SAPIENZA
UNIVERSITÀ DI ROMA

Swarm Based Mobile Quantum Network

Master INTERFACOLTÀ ICI - I3S
INGEGNERIA CIVILE INDUSTRIALE E
INGEGNERIA DELL' INFORMAZIONE INFORMATICA E STATISTICA
in Optics & Quantum Information

Vittorio Calligaris
Matricola 1931563

Relatore
Ch.mo Prof. Fabio Antonio Bovino

A.A. 2019-2020

The fiercest serpent may be overcome by a swarm of ants

Isoroku Yamamoto

Abstract

This thesis aims to propose a possible solution to generate and distribute secure keys between users spread over a wide area via a Swarm Based Mobile Quantum Network. In the first chapter, we will give an insight over the drone swarm technology focusing particularly on military application and security issues. In the second chapter, after an overview on cryptography, we will spend a few pages to explain the basic concepts of quantum physics and Quantum Key Distribution (QKD) with particular focus on quantum networks. In the third chapter, we will propose a swarm system capable of distributing secure keys via QKD. We will describe both the architecture and the components of the proposed system, we will estimate performances and compare them with other solutions for realizing QKD over a wide area. In the last chapter, we will give an overview over possible application over satellite constellations.

Acknowledgments

I am grateful to AFCEA capitolo di Roma for the opportunity to attend this Master and expand my professionality in a completely new field.

I would like to express my very great appreciation to Prof. Fabio Antonio Bovino who lectured the major part of the lessons of the Master with passion and dedication and is the advisor for this thesis. He is a real example of excellence and dedication to the research.

I would like to thank all the colleagues of Reparto Sperimentale di Volo and particularly of Gruppo Tecnico for all the support given in this year. I am thankful to the Aeronautica Militare for the opportunities that offers me every day.

Finally, I thank my family, Roberto Milena and Serena for everything you have taught me since I was a child.

List of Figures

List of Tables

Index

Introduction

Technology advancement in autonomous flight had led to the emergence of Swarms of Unmanned Aerial Vehicles (UAVs) or drones as potential new weapon and their use is under valuation for many critical mission as reconnaissance, electronic warfare and strike. Swarms have many benefits when compared with a single standalone large UAV, in fact a swarm can perform tasks in smarter ways, optimizing aspect that with one drone are simply not possible, such as simultaneously covering large areas or utilizing some elements as a relay to access area with no coverage from the Ground Station. Swarms of UAVs can be completely autonomous or controlled by a remote location, in both cases communication between the elements of the swarm is one of the key element of the swarm behavior and network managing is one of the main problems in the design of a swarm. Networking aspects are also worsen by the little computational power available on small drones that are usually employed in swarms and by the fact that, if not properly managed, the number of messages exchanged between elements of a swarm grows exponentially with the number of UAVs. Cryptography is the science that study how to provide privacy, authentication and confidentiality to users, in this case to the members of the swarm. Picture in the security field changed drastically from the ‘80s when Bennet and Brassard proposed a solution to the key distribution problem based on quantum physic. Quantum Key Distribution (QKD) is a technology that exploit laws of quantum physics for the generation and distribution of encryption keys. At the opposite of traditional encryption, that bases its security on the privacy of the keys and on the computational unfeasibility of the decryption without the keys, QKD bases its security on unbreakable physical laws, no matter the computational power available. In this thesis, after a discussion about the potentiality of drone swarms and Quantum Key Distribution, we will propose a possible solution to establish a secure communication between a command center and many users spread on a wide area via a mobile quantum network. The network will employ drones as nodes and will include a space segment in order to connect the command center with an oversea scenario.

1. Drone SWARMS

1.1. Introduction to Swarms

Advancements in mechanics, semiconductors, batteries, sensor and artificial intelligence made possible giant advancements in drone technology and what was just a hobby is projected to be a 63 Billion Dollar market in 2025 with well-established application in almost every economic sector from agriculture to national security (Businessinsider 2021). Last trends in research shifted in applications with a large number of drones that collaborate on a common goal showing a swarming behavior. Such concept appears in the animal kingdom long before it does in human affairs. Although human built swarms cannot be precisely modeled after swarm of insects of other animals, some useful lessons and insights may be drawn from the nature. (Arqiulla e Ronfeldt 2000). Examples swarming behavior can be observed in many insects but also in colonies of bacteria. A key element in all nature swarms is achieving a notable effect by the decentralized action of many simple agents. Another vital element in swarming is the self-organization and the swarm intelligence that emerge on a global scale from the local interactions among individuals that have no or little knowledge over the entire pictures. Natural swarms also typically are scalable, robust and flexible. Main advantages of both nature and robot swarms are the intrinsic parallelism in doing task, distributed sensing and distributed action, fault tolerance and enablement of task that a single agent simply cannot accomplish. (Ilachinski 2017).

Figure 1 – A swarm of ants attacks a snake

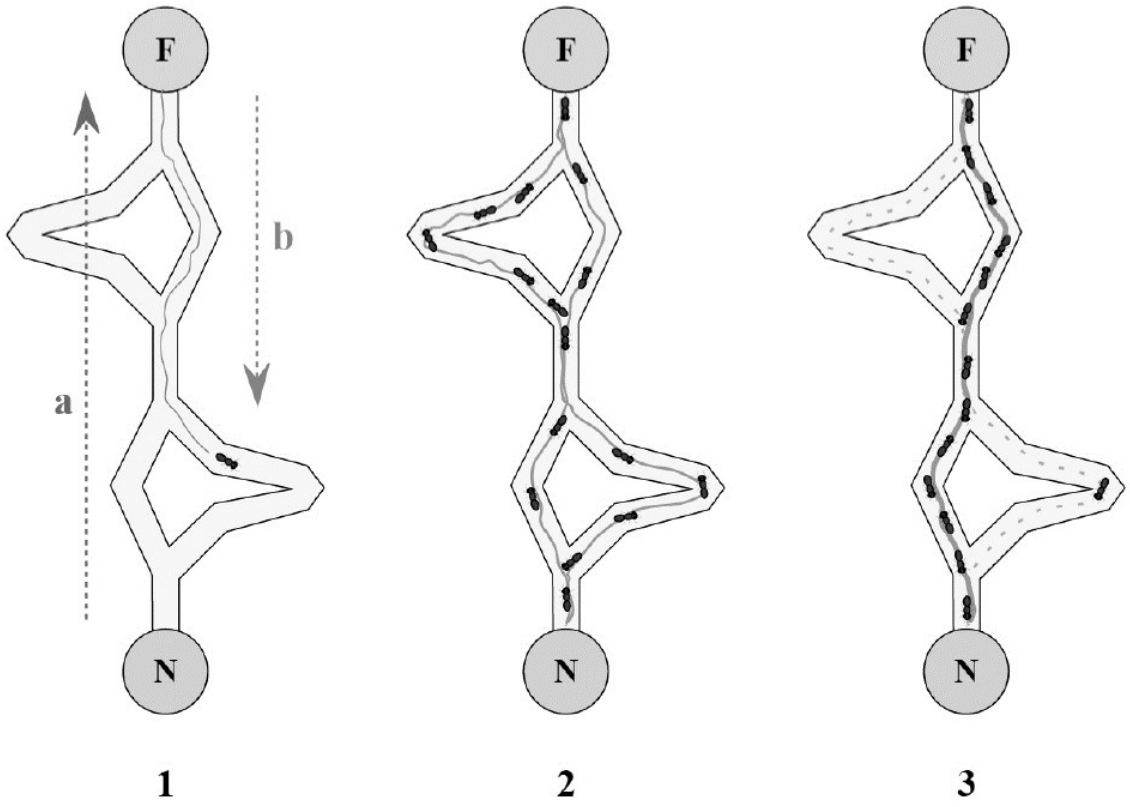

Figure 2 - Ant Colony Optimization Algorithm is an example of swarm intelligence: although single ants do not know the entire map of the colony, the swarm is still able to find the shortest path between the Nest (N) and the Food (F) (Ilachinski 2017)

1.2. Military Application of Drone Swarms

Swarming is a well-known warfare doctrine and many examples can be found throughout history, from the Ancient Greece to the Second World War and beyond. Techniques and weapons changed many times in the history of warfare but the basic concept of swarming remained the same. John Arquilla and David Ronfeldt well define the swarming concept in their work *Swarming & The Future of Conflict*: "*Swarming is seemingly amorphous, but it is a deliberately structured, coordinated, strategic way to strike from all directions, by means of a sustainable pulsing of force and/or fire, close-in as well as from stand-off positions*" (John Arquilla, 2000). In the information age, the advancement in autonomous navigation and the substantial drop in cost of small drones, made possible to apply the swarm concept to group of small Unmanned Air Vehicles (UAVs) or simply drones. Such devices equipped with various type of payload are capable of accomplish many type of mission with the redundancy and

resiliency that only swarming technique can deliver. In nature, swarms can vary from few elements to millions however, also the most cutting edge technology applications are limited to few hundreds of UAV.

Swarming drones can be effectively employed in three main area: attack, defense and support. The first is easy to understand and is implicit in Arquilla definition: a swarm can very quickly outnumber or saturate enemy defenses, guaranteeing that at least some elements hit the target. Swarming is also useful for defensive purposes: a swarm of drones can act as distributed decoy and mask the real target. Lastly swarming drones can be used for recognition mission, providing a wider area coverage, increased persistence and resilience when compared to a single ISR platform (Lachow 2017). Other advantages are the ability to reach areas with little or no coverage from the GCS utilizing some drones as relay, the ability to perform multiple task at the same time and the smaller RCS offered by a swarm of small drone compared to a single big drone. Small drones can also be cheaply mass-produced resulting less expensive than a single drone (Akram, et al. 2017). Lastly swarming drones will have a very strong psychological effect on the enemy whose defense are not prepared for this kind of threat (Cevik, et al. 2012). Some cases of study from this three area are detailed in the following paragraph. Since some of the most important benefits of swarms are lost when large UAV are involved, we will concentrate on UAV of SMALL category and lighter (below 150kg).

1.2.1. Intelligence surveillance recognize

Intelligence Surveillance and Recognition (ISR) is the integrated process of acquisition, processing and dissemination of intelligence information to support current and future operations. UAVs with their low operational cost and long persistence over the operation area when compared to manned aircraft already have revolutionized this kind of mission making possible monitoring high value targets for long periods. Strategic UAVs, such as the Global Hawk and Predator, had a so widely operative success that become part of the collective imagination and are well represented in the media. However, information from this type of platform are mainly used for strategical purposes and are rarely available to frontline troops. Smaller, platoon level UAV like the RQ-7 Shadow try to overcome this problem but still have some logistical requirement (like a catapult for the launch, a safe area for the ground station far

from the frontline etc.) that prevent them to be instantaneously available on target. In this framework a swarm of small, hand launchable drones can provide a greater area coverage and a shorter time to relocate on the point of interest with very little or no logistic requirements in addition to all the previously discussed benefits in terms of survivability and low operating cost that a swarm have. It could be shown that the minimum time to cover an area A_S with a swarm of N UAVs equipped with a sensor of footprint radius R_f is:

$$t_{min} = \frac{A_s - A_i}{2R_f V_n N_a} E$$

Where V_n is the velocity of the UAVs and A_i is the area observed at $t = 0$, usually $A_i = N_a 2\pi {R_f}^2$ and $E < 1$ is the efficiency of the swarm in performing the surveillance task, experimental result shown a typical efficiency of 60% (Garcia-Aunon, Cerro e Barrientos 2019). Now, as an example of swarm potential in ISR missions, let consider a comparison of the Boeing Scan Eagle (25kg SMALL class) and a swarm of 10 DJI Phantom (1,4kg MICRO class) patrolling an area of 5x5km:

UAV	*FOV (deg)*	*Resolution (px)*	*Altitude (m)*	*m/px*	*Speed (m/s)*
ScanEagle (Insitu 2021)	1.5	720	3000	0.1	30
DJI Phantom (DJI 2021)	27	1080	250	0.1	10

Table 1 – Phantom – ScanEagle comparison table

Where operative altitude of the two UAV is chosen to match performance of the two sensors at a resolution of 10 cm per pixel. With this parameter we obtain a t_{min} of 18 min for the swarm and 171 min for the ScanEagle. As expected the employment of 10 drones cut the time approximately of an order of magnitude, however at the same time the cost dropped form 3,2 million of ScanEagle system (US Air Force 2011) to 16.000 dollars of 10 DJI Phantom drones (DJI 2021). Although this comparison is just a pen and paper example and do not consider many aspects, such as the possibility to steer the sensor (the formula consider a fixed camera), the 30min autonomy of the DJIs versus the 4h+ autonomy of the ScanEagle, the different EO

sensor, the different cost of commercial and military grade hardware etc., it well illustrate the benefits of employing a swarm of UAV for ISR missions.

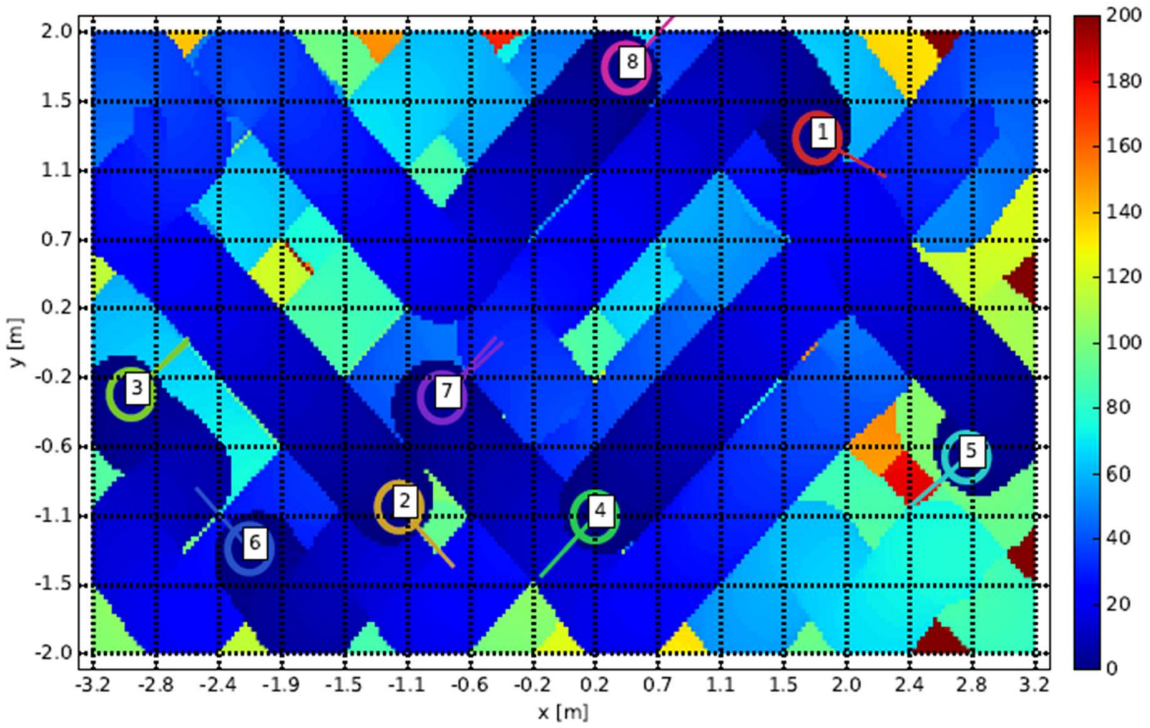

Figure 3 - Example of surveillance mission with 8 drones and a nominal speed of 0.10 m/s after 300 s. The colored background represents the age of each cell. (Garcia-Aunon, Cerro e Barrientos 2019)

1.2.2. Decoys

Decoys are passive or active devices that are designed to look like real targets to enemy radars. They implement the deception tactic, offering to the enemy realistic alternative targets with the scope to hide the real target between the false ones or to mask the real target with a bigger one. Decoys can be towed, expendable or independent maneuvering drones (Stimson, et al. 2014), in this section we will concentrate on the last ones.

The first operational example of a decoy drone was the McDonnell-Douglas ADM-20 Quail. Quail, operational in 1960, was an air-launched decoy carried by the Boing B-52 Stratofortess that could replicate its radar image. The decoy was able to fly at Mach 0.9 for 445 nautical miles releasing chaff and flare and making turns and speed change to further confuse enemy radars. Soviets became capable of distinguishing the ADM-20 from B-52 as early as 1969, ending its operational history (Erdemli, Fisher e Baer 2009).

Figure 4 - ADM-20 Quail (Erdemli, Fisher e Baer 2009)

Although Quail operation history was only 9 years long, his inheritors like the Raytheon Miniature Air-Launched Decoy (MALD) ADM-160 are still in service. In 2011 Raytheon demonstrated the capability to launch multiple MADL from the cargo bay of a C-130. This technique opens the possibility to deliver hundreds of MALD to the battlefield with a single high capacity cargo plane (Raytheon Missiles and Defense 2011). This in turn will give the ability to overwhelm enemy air defense with hundreds of false targets. In an operational contest, a swarm of MALD will precede the attacking package in enemy territory, obliging SAM sites to turn on radar and come out, as well as to waste precious missiles (Raytheon Missiles and Defense 2021).

