CYBER-ATTACKS ON THE DATA COMMUNICATION OF DRONES MONITORING CRITICAL INFRASTRUCTURE

Hadjer Benkraouda, Ezedin Barka and Khaled Shuaib

College of Information Technology,
United Arab Emirates University, P.O. Box 15551, Al Ain, UAE

ABSTRACT

With the exponential growth in the digitalization of critical infrastructures such as nuclear plants and transmission and distribution grids, these systems have become more prone to coordinated cyber-physical attacks. One of the ways used to harden the security of these infrastructures is by utilizing UAVs for monitoring, surveillance and data collection. UAVs use data communication links to send the data collected to ground control stations (GCSs). The literature [1] suggests that there is a lack of research in the area of the cybersecurity of data communication from drones to GCSs. Therefore, this paper addresses this research gap and analyzes the vulnerabilities and attacks on the collected sensor data, mainly on: data availability, data integrity and data confidentiality, and will propose solutions for securing the drone's data communication systems.

KEYWORDS

Information security, UAV Security, Critical Infrastructure Security.

1. INTRODUCTION

Unmanned aerial vehicles (UAVs), also known as drones, have seen an increase in use in the last few years [2]. UAV functions range from entertainment for hobbyists to critical mission for the military. In recent years, UAVs have seen technical development that made them eligible to be used in many fields to help in reducing risk and cost, accomplishing dangerous and expensive missions by replacing human operators.

For example, UAVs are used as first responders after disasters like earthquakes, floods or fires for survivor location and rescue missions [3]. [4] reports that UAV aided sensing was also used to log telemetry data of the levels of toxic gases to determine gas leakages. More recently and in line with the big data movement, the data collected from UAV sensors has been used to perform analyses for predicative development and preventative maintenance [5]. Another important field that UAVs are entering is the field of surveillance and monitoring. This only became possible with the advancements in battery life (trip length), autonomous charging methods and fast communication mediums. These advanced UAVs are suitable for monitoring critical infrastructure, such as the power grid, water management systems and transportation systems. Industrial systems are all moving towards digitalizing their processes to offer the prospect of smoother operations, improved efficiency, and better economics. However, this growth in connectivity within industrial operations has opened a door to cyber threats. Cyber-attacks can

Natarajan Meghanathan et al. (Eds) : SPPR, SCAI, CSIA, WiMoA, ICCSEA, InWeS, NECO, GridCom - 2018
pp. 83–93, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.81708

damage hardware and lead to downtime both causing economic losses, and in more serious cases can lead to human fatality.

While industrial control systems, such as the ones used to control the smart grid, are becoming more connected, they are still dispersed and located in remote areas. In recent decades, vital components of critical infrastructure such as power generation plants and substations have been heavily protected with physical barriers: gates, CCTV, two-factor authentication entry access, and guards. These solutions are less effective in ensuring the physical security dispersed and remote areas, making critical infrastructure ICSs more prone to coordinated cyber-physical attacks. The low cost and technological advances in UAVs made them strong contenders to be used to augment security in these systems by monitoring and providing real-time data to operators. However, surveillance UAVs like other connected devices are themselves prone to cyber-attacks. This paper will analyze the attacks that target the data communication link in surveillance UAVs and propose solutions.

The rest of the paper is organized as follows. Section II reviews previous research and related work in the area of UAV cybersecurity. Section III gives an overview of the Unmanned aerial system (UAS) architecture. Section IV presents the types of UAV reconnaissance. Section V analyzes the security threats on data communication between UAVs and the GCS. In section VI, we propose solutions that address the identified vulnerabilities and provide insights on how to secure UAV data communications. Finally, section VII concludes this paper and suggests future work.

