Pakistan
hamzaameeer50@gmail.com

Urooj Akram
Department of Computer Science
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
uroojakram.cs@gmail.com

Ali Samad
Department of Computer Science
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
ali6345@hotmail.com

Saima Noreen Khosa
Department of Information Technology
Khwaja Fareed UEIT
Rahim Yar Khan, Pakistan
saima.khosa@kfueit.edu.pk

Rida Fatima
Department of Computer Science
Khwaja Fareed UEIT
Rahim Yar Khan, Pakistan
rida.fatima@kfueit.edu.pk

Muhammad Faheem Mushtaq
Department of Information Technology
Khwaja Fareed UEIT
Rahim Yar Khan, Pakistan
faheem.mushtaq@kfueit.edu.pk

***Abstract*—Unmanned aerial vehicles likely know as drones have become the most optimistic solution with a bundle of applications in the field of monitoring environment, transportation, media live streaming, and military operations. The autopilot UAV system is normally used in exigent operations to acquire critical information. The basic UAV system consists of three major components which include aerial vehicles contain some sensors and actuators, ground control stations, and communication channels. UAV systems are vulnerable to different security threats due to their deployment in serval crucial domains. There exist numerous attack techniques includes, GPS spoofing, de-authentication, denial of services, injecting false information, damaging UAV sensors, Key loggers, which can be unfavorable for our security objectives. Over the last decade, their innumerable defense mechanisms are proposed to mitigate security risks from these kinds of attacks. In this review, we will discuss major components of UAV, prime vulnerabilities for cyber-attacks, and their defense solutions.**

***Index Terms*—Unmanned Aerial Vehicle, UAV Cyber Attacks, Defense techniques, Sensors, GPS Spoofing**

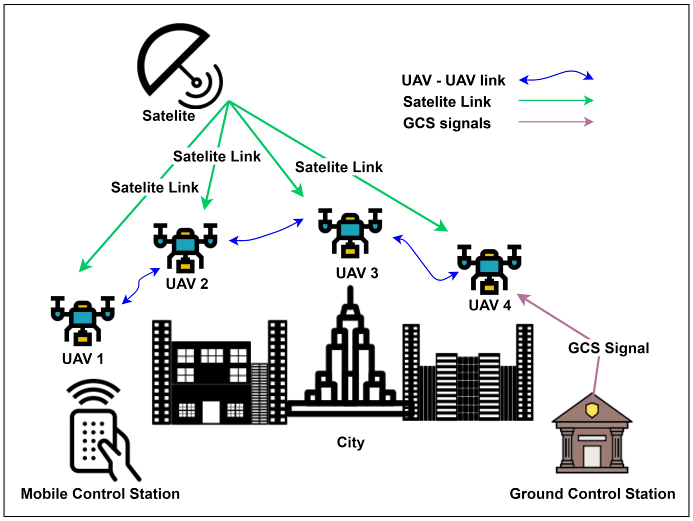

Fig. 1. Communication in UAV system

I. Introduction

Unmanned Aerial Vehicles (UAV) is the aerial vehicle with no pilots, it can control through a remote site called a control station. These vehicles can be fully autonomous or partially autonomous. In today's life due to an effective piece of work Unmanned Aerial Vehicles (UAVs) play a vital role in different civil and military aspects. Initially, UAV was only used for military proposes, mainly to overcome the loss of pilots in various military operations. However, Due to its high mobility, cost-effectiveness, compact size, and high-efficiency UAVs are widely used in civil applications as well as military applications such as traffic monitoring [1], sensing data for scientific research [2], monitoring of sensitive areas [3], Cargo transportation [4], Agriculture [5].

A basic UAV system composed in Figure 1, (UAV) system [6] it receives control signals from the Control Unit (CS), and get GPS coordinates through satellite, and captures interested data (e.g. sensing material) and send to the closest control unit and then Ground Control Station (GCS) will connect to Surveillance Center (SC) through a private channel. Data from GC will be used by SC for the analysis of interested behavior. The performance of a UAV system depends upon how effective it makes communication with other entities or nodes (e.g. other UAVs, GCS, SC) in the aerial vehicle network.