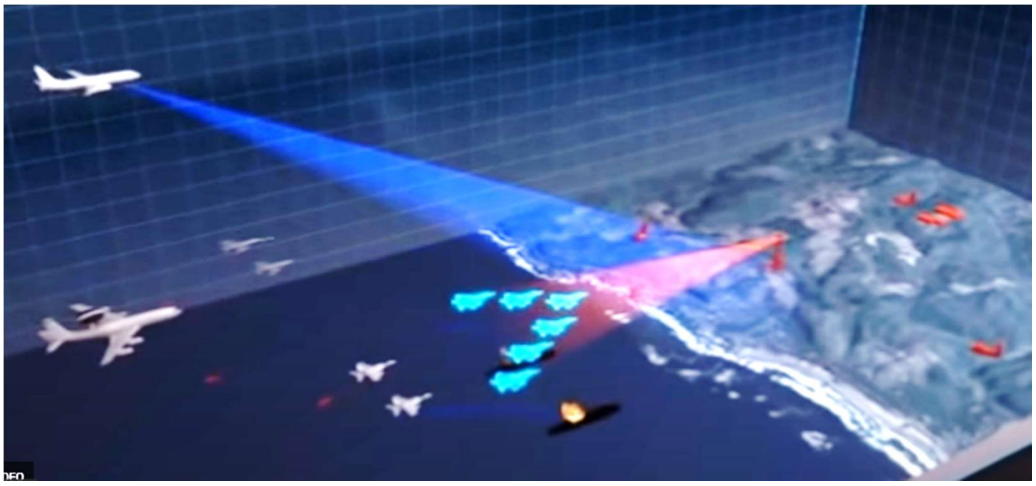

Figure 5 - A Swarm of MADL preceding an offensive package (Raytheon Missiles and Defense 2021)

A similar idea was explored in June 2021 by the Italian Fly Test wing and University Federico II di Napoli that successfully demonstrated the possibility to mask an ally drone with a swarm of three decoy drones [Figure 6]. The experiment was conducted with a swarm of mini category drones equipped with corner reflectors and a 24GHz Radar. The three decoy drones were flown between the radar and the allied drone in order to offer a strong return to the radar and hide the real target. The experiment demonstrate the concept and further development of the project will scale the system to bigger drones in order to mask a full size aircrafts (Verini Supplizi, et al. 2021).

Figure 6 – Swarm activity at Italian Flight Test Wing – A swarm of three mini-class decoy drones (1) mask an allied drone (2) from a 24GHz radar (3) (Verini Supplizi, et al. 2021)

1.2.3. Electronic Attack & Jamming

Electronic Attack missions aim to reduce the effectiveness of hostile radars by the use of the electromagnetic radiation (Jamming, High Power Radiation) or by physical action (Anti-Radiation Missiles). Jamming is the transmission of undesired signals into enemy receivers to disrupt his ability to correctly process target signals (Stimson, et al. 2014). The advantages of a swarm in a jamming mission derive from the ability of the swarm to act as a distributed source of noise, making impossible locate the source of noise. At the same time, the small RCS of the

drones allows to fly very close to the radar site undetected. This in turn has a very beneficial effect and overcome one of the most critical downside of standoff jamming: power, in fact power needed to effectively jam the radar follow square law of distance and could be prohibitive if the jamming platform is far from the radar site. At the opposite, drones transmitting very close to the victim radar and spreading the necessary power among the swarm are able to accomplish a EA mission also with very little power available (in the order of 100mW) (Cevik, et al. 2012).

Let now determinate the power needed to successfully jam a radar and hide an allied platform at R_{TG} from the radar. Power received at radar from target is:

$$S = \frac{P_R G_R \sigma}{(4\pi)^2 R_{TG}^4} A_{eff}$$

Where P_R, G_R, A_{eff} and σ are respectively the transmitted power of the radar, its gain and effective area and the radar cross section of the target. At the same time power received at radar from jammer is:

$$J = \frac{P_j G_j}{4\pi R_j^2} \cdot \frac{B_{IF}}{B_j} A_{eff}$$

Where B_{IF} and B_j are the bandwidth of the intermediate filter of the radar and of the jammer. If the bandwidth of the jammer perfectly match the bandwidth of the IF, the jam to signal ratio is:

$$\frac{J}{S} = \frac{P_j G_j 4\pi R_{TG}^4}{P_R G_R \sigma R_j^2}$$

Now if $\left(J/S\right)_{req}$ is the jam to signal ratio needed to jam effectively the radar, the power needed from the jammer is:

$$P_j = \frac{P_R G_R \sigma R_j^2}{G_j 4\pi R_{TG}^4} \left(J/S\right)_{req}$$

Alternatively, explicating the R_{TG}, known also as burn through range, that is the minimum distance that the allied platform can reach from the radar remaining undetected:

$$R_{BT} = \sqrt[4]{\frac{P_R G_R \sigma R_j^2}{P_j G_j 4\pi}\left(J/S\right)_{req}} = \sqrt[4]{\frac{ERP_R \sigma R_j^2}{ERP_j 4\pi}\left(J/S\right)_{req}}$$

Where it was assumed that the jammer is transmitting into the main lobe of the radar. If it is not true, the ratio between the main lobe gain and the side lobe gain must be considered (Stimson, et al. 2014):

$$R_{BT} = \sqrt[4]{\frac{ERP_R \sigma R_j^2}{ERP_j 4\pi}\left(J/S\right)_{req}\frac{G_m}{G_s}}$$

Now as an example consider a radar with an Effective Radiated Power of 10MW and a swarm of 10 elements equipped with 100mW ERP jammer that navigate undetected until 9Km (5nm) from the enemy radar trying to hide a 10sqm target with a 20dB J/S ratio. Side lobe isolation $(G_m/G_s): 50db$. The burn through range is:

$$R_{TG} = \sqrt[4]{\frac{ERP_R \sigma R_j^2}{N \cdot ERP_j 4\pi}\left(J/S\right)_{req}\frac{G_m}{G_s}}$$

$$R_{TG} = \sqrt[4]{\frac{10MW \cdot 10m^2 \cdot (9km)^2}{10 \cdot 0.1W \cdot 4\pi} \cdot 100 \cdot 100000}$$

$$R_{TG} = 22.5km \sim 12nm$$

That means that an allied aircraft can approach the enemy radar up to 12nm, allowing it to use its armament while remaining undetected and shows the huge potential that also a Swarm of small, low power drones has for an EA mission.

The concept of employing a swarm of drones for EA can be effectively realized as the Royal Air Force (RAF) successfully demonstrated in 2020. During the 2020 demonstration, RAF equipped a swarm a fixed wing drones with modified Leonardo BriteCloud expendable active decoys and performed an Electronic Attack mission against a hostile radar. The BriteCloud

was initially developed as countermeasure for manned aircraft against modern radar guided missile. The decoy, that have the same dimension of a standard chaff and can be deployed with a standard chaff dispenser, was modified in order to be employed on a swarm of drones that collaborate to produce the maximum effect of the enemy radar (Leonardo 2020).

Figure 7 - Swarm of Drones equipped with Britecloud Active Decoy (Leonardo 2020)

1.2.4. CAS - Loitering munitions

A loitering munition, also known as kamikaze drone is a special type of drone with a built-in warhead that once launched can loiter in the target area until the target is precisely located. This type of drones was initially developed for Suppression of Enemy Air Defense (SEAD) missions. In fact, modern mobile SAM sites usually emit just for a brief period, not sufficient for a standard engagement. Loitering munition can simply wait in the target area and hit when the radar is activated. However is in the Close Air Support (CAS) role that loitering munition expressed their maximum potential. Many modern weapons of this class are managed directly from infantry that can now dispose of instant on-demand precision strikes. As an example AeroVironment Switchblade 300 is a loitering munition that weighting just 2,5 Kg can be backpacked and launched by the troops on patrol [Figure 8]. This aspect should not be undervalued, in fact it means that the entire expensive infrastructure that support a classical

UAV (an airstrip or at least a catapult in a safe area) is avoided and the drone is instantly available after launch without having to fly to the battlefield. Switchblade dispose of its own suite of sensor for the identification of the target and with a range of 10km and 15min of autonomy is capable of delivering a high value support to ground troops. It has been deployed with success and great appreciation by troops in large numbers in Afghanistan (Scharre 2014). To follow up this trend, on November the 17th 2020 the USMC released a request for Information (RFI) for the so called "Organic Precision Fires - Infantry Light" program that will substitute the Switchblade in the next years. The program is seeking the next generation loitering munition for the Marines and the swarming capability is explicitly mentioned in the requirement (US Department of Defense 2020), making clear that head of the Marines Corp has well understood the potential of having a swarm of loitering munition persistently over the battlefield.

Another proposed loitering munition is the Defendtex Drone 40. This small drone has the dimensions of a standard 40mm grenade and can be deployed by troops with a grenade launcher or by hand without any additional support [Figure 9]. The munition is natively capable of operating in swarm (Defendtex 2021). A swarm of this type could hit in a matter of second any target with a force that can vary from a single drone to the entire swarm providing at the same time a real time picture of the entire battlefield.

Figure 8 - Switchblade launch (AeroVironment 2021)

Figure 9 – Defendtex Drone40 (Defendtex 2021)

1.3. Architectures

Swarms can be classified by two main paradigms, the ability of the swarm of accepting a new member and the architecture of the control logic. In the first classification, swarms can be divided in:

- **static**, if the members of the swarm are predefined in the mission planning stage and are there is no possibility to add a new member in flight, for its simplicity it is the most used configuration;
- **dynamic**, if the swarm can include new members at any moment during the mission. The new drones could not be limited to drones of the same organization and could also be third party drones. This solution open an entire new class of problems about the identification and the trustiness of the new drones;
- **hybrid**, if there is a static core swarm that cannot be modified in flight but new drones are allowed to join the swarm with less privileges and priority than the core drones (Akram, et al. 2017).

At the same time swarm can by classified by the control logic, the main model are:

- **Centralized**, if there is a master drone that collect all the data from the swarm, make decision and assign tasks. Benefits of this architecture are that the master drone has a complete situation awareness of the scenario and can make decision with the maximum amount of information available. At the same time, this configuration require constant communication of all the members with the master drone that could be quickly become a bottleneck for the network or be limited by its computational power. This translate in a very poorly scalable system. Of course in this architecture the master drone is a single point of failure is highly vulnerable both to attack and malfunctions (Barca e Sekercioglu 2013);
- **Hierarchical**, if the members of the swarm are divided in small groups each of them with a local master drone that make some decision, collect and synthetize data but still receive order from a superior level drone. This reduce the workload of the master drone and is more scalable than the centralized architecture but still present the vulnerabilities of a structure completely dependent from a very little number of master drones;

- **Distributed**, if the drones are organized in a peer to peer logic without a central drone. This reduce the computational complexity associated with a centralized system making the swarm intrinsically parallel and more scalable. At the same time the system have a very little sensitivity to the loss of any of the members eliminating the dependency from the master. The main disadvantage of a distributed system is the inability of a generic member to access at the entire data set available, limiting its decisional power. Another problem is that the self-organization of the swarm could be difficult to predict and can lead to local persistent oscillation of the members that translate in a waste of energy (Barca e Sekercioglu 2013);
- **Hybrid**, any combination of the three options above, as an example a distributed swarm core with a second level of smaller drones at the direct dependency of the core drones. Currently many of leading edge swarm use a hybrid approach, combining benefits both centralized and distributed architectures (Rinaldi, et al. 2020).

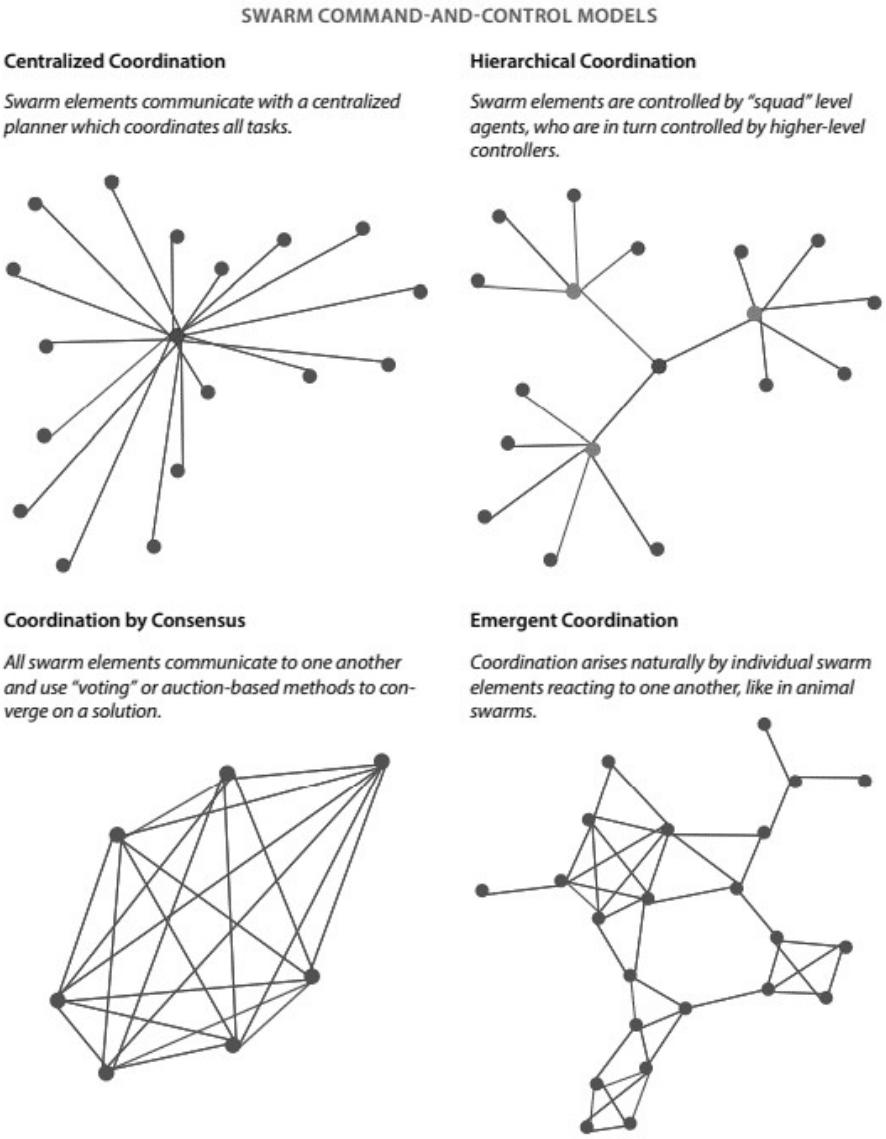

Figure 10 - Swarm Architectures - (Scharre 2014)

1.4. Communication and Security threats

Employing drone swarms in critical mission create the need to establish a secure communication between the members of the swarm. Peculiarity of swarms also make more critical the generic security issues that are present also in a classical single-drone mission. In a swarm the number of messages, a so the possibility of a breach, is many time higher than in a single-drone system. In fact a single drone can navigate autonomously and make just brief communications with the ground station, limiting the probability of been intercepted. On the other side, members of a swarm need high frequency communications to coordinate and

perform their tasks. At the same time, drones implied in swarms are much smaller and cheaper than standalone drones, and this put serous constraints on the computational power available.

Elements of a swarm form a network that can be easily modelled as a Mobile Ad-hoc NETwork (MANET) or as a Wireless Sensor Network (WSN) (Rinaldi, et al. 2020). In the swarm's network, as in all wireless network, each node receive all packets in its range and due this fundamental intrinsic characteristic, each node can easily gain access to all the packets or inject malicious packets in the network. For this reason defense against malicious nodes is the base of security in MANETS (Dorri, Kamel and kheyrkhah 2015). It easy to think that drone swarms are immune to this attack since the relatively low power of the infra-swarm communication provide a kind of protection against attacks. However, a malicious node could be an attacking drone that tries to join the swarm or a previously infected drone of the swarm.

There are three key concepts at the very fundamental of information security and they form the so-called CIA triad: Confidentiality, Integrity and Availability. Confidentiality involves preserving information from unauthorized access; Integrity regards protection against modification or destruction of information and Availability ensure reliable access to the information (Stallings 2011). In the swarm context Availability means that only authorized drones of the swarm can have access to the communication, Integrity means that member of the swarm trust each other and the information is not modified or corrupted by an external agent, lastly Availability means that the drones are able to communicate also in a noisy or electromagnetically non-permissive environment.

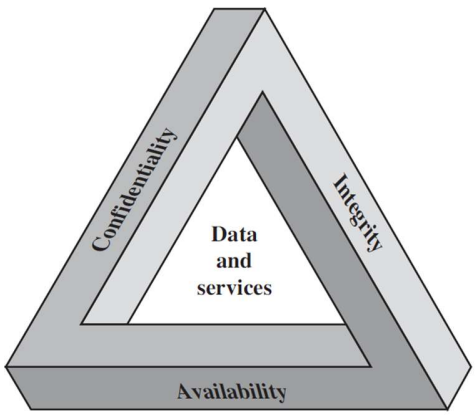

Figure 11 - CIA Triad (Stallings 2011)

2. Quantum Key Distribution

Quantum Key Distribution is a possible solution to the key distribution problem of all crypto system. In fact, classical cryptosystems rely their security upon the secrecy of the keys and on the computational security of the crypto algorithm. Quantum key distribution exploits laws of quantum physic in order to obtain pairs of identical keys at the two endpoint of the communication channel. Laws of physics guarantee that the key is a true random string and that an eavesdropper cannot get any information about the key without being detected. At the same time, the availability of large keys enables the use of mathematically secure crypto algorithms. In this chapter we will give an overview over classical cryptography in order to introduce quantum key distribution discussed in section 2.2. In section 2.3 we will discuss devices involved in QKD and finally we will spend few pages on QKD networks in section 2.4.

2.1. Classical Cryptography

Cryptography is the science that provide privacy, authentication and confidentially in storage or transmission to users. In addition, cryptography provide other important functions as signature and non-repudiation. This section aims to introduce classical cryptography, focusing particularly on the areas that are relevant to quantum cryptography.

2.1.1. Crypto Systems

Three elements compose a classical communication system: the message, the sender and the receiver, usually referred as Alice and Bob (A and B). The message is coded and then it is sent though a physical communication channel, like the air or a fiber optic. The communication channel is considered insecure, in fact, it can be object to attacks from an Eavesdropper. To guarantee the confidentiality of the message the plain text is encrypted with a key and an encryption algorithm to obtain the cipher text. To ensure the security of the message the algorithm could be public but only the sender and the receiver must know the key. If the key for the encryption and decryption is the same the algorithm is called symmetric, in the opposite case is called asymmetric (F. A. Bovino 2014).

A generic cryptography system is defined as the quintuplet $(P; C; K; e_K; d_K)$ where:

P is the set of the possible plain text symbols;

C Is the set of the possible cypher text symbols;

K is the space of the keys;

$e_K: P \rightarrow C$ is the encryption function;

$d_K: C \rightarrow P$ is the decryption function;

And where $d_K\big(e_K(m)\big) = m \quad \forall\, m \in P$. The system works as following:

1. Alice and Bob chose and share a random key $k \in K$;
2. Alice create the message m composed by a series of symbols $m_i \in P$ and apply the encryption algorithm e_K to every symbol m_i obtaining the cypher message y composed by the symbols: $y_i = e_K(m_i)$.
3. The cypher message is now set to Bob thought a public channel;
4. Bob receive the cypher message y, apply the decryption algorithm to every symbol $m_i = d_K(y_i)$ an obtain the original message m.

