Fall 2017

Authentication and Encryption of Aerial Robotics Communication

Maojie Han
San Jose State University

AUTHENTICATION AND ENCRYPTION OF AERIAL ROBOTICS COMMUNICATION

A Thesis

Presented to

The Faculty of the Department of Electrical Engineering

San José State University

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

by

Maojie Han

December 2017

The Designated Thesis Committee Approves the Thesis Titled

AUTHENTICATION AND ENCRYPTION OF
AERIAL ROBOTICS COMMUNICATION

by

Maojie Han

APPROVED FOR THE DEPARTMENT OF ELECTRICAL ENGINEERING

SAN JOSÉ STATE UNIVERSITY

December 2017

Chao-li Tarng, Ph.D.	Department of Electrical Engineering
Pedro Santacruz, Ph.D.	Department of Electrical Engineering
Nader F. Mir, Ph.D.	Department of Electrical Engineering

ABSTRACT

AUTHENTICATION AND ENCRYPTION OF AERIAL ROBOTICS COMMUNICATION

by Maojie Han

As designed to accept custom modules, autonomous aircrafts has developed into a fast-paced industry. The remote-control system of aerial robotics is typically based on wireless communications methods, such as 2.4 GHz, 5.8 GHz, or Wi-Fi. Because the services vary with the communication method, users face different kinds of cybersecurity challenges. This thesis provides an innovative solution for the authentication and security methods in proposed aerial robotics communication network. The thesis begins with an introduction to RF drone communications. After a discussion of the MAV Link communication protocol, the thesis will focus on the differences between the existing one-to-one network and the proposed one-to-many network. This thesis will then address the application of the transport layer security (TLS) layer, in connection with communication protocols, encryption, decryption, key distribution and authentication. The thesis concludes with a discussion of the future of Wi-Fi based aerial robotics networks.

ACKNOWLEDGMENTS

I greatly appreciate Professor Chao-Li Tarng’s invaluable comments and assistance in preparation of this thesis.

I also want to thank Professor Pedro Santacruz and Professor Nader Mir for their generous help in this study.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

I. INTRODUCTION

Aerial robotics has developed into a fast-paced industry. Autonomous aircrafts are designed to accept custom modules. The remote-control system of aerial robotics is typically based on different wireless communications methods. To ensure the security of these communication methods. The following eight chapters propose aerial robotics frameworks and discuss the relevant security methods. Chapter 2 provides relevant background knowledge that focuses on the current aerial robots' communication network, communication channel, authentication and cryptography used in the current drone network. Chapter 3 examines the security and structural weaknesses of the current communication network by comparing the one-to-one network with the one-to-many network.

In Chapter 4 after the selection of the one-to-many communication network structure, security issues such as threats and attacks towards the wireless communication channel are discussed. Chapter 5 explores the deployment of the proposed security methods, and a more complex network structure is given, including the communication structure, messages types, and communication schedule. Chapters 6 and 7 propose an encryption and authentication method for an aerial robotics communication network along with a key distribution system for that network. I conclude that that the key distribution in the network is very important in ensuring the security of aerial robotics networks. The thesis also concludes that the one-to-many network will soon become ubiquitous in the aerial robotics industry.

Lastly, in Chapters 8 and 9, I summarize my findings and offer my conclusions about the direction of future research in aerial robotics networks.

II. BACKGROUND KNOWLEDGE

This chapter discusses the background of communication protocols, communication methods, security methods, and Wi-Fi communication methods of aerial robotics.

A. Communication Protocols

Aerial robotics drones are more widely known as unmanned aerial vehicles (UAVs). Drones are flying robots. The aircraft can be remotely controlled or can fly autonomously through software-controlled flight commands in its embedded systems working in conjunction with the embedded air pressure sensor, compass, and GPS.

The various types of drones, such as fixed-wings, multi-motors, and helicopters, are divided into different categories for military, commercial, and consumer use. Since types and categories vary, different drones have distinct speeds and ranges in order to accomplish dissimilar tasks; therefore, they require different communication methods. Because communication distance requires flexibility, all communication methods should be wireless. Selecting the most compatible wireless communication methods and communication protocol will help aerial robotics to be more efficient.

Today, users can buy their own drones, build their own drones, and modify their own protocols without any industry standards to organize drone communications, which could lead to confusion in the air. So, Micro Air Vehicle (MAV) Link protocols were instituted in consumer and commercial drones. The MAV Link is a protocol for communicating with small, unmanned vehicles that provides a sample framework for UAV communications. First released early 2009 by Lorenz Meier under LGPL licensing [7], MAV Link typically communicates between a ground control station (GCS) and aerial robots and between the subsystems of the robots.

MAV Link is designed as a header-only message marshaling library that can be used to transmit the orientation of the robots, their GPS locations and speeds. We can use the same structure in Wi-Fi communications for aerial robotics.

MAV Link messages come in two signal types [1], heartbeat and control. The heartbeat signal periodically sends and receives, usually at the rate of one heartbeat per second. The heartbeat signal, used for the drones to provide feedback of their status to the ground control station, is a message containing several fields, including type, autopilot, mode, system status, and the specific MAV Link version. The type field indicates the shape of the aerial robotics' type, such as fixed-wing, multi-motor, helicopter. The autopilot field is the flying control algorithm; generally, this algorithm will be selected among APM, PPZ, and PIX HAWK. The mode field contains the mode of aerial robotics control, including a base mode and a sub mode (the details of modes will be explained in the following chapters). The system status field indicates whether the aircraft is on the ground or airborne (preparing, taking off, loitering, flying back, landing). Since different versions of protocols have different frames, which might lead to different checksums, the message should also announce the exact MAV Link version it uses because a drone might use a different MAV Link version from that of the ground station. The communication protocol should pair the versions to ensure the success of message transformation.

The control signal has three base modes: auto, position control, and manual. Under auto mode, software completely controls the drone. The drone takes off, finishes tasks, and lands automatically. Under position control mode, the robotics control combines manual control with the GPS signal. The controller can send a position, and the drone re-positions itself to finish the mission. Under manual mode, controllers can directly control the drone's throttle, pitch, yaw, and roll angle to fly the drone to any position the user wants. Fig. 1. is an example for the Mav link message frame.

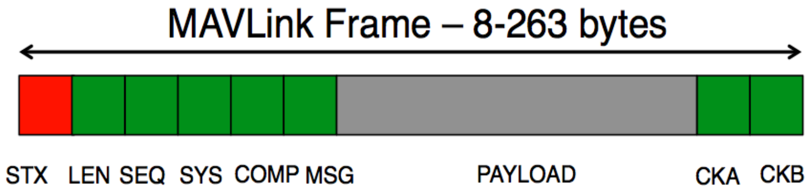


Fig. 1. Mav link message frame.

B. Communication Methods

Users employ three kinds of communication methods, satellite communications, 2.4 G Wi-Fi signal, 2.4 G radio signal. Military drones use satellite communications. From taking off until it leaves the line of sight, the ground-control station controls the drone via a direct data link. After the drone disappears from line of sight, satellites serve as the access point in the link. The drones also use GPS to relay their positions. The communication rate of this method is from 1.5 Mbps to 20 Mbps. Moreover, the delay can be more than 600 ms, and the communication distance can be more than 300 km.

Some of the consumer drones use 2.4 G Wi-Fi to transfer information. Data rate can be up to 54 Mbps, but the communication distance in this case is 300 m. Most of the consumer and commercial drones use a 2.4 G GFSK analog signal. Frequency-shift keying (FSK) is a frequency modulation scheme in which digital information is transmitted through discrete frequency changes of a carrier signal. The Gaussian frequency-shift keying (GFSK) filters the data pulses to make the transitions smoother. This filter has the advantage of reducing sideband power in order to reduce interference with neighboring channels, but at the cost of increasing inter-symbol interference. This filter improves the communication distance.

In drone communications, users employ pulse width modulation (PWM). PWM, or pulse-duration modulation (PDM), is a modulation technique used to encode a message into a pulsing signal. Although this modulation technique can be used to encode information for transmission, its main use is to control the power supplied to electrical devices, especially to inertial loads such as motors. In the drone control system, the PWM signal controls the motor and the flying control system. Different signal widths control different ports in the system. The PWM signal is modulated on the GFSK signal.

PWM frequency is between 2400 MHz and 2525 MHz. The sender signal is 20 dBm, and the receiver signal is -106 dBm. The communication distance is from 2100 m to 800 m. There is no received signal strength indication (RSSI) in the communication sequence. Data rate is from 250 bps to 2 Mbps. Real-time video streaming communication uses a 5.8 G analog signal, which can extend communication distances in clean space; however, because of its shorter wavelength, in complex environments the communication quality of the 5.8 G signal is worse than that of the 2.4 G signal.

C. Security Methods

To protect essential communication and configuration information and to prevent aerial communication systems from hacking and attack, appropriate security methods in the channel are crucial.

Security methods that used nowadays can be separated into software and hardware approaches. Spread-spectrum signals as a current hardware security function are highly resistant to deliberate jamming unless the adversary has knowledge of the spreading characteristics. Military radios use cryptographic techniques to generate the channel sequence under the control of a secret called the transmission security key (TRANSEC) that the sender and receiver share in advance.

Software security methods use authentication and encryption algorithms to protect the communication channels. There are 16 identical stages of processing, termed rounds. There is also an initial and a final permutation, termed IP and FP, respectively, which are inverses (IP "undoes" the action of FP, and vice versa). IP and FP have no cryptographic significance, but are included in order to facilitate loading blocks in and out of mid-1970s 8-bit based hardware. Before the main rounds, the block is divided into two, 32-bit halves and processed alternately; this crisscrossing is known as the Feistel scheme. The Feistel structure ensures that decryption and encryption are very similar processes. The only difference is that the sub keys are applied in the reverse order when decrypting. The rest of the algorithm is identical. This greatly simplifies implementation, particularly in hardware, as it eliminates the need for separate encryption and decryption algorithms.

Based on a design principle known as the substitution-permutation network, the AES speedily combines the substitution and the permutation in both software and hardware. Unlike its predecessor DES, the AES does not use a Feistel network. The AES is a variant of Rijndael, with its fixed block size of 128 bits and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specifies that block and key sizes may be any multiple of 32 bits (with a minimum of 128 and a maximum of 256 bits). The AES operates on a 4×4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have larger block sizes and have additional columns in the state. Most AES calculations are done in a special finite field. The algorithm is displayed below.

1) Wi-Fi Communication Methods. The current method to control consumer drones is based on the 2.4 GHz RF ground station with a RF based (MAV Link) protocol. Under this method, every drone is controlled by it respective ground station, which means one person can control only one drone at one time. In the future development of the drone industry, users might need drones to achieve many new utilities and purposes, such as drone deliveries, drone detection. In this scenario, one person controlling multi-drones becomes necessary. So, using Wi-Fi as the communication protocol is a better choice since, under a Wi-Fi network with multiple drones, each drone can have its own IP address, with which it can communicate with the same ground station at same time as the other drones.

Under the current RF wireless communication, each drone and ground station matches each other with a process called binding. During the binding process, the ground station is in listening mode, and individual drones send out a broadcast signal to announce their communication frequency and their frequency hopping table, and to synchronize their RF system with that of ground control. In this way, there is a pairing of the unique frequency hopping table between the drone and the ground station, which means every communication channel needs its own RF module. Even though this binding process achieves multiple connections, this precise and complicated system may not be efficient. Wi-Fi multi-connection can be established much more easily because every node works on the same frequency; in fact, users could work with an ad hoc network in this system.

2) Wi-Fi Based Encryption. The visual communication range of aerial robotics is between 0~2 km while the out-of-sight range is 2-6 km. The Wi-Fi based aerial robotics communications, a LAN or MAN could be established. Because every drone ground-station network can be treated as an IP subnet, multi connections can share the same network. The Wi-Fi protocol has its own encryption method; however, in this scenario, every drone has access to the same network in order to minimize potential risk by reducing the encryption/decryption calculations and by improving the frequency of key updating. For the purpose of comparison, all the encryption methods are listed below. In comparing the security methods of Wi-Fi with the security methods proposed in this thesis, the insufficiency of the Wi-Fi security methods is clear. For greater efficiency, aerial communication Wi-Fi can be set up as part of a public network that every device can access.

WEP[3]: standard 64-bit WEP uses a 40-bit key (also known as WEP-40), which is concatenated with a 24-bit initialization vector (IV) to form the RC4 key. At the time that the original WEP standard was drafted, the U.S. government export restrictions on cryptographic technology limited the key size. Once the restrictions were lifted, manufacturers of access points implemented an extended 128-bit WEP protocol using a 104-bit key size (WEP-104).

A 64-bit WEP key is usually entered as a string of 10 hexadecimal (base 16) characters (0–9 and A–F). Each character represents 4 bits, so 10 digits of 4 bits each produces 40 bits; adding the 24-bit IV produces the completes the 64-bit WEP key (4 bits × 10 + 24 bits IV = 64 bits of WEP key). Most devices also allow the user to enter the key as 5 ASCII characters (0–9, a–z, A–Z), each of which is turned into 8 bits using the character's byte value in ASCII (8 bits × 5 + 24 bits IV = 64 bits of WEP key); however, this restricts each byte to be a printable ASCII character, which is only a small fraction of possible byte value and so greatly reduces the space of possible keys.

A 128-bit WEP key is usually entered as a string of 26 hexadecimal characters. Twenty-six digits of 4 bits each produces 104 bits; adding the 24-bit IV completes the 128-bit WEP key (4 bits × 26 + 24 bits IV = 128 bits of WEP key). Most devices also allow the user to enter this key as 13 ASCII characters (8 bits × 13 + 24 bits IV = 128 bits of WEP key).

A 152-bit and a 256-bit WEP system are available from some vendors. As with the other WEP variants, 24 bits are for the IV, leaving 128 or 232 bits for actual protection. These 128 or 232 bits are typically entered as 32 or 58 hexadecimal characters (4 bits × 32 + 24 bits IV = 152 bits of WEP key, 4 bits × 58 + 24 bits IV = 256 bits of WEP key). Most devices also allow the user to enter it as 16 or 29 ASCII characters (8 bits × 16 + 24 bits IV = 152 bits of WEP key, 8 bits × 29 + 24 bits IV = 256 bits of WEP key).

TKIP [4]: TKIP uses the same underlying mechanism as WEP; consequently, it is vulnerable to a number of similar attacks. The message integrity check, per-packet key hashing, broadcast key rotation, and a sequence counter discourage many attacks. The key mixing function also eliminates the WEP key recovery attacks. Notwithstanding these changes, the weakness of some of these additions have allowed for new, although narrower, attacks.

WPA/WPA2 [5]: WPA uses a message integrity check algorithm called TKIP to verify the integrity of the packets. TKIP is much stronger than CRC, but it is not as strong as the algorithm used in WPA2. Researchers have since discovered a flaw in

WPA, its reliance on older weaknesses in WEP and the limitations of Michael to retrieve the key stream from short packets to use for re-injection and spoofing.