However, the extensive use of UAVs may create various security challenges related to safety, privacy and cyber security aspects. UAVs can also be used to transfer explosive materials at important sites. Recently, Saudi Arabia has faced an armed drone attack on its oil refinery site [7]. UAVs are mainly used to sense information from a specific environment and this information can be used by attackers to threaten that environment [8].

Identify applicable funding agency here. If none, delete this.

978-1-7281-9893-4/20/$31.00 ©2020 IEEE

As we know, UAV is controlled from remote sites, it gets a control signals from CS it has to make communication between its different entities (CS, other UAVs, Satellite, GS) using different communication protocols (e.g. Mav link) through a secure communication channel to make its operation successful. These protocols also have some cyber vulnerabilities [9]. The secure communication between different nodes of the UAVs network is a challenging issue in the UAV system. In [10] discusses that there are many civilians drone with no authentication methods, insecure un-encrypted communication channels, and GPS signals. These drones are more vulnerable to cyber-attacks and that can cause unsuitable condition in society that's why there should be a solution and countermeasures of these attacks. This research discusses the flow of UAV first then security objectives, goals of UAV, attacks and their counter measures.

II. Majors Components of UAV System

Unmanned aerial vehicle system majorly contains three main components include unmanned aerial vehicles, Ground Control Station (CGS), and communication link which is commonly used to perform communications between different entities of the UAV system as shown in Figure 2. The Aerial vehicles comprise different types of sensors such as gyroscope, environment sensing sensors, GPS, etc. and actuators. CGS has several computing systems with high processing power. These systems are used for process and analyzing the data obtained from Sensors of aerial vehicle's [11].

A. Aerial Vehicle

The aerial vehicle is mainly comprised of the following onboard components to communicate with external sensors [12].

B. Base System

The base system performs basic processing for the UAV system. The base system has an operating system of UAV. This component implements the main control of UAV.

C. GPS Receiver

In advance, autopilot autonomous system GPS is used for obtaining GPS signals from satellites to navigate the autonomous system. GPS receiver gets a coordinate (latitude, longitude from satellite through a secure communication link [13].

D. Communication sensor

The communication sensor is responsible for making communication in different nodes of the UAV system.

E. MEMS Gyroscope

The MEMS gyroscope is generally used for calculating angular velocity which is used for measuring the position of a drone's main propose is to find the orientation of drones relative to earth surfaces [14].

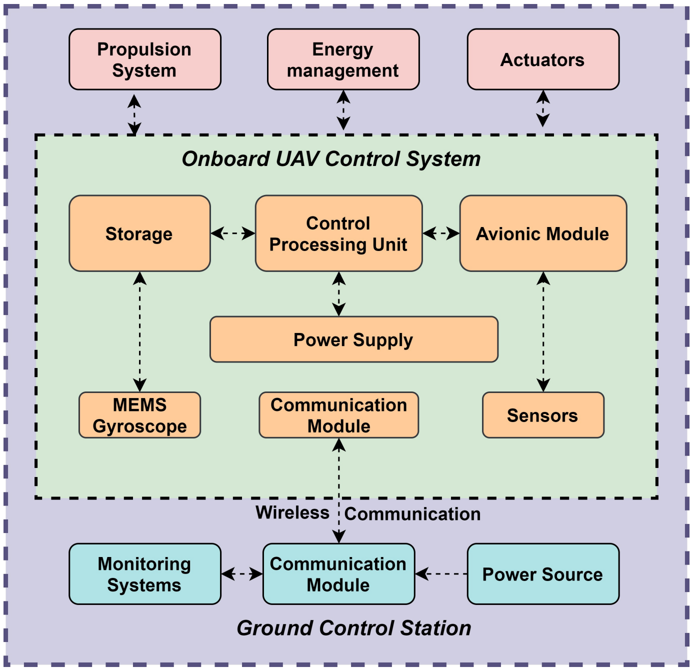

Fig. 2. UAV system Architecture

F. Power Supply

The power supply is used to give electric power to activate various sensors. Mostly civil drones have dry cell batteries for power supply.

