International Journal of Latest Research in Engineering and Technology (IJLRET)
ISSN: 2454-5031
www.ijlret.com ǁ PP. 73-79

Development of light weight algorithms in a customized communication protocol for Micro Air Vehicles

Hamsavahini R[1], Rashmi N[2],Varun N, Swaroop R S, Vuppu Satya Praneeth, Sankar Narayana R N
[1,2]*(Department of Electronics and Communication, BMS Institute of Technology and Management, India)*

ABSTRACT: In this paper, a secure communication protocol between drones and smart objects is presented. This paper suggests the improvement of security in MAV communication protocol for the communication between the GCS and the MAV. Proposed method involves the implementation of the Caesar Cipher method of data encryption with a secured key. The method of Ciphering is used for authentication of the Micro Aerial Vehicle at the beginning of the communication.
KEYWORDS: Cipher , Encryption, GCS, MAV, Protocol

I. INTRODUCTION

1.1 Unmanned Air Vehicles

UAV(Unmannned Air Vehicle), commonly known as a drone and also referred by several other names is an aircraft without a human pilot aboard. The flight of UAVs may be controlled either autonomously by on-board computers or by the remote control of a pilot on the ground or in another vehicle. UAVs are often preferred for missions that are too risky for manned aircrafts. The United States DOD in accordance with United States Federal Aviation Administration first coined the term UAS in 2005. The same term has also been accepted and used by The International Civil Aviation Organization and the British Civil Aviation Authority. Unmanned aircraft system emphasizes the importance of other elements beyond an aircraft itself. It includes elements such as the GCS(Ground Control Station), data links and other related support equipment. UAVs are commonly mistaken for missiles. In order to distinguish UAVs from missiles, a UAV is defined as a "powered, aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or nonlethal payload". Therefore, cruise missiles are not considered UAVs because, like many other guided missiles, the vehicle itself is a weapon that is not reused, though it is also unmanned and in some cases remotely guided.

1.2 Micro Air Vehicle

Micro Air Vehicle(MAV), is a class of Miniature UAVs that has a size restriction and may be autonomous. The concept of MAV has gained increasing interest over the past few years, with the principal aim of carrying out surveillance missions. MAV, in contrast, operate at significantly lower speeds and have smaller dimensions. The primary payload of these tiny aircraft is usually a miniature image sensor. Operating in certain range from the launch point, MAVs are used to acquire real-time visual information for a wide range of applications. These small crafts allows remote observation of hazardous environments inaccessible to personnel and ground vehicles. Micro Air Vehicles usually has no pilot on board. They can be remote controlled aircraft (e.g. flown by a pilot at a ground control station) or can fly autonomously based on pre-programmed flight plans or more complex dynamic automation systems. It is also sometimes referred to as DRONE (Dynamically Remotely Operated Navigation Equipment). Communication protocols are used in order to transmit messages from GCS to MAV. MAVs are not small versions of larger aircraft, but they are fully-functional, militarily capable, six-degree-of-freedom aerial robots. Their mobility provides the capability of deploying a useful micro payload to a remote or otherwise hazardous location where it may perform any of a variety of missions. Such missions may include reconnaissance and surveillance, targeting, tagging, and bio-chemical sensing. Initial missions for MAVs would include reconnaissance and surveillance, but they also could encompass targeting artillery and mortars, assessing battle damage, carrying acoustic sensors to listen for the movement of heavy equipment, and transporting detectors to sense radiation or biological and chemical weapons.

Micro aerial vehicles, in contrast, operate at significantly lower speeds and have smaller dimensions. Small enough to fit in the palm of your hand, an MAV would have an operating range of several kilometres and transmit detailed pictures back to a portable base station. Several MAVs and their base station could be carried by a single person, this is an impossible scenario with the much larger UAVs, which have wingspans of 2 to 35 m. The MAVs would be ten times smaller than the smallest UAV currently flying for defence applications. Potential capabilities for MAVs range from a fixed wing surveillance MAV that uses a data link and line-of-

sight control to an advanced MAV that hovers and navigates independently and carries multiple sensors. Because of their small size and low power, such MAVs would be quite covert. In addition, exploiting micro fabrication technology would make possible the production in large quantities of MAVs at low unit cost. The primary payload of these tiny aircraft (~15 centimetres or 6 inches wingspan) is usually a miniature image sensor. Operating in an approximate radius of 600 metres from the launch point, μAVs are used to acquire real-time visual information for a wide range of applications.