WPA2, which requires testing and certification by the Wi-Fi Alliance, implements the mandatory elements of IEEE 802.11i. WPA2 includes mandatory support for CCMP, an AES-based encryption mode with strong security. Certification began in September 2004; since March 13, 2006, WPA2 certification has become mandatory for all new devices that bear the Wi-Fi trademark.

III. WEAKNESSES OF CURRENT COMMUNICATION NETWORKS

The structure of an aerial robotics network can be separated into two modes, one-to-one communication and one-to-many communication. Current drone communication normally utilizes the one-to-one network frame. This chapter discusses the weaknesses of current communication networks.

A. Comparison of Network Structures

The one-to-one communication structure of the current network framework for commercial and consumer drone can be achieved by the 2.4 G radio communication signal. This kind of structure can provide a large, stable bandwidth of communications. One ground control station controls one aerial robot, and different channels are selected to avoid interference. Before the drone takes off, the authentication method of this network structure binds the drone to the ground control station. The communication channel is set on a selected frequency and flipped on the same frequency jumping table. Using this channel, messages are exchanged without encryption.

In the one-to-many communication structure, a new kind of network framework for consumer and military drones can be achieved using IP based wireless technology or other likely technologies, such as the Wi-Fi network. With this network, one ground control station can control several aerial robots at the same time, and aerial robots can communicate with other robots and several ground control stations simultaneously. According to an analysis of consumer use of this type of network, the authentication and encryption methods are based on Wi-Fi, which include the WPA2 password and AES cryptography [9].

B. Security Weaknesses of the Current Communication Structure

As new uses for aerial robotics develop, the security measures of the one-to-one network will prove inadequate. In the future, it will be impossible to ignore the issues enumerated below:

1. The current communication structure allows the owner to control only one drone at any time. In some scenarios, one project may need multiple kinds of information, so the drone is required to carry multiple sensors. A drone with even one broken sensor can sabotage the entire project since the drone flies back, resulting in wasted time and money.
2. In the current communication structure, messages are sent in plain text in the channel, which is a vulnerability for network security concern. The man-in-the-middle attack can be easily deployed in the channel (details of such attacks will be discussed later). The current drone communication structure is a concern for network security since messages are sent in plain text in the channel.
3. The current communication structure cannot provide a port for the drone's flying traffic observation and the drone's flying tracking. Moreover, the one-to-one network structure can hardly provide a port for a third party to get access to the identification, control and feedback information and save the information from the communication channel for later usage.
4. The current communication structure for consumer and commercial use aerial robotics cannot allow users to deploy an ad hoc network, which means the flying devices can be controlled only within the communication range of the ground control station's antenna.

The one-to-one network exhibits several security challenges, but the one-to-many aerial robotics network, by combining cryptography and authentication applications, can address such security problems. Enumerated below are some of the most relevant issues:

1. For projects that need to synthesize diverse kinds of information, the one-to-many network allows the ground control station to link to multiple flying devices. Different devices can carry different sensors, and ground control stations can manage the organization of different devices to meet various requirements and goals.

2. The one-to-many network can combine with an authentication and encryption method in its application layer or its TLS layer, which can help users to defend and avoid different kinds of passive and active attacks. Details will be discussed in a later chapter.

3. The one-to-many network structure can transmit all the control and feedback information in the same network; therefore, users can achieve traffic observation and flying tracking by looking through the feedback information from all aerial robots in the network.

4. The one-to-many network structure can help users to deploy an ad hoc network easily to extend the communication range of the entire network, so aerial robots in the same network can communicate with one other.

5. Lastly the one-to-many network structure can control the position of every device and transmit all the messages in the network simultaneously to ensure that some devices can fly within the communication range of other devices while other devices can fly out of communication range of ground control.

In conclusion, the one-to-many network structure and its superior security technology will have great impact on aerial robotics communication in the future.

IV. THREATS AND ATTACKS TOWARDS AERIAL ROBOTICS COMMUNICATION NETWORKS

In this paper, threat and attack describe almost the same kind of entities which influence the cyber security of an aerial robotics communication system. Typically, attacks can be divided into active attacks and passive attacks.

A. Definition

Based on RFC4949, entities that influence system security can be divided into two types: threats and attacks [6].

Threat: A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm.

Attack: An intentional act by which an entity attempts to evade security services and violate the security policy of a system. That is, an actual assault on system security that derives from an intelligent threat. Or a method or technique used in an assault.

An active attack attempts to alter system resources or affect their operation. In an aerial robotic communication system, active attacks involve modifications of the data stream or the creation of false streams and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of services.

A masquerade attack takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack. For example, the authentication sequences between drones and ground control stations can be captured and replayed after a valid authentication sequence has taken place, thus enabling malicious GCSs to be authorized. This now hostile GCS can access a specific drone, intercept communications, and send harmful commands.

Replay involves the passive capture of an authentication stream and/or a command stream and the retransmission to produce an unauthorized effect.

Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect. For example, a message meaning “Allow GCS1 to access the key database and take charge of Drone1” is modified to mean “Allow GCS null access to the key database and take charge of Drone1.”

A denial of service attack prevents or inhibits the normal use or management of communications facilities. This attack usually has a specific target. For example, an entity may suppress all messages directed to a particular drone and lead to an auto landing or fly back. Another form of service denial is the disruption of an entire control network, either by disabling the network or by overloading it with messages in order to degrade its performance.

This kind of attack always aims at the data saved in the cyber devices, such as the drone and the GCS, or the sensitive information transferred though the communication channel, such as control messages, key exchange messages and so on. So, it is easier for the system to detect them. However, because of the variety of attacks, it is may be hard for systems to prevent them. The security methods towards active attacks are authentication and system security checking.

A passive attack attempts to learn or make use of information from a system but does not affect system resources in that system.

Passive attacks are a form of monitoring, or eavesdropping upon transmissions. The goal of the opponent is to obtain any information that is being transmitted. Passive attacks come in two types: release of message contents and traffic analysis. The release of message contents is easily understood. For example, a key transfer message or a drone control message may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

The second type of passive attack, traffic analysis, is more subtle. Suppose users could encrypt the contents of key transfer messages or flying control messages so that opponents, even if they capture the messages, cannot extract any useful content from them. Even if encryption protection is in place, an opponent might still be able to observe the patterns of the encrypted messages. In addition, the opponent could determine the location and identity of communicating a GCS and aerial robots and could observe the frequency and length of messages being exchanged. This information could easily lead to conclusions about the nature of the communication, such as the type of flying control messages or the key exchange messages, which can be used to decipher messages or access the entire network. A detailed study of security methods is provided in the following chapters.

B. Network-based Communication Threats and Attacks

The nature of wireless aerial robotics communication results in several shortcomings:

1. Inadequacy of the authentication and identity detection methods.
2. Inadequacy of the cryptography on the message transformation channel.
3. Ease of access to the network.
4. Inconsistent versions of communication protocols

Knowing those shortcomings, multiple attacks could be deployed towards the communication network. Depending on the type of attacks, the security methods that could be taken to strengthen the weakness are discussed below.

1) Introduction of Incorrect Input Commands. With access to the aerial robotics communications network, it becomes possible to lead aerial devices into an incorrect action by generating fake input messages. Also, by passing themselves off as aerial devices, GCS or other information provider, aggressive third parties can access all message exchange information, such as control messages, authentication messages, status feedback messages, and key exchange messages. Certain aspects of the airborne devices could be controlled by an unauthorized third party. Various defensive mechanisms can be applied to protect the system security: system authentication, frequent position checking combined with feedback information, and encryption of key exchange messages.

2) Sender-Receiver Related Weaknesses. Because of the nature of message exchange, third parties could introduce several classic errors into the aerial robotics communication network. These errors are explained below.

3) Buffer Overflow Attack, Encoding/Decoding Errors, and Message Format Errors. These sorts of problems can be prevented by using a better detection function algorithm, and matching the different stacks between different code transfer algorithms, such as the Unicode and ANSI formats.

4) Network Deny of Service (DoS) Attack. Because wireless communication channels can be easily accessed, when the network becomes larger. the routing in the network becomes more complex. In this scenario, very long delays in communication and very long times to initiate communications will occur. When the delay is long enough, a DoS will occur.

To prevent and defend from this kind of attack, a different message transformation protocol should be taken in the network for different kinds of messages; for example, one could use TCP for control and key exchanging messages and use UDP for status feedback messages. At the same time, because the position of flying devices changes from time to time, a smarter routing algorithm could reduce the path loss and shadowing effect of the signal power, and this beneficial method of self-protection should be taken in case of scenarios like auto fly back or auto landing. When attacked, drones could use beneficial methods of self-protection like auto fly back or auto landing.

5) Generation of Incorrect Output Values or Commands. In a manner similar to incorrect inputs, fake output values can be sent to network-connected flying devices and other controllers. All the devices in the same network are influenced and an aggressive, third-party GCS is recognized as the authorized controller. Various defensive mechanisms can be applied to protect against erroneous outputs, including authentication, protection of the key exchanges, and frequently key updates in the network.

6) Insertion of Messages to Indicate Incorrect Feedback Status of Parts of the System. Malicious messages can be sent to lead the GCS into an abnormal auto control reflection by generating fake status feedback messages. Such tactics can be used to spoof the GCS, pretend that the flying devices in a specific status and lead to erroneous commands from the GCS. This technique is called feedback spoofing.

Aerial robots have self-control features, accomplished by the self-control algorithm together with the GPS signal. Attackers can spoof the GPS signal or capture and resend the GPS signal to the drone. A wrong GPS signal will lead to incorrect commands and cause the drone to fly out of visual range from the GCS. For example [11], on December 4, 2011, Iranian forces near the city of Kashmir captured an

American Lockheed Martin RQ-170 Sentinel UAV (Unmanned aerial vehicle). The Iranian government announced that the UAV was brought down by its cyber warfare unit, which had taken control of the aircraft and safely landed it. According to an Iranian engineer's assertion in a Christian Science Monitor article, the drone was first captured by jamming both satellite and land-originated control signals to the UAV and then subjected to a GPS spoofing attack that fed the UAV false GPS data to make it land in Iran rather that at its home base in Afghanistan. Analysis of the robotics' ability to move and the drone's voting algorithm and the signature in feedback messages can prevent such feedback spoofing.

7) Collection of Essential Information. Generally, accessing drone communication streams makes it possible to determine essential operating messages and system states that can cause harm by an adversary in more complex cyber-attacks. For example, third parties can determine the message types by simple traffic analysis of the messages length, then replay attack could be deployed in the channel. For example, by determining the message types by simple traffic analysis of the messages' length, third parties can then determine the types of messages intercepted. To prevent harm from this weakness, key distribution in the network is crucial.

8) Interruption or Corruption of Communications among Control System Components. Rather than directly leading to error process signals for controllers or robotics to act on, third parties can interfere with communications and disrupt the stability of communication in the channel. Depending on the network type and configuration, the following failure types may be created.

9) Incorrect Signal Sequence, Unusual Delay, Masquerade, Excessive Jitter, Broadcast Storm (Denial-of-Service of Service), Unintended Repetition, Inconsistency

(More-or-Less Judgment), Loss, Insertion, Addressing, and Collision. In the above scenarios, a clear and precise network and communication protocol is needed for defense. The following chapters will introduce a proposed communication structure. Then several encryption and authentication algorithms will be discussed for all messaging. The subsequent chapter discusses a proposed key exchange solution.

V. AERIAL ROBOTICS COMMUNICATION FRAMEWORK

To meet the requirements of the security issues in increasingly complex networks, the existing aerial robotics communication protocol, such as the MAV Link, is clearly insufficient to meet the growing needs of this industry. In this chapter, a new communication structure based on the current framework is proposed. In this chapter, the types of communication messages, the framework of drone communications, and the structure of all four kinds of messages will be discussed.

A. Aerial Robotics Communication Structure

Since communication methods for aerial robotics vary, in this thesis Wi-Fi communication is selected as an example. Wi-Fi based 2.4 G or 5.8 G communication could be deployed easily, and the whole communication network could thus be IP based. Packets could be sent under either a TCP or UDP protocol, depending on the type of message. If the communication network is deployed using other communication methods, such as MAV Link, every device will have its own unique ID number in the network similar to an IP address in Wi-Fi. Users can establish transportation layer protocols in their own communication system similar to TCP or UDP.

Four kinds of network structures (modes) can be established to accomplish Wi-Fi-based aerial robotics communication: point-to-point mode, ad hoc mode, AP mode, and ground-control center mode.

1) Point-to-point Mode. Point-to-point communication can be established between ground control stations (GCSs) and aerial robotics. Details are shown in Fig. 2. Users can have their own Wi-Fi router and a GCS, and an aerial robot can be connected using the same router for TCP/IP communications. In this point-to-point mode, users establish their private networks, and each UAV has its own, unique IP address. Users can have a base station network to control multi UAVs simultaneously. In this mode, the GCS-UAV system is considered a mobile system, which can be established ubiquitously. Because of the limitation of the power supply, the communication range of this system is less than 500 m. In this network, communication has the lowest packet delay, but if different systems work near one other and share the same channel, interference will become a problem.

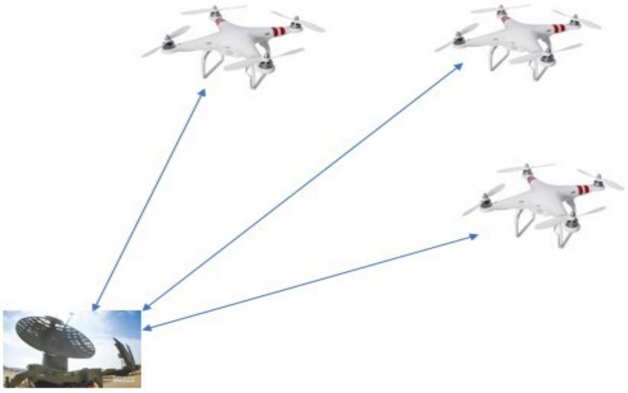


Fig. 2. Point-to-point mode communication structure. (Photograph is public access)

2) Ad hoc Mode. An ad hoc communication can be established between GCS and aerial robotics. Users can have their own Wi-Fi router, and each UAV can act as an access point in the air. Details are shown in Fig. 3. UAVs can communicate with one other or with the GCS. In the ad hoc mode, users have their own private networks, and each UAV has a unique IP address. Users can use an ad hoc network to control multi UAVs simultaneously. In this mode, the GCS-UAV system is also considered a mobile system, which can be established ubiquitously. Because of the limitation of the power supply, the communication range of this system is less than 500 m between each node, but the entire communication system could range between 0 and 7 km in this network. Unfortunately, the communication has a larger packet delay than the point-to-point mode does.