G. Avionic Module

It converts received control command signals into system command to operate engines, spoilers, and other hardware components of UAV

H. Ground Control station

Ground control stations provide the facility to the administrator for controlling and monitoring UAV operations. GCS receives sensing data from UAVs, analyzes and processes the data. Operators perform analyzing and monitoring the process of data through high computation machines and further operation is performed based on analyzed data. As we know the sensitive records are monitored and examine at GCS so, it has highly vulnerable for cyber-attacks like key loggers, viruses and other malicious contacts.In [15] author present a threat model for analysis of major threat for smart devices in Ground control station of UAV system.

I. Communication Link

Aerial vehicles obtained remotely controlled signals through the communication link. In the UAV system, different Nodes (CS, GCS, Satellites, and other UAVs in the system) communicate with each other through the communication channel. UAV also use communication link for sending and receiving data from remotely storage devices [16]. Furthermore, the basic network architecture of wireless communications in the UAV

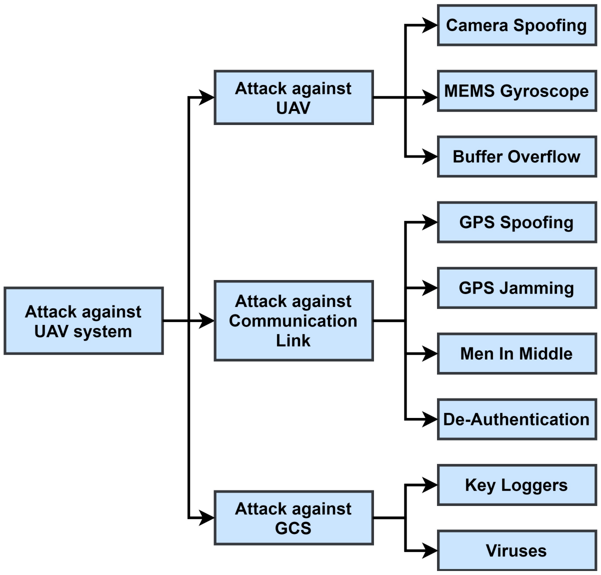

Fig. 3. Taxonomy of attacks in UAV system

system and describe how can we make our communications more effective and reliable [17].

III. Taxonomy of security Threats and Techniques for Mitigation

There are various security threats and challenges to each component of the UAV system as shown in Figure 3.

A. GPS Spoofing Attack

A GPS spoofing attack is the most common attack in a UAV System. GPS is a navigation system which gets signals from the satellite to navigate the autopilot aerial vehicles. GPS signals are broadcasted by a satellite through a communication link which is majorly used for various military and civil applications like autonomous cars and other aerial vehicles for path navigation. Those GPS signals which are used by military applications are commonly processed by some kind of encryption techniques for preventing from unauthorized access but on the other hand, the civil applications are used unencrypted GPS signals the adversary can easily get accessed to those unencrypted signals and these unencrypted signals are vulnerable for cyber-attack such as GPS spoofing [18] by using these signals adversary may create a disturbance in our system for example by altering these signals adversary can easily hijack or crash our UAV. In a GPS spoofing attack, the attacker creates a disturbance in the GPS sensor and satellite communication link and creates fake GPS signals with high intensity as compared to the original. So, the GPS sensor dropped the original GPS signals and get faked GPS coordinates and these Fake coordinates are processed by an actuator. In several studies [19], [20] shows to perform a successful GPS spoofing attack to transmit fake GPS signals to GPS receiver.

B. Defense techniques for GPS Spoofing

Serval solution exists to overcome a GPS spoofing attack and different authors proposed different techniques to mitigate the risk of this kind of cyber-attack. These techniques include detection and jamming of noisy signals, using encryption algorithms for authenticating signals, and machine learning techniques for intrusion detection these techniques are discussed in [21]–[23]. All the GPS signals are scan from the system environment, whereas the spoofing signals have high intensity from originals then they can be captured by the detection sensor and the jamming noise sensor [21]. It will take action to jam those fake signals and mitigate the intensity of fake signals. The major drawback of this technique is that if the spoofing signals and original signals have the same intensity the sensor can distinguish between fake and originals. Various GPS signals can be easily spoofed because they are unencrypted signals using suitable encryption techniques then we need to protect our system from spoofing attacks. In [22] uses the asymmetric cryptography approach was introduced to aid in the detection of GPS spoofing attacks. In civil navigation messages, there are the bits reserved and available for the periodic signature that is used to sign the remaining broadcast data. The signature and the source of the GPS signal will be verified by the receiver.This problem can be solved through machine learning techniques. [23] presented a supervised based machine learning approach for the prevention of GPS spoofing Attack. This method uses a multi-layer artificial neural network to overcome that problem. In this technique, they extract some features (doppler shift, signal to noise ratio, satellite vehicle number, pseudo-range) from original GPS signals and then they trained the ML algorithm by using these specific features for the detection of fake packets of GPS signals. In[24]the state estimation based solution suggested for a GPS spoofing attack the presented algorithm detects the spoofing attack location and also retrieves the original GPS data.in [25] the author review about various defense mechanism against GPS spoofing the method include signal processing base techniques, encryption base techniques, drift monitoring, and signal geometry-based techniques.