It should be noticed that if P and C are the same, the encryption algorithm is a permutation and if e_K and d_K are the same, the algorithm is called symmetric. In order to be practical the quintuplet $(P; C; K; e_K; d_K)$ must respect the following conditions: the encryption and decryption functions e_K and d_K shall be computable efficiently but an Eavesdropper shall not be capable to determinate k from the cypher message y. A common assumption is that e_K and d_K are public and known by the Eavesdropper (F. A. Bovino 2014).

2.1.2. One Time Pad

Cryptography systems are classified in:

- Perfect, if they are mathematically secure;
- Computationally secure, if they are not mathematically secure but the crypto problem is analytically unfeasible;
- Conditionally Secure, if they are mathematically secure only if specific condition are verified.

Information Theory define a perfect crypto system as a system where the knowledge of the cypher text add no info about the plain text. In mathematical terms, this means that the cypher text and the plain text are two independent aleatory variables. With this definition it is possible to demonstrate that exist only one crypto system perfectly secure and it is called One Time Pad (OTP) or Vernam Cypher. In this system the key is as long as the message, it is perfectly aleatory and, as the name suggest, it is used only one time. If the message and the key are two Boolean strings the encryption and decryption function are just an XOR between the message and the key:

$$y = e_K(m) = m \oplus k$$

$$m = d_K(y) = y \oplus k$$

With this system the communication of message is perfectly secure and the cypher text could be sent on a public channel. Anyway the problem is now shifted from the transmission of the message to the generation and distribution of an equally length key that must be periodically shared between Alice and Bob (F. A. Bovino 2014).

2.1.3. Public Key System

As seen in the previous paragraph the main problem of OTP and all private key encryptions is the communication of the key that must be secure in order to guarantee the privacy of the communication. In order to achieve this it is not unusual physically transfer the key from Alice to Bob and vice versa. Public key system overcome this problem by using two different keys for encryption and decryption. Making public the encryption key, everyone can use it to cypher the message and be sure that only the legitimate receiver is able to decrypt it. In addition, if the public key can also be used to decrypt a message encrypted with the private one, it is possible to authenticate the sender. Now let be E_k, D_k the encryption and decryption functions and k_s and k_p the secret and public key with the following propriety:

$$\forall m \in P \quad D_{k_s}\left(E_{k_p}(m)\right) = m$$

$$\forall m \in P \quad D_{k_p}\left(E_{k_s}(m)\right) = m$$

$$E_{k_p^B}\left(E_{k_s^A}(m)\right) = E_{k_s^A}\left(E_{k_p^B}(m)\right)$$

So in case of Alice sending a message Bob she apply the encryption algorithm twice, once with her private key and once with Bob public key :

$$c = E_{k_p^B}\left(E_{k_s^A}(m)\right)$$

When Bob receive the message first apply the decryption algorithm with his private key and then with Alice public key:

$$m = D_{k_p^A}\left(D_{k_s^B}(c)\right) = D_{k_p^A}\left(D_{k_s^B}\left(E_{k_p^B}\left(E_{k_s^A}(m)\right)\right)\right) = D_{k_p^A}\left(E_{k_s^A}(m)\right) = m$$

The requirements for a system of this type are that it is computationally easy for Alice and Bob generate the pair of keys and it is computationally easy apply the encryption and decryption algorithms knowing the keys but it is computationally unfeasible determinate the private key or the plain text from the public key and the cipher message. In order to achieve this requirements Rivest, Shamir and Adleman developed their famous RSA cryptography. Public key system as symmetric encryption depends on an invertible mathematical function and are vulnerable to brute force attack. However in this case the complexity of calculate the inverse of the encryption function without knowing the key scale more than linearly with the length of the key and so if the key is large enough brute force attack are not feasible (Stallings 2011). The RSA algorithm found his strength on the huge computational power needed to factorize the product of two large prime numbers: it is an easy task knowing one of the factor but in the other case it requires a huge computational power.

However, this paradigm changed radically with the eve of Quantum Information. In fact Shor in his famous paper of 1994 proposed an algorithm that, exploiting the possibility offered by quantum information was able to perform the factorization of an integer in a polynomial time (Shor 1994). In particular, Shor algorithm time required from such algorithm scale with n^3, a substantial gain when compared to fastest classical algorithm that scale with $e^{n^{1/3}}$ (Mermin 2007). Using the Shor algorithm a Quantum Computer with a sufficient number of qbits could represent a threat to all the system that employ the RSA cryptography scheme. This possibility

was experimentally demonstrated in 2001 when a research team successfully implement the Shor algorithm on a Quantum Computer with 7 qbits and factorized the number 15 (Vandersypen, et al. 2001). Although possibilities offered by Shor algorithm are currently limited by the number of qbits effectively available on today's quantum computers, the competition between Quantum Computer producers is leading to market devices with increasingly high number of qbits (in the order of hundreds), opening the possibility to a real threat for the RSA cryptography in the next years.

2.2. Principles of Quantum Key distribution

Quantum Key Distribution (QKD) offer a possible solution of the key distribution problem in the OTP cryptography, allowing the generation of a shared and random key between Alice and Bob. This is done exploiting principles of quantum mechanics, in particular the no-cloning theorem that declare the impossibility of copying an unknown quantum state, assuring the impossibility from an Eavesdropper to create a copy of the key during the generation process. Because of the theorem, any attack to the system will translate in an anomaly of the key generation process that can be detected by Alice and Bob making them aware of the attack (F. A. Bovino 2014).

2.2.1. No Cloning Theorem

The theorem was first introduced by Wooters and Zurek in 1982 and is the following:

"An arbitrary quantum state cannot be cloned perfectly".

Let now be A and B two a generic quantum systems and $|\psi\rangle_A$ and $|e\rangle_B$ two quantum states of A and B respectively. Suppose that A and B share a common Hilbert space $H = H_A \otimes H_B$. Now we want to copy the state $|\psi\rangle_A$ over $|e\rangle_B$ for any possible choice of $|\psi\rangle_A$ and $|e\rangle_B$. The initial state is so $|\psi\rangle_A \otimes |e\rangle_B$ and the aimed final state is $|\psi\rangle_A \otimes |\psi\rangle_B$ where $|e\rangle_B$ is independent from $|\psi\rangle_A$ and $|\psi\rangle_A$ is unknown.

The only two possible operation that we can make on the initial state are measuring, with the result of collapsing the state in one of the auto-state, or controlling the Hamiltonian of the combined system, that means applying the time evolution operator $U(t)$. The time evolution operator is a cloning machine if:

$$U|\psi\rangle_A|e\rangle_B = |\psi\rangle_A|\psi\rangle_B$$

Let now be $|\phi\rangle_A$ another generic state of A, because U is unitary:

$$\langle e|_B\langle\phi|_A|\psi\rangle_A|e\rangle_B = \langle e|_B\langle\phi|_A UU^\dagger|\psi\rangle_A|e\rangle_B = \langle\phi|_B\langle\phi|_A|\psi\rangle_A|\psi\rangle_B$$

Since $|e\rangle$ states are normalized, we get:

$$\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2$$

And it means that $|\psi\rangle$ and $|\phi\rangle$ are orthogonal (and so $\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2 = 0$) or are the same state ($\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2 = 1$) that it is not true for generics $|\psi\rangle$ and $|\phi\rangle$. This imply that a single U is not able to clone a general quantum state and prove the theorem (F. A. Bovino 2014).

2.2.2. BB84 Protocol

In the BB84 protocol, the quantum channel is not used to send any message, but it is used to generate two identical random strings. Someone can argue that there is no information exchange in such process but now the two identical strings can be used as key for an OTP cryptography. The protocol is the following:

In a first phase (also known as quantum phase) Alice sends through a quantum channel a series of single photon, choosing randomly both the base (rectilinear or diagonal) and the polarization. A 0 or 1 value is assigned to the value of polarization. In the quantum state notation, this means sending the states $|0\rangle$ (horizontal polarization), $|1\rangle$ (vertical), $H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} = |\nearrow\rangle$ (diagonal) or $H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}} = |\searrow\rangle$ (anti diagonal). For each received photon Bob randomly choses the polarization base and then measures the polarization of the incoming photon obtaining a string of bits corresponding to the measured polarization [Figure 12]. It follows a second phase (known as public phase), now Alice and Bob communicate on the public channel and declare the polarization basis on which photons were coded and measured (but not the value of the polarization). Photons that was not sent and measured on the same base are discarded and the polarization of the remaining photons constitute the key for the one time pad (Bennett e Brassard 1984).

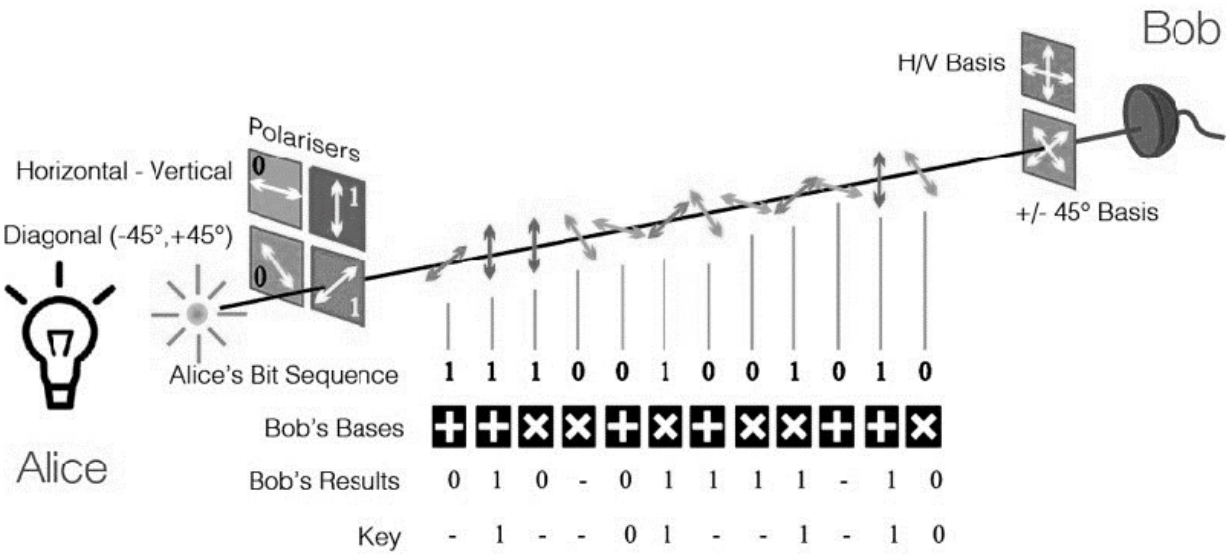

Figure 12 – BB84 Protocol (Quantum Flagship 2021)

To verify the presence or not of an Eavesdropper Alice and Bob reveal the polarization of a fraction of valid photons. If Eve intercepted some photons, made random measurements and sent the result to Bob then a quarter of the useful photons on which Alice and Bob should agree will not be the same. This because since Bob is measuring on a random base his choice of the base will agree with Eve's one only in the 50% of the case. If Bob and Eve measure on the same base they will obtain the same value but if they measure on different base Bob will obtain a random value (that is still correct in the 50% of cases). Overall, if an Eavesdropper try to intercept the message Alice and Bob would disagree on 25% of the check bits and this warns on the presence of an Eavesdropper (Bennett e Brassard 1984).

In the version of the BB84 described above Alice generate random polarized photons and then send them to Bob that perform random measurements; however, there is another version of the protocol that involves a central source of entangled photons that are sent to Alice and Bob and then measured. It could be shown that it is the same as the original protocol. In this modified version a central source of entangled photon generate two photons in the entangled state $|\psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ and send them to Alice and Bob. Now Alice and Bob both make random measurements and then communicate the measurement base on the classical channel. As in the previous case if the discard the value obtained measuring on different basis and obtain the one time pad key (Mermin 2007).

At the basis of the BB84 protocol there is the No-Cloning theorem and the assumption that Eve cannot clone the qubits sent by Alice without altering them. Let be $|\psi\rangle$ and $|\phi\rangle$ two non-orthogonal states on which Eve tries to gain information and $|u\rangle$ an ancilla state. Eve tries to gain information by the interaction between $|\psi\rangle$ or $|\phi\rangle$ with $|u\rangle$. If the process does not disturb the initial states, the process is:

$$|\psi\rangle|u\rangle \rightarrow |\psi\rangle|v\rangle$$

$$|\phi\rangle|u\rangle \rightarrow |\phi\rangle|v'\rangle$$

Where $|v\rangle$ and $|v'\rangle$ should be two distinguishable states in order to discriminate if the original state from Alice was $|\psi\rangle$ or $|\phi\rangle$. However since the internal product must be same before and after the transformation:

$$\langle v|v'\rangle\langle\psi|\phi\rangle = \langle u|u\rangle\langle\psi|\phi\rangle$$

$$\langle v|v'\rangle = \langle u|u\rangle = 1$$

And this imply that $|v\rangle$ and $|v'\rangle$ are the same. So in order to not alter the qbit sent from Alice and remain undetected Eve has to gain no information at all (F. A. Bovino 2014). Authentication

QKD protocols as the BB84 described in the previous section has been proven to be unconditionally secure with the assumption that all devices are perfect. However, this is far from the truth in real devices and imperfection can be exploited from an eavesdropper to break the QKD. Many kind of attacks has been studied like the photon number splitting attack, Trojan horse attack, phase remapping attack, partially random phase attack, detector control attack, side channel attack and others (Fei, et al. 2018). All this possible attacks however focus on the key distribution process ignoring the establishment of the quantum channel. In fact, the success of this process is usually considered an assumption, however it can be hacked with a so-called man in the middle attack. In this type of attack, Eve intercept both the quantum and classical channel faking Alice and Bobs responses to each other. Since Eve is present from the very first communication on the channel Alice and Bob are convinced to talk with the legitimate partner and are not able to detect the attack. In fact, from Alice and Bob point of view it is impossible distinguish Eve from Bob and Alice respectively. To avoid this possibility Alice and Bob must

share a short initial secret key for the initial authentication. After this phase, the key can be exponentially expanded and used to authenticate the following phases of the communication (everlasting security property) (Alléaume, et al. 2014).

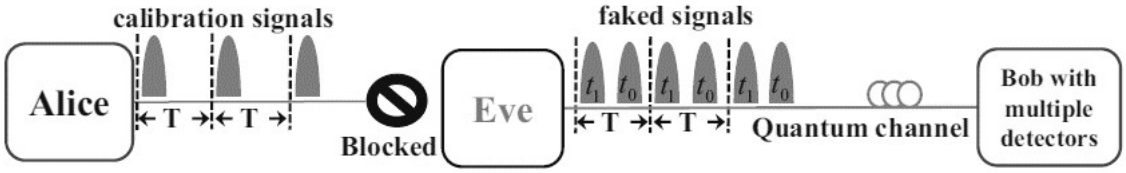

Figure 13 - Simple diagram of our quantum man-in-the-middle attack strategy on the calibration process. (Fei, et al. 2018)

2.2.3. QKD with symmetric encryption

As already mentioned in cap 2.1.2 OTP is the only mathematically secure encryption so it is logical to combine it with QKD. This is possible because it could be proven that QKD has the fundamental property to be universally composable. This in turn imply that when QKD is combined with OTP the resulting encryption protocol is an unconditionally secure protocol. Taking the advance of both OTP and QKD such protocol has a level of security that cannot be matched with any other protocol with a key agreement system that is not QKD (Alléaume, et al. 2014). Now we will analyze a much more adopted configuration: QKD in combination with symmetrical encryption such AES. In fact, this is the solution currently adopted by many commercial solution and research projects. A system with this combination can be implemented in layer 2 (link) of the OSI model or directly in layer 3 (network). In this case, the security of the data cannot be stronger than the security offered by the encryption scheme. For a symmetric key cypher this depends from:

- The security of the key;
- The number of blocks encrypted with the same key (key renewal rate);
- The length of the key;
- The security of the algorithm.

Where the length of the key and the security of the algorithm do not depend from the key agreement technique. At the same time, security of the key and renewal rate strongly depend

from the key agreement scheme that is QKD in our case. As already mentioned QKD is the only technique that can offer information-theoretic security. In addition, using QKD as key renewing method guarantee long-term security for the key compared with classical system that rely on asymmetric encryption to establish keys and are exposed to computational attacks. Further advantage of QKD is the so-called forward-secrecy property of the established keys that means that keys obtained with a QKD system are independent form one another and this guarantee that compromising a single key do not compromise the entire system. This property follows from the everlasting secrecy property already mentioned and can also be obtained with public key systems under computational assumption but not with symmetric systems (Alléaume, et al. 2014). From the key renewal rate strongly depends the security of the data and it should be grater than key aging factor in order to guarantee security. The key aging factor respond to a very simple question: how often a key should be changed and how this affects the security of the system? As an example consider module that implement a 128bit AES ad can cypher 2,2 Gbit/s. In this case the number of 128 bits blocks encrypted per second is $\sim 2^{27}$ blocks/s. An exhaustive attack will take $\sim 8 \cdot 10^{22}$ years which means that this kind of attack is not a threat. If AES is considered secure, then the upper limit of the key renewal rate is $2^{keylength}$ blocks, in fact after this limit the key must be changed in order to avoid collision-related problems. However exist argument that indicate the existence of algorithmic weakness of AES and so it is beneficial for the global security of AES to renewal the keys way earlier than the $2^{keylength}$ blocks limit (Alléaume, et al. 2014).

2.3. QKD Devices

First experiment with quantum channels was performed over a distance of 30 cm. However, this was just the start of impressive improvements and with today technology transmission of a quantum state was successfully demonstrated over distance of 144 km in air (Ursin, et al. 2007). Photons are the main way to transmit quantum states and research explored both optical fibers and free space with different performances and applications. Once chosen between guided and free propagation the remaining problem is the choice of sources and detectors. Commercially available products offers different solutions at 800nm where efficient photon counters are available but require special fibers or between 1300 nm and 1550nm, which are compatibles with telecommunication fiber. The most common choice usually is the first for

free space propagation and the second for guided propagation, in fact the quality of telecommunication fiber compensate with minor losses the less efficiency of the detectors at telecommunication wavelength (Gisin, et al. 2002). In the next paragraphs we will analyze how to generate single photons, how to transmit them and finally how to detect them.