2. RELATED WORK

Since the area we are looking into is novel, we looked into adjacent security issues in UAVs and papers that review the communication mediums from UAVs to GCSs. Rudinskas et al performed a security analysis of UAV radio communication systems. The research paper studies the security of transferred information between the SAMONIT (Polish UAV project “Aircraft for monitoring”) and other entities. One of the key conclusions that the researchers highlight, is the importance of ciphering transferred information to ensure security [6]. [7], [8] both model the threats in UAVs, and AVs respectively and propose solutions. They both aim at giving a better understanding of the security vulnerabilities, attack types and the counter solutions that mitigate them. The aim of both papers is to help technologists make informed design and deployment decisions.

The most researched areas in UAV cybersecurity are GPS jamming and spoofing [1]. [9] demonstrates that UAVs that rely primarily on commercial GPS systems for positioning are vulnerable to jamming attacks. [10] exhibits the viability of spoofing commercial GPS due to the lack of encryption. Both these attack can lead to the crash or capture of critical UAVs by malicious users.

A lot of researchers have explored security vulnerabilities related to UAVs, [1] surveys all research that has been done in the area of UAV security and concludes that there is a scarcity of research about security threats related to UAV data communication. To this end, this paper analyzes these security threats.

3. UAS ARCHITECTURE

In this paper, the term UAS is used to refer to the system that is comprised of: an unmanned aerial vehicle (UAV), a ground control station (GCS) and communication links for the UAV-GCS interactions. UAVs have infiltrated many fields and this has made UAVs very diverse in their components each to suit its functionality. But most UAVs share some main components.

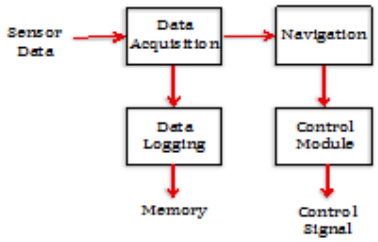

Figure 1: UAV entities

3.1.Unmanned aerial vehicles entities:

The basic UAV model can be defined as a combination of four separate, but dependent systems, figure 1 gives an overview of the interactions between UAV entities [7]:

Data acquisition: The system responsible for gathering data from the environment of the UAV. This is usually from sensors that the UAV is equipped with.

Navigation system: The system used to help in piloting the UAV. This is typically done by providing the UAV's orientation (roll, the pitch and the yaw positions). The accuracy of the navigation system is further improved by using a GPS system.

Control module: This module uses the data from the navigation system to pilot the UAV either manually through an operator or autonomously through a program.

Data logging module: This module is used for temporarily saving data before sending it to the GCS.

3.2.Ground control station entities:

Operator: This can be either a person or a program that is used to control and/or monitor UAVs during their operations.

Data storage module: This module stores data that can be used for inspection and monitoring or analysis

Data analysis module: This module is compromised of workstations that use the data received from the UAV and the data storage module for analytics.

3.3.UAV communication networks

There are two different directions of communication between UAVs and GCS (either GCS or HQ GCS) as can be seen from figure 2. The first type is control signal communication; this is usually sent from the GCS to the UAV and is used to control the UAV's motion. The other type, the category that this paper focuses on, which is data communication. This type usually refers to data sent from the UAV to the GCS. The data that is sent is mostly composed from sensor data that either aids in UAV control or telemetry data that is collected for monitoring or mission aiding purposes.

The data is communicated in phases. The sensor first collects the data. Next, it is delivered to the UAV, which either communicates it to GSC or HQ GCS. At each stage the communication

methods will vary based on the sensor's functionality, size of the data packets to be sent and the distance that the data packet has to travel. Below are the most common data communication methods.

Wired communication: This method is a physical connection and is more effective for short and immobile connections. This method is used to connect sensors to the UAV.