C. De-Authentication Attack

De-Authentication attacks target a communication link between two entities. In the UAV system, several nodes are communicating with each other commonly through wireless communication. Different nodes obtained wireless signals from wireless access points. Wireless network access points can be hacked by continuously sending de authenticating requests [17]. These requests are consumed its memory due to this memory exhausting access point cannot be accessible or available for the clients. In a de-authentication attack attacker target, a MAC address of a targeted device, and all the clients which are connected with the specified target are disconnected. De-Authentication attack is performed by sending disassociate frames to a targeted device [18]. De-Authentication packets are sent and the most efficient method to avoid this type of attack is encryption which can be breakthrough by using brute force techniques if the encryption key is not properly selected [19].

D. Defense Techniques for De-Authentication Attack

De-Authentication attack is vulnerable for the availability of a UAV system. Various methods to overcome these types of attacks [26]. One approach is using encryption. however, a Wi-Fi protracted access protocol is used for communication inefficient and secure approach. In cryptography, the effective key size is a very important factor for encryption if the size of the key will small then encryption can be break using a brute force or cryptanalysis approaches. On the other hand, a bigger key size may impact on system light weightiness and processing speed. A hierarchical structure for key distribution is proposed that provides highly effective methods for encryption [27]. Furthermore, the prevention of broadcast of Service Set Identifier (SSID) to hide access point after establishing the connections of all trusted devices [26].

E. Jamming Attack

In this attack, malicious packets are sent by the attacker for creating a disturbance in communication between the sender and receiver. This disturbance can create a denial of service situation. In the UAV system, it acquires control signal and GPS signals from remote sites to make its operations successful. UAV can be under attack by jamming out control signals or GPS signals, once control signals are jammed it will isolate from the link-state. Normally drones are designed to enable lost link protocol if they will discontent form the control station for a specific period of time. iI this result, it will follow a fail-safe autonomous procedure, it can be returned to a base station. Although jamming is a key issue because of the critical nature of the communication system of unmanned aerial vehicles. This issue can drive our operations towards failure. Recently Russia jams out American drones in Syria [28]. This study addressed various methods for jamming out UAV signals [29]. These studies show possible vulnerabilities for jamming attacks in the UAV system [30][31][32].

F. Defense Techniques for Jamming Attack

An approach for the prevention from jamming the attack is proposed using the sandbox hardware technique. In this technique, the field-programmable gate array is used for monitoring signals and isolation of the non-trusted component of the UAV system[33]. One more study [34] shows a statistical process control technique for detecting of Jamming attack, it deploys exponentially weight moving technique on packet inter-arrival feature for detection of anomalous change. This study [35] shows a reinforcement learning approach to find its path autonomously in the jamming situation of the UAV system. One more approach to mitigation of jamming shows in [36] by using antenna array, Special kind of antenna is configured in UAV which detects jamming signals and through the array beam In the direction of the jammer for stop jamming signals.