1.3 MAV requirements and configurations

The definition employed in DARPA's program limits these aircraft to a size less than 15 centimetres (6 in.) in length, width, or height. MAVs must have a weight of 50 grams or less and must be capable of staying aloft for 20 to 60 minutes for a distance of 10 kilometres. The aircraft will have to be light and small enough to fit in a soldier's backpack, yet be capable of carrying a solid-state camera, infrared sensor or radar detector on flights of several kilometres. The MAV would have to carry out most of its operations autonomously, controlled by an on-board computer that would use the sensory data collected to fly around hazards such as trees and buildings. MAVs must carry a power supply that will keep them in the air long enough to complete their mission, and MAV engines will have to be powerful enough to propel each aircraft at more than 30 kilometres per hour.

Interest groups from the military, universities, and private companies have proposed multiple designs of MAVs. These vehicles may display a wide variety of configurations depending on specific mission requirements. Design proposals differ in both outward and inward appearances. Some designs have wings and tails similar to conventional aircraft, while others take the configurations of tail-less flying wings, oval disks, insects, or other miscellaneous shapes.

2 Communication Protocols

Communication protocols are formal descriptions of digital message formats and rules. They are required to exchange messages in or between computing systems and are required in telecommunication.
Communication protocols cover authentication, error detection and correction and signalling. They can also describe the syntax, semantics and synchronization of analog and digital communication. Communication protocols are implemented in hardware and software. There are thousands of communication protocols that are used everywhere in analog and digital communication. Computer networks cannot exist without them.
Communication protocols used in MAVs are digital data link system used for transmission of short messages between aircraft and ground stations via air-band radio or satellite.

2.1 Socket Communication

A socketis a mechanism that most popular operating systems provide to give programs access to the network. It allows messages to be sent and received between applications (unrelated processes) on different networked machines. The sockets mechanism has been created to be independent of any specific type of network. IP, however, is by far the most dominant network and the most popular user of sockets.

2.2 Mavlink Protocol

Mavlink or Micro Air Vehicle Link is a protocol for communicating with small unmanned vehicle. It is designed as a header-only message marshaling library. Mavlink was first releasedearly 2009 by Lorenz Meier under LGPL license. LGPL license allows one to use this protocol as a liberty royalty-free in closed-source and open-source applications. It is used mostly for communication between a GCS and unmanned vehicles, and in the inter-communication of the subsystem— of the vehicle. It can be used to transmit the orientation of the vehicle, its GPS location and speed. [1].Mavlink is nothing but a message. It can be used with ground robots as well. Mavlink is a very lightweight, header-only message marshalling library for micro air vehicles. It can pack C-structs over serial channels with high efficiency and send these packets to the ground control station. It is extensively tested on the PX4, PIXHAWK, APM and Parrot AR.Drone platforms and serves there as communication backbone for the MCU/IMU communication as well as for Linux inter-process and ground link communication.The Mavlink message is basically a stream of bytes that has been encoded by GCS (Ground Station Control) and is sent to the APM via USB serial OR Telemetry (both cannot be used at the same time. If they are plugged in at the same time, USB is given preference and Telemetry is ignored). Encoding a message packet means is to put the packet into a data structure and send it via the channel in bytes adding some error correction alongside. The software checks whether it is a valid message (by checking the checksum and it is not corrupted, if so discards the message). That is one primary reason, why the baud rate for telemetry is set to 57,600 and not 115,200 bps. The lower it is, the less errors it is prone to, although slower it will be in updating to Ground station. If user wants to get a greater distance with Mavlink, it may be a good idea to further reduce the baud rate. However, the tested baud rate 57,600 bps would give, around a mile of radius coverage with 3DR telemetry radio.