Wireless communication: This form of communication is commonly used to communicate data between UAVs and GCSs. Different wireless communication technologies are used. For example Bluetooth, Zigbee and WiFi are used for short ranges. WiMAX and Cellular, on the other hand, are used for longer distances and can accommodate higher data rates. Satellite communications are mostly used to communicate GPS coordinates to the UAVs and in areas where WiMAX and cellular networks are not available. Furthermore UAV manufacturers have developed proprietary transmitters and receivers used to accommodate for UAV environments such as Ocusync and Lightbridge by DJI.[11]

4. TYPES OF RECONNAISSANCE

To have a better understating of the security requirements and possible cyber-attacks the use cases of data communication links are described in this section. The UAVs that send data signals to the GCS can be categorized into three types monitoring, surveillance and data acquisition UAVs.

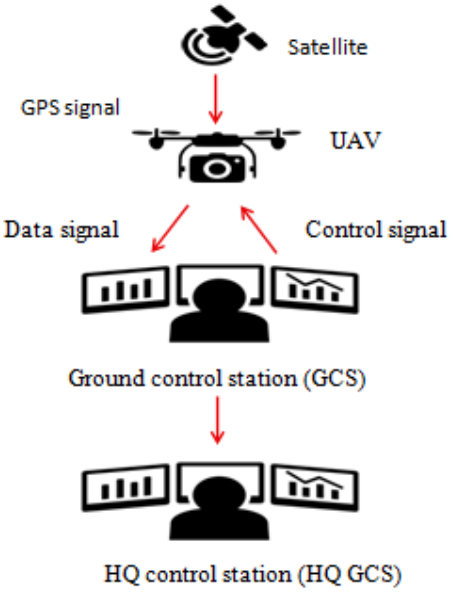

Figure 2: An overview of UAS

4.1 Monitoring

These UAVs are used to monitor the state of a target area. Monitoring UAVs are equipped with sensors; these sensors differ based on the mission of the UAV. For example, a UAV that is equipped with a temperature sensor (thermometer) can measure temperature and send it to the GCS. The operator will receive an alarm in case the readings exceed the normal range. The success of any monitoring mission depends on the correctness and availability of the sensor data. Any attacks that compromise these aspects will cause a failure of the mission.

4.2 Surveillance

Surveillance drones are used to keep a target area under observation using live stream video data that is sent to the GCS. Drones used for surveillance have become more common and they are used in many fields. For example, they are used by law enforcement agencies as part of their investigations, stakeouts and criminal pursuits. These UAVs are also used in securing critical infrastructure in remote areas like wind farms or PV plants. These critical infrastructures need continuous observation because they have become more susceptible to coordinated cyber-physical attacks [12]. In many cases surveillance data is time sensitive and needs to be sent to the operators instantaneously, this makes any attacks that result in delays can cause mission failure. Additionally, the video data is confidential and contains sensitive data, attacks that compromise the confidentiality of the video data can result in sharing the data with threat actors.

4.3 Data acquisition:

UAVs can be used for data acquisition and logging where the data is saved in the memory. In the age of big data, data is collected for many reasons such as aligning with compliance and analysis. UAVs can be particularly suitable for data collection in dangerous areas such as disaster sites, war zones or hazardous power plants. The success of any monitoring mission depends on the correctness and availability of the sensor data. Any attacks that compromise these aspects will cause a failure of the mission.

5. THREAT ANALYSIS

In this section, the vulnerabilities of UAV data communication are explored. These vulnerabilities can lead to cyber-attacks that can be classified into three categories attacks that compromise data 1) confidentiality, 2) integrity or 3) availability. Figure 3 depicts the taxonomy of the attack types in order to effectively map our proposed mitigations scheme.

5.1. Availability attacks

Attacks that compromise the availability of sensor data in UAVs can be achieved in two ways; namely through controlling the UAV or communication interruption.

In the first method of attack, the attacker compromises the UAV or the GCS. The attacker is able to gain control of the UAV and modify the functionality of its components. In the case of a camera sensor, after gaining control of the system, the attacker is able to turn-off the camera. This attack can be part of a robbery attack where the building being robbed is monitored by surveillance drones. When the attackers gain control of the UAV-GCS system they can turn off the camera during their robbery and the video becomes unavailable to the security team.