G. Man in a middle Attack

Man in the middle attack can be performed from some kilometers to take control of the UAV system. In a Man in Middle (MIM) attack the communication link is interrupted to gain control between the UAV and control center. The attacker can interrupt or inject false control signals within the network [37]. In the MIM attack, communication between the UAV and the control station will be monitored and controlled through unauthorized access in which the UAV and ground station both have unaware of that. In 2016 this type of attack was occurred in Australia [38]. Attackers exploit air traffic control frequency and communicate with the pilot and control tower and sent a false message of “GO Around” instead of land. In [39] shows a MIM attack in the UAV network. MIM attack is performed by using ”Remote AT command” which allows the user to change internal parameters such as destination high (DH) and destination low (DL) addresses and can easily route any traffic. This allows the attacker to understand existing traffic, alter a packet by meaningful information, and can inject new false information in a UAV system. In [40] proposed a model to mount a MIM attack at the Access point and its connected devices by using WPA2 encryption. Devices are disconnected from the original access point and automatically connected with fake access points due to stronger fake wireless signals. Victims connected with an attacker network and attacker can easily monitor everything in a network.

H. Defense Techniques for Man in Middle Attack

A tree approach to mitigate the risk of MIM attack first is on-board encryption for prevention from Remote AT command [39]. The second approach using encryption at the hardware level, where the hardware should not be sent data signals in clear text form, and the third approach using encryption at the application layer.

I. Key logger attack

Key loggers refer to keystroke logging, it’s a process of monitoring keystrokes. They are initially used in different organizations to monitor the unofficial activities of their employees. Key loggers can be software system or can found in hardware chips, these chips are installed inside the keyboards and send all records about keystrokes to a specific person [41] Key loggers can be used by the adversary as a spy tool for monitoring system screen and other processes. Nowadays, the major issue about key loggers is most key loggers are can’t be detected through the antiviruses system. In the UAV system, data captured from UAV sensors are sent to the ground control station, where data is monitored and analyzed through high processing computer systems. Systems which is used for monitoring and analyzing operations of UAV in a ground control station are highly vulnerable for key logger attack. The adversary can install key loggers in those Computer systems, and can easily monitor all the actives performed in UAV operations. In 2011 the incident [42] was found in Creech air force base ground. They found the installation of a key logger in the ground control station that causes leakage of privacy.

J. Defense Techniques for key Loggers Attack

Many solutions exist for the keylogging attack but two approaches are commonly used for mitigation of key logger attacks. Firstly, the on-screen virtual keyboard allows the user to input through an on-screen virtual keyboard and the other approach using effective antivirus software application which can successfully detect key loggers in a system [43]. Another approach is examining those software applications that can access sensitive information before launching it [44]. A defensive technique by mitigation at the OS level can beneficial for all applications [45]. OS can reject accessing request of untrusted applications for accessing sensitive information is constantly warned a user, whenever an application uses a sensitive information system to warn a user. User can decide whether to put information or not, the major issue is user normally ignore system warnings [46].

K. MESM gyroscope Attack

The MEMS gyroscope is generally used for calculating angular velocity which is used for measuring a position of a drone's main purpose is to find the orientation of drones relative to earth surfaces. The study [47] shows using the gyroscope poster divergence problem of UAV can be solved and also can detect real-time flight angle. Normally MEMS gyroscope has high resonance frequency but discovered some of the gyroscopes have its resonance in the band of audible frequencies [48]. Due to this vulnerability, it can be attacked by cyber-attack. [48] showed that drones can be crashed by using intentional noise. In this study, they produce noise at the resonance of the gyroscope to crash a vehicle.

L. Camera spoofing Attack

Many civilians drones are generally used for monitoring or rendering some kinds of video streams or snaps, for this purpose they have equipped with high definition cameras as sensing sensors. These cameras capture a video or pictures and send captured data to the control center through the communication channel. In a camera sensor attack, the attacker attacks the camera output by modifying a pixels value of a sensor stream [50].

M. Defense Techniques for MEMS Camera Spoofing Attack

A solution based on monitoring a change in movement in the camera is discussed in [50] that proposed a RANSAC algorithm to overcome that situation the algorithm take randomly K features and perform a hypothesis that samples then compare the each of hypothesis with each of other features. Finally, the algorithm selects a hypothesis of higher value for the frame.

N. Buffer Overflow Attack

Buffers are temporary data storage devices and are normally used for holding small data. When more data is allocated in a buffer from the system process, then extra data would be overflow and data can be leaked for other buffers which can damage or overwrite other buffer data [51]. UAV bundles of buffers are placed for holding temporary signals and these buffers can be vulnerable for cyber-attacks. In a UAV attacker, increased data in buffer memory through some malicious scripts and extra data will corrupt or hold some important command instructions (e.g. trigging commands) as a result the behavior of the UAV will be disturbed. Buffer overflow attack is performed using JSON script with up to 1000 records in its first field [52]. In the experiment, the attacker invaded system statistics from the proc/stats directory and start increasing the length of the first fiend of the JSON record from 926 to until the UAV not crashed. Normally UAV crashed at 1000 characters.