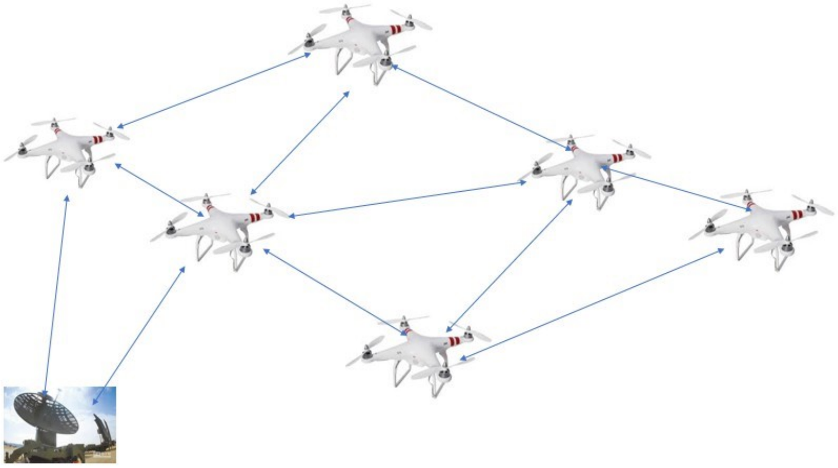


Fig. 3. Ad hoc mode communication structure. (Photograph is public access)

3) AP Mode. AP mode communication could be established between a GCS and two kinds aerial robotics: normal UAVs and AP UAVs. Users can have their own Wi-Fi router, and the GCS and the AP UAVs can be connected in an ad hoc network while normal UAVs are connected to AP UAVs. Details are shown in Fig. 4. In this mode, users have their own private networks, and different UAVs have different IP addresses. Users can have a AP-based, ad hoc network to control multi UAVs simultaneously. In the AP mode, the GCS-UAV system is also considered a mobile system, which can be established ubiquitously. Because of the limitation of the power supply, the communication range of this system is also between 0 and 7 km. In this mode, a network structure is simpler than the ad hoc mode; therefore, this mode has less packet exchange than does the ad hoc mode. The packet delay for this mode is between point-to-point mode and ad hoc mode.

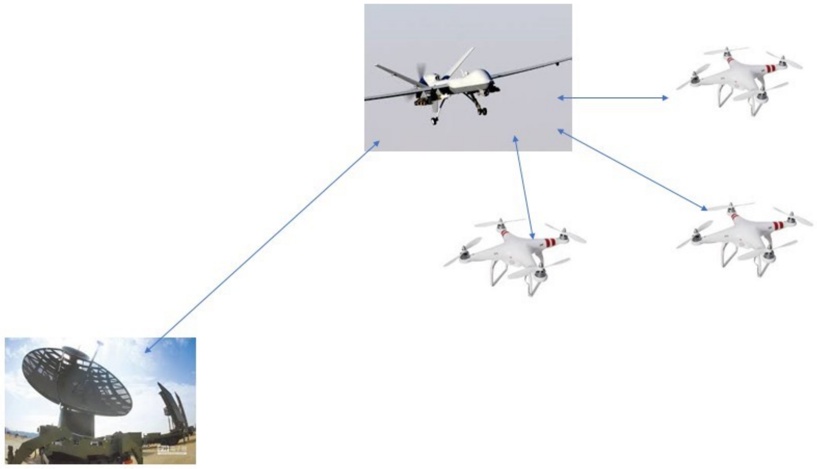


Fig. 4. AP mode communication structure. (Photograph is public access)

4) Ground Control Center Mode. Ground control center(GCC) mode can be established between a GCC and aerial robotics[8]. Users, i.e., GCSs connect to UAVs via a permanent GCC. A GCS and a UAV can be connected to a permanent Wi-Fi network to have TCP/IP communications. Details are shown in Fig. 5. In this mode, all users share one public network, and different UAVs and different GCSs have separate IP addresses. Users can access a metropolitan-area wireless network to control multi UAVs simultaneously. In this mode, the GCS-UAV system is also considered a mobile system, and the network is an extendable, permanent wireless network. Thus, AP can be deployed permanently on the ground or in the air while the GCC manages the network. Because the connection between GCS and UAV is enlarged to a metropolitan area network (MAN), the communication range of this system can be over 10 km. In this network, communication has a lower packet delay than the AP mode does.

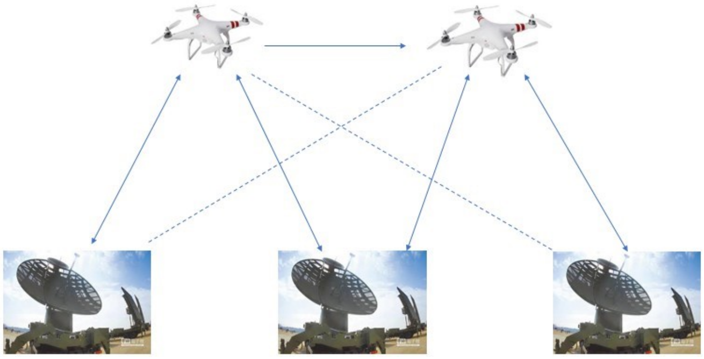


Fig. 5. GCS mode communication structure. (Photograph is public access)

B. Messages Types

Besides key exchange messages, current communication methods in aerial robotics includes two types of information messages: heartbeat and control [10]. Adding the routing message results in four types messages total that are sent in the new communication channel. They are discussed here in order of low priority to high priority.

1. States feedback message (heartbeat message)
2. Control message
3. Routing message
4. Key exchange message

Different communication protocols can be established among different kinds of messages. Therefore, different encryption methods should be used for different types of messages. The content of various kinds of messages is discussed below.

1) Heartbeat Message. A heartbeat message is sent periodically between the GCS and a UAV to ensure that the connection is still active. Depending on the heartbeat messages sent from UAV, the GCS is aware of the status of the drones, such as the altitude, speed, and position. Depending on the heartbeat messages sent from GCS, the UAV is aware that the channel is still stable.

2) Control Message. Managing the task detail of all the drones in the network, the GCS generates control messages. Two types of control modes exist for consumer and commercial drones: manual mode and auto mode.

3) Routing Message. A routing message is exchanged before the communication link is established, especially in the ad hoc mode, AP mode, and GCC mode. Because of the high flexibility of drone positions, routing messages will be sent frequently in the channel to achieve the highest quality of communication.

4) Key Exchange Messages. Key exchange messages are the most important part in key distribution. To establish the authentication and message encryption, every device needs to exchange its keys with others in the network.

C. Communication Phases

To ensure efficiency and security, the drone's in-air communication is divided into five message types, as listed below.

The channel message exchange can be divided into five types:

1. Initialization
2. Routing in air
3. Key exchange
4. Command message exchange
5. Heart beat message exchange

In the next chapter, key distribution details are discussed; in this chapter, all the keys are assumed to be already distributed.

1) Initialization. Initialization occurs when a new device (drone or ground control point) is powered on and linked to the network for first time. During the initialization phase, the new device accesses the network of the main ground control station

(MGCS). The MGCS then update the routing table of the new device and sends the key for the first session. Next, the MGCS will select the control and the communication modes to prepare for the subsequent communication phases.

A figure of the initialization is shown in Fig. 6. If a GCS sends a message, but the device does not receive the ACK message, this message is sent to the drone again.

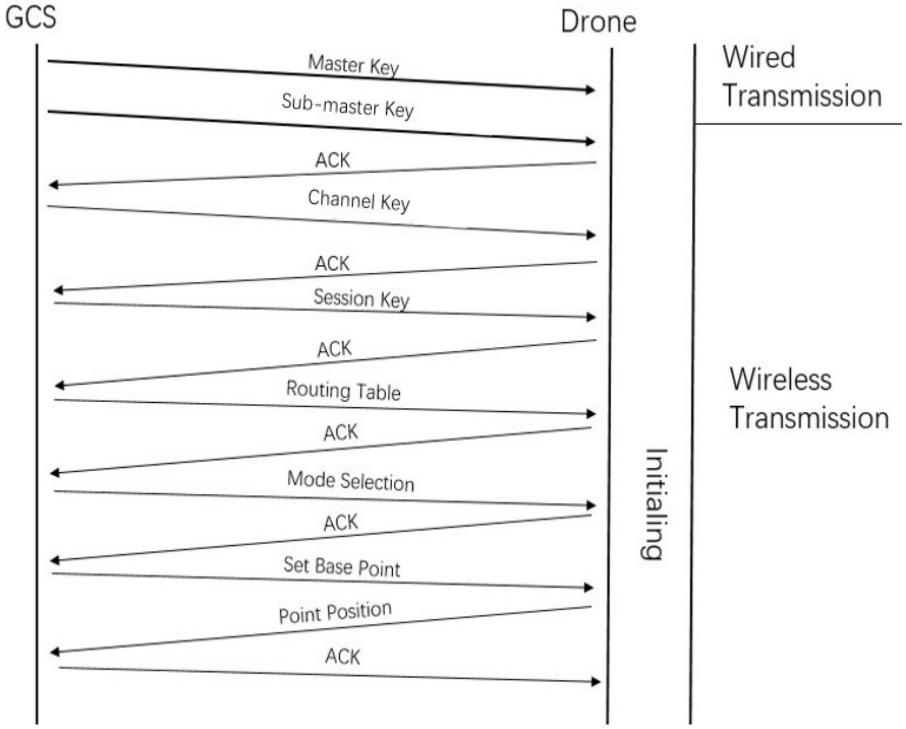


Fig. 6. Initialization phases.

2) Routing in Air. When the drone is airborne, the routing messages should be exchanged in the ad hoc mode, AP mode, and GCC mode whenever the communication mode is changed or the structure (position) of the network is changed. Because routing in the air is a complex problem, this paper does not address this issue.

3) Key Exchange. After the initialization phase, the MGCS generates the key exchange messages and sends them to the specific drone whenever the key chain is updated. The most important issue is deciding when to use the new key instead of the former one. Details are shown in Fig. 7. Every new key will be sent out before the old key expires.

After the drone sends out the key update massage and received the ACK, the key will be updated; otherwise, the key will not be updated until the former steps are completed.

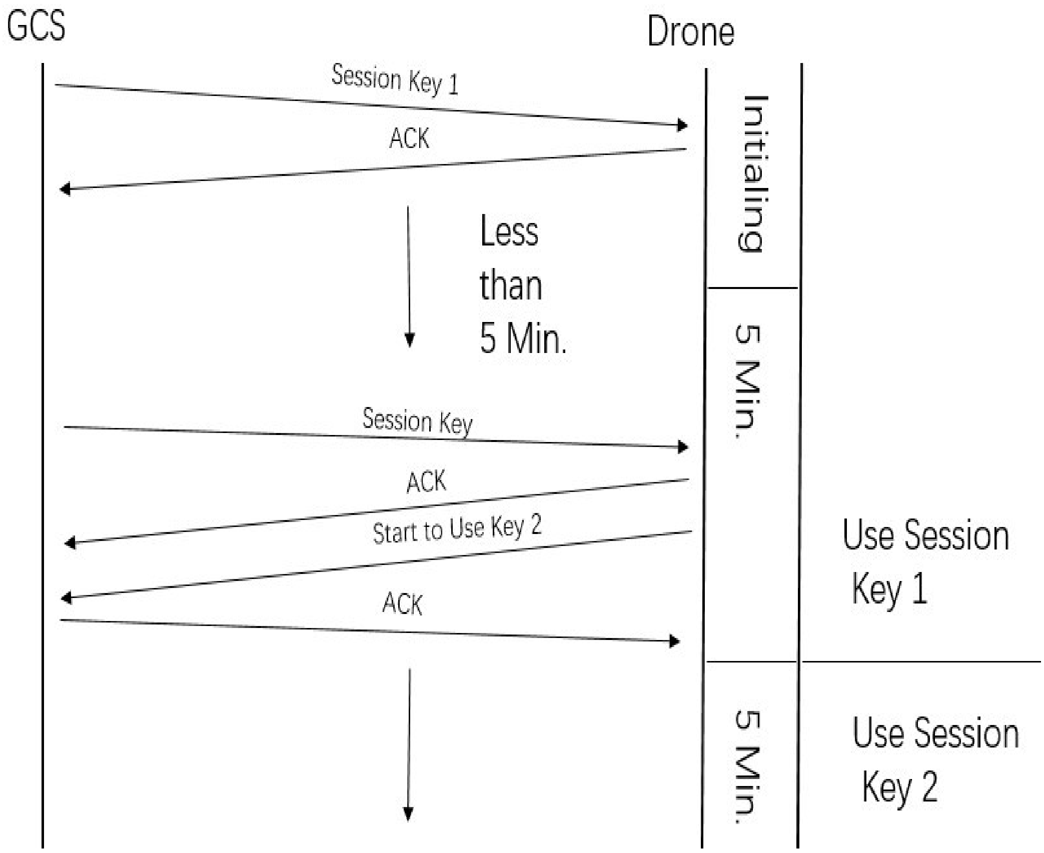


Fig. 7. Key exchange phases (in air).

4) Command Message Exchange. To transfer the command messages within the network, the control of the drone can be divided into two modes: manual and auto. If the drone is in auto mode and has not received any ACK, the GCS sends the command message again. As introduced in the background knowledge, the manual mode control is more sensitive and can tolerate less delay than the auto mode while the stability of auto mode is problematic. So, these two control modes need different communication protocols; the details of which are shown in Fig. 8. and Fig. 9.

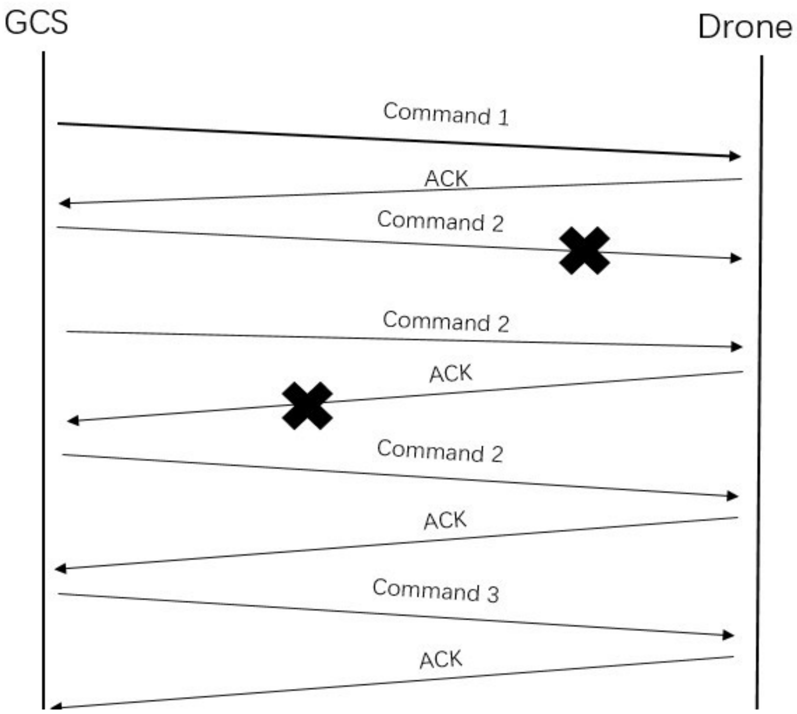


Fig. 8. Command exchange (auto mode) phases.