In another scenario the attacker, after taking control of the UAV, can relocate the UAV to a different geographical location. In this scenario, the data collected by a temperature sensor, for example, is not representative of the actual intended parameter. The data collected can give the operator a false sense of a safe operation environment or cause the operator to send a repair team all in vain.

In the second method of attack that compromises the availability of the system, the attackers interrupt the communication link between the UAV and the GCS. This can be done in different ways, most prominently through jamming and GPS spoofing.

Jamming aims at disrupting communication through interference or collision before reception. During a jamming attack the adversary can, for example, block or delay critical fault detection

from propagating towards the ground station. Jamming attacks can be launched without extensive knowledge or information about the attack target, this makes this attack easy to perform successfully.

DoS/DDoS are types of jamming attacks, their realization happens by flooding the network with bogus requests to make the system appear unavailable and disallow other legitimate packets from being sent. There are three ways that a DoS attack can be launched: flooding, spoofing and buffer overflow.

GPS is among the most ubiquitous technologies used for path finding in transportation. Most devices, including commercial UAVs, use civilian GPS that is unencrypted and this makes them prone to attacks.

Based on [1], *GPS spoofing* is among the most researched attacks. But in this case, GPS spoofing is used to alter the geo-location of the UAV to contaminate the data collected by sensors.

5.2.Integrity attacks:

This type of attack is achieved by either modifying the data being sent or by fabricating malicious data to replace the legitimate data. There are 2 prominent ways to compromise the integrity of the data communication of a UAV; Sensor replay attack and replacing authentic sensory data with bogus data (spoofing).

In one scenario, attackers target a camera that is used for the surveillance of critical infrastructure; the camera sends a live stream video feed to a security team that ensures that no intruders can launch a coordinated cyber-physical attack. One way around this security safeguard is by recording the monitored area aforetime and then executing a video replay attack

