Vulnerabilities Assessment for Unmanned Aerial Vehicles Communication Systems

Lamia CHAARI[1], Sana CHAHBANI[1] and Jihene REZGUI [2]
[1]Digital Research Center of Sfax (CRNS)
Laboratory of Technology and Smart Systems (LT2S), Sfax University, Tunisia
[2]Laboratoire Recherche Informatique Maisonneuve (LRIMa)
Montreal, Canada
lamiachaari1@gmail.com, jrezgui@cmaisonneuve.qc.ca

Abstract: Nowadays, Unmanned Aerial Vehicles (UAV) are being widely deployed due to new technology advancements. Therefore, UAVs used for diverse applications and for various contexts and scenarios to provide to humans advanced services and to support them in hazardous areas and difficult environments. Accordingly, UAVs and swarms' UAVs are widely deployed for smart agriculture, public safety, logistics inspection and supervision. Furthermore, UAVs used to increase the performance and to boost the coverage of existing cellular systems. However, UAVs communication systems could be attacked. In this context, this paper focus on assessing vulnerabilities and enhancing the security of the communication links between UAVs and the ground control Station (GCS). Accordingly, several mechanisms and UAV security issues were investigated. Furthermore, we have identified the MAVLINK protocol vulnerabilities by implementing different scenarios of attacks.

Keywords— Unmanned Aerial Vehicles, Ground control station, Vulnerabilities, Attacks, Security, MAVLINK.

I. INTRODUCTION

The Unmanned Aerial Vehicle (UAV) [1] is a driverless system operating autonomously according to its pre-programmed software or managed remotely from a system embedded in a Ground Control Station (GCS). UAVs are equipped with multi remote sensing devices that could be controlled and monitored in real time to execute the critical mission and to facilitate any inspections. The baseline scenario for UAVs usage is to capture from a different point of views images and video utilizing mounted cameras (optical, thermal and so forth) on UAVs. With a reliable and high-speed network especially within 5G and beyond networks, these images and videos transmitted in real time to the GCS and displayed to the supervisor in order to detect any suspect. Additionally, each UAV sends periodically to the GCS its speed, battery level, position (from GPS) and its current flight mode, etc.

UAVs can act on networks as an isolated node (single UAV system) or in cooperative mode. UAVs can be organized in swarms when there are many UAVs used in the network and the mission area is large. The swarm behavior can complete complex missions successfully and swarm UAVs must prevent themselves from collisions through communication and coordination functions. The swarm [2] mode is more interesting than the single mode. In fact, for the same task, the overall cost of a single large UAV acquisition and maintenance can be higher than the overall cost of several small UAVs. Moreover, swarm mode inherently provides fault-tolerance by the use of swarms because the impact of discarding a single drone on the overall formation is limited. Besides that, swarm mode also called flying ad hoc networks (FANETs) [3] is able to function without fixed infrastructure, therefore, is scalable and flexible. Indeed, under changing conditions (such as flight pattern or flight trajectory or UAV battery depletion) swarm architecture could be the suitable one. However, designing UAVs based secure communication system is a vital issue to solve.

UAV networks exposed to several types of attacks that can affect its software or hardware components. For that reason, security mechanisms are required to minimize or neglect the attack's effect. In this context, the main motivation of this paper is to assess the most vulnerabilities related to MAVLINK as a communication protocol between UAVs and GCS. Although there exist studies that deal with the assessment of some MAVLINK threats and attacks. However, to the best of our knowledge, this is the first study, that provides experimental illustrating the implementation of threats against the MAVLINK protocol that can disable the UAV missions. Accordingly, we proposed a security solution for the communication between UAV and GCS.

Accordingly, the rest of this paper structured as follows. Section II describes UAVs communication systems. A pinpoint of several attacks that can target UAVs System introduced in section III. Section IV highlights recent related works securing communication between UAV and GCS and communications between UAVs as well as related works securing the MAVLINK protocol. We provide the implementation details related to different scenario of attacks in Section V. The obtained results are sketched and analyzed. Finally, we conclude the paper in Section VI.