2.3.1. Sources

Lasers are the most common source of light for quantum information applications for their practicality and versatility. The output of a laser in a specific mode is described as a coherent state:

$$|\alpha\rangle = \left|\sqrt{\mu}e^{i\theta}\right\rangle = e^{-\mu/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle$$

Where $\mu = |\alpha^2|$ is the average photon number and the phase factor $e^{i\theta}$ is accessible if a reference phase is available. If the reference phase is not available, the state can be described as a mixture:

$$\rho = \int_0^{2\pi}\frac{d\theta}{2\pi}|\alpha\rangle\langle\alpha| = \sum_n P(n|\mu)|n\rangle\langle n|$$

Where $P(n|\mu) = e^{-\mu}\frac{\mu^n}{n!}$ is a Poisson distribution. When attenuated lasers are used to generate quantum signals the phase reference does not play any role. Since coefficients of the distribution have a non-zero value for any n this open the possibility to photon-number-splitting attacks (Scarani, et al. 2009).

Sub-Poissonian sources or single photon sources have a probability of emitting two photon lower than attenuated lasers and are a better approximation of a single-photon source. In this kind of sources the quantum signal is considered to be a photon-number diagonal mixture with very little contribution from the multiphoton terms. To measure the quality of a source the second order correlation function is usually considered:

$$g_2 = (\tau) = \frac{\langle : I(t)I(t+\tau) : \rangle}{\langle I(t)\rangle^2}$$

With $I(t)$ the source signal intensity and where : - : indicate the normal ordering of creation and annihilation operators and:

$$g_2(0) \approx \frac{2p(2)}{p(1)^2}$$

Where $p(n)$ is the probability of the emission of n photons. It could be shown that the performances of a source in an implementation of the BB84 protocol are characterized by the g_2 parameter, the smaller it is and the closer is the source to a single-photon source (Scarani, et al. 2009).

In entanglement-based implementations of QKD, pairs of entangled photons are mostly obtained from spontaneous parametric down conversion. In this case photons from a pump laser are directed to a non-linear crystal where are converted in pairs of photons. In the approximation of two output modes the resulting state is the so called two mode squeezed vacuum:

$$|\psi\rangle_{PDC} = \sqrt{1-\lambda^2} \sum_{n=0}^{\infty} \lambda^2 \, |n_A, n_B\rangle$$

With $\lambda = \tanh \xi$ and ξ proportional to the amplitude of the pump and where n_A, n_B represent the state with n photons destined to Alice and Bob. States prepared with this technique can be directly utilized in case of continuous variable protocols. In case of discrete variable protocols (like the BB84 protocol) it should be noticed that spontaneous parametric down conversion always produces multi-pairs components and so it is vulnerable to photon number attacks (Scarani, et al. 2009).

2.3.2. Physical Channels

The two main quantum channels for light are fiber optics and free space and the most important parameter for QKD application is the amount of loss introduced by the channel. In fact the amount of key that can be extracted and the maximum distance directly depend from the amount of photons that are effectively detected at the end of the channel, that in turn depend from the loss of the medium and form the dark counts. Optical fibers have been extensively

studied for their wide usage in telecommunication, their losses are due to scattering and depend exponentially from the length of the fiber:

$$t = 10^{-\alpha l/10}$$

Where the value of α depend from the wavelength and has a minimum in the two so-called "telecom windows" around 1330nm and 1550nm where losses are respectively 0.34dB/km and 0.2dB/km. At the same time, free space combined with small telescopes is equally effective for line-of-sight short-range application. In this case, the main source of losses is atmospheric scattering although there are windows as 780-850nm and 1520-1600nm where losses are less than 0.1dB/km in clean weather [Figure 14] (Henniger e Giggenbach 2006).

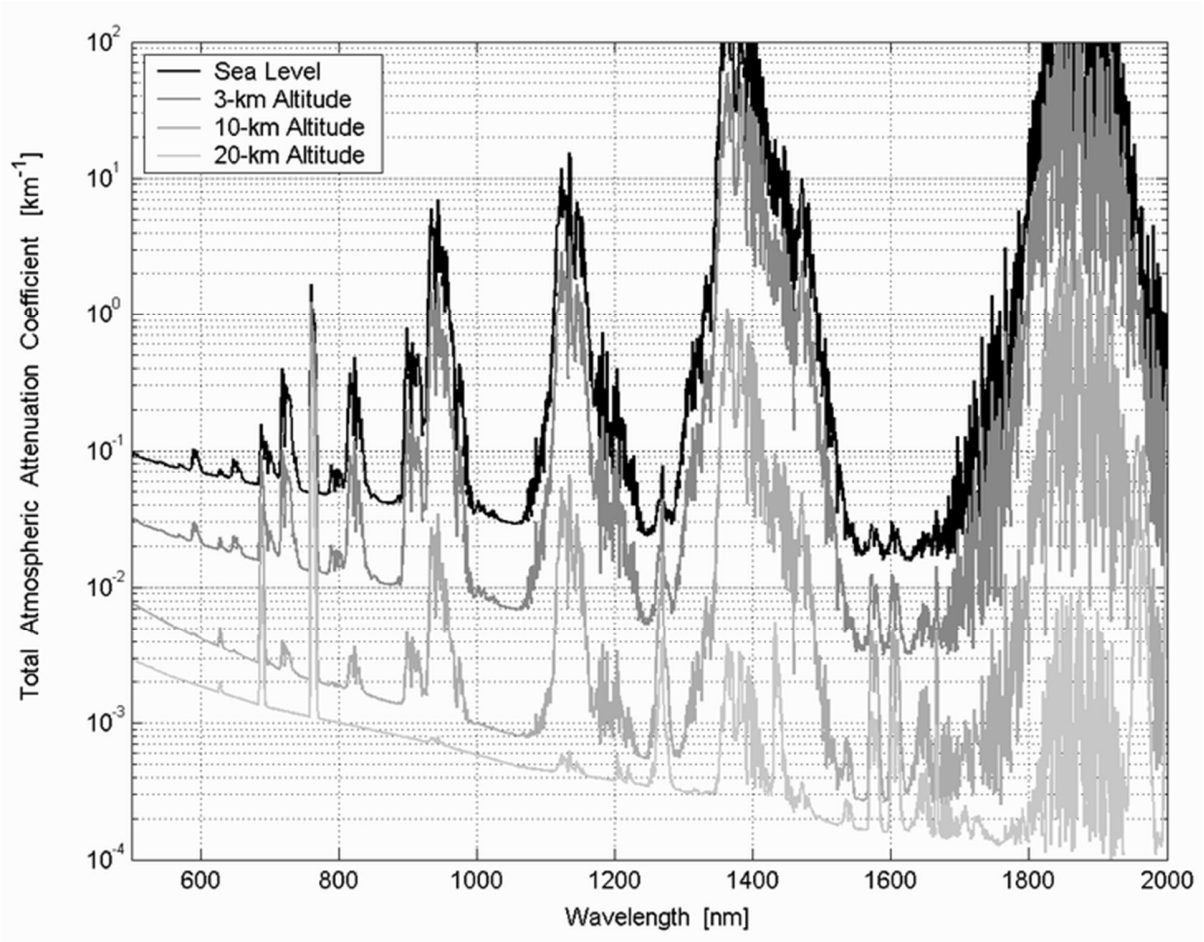

Figure 14 - Altitude dependant coefficient of clear-sky atmospheric attenuation vs. optical and near-infrared wavelengths. Four different altitudes are considered: sea level (uppermost curve), 3 km, 10km, 20 km (lowest curve) Attenuation values are averaged over 1 nm (Henniger e Giggenbach 2006)

A simple model for free-space applications is:

$$t \approx \left(\frac{d_r}{d_s + Dl}\right) 10^{-\alpha l/1}$$

Where d_r and d_s are the apertures of sending and receiving telescopes, D is the divergence of the beam and $\left(\frac{d_r}{d_s+D}\right)$ approximate geometric losses. Of course, in space applications like communication between satellites attenuation in negligible and losses are due only to the geometric factor (Scarani, et al. 2009).

2.3.3. Detectors

In discrete-variables protocols like BB84, photon-counters are used as detectors. Main parameters to consider for this devices are the dark count rate p_d and the quantum efficiency η, characterizing respectively the probability of a detector click without any photon (the noise of the detector) and the probability of a detector click when it is hit by a photon. Another parameter to consider is the dead time of the detector that is the time needed to reset the detector after a click and determine the maximum repetition rate of the system. Avalanche Photodiodes (APD) are the most commonly used detectors, particularly Si and InGaAs/InP APD are used respectively for the 400-1000nm and 950-1650nm intervals. Typical parameters are listed in Table 2. Other type of less used single-photon detectors are Visible light Photon Counters, Superconducting Single Photon Counters and Transition edge Sensors (Scarani, et al. 2009).

Name	*λ [nm]*	*η*	*p_d*	*Rep. [MHz]*	*Count [MHz]*	*Jitter [ps]*	*T [K]*
Si	600	50%	100Hz	Cw	15	500-200	250
InGaAs	1550	10%	10^{-5}/g	10	0.1	500	220

Table 2 – Overview of typical parameters of single-photon detectors (Scarani, et al. 2009)

2.4. QKD networks

QKD as we defined it in the previous chapters is a point-to-point protocol and this impose many limits on what can be reached with standalone QKD links. In addition, QKD links are limited in both rate and distance. To overcome this problems many architectures of Quantum Networks connecting many nodes with a series of quantum link has been proposed. We will

now analyze the three main different families of Quantum Network: optical switching, quantum relaying and trusted relaying:

- **Optical switched quantum networks:** In this type of network the quantum signal is routed between the nodes with a series of optical devices as beam splitters and optical switches. This enable to go beyond the two users scheme and has the main benefits of an uninterrupted quantum signal form Alice to Bob removing the need of trusted intermediate nodes. However, this type of network has the main disadvantage to not providing any extension in the distance over which keys can be distributed. On the contrary, the additional losses introduced by the intermediate nodes reduce the practical distance of operation (Alléaume, et al. 2014).
- **Quantum relaying:** With these networks it is possible to overcome the problem of losses in optical switched quantum networks with quantum repeaters. This kind of devices rely on entanglement swapping to partition the channel in smaller segments and this in turn allow low noise level [Figure 15]. Although this technique in theory could propagate a quantum signal over an arbitrary distance in real devices the accumulation of noise over each hop provide a limit to the maximum number of repeaters. As in the previous case this kind of nodes do not need to be trusted (Dür, et al. 1999).

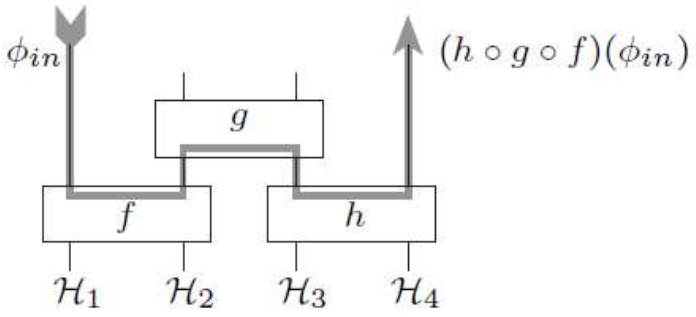

Figure 15 – Entanglement Swapping scheme (Coecke 2004)

- **Classical trusted relaying:** it is a type of quantum network where local keys are generated between consecutive network nodes and stored in classical memory. When a message is transmitted between two non-consecutive nodes, a series of encryption-decryption operations is performed over each node [Figure 16]. In other words, a classical trusted relaying quantum network is a classical network where each exchange

between nodes is protected with a QKD based encryption. However, the overall security is guaranteed only if the nodes can be trusted (Alléaume, et al. 2014).

As already mentioned QKD rely on an initial trust between nodes in order to guarantee security. This can be achieved with an initial secret key shared by the terminals (key pre-distribution) or with authentication over a classical channel. In the case of a quantum network initialized with key pre-distribution n(n-1)/2 initial keys are needed (Alléaume, et al. 2014).

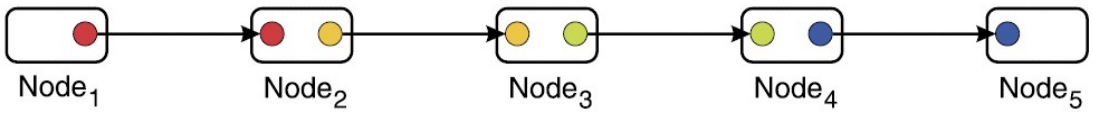

Figure 16 - "Hop-by-hop" unconditionally secure message passing on a path made of trusted relay nodes connected by QKD links. Message decryption/re-encryption is done at each intermediate node by using the local key distributed by QKD. Different key associations are symbolized by different colors (Alléaume, et al. 2014).

3. Mobile quantum network

As seen in the previous chapter limits of classical cryptography make security issue critical for present and future military application. At the same time, recent advancement in free-space QKD device made feasible the realization of a quantum network over the distance of 144 kilometers (Ursin, et al. 2007) enabling the possibility to employing QKD in the battlespace.

The possibility to realize a quantum communication between a ground station and a fast moving aerial platform was successfully demonstrated by in 2013 stablishing a BB84 based QKD between a plane moving at a 290 km/h and a ground station at 20km (Nauerth, et al. 2013) [Figure 17] opening the possibility to employ QKD also for aeronautical applications. Miniaturization of hardware allowed application of the same architecture on small drones and studies and patents on a two node drone based quantum network already exist (Kwiat and Gauthier 2017) (Hill, et al. 2020) and (Liu, Tian, et al. 2020). In this chapter, we will extend the concept to a drone swarm realizing a mobile QKD network.

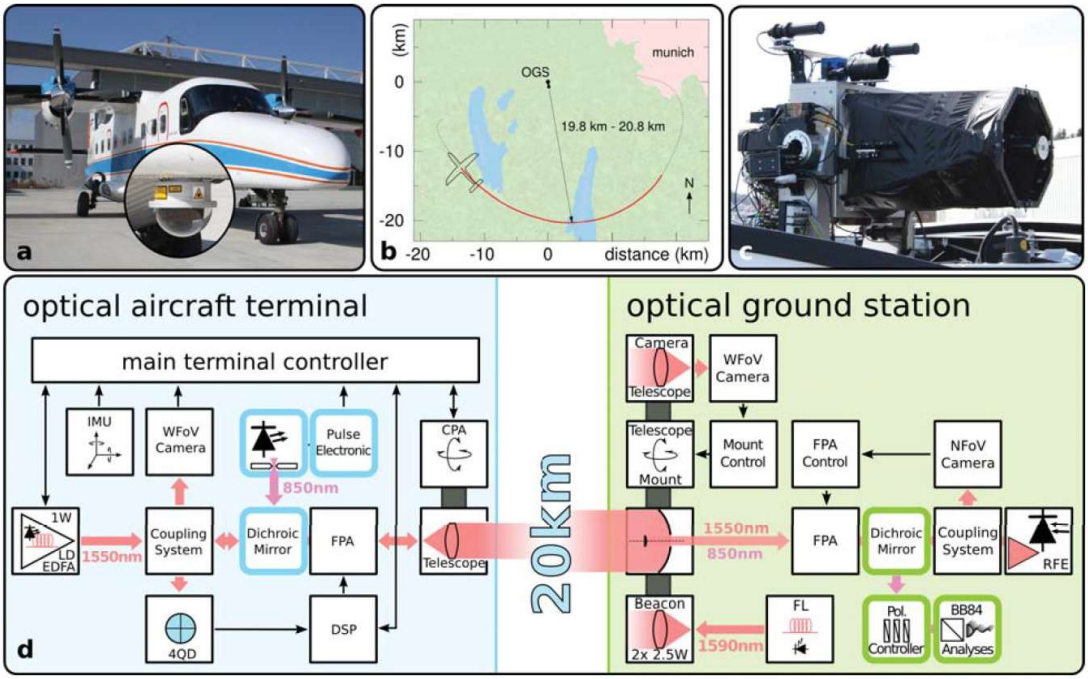

*Figure 17 – **a**: Dornier 228 with the inset showing the optical dome housing the coarse pointing assembly. **b**: Airplane track with the red section indicating the positions during QKD-transmission. **c:** Optical Ground Station telescope. **d**: Sketch of airborne and ground terminal with integrated QKD system (colored boxes). (Nauerth, et al. 2013)*

Figure 18 - Left: Optical Terminal in Lab. Right: View of Do228 aircraft firing its laser during trials (Fuchs e Giggenbach 2010)

3.1. Mission of the SWARM

The mission of the proposed swarm is to implement a mobile quantum network in order to connect a command and control center with ground and aerial platforms spread over the battlefield, enabling quantum security level for communication between all the elements of the network (Figure 19). Swarm elements will act as nodes of the network providing a wide area coverage, a great redundancy and resilience with a small cost of operation. The main advantage of employing a large number of drones for this particular mission is the possibility to keep the length of the optical link between the nodes in the optimal range, minimizing losses of the system without the need of large optics.

In order to be able to be deployed also in remote oversea scenario we propose a swarm able to communicate with the command center also via a dedicated quantum satellite, a special platform might be considered for this role. The key generation rate should be at least 1kb/s in order to provide enough keys for tactical data link.

The entire system will be available also for civil application such as providing keys for critical services in urban areas [Figure 20].

We will now propose a possible solution for this mission requirements; in paragraph 3.2 and 3.3 we will describe the optical hardware needed to implement the quantum network and the swarm respectively.