3 System Architecture

3.1 Block Diagram

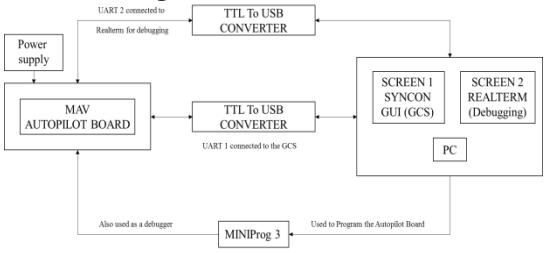

Fig1.Wired Setup

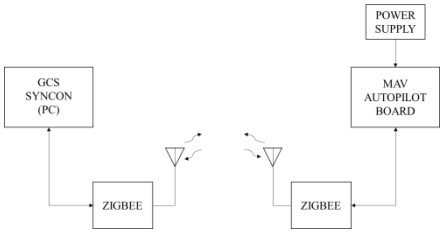

Fig 2.Wireless Setup

The Fig 1 and 2 show all the systems used for the realization of the project and their interconnections. There are two softwares running on the PC namely Syncon which is the Ground Control Station, used to send and receive data from the MAV and Realterm, which is used as a debugging software which helps us in diagnosing the setup. There are two com ports implemented for communicating with Syncon and Realterm. Since the MAV board is communicating using TTL logic and the PC has an USB port, we use TTL to USB converters to make sure the data flows freely between the two systems. The Miniprog 3 is used as a mediator between the MAV board and PC so that the MAV Autopilot board is programmed according to the firmware written by the user. An independent battery pack is connected to the MAV board for power supply.

3.2 working

3.2.1 Message formats

The format of message packet will depend on the transmitter, i.e., GCS or MAV. Message packet structure in this protocol is two-fold.

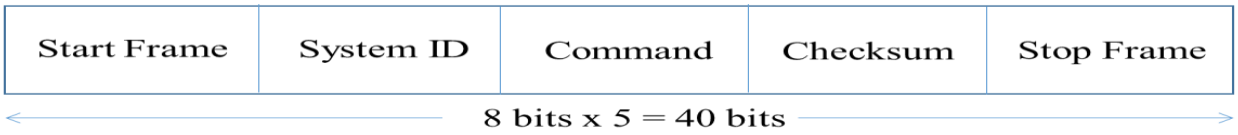

Fig3.GCS to MAV message formats

This frame structure has 5 blocks of data. Each block is of 8 bits, thus totally making 40 bit frame.

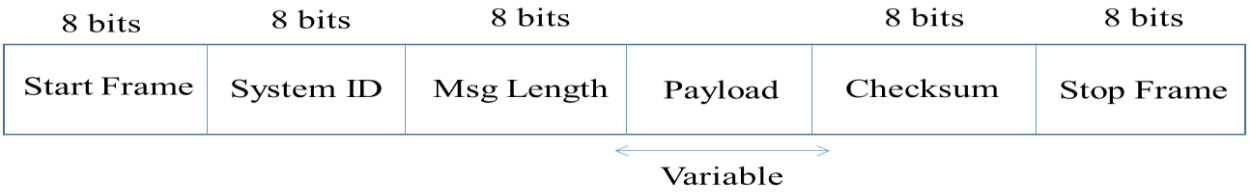

Fig.4 MAV to GCS Message formats

This frame structure has 8 bits each of start frame, system ID, message length, checksum, stop frame. It also has payload field and its size is variable depending on the data being sent by the MAV.

3.3 Custom message packet

3.3.1 Heartbeat message packet

A heartbeat is a periodic signal generated by hardware or software to indicate normal operation or to synchronize other parts of a system. Usually a heartbeat is sent between machines at a regular interval in the order of seconds. If a heartbeat isn't received for a time,usually a few heartbeat intervals—the machine that should have sent the heartbeat is assumed to have failed. A heartbeat is a signal that is generated at regular intervals to indicate that something is working correctly. A heartbeat is intended to indicate the health of a machine, it is important that the heartbeat protocol and the transport that it runs on is as reliable as possible.

3.3.2 GPS message packet

The GPS satellites broadcast radio signals containing their position and time, which the GPS receiver picks up. The receiver knows exactly where in the sky the satellite is, it just doesn't know exactly where on earth it is, until it determines the distance from the satellite. It does this by calculating the time it took for the signal to reach it. The radio waves travel at the speed of light. It calculates the time since the GPS signal is set off. With this information, it can calculate the distance. It provides three different parameters: Altitude, Longitude, and Latitude. These three parameters are then framed into a message packet before being transmitted to GCS.
These two are one of the most important message packets. Our new protocol tries to combine these two message packets into one. The new message packet so formed, not only provides information that the connection link to MAV is alive, it indicates position of the MAV. It eliminates the usage of two different packets and thereby making the system more efficient.