II. UAVS COMMUNICATION SYSTEMS

Currently, developers and researchers are interested in designing intelligent control systems automating UAV activities. In this context, in our previous work [4], we studied the communication system architecture for controlling hostile areas using UAVs and WSN. We identified various

978-1-7281-5628-6/20/$31.00 ©2020 IEEE

communication links and we examined various architecture model and different technologies that can be used in the communication link between the flying vehicles and the ground terminal. Diverse architectures could be considered providing communication links between UAVs and GCS.

The communication between UAVs or between UAV and GCS is established by several protocols such as MAVLINK protocol (Micro Air Vehicle LINK) [5] or STANAG 4586 [6].
- STANAG protocol: STANAG 4586 is a NATO (North Atlantic Treaty Organization) protocol that creates interfaces and allows interoperability between UAS (Unmanned Ariel System). It describes the messages exchanged between the UAV and the control station.
- MAVLINK protocol: MAVLINK is an open source, a point-to-point networking protocol used to get telemetry data from UAVs and to send control and navigation command from GCS to UAVs. This protocol was widely tested on several UAV platforms and GCS software applications, which run on Microsoft Windows, Mac, and Linux OSs. However, securing MAVLINK protocol is still a challenging issue. Our contributions focused on MAVLINK protocol drawbacks.

III. UAVS RELATED ATTACKS

UAVs are vulnerable to several attacks. These vulnerabilities can target UAV network to jam the communication, disturb the network operation, inject wrong data, etc. Many studies [7] [8] [9] have proposed different UAVs attacks classifications. In this paper, we focused on four attacks categories related to confidentiality, authenticity, integrity and availability.

A- Authenticity attacks: Authentication is a process that ensures and confirms a user's identity, without authenticity guarantee, an attacker can masquerade an UAV easily. It can be able to have unauthorized access for all the resources and may manage the entire network.
- Message forgery [10]: the attacker can create multiple virtual identities for transmitting fake messages using different forged positions in potential UAVs.
- GPS spoofing [11]: GPS used to define the position of the UAVs. It provides waypoints to fly at the indicated position. The open nature of the GPS signals enables spoofing attacks and allows the attacker to emit false GPS signals orienting the UAV to a false location.
- Identity spoofing [10]: The identity spoofing allow the attacker to masquerade as a legitimate user in the UAV network with the spoofing ID of the legitimate user and then he gets the access to all network parameters.

B- Confidentiality attacks: Confidentiality means that information should stay secret and accessible only to the authorized users. Both UAV, GCS and communication link are vulnerable to this type of attack.
- Maldrone [12]: Maldrone is a virus, which, once installed on the UAV, it enables the attacker to take control of the UAV. It acts as a proxy for the UAVs flight controller enabling the injection of the desired values for UAVs /GCS communications.
- Keylogger [12]: A keylogger is a program that has the capability to intercept and records input from the keyboard strokes made by UAV operators to manage the UAV.
- Trojans [12]: Trojan is a malicious program or software that monitors the UAV. It causes harmful effects by destroying files and damaging hard drives in the GCS system. The attacker get remote access to the UAV.
- Hacking [12]: A major threat to a UAV is hacking through which the attacker can transmit unauthorized commands to the UAV and take control of it from the GCS.
- Eavesdropping [10]: The eavesdropping is specified as unauthorized real-time interception of UAV communication allowing an attacker to detect all the commands sent from the GCS to the UAV.
- Man-In-The-Middle attack [13]: All the exchanged messages between the UAVs and the GCS transit via the attacker where the UAV and the GCS believe that they are communicating directly to each other into a private connection whereas, in reality, the entire communication controlled by the attacker.

C- Integrity attacks: The integrity means that exchanged messages delivered between UAVs and the GCS not intercepted during their transfer. Without integrity, an adversary could manipulate critical data by insertion, deletion or modification.
- Modification of existing information [14]: aims to modify the data during transmission or while in storage. The attackers send high-powered signals to change the data.
- Fabrication of new information [14]: aims to create a new fake message.