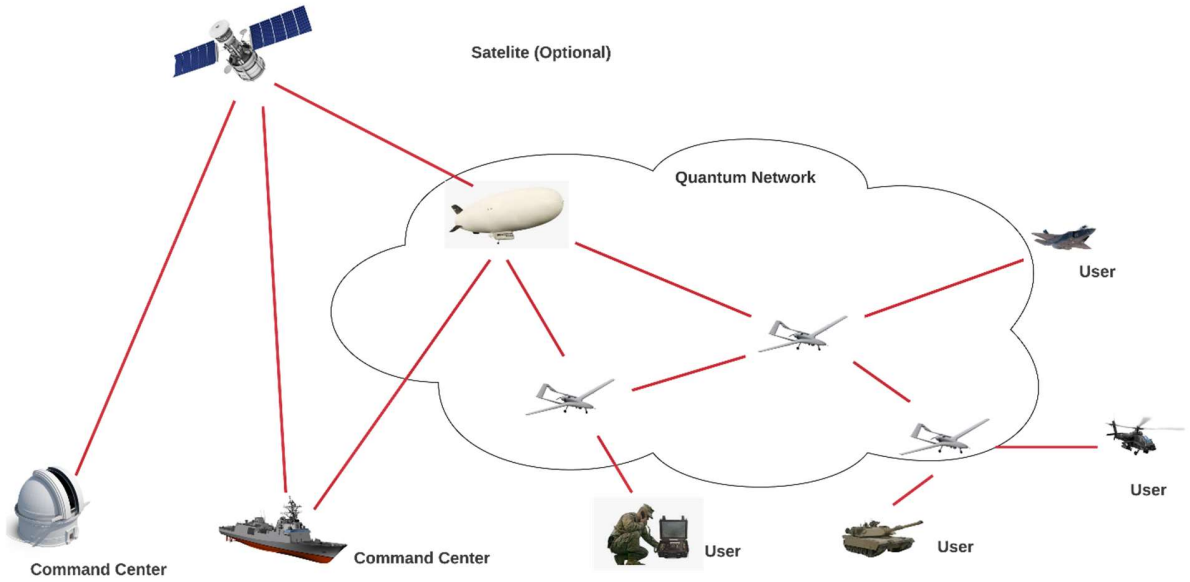

Figure 19 – Illustration of the proposed Quantum Network

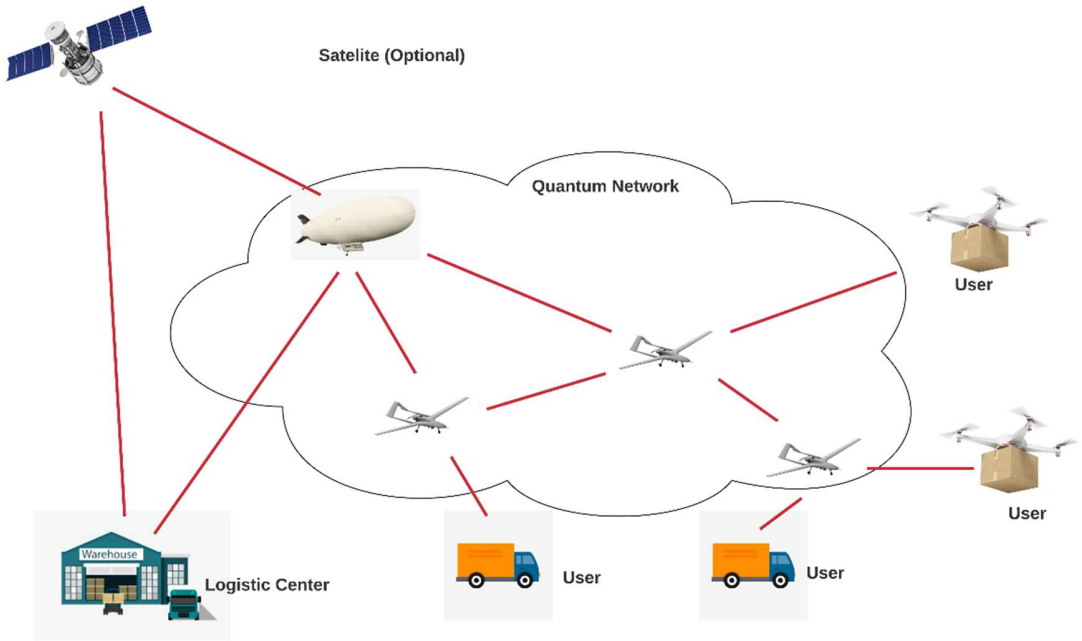

Figure 20 – Dual Use of the proposed Quantum Network

3.2. QKD Network Setup

In order to satisfy the mission requirements we propose a swarm where each drone realize a trusted node of the quantum network and is equipped with all the hardware needed to implement the BB84 protocol in both the Alice and Bob roles. Therefore, each drone will be equipped with both a single photon source and a detector. On the other hand, in order to minimize dimensions and weight, user terminals will be equipped only with detectors and will implement only the Bob role. User terminals will be sufficiently compact to be hand-portable or integrated with low effort on ground and aerial platform. Since the proposed architecture do not allow direct key agreement between users, the fact that user terminals will not able to realize Alice's role will not imply any limitation. When a user need to communicate with the command center or with another user on the network, it will receive the key from the nearest node and then the message will be transmitted over a classical channel encrypted with an OTP cryptography. In order to make it possible, drones have to fly in area where they are able to establish a quantum channel with the command center, generate keys and store them until it will reach the user, establish another couple of keys and use them to encrypt the previous key that are now sent to the user. In case of immediate need of new keys, also a hop-by-hop approach can be used to deliver keys through the network eliminating the time necessary to fly from a point to another.

Since the BB84 do not provide any authentication mechanism all the nodes of the network and the user terminals will necessary be pre-authenticated in the network setup phase and it will not be possible to add ne nodes during the operation.

3.2.1. QKD system architecture

The core of the system is an airborne device capable to realize QKD in both Alice and Bob's role transmitting or receiving photons between two nodes or between a node and a user terminal. The possibility of switch between Alice and Bob role will be obtained adding an optical switch before the pointing and tracking device commuting the two optical paths between source and detector. In the Alice's role, photons will be routed from the source to the polarizer filter and then will be guided to the pointing and tracking device. Photons will propagate in free space to Bob's turret, and then they will measured by one detector in a

Detection Time Bin Shift (DTBS) configuration. Operative frequency is chosen at 830nm due the low atmospheric loss and the commercial availability of small, light and high efficiency detectors at this frequency.

Incoming photons are directed through a 50-50 beam splitter, then one arm pass through polarizing filter that rotate the polarization by 45° and this allow to randomly choose the measurement base, an essential element of the BB84 protocol. Now the two lines will encounter a polarizing beam splitter. In the original BB84 configuration four detectors are connected at the output of the two polarizing beam splitters, however in the DTBS configuration the four outputs are connected to four different delay lines and then rejoined in one line connected to a single detector. Because the four paths are now time distinguishable there is no loss of information and this allow to reduce detectors form four to only one, reducing weight of this part of the system by a factor of four. DTBS require precise timing to resolve the four time bin and for this reason, an additional laser is needed as time reference. This timing laser will be coaxial to the main system and will also allow to activate the detectors only when is there is a key exchange attempt reducing noise from solar radiation. We will now describe one by one the components of the system.

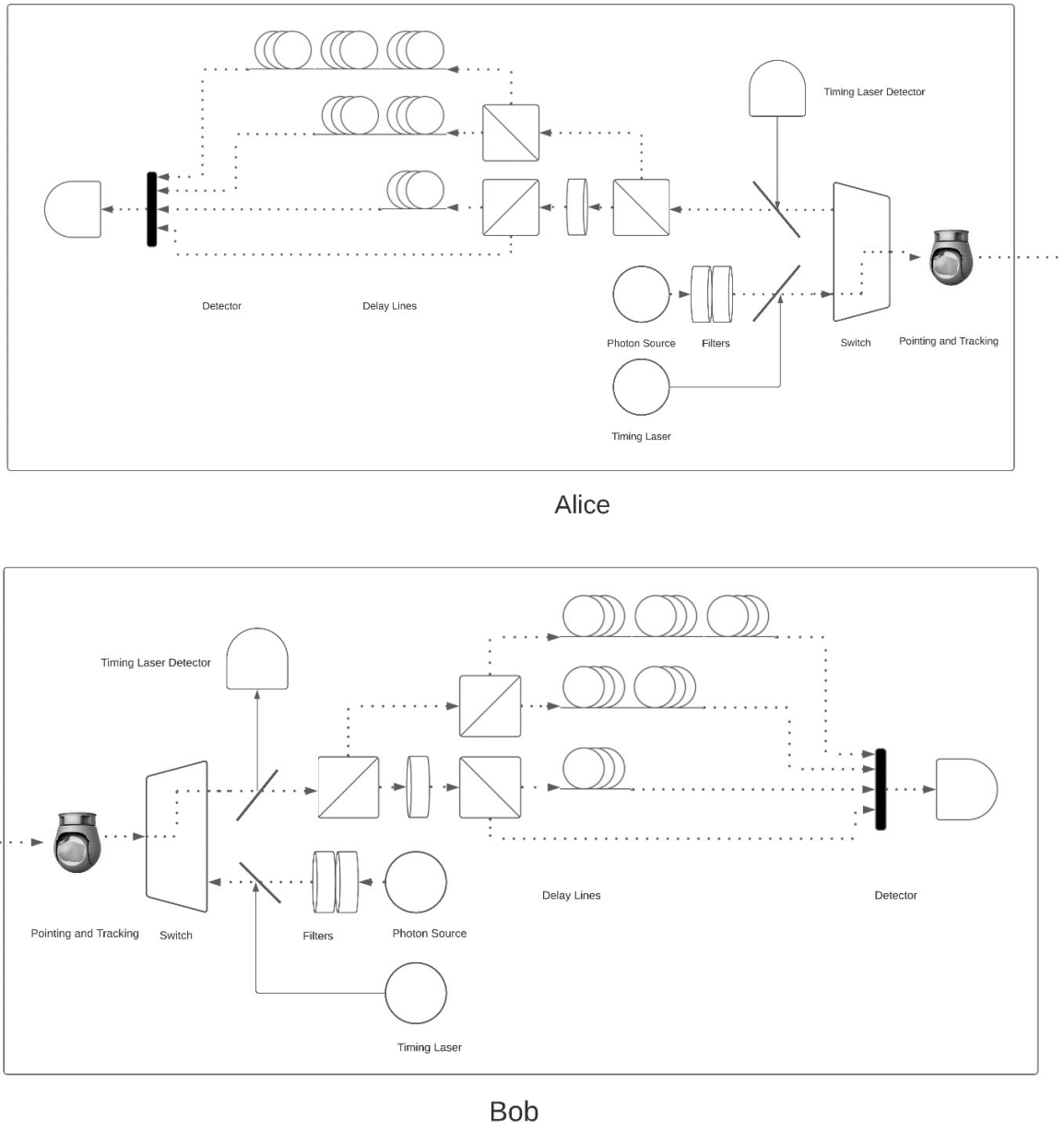

Figure 21 – Scheme of the Alice (top) and Bob (bottom) airborne QKD devices.

3.2.2. Weak coherent state source

As already mentioned in paragraph 2.3.1, the output of a laser in a specific mode is described as a coherent state:

$$|\alpha\rangle = \left|\sqrt{\mu}e^{i\theta}\right\rangle = e^{-\mu/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle$$

Where $\mu = |\alpha^2|$ is the average photon number. In order to obtain an average photon number of the order 0,6 - 1,0 a laser source will be directed to a Beam Splitter. One arm of the BS will be the output of the source while the other will be measured in order to monitor the output power and modulate the laser source. Average photon number per pulse will be:

$$\bar{n} = \frac{\lambda(P_s - P_m)}{hc} \cdot \frac{1}{r}$$

Where P_s and P_m are the power of the source and the power measured and r is the repetition rate. As a possible source we propose the one of the ID 3000 Series – Picosecond Lasers (Figure 22). This source is based on high-reliability semiconductor laser diodes operated in gain-switched mode, emitting laser pulses shorter than 30 ps. Repetition rate is tunable from pulse on-demand up to 40MHz. Dimensions of the control unit and laser head are respectively 326 mm x 88 mm x 235 mm and 95 mm x 31 mm x 181 mm, weights are 2,5kg for the control unit and 0,45 for the lase head. Power consumption is less than 30W allowing its use on drones (ID Quantique 2021). Additional information are provided in (Table 3).

Figure 22 - ID3000-Picosecond-Lasers

Optical	
Pulse repetition rate	Pulse-on-demand (0 HZ TO 40 MHZ)
Frequency resolution	1 @ 50 Hz
Beam quality, TEM	$M^2 < 1.2$
Polarization extinction ratio	> 20DB (Unpolarized Fibre)
Timing jitter, rms	Timing Jitter, RMS
Mechanical/Electrical/Environmental	
Power consumption	< 30 W
Laser head dimensions	95 mm x 31 mm x 181 mm
Laser head weight	0.45 kg
Control unit dimensions (W x H x L)	326 mm x 88 mm x 235 mm
Control unit weight	2.5 kg

Table 3 – Laser Source Specifications

3.2.3. Detector

The detector chosen for the system is the ID Quantique ID120 Single Photon detector (Figure 24). It is a commercially available silicon single photon avalanche photodiode sensitive in the visible spectral range. The quantum efficiency is 80% in the around of 800nm (Figure 25) that is the frequency chosen for the system. The dark count rate is less than 300Hz for the Ultra Low Noise (ULN) version of the detector. Weight and power consumption of such detector are 650g and 12W (ID Quantique 2021), allowing its use on a small aerial platform. Additional details are provided in (Table 4). A single detector with four different delay lines will be mounted in a detection time bin shift (DTBS) configuration. In order to reduce volume and weight of the device the BS, the polarizer filter and the PBS could be integrated in a single component as shown in [Figure 26] (Bovino, et al. 2005). The four output port will be connected to four different delay line of 0, 1, 2 and 3 μs and then rejoined and connected to the detector [Figure 23].

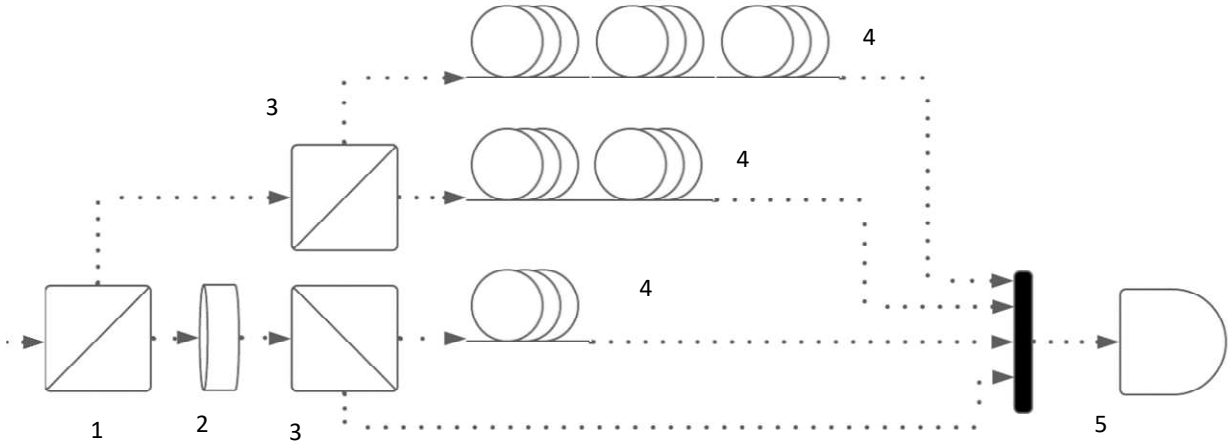

Figure 23 – Scheme of the BS 5-50 [1], Polarizer [2], Polarizing BS [3], delay lines [4] and detector [5] connections

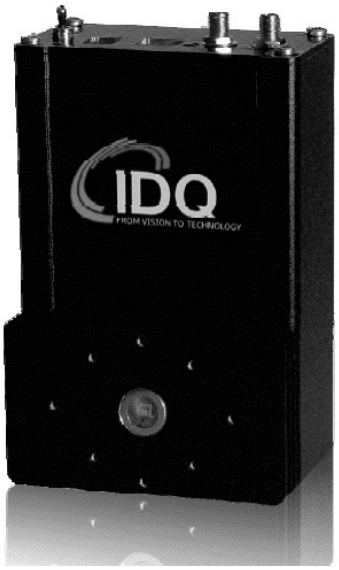

Figure 24 - ID Quantique ID120 detector (ID Quantique 2021)

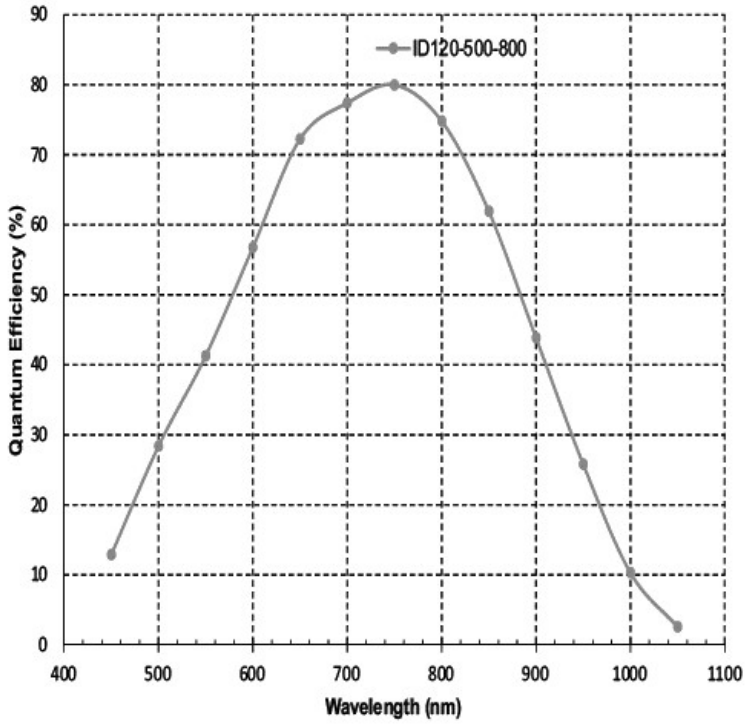

Figure 25 – ID120 Quantum efficiency between 400 and 1100nm (ID Quantique 2021)

Parameter	*Min*	*Typical*	*Max*	*Units*
Wavelength range	350		1000	nm
Active Area	500			µm
Single-photon detection probability (SPDE)				
at 650 nm (at max. excess bias)			60	%
at 800 nm (at max. excess bias)			80	%
Dark Count Rate (at -40°C, Vbias =Vbreakdown +30V)				
ULN			<300	Hz
STD			<1000	Hz
EDU			<4000	Hz
Timing resolution (at max. excess bias)	200	400	1000	ps
Dead time		1		µs
Output pulse		NIM & LVTTL		
Output pulse width		25		Ns

Storage temperature	-40	70	°C
Weight	650		g
Power Consumption	12		W
Size	14x11x6		cm

Table 4 – ID Quantique ID120 detector specification (ID Quantique 2021)

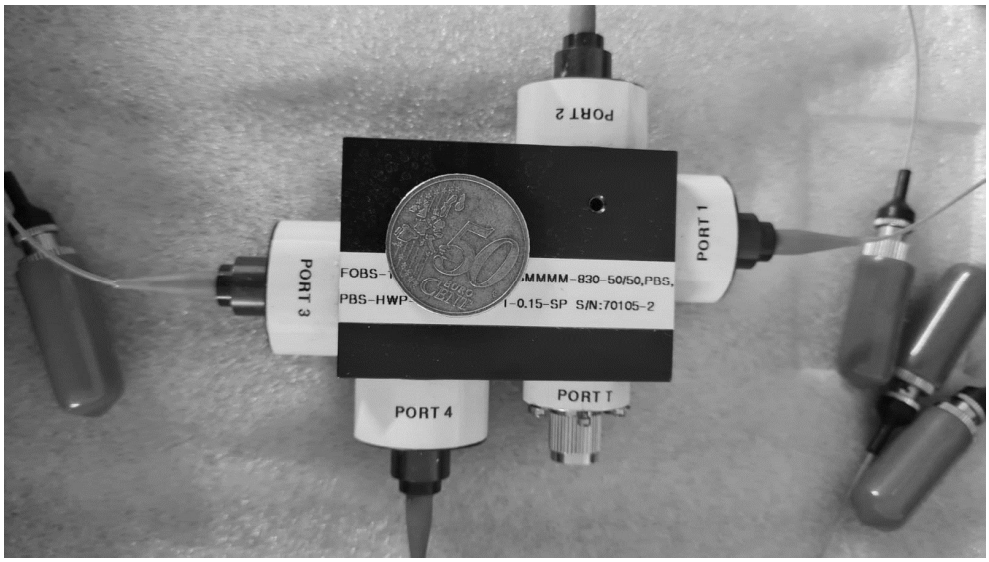

Figure 26 – Integration of the BS 50-50, the polarizer and the two PBS in a single device (Bovino, et al. 2005)

3.2.4. Estimation of the key rate

In order to determine if the chosen hardware is suitable for the desired key rate let now estimate the key rate in dependence of the distance z between Alice and Bob devices.