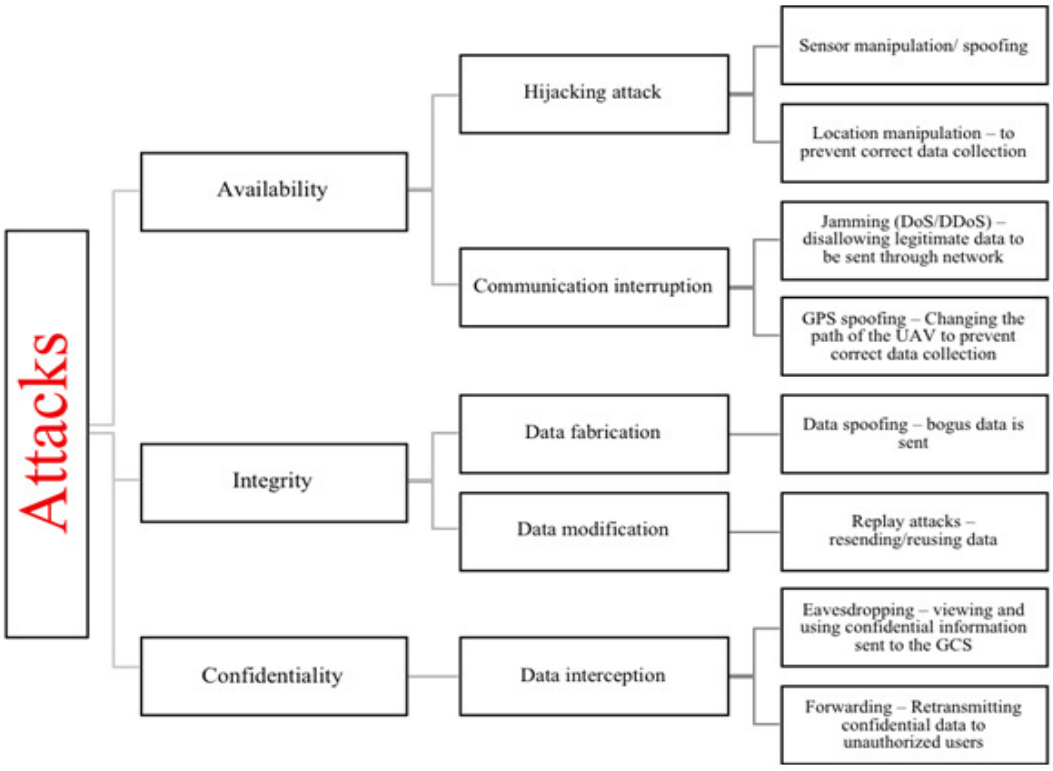

Figure 3: Taxonomy of attacks on the UAV-to-GCS communication links and data.

where the pre-recorded video is played instead. Without additional cyber-security safeguards, the security/inspecting team will not be able to detect that the video is replayed and the attackers are successful.

In another scenario, the attackers fabricate sensor data and send it to the inspector/security team. In this attack the adversary performs an active man-in-the middle attack where they intercept the information sent from the sensor, block or redirect that data and send fabricated data instead. This can cause the inspectors/security team to take misinformed decisions that may lead to expensive or harmful actions.

5.3.Confidentiality attacks:

In this attack, the adversary gets unauthorized access to confidential information by intercepting the sensor data. Attacks under this category can be either passive or active. In a passive attack, the malicious actor can eavesdrop on communication links between the UAV and GCS. In the case of a camera sensor the attacker will have live video feed of critical infrastructure. An attacker can use this as part of intelligence gathering in the reconnaissance phase of an attack targeting a critical infrastructure such as a nuclear power plant. In an active attack the adversary intercepts the signal and forwards the data to another unauthorized entity. This can be done for monetary gain; the data can be sold on the black market for example.

6. PROPOSED SOLUTIONS FOR SECURE DATA COMMUNICATION SYSTEM

This section describes safeguards that ensure data communication security. The proposed solution is depicted in figure 4. The attacks that the solution addresses are those mentioned in the previous section and they fall into three categories: availability, integrity and confidentiality.

6.1. Safeguards ensuring availability:

In real-time systems such as UAVs, the availability of data becomes of critical importance. Therefore, protecting the UAV and ensuring its resiliency against availability attacks is vital for the success of UAV missions. There are different attacks that target the availability of sensor data; likewise, there are different safeguards that help in preventing these attacks.

Hijacking attacks, either to manipulate sensors or to execute relocation attacks can be prevented by ensuring that only authorized users can modify UAV operation. A step that has to precede authorization is user authentication, to confirm that the users are valid users.

Jamming attacks, including DoS and DDoS attacks, can be prevented in several ways. One solution is by placing a firewall in the network. A firewall is a network security safeguards that filters and controls ingress and egress network traffic based on a set of rules. For example, if many packets are sent from the same address (DoS), the firewall can block incoming traffic from that source. Another way to detect that a jamming attack is happening is by setting a window and checking the rate of collision; if the rate becomes higher than normal, this would indicate that the system is under a jamming attack. The operator can then block the source of jamming attack [13]. Or adjust the transmission rate in order to contain jamming interference (Li et al. 2007).

6.2. Safeguards ensuring integrity:

UAV data communication links are being used to deliver important data that drives the decisions for missions in the army and in the industry. The integrity of data that is sent by the UAV is vital to mission success. As section V discusses, there are 2 types of attacks on data integrity: modification and fabrication attacks. Modification attacks, like replaying the same data packet or altering the contents of the data packet, can be prevented by adding a nonce/timestamp and a hash

(irreversible mathematical function/ one-way function) to each packet. The timestamp makes sure that the data packet can only be used once while the hash ensures the integrity of the message.