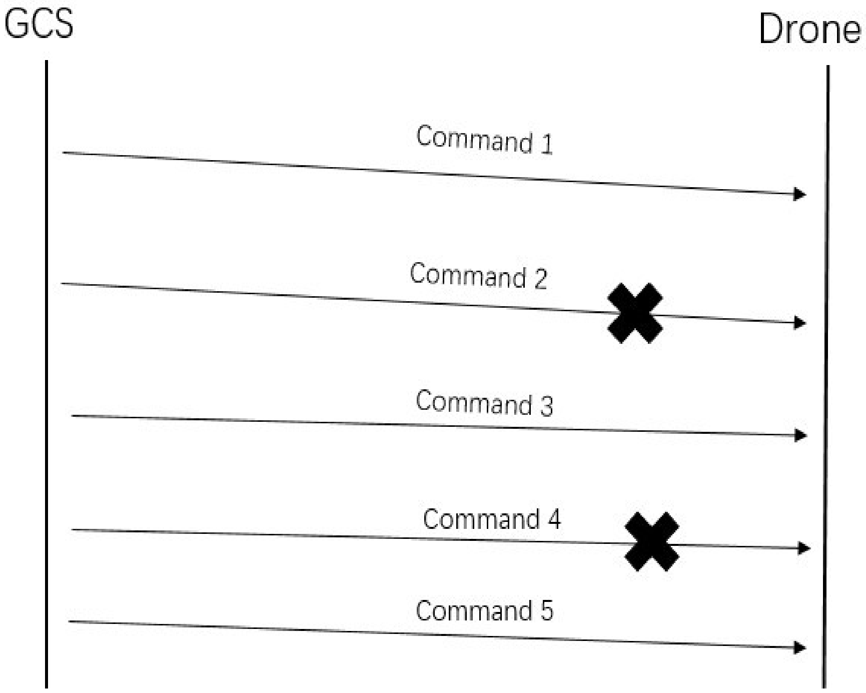


Fig. 9. Command exchange (manual mode) phases.

If the drone is in manual mode, any lost commands are not sent again, so the user must make adjustments to the commands on their own.

5) Heartbeat Message Exchange. The wireless communication environment is a complex one for the heart beat message. Although it may result in unpredictable path loss and shadowing effect on the channel, the frequency of the heart beat message is presumed stable. Package loss in the channel can actually be tolerated. Details are shown in Fig. 10.

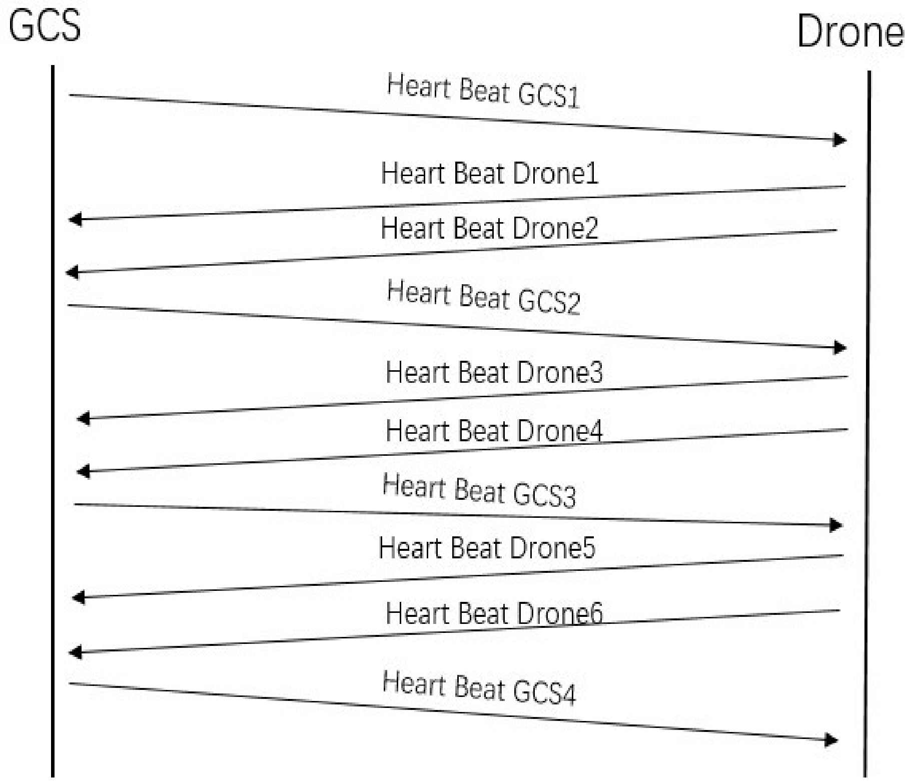


Fig. 10. Heart beat exchange phases.

Heart beat messages are sent periodically between GCS and drone; if the drone has continuously lost heart beat messages from the GCS, the drone automatically flies back.

VI. ENCRYPTION AND AUTHENTICATION IN COMMUNICATION NETWORK

To protect essential information in the network, the user should select encryption algorithms for different messages carefully. In this chapter, the encryption algorithm for each layer will be discussed thoroughly.

A. Comparison of Key Exchange Message ECC

Key exchange messages are used to deliver the sub-master, the session, and the channel keys. In the drone communication phases, the master key encrypts the sub-master key, and the sub-master key encrypts the session and channel keys.

Because protection for the communication system is established through encryption and authentication, the security of the key exchange message is the most essential part.

During initialization, key exchange messages are transferred first in the channel, with the sub-master key, channel key and the first session key being delivered to the drone step-by-step. In this case, we use public-key cryptography to establish authentication and encryption.

1) Public-key Cryptography. The key pair, or public-key cryptography, has two parts: the public key and the private key. People can use either of the keys for encryption and the other key for decryption.

In the proposed drone communication network, GCS first generates its own and the drone's public keys and private keys, then send GCS's public key and drone's private key to the drone. When the GCS sends a key distribution message to a drone, the message will first be encrypted by GCS's private key, then it will be encrypted by the drone's public key. To decrypt packages from the GCS, the drone should first use its own private key before using the GCS’s public key. The drone’s public-key pair ensure the message can be decrypted only by the drone for encryption purpose and GCS’s public-key pair to ensure that the drone recognizes the message that the GSC had sent for authentication purpose.

In the network, one device has its own private key and others’ public keys.

In this paper, RSA and ECC algorithms are compared in order to determine the better system performance.

2) RSA Cryptography. RSA is the oldest and most widely used public-key cryptography algorithm. RSA cryptography relies on the assumption that factoring is a hard task for calculation. This means that even though attackers have sufficient computing resources and sufficient time, an adversary should not be able to penetrate the RSA by factoring.

3) RSA Key Generation. A RSA public and private key pair can be generated using the algorithm below [2]:

1. Choose two random prime numbers p and q such that the bit length of p is approximately equal to the bit length of q.

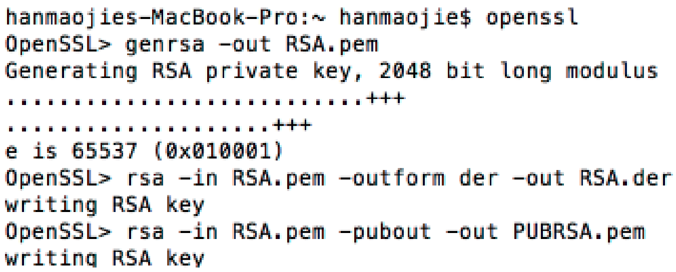
2. Compute n such that $n = p * q$.

3. Compute Euler’s totient function such that $\varphi(n) = (p – 1) *(q – 1)$.

4. Choose a random integer e such that $e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$, and then compute the integer d such that: $e*d \equiv 1 \bmod \varphi(n)$.

5. (n, e) is the public key, and d is the private key.

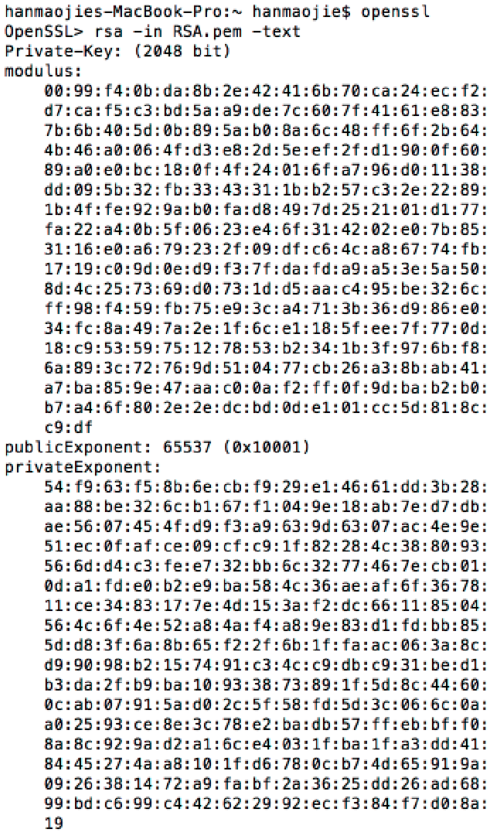
The generation of the key is shown in Fig. 11.



```
hanmaojies-MacBook-Pro:~ hanmaojie$ openssl
OpenSSL> genrsa -out RSA.pem
Generating RSA private key, 2048 bit long modulus
...........................+++
....................+++
e is 65537 (0x010001)
OpenSSL> rsa -in RSA.pem -outform der -out RSA.der
writing RSA key
OpenSSL> rsa -in RSA.pem -pubout -out PUBRSA.pem
writing RSA key
```

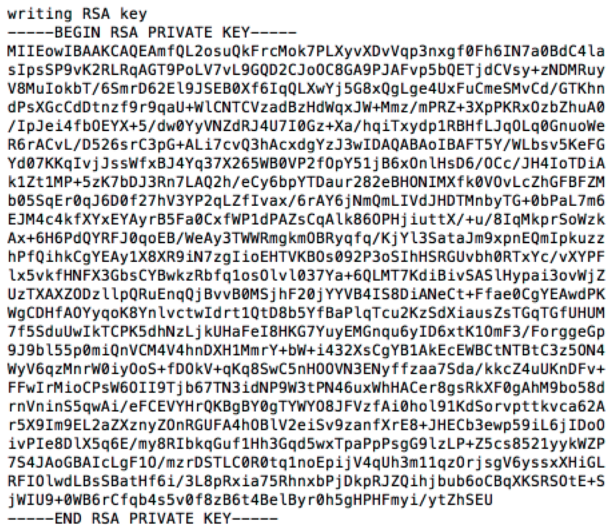
Fig. 11. RSA key pair generation.

The public key and the private key are shown in Fig. 12., Fig. 13. and Fig. 14.



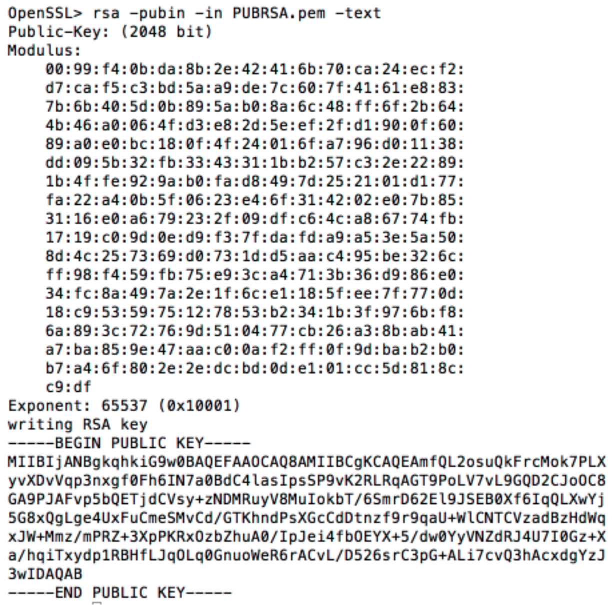
```
hanmaojies-MacBook-Pro:~ hanmaojie$ openssl
OpenSSL> rsa -in RSA.pem -text
Private-Key: (2048 bit)
modulus:
    00:99:f4:0b:da:8b:2e:42:41:6b:70:ca:24:ec:f2:
    d7:ca:f5:c3:bd:5a:a9:de:7c:60:7f:41:61:e8:83:
    7b:6b:40:5d:0b:89:5a:b0:8a:6c:48:ff:6f:2b:64:
    4b:46:a0:06:4f:d3:e8:2d:5e:ef:2f:d1:90:0f:60:
    89:a0:e0:bc:18:0f:4f:24:01:6f:a7:96:d0:11:38:
    dd:09:5b:32:fb:33:43:31:1b:b2:57:c3:2e:22:89:
    1b:4f:fe:92:9a:b0:fa:d8:49:7d:25:21:01:d1:77:
    fa:22:a4:0b:5f:06:23:e4:6f:31:42:02:e0:7b:85:
    31:16:e0:a6:79:23:2f:09:df:c6:4c:a8:67:74:fb:
    17:19:c0:9d:0e:d9:f3:7f:da:fd:a9:a5:3e:5a:50:
    8d:4c:25:73:69:d0:73:1d:d5:aa:c4:95:be:32:6c:
    ff:98:f4:59:fb:75:e9:3c:a4:71:3b:36:d9:86:e0:
    34:fc:8a:49:7a:2e:1f:6c:e1:18:5f:ee:7f:77:0d:
    18:c9:53:59:75:12:78:53:b2:34:1b:3f:97:6b:f8:
    6a:89:3c:72:76:9d:51:04:77:cb:26:a3:8b:ab:41:
    a7:ba:85:9e:47:aa:c0:0a:f2:ff:0f:9d:ba:b2:b0:
    b7:a4:6f:80:2e:2e:dc:bd:0d:e1:01:cc:5d:81:8c:
    c9:df
publicExponent: 65537 (0x10001)
privateExponent:
    54:f9:63:f5:8b:6e:cb:f9:29:e1:46:61:dd:3b:28:
    aa:88:be:32:6c:b1:67:f1:04:9e:18:ab:7e:d7:db:
    ae:56:07:45:4f:d9:f3:a9:63:9d:63:07:ac:4e:9e:
    51:ec:0f:af:ce:09:cf:c9:1f:82:28:4c:38:80:93:
    56:6d:d4:c3:fe:e7:32:bb:6c:32:77:46:7e:cb:01:
    0d:a1:fd:e0:b2:e9:ba:58:4c:36:ae:af:6f:36:78:
    11:ce:34:83:17:7e:4d:15:3a:f2:dc:66:11:85:04:
    56:4c:6f:4e:52:a8:4a:f4:a8:9e:83:d1:fd:bb:85:
    5d:d8:3f:6a:8b:65:f2:2f:6b:1f:fa:ac:06:3a:8c:
    d9:90:98:b2:15:74:91:c3:4c:c9:db:c9:31:be:d1:
    b3:da:2f:b9:ba:10:93:38:73:89:1f:5d:8c:44:60:
    0c:ab:07:91:5a:d0:2c:5f:58:fd:5d:3c:06:6c:0a:
    a0:25:93:ce:8e:3c:78:e2:ba:db:57:ff:eb:bf:f0:
    8a:8c:92:9a:d2:a1:6c:e4:03:1f:ba:1f:a3:dd:41:
    84:45:27:4a:a8:10:1f:d6:78:0c:b7:4d:65:91:9a:
    09:26:38:14:72:a9:fa:bf:2a:36:25:dd:26:ad:68:
    99:bd:c6:99:c4:42:62:29:92:ec:f3:84:f7:d0:8a:
    19
```