The spot radius $w_{(z)}$ of the photon source diverges with the propagation rules of a Gaussian beam:

$$w_{(z)} = w_0 \sqrt{1 + \left(\frac{z}{L}\right)^2}$$

With:

$$L = \frac{\pi {w_0}^2}{\lambda}$$

The Rayleigh length and w_0 the radius of the aperture of the source. In our case at $830nm$ and with $w_0 = 7{,}5m$ $(15cm\ diameter)$ we obtain:

$$L = \frac{\pi \cdot (0{,}075m)^2}{830nm} = 21291m$$

With this spot, the irradiance is:

$$I = \frac{2P}{\pi {w_{(z)}}^2} = \frac{2hc \cdot r}{\lambda \pi {w_{(z)}}^2}$$

Where P is the power at the source ant it is equal to $hc\lambda \cdot r$, with r the repetition rate of the source. In our case, the detector has a dead time of 1μs and so it could detect successfully a 1MHz rate.

Due atmospheric losses irradiance at receiver is:

$$I_r = I10^{-\alpha z/}$$

Where $\alpha{\sim}0{,}2\ dB/km$ at sea level. Collected power depend from the receiving optics dimensions, in our case $15cm$, further details of the receiving optics will be given in the next section. Collected Power is:

$$P_c = \frac{\pi a^2 I_r}{2} = P\frac{a^2}{{w_{(z)}}^2}10^{-\alpha z/10} = \frac{hc \cdot r}{\lambda}\frac{a^2}{{w_{(z)}}^2}10^{-\alpha z/10}$$

That means a number of photon at the detector per second:

$$n = \frac{\lambda P_c}{hc} = \frac{\lambda}{hc}\frac{hc \cdot r}{\lambda}\frac{a^2}{{w_{(z)}}^2}10^{-\alpha z/10} = r \cdot \frac{a^2}{{w_{(z)}}^2}10^{-\alpha z/10}$$

However the efficiency of the detector at 830nm is $\mu = 80\%$ and this reduce the number of detected photon per second at:

$$n_d = \mu \cdot r \cdot \frac{a^2}{{w_{(z)}}^2}10^{-\alpha z/}$$

The theoretical key rate of BB84 protocol is 50% of the photon per second at the detectors. However, in practical QKD devices the key rate can be approximated in ~1% of the number

of photons per second due to privacy amplification and internal additional losses that are not considered in this model, such as coupling losses between fibers, losses of the delay lines, tracking errors etc. The relation between key rate and distance at sea level is plotted in [Figure 27] (blue line).

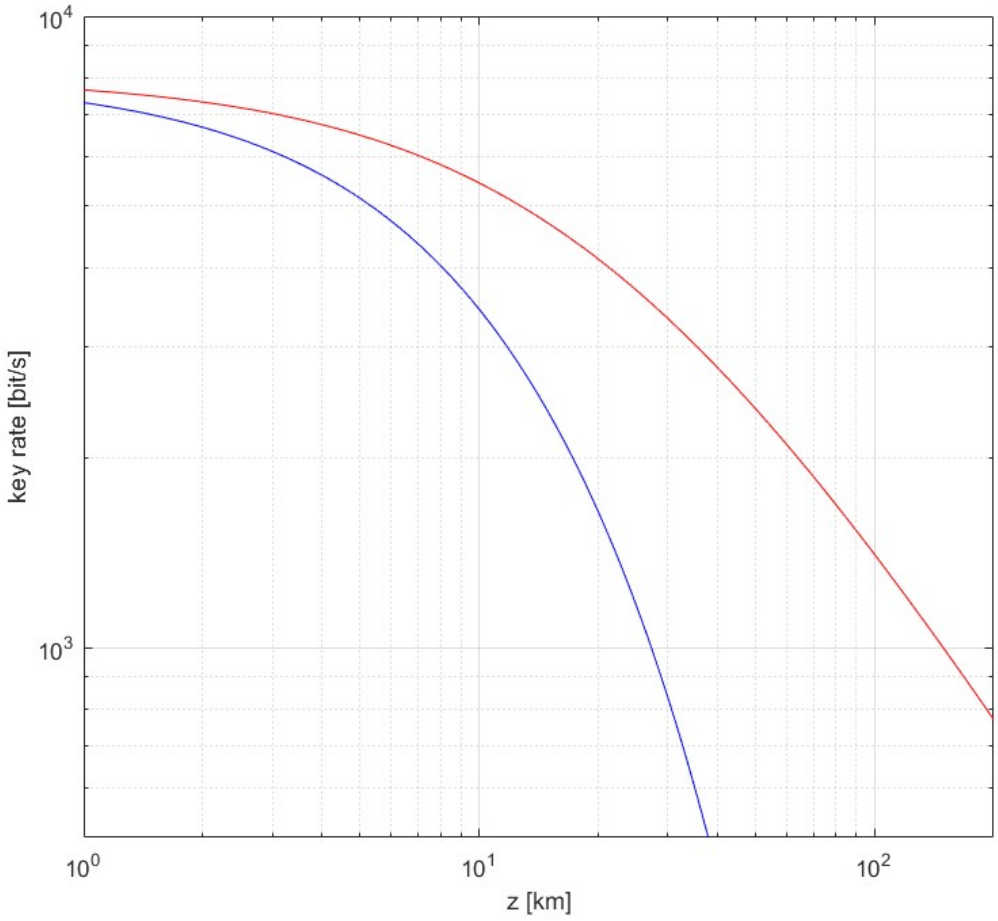

Figure 27 – Relation between key rate and distance between Alice and Bob terminals with the proposed hardware at sea level (blue line) and high altitude (red line)

From the figure, we can derive that in our case to obtain a key rate of 1kb/s the maximum distance with this hardware is ~27km. In the same figure it is plotted the key rate achievable with the same hardware between two HAP at an altitude of 20km where the atmospheric attenuation is negligible (red line), in this case the maximum achievable distance is ~149km. It should be noticed that if source and detector capable of working at 100Mhz will be available in the future, the same system can be upgraded and reach 100kb/s at 27km or 1kb/s up to 103km [Figure 28].

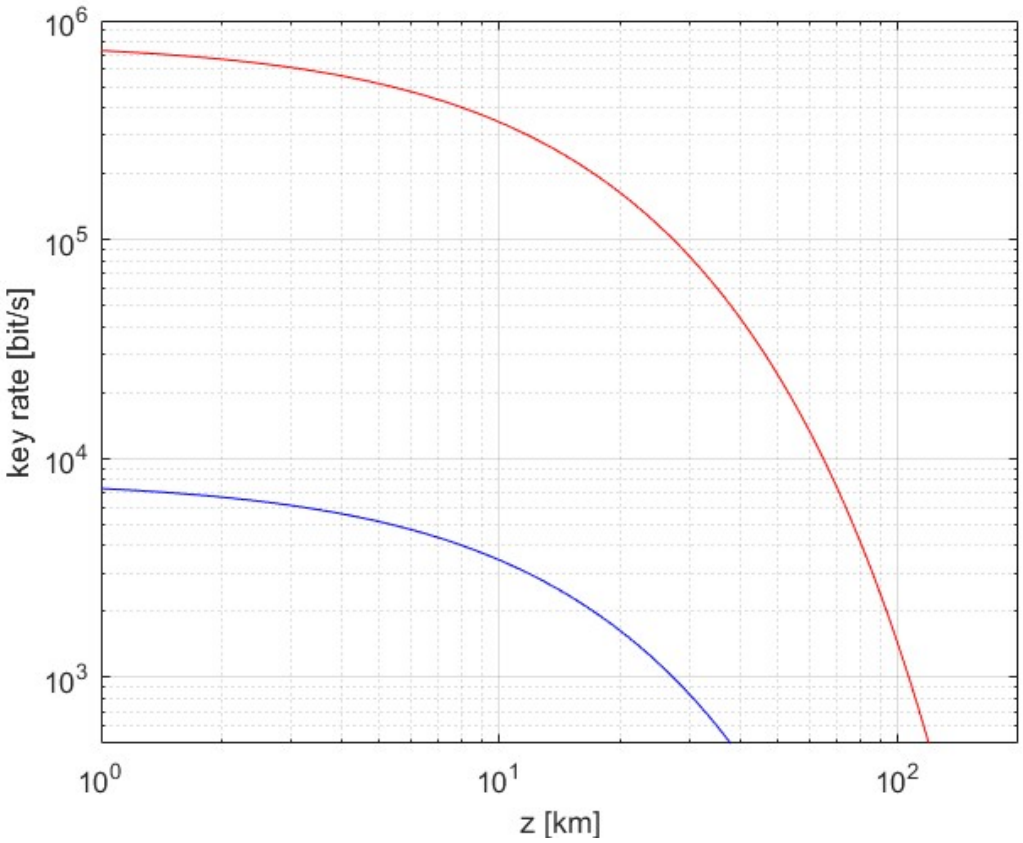

Figure 28 – Comparison of achievable sea level key rate with 1MHz (red line) and 100MHz (blue line) repetition rate

Let now determinate the signal to noise ratio as:

$$\left(S/N\right) = \frac{n_c}{DCR}$$

Where DCR is the Dark Count Rate, in our case 300Hz for the ULN model of the chosen detector, results are plotted in [Figure 29]. Signal to noise ratio at 27km is ~25dB (sea level).

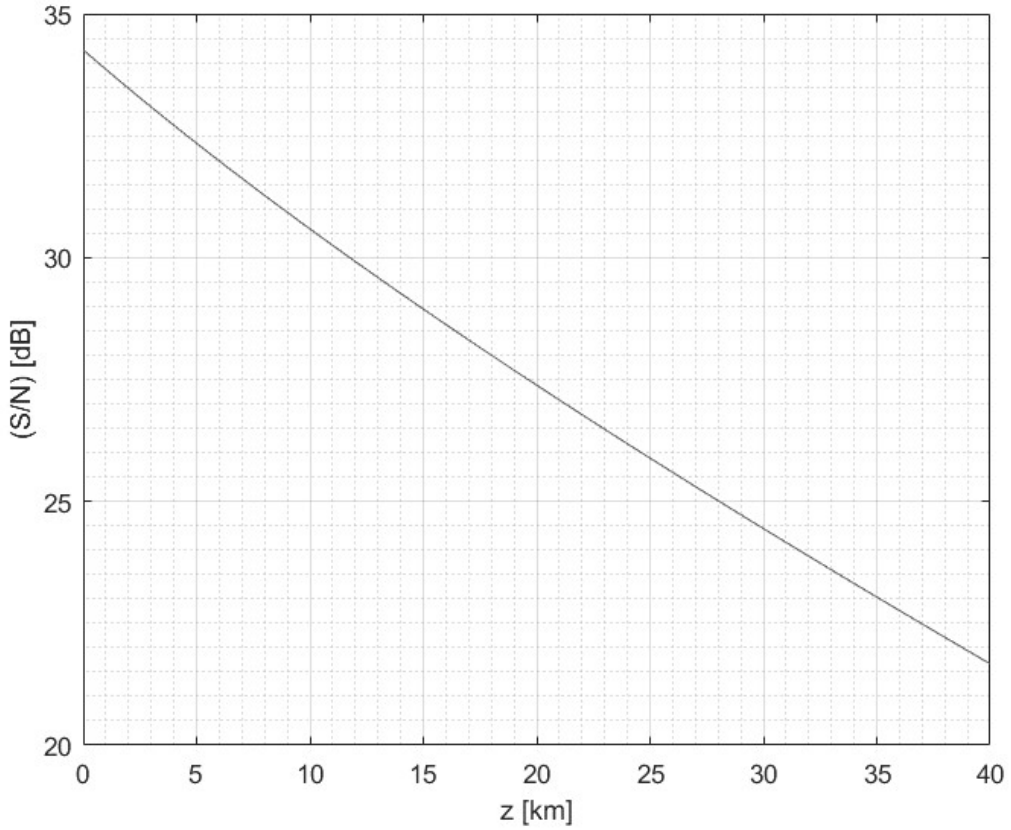

Figure 29 – Relation between signal to noise ratio and distance between Alice and Bob terminals with proposed hardware

3.2.5. Pointing and tracking

The effectiveness of the entire system depend by the alignment of the optical bam between the drones. The possibility to align lasers in fast airborne platform was demonstrated in 2014 by the German Aerospace Center (DLR), that achieved high-rate laser communications from a Panavia Tornado flying at mach 0,7 to a ground station [Figure 30]. In such experiment the Tornado was successfully tracked at a maximum distance of 79 (Moll 2014). The system proposed in this thesis bases the system used by (Liu, Tian, et al. 2020): two pair of custom-built Acquiring, Pointing and Tracking (APT) systems with the same architecture of the DLR's APT but much more compact. However, while Liu's work an entanglement based QKD system is used in this thesis we propose the QKD in his non-entangled version. This choice avoid the usage of an Airborne Entangled-Photon Source with great reduction in weight and complexity.

Figure 30 - Left: Tornado with attached ADT-Pod during the second flight test. The white long box is the ADT-Pod with integrated MLT. (Source: Josef Gietl/Airbus Defense & Space). Upper right: close-up of the ADT-Pod revealing the MLT dome. Lower right: MLT CPA without glass dome during inspection (Source: ViaLight Communications). (Moll 2014)

APT units are composed by a three-axis gimbal that provide the coarse allineation and a telescope. In Liu's work the gimbal is controlled by a PID controller that uses images from a coaxial zoom camera as reference. The target for this camera is an un-collimated 940 nm LD on the TX side [Figure 31]. However due the greater distance involved in the proposed system the coarse allineation will be obtained from attitude and position data of drones and ground units. In Liu's work a 50 mm 90 degree off-axis parabolic mirror (OAPM) is used for this collimation. In this thesis we propose the substitution of the 50mm parabolic mirror with a 150 mm one in order to achieve the desired key rate. For the fine tracking a 637 nm light is used. This light passes through the central hole of the parabolic mirror and the small aperture result in a large divergence angle and thus a sufficient field of view for the fine tracking. The fine tracking loop is integrated on the telescope where a CMOS position-sensitive detector (PSD) control a fast steering mirror (FSM). Before the PSD a dichroic mirror (DM) allow the quantum signal to be collected by the fiber optics (Liu, Tian, et al. 2020). The total weight of ach TX APT is 3,75kg which allow the employment on drones. For the employment on fixed wing fast moving drones the APT turret will be protected from a quartz dome. Additional information are provided in [Table 5].