Another way to reinforce security is by increasing fault tolerance by introducing hardware redundancy [14]. This solution is successful in some cases, while in other cases when the size, weight, and battery constraints of UAVs are exceeded they become infeasible. Alternatively, [15] proposes that an analytical redundancy is introduced instead, that would compensate for the failures by reconfiguring the control scheme of the UAV. A hybrid of these two solutions can be used.

To prevent fabrication attacks, the sender has to be authenticated. Authentication can be achieved by using public key infrastructure, certificates and certificate authorities. Or through hard coding pre-approved MAC addresses in both the UAVs and the GCS since the numbers of UAVs and GCSs are limited.

6.3. Safeguards ensuring confidentiality:

UAV data is not of itself confidential therefore in many cases; efficiency and speed of communication are favored over confidentiality in commercial UAVs. Nowadays, commercial UAVs are part of critical missions like critical infrastructure and police surveillance. To ensure confidentiality the UAV data has to be encrypted (encoding data so that only authorized users can access it) before being sent and then authenticated and decrypted at the receiver's end. It is important to note that many encryption algorithms are computation and communication intensive and can throttle the bandwidth of a network and cause delays. It is therefore advisable for symmetric encryption to be primarily used while reserving the use of asymmetric encryption only for sensitive operations like digital signatures. In applications where live steam video is being transferred encryption can cause delays that make data to be unusable. Therefore, the encryption algorithm has to be chosen accordingly. Selective encryption is one way to reduce delays caused by encryption. This is achieved by minimizing the data that needs to be encrypted while still achieving sufficient security. This encryption algorithm works by applying encryption to a subset of the live data [16].

ACKNOWLEDGEMENTS

This research is funded by the UAEU research grant number 31T065.