O. Defense Techniques for Buffer Overflow Attack

These types of attacks can be defeated by input filtering methods. Hooper et al. proposed an algorithm for input filtering by determining the length of input characters we can successfully mitigate this type of risk [52]. Another approach to reducing this type of risk is the machine learning approach to the intrusion detection system. Intrusion detection methods are further categorized into two main approaches [53]–[56] such as (1) Rule-based detection: based on comparing behavior with some set of pre-defined rules. we can define a set of rules according to the input capacity of the buffer (e.g. if the size of the input character exceeds the specific value then block those packets). (2) Bio-Inspired Detection technique: based on some biological systems like game theory, support vector machine (SVM), and multi-layered neural networks approach.

Conclusion and Future Research Directions:

From the last decade, the increasing of cybersecurity issues of UAV has taken the big attention of researchers. Numerous techniques are proposed to mitigate these security risks. In this review, we investigate some major attacks against each UAV component and give an overview of possible defending techniques that can be adopted for preventing these attacks but there are bundles of security challenges and risks exist which are needed to be addressed yet. As we know, for the navigation process UAV process depends on GPS signals which are coming from satellite's and these signals can be jammed or spoofed to fail UAV operation. So, we need to propose more effective techniques which are less dependent on GPS and can successfully complete their operation in jamming and spoofing situation. Another challenging issue is to develop a highly effective anomaly detection technique that has a higher true positive and true negative detection rate. Moreover, we need to develop highly secure communication protocols that ensure our secure communication in the UAV system.

References

[1] K. P. Valavanis and G. J. Vachtsevanos, "Survey of Unmanned Aerial Vehicles (UAVs) for Traffic Monitoring," Handb. Unmanned Aer. Veh., pp. 19–21, 2015.

[2] M. M. Nowak, K. Dzióbb, and P. Bogawski, "Unmanned Aerial Vehicles (UAVs) in environmental biology: A review," Eur. J. Ecol., vol. 4, no. 2, pp. 56–74, 2019.

[3] R. Ibrahim, H. Abushahma, M. A. M. Ali, N. Adilah, A. Rahman, and O. I. Al-sanjary, "Comparative Features of Unmanned Aerial Vehicle (UAV) for Border Protection of Libya: A Review," 2019 IEEE 15th Int. Colloq. Signal Process. Its Appl., no. March, pp. 114–119, 2019.

[4] E. N. Barmpounakis, E. I. Vlahogianni, and J. C. Golias, "Unmanned Aerial Aircraft Systems for transportation engineering: Current practice and future challenges," Int. J. Transp. Sci. Technol., vol. 5, no. 3, pp. 111–122, 2017.

[5] W. H. Maes and K. Steppe, "Perspectives for Remote Sensing with Unmanned Aerial Vehicles in Precision Agriculture," Trends Plant Sci., vol. 24, no. 2, pp. 152–164, 2019.

[6] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," 2012 IEEE Int. Conf. Technol. Homel. Secur. HST 2012, pp. 585–590, 2012.

[7] A. j. AJ, A. A. A. AAwsat, J. P. JP and M. E. M. Memo, "Arab-Israeli Conflict", Middle East Journal, vol. 74, no. 1, 2020.

[8] Hartmann, K. and Giles, K., UAV exploitation: A new domain for cyber power, "In 2016 8th International Conference on Cyber Conflict (CyCon)" IEEE., pp. 205-221, 2016, May"

[9] Y. Kwon, J. Yu, B. Cho, and Y. Eun, "Empirical Analysis of MAVLink Protocol Vulnerability for Attacking Unmanned Aerial Vehicles," IEEE Access, vol. 6, pp. 43203–43212, 2018.

[10] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned Aircraft Capture and Control Via GPS Spoofing," 2014.