3.4 Module design in PSoC

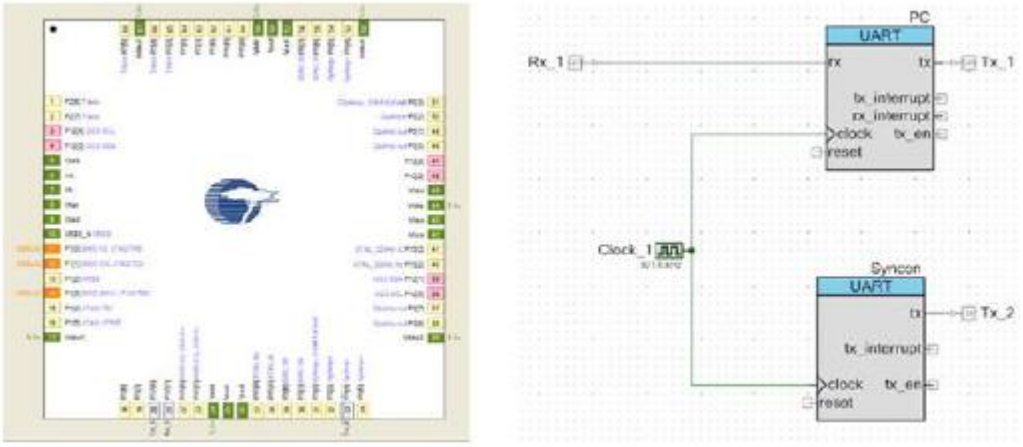

Fig.5 Design in PSoC

The Fig.5 shows the complete pin configuration details of the microcontroller. The pins coloured green are assigned for input voltages. The yellow coloured pins are free to be customized by the user. This diagram can be viewed by using the Top Design page in PSoC Creator.The chip offered by Cypress offers a couple of UART ports which can be used by the user to communicate to the external environment. Since the board is customised by the requirements of the end user, we have chosen to use only 2 UART ports. A UART port is essentially a COM port when connected to any application. When one UART is being used i.e., an application is connected to it using the COM port, no other application is granted access to use that particular COM port. Generally, when a user wishes to debug the program for error detection or step-wise debugging he uses a specialized software. To use this software it must be connected to the same UART through which, all communication takes place. Since an application is already connected, the debugging software is denied access. To overcome this difficulty, two UART ports are being used one for communication with the main application and the other port can be used for the debugging purposes.

3.5 Caesar cipher cryptography

Encryption, is the process of changing information in such a way as to make it unreadable by anyone except those processing special knowledge (usually referred to as a "key") that allows them to change the information back to its original, readable form. Encryption is important because it allows user to securely protect data that restricts unauthorized access. Through cryptography technique, the message packets or commands can be encrypted. This ensures that no secondary system gains illegal control over the GCS or MAV. It also helps to keep mission data classified. Caesar cipher cryptography technique is used for encryption of data in this protocol. There will be a common key known to both GCS and MAV. This key is used to modify the commands or vital sensor values before transmission of message packets. Modification is usually done by replacing each character with another, by moving down the number of places defined by the key from the referenced character.[5][6] Here, the command is being encrypted using this technique. The command that is being transmitted in the frame is of 8 bytes. In order to get proper values, the data along with key is mod with 256 (in cases of roll-overs) where the value goes beyond the range.