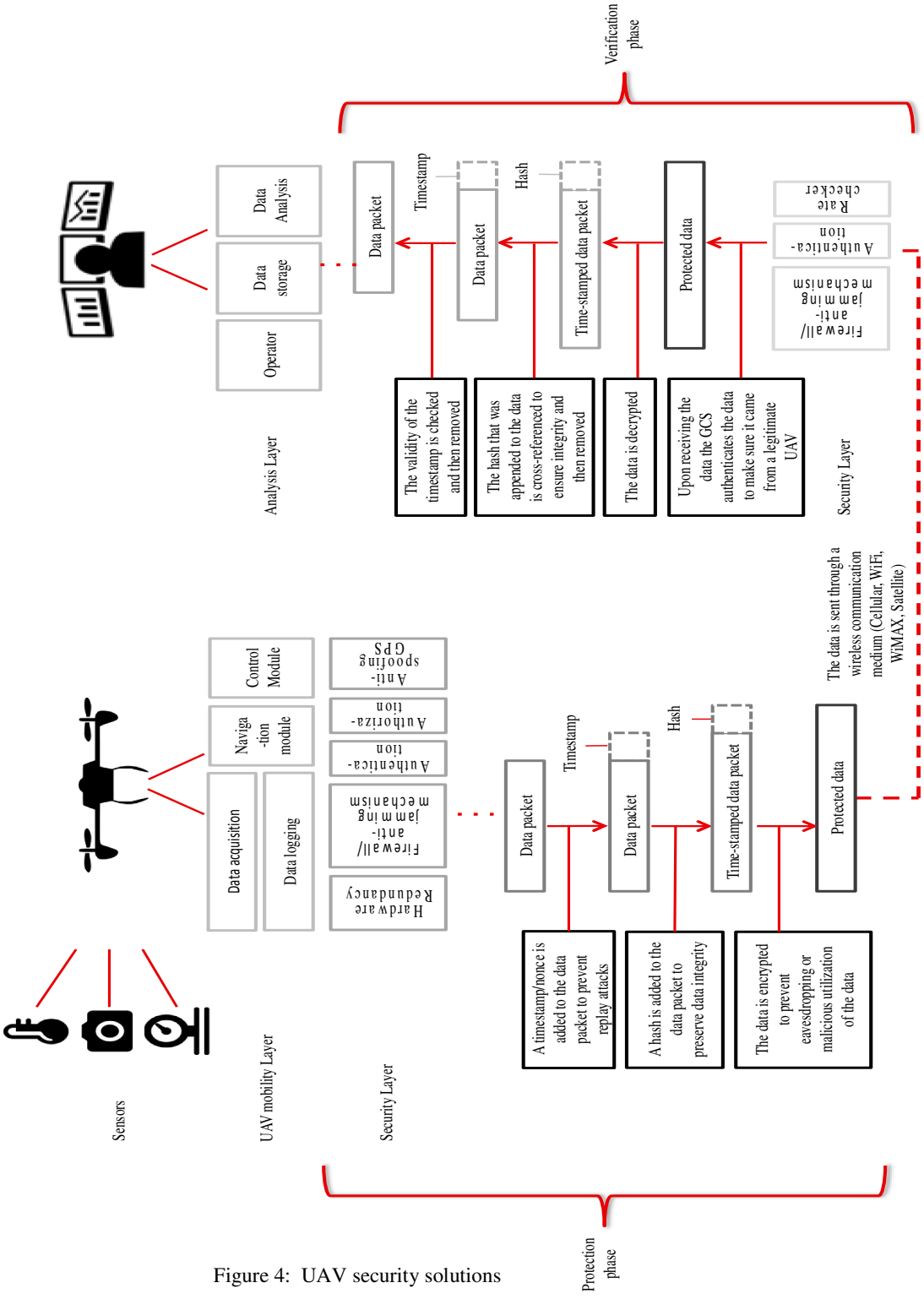

Figure 4: UAV security solutions

REFERENCES

[1] Krishna, C. G., & Murphy, R. R. (2017). A review on cybersecurity vulnerabilities for unmanned aerial vehicles. 2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR). doi:10.1109/ssrr.2017.8088163

[2] Rise of the Drones - Managing the Unique Risks Associated with Unmanned Aircraft Systems.(n.d.). Retrieved April 15, 2018, from http://www.agcs.allianz.com/insights/white-papers-andcase-studies/rise-of-the-drones/

[3] 5 Ways Drones Could Come to Your Rescue." Popular Mechanics. November 14, 2017. Accessed April 24, 2018. https://www.popularmechanics.com/military/g1437/5-ways-dronescould-come-to-your-rescue/.

[4] Gas-Drone: Portable gas sensing system on UAVs for gas leakage localization - IEEE Conference Publication. (n.d.). Retrieved April 19, 2018, from http://ieeexplore.ieee.org/document/6985282/

[5] Upstream Oil, Gas Companies Keep Exploring Benefits of UAVs. (n.d.). Retrieved April 16, 2018, from https://www.rigzone.com/news/oil_gas/a/146416/upstream_oil_gas_companies_keep_exploring_benefits_of_uavs/?all=hg2

[6] Rudinskas, D., Goraj, Z., & Stankūnas, J. (2009). Security analysis of uav radio communication system. Aviation,13(4), 116-121. doi:10.3846/1648-7788.2009.13.116-121

[7] Javaid, A. Y., Sun, W., Devabhaktuni, V. K., & Alam, M. (2012). Cyber security threat analysis and modeling of an unmanned aerial vehicle system. 2012 IEEE Conference on Technologies for Homeland Security (HST). doi:10.1109/ths.2012.6459914

[8] Thing, V. L., & Wu, J. (2016). Autonomous Vehicle Security: A Taxonomy of Attacks and Defences. 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). doi:10.1109/ithings-greencom-cpscomsmartdata. 2016.52

[9] K. Wesson and T. Humphreys, “Hacking drones,” Scientific American, vol. 309, no. 5, pp. 54–59, 2013.