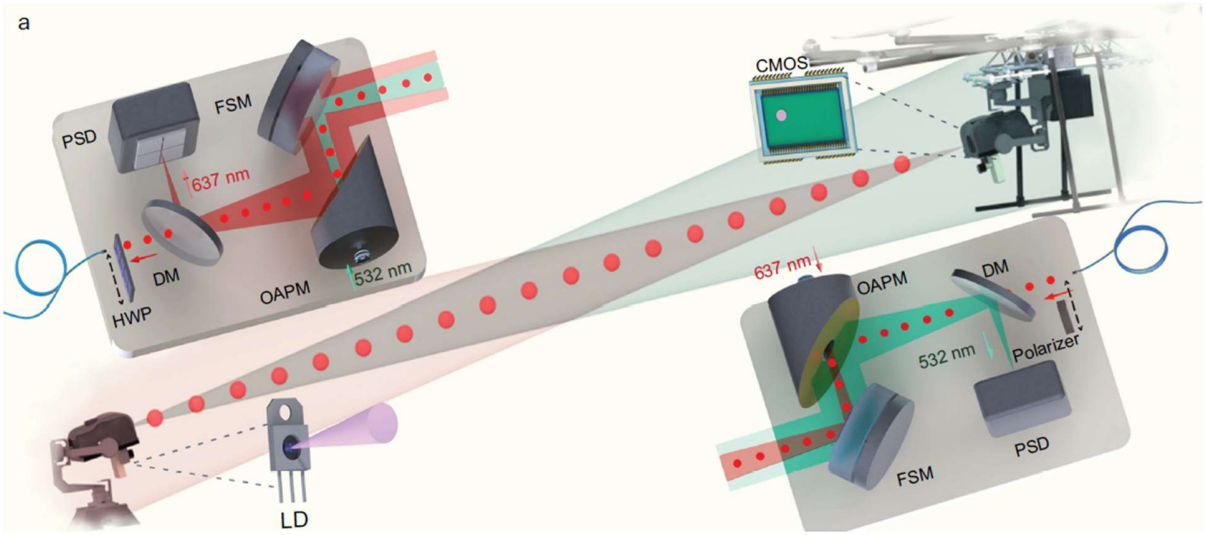

Figure 31 – Acquiring, Pointing and Tracking Device (Liu, Tian, et al. 2020)

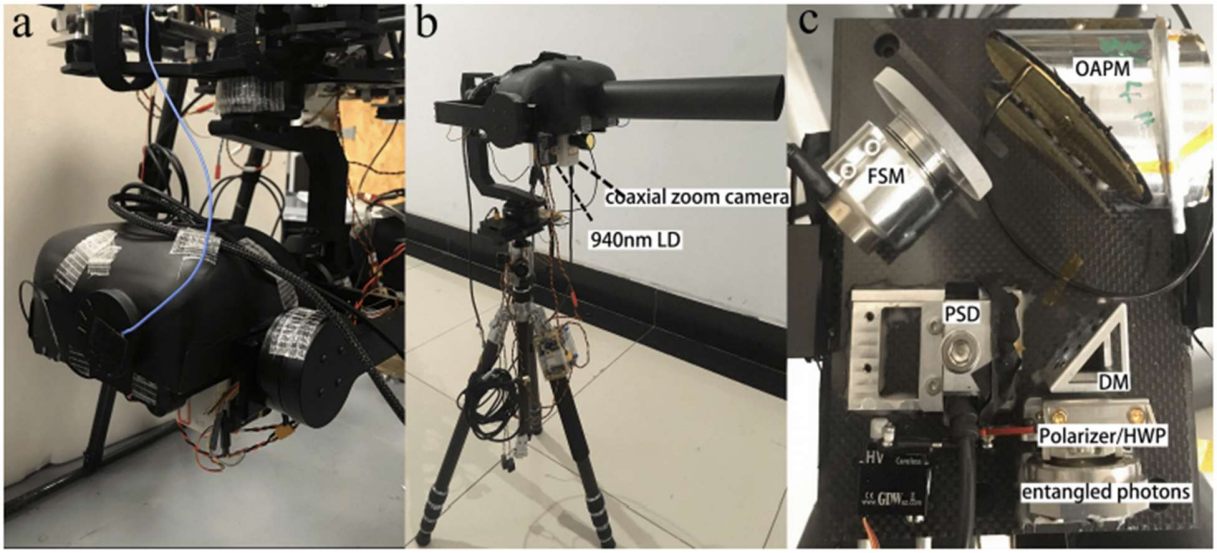

*Figure 32 – **a**: A picture of TX unit. The telescope S-8 platform is sealed in an enclosure to avoid direct exposure to dirt, rain, and background light. **b**: A picture of the RX unit. **c**: A picture of an APT telescope (Liu, Tian, et al. 2020)*

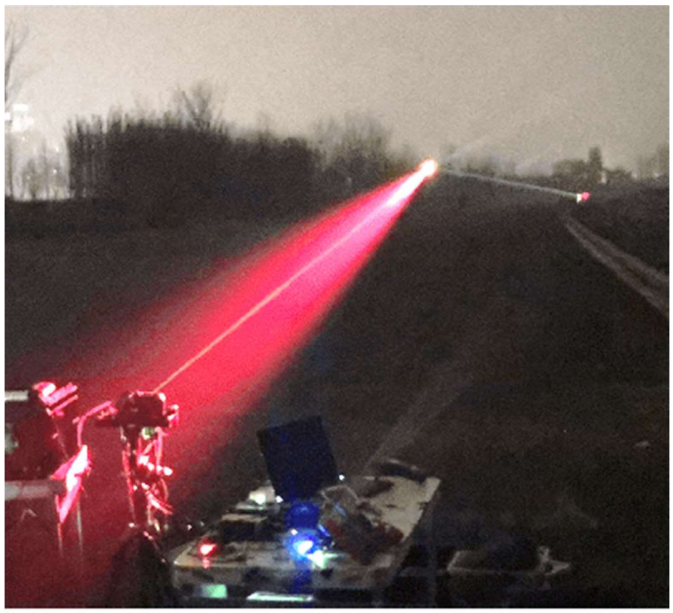

Figure 33 - View of the test of the drone-based system at night (Liu, Tian, et al. 2020)

Components		*Components*	*Components*
Coarse pointing mechanism	Type	3-axis motorized gimbal stage	3-axis motorized gimbal stage
	Tracking range	Yaw：± 45 ° Pitch：± 15 ° （With Roll fixed）	Yaw：± 45 ° Pitch：± 15° （With Roll fixed）
Coarse pointing camera	Type	COMS	COMS
	FOV	0.11 rad × 0.08 rad	0.11 rad × 0.08 rad
	Size & Frame rate	640 × 480 pixels & 60 Hz	640 × 480 pixels & 60 Hz
Coarse pointing beacon laser	Power	2 W	2 W
	Wavelength	940 nm	940 nm
	Divergence	0.35 rad × 0.07 rad	0.35 rad × 0.07 rad
Fine tracking mechanism	Type	PSD	PSD
	FOV	40 mrad × 40 mrad	40 mrad × 40 mrad
	Size & Frame rate	4 mm × 4 mm & 60 kHz	4 mm × 4 mm & 60 kHz
Fine tracking beacon laser	Power	30 mW	70 mW
	Wavelength	532 nm	637 nm
	Divergence	10 mrad	10 mrad
Tracking error		1.15 × 1.33 μm	0.62 × 0.46 μm

Table 5 - Performance of the APT system (Liu, Tian, et al. 2020)

3.3. The SWARM

In the previous sections, we have estimated the total weight of the payload in ~8kg (2,95kg source, 0,65kg detector, 3,75kg APT and 0,65kg for other components) and the power consumption in <100 W. In order to satisfy the mission requirements given in 3.1 we will now describe the chosen architecture of the swarm and the drones that compose it.

3.3.1. Architecture of the swarm

As first QKD swarm application, we have imagined a hierarchical swarm architecture as described in paragraph 1.3 with heterogeneous drones. The swarm will be composed by one or more High Altitude Platform (HAP) with the role of master of the swarm and the specialized in communications with satellites and the ground station and regular SMALL class fixed wing drones for the other nodes of the network. In case of more HAPs each of them will be in command of a subset of the swarm realizing a multilevel swarm. The HAP is necessary in order to provide a large, stable and high endurance platform to communicate with satellites or command center. In fact, the great distance between satellites or command center and drones requires large optics and the finest alignment between platforms in order to make QKD feasible, adding weight and complexity to drones. The high operational altitude of HAPs also provide a great horizon for line of sight communications at the opposite of the low level flying drones. In addition, altitude of HAPs is well above clouds ceiling in very thin air allowing operation with limited amount of atmospheric losses (Fuchs e Giggenbach 2010). For this reasons, employing a specialized platform for the satellite link was considered a feasible solution. Since the HAP will have high payload and computational capability and will fly in secure areas far from threats it was also chosen as maser drone of the swarm allowing lighter and simpler design for the node drones.

The implementation of QKD devices for the HAP, satellites, command center and users could exploit the same devices proposed for the drones. However for HAP, satellites and command center higher performance hardware and bigger optics could be employed in order to realize a stronger link in the first part of the system, while for the user terminals a simplified version of the device realizing only Bob's role will be used in order to obtain a more compact device. Anyway, this type of considerations as well the design of such platform are well beyond the

scope of this thesis and we will not be explored. In the following simulations, the only difference of the satellites and HAP hardware is the optical aperture, set at 0,5m of diameter for both.

With the chosen payload and supposing that users will have hardware with comparable performances, each drone is able to cover persistently and area of ~2300 km^2 or 23 Hectares. However, the nature of the QKD system allow the drone to cover a much greater area flying over users only when the need a key refresh. At the same time, distance between drones of the swarm can be greater than 27 km and two nodes may approach only when a high key rate is necessary. Therefore, the number of drones in the swarm could vary from a couple some dozens depending from the area to be covered and the number of users.

As already mentioned since the BB84 do not provide any authentication mechanism the swarm will necessary be static swarm, with pre-defined members and without the possibility to include new members.

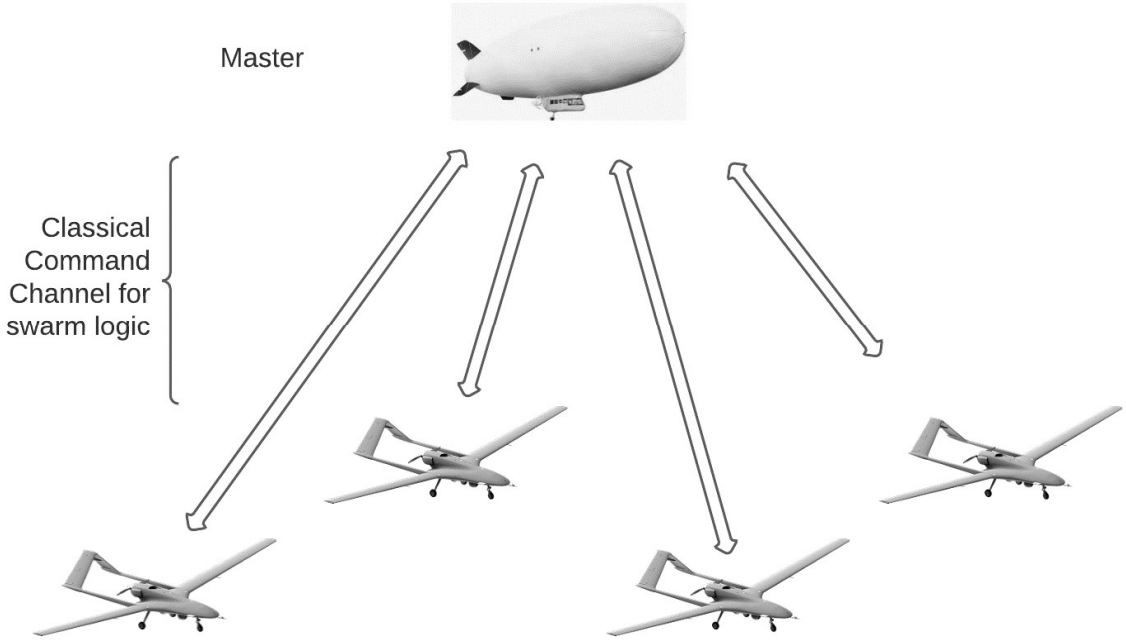

Figure 34 - Architecture of the Swarm

3.3.2. Drones

Since the weight and power requirement of the payload drones of the SMALL (25 – 150 kg) well adapt to our purpose. Smaller drones of the MINI category (2 – 25 kg) have been excluded

since they lack the spare payload capacity needed for the QKD equipment. Larger drones have also been excluded since their high operational cost doesn't allow operating them in large numbers and consequently they are not suitable to operate in swarms.

Precedent works of (Hill, et al. 2020), (Liu, Tian, et al. 2021) and (Liu, Tian, et al. 2020) used multirotors to demonstrate the feasibility of a drone based QKD. However such technology demonstrators are not suited to be employed in real operations. In order to satisfy mission requirements we have chosen the Textron Systems Aerosonde, a fixed wing drone capable of automatic launch and recovery via a pneumatic launcher and a net recover. The Aerosonde has a 3,7m wingspan, a take of weight of 36,5kg and a max payload capacity slightly less than 10kg. It is equipped with a 4Hp motor capable of provide up to 200W for the payload (Textron Systems 2021). The drone is designed for ISR missions and is already equipped with an EO turret that will be replaced by the acquiring and tracking device described in 3.2.5 that is of comparable dimensions [Figure 35]. All the other hardware will be arranged inside. Control software of the drone will be modified as well in order to enable swarm operations. Specification of the drone are detailed in [Table 6].

Figure 35 – View of the Aerosonde EO sensor while the drone is on the launch catapult (Textron Systems 2021). This component will be replaced by the acquiring and tracking device. All the other components will be accommodated inside the drone.

Parameter	*Aerosonde fixed wing*
Payload	Up to 9,1 kg and 200W
Wingspan	3,7m
Ceiling	15.000ft (4.572m)
Range	140 km (75nm)
Weight	36,4 kg
Endurance	>14h
Automated launch and recovery	Hydraulic pneumatic launcher and net recovery
Airspeed	45-65 kt
Engine power	4Hp

Table 6 – Specification of the drone (Textron Systems 2021)

3.4. Benefits & Drawbacks

Benefits of the proposed system are numerous, and vary from the quantum grade security provided to users to the wide area coverage that can be obtained with just a few drones in the swarm. In particular, drones do not have to cover the entire area of operation simultaneously and can move between users on demand keeping short the optical length, minimizing losses and maximizing the key rate. At the same time it is not necessary realize a chain of drones between the HAP and the user since drones can move between the two endpoint of the system. In this case, the key generation process will require an extra time in order to fly drones between the HAP and the user but it will require just two hop with a great reduction in complexity of the network. In addition the swarm based architecture enable all the benefits described in chapter 1 as the intrinsic redundancy, persistence and resilience of the system, the stealthy profile that enable operation in non-permissive airspace end the possibility to cover area that are beyond line of sight of the command center or the HAP. The mobility of the drones also makes difficult to intercept the optical link preventing denial of service attacks. Both the chosen drones and the quantum hardware are commercially available and relatively cheap to acquire when compare to alternatives system for QKD over a wide area.

In particular, the proposed architecture offer a greater key ratio at a lower cost of operation when compared to distributing keys directly from satellites to ground. In fact, early experiments of QKD between satellites and ground reached a maximum key rate of 1,1kbit/s but required a receiver with a telescope of 1m diameter that it is not easily field deployable (Sheng-Kai, Wen-Qi e Jian-Wei 2017).

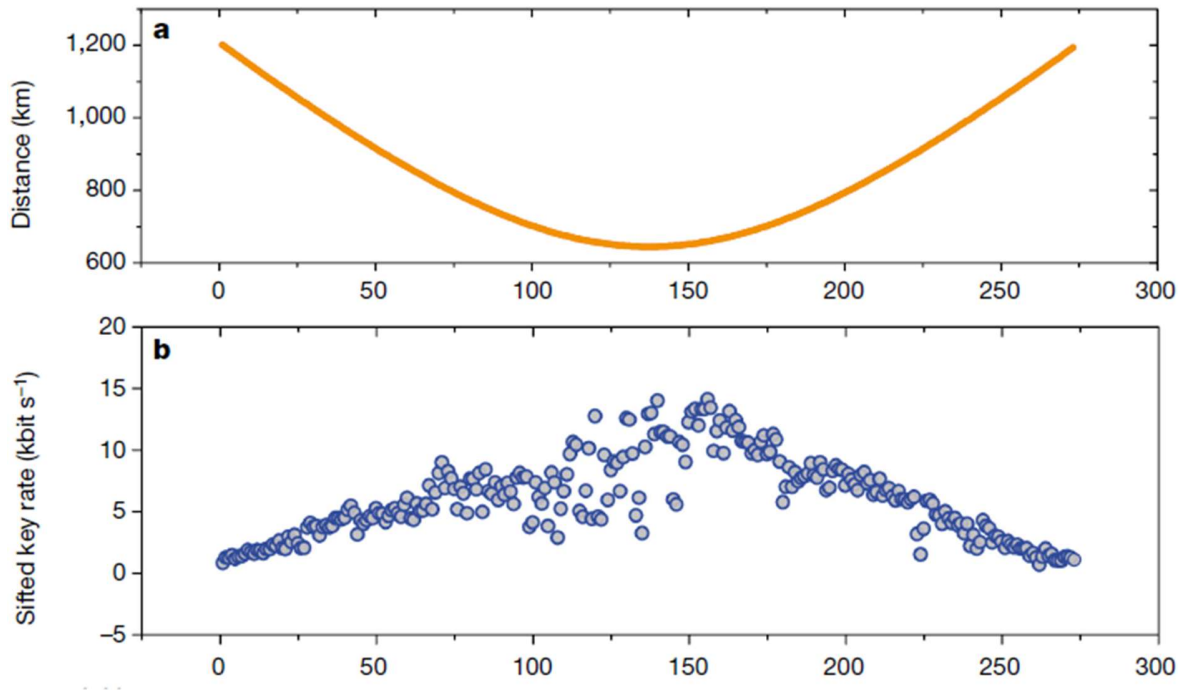

Figure 36 – Relation between key rate distance and time in the (Sheng-Kai, Wen-Qi e Jian-Wei 2017) experiment. Key rate scale does not consider error correction and privacy amplification, useful key rate was about ~17% the indicated value.

If a mobile receiver similar to that proposed in this thesis for drones and users is employed, the key rate will decrease to ~0,1 kbit/s for a satellite in the same 600km orbit [Figure 37]. Considering that, such a satellite will be at a useful height over the horizon for about 5 minutes a negligible amount of key will be generated for each passage of the satellite. At the opposite in the proposed system, the key rate between a satellite in the same 600km orbit and the HAP at 20km is much greater, in the order of ~2,3 kbit/s, since the thicker part of the atmosphere is avoided and bigger optics can be employed. At the same time, the satellite segment of the proposed system is completely avoidable if the command center is in the line of sight of the HAP, further increasing the achievable key rate and eliminating an expensive quantum satellite.

Another benefit of the proposed system over a direct satellite-ground system is that a direct link allow key generation only one user at the time while a in a swarm based system the number of user that can simultaneously generate key is equal to the number of drones. In other words in a swarm based system the total key generation rate scale linearly with the number of drones, in a satellite based system is fixed.