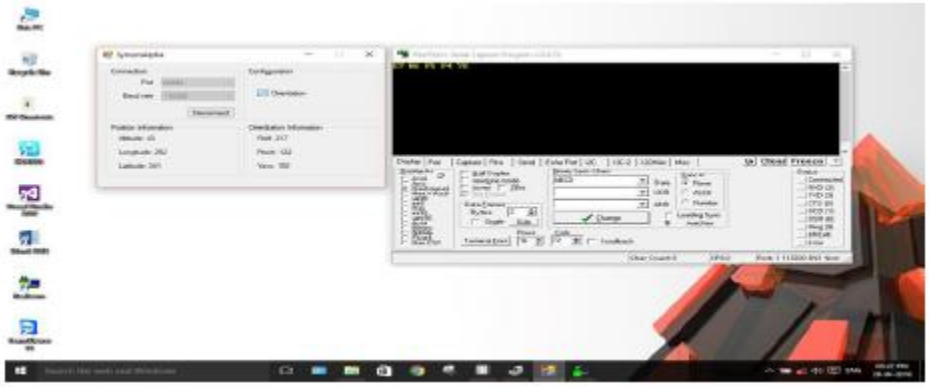

Fig.6 Caeser Cipher cryptography

3.6 Checksum

A checksum or hash sum is a small-size datum from a block of digital data for the purpose of detecting errors which may have been introduced during its transmission. A checksum algorithm will usually output a significantly different value, even for small changes made to the input. This is especially true of cryptographic hash functions, which may be used to detect many data corruption errors and verify overall data integrity. If the computed checksum for the current data input matches the stored value of a previously computed checksum, there is a very high probability the data has not been accidentally altered or corrupted.

The checksum method used in this protocol is XOR checksum model. In this type, all the bits of the data word are XORed together to form 1 bit of parity. This is later attached to the frame before transmission.

3.7 Signal flow diagram

The working flow of the protocol is as depicted below in signal flow diagram

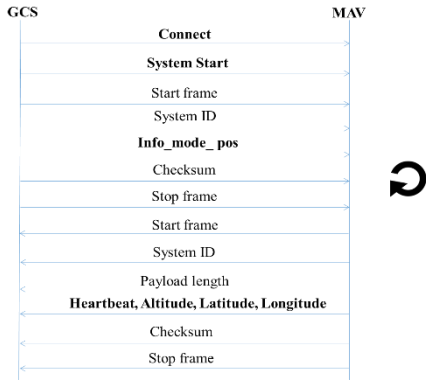

Fig.7 GCS to MAV GPS message packet

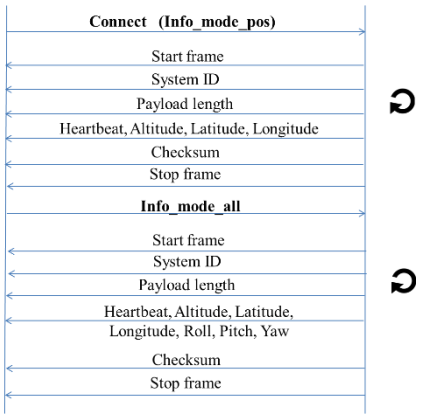

Fig.8 GCS to MAV. GPS and Orientation message packet

3.8 Graphical user interface (GUI):

To make GCS user friendly a windows form application has been created. This enables the user to interact with the application and view the received data. The application takes care of selection of baud rate for connection, COM port, and decryption of received message.