[10] Y. Javaid, F. Jahan, and W. Sun, “Analysis of global positioning system-based attacks and a novel global positioning system spoofing detection/mitigation algorithm for unmanned aerial vehicle simulation,” Simulation, vol. 93, no. 5, pp. 427–441, 2017.

[11] Jawhar, I., Mohamed, N., Al-Jaroodi, J., Agrawal, D. P., & Zhang, S. (2017). Communication and networking of UAV-based systems: Classification and associated architectures. Journal of Network and Computer Applications,84, 93-108. doi:10.1016/j.jnca.2017.02.008

[12] Researchers Found They Could Hack Entire Wind Farms. (n.d.). Retrieved April 25, 2018, from https://www.wired.com/story/wind-turbine-hack/

[13] Petnga, L., & Xu, H. (2016). Security of unmanned aerial vehicles: Dynamic state estimation under cyber-physical attacks. 2016 International Conference on Unmanned Aircraft Systems (ICUAS). doi:10.1109/icuas.2016.7502663

[14] SADEGHI, M., SOLTAN, H., & KHAYYAMBASHI, M. (n.d.). The study of hardware redundancy techniques to provide a fault tolerant system. Retrieved from http://dergi.cumhuriyet.edu.tr/cumuscij/article/view/5000121174

[15] Evans, J., Inalhan, G., Jang, J. S., Teo, R., & Tomlin, C. (n.d.). DragonFly: A versatile UAV platform for the advancement of aircraft navigation and control. 20th DASC. 20th Digital Avionics Systems Conference (Cat. No.01CH37219). doi:10.1109/dasc.2001.963312

[16] Massoudi, A., Lefebvre, F., Vleeschouwer, C. D., Macq, B., & Quisquater, J. (2008). Overview on Selective Encryption of Image and Video: Challenges and Perspectives. EURASIP Journal on Information Security,2008, 1-18. doi:10.1155/2008/179290

AUTHORS

Hadjer Benkraouda. Msc

Hadjer Benkraouda received her B.Sc. in Electrical Engineering from the United Arab Emirates University (2015), and an M.Sc. in Cybersecurity from New York University (2017). She held cooperate (Bloomberg) and research positions (UAEU and NYU-AD). Her current research interests include Industrial Control Systems security and Network Security.

Ezedin Barka, PhD

Dr. Barka is currently an Associate Professor at the United Arab Emirate University. He received his Ph.D. in Information Technology from George Mason University, Fairfax, VA in 2002, where he was a member, and still associated, with the Laboratory for Information Security Technology (LIST). His current research interests include Access Control, where he published some papers addressing delegation of rights using RBAC. Other research areas include Digital Rights Management (DRM), Large-scale security architectures and models, Trust engineering, B2C e-commerce, and Network "Wired & Wireless" and distributed systems security. Dr. Barka is an IEEE member, member of the IEEE Communications Society and member of the IEEE Communications & Information Security Technical Committee (CISTC). He serves on the technical program committees of many international IEEE conferences such as ACSAC, GLOBECOM, ICC, WIMOB, and WCNC. In addition, he has been a reviewer for several international journals and conferences.

Khaled Shuaib, PhD

Khaled Shuaib Received his Ph.D. in Electrical Engineering from the Graduate Center of the City University of New York, 1999, his ME and BE in Electrical Engineering from the City College of New York, 1993 and 1991 respectively. Since September 2002, Khaled has been with the College of Information Technology (CIT), at the UAEU where he is currently a Professor and a Department Chair. His research interests are in the area of network design and performance, wireless communication networks, Blockchains, IoT, network security and Smart Grid. Khaled is a Senior member of IEEE. Prior to joining the UAEU, Khaled had several years of industrial experience in the US working as a Senior Member of Technical staff at GTE Labs, Waltham, MA (1997-1999), and as a Principle Performance Engineer for Lucent Technologies, Westford, MA (1999-2002).