[11] R. Altawy and A. M. Youssef, "Security, Privacy, and Safety Aspects of Civilian Drones," ACM Trans. Cyber-Physical Syst., vol. 1, no. 2, pp. 1–25, 2017.

[12] A. Kim, B. Wampler, J. Goppert, I. Hwang, and H. Aldridge, "Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles," pp. 1–30, 2012.

[13] J. Wang, "Integration of GPS / INS / Vision Sensors to Navigate Unmanned Aerial Vehicles," pp. 963–970, 2004.

[14] J. S. Jang and D. Liccardo, "Small UAV Automation Using MEMS," no. May, pp. 30–34, 2007.

[15] K. Mansfield, T. Eveleigh, D. Sc, T. H. H. D. Sc, S. Sarkani, and D. Sc, "Control Station Cyber Security Threat Model," pp. 722–728, 2013.

[16] I. Andrew, C. Tebay, and S. G. Stockton, "UNMANNED VEHICLE SELECTIVE DATA TRANSFER SYSTEMAND METHOD THEREOF," vol. 2, no. 12, 2016.

[17] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," IEEE Commun. Mag., vol. 54, no. 5, pp. 36–42, 2016.

[18] J. Su, J. He, P. Cheng, and J. Chen, "A Stealthy GPS Spoofing Strategy for Manipulating the Trajectory of an Unmanned Aerial Vehicle," IFAC-PapersOnLine, vol. 49, no. 22, pp. 291–296, 2016.

[19] K. C. Zeng, Y. Shu, S. Liu, Y. Dou, and Y. Yang, "A Practical GPS Location Spoofing Attack in Road Navigation Scenario."

[20] D. He et al., "A Friendly and Low-Cost Technique for Capturing Non-Cooperative Civilian Unmanned Aerial Vehicles," IEEE Netw., vol. 33, no. 2, pp. 146–151, 2019.

[21] D. Borio and C. Gioia, "Real-time jamming detection using the sum-of-squares paradigm," Proc. 2015 Int. Conf. Localization GNSS, ICL-GNSS 2015, 2015.

[22] A. J. Kerns, K. D. Wesson, and T. E. Humphreys, "A Blueprint for Civil GPS Navigation Message Authentication," pp. 262–269.

[23] M. R. Manesh, J. Kenney, W. C. Hu, V. K. Devabhaktuni, and N. Kaabouch, "Detection of GPS Spoofing Attacks on Unmanned Aerial Systems," 2019 16th IEEE Annu. Consum. Commun. Netw. Conf. CCNC 2019, pp. 1–6, 2019.

[24] X. Fan, L. Du, and D. Duan, "Synchrophasor data correction under GPS spoofing attack: A state estimation-based approach," IEEE Trans. Smart Grid, vol. 9, no. 5, pp. 4538–4546, 2018.

[25] M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," Proc. IEEE, vol. 104, no. 6, pp. 1258–1270, 2016.

[26] U. A. Vehicles, W. Uavs, and V. It, "C ommunication S ecurity of U nmanned A erial V ehicles," pp. 134–139, 2017.

[27] S. Haque, A New Cyber Security Framework Towards Secure Data Communication for Unmanned Aerial Vehicle (UAV). Springer International Publishing, 2018.

[28] "Russia has figured out how to jam U.S. drones in Syria, officials say." .

[29] A. Höggren, "Methods for locating signal jammers with a UAV Methods for locating signal jammers with a UAV Examensarbete utfört i Elektroteknik Andreas Höggren," 2018.

[30] C. G. L. Krishna and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," SSRR 2017 - 15th IEEE Int. Symp. Safety, Secur. Rescue Robot. Conf., pp. 194–199, 2017.

[31] S. Vadlamani, B. Eksioglu, H. Medal, and A. Nandi, "Jamming attacks on wireless networks: A taxonomic survey," Int. J. Prod. Econ., vol. 172, pp. 76–94, 2016.

[32] M. Gill, "System and method for jamming cellular signals using aerial vehicles," vol. 2, 2018.

[33] J. Mead, C. Bobda, and T. J. L. Whitaker, "Defeating drone jamming with hardware sandboxing," Proc. 2016 IEEE Asian Hardw. Oriented Secur. Trust Symp. AsianHOST 2016, 2017.