D- Availability attacks: It assures that all of the services provided by the UAV system are always available.
- Jamming [12]: In Jamming, the attacker prevents the UAV from capturing the genuine signals and retransmitting them to the receiver with added delay. This attack achieved by sending signals in the same frequency but with a higher power to jam signals.
- Denial of Service attacks (DoS): DoS results in the UAV becoming unresponsive to the GCS, and vice versa, due to the violation of the system's availability. An attacker could build a spark gap transmitter to jam the frequency used to command and control the UAV. This attack denies the communication between the GCS and the UAV since the UAV occupied by responding to the attacker commands.
- Falsifying signals: sending fake signals to prohibit the UAV to check the authenticity of the received signals and to oblige it responding to the fake signals.
-Flooding attack [17]: exhausts the network bandwidth and it consumes UAVs and GCS resources such as computational and battery power.
- Replay attack [17]: enables adversary nodes to record legitimate control messages, store and retransmit them later.
- Byzantine attack [17]: aims to create routing loops, and to forward packets via non-optimal paths, or to drop selectively packets. These actions result in the perturbation or degradation of routing services.
- Wormhole attack [14]: involves two attackers performing a colluding attack. One attacker records packets at a particular

location and replays them to another attacker in order to analyze or simply drop them to cause anomalies by using a high-speed private network.

- Blackhole attack [14]: The attacker attempts to advertise that it has a fresh route. By generating forge control packets, the adversary node may succeed in becoming part of the network route. Then, once chosen as an intermediate node, the attacker drops the packets instead of processing them.
- Rushing attack [14]: The attacker node has the ability to send discovery messages much faster and in a very offensive manner comparing with the other nodes. The main constraint in this type is that the attacker node must sent the discovery messages before the other nodes begin sending their own discovery messages so that the receiver node cannot exploit their functions correctly expect the attacker node.

IV- SECURITY MECHANISMS FOR UAVS SYSTEM

Securing UAV communications is a critical issue due to the critical UAV missions to protect the UAV network from cyber threats. However, the deployment of an exhaustive security system for UAV is a difficult task as there are various challenges and security issues to overcome. Accordingly, researchers proposed solutions to secure UAVs and their communications links: either, communication between UAV and GCS, or communication between multi-UAVs.

A- Mechanisms securing the communication between UAV and GCS

Recently, different papers proposed approaches to protect the communication between UAV and the GCS. In [18] the authors suggested a solution to establish a secure channel protocol when GCS is in the UAV communication range. Their proposal ensures confidentiality of sensed data and privacy protection of collected data by using efficient cryptographic techniques; when attackers embrace UAVs, they could not get access to the stored encrypted data. To encrypt sensed data, each key utilized only one time. In [19], K. Yoon et al proposed a secure communication integrating an authentication algorithm used where the UAV generates an encrypted random index to send it to the GCS. When the GCS receives the data, it decrypts the index using the public key. In [20] the authors proposed an approach-providing authentication and security through key negotiation including a modified cryptographic protocol that uses a combination of an Off-The-Record (OTR) and Pretty Good Privacy (PGP) algorithms to encrypt the data stored on UAV and the data transmitted through the communication link between the GCS and the UAV.

B- Security mechanisms for the communication between UAVs

Concerning swarm UAVs security, the authors of [21] proposed a secure routing protocol called SUAP (Secure UAV Ad hoc Routing Protocol) which is a security extension of the SAODV routing protocol [22]. SUAP performs against wormhole attacks. SUAP uses digital signatures for authentication and hash function for data integrity. The authors used AVISPA (Automated Validation of Internet Security Protocols) [23], which is an automated formal verification tool to check the security properties of SUAP. In [24], the authors propose a Secure and Trusted Channel Protocol (STCP) to establish a secure channel between the communicating UAVs and to provide security assurance that each UAV is in the secure and trusted state. Each communicating UAV has Trusted Platform Module (TPM) and preconfigured with the signature verification keys (public keys). STCP provides either or both of entity authentication and key exchange between communicating UAVs that preserve the confidentiality and integrity of the messages by using the Secure Channel Protocol (SCP). In [25], the authors proposed secure elements (SE) embedded on each UAVs. Indeed, these SEs build a control network layer securing exchanged messages in the network. They used Trusted Platform Module (TPM) to ensure the integrity. The authors in [26] establish a secure communications channel between UAVs by using the Advanced Encryption Standard (AES) in Galois/Counter (GCM) mode to ensure messages privacy and authenticity.