Fig. 12. RSA private key modulus and exponent.



```
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAmfQL2osuQkFrcMok7PLXyvXDvVqp3nxgf0Fh6IN7a0BdC4la
sIpsSP9vK2RLRqAGT9PoLV7vL9GQD2CJoOC8GA9PJAFvp5bQETjdCVsy+zNDMRuy
V8MuIokbT/6SmrD62El9JSEB0Xf6IqQLXwYj5G8xQgLge4UxFuCmeSMvCd/GTKhn
dPsXGcCdDtnzf9r9qaU+WlCNTCVzadBzHdWqxJW+Mmz/mPRZ+3XpPKRxOzbZhuA0
/IpJei4fbOEYX+5/dw0YyVNZdRJ4U7I0Gz+Xa/hqiTxydp1RBHfLJqOLq0GnuoWe
R6rACvL/D526srC3pG+ALi7cvQ3hAcxdgYzJ3wIDAQABAoIBAFT5Y/WLbsv5KeFG
Yd07KKqIvjJssWfxBJ4Yq37X265WB0VP2fOpY51jB6xOnlHsD6/OCc/JH4IoTDiA
k1Zt1MP+5zK7bDJ3Rn7LAQ2h/eCy6bpYTDaur282eBHONIMXfk0VOvLcZhGFBFZM
b05SqEr0qJ6D0f27hV3YP2qLZfIvax/6rAY6jNmQmLIVdJHDTMnbyTG+0bPaL7m6
EJM4c4kfXYxEYAyrB5Fa0CxfWP1dPAZsCqAlk86OPHjiuttX/+u/8IqMkprSoWzk
Ax+6H6PdQYRFJ0qoEB/WeAy3TWWRmgkmOBRyqfq/KjYl3SataJm9xpnEQmIpkuzz
hPfQihkCgYEAy1X8XR9iN7zgIioEHTVKBOs092P3oSIhHSRGUvbh0RTxYc/vXYPF
lx5vkfHNFX3GbsCYBwkzRbfq1osOlvl037Ya+6QLMT7KdiBivSASlHypai3ovWjZ
UzTXAXZODzllpQRuEnqQjBvvB0MSjhF20jYYVB4IS8DiANeCt+Ffae0CgYEAwdPK
WgCDHfAOYyqoK8YnlvctwIdrt1QtD8b5YfBaPlqTcu2KzSdXiausZsTGqTGfUHUM
7f5SduUwIkTCPK5dhNzLjkUHaFeI8HKG7YuyEMGnqu6yID6xtK1OmF3/ForggeGp
9J9bl55p0miQnVCM4V4hnDXH1MmrY+bW+i432XsCgYB1AkEcEWBCtNTBtC3z5ON4
WyV6qzMnrW0iyOoS+fDOkV+qKq8SwC5nHOOVN3ENyffzaa7Sda/kkcZ4uUKnDFv+
FFwIrMioCPsW6OII9Tjb67TN3idNP9W3tPN46uxWhHACer8gsRkXF0gAhM9bo58d
rnVninS5qwAi/eFCEVYHrQKBgBY0gTYWYO8JFVzfAi0hol91KdSorvpttkvca62A
r5X9Im9EL2aZXznyZOnRGUFA4hOBlV2eiSv9zanfXrE8+JHECb3ewp59iL6jIDoO
ivPIe8DlX5q6E/my8RIbkqGuf1Hh3Gqd5wxTpaPpPsgG9lzLP+Z5cs8521yykWZP
7S4JAoGBAIcLgF1O/mzrDSTLC0R0tq1noEpijV4qUh3m11qzOrjsgV6yssxXHiGL
RFIOlwdLBsSBatHf6i/3L8pRxia75RhnxbPjDkpRJZQihjbub6oCBqXKSRSOtE+S
jWIU9+0WB6rCfqb4s5v0f8zB6t4BelByr0h5gHPHFmyi/ytZhSEU
-----END RSA PRIVATE KEY-----
```

Fig. 13. RSA private key.



```
OpenSSL> rsa -pubin -in PUBRSA.pem -text
Public-Key: (2048 bit)
Modulus:
    00:99:f4:0b:da:8b:2e:42:41:6b:70:ca:24:ec:f2:
    d7:ca:f5:c3:bd:5a:a9:de:7c:60:7f:41:61:e8:83:
    7b:6b:40:5d:0b:89:5a:b0:8a:6c:48:ff:6f:2b:64:
    4b:46:a0:06:4f:d3:e8:2d:5e:ef:2f:d1:90:0f:60:
    89:a0:e0:bc:18:0f:4f:24:01:6f:a7:96:d0:11:38:
    dd:09:5b:32:fb:33:43:31:1b:b2:57:c3:2e:22:89:
    1b:4f:fe:92:9a:b0:fa:d8:49:7d:25:21:01:d1:77:
    fa:22:a4:0b:5f:06:23:e4:6f:31:42:02:e0:7b:85:
    31:16:e0:a6:79:23:2f:09:df:c6:4c:a8:67:74:fb:
    17:19:c0:9d:0e:d9:f3:7f:da:fd:a9:a5:3e:5a:50:
    8d:4c:25:73:69:d0:73:1d:d5:aa:c4:95:be:32:6c:
    ff:98:f4:59:fb:75:e9:3c:a4:71:3b:36:d9:86:e0:
    34:fc:8a:49:7a:2e:1f:6c:e1:18:5f:ee:7f:77:0d:
    18:c9:53:59:75:12:78:53:b2:34:1b:3f:97:6b:f8:
    6a:89:3c:72:76:9d:51:04:77:cb:26:a3:8b:ab:41:
    a7:ba:85:9e:47:aa:c0:0a:f2:ff:0f:9d:ba:b2:b0:
    b7:a4:6f:80:2e:2e:dc:bd:0d:e1:01:cc:5d:81:8c:
    c9:df
Exponent: 65537 (0x10001)
writing RSA key
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmfQL2osuQkFrcMok7PLX
yvXDvVqp3nxgf0Fh6IN7a0BdC4lasIpsSP9vK2RLRqAGT9PoLV7vL9GQD2CJoOC8
GA9PJAFvp5bQETjdCVsy+zNDMRuyV8MuIokbT/6SmrD62El9JSEB0Xf6IqQLXwYj
5G8xQgLge4UxFuCmeSMvCd/GTKhndPsXGcCdDtnzf9r9qaU+WlCNTCVzadBzHdWq
xJW+Mmz/mPRZ+3XpPKRxOzbZhuA0/IpJei4fbOEYX+5/dw0YyVNZdRJ4U7I0Gz+X
a/hqiTxydp1RBHfLJqOLq0GnuoWeR6rACvL/D526srC3pG+ALi7cvQ3hAcxdgYzJ
3wIDAQAB
-----END PUBLIC KEY-----
```

Fig. 14. RSA public key.

4) Elliptic Curve Cryptography (ECC). An elliptic curve is given by an equation [2] in the form of

$$y^2 = x^3 + ax + b$$

where $4a^3 + 27b^2 \neq 0$

Many interesting problems arise from the set of points on elliptic curves over a finite field under group operations. The finite fields that are commonly used are those over primes (Fp) and binary fields (F2n). The security of ECC is based on the elliptic curve discrete logarithm problem (ECDLP). This problem is defined as follows:

Given points X, Y on the elliptic curve, find z such that:

$X=zY$

The discrete logarithm problem over this group in a finite field is a trapdoor one-way function because there are currently no known polynomial time attacks for solving the problem. The methods for computing the solutions to the ECDPL are much less efficient than that of factoring, so ECC, which was developed independently by Neal Koblitz and Victor Miller in 1985, can provide the same security as RSA with smaller key lengths.

5) ECC Key Generation. To generate a public and a private key pair to use in ECC communications, an entity would perform the following steps:

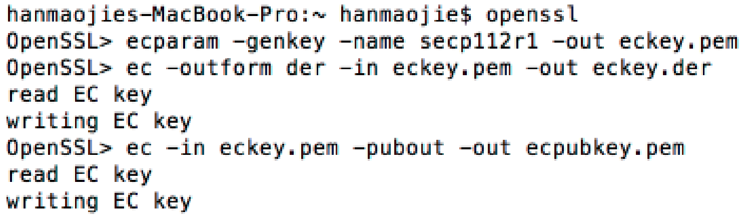
1. Find an elliptic curve E(K), where K is a finite field such as Fp or F2n, and a given point on E(K). n is the order of Q.

2. Select a pseudo random number x such that $1 \leq x \leq (n - 1)$.

3. Compute point P = xQ.

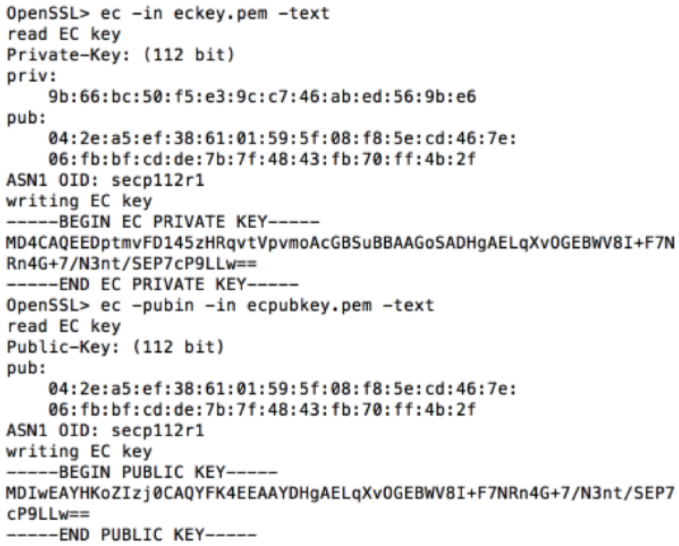
4. The ECC key pair is (P, x), where P is the public key, and x is the private key.

The generation of the ECC key is shown in Fig. 15. and an example of the ECC key is shown in Fig. 16.



```
hanmaojies-MacBook-Pro:~ hanmaojie$ openssl
OpenSSL> ecparam -genkey -name secp112r1 -out eckey.pem
OpenSSL> ec -outform der -in eckey.pem -out eckey.der
read EC key
writing EC key
OpenSSL> ec -in eckey.pem -pubout -out ecpubkey.pem
read EC key
writing EC key
```

Fig. 15. ECC key generation.



```
OpenSSL> ec -in eckey.pem -text
read EC key
Private-Key: (112 bit)
priv:
    9b:66:bc:50:f5:e3:9c:c7:46:ab:ed:56:9b:e6
pub:
    04:2e:a5:ef:38:61:01:59:5f:08:f8:5e:cd:46:7e:
    06:fb:bf:cd:de:7b:7f:48:43:fb:70:ff:4b:2f
ASN1 OID: secp112r1
writing EC key
-----BEGIN EC PRIVATE KEY-----
MD4CAQEEDptmvFD145zHRqvtVpvmoAcGBSuBBAAGoSADHgAELqXvOGEBWV8I+F7N
Rn4G+7/N3nt/SEP7cP9LLw==
-----END EC PRIVATE KEY-----
OpenSSL> ec -pubin -in ecpubkey.pem -text
read EC key
Public-Key: (112 bit)
pub:
    04:2e:a5:ef:38:61:01:59:5f:08:f8:5e:cd:46:7e:
    06:fb:bf:cd:de:7b:7f:48:43:fb:70:ff:4b:2f
ASN1 OID: secp112r1
writing EC key
-----BEGIN PUBLIC KEY-----
MDIwEAYHKoZIzj0CAQYFK4EEAAYDHgAELqXvOGEBWV8I+F7NRn4G+7/N3nt/SEP7
cP9LLw==
-----END PUBLIC KEY-----
```

Fig. 16. ECC private key and public key.

Based on the algorithm details, the ECC algorithm can use shorter keys to ensure the same level of security for the messages, as in RSA. The processing time for encryption and decryption is less than that for the RSA. In this scenario, we select ECC to encrypt messages in the aerial robotics communication channel.

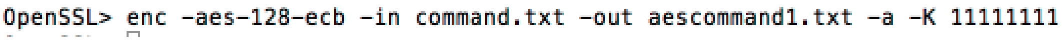
B. Comparison of Command Message AES

For the command message, users can select a block cipher to protect the message. Compared to stream ciphers, block ciphers such as AES can provide better protection with shorter keys.

Session keys and channel keys are two parts of the AES key; both keys are transferred and updated separately to ensure the security.

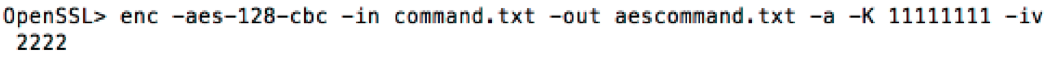
In AES, the cipher takes a plaintext block size of 128 bits, or 16 bytes. The key length can be 16, 24, or 32 bytes (128, 192, or 256 bits). The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key’s length, respectively.

A sample for AES encryption and decryption, commands for encryption and decryption are shown below, in Fig. 17., Fig. 18., and Fig. 19.