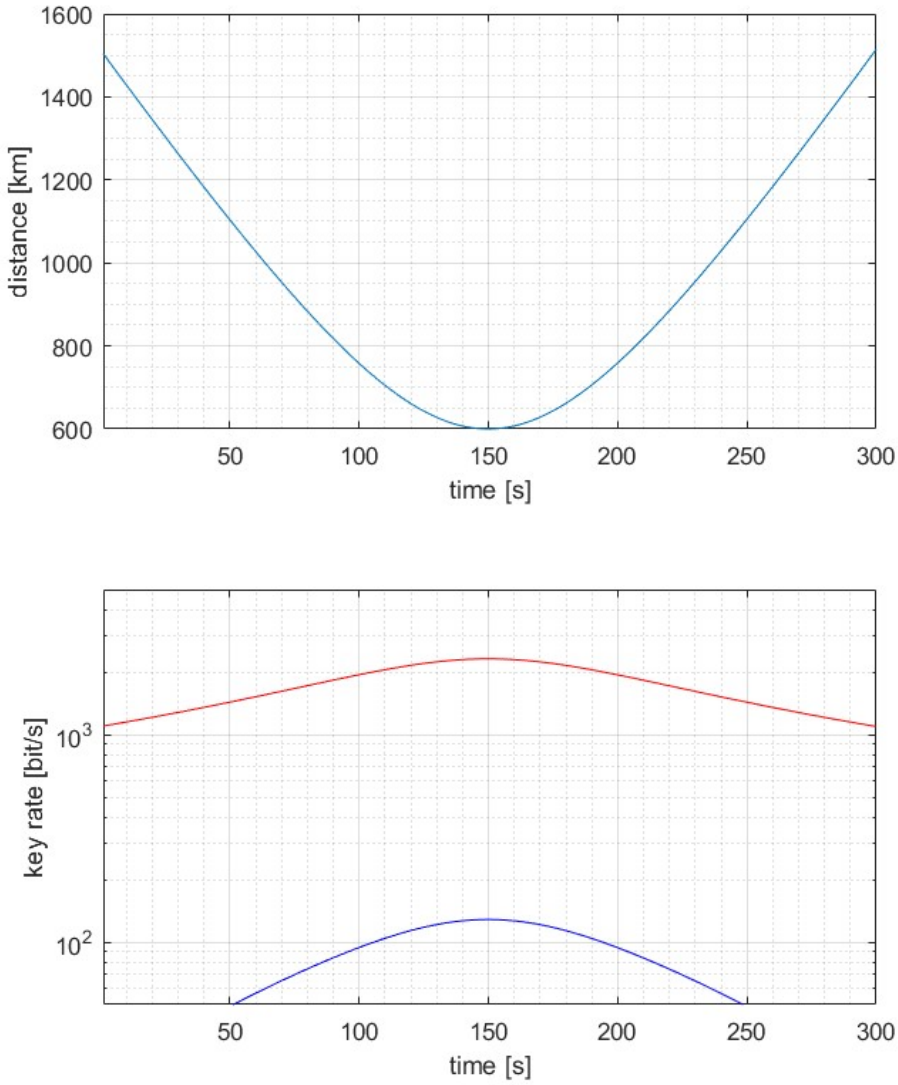

Figure 37 – Distance Satellite-Ground over time (top) and comparison of the achievable key rate of the Satellite-Ground (blue line) and Satellite-HAP (red line) configuration (bottom). Both cases consider a satellite at 600km altitude with an aperture diameter of 0,5m, ground unit consider a 0,15m aperture diameter, HAP a 0,5m aperture diameter and 20km operative altitude. Atmospheric loss is considered negligible over 10km. All the other parameters are the same of the proposed drone hardware.

Drawbacks of the proposed system regard typical limitations of an optical system like susceptibility to atmospheric conditions and the vulnerability to denial of service attack. However, the possibility to fly the drones around and find an unobstructed view of the user is a mitigation to this problem. Since the network employ a trusted node architecture one possible way to attack the network is thought having physical access to one node. However since nodes are onboard the swarm drones this imply the capture of an intact drone. Admitting the feasibility of an in-flight capture of a non-collaborative drone (or of a hijacking), this possibility could be avoided banning a node from the network as soon as its carrier drone is out of the master control. Others drawbacks of the proposed system regard the logistic effort needed in order to operate, manage and maintenance a fleet of drones and user terminals equipped with high-tech quantum hardware.

4. Conclusions

With the hardware proposed in this thesis, we have proposed a multi-drone architecture realizing a quantum network capable of distributing secret keys over a wide area and capable to integrate with other space based quantum networks. The proposed architecture rely on a hierarchical swarm with a HAP in the role of master. The swarm is able to provide a 1kb/s key rate up to 27km and each drone is able cover an area of ~23000 km^2 or 23 Hectares. The optical link can be extended up to 149km between two HAP flying at 20km. Key rate performances can be upgraded if faster detectors will be available in the near future. The swarm architecture provide the redundancy and resilience needed for military application and is able to extend his operation area far beyond the line of sight of the HAP or of the command center. The loss of a done do not compromise the integrity of the network. The same swarm architecture could be employed also for civil application and it is well suited to operate in "urban canyons" where the line of sight between the HAP and the users could be obstructed. The presence of a HAP dedicated to the satellite link offer major benefits especially when compared with a satellite-ground direct approach. Such benefits vary from the higher key rate achievable to the possibility of generate simultaneously over multiple users, achieving a further higher cumulative key rate. All the proposed hardware is commercially available and can be built with existing hardware with minor changes.

4.1. Satellite quantum Network

The proposed system allow to establish a QKD protocol also with a satellite, however the low revisit time that a single satellite in low orbit can provide is not sufficient to have a continuous coverage of the operational area. For this reason, a satellite constellation realizing a satellite quantum network should be considered if a global scale quantum network with continuous coverage is needed. All the optical hardware proposed in this thesis is suitable to be employed on such satellite network with minor modifications although the greater distances in space will require bigger optics. The architecture of the constellation will be similar to the architecture of the swarm with satellites instead of drones. In addiction satellites will travel along fixed orbits and the role of master drone will not be needed. Benefits of such system will be impressive since optical signals can propagate in the vacuum of space with minimum loss. A satellite

network will be capable of implement a hop-by-hop quantum network on a global scale. This will eliminate the delay in key generation due to the movement of the satellites from the Command Centre Line Of Sight to the HAP Line Of Sight (Figure 38) enabling instant generation in every point covered by the satellite constellation.

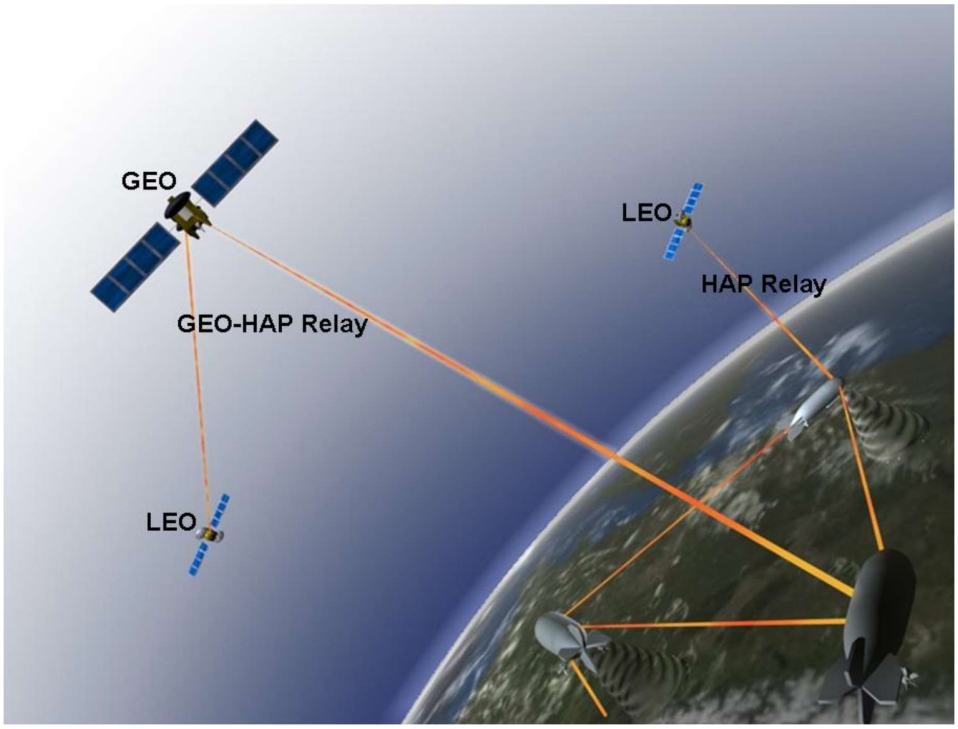

Figure 38 – Illustration of Multi Satellite Network (Fuchs e Giggenbach 2010)

Bibliography

AeroVironment. *SWITCHBLADE 300.* 2021. https://www.avinc.com/tms/switchblade.

Akram, Raja Naeem, et al. "Security, Privacy and Safety Evaluation of Dynamic and Static Fleets of Drones." *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC).* St. Petersburg, FL, USA, 2017.

Alléaume, R., et al. "Using quantum key distribution for cryptographic purposes: A Survey." *Theoretical Computer Science*, 2014: 560 61-81.

Arqiulla, John, and Davld Ronfeldt. *Swarming & The Future of Conflict.* RAND, 2000.

Barca, Jan Carlo, and Y. Ahmet Sekercioglu. "Swarm robotics reviewed." *Robotica*, 2013: Volume 31 / Issue 03 / May 2013, pp 345 - 359.

Bennett, Charles H., and Gilles Brassard. "Quantum Cryptography: Public Key Distribution and Coin Tossing." *International Conference on Computers, Systems & Signal Processing.* Bangalore India, 1984. Vol 1 of 3, pages 175 - 179.

Bovino, Fabio Antonio. "Introduzione alla crittografia quantistica." In *Optoelettronica e Fotonica*, by Antonello Cutolo, 583-688. Roma: ARACNE Editrice, 2014.

Bovino, Fabio Antonio, et al. "Practical Quantum Key Distribution Using Polarization Entangled States." *International Journal of Quantum Information*, 2005: 3:1 1-6.

Businessinsider. feb 4, 2021. https://www.businessinsider.com/drone-industry-analysis-market-trends-growth-forecasts?IR=T#:~:text=Drone%20Market%20Stats%20%26%20Sales&text=Sales%20of%20US%20consumer%20drones,the%20commercial%20and%20government%20sectors.

Cevik, Polat, Ibrahim Kocaman, Abdullah S. Akgul, and Barbaros Akca. *The Small and Silet Force Multiplier: A Swarm UAV - Electronic Attack.* Springler Science, 2012.

Coecke, Bob. "The Logic of Entanglement." (Springer International Publishing) 2004.

Defendtex. *Defendtex Unmanned Aerial Vehicles.* 2021. https://www.defendtex.com/uav/.

DJI. *DJI Phantom 4 pro v2.0.* 2021. https://www.dji.com/it/phantom-4-pro-v2/specs.

Dorri, Ali, Seyed Reza Kamel, and Esmail kheyrkhah. "SECURITY CHALLENGES IN MOBILE AD HOC NETWORKS: A SURVEY." *International Journal of Computer Science & Engineering Survey*, 2015: Vol.6, No.1.

Dür, W., H. J. Briegel, J. I. Cirac, and P. Zoller. "Quantum repeaters based on entanglement purification,." *Phys. Rev.*, 1999: A 59, 169.

Erdemli, Mustafa Gokhan, Edward Fisher, and Wolfgang Baer. *General use of UAS in EW environment--EW concepts and tactics for single or multiple UAS over the net-centric battlefield.* Monterey, California: Naval Postgraduate School, 09 2009.

Fei, Yang-Yang, Xiang Dong Meng, Ming Gao, Hong Wang, and Zhi Ma. "Quantum man-in-the-middle attack on the calibration process of quantum key distribution." *Scientific Reports*, 2018: 8. 10.1038.

Fuchs, Christian, and Dr. Dirk Giggenbach. "Optical Free-Space Communication on Earth and in Space regarding Quantum Cryptography Aspects." In *Quantum Communication and Quantum Networking. QuantumComm 2009. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 36*, by Sergienko A., Pascazio S. and Villoresi P., 82-95. Berlin: Springer, 2010.

Garcia-Aunon, Pablo, Jaime del Cerro, and Antonio Barrientos. "Behavior-Based Control for an Aerial Robotic Swarm in Surveillance Missions." *Sensors*, 2019.

Gisin, Nicolas, Gre´goire Ribordy, Wolfgang Tittel, and Hugo Zbinden. "Quantum cryptography." *REVIEWS OF MODERN PHYSICS*, 2002: 74 145-195.

Henniger, Hennes, and Dirk Giggenbach. "AVIONIC OPTICAL LINKS FOR HIGH DATA-RATE COMMUNICATIONS." *25TH INTERNATIONAL CONGRESS OF THE AERONAUTICAL SCIENCES.* 2006.

Hill, Alexander D., Joseph Chapman, Kyle Herndon, and Christopher Chopp. "Drone-based Quantum Key Distribution." *2020 Conference on Lasers and Electro-Optics (CLEO).* San Jose, CA, USA, 2020. pp. 1-2.

ID Quantique . *ID120 Visible Single-Photon Detector.* 2021. https://www.idquantique.com/quantum-sensing/products/id120-visible-single-photon-detector/.

ID Quantique. *ID 3000 Series – Picosecond Lasers.* 2021. https://www.idquantique.com/quantum-sensing/products/id-3000-picosecond-lasers/.

Ilachinski, Andrew. *AI, Robots, and Swarms.* CNA, 2017.

Insitu. *EO950.* 2021. https://www.insitu.com/products/eo950.

Kwiat, Paul G., and Daniel J. Gauthier. U.S. Patent 15/434,313. 2017.

Lachow, Irving. "The upside and downside of swarming drones." *Bulletin of the atomic scientist*, 2017: Vol. 73, NO. 2, 96-101.

Leonardo. "Britecloud Swarming Drones capability." Roma, 2020.

Leonardo. "Leonardo Electronic Warfare capability at the heart of Royal Air Force swarming drones capability demonstration." October 2020.

Liu, Hua Ying, Xiao Hui Tian, Changsheng Gu, and Pengfei Fan. "Drone based entanglement distribution towards mobile quantum networks." *National Science Review*, 2020: n.7 921–928.

Liu, Hua Ying, Xiao Hui Tian, Changsheng Gu, and Pengfei Fan. "Optical Relayed Entanglement Distribution Using Drones as Mobile Nodes." *PHYSICAL REVIEW LETTERS*, 2021: 126.

Ma, Lijun, Tiejun Chang, Alan Mink, Oliver Slattery, Barry Hershman, and Xiao Tang. "Experimental Demonstration of a Detection-Time-Bin-Shift Polarization Encoding Quantum Key Distribution System." *IEEE COMMUNICATIONS LETTERS, VOL. 12, NO. 6*, 2008.

Mermin, David D. *Quantum Computer Science An Introduction.* Cambridge: Cambridge Universiy Press, 2007.

Moll, Florian & Mitzkus, Wolfgang & Horwath, Joachim & Shrestha, Amita & Brechtelsbauer, Martin & Navajas, Luis & Souto, Alberto & Gonzalez, Dionisio M. "Demonstration of high-rate laser communications from fast airborne platform: Flight campaign and results." *IEEE Journal on Selected Areas in Communications · September 2015*, October 2014: DOI: 10.1109/JSAC.2015.2433054.

Nauerth, Sebastian, et al. "Air to Ground Quantum Communication." *Nature Photonics*, 2013: vol 7, 382-386.

Quantum Flagship. *Quantum Key Distribution (QKD).* 2021. https://qt.eu/discover-quantum/underlying-principles/quantum-key-distribution-qkd/ (accessed 2021).

Raytheon Missiles and Defense. 2021. https://www.raytheonmissilesanddefense.com/capabilities/products/mald-decoy.

Raytheon Missiles and Defense. "Raytheon Deploys Miniature Air Launched Decoys From C-130 Cargo Aircraft." May 2011.

Rinaldi, Alessandro, Domenico Accardo, Luca Viarengo, Antonio Mele, and Vittorio Calligaris. "Application and Countermeasures for Swarms of Small Unmanned Aircraft Systems." Napoli: Università degli Studi di Napoli “Federico II”, 2020.

Scarani, Valerio, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dusek, Norbert Lutkenhaus, and Momtchil Peev. "The Security of Practical Quantum Key Distribution." *Review of Modern Physics*, 2009: 81(3):1301.

Scharre, Paul. *Robotics on the Battlefield Part II: The Coming Swarm.* Center for a New American Security, 2014.

Sheng-Kai, Liao, Cai Wen-Qi, and Pan Jian-Wei. "Satellite-to-ground quantum key distribution." *Nature*, 2017: volume 549, pages43–47.

Shor, Peter W. "Algorithms for Quantum Computation: Discrete Logarithms and Factoring ." *Proceedings 35th Annual Symposium on Foundations of Computer Science,*, 1994: pp. 124-134.

Stallings, William. *Cryptography and Network Securety Principles and Practice.* Prentice Hall, 2011.

Stimson, George W., Hugh D. Griffiths, Chris J. Baker, and Dave Adamy. *Stimson's Introduction to Airborne Radar.* Edison NJ: SciTech Publishing, 2014.

Textron Systems. *Textron Systems Aerosonde Small Unmanned Aircraft System.* 2021. https://www.textronsystems.com/products/aerosonde.

Ursin, R., et al. "Entanglement-based quantum communication over 144 km." *Nature Physics* , 2007: volume 3, pages481–486.

US Air Force. *Scan Eagle.* 2011. http://www.af.mil/information/factsheets/factsheet.asp?id=10468.

US Department of Defense. *REQUEST FOR INFORMATION FOR ORGANIC PRECISION FIRE-INFANTRY (OPF-I) LIGHT SYSTEM CAPABILITY.* Quantico, 2020.

Vandersypen, Lieven M. K., Matthias Steffen, Gregory Breyta, Costantino S. Yannoni, Mark H. Sherwood, and Isaac L. Chuang. "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance." *Nature*, 2001: 414 (6866): 883–887.

Verini Supplizi, Sofia, Domenico Accardo, Antonio Mele, and Vittorio Calligaris. "Swarms of Small UAS as Countermeasure against Ground-based Radar Detection." Napoli: Università degli Studi di Napoli Federico II, 2021.