[34] O. Osanaiye, A. S. Alfa, and G. P. Hancke, "A statistical approach to detect jamming attacks in wireless sensor networks," Sensors (Switzerland), vol. 18, no. 6, 2018.

[35] R. Johansson, P. Hammar, and P. Thoren, "On simulation-based adaptive UAS behavior during jamming," 2017 Work. Res. Educ. Dev. Unmanned Aer. Syst. RED-UAS 2017, pp. 78–83, 2017.

[36] S. Ni, J. Cui, N. Cheng, and Y. Liao, "Detection and elimination method for deception jamming based on an antenna array," Int. J. Distrib. Sens. Networks, vol. 14, no. 5, 2018.

[37] C. Gudla, S. Rana, and A. H. Sung, "Defense Techniques Against Cyber Attacks on Unmanned Aerial Vehicles," no. October, 2018.

[38] Fouda, R. M., "Security vulnerabilities of cyberphysical unmanned aircraft systems", IEEE Aerospace and Electronic Systems Magazine, vol. 33, no.9, pp. 4-17.

[39] N. M. Rodday, R. D. O. Schmidt, and A. Pras, "Exploring Security Vulnerabilities of Unmanned Aerial Vehicles," no. Noms, pp. 993–994, 2016.

[40] A. Conferences and P. International, "Vulnerability Testing of Wireless Access Points Using Unmanned Aerial Vehicles," no. February, 2016.

[41] Nasaka K, Takami T, Yamamoto T, Nishigaki M.,"A keystroke logger detection using keyboard-input-related API monitoring", In 2011 14th International Conference on Network-Based Information Systems IEEE, pp. 651-656. 2011.

[42] "Virus attacks military drones, exposes vulnerabilities — ZDNet." .

[43] Z. Trabelsi and H. Saleous, "Teaching keylogging and network eavesdropping attacks: Student threat and school liability concerns," in 2018 IEEE Global Engineering Education Conference (EDUCON), 2018, pp. 437–444.

[44] A. J. Aviv, B. Sapp, M. Blaze, and J. M. Smith, "Practicality of accelerometer side channels on smartphones," p. 41, 2012.

[45] L. Simon, "PIN Skimmer: Inferring PINs Through The Camera and Microphone Categories and Subject Descriptors," pp. 67–78.

[46] L. Cai, S. Machiraju, and H. Chen, "Defending against sensor-sniffing attacks on mobile phones," in Proceedings of the 1st ACM workshop on Networking, systems, and applications for mobile handhelds - MobiHeld '09, 2009, p. 31.

[47] X. Shi, L. Lu, G. Jin, and L. Tan, "Research on the attitude of small UAV based on MEMS devices Research on the Attitude of Small UAV Based on MEMS Devices," vol. 020094, no. May, 2017.

[48] Y. Son et al., "Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors This paper is included in the Proceedings of the Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors," USENIX Secur. Symp., pp. 881–896, 2015.

[49] H. Choi et al., "Detecting Attacks Against Robotic Vehicles: A bv Control Invariant Approach," Ccs, vol. 16, no. 18, pp. 801–816, 2018.

[50] D. Davidson, H. Wu, R. Jellinek, T. Ristenpart, and V. Singh, "Controlling UAVs with Sensor Input Spoofing Attacks," 10th USENIX Work. Offensive Technol. (WOOT 16), 2016.

[51] "Buffer Overflow Attack with Example - GeeksforGeeks." .

[52] M. Hooper et al., "Securing Commercial WiFi-Based UAVs From Common Security Attacks," 2016.

[53] H. Sedjelmaci, S. M. Senouci, and M. Messous, "How to Detect Cyber-attacks in Unmanned Aerial Vehicles Network?," 2016.

[54] M. S. B, V. Lenders, and I. Martinovic, "Intrusion Detection for Airborne Communication Using PHY-Layer Information," vol. 1, pp. 67–77, 2015.

[55] S. G. Casals and T. Avionics, "CYBER-THREAT DETECTION Architecture Evolutions and Threats," pp. 1–14, 2013.

[56] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "Intrusion Detection and Ejection Framework Against Lethal Attacks in UAV-Aided Networks: A Bayesian Game-Theoretic Methodology," pp. 1–11, 2016.