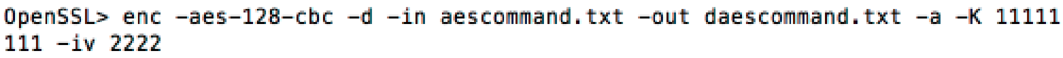
```
OpenSSL> enc -aes-128-ecb -in command.txt -out aescommand1.txt -a -K 11111111
```

Fig. 17. AES ECB encryption.



```
OpenSSL> enc -aes-128-cbc -in command.txt -out aescommand.txt -a -K 11111111 -iv
 2222
```

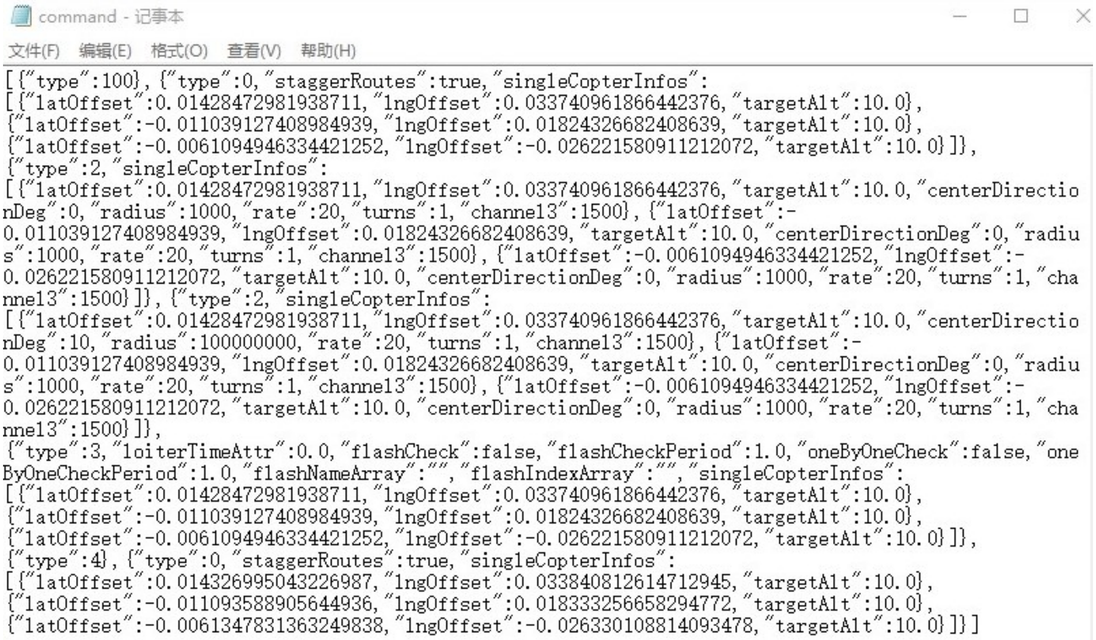
Fig. 18. AES CBC encryption.



```
OpenSSL> enc -aes-128-cbc -d -in aescommand.txt -out daescommand.txt -a -K 11111
111 -iv 2222
```

Fig. 19. AES CBC decryption.

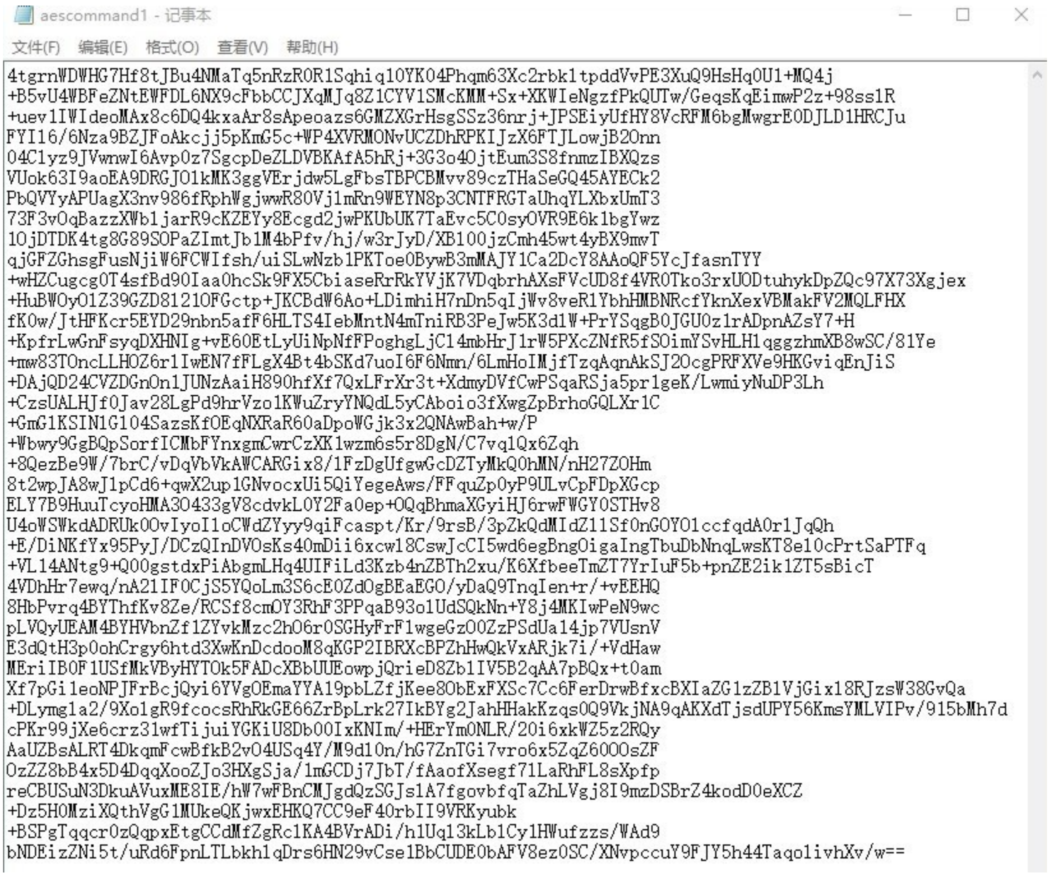
And consequences for these commands are shown below. In Fig. 20, a sample way-point mode command of the drone is given, which includes several steps that are informed by position order. This is a plain text message, which will be encrypted below.



```
[{"type":100},{"type":0,"staggerRoutes":true,"singleCopterInfos":
[{"latOffset":0.01428472981938711,"lngOffset":0.033740961866442376,"targetAlt":10.0},
{"latOffset":-0.011039127408984939,"lngOffset":0.01824326682408639,"targetAlt":10.0},
{"latOffset":-0.0061094946334421252,"lngOffset":-0.026221580911212072,"targetAlt":10.0}]},
{"type":2,"singleCopterInfos":
[{"latOffset":0.01428472981938711,"lngOffset":0.033740961866442376,"targetAlt":10.0,"centerDirectio
nDeg":0,"radius":1000,"rate":20,"turns":1,"channel3":1500},{"latOffset":-
0.011039127408984939,"lngOffset":0.01824326682408639,"targetAlt":10.0,"centerDirectionDeg":0,"radiu
s":1000,"rate":20,"turns":1,"channel3":1500},{"latOffset":-0.0061094946334421252,"lngOffset":-
0.026221580911212072,"targetAlt":10.0,"centerDirectionDeg":0,"radius":1000,"rate":20,"turns":1,"cha
nnel3":1500}]},{"type":2,"singleCopterInfos":
[{"latOffset":0.01428472981938711,"lngOffset":0.033740961866442376,"targetAlt":10.0,"centerDirectio
nDeg":10,"radius":100000000,"rate":20,"turns":1,"channel3":1500},{"latOffset":-
0.011039127408984939,"lngOffset":0.01824326682408639,"targetAlt":10.0,"centerDirectionDeg":0,"radiu
s":1000,"rate":20,"turns":1,"channel3":1500},{"latOffset":-0.0061094946334421252,"lngOffset":-
0.026221580911212072,"targetAlt":10.0,"centerDirectionDeg":0,"radius":1000,"rate":20,"turns":1,"cha
nnel3":1500}]},
{"type":3,"loiterTimeAttr":0.0,"flashCheck":false,"flashCheckPeriod":1.0,"oneByOneCheck":false,"one
ByOneCheckPeriod":1.0,"flashNameArray":"","flashIndexArray":"","singleCopterInfos":
[{"latOffset":0.01428472981938711,"lngOffset":0.033740961866442376,"targetAlt":10.0},
{"latOffset":-0.011039127408984939,"lngOffset":0.01824326682408639,"targetAlt":10.0},
{"latOffset":-0.0061094946334421252,"lngOffset":-0.026221580911212072,"targetAlt":10.0}]},
{"type":4},{"type":0,"staggerRoutes":true,"singleCopterInfos":
[{"latOffset":0.014326995043226987,"lngOffset":0.03384081261471294 5,"targetAlt":10.0},
{"latOffset":-0.011093588905644936,"lngOffset":0.018333256658294772,"targetAlt":10.0},
{"latOffset":-0.0061347831363249838,"lngOffset":-0.026330108814093478,"targetAlt":10.0}]}]
```

Fig. 20. Command message plain text.

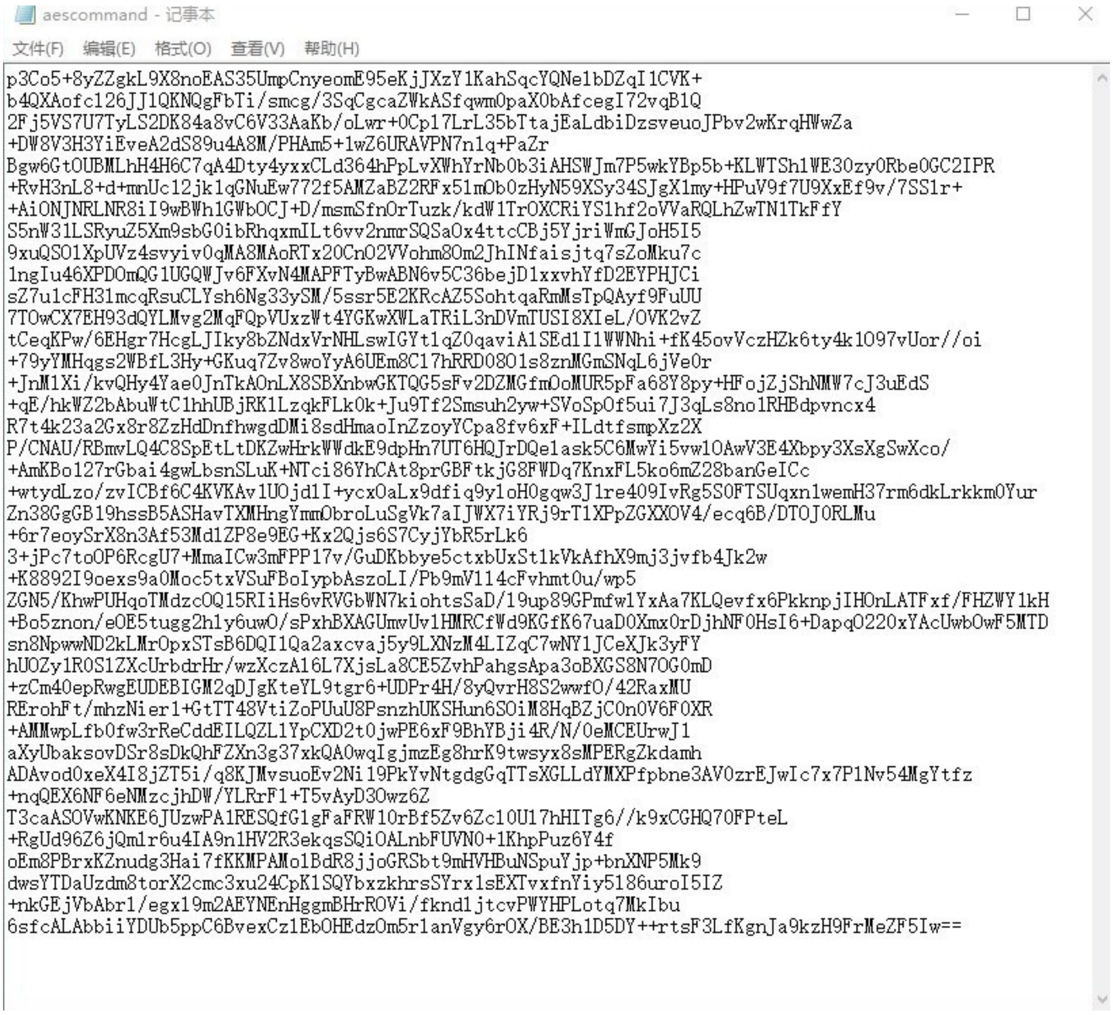
In Fig. 21, the former plain text is encrypted by the AES-ECB method. The key length is 128 bits. In this method, the plain text is divided into several blocks, and each block is encrypted independently by the AES key.



```
4tgrnWDWHG7Hf8tJBu4NMaTq5nRzR0R1Sqhiq10YK04Phqm63Xc2rbk1tpddVvPE3XuQ9HsHq0U1+MQ4j
+B5vU4WBFeZNtEWFDL6NX9cFbbCCJXqMJq8Z1CYV1SMcKMM+Sx+XKWIeNgzfPkQUTw/GeqsKqEimwP2z+98ss1R
+uev1IWIdeoMAx8c6DQ4kxaAr8sApeoazs6GMZXGrHsgSSz36nrj+JPSEiyUfHY8VcRFM6bgMwgrE0DJLD1HRCJu
FYI16/6Nza9BZJFoAkcjj5pKmG5c+WP4XVRMONvUCZDhRPKIJzX6FTJLowjB2Onn
04C1yz9JVwnwI6Avp0z7SgcpDeZLDVBKAfA5hRj+3G3o40jtEum3S8fnmzIBXQzs
VUok63I9aoEA9DRGJO1kMK3ggVErjdw5LgFbsTBPCBMvv89czTHaSeGQ45AYECk2
PbQVYyAPUagX3nv986fRphWgjwwR80Vj1mRn9WEYN8p3CNTFRGTaUhqYLXbxUmT3
73F3v0qBazzXWb1jarR9cKZEYy8Ecgd2jwPKUbUK7TaEvc5C0sy0VR9E6k1bgYwz
10jDTDK4tg8G89SOPaZImtJb1M4bPfv/hj/w3rJyD/XB100jzCmh45wt4yBX9mwT
qjGFZGhsgFusNjiW6FCWIfsh/uiSLwNzb1PKToe0BywB3mMAJY1Ca2DcY8AAoQF5YcJfasnTYY
+wHZCugcg0T4sfBd90Iaa0hcSk9FX5CbiaseRrRkYVjK7VDqbrhAXsFVcUD8f4VR0Tko3rxUODtuhykDpZQc97X73Xgjex
+HuBWOy01Z39GZD81210FGctp+JKCBdW6Ao+LDimhiH7nDn5qIjWv8veR1YbhHMBNRcfYknXexVBMakFV2MQLFHX
fK0w/JtHFKcr5EYD29nbn5afF6HLTS4IebMntN4mTniRB3PeJw5K3d1W+PrYSqgB0JGU0z1rADpnAZsY7+H
+KpfrLwGnFsyqDXHNIg+vE60EtLyUiNpNfFPoghgLjC14mbHrJ1rW5PXcZNfR5fSOimYSvHLH1qggzhmXB8wSC/81Ye
+mw83TOncLLHOZ6r1IwEN7fFLgX4Bt4bSKd7uoI6F6Nmn/6LmHoIMjfTzqAqnAkSJ2OcgPRFXVe9HKGviqEnJiS
+DAjQD24CVZDGnOn1JUNzAaiH890hfXf7QxLFrXr3t+XdmyDVfCwPSqaRSja5pr1geK/LwmiyNuDP3Lh
+CzsUALHJf0Jav28LgPd9hrVzo1KWuZryYNQdL5yCAboio3fXwgZpBrhoGQLXr1C
+GmG1KSIN1G104SazsKfOEqNXRaR60aDpoWGjk3x2QNAwBah+w/P
+Wbwy9GgBQpSorfICMbFYnxgmCwrCzXK1wzm6s5r8DgN/C7vq1Qx6Zqh
+8QezBe9W/7brC/vDqVbVkAWCARGix8/1FzDgUfgwGcDZTyMkQ0hMN/nH27ZOHm
8t2wpJA8wJ1pCd6+qwX2up1GNvocxUi5QiYegeAws/FFquZp0yP9ULvCpFDpXGcp
ELY7B9HuuTcyoHMA30433gV8cdvkL0Y2Fa0ep+OQqBhmaXGyiHJ6rwFWGY0STHv8
U4oWSWkdADRUk0OvIyoI1oCWdZYyy9qiFcaspt/Kr/9rsB/3pZkQdMIdZ11Sf0nGOYO1ccfqdA0r1JqQh
+E/DiNKfYx95PyJ/DCzQInDVOsKs40mDii6xcw18CswJcCI5wd6egBngOigaIngTbuDbNnqLwsKT8e10cPrtSaPTFq
+VL14ANtg9+Q00gstdxPiAbgmLHq4UIFiLd3Kzb4nZBTh2xu/K6XfbeeTmZT7YrIuF5b+pnZE2ik1ZT5sBicT
4VDhHr7ewq/nA21IF0CjS5YQoLm3S6cE0Zd0gBEaEGO/yDaQ9TnqIen+r/+vEEHQ
8HbPvrq4BYThfKv8Ze/RCSf8cmOY3RhF3PPqaB93o1UdSQkNn+Y8j4MKIwPeN9wc
pLVQyUEAM4BYHVbnZf1ZYvkMzc2hO6r0SGHyFrF1wgeGzO0ZzPSdUa14jp7VUsnV
E3dQtH3p0ohCrgy6htd3XwKnDcdooM8qKGP2IBRXcBPZhHwQkVxARjk7i/+VdHaw
MEriIB0F1USfMkVByHYTOk5FADcXBbUUEowpjQrieD8Zb1IV5B2qAA7pBQx+t0am
Xf7pGi1eoNPJFrBcjQyi6YVgOEmaYYA19pbLZfjKee80bExFXSc7Cc6FerDrwBfxcBXIaZG1zZB1VjGix18RJzsW38GvQa
+DLymg1a2/9Xo1gR9fcocsRhRkGE66ZrBpLrk27IkBYg2JahHHakKzqs0Q9VkjNA9qAKXdTjsdUPY56KmsYMLVIPv/915bMh7d
cPKr99jXe6crz31wfTijuiYGKiU8Db00IxKNIm/+HErYm0NLR/20i6xkWZ5z2RQy
AaUZBsALRT4DkqmFcwBfkB2vO4USq4Y/M9d10n/hG7ZnTGi7vro6x5ZqZ6000sZF
0zZZ8bB4x5D4DqqXooZJo3HXgSja/1mGCDj7JbT/fAaofXsegf71LaRhFL8sXpfp
reCBUSuN3DkuAVuxME8IE/hW7wFBnCMJgdQzSGJs1A7fgovbfqTaZhLVgj8I9mzDSBrZ4kodD0eXCZ
+Dz5H0MziXQthVgG1MUkeQKjwxEHKQ7CC9eF40rbII9VRKyubk
+BSPgTqqcr0zQqpxEtgCCdMfZgRc1KA4BVrADi/h1Uq13kLb1Cy1HWufzzs/WAd9
bNDEizZNi5t/uRd6FpnLTLbkh1qDrs6HN29vCse1BbCUDE0bAFV8ez0SC/XNvpccuY9FJY5h44Taqo1ivhXv/w==
```