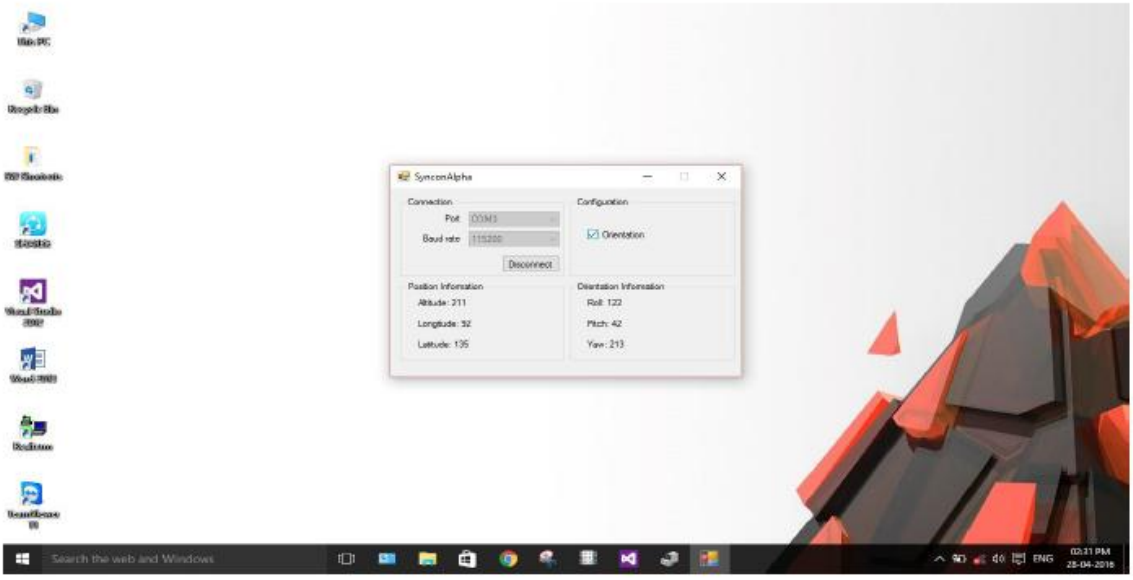

Fig.9 Graphical user Interface

As depicted in the Fig.9, there is a drop down list provided for selection of COM port and baud rate. COM port is used to select specific MAV and baud rate defines the rate at which communication of message packets takes place between MAV and GCS. Usual baud rate selected is 115200 bps. There is also GPS and orientation information. GPS information consists of altitude, longitude and latitude values. This indicates the current position of MAV. GPS information is sent along with the heartbeat signal. In order to receive orientation information, the user has to check the orientation box on top right corner. Once this is checked, it sends a message packet to MAV indicating it to transmit orientation information. The command is encrypted using Caesar cipher cryptography technique. The values shown in above figure are first decrypted by GCS before being displayed on screen. In background, there is also verification of checksum. If the checksum does not match, the message packet is dropped and hashed values are displayed.

4 RESULTS

Once appropriate COM ports and baud rates are selected, the MAV is connected to GCS by clicking "connect" button. The GCS then receives the values, deciphers it using Caesar cipher cryptography and displays it. Initially when connection link between MAV and GCS are established, the GUI starts to display only GPS values . GCS calculates the checksum for received packet. If this value matches with the received value, then the message packet is received without any loss. If there exists any mismatch, then the message packet is discarded.When the user clicks on "Disconnect", the GCS closes the COM port and further communication with the MAV is disconnected.

5 CONCLUSION

New command sets for theproposedprotocol has been developed .These command sets have beentestedfor initial functionality.Various enhancementshaveto be doneand tested in orderto release the protocol.The communication is secured using Caesar Cipher Cryptographyso that there will not be any unauthorized access.A new heartbeat has been created. This includes vital GPS co-ordinates information.Therefore, the MAV not only indicates to GCS that the communication is alive, it notifies its location periodically along with heartbeat. A GUI has been developed at GCS end to facilitate friendly user interface.The user further can modify this GUI based on his applications.The protocol is proved to be light weight compared with its compatriots.

REFERENCES

[1]. Meier, L. (2013). *MAVLink Micro Air Vehicle Communication Protocol. Retrieved Online*. accessed 13-01-2013, from http://qgroundcontrol. org/mavlink/start.

[2]. Mathias, H. David. "An autonomous drone platform for student research projects." *Journal of Computing Sciences in Colleges* 31.5 (2016): 12-20

[3]. G. Crespo, G. Glez-de-Rivera, J. Garrido and R. Ponticelli, "Setup of a communication and control systems of a quadrotor type Unmanned Aerial Vehicle," *Design of Circuits and Integrated Circuits (DCIS), 2014 Conference on*, Madrid, 2014,pp.1-6. doi: 10.1109/DCIS.2014.7035590

[4]. Marty, J. A. (2013). *Vulnerability analysis of the mavlink protocol for command and control of unmanned aircraft* (No. AFIT-ENG-14-M-50). AIR FORCE INSTITUTE OF TECHNOLOGY WRIGHT-PATTERSON AFB OH GRADUATE SCHOOL OF ENGINEERING AND MANAGEMENT.

[5]. Won, Jongho, Seung-Hyun Seo, and Elisa Bertino. "A Secure Communication Protocol for Drones and Smart Objects." *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*. ACM, 2015.

[6]. Rajatha, B. S., C. M. Ananda, and S. Nagaraj. "Authentication of MAV communication using Caesar Cipher cryptography." *Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2015 International Conference on*. IEEE, 2015.

[7]. Maxa, Jean-Aimé, Mohamed-Slim Ben Mahmoud, and Nicolas Larrieu. "Joint model-driven design and real experiment-based validation for a secure UAV ad hoc network routing protocol." *ICNS 2016, 2016 Integrated Communications Navigation and Surveillance Conference*. 2016.

[8]. J. Li, Y. Zhou and L. Lamont, "Communication architectures and protocols for networking unmanned aerial vehicles," *2013 IEEE Globecom Workshops (GC Workshops)*, Atlanta, GA, 2013, pp. 1415-1420. doi: 10.1109/GLOCOMW.2013.6825193.