C- Security mechanisms for MAVLINK protocol

In [27], Joseph Marty tested the security level of the MAVLink protocol and assessed several failures. Accordingly, he proposed the Networking and Cryptography library (NaCl) providing methods to protect the integrity and confidentiality of an UAV based communication system [28]. The NaCl for 8-bit AVR micro-controllers utilized to secure the MAVLink protocol by implementing symmetric encryption using the Salsa20 stream cipher [29], and authentication using the Poly1305 Message Authentication Code (MAC). Moreover, LibTomCrypt is the cryptographic toolkit currently proposed by the developers of the MAVLink protocol to be used in creating the secured MAVLink protocol named sMAVLink. It uses the Advanced Encryption Standard (AES) in Galois/Counter Mode (GCM) for authenticated encryption. The algorithm takes as input a secret key, an Initialization Vector (IV), Additional Authentication Data (AAD), and the plaintext message and outputs the ciphertext with an appended authentication tag. The authentication tag, IV, AAD are sent with the encrypted message to the recipient, which will then process this data employing AES-GCM and using the same key to check the authenticity and integrity of the message and recover the plaintext message. In [30] Rabbit suggested as a high-speed stream cipher to secure MAVLINK protocol. Furthermore, a lightweight cryptographic algorithm named the Corrected Block Tiny Encryption Algorithm (XXTEA) suggested to ensure MAVLINK messages confidentiality. Authors in [31] proposed method involving the implementation of the Caesar Cipher method to encrypt data with a secured key to authenticate MAVLINK based communication. In [32], N. Prapulla et al provide encryption and authentication schemes to ensure the confidentiality and the integrity of MAVLINK communication. The authors employ ciphers that use Advanced Encryption Standard in Counter mode (AESCTR) algorithm for data encryption, SHA-256 for key Hashing and Diffie-Hellman(D-H) for key exchange. Authors in [15] have investigated the integration of MAVLINK protocol in a security architecture in order to

enhance secure messages dissemination. The proposed architectures are based on Virtual Proxy Network, providing a secure end-to-end communication between GCSs and UAVs.

V- Experimental Study for MAVLINK Vulnerabilities Assessments

This section describes the simulation tools used during the experimentation. First, we define the hardware and software devices and we detail the connection process between those components. Then, we identify the vulnerability of the MAVLINK protocol The simulation results provided and a deep analysis for each scenario performed.

A- Deployed Software's

Actually, there are many simulation tools and frameworks allowing research to test and to evaluate UAVs systems. Accordingly, in our previous paper [16] we have studied and identified the most suitable simulation tools for UAV Systems performance analysis. Accordingly, in this work we will consider Software In The Loop (SITL) paradigm. SITL provides simulators for the ArduCopter, ArduPlane, and ArduRover. The SITL simulator allows studying the behavior of the drone without any special hardware. It is a build of the drone's operation system using a C++ compiler. Because ArduPilot is a portable autopilot, it can run on a variety of platforms like Linux and Windows. Moreover, SITL provides access to development tools, such as interactive debuggers, static analyzers, and dynamic analysis tools. This makes developing and testing in ArduPilot much simpler. We have also used the QGroundControl, MAVProxy, FlightGear, PyMAVLINK, Rasbian Debian Stretch and Scapy.

- QGroundControl: is a ground control station application (GCS) developed by Lorenz Meier and written in C++ using the Qt libraries. This GCS operate on various platforms like Windows, Mac OS X, Linux, and Android. It provides configuration for both PX4 Pro and ArduPilot firmware supports the MAVLINK protocol. This type of application offers the opportunity to visualize details of the MAVLink protocol messages, exchanged between it and the UAV. Furthermore, QGroundControl proposes a graphical interface, which integrates 2D map, to facilitate the management of one or multiple UAVs and to control the location of drones.
- MAVProxy: is an open source, command-line GCS based on Python that allows a pilot to command and control any UAV that supports the MAVLINK protocol. It enables every function of QGroundControl to be executed using commands entered in a console.
- FlightGear: is an open source multi-platform flight simulator implemented by the FlightGear project. This simulator has specific builds for a diversity of operating systems such as Windows, Linux (Ubuntu, Debian,...), MAC. The FlightGear code is released under the GNU General Public License. This flight simulator was created using custom 3D graphics code with integrating an XML file that illustrates various UAVs features. In addition, FlightGear can be deployed on a local area network due to the multiplayer protocols developed for the multi-aircraft environment. This functionality can be applicated for air traffic control (ATC) or formation flight simulation.
- Pymavlink: is a python library for the MAVLINK protocol which allows creating a python script to extract and analyze data from sensors and send commands to the UAV.
- Raspbian is a free operating system (OS) based on Debian used for the Raspberry Pi hardware.
- Scapy: is a packet manipulation tool for computer network written in Python. It permits the user to forge, capture, sniff, construct, decode packets and send them across the network.

B- Communication between UAV and GCS (without Attacks)

This subsection highlights an example of exchanged MAVLINK messages between an UAV and a GCS according the baseline scenario (No attacks). Thus, we have used two PC as shown in figure 1. The first one is a DELL laptop with 4 Gigabytes (GB) of Random Access Memory (RAM) in which we have installed the QGroundControl simulator. Through this software, we command and control the different parameters of the UAV (altitude, speed, location...). The second one is a SAMSUNG laptop with 4 GB of RAM and Ubuntu 16.04 in which we have installed the Flightgear as UAV simulator that permit us to visualize the UAV in real time and in a real environment with its opportunity to display the scene in 3D.

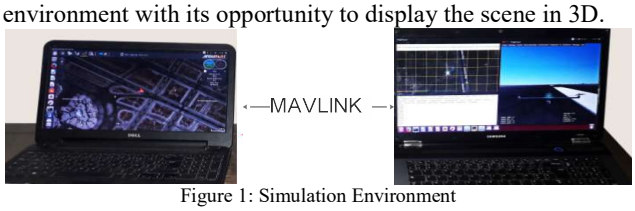


Figure 1: Simulation Environment

Moreover, we have used the Arducopter from the SITL environment and we fixed the transmission range equal to 250 m, the area of simulation is San Francisco Airport and the battery power is equal to 3800 mAh. We begin simulation by establishing a communication link between the UAV (Arducopter) and the GCS (QGroundControl) via the MAVLINK protocol. A 'takeoff' command was sent from the QGroundControl to the UAV, thus, FlightGear was connected immediately to the QGroundControl and run the received command allowing us to visualize the execution of the command graphically as shown in figure 2.

Figure 2: Exchange information between QGroundControl and FlightGear

At the same time, the exchanged messages details are saved progressively into a log file that stores all the command send from the QGroundControl and the data transmitted by the UAV as shown in figure 3.

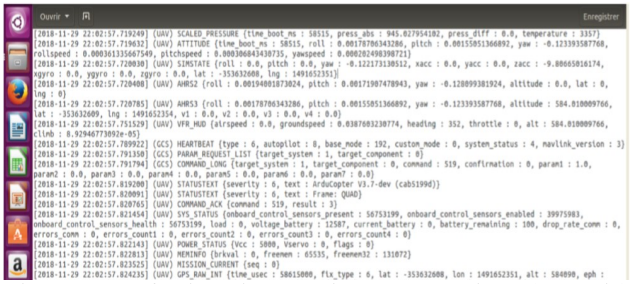


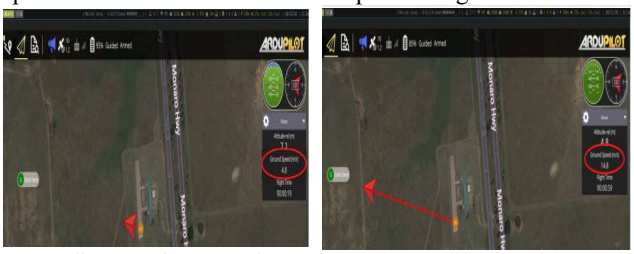
Figure 3: Trace of exchanged messages between UAV and GCS (No attacks)

C- Experimental study for Vulnerabilities assessments of the MAVLINK protocol

During this subsection, we assess the vulnerability of the MAVLINK protocol by implementing different attacks. Indeed, to perform these attacks, we used a Raspberry Pi model B with 1 GB of RAM and the Raspbian OS which plays the role of an attacker. We implemented four categories of attacks: authenticity (GPS spoofing), confidentiality (Man-In-The-Middle), Integrity (modification of existing information), and availability (DOS).

Modification of existing information:

This type of attack is based on the man in the middle mechanism to attack the communication link and extract all the needed information. When the GCS sent a command to the UAV, the attacker block that command by preventing it to arrive into the UAV. Then, the attacker modifies the UAV ground speed using the following command: MAV CMD DO CHANGE SPEED. This command has seven parameters and each one refers to a specific type of speed. For our case, during landing, the GCS sent a command containing the UAV landing speed, since we attacked the communication link, we extracted the ground speed sent from the GCS to the UAV and we changed the value to 14.8 m/s. Figure 4 shows the current speed of the UAV before and after performing the attack.



a- Landing scenario (No attack) b- Landing (modification of the speed)

Figure 4: Data Integrity attack of the MAVLINK protocol

GPS spoofing:

Concerning this attack, our main goal is to change the localization of the UAV. The GCS sent periodically a heartbeat message to the UAV in order to evaluate the communication link with the UAV. At this point, we sent also heartbeat message in an intensive way to the UAV. Through the heartbeat message, a communication link established between the attacker and the UAV. Accordingly, the attacker will be able to send any types of command. In this context, we choose to modify the position of the UAV by using MAV CMD NAV WAYPOINT. We changed the parameters values related to the longitude and latitude. The figure 5 depicts different scenario of a modified itinerary (as GPS spoofing attack).the dashed lines correspond to the hacked itinerary.

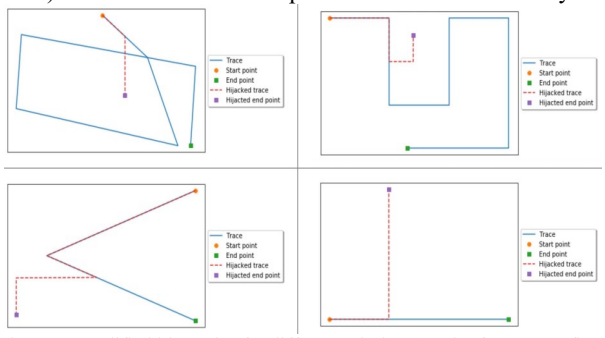


Figure 5: Modified itineraries for different mission (result of GPS spoofing)

DoS attack:

In this type of attack the attacker, send heartbeat message in order to connect to the UAV. The UAV then became unresponsive to the GCS due to the violation of the system's availability. So that, the attacker sent a command which obliges the UAV to reboot. This command is called MAV CMD PREFLIGHT REBOOT SHUTDOWN, which contains seven parameters in this case; the first parameter, which refers to restarting the UAV, was used. This attack causes the crash of the UAV as illustrated in figure 6.

Figure 6: UAV Crash (DoS attack)

Impact of attacks

We have computed the impact of the previous attacks on the power consumption and on the latency. Accordingly, Table 1 illustrates the obtained results regarding the consumed energy and the latency for the previous described attacks.

Table 1: Impact of attacks on MAVLINK protocol

Attack type	Average power consumption	Confidence Interval (Power Consumption)	Average latency	Confidence Interval (latency
No attacks (ref)	515 watt	[503, 527]	0.25 s	[0.22,0.28]
MITM	520 watt	[503, 542]	0.27 s	[0.22,0.31]
GPS spoofing	547 watt	[530, 564]	0.3 s	[0.26,0.34]
Data Modification	528 watt	[500, 556]	0.41 s	[0.36,0.47]
DoS	813 watt	[733, 893]	0.91 s	[0.73,1.1]

Based on the obtained results, we remark that the attacks decrease the network performances (latency and consumed energy). The measured power consumption during an attack on authenticity (GPS spoofing) is high because the attacker has modified the main itinerary of the UAV and ordered it to

go to a further place. This increases the consumed energy by the UAV when going to the fake localization. The measured power consumption during an attack on availability (DoS) is the highest value because the attacker system is sending a reboot command every second causing additional processing on the UAV. In general, the phase of starting the UAV is the most phase that consumes energy from the UAV's battery. So that, when we order the UAV to reboot several times consecutively, the energy consumed will increase.

VI. CONCLUSION

During this paper, we highlighted UAVs related attacks and implemented different types of attacks to assess the vulnerabilities of the MAVLINK protocol that is considered as the main communication protocol between GCS and an UAV. Accordingly, we exploited the MAVLink protocol vulnerabilities and the fact that the exchanged messages are not encrypt. We experimented various network attacks to disable an UAV. Furthermore, we evaluated the impact of the attacks on the energy consumption and the latency.

ACKNOWLEDGMENT

This work is supported by the Tunisian program, "Tunisian Federated Research Project" within the framework of the project « Supervision Sensitive de lieux Sensibles multicapteurs : Super-Sens » and by the "Fonds Québécois de la recherche sur la nature et les technologies (FRQNT)."

REFERENCES

[1] Jawhar, I., Mohamed, N., Al-Jaroodi, J., Agrawal, D. P., Zhang, S.: Communication and networking of UAV-based systems: Classification and associated architectures. JNCA Journal, 5(84), 93–108(2017).

[2] Day, M. A., Clement, M. R., Russo, J. D., Davis, D., and Chung, T. H.: Multi-UAV software systems and simulation architecture. International Conference on Unmanned Aircraft Systems (ICUAS), 2015 (pp. 426–435).

[3] Bekmezci, I., Sahingoz, O. K., and Temel,.: Flying ad-hoc networks (FANETs): A survey. Ad Hoc Networks,11(3) , 1254-1270,(2013).

[4] Krichen L., Fourati M., Fourati L.C. (2018) Communication Architecture for Unmanned Aerial Vehicle System. In: Montavont N., Papadopoulos G. (eds) Ad-hoc, Mobile, and Wireless Networks. ADHOC-NOW 2018. Lecture Notes in Computer Science, vol 11104. Springer, Cham.

[5] Sukhrob Atoev, Ki-Ryong Kwon, Suk-Hwan Lee, and Kwang-Seok Moon. Data analysis of the MAVLINK communication protocol. In Information Bibliography 40 Science and Communications Technologies (ICISCT), 2017 International Conference on, pages 1–3. IEEE, 2017.

[6] Alexandre Valerio Rodrigues, Rodolfo Santos Carapau, Mario Monteiro Marques, Victor Lobo, and Fernando Coito. Unmanned systems interoperability in military maritime operations: MAVLINK to STANAG 4586 bridge. In OCEANS 2017-Aberdeen, pages 1–5. IEEE, 2017.

[7] Daojing He, Sammy Chan, and Mohsen Guizani. Drone-assisted public safety networks: The security aspect. IEEE Com. Magazine, 55 (8):218–223.

[8] CG Leela Krishna and Robin R Murphy. A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In Safety, Security and Rescue Robotics (SSRR), 2017 IEEE International Symposium on, pages 194–199.

[9] Ahmad Y Javaid, Weiqing Sun, Vijay K Devabhaktuni, and Mansoor Alam. Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In Homeland Security (HST), 2012 IEEE Conference on Technologies for, pages 585–590. IEEE, 2012.

[10] Gaurav Choudhary, Vishal Sharma, Takshi Gupta, and Ilsun You. Internet of drones (IoD): Threats, vulnerability, and security perspectives. arXiv preprint arXiv:1808.00203, 2018.

[11] Daniel P Shepard, Jahshan A Bhatti, Todd E Humphreys, and Aaron A Fansler. Evaluation of smart grid and civilian uav vulnerability to GPS spoofing attacks. In Radio navigation Laboratory Conference, 2012.

[12] Riham Altawy and A.M Youssef. Security, privacy, and safety aspects of civilian drones: A survey. Trans. on Cyber-Physical Systems, 1 (2):7, 2017.

[13] Nils Miro Rodday, Ricardo de O Schmidt, and Aiko Pras. Exploring security vulnerabilities of unmanned aerial vehicles. In Network Operations and Management Symposium (NOMS), 2016 IEEE/IFIP, pages 993–994.

[14] ˙Ilker Bekmezci, Eren S¸enturk, and Tolgahan Turker. Security issues in flying ad-hoc networks (FANETs). Journal Of Aeronautics and Space Technologies, 9(2):13–21, 2016.

[15] Maher Aljehani and Masahiro Inoue. Communication and autonomous control of multi-uav system in disaster response tasks. In KES International Symposium on Agent and Multi-Agent Systems: Technologies and Applications, pages 123–132. Springer, 2017.

[16] A. I. Hentati, L. Krichen, M. Fourati and L. C. Fourati, "Simulation Tools, Environments and Frameworks for UAV Systems Performance Analysis," 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, 2018, pp. 1495-1500.

[17] Robin D Grodi. Design, analysis and evaluation of unmanned aerial vehicle ad hoc network for emergency response communications. 2016.

[18] Olivier Blazy, Pierre-Fran¸cois Bonnefoi, Emmanuel Conchon, Damien Sauveron, Raja Naeem Akram, Konstantinos Markantonakis, Keith Mayes, and Serge Chaumette. An efficient protocol for UAS security. In Integrated Communications, Navigation and Surveillance Conference (ICNS), 2017.

[19] Kwanwoong Yoon, Daejun Park, Yujin Yim, Kyounghee Kim, Szu Kai Yang, and Myles Robinson. Security authentication system using encrypted channel on uav network. In Robotic Computing (IRC), IEEE International Conference on, pages 393–398. IEEE, 2017.

[20] Jessica A Steinmann, Radu F Babiceanu, and Remzi Seker. Uas security: Encryption key negotiation for partitioned data. In Integrated Communications Navigation and Surveillance (ICNS), 2016.

[21] Jean-Aime Maxa, Mohamed Slim Ben Mahmoud, and Nicolas Larrieu. Extended verification of secure uaanet routing protocol. In Digital Avionics Systems Conference (DASC), 2016 IEEE/AIAA 35th, pages 1–16. IEEE.

[22] Manel Guerrero Zapata. Secure ad hoc on-demand distance vector routing. ACM SIGMOBILE Mobile Computing and Communications Review, 6(3): 106–107, 2002.

[23] Alessandro Armando, David Basin, Yohan Boichut, Yannick Chevalier, Luca Compagna, Jorge Cu´ellar, P Hankes Drielsma, Pierre-Cyrille H´eam, Olga Kouchnarenko, Jacopo Mantovani, et al. The avispa tool for the automated validation of internet security protocols and applications. In Int. conference on computer-aided verification, pages 281–285. Springer, 2005.

[24] Raja Naeem Akram, Konstantinos Markantonakis, Keith Mayes, Pierre-Fran¸cois Bonnefoi, Damien Sauveron, and Serge Chaumette. An efficient, secure and trusted channel protocol for avionics wireless networks. In Digital Avionics Systems Conference (DASC), 2016 IEEE/AIAA 35th, pages 1–10.

[25] Raja Naeem Akram, Pierre-Fran¸cois Bonnefoi, Serge Chaumette, Konstantinos Markantonakis, and Damien Sauveron. Secure autonomous uavs fleets by using new specific embedded secure elements. In Trustcom/BigDataSE/ISPA, pages 606–614, 2016.

[26] Richard B Thompson and Preetha Thulasiraman. Confidential and authenticated communications in a large fixed-wing uav swarm. In Network Computing and Applications (NCA), 2016 IEEE 15th International Symposium on, pages 375–382. IEEE, 2016.

[27] Joseph A Marty. Vulnerability analysis of the MAVLINK protocol for command and control of unmanned aircraft. Technical report, Air Force Institute of Technology Wright-Patterson, Graduate School of Engineering And Management, 2013.

[28] Michael Hutter and Peter Schwabe. Nacl on 8-bit avr µcontrollers. In Int. Conference on Cryptology in Africa, pages 156–172. Springer, 2013.

[29] Daniel J Bernstein. The salsa20 family of stream ciphers. In New stream cipher designs, pages 84–97. Springer, 2008.

[30] Martin Boesgaard, Mette Vesterager, Thomas Pedersen, Jesper Christiansen, and Ove Scavenius. Rabbit: A new high-performance stream cipher. In International Workshop on Fast Software Encryption, pages 307–329. Springer, 2003.

[31] BS Rajatha, CM Ananda, and S Nagaraj. Authentication of mav communication using caesar cipher cryptography. In Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2015 International Conference on, pages 58–63. IEEE, 2015.

[32] N Prapulla, S Veena, and G Srinivasalu. Development of algorithms for mav security. In Recent Trends in Electronics, Information & Communication Technology, IEEE International Conference on, pages 799–802. IEEE, 2016.