Fig. 21. Command message AES ECB encrypted text.

In Fig. 22, the AES-CBC method encrypts the former plain text message. The key length is 128 bits.

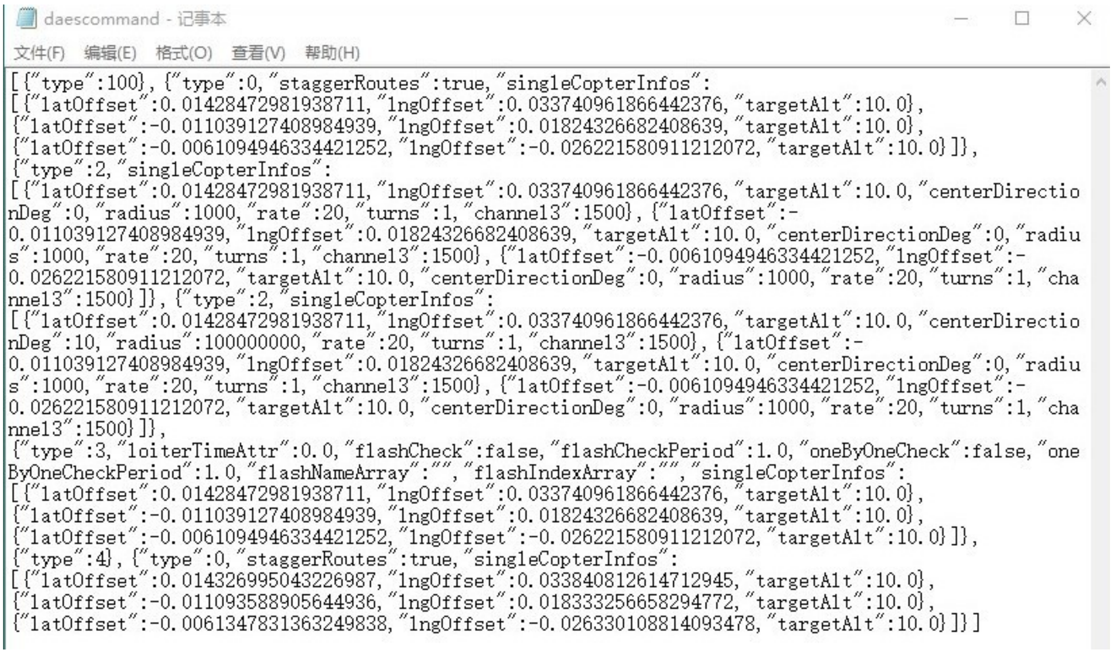


```
p3Co5+8yZZgkL9X8noEAS35UmpCnyeomE95eKjJXzY1KahSqcYQNe1bDZqI1CVK+
b4QXAofc126JJ1QKNQgFbTi/smcg/3SqCgcaZWkASfqwm0paX0bAfcegI72vqB1Q
2Fj5VS7U7TyLS2DK84a8vC6V33AaKb/oLwr+0Cp17LrL35bTtajEaLdbiDzsveuoJPbv2wKrqHWwZa
+DW8V3H3YiEveA2dS89u4A8M/PHAm5+1wZ6URAVPN7n1q+PaZr
Bgw6GtOUBMLhH4H6C7qA4Dty4yxxCLd364hPpLvXWhYrNb0b3iAHSWJm7P5wkYBp5b+KLWTSh1WE30zy0Rbe0GC2IPR
+RvH3nL8+d+mnUc12jk1qGNuEw772f5AMZaBZ2RFx51m0b0zHyN59XSy34SJgX1my+HPuV9f7U9XxEf9v/7SS1r+
+AiONJNRLNR8iI9wBWh1GWbOCJ+D/msmSfnOrTuzk/kdW1TrOXCRiYS1hf2oVVaRQLhZwTN1TkFfY
S5nW31LSRyuZ5Xm9sbG0ibRhqxmILt6vv2nmrSQSaOx4ttcCBj5YjriWmGJoH5I5
9xuQSO1XpUVz4svyiv0qMA8MAoRTx20CnO2VVohm8Om2JhINfaisjtq7sZoMku7c
1ngIu46XPDOmQG1UGQWJv6FXvN4MAPFTyBwABN6v5C36bejD1xxvhYfD2EYPHJCi
sZ7u1cFH31mcqRsuCLYsh6Ng33ySM/5ssr5E2KRcAZ5SohtqaRmMsTpQAyf9FuUU
7TOwCX7EH93dQYLMvg2MqFQpVUxzWt4YGKwXWLaTRiL3nDVmTUSI8XIeL/OVK2vZ
tCeqKPw/6EHgr7HcgLJIky8bZNdxVrNHLswIGYt1qZ0qaviA1SEd1I1WWNhi+fK45ovVczHZk6ty4k1O97vUor//oi
+79yYMHqgs2WBfL3Hy+GKuq7Zv8woYyA6UEm8C17hRRD08O1s8znMGmSNqL6jVe0r
+JnM1Xi/kvQHy4Yae0JnTkAOnLX8SBXnbwGKTQG5sFv2DZMGfmOoMUR5pFa68Y8py+HFojZjShNMW7cJ3uEdS
+qE/hkWZ2bAbuWtC1hhUBjRK1LzqkFLk0k+Ju9Tf2Smsuh2yw+SVoSpOf5ui7J3qLs8no1RHBdpvncx4
R7t4k23a2Gx8r8ZzHdDnfhwgdDMi8sdHmaoInZzoyYCpa8fv6xF+ILdtfsmpXz2X
P/CNAU/RBmvLQ4C8SpEtLtDKZwHrkWWdkE9dpHn7UT6HQJrDQe1ask5C6MwYi5vw1OAwV3E4Xbpy3XsXgSwXco/
+AmKBo127rGbai4gwLbsnSLuK+NTci86YhCAt8prGBFtkjG8FWDq7KnxFL5ko6mZ28banGeICc
+wtydLzo/zvICBf6C4KVKAv1UOjd1I+ycxOaLx9dfiq9y1oH0gqw3J1re409IvRg5SOFTSUqxn1wemH37rm6dkLrkkm0Yur
Zn38GgGB19hssB5ASHavTXMHngYmmObroLuSgVk7aIJWX7iYRj9rT1XPpZGXXOV4/ecq6B/DTOJ0RLMu
+6r7eoySrX8n3Af53Md1ZP8e9EG+Kx2Qjs6S7CyjYbR5rLk6
3+jPc7toOP6RcgU7+MmaICw3mFPP17v/GuDKbbye5ctxbUxSt1kVkAfhX9mj3jvfb4Jk2w
+K8892I9oexs9a0Moc5txVSuFBoIypbAszoLI/Pb9mV114cFvhmt0u/wp5
ZGN5/KhwPUHqoTMdzcOQ15RIiHs6vRVGbWN7kiohtsSaD/19up89GPmfw1YxAa7KLQevfx6PkknpjIHOnLATFxf/FHZWY1kH
+Bo5znon/eOE5tugg2h1y6uwO/sPxhBXAGUmvUv1HMRCfWd9KGfK67uaD0Xmx0rDjhNF0HsI6+DapqO220xYAcUwbOwF5MTD
sn8NpwwND2kLMrOpxSTsB6DQI1Qa2axcvaj5y9LXNzM4LIZqC7wNY1JCeXJk3yFY
hUOZy1R0S1ZXcUrbdrHr/wzXczA16L7XjsLa8CE5ZvhPahgsApa3oBXGS8N7OG0mD
+zCm40epRwgEUDEBIGM2qDJgKteYL9tgr6+UDPr4H/8yQvrH8S2wwfO/42RaxMU
RErohFt/mhzNier1+GtTT48VtiZoPUuU8PsnzhUKSHun6SOiM8HqBZjCOn0V6F0XR
+AMMwpLfb0fw3rReCddEILQZL1YpCXD2t0jwPE6xF9BhYBji4R/N/0eMCEUrwJ1
aXyUbaksovDSr8sDkQhFZXn3g37xkQA0wqIgjmzEg8hrK9twsyx8sMPERgZkdamh
ADAvod0xeX4I8jZT5i/q8KJMvsuoEv2Ni19PkYvNtgdgGqTTsXGLLdYMXPfpbne3AV0zrEJwIc7x7P1Nv54MgYtfz
+nqQEX6NF6eNMzcjhDW/YLRrF1+T5vAyD3Owz6Z
T3caASOVwKNKE6JUzwPA1RESQfG1gFaFRW10rBf5Zv6Zc10U17hHITg6//k9xCGHQ70FPteL
+RgUd96Z6jQm1r6u4IA9n1HV2R3ekqsSQiOALnbFUVN0+1KhpPuz6Y4f
oEm8PBrxKZnudg3Hai7fKKMPAMo1BdR8jjoGRSbt9mHVHBuNSpuYjp+bnXNP5Mk9
dwsYTDaUzdm8torX2cmc3xu24CpK1SQYbxzkhrsSYrx1sEXTvxfnYiy5186uroI5IZ
+nkGEjVbAbr1/egx19m2AEYNEnHggmBHrROVi/fknd1jtcvPWYHPLotq7MkIbu
6sfcALAbbiiYDUb5ppC6BvexCz1EbOHEdzOm5r1anVgy6rOX/BE3h1D5DY++rtsF3LfKgnJa9kzH9FrMeZF5Iw==
```

Fig.22. Command message AES CBC encrypted text.

In this method, the plain text is divided into several blocks, and each block is encrypted independently. The key of the encryption is generated from the combination of the outcome of the former block and the AES key.

In Fig. 23, the former AES-CBC encrypted message is decrypted by the AES-CBC key. The key length is 128 bits. The encrypted message is divided into several blocks, and decrypted block by block. One can see the decrypted message is as same as the plaintext.



```
[{"type":100},{"type":0,"staggerRoutes":true,"singleCopterInfos":
[{"latOffset":0.01428472981938711,"lngOffset":0.033740961866442376,"targetAlt":10.0},
{"latOffset":-0.011039127408984939,"lngOffset":0.01824326682408639,"targetAlt":10.0},
{"latOffset":-0.0061094946334421252,"lngOffset":-0.026221580911212072,"targetAlt":10.0}]},
{"type":2,"singleCopterInfos":
[{"latOffset":0.01428472981938711,"lngOffset":0.033740961866442376,"targetAlt":10.0,"centerDirectio
nDeg":0,"radius":1000,"rate":20,"turns":1,"channel3":1500},{"latOffset":-
0.011039127408984939,"lngOffset":0.01824326682408639,"targetAlt":10.0,"centerDirectionDeg":0,"radiu
s":1000,"rate":20,"turns":1,"channel3":1500},{"latOffset":-0.0061094946334421252,"lngOffset":-
0.026221580911212072,"targetAlt":10.0,"centerDirectionDeg":0,"radius":1000,"rate":20,"turns":1,"cha
nnel3":1500}]},{"type":2,"singleCopterInfos":
[{"latOffset":0.01428472981938711,"lngOffset":0.033740961866442376,"targetAlt":10.0,"centerDirectio
nDeg":10,"radius":100000000,"rate":20,"turns":1,"channel3":1500},{"latOffset":-
0.011039127408984939,"lngOffset":0.01824326682408639,"targetAlt":10.0,"centerDirectionDeg":0,"radiu
s":1000,"rate":20,"turns":1,"channel3":1500},{"latOffset":-0.0061094946334421252,"lngOffset":-
0.026221580911212072,"targetAlt":10.0,"centerDirectionDeg":0,"radius":1000,"rate":20,"turns":1,"cha
nnel3":1500}]},
{"type":3,"loiterTimeAttr":0.0,"flashCheck":false,"flashCheckPeriod":1.0,"oneByOneCheck":false,"one
ByOneCheckPeriod":1.0,"flashNameArray":"","flashIndexArray":"","singleCopterInfos":
[{"latOffset":0.01428472981938711,"lngOffset":0.033740961866442376,"targetAlt":10.0},
{"latOffset":-0.011039127408984939,"lngOffset":0.01824326682408639,"targetAlt":10.0},
{"latOffset":-0.0061094946334421252,"lngOffset":-0.026221580911212072,"targetAlt":10.0}]},
{"type":4},{"type":0,"staggerRoutes":true,"singleCopterInfos":
[{"latOffset":0.014326995043226987,"lngOffset":0.033840812614712945,"targetAlt":10.0},
{"latOffset":-0.011093588905644936,"lngOffset":0.018333256658294772,"targetAlt":10.0},
{"latOffset":-0.0061347831363249838,"lngOffset":-0.026330108814093478,"targetAlt":10.0}]}]
```

Fig. 23. Command message AES CBC decrypted text.

C. Heart Beat Message ECCDSA

For the heart beat messages, users can employ the drone's key public-key pair as a signature. The drone's private key encrypts all the messages. This means only the drone's public key can decipher the message, which ensures that the receiver authenticates where the feedback messages came from.

However, this method provides a window for a third party to analyze drone traffic.

If third parties access the drone communication network and have the public key of all the devices in the network, they can read all the feedback messages in the channel. Additionally, because third parties cannot access the private key of any other devices, the third party can hardly modify the heart beat messages for traffic observation.

Because of the limitation of the drone's communication bandwidth, and because the ECC algorithm can provide the same level of security with smaller keys than that of the RSA, ECCDSA protects the feedback messages in the channel much more effectively.

The algorithm for the ECCDSA is same as the ECC algorithm for the key distribution message.

VII. KEY DISTRIBUTION IN THE KEY EXCHANGE LAYER

Earlier chapters have already provided details about the communication structure of aerial robotics and the cryptography used for different kinds of messages. In this chapter, discussion focuses on the keys.

Key exchange in presentation layer can be divided into four types of keys: master, sub-master, channel, and session. These keys are used in different steps in the network. Combining these keys ensures the security of the keys and messages.

In this chapter, the types of keys, the usage of keys, the transformation method, key use frequency, key distribution and key distribution timing are discussed.

A. Master Key

The master key is used to encrypt and decrypt the sub-master key in key transmission. The main ground control station of the wireless communication subnet generates the 128 bits master key. Different sub hosts (devices) in the subnet have their own, individual *master keys*. To synchronize the master key with the main ground control station and other devices, the devices link to the MGCS by wire while it is on the ground; then, the wired channel transfers the key to the device because the wired channel provides better protection for the master keys. A third party who cannot physically access the main ground control station would never get the master key. The master key should be updated annually.

TABLE I.
MASTER KEY.

Type	Algorithm	Payload	Update Frequency
Master Key	ECC	Sub-master Key	Once a year

B. Sub-master Key

The *sub-master key* is used to encrypt and decrypt channel keys and session keys in key transmission. The main ground station of the communication subnet generates the 128-bit sub-master key. Different sub hosts (devices) in the subnet would have their own, individual sub-master key. To synchronize the sub-master key with the MGCS and other devices, the devices should connect to the subnet first. Then the sub-master key, which was encrypted by the master key, will be sent wirelessly. The sub-master key is updated every 20 connections.

TABLE II.
SUB-MASTER KEY.

Type	Algorithm	Payload	Update Frequency
Sub-master Key	ECC	Channel Key Session Key	Every 20 Connection

C. Channel Key

The channel key is combined with the session key to encrypt and decrypt messages in command transmissions. The main ground station of the communication subnet generates the 128-bit channel key. Different sub hosts (devices) in the subnet would have their own, individual channel key. To synchronize the channel key with the

MGCS and other devices, the devices should connect to the subnet first. Then, the channel key, which was encrypted by the sub-master key, is sent wirelessly. The channel key is updated when every connection has been established.

TABLE III.
CHANNEL KEY.

Type	Algorithm	Payload	Update Frequency
Channel Key	AES	Command Message	Every Connection

D. Session Key

The session key is combined with the channel key to encrypt and decrypt messages in the key transmission. The main ground station of the communication subnet generates the 128-bit session key. Different sub hosts (devices) in the subnet would have their own individual session key. To synchronize the session key with the MGCS and other devices, the devices should connect to the subnet first. Then, the session key, which was encrypted by the sub-master key, is sent wirelessly. The session key is updated every 5 min during the connection.

TABLE IV.
SESSION KEY.

Type	Algorithm	Payload	Update Frequency
Session Key	AES	Command Message	5 Minutes During Connection

E. Key Distribution

The master key is used to transfer the sub-master key, the sub-master key is used to transfer the session key channel keys, and different keys are protected layer by layer to reduce potential attack and threat. Details are discussed below.

1) Key Types. Different usages require different types of keys.

As introduced in chapter 6, the ECC algorithm protects key exchange and key distribution messages. Therefore, the master key and the sub-master key have two parts, a public-private key pair for ground control stations and a public-private key pair for drones.

As is introduced in chapter 6, AES protects control messages. In this case, the keys for AES cryptography are separated into session keys and channel keys.

2) Key Distribution. To establish the ECC and AES key distribution in drone communication networks, key exchange is different from that of the internet because in the drone communication network, even in ad hoc mode, drones do not need to share keys with other drones.

In this case, the main ground control station needs to generate public-private key pairs for ECC encryption and session key/channel key for AES encryption, which means MGCS is used as the key distribution center (KDC). Then, the MGCS need to deliver the GCS's public key, the drone's private key and the drone's session key/channel key to every drone individually.

The session key and channel key are delivered separately to the drone, and the MGCS and the drone need to combine these two types of keys into one key for AES cryptography.

F. Key Distribution Timing

The master key is written into the drone first. Then, during communication initialization, the sub-master, the channel and the first session keys are distributed step by step. Later, during a drone flight, new session keys are periodically sent to the drone. Whenever a new session key is delivered, the protocol data unit (PDU) number is reset.

Details are shown in Fig. 24. In this figure, one can see the key distribution in initialization and in the air. All the keys are distributed step by step.

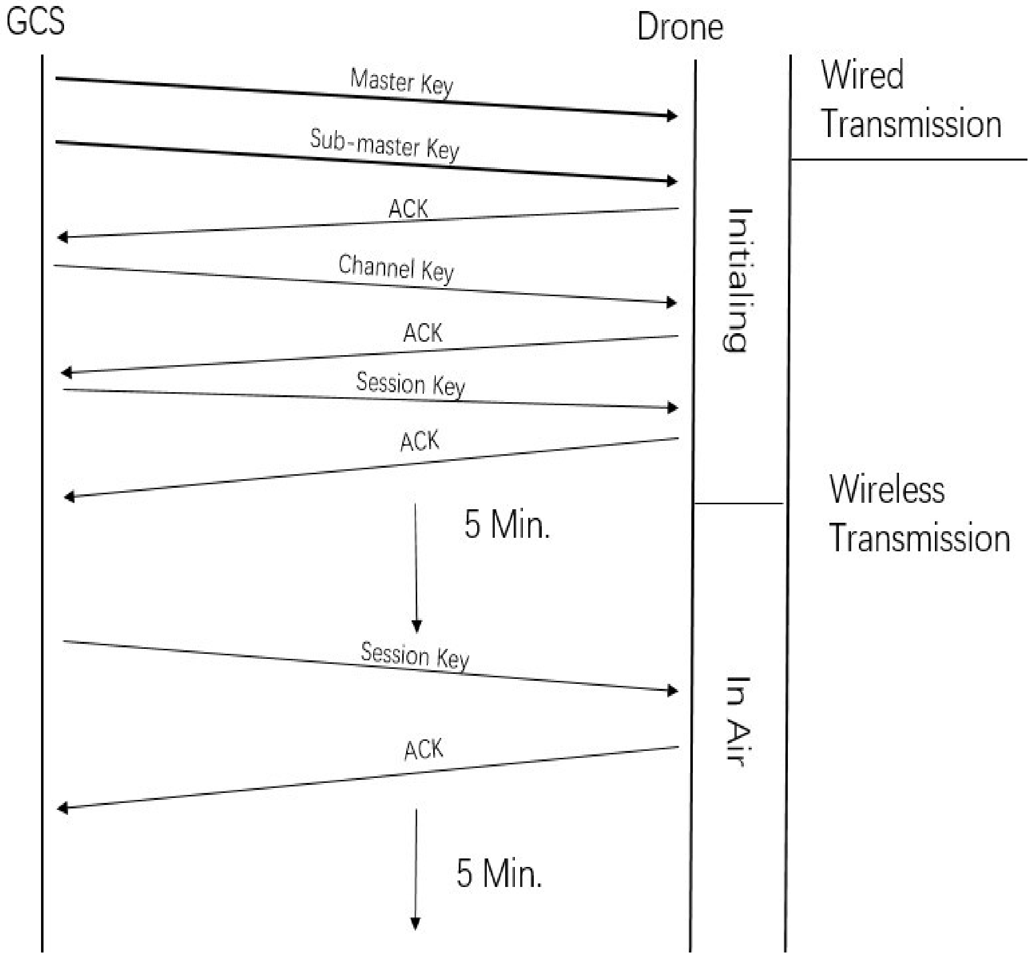


Fig. 24. Key exchange phases.

Analysis: If the session key update frequency rises higher, the encryption for the command message is harder to break. In this scenario, one can select a lighter algorithm to protect command messages. To reduce the complexity of the cryptography computing, one simply needs to ensure that the encryption is not penetrated in one session.

VIII. SUMMARY AND CONCLUSION

In this thesis, a presumed aerial robotics communication network was established, which includes the network structure, communication message types, authentication and security methods.

The goal of the proposed communication solution was to improve the current drone communications, extend the communication distance, enlarge the communication network, and enable more devices access to a same communication channel. This communication framework allows a third party to access information about the state of the flying feedback status information, supervise flying details to ensure communication security, and prevent aerial robotics devices from hacking and attack.

Through the exploration in this thesis, I established a more considerate communication structure that can be deployed on network, transport, and presentation layers; all of which can be used in digital signal aerial robotics and ground control stations. Then, depending on the nature of the drone's wireless communication, I proposed a key distribution structure that can help to ensure the security of aerial communications. Finally, I selected the cryptography for each message type that fits the given communication network best.

This thesis merely begins the consideration of the security of aerial robotics communication that will become increasingly vital to the military, to businesses, and to consumers in the future.

IX. FUTURE DIRECTIONS

The current aerial robotics communication solution has been improved by this proposed security system. Still, several insufficiencies can be improved in the future.

1. Communication Structure. First, the structure of the aerial communication system is achieved as a Wi-Fi and IP protocol, but the communication methods in consumer and commercial drones vary. In the future, a communication protocol should be established in network and the application layer that can be deployed on all current communication methods.

2. Communication Streaming for Manual Control. In the proposed communication network, messages are transferred as packages. The proposed network can ensure the security of key distribution and auto control messages and prevent messages from package loss. But, for control signals under manual mode, packaged messages lead to longer delays. In this scenario, control commands will reduce the delay in the channel by streaming. (e.g., cryptography for PWM or PAM constant signal).

3. Routing. As described in the paper, network structures can vary. In the drone's ad hoc network, the routing table will be updated frequently. Because aerial devices are so active, the physical structure of the network will change from time to time. In this case, the hand shake and routing algorithms can rely on the drone's moving schedule. In this scenario, the drone could fly out of communication range and lose the connection.

4. Video Streaming. In this paper, the proposed security system does not address video streaming messages in the drone communication channel. In the future, if drones fly out of the visual range from the ground control station but the drone needs to finish some projects that need visual analysis, real-time video streaming will be

necessary. Transferring video streaming messages with shorter delays should be a concern in the future.

5. Cryptography. As introduced in this thesis, because the duration of the aerial communication channel is largely shorter than that of the internet, security methods for the internet could be too complex for use. In the future, easier cryptography should be designed to fit special scenarios.

6. Observation on Traffic. Although in the proposed security system the drone's private key encrypts the feedback massages, every device that has the public key can read the feedback messages. The task could be too complex when a user needs to observe several channels simultaneously. Such details need to be explored in the future.

7. Combined Authentication Method. In the proposed security system, every device has its own in-net ID. Relating the ID of the drone to owner's ID would be helpful to UAV organization. For example, if a drone's ID is generated from an owner's FAA ID code, or if the drone has a unique ID to pair with the owner's ID, the government might find it easier to determine responsibility.

8. Data Security. In this paper, the issue of saving and protecting sensitive information in the drone or in the ground control station has not yet arisen. More effort is needed in this area because solving such problems is necessary for the entire system to work efficiently, effectively, and flexibly.

REFERENCES

[1] OpenSSL Foundation, I. (2017, Nov. 1). *Openssl.org* [online]. Available: http://www.openssl.org

[2] W. Stallings, *Cryptography and network security*, 6th ed. Boston: Pearson, 2014, pp. 61-313.

[3] En.wikipedia.org. (2017, Nov. 1). *Wired Equivalent Privacy* [online] Available: https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

[4] En.wikipedia.org. (2017, Nov. 1). *Temporal Key Integrity Protocol* [online] Available: https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol

[5] En.wikipedia.org. (2017, Nov. 1). *Wi-Fi Protected Access* [online] Available: https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#WPA2

[6] Tools.ietf.org. (2017, Nov. 1). *RFC 4949 - Internet Security Glossary (2nd ed.)* [online] Available : https://tools.ietf.org/html/rfc4949

[7] Qgroundcontrol.org. (2017, Nov. 1). *MAVLink Micro Air Vehicle Communication Protocol - QGroundControl GCS* [online] Available: http://qgroundcontrol.org/mavlink/start

[8] F. Fahroo *et al.*, *Recent advances in research on unmanned aerial vehicles*. Berlin Heidelberg, German: Springer, 2013, pp. 181-205.

[9] C. Rani *et al.*, “Security of unmanned aerial vehicle systems against cyber-physical attacks,” *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, vol. 13, no. 3, pp.331-342, 2016.

[10] K. Valavanis, *Handbook of unmanned aerial vehicles*. Dordrecht: Springer, 2015, pp. 347-380.

[11] T. Monitor. (2017, Nov. 1). *Exclusive: Iran hijacked US drone, says Iranian engineer* [online]. Available: https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer