Enhancement of AGT Telecommunication Security using Quantum Cryptography

Quoc-Cuong Le, Patrick Bellot

***Abstract*— Aeronautical Telecommunication Network (ATN) is the network used by the Air Traffic Authorities, the *Air Traffic Controllers* (ATCo), the aircrafts and all *Ground Stations* (GS) to communicate voice and data. This paper describes how the ATN can be secured by using *Quantum Cryptography* (QC), either fiber-based QC or free-space QC, instead of classical PKI. ATN is a good example of special-purpose dedicated networks that could be secured by QC.**

***Index Terms*— Quantum Key Distribution (QKD), Aeronautical Telecommunication Network (ATN), ATN security, quantum network, free space, satellite**

I. Introduction

The objective of our study is related to the security of *Air-Ground Telecommunications (AGT)* in the dangerous after 9/11 world where one may expect serious threats to aircraft safety. We may be concerned by attack on confidentiality, integrity and availability of telecommunications. A wrong message or the absence of message may have strong consequences for aircraft safety. Eavesdropping attempts may inform ill-intentioned actors. These hard facts plead for a permanent search of a maximal AGT security.

II. Aeronautical Telecommunication Network

Air transportation communications are handled by the *Aeronautical Telecommunication Network* (ATN). The ATN is incrementally built using existing communication networks ([1]). It is a data communication network.

- It provides a common communication service for all *Air Traffic Services Communication* (ATSC) and *Aeronautical Industry Service Communication* (AINSC). Communications can be either Ground/Ground or Air/Ground.
- It integrates and uses existing communication networks and infrastructures if possible. Investments in existing leased networks, *Common ICAO Data Interchange Network* (CIDIN) and X25 networks, must be preserved.
- It must meet security and safety requirements of ATSC and AINSC applications and accommodate the different levels of service required by each ATSC and AINSC application.
- It must provide ATN users with a robust and reliable communication service. Its design ensures high availability because there is no single point of failure and because it permits multiple alternative routes to the same destination with dynamic switching between alternatives, for both fixed and mobile communication.
- It must support mobile systems since an aircraft is basically mobile. It must support a wide variety of mobile communication networks including *Aeronautical Mobile Satellite Service* (AMSS), *VHF Digital Link* (VDL) and Mode S. It must be possible for any system to communicate with aircraft equipment all over the world.

The services provided by the ATN are implementing the OSI Transport Service referred as ISO 8072. In order to build ATN applications, ATN proposes common functional components in an architecture known as the *Upper Layer Architecture* (ULA) based on the layered OSI Reference Model. There exist seven layers. Two types of entities are identified:

- *End-systems* such as computers using the 7 layers.
- *Intermediate systems* such as routers using the 3 lower layers.

The seven OSI layers are listed from the upper to the lower:

- *Application Layer*: semantics of end-to-end exchanged information;
- *Presentation Layer*: syntax of end-to-end exchanged information;
- *Session Layer*: format of end-to-end exchanged information;
- *Transport Layer*: end-to-end flow control and information exchange;
- *Network Layer*: establish, maintain and terminate switched connections;
- *Data Link Layer*: synchronization and error control over the physical link;
- *Physical Layer*: management of the physical link.

The three upper layers provide common functions that are used for the establishment and release of connection and for the encoding of information.

The *Communications, Navigation and Surveillance / Air Traffic Management* (CNS/ATM) Applications that has been specified for the first phase of ATN are:

- *Context Management* (CM) provides a mean to find out communications services within a given flight region, and for a ground system or controller to direct an aircraft's Context Management Application to contact a different flight region.
- *Automatic Dependent Surveillance* (ADS) is designed to give automatic reports from an aircraft to a ground system. This information is provided on demand and in an

This work has been funded by Eurocontrol CARE project QCRYPT, `www.eurocontrol.int`, by IST project SECOQC, sub-project NET, `www.secoqc.org`, and by a grant from AUF-IFI, `www.ifi.edu.vn`.

The authors are at the École nationale supérieure des télécommunications. Département Informatique et réseaux, 46 rue Barrault, 75013 Paris, France. Email: {qle, bellot}@infres.enst.fr

emergency. Position, trajectory and meteorological data are typical uses of this service.

- *Controller-Pilot Data Link Communications* (CPDLC) provides a mean for two-way messages oriented communications including a set of clearance-information-request messages corresponding to current voice phraseology employed by ATCo.
- *Flight Information Services* (FIS) can support a variety of information services, providing information about the ground to an aircraft. This can include information about an airport, such as runways in use and weather conditions.
- *ATS Interfacility Data Communication* (AIDC) provides a mean for the exchange of ATC information between Air Traffic Services Units in support of ATC functions, including notifications of flights approaching a Flight Information Region boundary, co-ordination of boundary crossing conditions, and transfer of control.
- The *Aeronautical Message Handling System* (AHMS) is a mean for the exchange and distribution of message-oriented traffic between Air Traffic Services Units. It is an AFTN replacement that may be used to provide new messaging services including E-Mail and Electronic Data Interchange. It is based on ITU recommendation X.400.

III. Security for ATN communication

The security of ATN is a crucial matter. For instance, *Aircraft Communications And Reporting System* (ACARS) *Data Link* (DLK) must be secured. *Inter Domain Routing Protocol* (IRDP) must be secured too. Airlines companies require secrecy too for economic reasons.

ATN may be secured by using classical cryptography which provides the so-called *cryptographic security*. A such security is based on the assumed but unproven intractability of some mathematical problems related to prime numbers or elliptic curves.

The Figure 1 shows the overview of ATN network. We can consider two types of communications in ATN: Ground/Ground (G/G) and Air/Ground (A/G). ATN is an Internet v4 network with fixed and mobile entities. In fact, ATN could switch to IPv6 in the future in order to provide IP addresses to all equipments on ground and on aircraft. *International Civil Aviation Organization* (ICAO) has determined that denial of service (DoS), masquerade, and modification of information are the primary threats in ATN's communications. ICAO has also summarized the main Security Requirements for ATN as the following:

- Authentication of Message Source
- Message Integrity Check
- Authenticate the source of routing informations

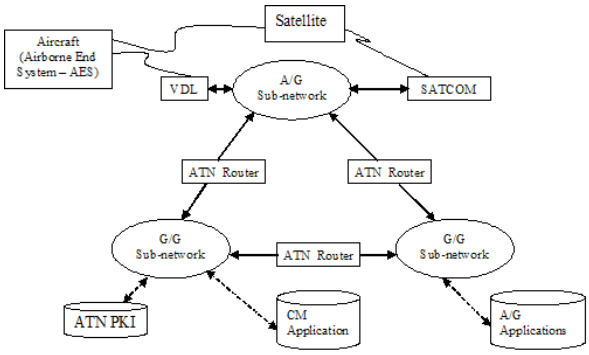

Fig. 1. ATN Network

Example of a secured ATN session with PKI. When an *Airborne End System* (AES) wants to communicate with an Air/Ground Application at a *Ground Station* (GS), e.g. the *Controller-Pilot Data Link Communication* (CPDLC) Application, AES and GS will cooperate to execute a basic scenario:

- **Step 0:** Initialization of ATN's PKI services for ATN entities.
- **Step 1:** AES creates a CM-Logon CPDLC Request and sends it to CM Application.
- **Step 2:** CM Application sends a CM-Logon CPDLC Response back to AES.
- **Step 3:** AES and CPDLC Application invoke ATN's PKI Services to compute a common secret Session Key.
- **Step 4:** AES and CPDLC Application protect messages by using this Session Key.

Security and confidentiality of ATN is now planned to be handled by using classical Public Key Cryptography ([2], [3]). However, public key cryptography is not proven to be unconditionally secure. No one can claim that heuristics do not exist to break Public Key Cryptography with high probability. Moreover, if Quantum Computers are built in a few years, then public key cryptography would be in great danger. The birth of Quantum Computers would be the death of public key cryptography because Quantum Computers support efficient algorithms, Shor's algorithm for instance, to solve the mathematical problems on which public key cryptography relies.

Public key cryptography necessitates a *Public Key Infrastructure* (PKI). This is a set of heavy hierarchical administrative tools. Any security failure in one element will compromise the security of the whole system. Thus, PKI is likely to be managed in well-trusted operator's areas. Moreover, PKI will increase remarkably the overhead on band-limited channels. For example, a classical X.509 certificate is about 20Kb. Another typical element of PKI is the *Certificates Revocation Lists* (CRLs), which are very large and must be dispatched to all parties.

Quantum Cryptography (QC) provides unconditional security relying on the quantum physics law. Such a security is called *information theoretic security* because it is proved by Shannon's theory of information. However, any solution for

improving the planned security of ATN must be done inside the framework of ATN. It must take into account the existing infrastructure and the developing costs of new solutions. The existing infrastructure must be re-used. And any proposed solution that uses QC to secure ATN must be incremental.

IV. Quantum Cryptography - QC

Security is based on **secret sharing** either a secret algorithm or a secret key to be used with public encryption algorithms.

- A secret can be shared by **physical means**. E.g.: using the army to share a key between White House and Kremlin.
- A secret may be shared by **algorithmic means**. That is Public Key Cryptography.
- A secret may be shared by **quantum means**. That is Quantum Key Distribution.

Quantum Cryptography ([4]–[6]) is an emerging technology that could, in a few years, provide a totally secure Internet architecture. The most interesting point is that QC uses single photons instead of electrical or optical signals to obtain secured communications. However, QC also have many of backdraws compared of normal communications as very low rate, difficulty in the manipulation of signals. Therefore, QC can not totally replace classical methods of communications. In fact, with nowadays technologies, QC only proposes an alternative and a complement of classical Public Key Cryptography.

The most famous application of QC now is *Quantum Key Distribution* (QKD) that allows an unconditionally secure transmission of encryption keys. Although the record of wired QKD distance now is 150 km, it will be expected the most interesting perspective: specialized Internet optical fiber architecture and protocols based on QC ([7], [8]).

Beside of the wired applications, the advantages of QC may be exploited in (air) free-space telecommunications. In these cases, photons are transmitted in the air by faint pulses laser beams. Works have been conducted in Europe and USA with significant results.

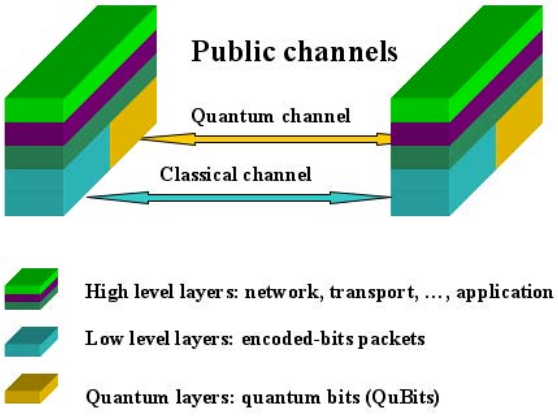

Fig. 2. Two public channels in QKD

In general, QKD is a technique which allows two endpoints to share a secret key. This secret key would be used with an unbreakable encryption algorithm, such as Vernam (one-time pad) cipher, to encode the communication.The basic QKD protocol is named BB84. QKD uses a classical open channel and a quantum channel which may be an optical fiber, or a free-space faint pulses laser beam, or any physical device able to transmit unaltered quantum states (see Figure 2). Quantum Physics laws instead of unproven mathematical assumptions guarantee the security: *Heisenberg's uncertainty principle* and *Non-cloning theorem*. With QKD, any eavesdropper (spy) will be detected because its interventions always perturb transmitted quantum states.

QKD relies on quantum equipments and specialized algorithms. Fiber-based QKD technology is quickly evolving. One year before, the maximum distance of QKD obtained with optical fiber technology was 70 km. Nine months later, it is 150 km ([9]) and many experiences using QKD to secure Internet links have been done. With QKD, we have two public channels: a classical channel to transmit ordinary bits and a quantum channel to transmit quantum states. Both channels are public and used to distill a common secret encryption key that is used to establish a secured communication.

Year	Distance	Where
1989	32 cm	IBM, USA)
1996	150 m	Baltimore, USA
1998	1 km	Los Alamos, USA
2000	1.6 km	Baltimore, USA
2001	1.9 km	QinetiQ, UK
2002	10 km	Los Alamos, USA
2003	23.4 km	Munich, Germany

TABLE I
The progress of free-space QKD technology

Free-space QKD uses a faint pulses laser beam. The progress of free-space QKD is shown on the Table I ([10]–[14]). The 2003's results and theoretical calculations allow us to hope a distance of 1600 km for Ground/Space QC. Thus, we can imagine QC based on a satellite network. It is the *Low Earth Orbit* (LEO) satellites at the altitude of 800 km. Embedded payload may be 3 to 5 kg and 10 to 30 cm optics. On the Earth, it uses a 50 to 100 cm optics. The satellites network depends on the payload: from 7 to 43 satellites.

QC can achieve unconditionally secured communication links over restricted distances depending on the used technology ([15]–[20]). The big progresses are made and other alternatives to the initial BB84 have been studying: *Quantum Continuous Variables* (QCV) and entangled photons (EPR-pairs). Therefore, we may assume that the distances will be enlarged! In this paper, we assumed that all foreseeable QKD technologies have been developed. For instance, we assumed Free-Space Satellite-based QKD that had not been experimented. We looked at the incremental insertion of QKD in the ATN. It means that we looked where PKI can be locally replaced by *Quantum Confidentiality Key Infrastructure* (QCKI) which would be the provider of confidential encryption keys for two arbitrary endpoints.

V. Quantum Key Distribution

The very efficient encryption algorithms exist and some have been proved to be unbreakable by Shannon's information theory. For instance, Vernam cipher, also called the one-time pad, assumes that two endpoints share a key as long as the message to be encrypted. Vernam encryption is just do an XOR, i.e., addition modulo 2, between the clear message and the encryption key. The corresponding decryption is also performed by doing an XOR, but between the encrypted message and the encryption key. Reading the encrypted message does not give any information about the clear message. However, the required length of key, and the fact that the encryption key must be changed after each use, rule out Vernam cipher for an everyday usage.

The modern *Data Encryption Algorithms* (DEAs) such as 3-DES, AES, and elliptic curves cryptosystems allow to have a good secure encryption using fixed-length keys. They are considered as "unbreakable". But all these algorithms assume that a key is shared between the two endpoints. Thus, security is a problem of key distribution.

A. Classical Key Distribution

Nowadays, key distribution can be done by using *Public Key Infrastructure* (PKI). This would be the case of Aeronautical Telecommunication Network. PKI is a security system which allows the distribution and management of keys using asymmetric encryption algorithms. But asymmetric encryption is subject to serious attacks with brute force, with progress in mathematics or with the possible creation of quantum computers. An encrypted message now currently unbreakable may be broken in ten years, or tomorrow, delivering a posterior secret.

In the general case, PKI assumes many trustable third parties. All is good enough for most of applications where there is no big business or industrial stake, no far future concerns, and when national security is not involved. For instance, one may admit a PKI system when it distributes certificates and keys for software download or for restricted electronic payment. But recent affairs[1], involving the Echelon electronic communications surveillance systems have proved that governments do not hesitate using military power to serve their own private companies. In recent UNO dispute on Irak, one has learned that the same techniques have been used by governments against UNO and opposite diplomacy. Perfect classical digital confidentiality needs huge organization and means. Quantum Cryptography may provide a good alternative solution ([21]).

The questions are: do we trust encryption algorithms that are potentially breakable? Which PKI can we trust? Even trustable, your PKI system may not be secure enough since a single break in a such complex system could open a large breach in the security.

B. Quantum Key Distribution

Quantum Key Distribution (QKD) allows two endpoints to share with total confidentiality a key which will be used in symmetric encryption algorithms. S.Wiesner described the first idea of QKD in the 70s. He officially published in 1983. It has been fully developed and finalized by Gilles Brassard and Charles Bennett in 1984, hence known as the BB84 protocol.

BB84 Basics

The quantum law underlying QKD is *Heisenberg principle of uncertainty*: two non-commuting observables of a quantum system cannot be both accurately measured. It ensures that it is not possible to clone a quantum system (*no-cloning theorem*). Otherwise, it would be possible to measure one observable on the original and the other observable on the clone.

The BB84 protocol is simple enough to be understood by a non-specialist of quantum physics. Photons can have a *rectangular* or a *diagonal* polarization, two non-commuting observables. Rectangular polarization can be horizontal noted "$\rightarrow$" or vertical noted "$\uparrow$". Diagonal polarization can be left noted "$\nwarrow$" or right noted "$\nearrow$". A physical measuring device can observe rectangular or diagonal polarization but not both. Moreover, if a physical device tries to measure diagonal polarization on a photon that is rectangular-polarized, then it gets a random result: either left or right, each with a probability of 50% . And the act of measurement changes the original state of the photon to be the result of the measurement. The situation is symmetric if a physical device measures rectangular polarization of a photon that is diagonally polarized.

Session keys are made of bits, 0 or 1. In QKD, we agree that: bit 0 can be encoded either by a horizontal ("$\rightarrow$") or a left ("$\nwarrow$") polarization of a photon and bit 1 can be encoded either by a vertical ("$\uparrow$") or a right ("$\nearrow$") polarization of a photon. Such an encoded bit is called a *quantum bit* or *qubit*. Transmitting a key becomes transmitting a sequence of polarized photons.

BB84 Key Exchange

Alice and Bob are connected using two channels. The first is a quantum channel, typically un optical fiber. The second is a classical channel, typically an Internet link.

1) First, Alice generates a random sequence of bits called the raw key. Randomness is crucial. For each bit, Alice randomly chooses to encode its value using either the rectangular or the diagonal basis. And she sends the photons, one after the other, to Bob using the quantum channel.
2) For each received photon, Bob randomly chooses to measure it using either the rectangular or the diagonal basis. Because Alice's and Bob's choices of basis are random, the probability that they use the same basis for a given photon is 50%. If they use the same basis for a given photon, then Bob gets the right decoded bit with a very high probability. If they do not use the same basis, then Bob gets a random result.
3) Then Bob uses the classical channel to tell Alice which basis he used for the measurements. And Alice, also using the classical channel, answers which basis are correct according to her own encoding choices, i.e. when they used the same basis. These communications are public.

[1] `http://news.bbc.co.uk/1/hi/world/europe/820758.stm`

4) When they used the same basis, the bit encoded by Alice is identical to bit decoded by Bob with a very high probability. They get a shared sequence of bits, called a sifted key, that can be used to build a session key. The length of sifted key is about half the length of raw key.

Example. In Table II on the next page, rectangular and circular bases are written $\oplus$ and $\otimes$, respectively. 1^{st} line ARK contains Alice's randomly chosen sequence of bits. 2^{nd} line ARB contains the encoding basis randomly chosen by Alice for each bit and the 3^{rd} line AQB contains the qubits, i.e., the polarized photons. 4^{th} line BRB contains Bob's randomly chosen measurement basis and 5^{th} line BQB contains the results of the measurements. We have put a symbol "?" to mention that Bob's measurement has a random result which will be discarded anyway.

The last line BSK contains the bits for which Alice and Bob have chosen the same basis, this is the sifted key whose value is "00100100111" in our example.

Eavesdroppers and Security

The eavesdropper, usually named Eve, has access to both channels. However, when Eve accesses a photon, she has no way to know the basis used by Alice to encode the bit. Thus, she has to guess a basis for measuring this photon. And then she resends this photon to Bob. It is the intercept-resend strategy. If she chooses the same basis as Alice for measurement, then she gets the right value and the resent photon is in an appropriate quantum state. If she chooses the wrong basis, then she destroys the quantum state of this photon and, in the cases where Bob chooses the right basis, he gets an incorrect result in 50% of the cases. On the average, Eve chooses the wrong basis in 50% of the cases. Thus, Eve's action introduces a supplementary error rate of about 25%. In this case, Alice and Bob can detect the intrusion and know that the sifted key cannot be trusted.

Another strategy for Eve is the *man-in-the-middle* attack. In this attack, Eve gets control over the two channels and lets Alice think she is communicating with Bob and conversely. Eve plays the role of Bob w.r.t. Alice and plays the role of Alice w.r.t. Bob. In this case, one must rely on authentication algorithms stemmed from classical cryptography or on recent quantum authentication algorithms ([22]).

Many papers give a rather complete description of the non-impossible quantum attack strategies, for instance beam splitting scheme or entanglement scheme or quantum copying scheme or collective attacks, in various configurations and for various QKD technologies, and why they are unlikely to succeed. Formal proofs of security rely on protocols such as the following BB84. They uses Shannon's Information Theory and, most important, the laws of Quantum Physics.

BB84 Protocol

The BB84 protocol is used over physical devices to handle key distribution. Rationales for this protocol are multiple.

First, the quantum devices, for producing quantum states, for transporting and measuring them, are not totally perfect.

For instance, one must consider the dark-count error. It is the probability of detection of an unsent photon. A low probability of about 10^{-5} could not be neglected according to the communication standards.

One must also consider the probability of measuring errors due to apparatus defects that is far more important.

Thus, if the sifted key length becomes a few percents of the initial bits string length, it can be considered as a performance. The protocol is to take into account the error rates due to technical imperfections and to the eavesdropper's action. The error rate in the sifted key is called QBER for *Quantum Bit Error Rate*. The aim of the protocol is to reduce QBER to standard communication *Bit Error Rate* (BER), about 10^{-9}, and to reduce as much as wanted Eve's knowledge about the key. The steps of the protocol are the following:

1) *Sifting.* Alice sends a random string of bits, the raw key, as described above. Alice and Bob must be synchronized to detect photons that Alice did not send but Bob received and, conversely, photons that Alice sent but Bob did not receive. The result is the sifted key. The length of the *sifted key* is about a few percents of the length of the raw key.
2) *Bit reconciliation.* The sifted key is made of qubits on which Alice and Bob agree because they have used the same encoding basis. However, some bits may differ because the quantum apparatus are not reliable or because there has been a light intrusion of Eve which will not been recognized as so. The error elimination algorithm uses the public classical channel. Several algorithms have been proposed. For instance, it has been proposed that Alice and Bob use the same random permutation of bits to randomize the locations of errors. Then, the key is divided into small enough equal-size blocks such that one block is unlikely to contain more than one error. Alice and Bob compare the parities of their respective blocks and discard blocks for which parities differ. After reconciliation, the sifted key may have been shortened but it is almost certainly shared between them.
3) *Eavesdropper detection.* At this step, Alice and Bob may detect Eve's intrusion because a significant intrusion must raise the usual error rate.
4) *Privacy amplification.* It may be that Eve knows some bits of the key resulting from the previous operations. Privacy amplification is a technique to reduce Eve's information. The price is once again shortening of the key. Again, several algorithms are possible. For instance, Alice randomly chooses two bits and tells Bob the position of these bits. Alice and Bob replaces the two bits by the result of their XOR. If Eve has only partial information on these two bits, i.e., if she knows only one bit then she has no information on the XOR result. Therefore, Eve's information is less than before. Alice and Bob may repeat this operation many times to reduce Eve's knowledge to as small as wished.
5) *Authentication.* The two parties identify themselves. This may rely on classical algorithms not especially related to Quantum Cryptography or to recent Quantum Authentication algorithms developed by the authors. These algorithms assume that a piece of data, an authentication key, is shared by Alice and Bob before all.

ARK	0	0	1	0	1	1	1	0	0	1	0	0	1	1	1	1	0	1
ARB	⊕	⊕	⊗	⊕	⊗	⊕	⊗	⊗	⊗	⊕	⊗	⊗	⊕	⊗	⊕	⊕	⊕	⊕
AQB	→	→	↗	→	↗	↑	↗	↖	↖	↑	↖	↖	↑	↗	↑	↑	→	↑
BRB	⊕	⊗	⊕	⊕	⊕	⊗	⊗	⊗	⊗	⊕	⊗	⊗	⊕	⊕	⊕	⊗	⊗	⊕
BQB	→	?	?	→	?	?	↗	↖	↖	↑	↖	↖	↑	?	↑	?	?	↑
BSK	0			0			1	0	0	1	0	0	1		1			1

TABLE II
A QKD SESSION.

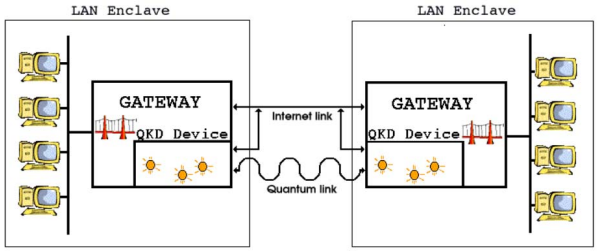

Fig. 3. A single QKD Link

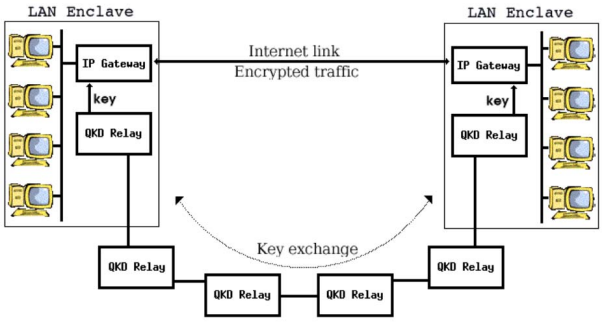

Fig. 4. A long QKD link using relays

In fact, they may share a stack of authentication keys. They are subject to keys exhaustion, and then *Denial of Service* (DoS), if an eavesdropper simulates a lot of connections. We proposed a new algorithm, which protects itself against keys exhaustion ([22]). At the difference of usual approach, this algorithm is dedicated to Quantum Cryptography.

Then Alice and Bob share a key with very high probability and Eve's information about this key is as small as wished.

A single QKD Link

A single QKD link may be used to significantly consolidate the security of networks. For example, one can design a single QKD link between two enclaves that marries QKD with a classical Internet security protocol, e.g, IPSec (see Figure 3). QKD is used only for the key sharing between two enclave gateways. By contrast, the IPSec protocol establishes a data link which connects two gateways. The enclave, a *Local Area Network (LAN)*, is assumed to be already secured. IPSec is a well-established Internet technology that allows traffic between two endpoints to be confidential, provided that the endpoints share encryption keys. The two gateways ensure the routing of IP packets. By that, the essential issue is how the gateways could obtain common encryption keys. The non-classical solution is that the keys necessary to the gateways are distributed by using the single QKD link. Two QKD devices produce continuous streams of secret random bits, which can be used for the regular key renewing.

The first commercial application of the single QKD link has done on April 2004. A team from the University of Vienna, and Ludwig-Maximilians University (Munich, Germany) performed a QKD-based transfer of money using a 1.45 km fiber-optic line under Vienna's streets to link the transmitter at city hall to the receiver at the headquarters of an Austrian bank. Using QKD keys,this team safely transferred funds from city hall to the bank.

A long QKD Link

Simple QKD links as above are limited to the length of several tens kilometers. In order to extend the length, one may use QKD data relays (see Figure 4). One must note that it do not yet exist the repeaters of arbitrary photons. QKD data relay is a chain of stations in which each can establish a single QKD link with the previous station and another QKD link with the following station. This is a data relays network with the following characteristics:

- Relay k establishes an encrypted communication, a QKD link, with relay k-1.
- Relay k receives encrypted data from relay k-1.
- Data are decrypted and stored in the memory of relay k.
- Relay k establishes an encrypted communication, a QKD link, with relay k+1.
- Data in memory are encoded and sent to relay k+1.

We can see that such a QKD data relays network present a serious weakness: data must appear unencrypted in the memories of all relays. QKD data relays network establishes pairwise QKD-based secure communications in order to securely transport a randomly generated encryption key, hop-by-hop from one endpoint to the other. In Figure 4, the QKD relays network at the bottom is used to exchange an encryption key that will be used to encrypt the communication on the top (Internet link).

Communication between QKD relay stations is done as the communication between LAN enclaves of the section above. The encryption key that is exchanged by QKD relays network appears unencrypted inside the relays. Thus, the relays must be seriously protected against eavesdropper. In Europe, due to the concentration of cities, a such scheme could be used by many institutions. However, it may not be applicable to larger countries such as USA, Canada or Russia where extended non-

urban areas exist.

Quantum Networks

The main difficulties of single quantum links are the low rate and the limited distance. The fastest rate of single quantum links is 1 Mb/s, over a 750 m free-space link. The current records of distance are 150 km in fiber and 23 km in free space, with a typical rate of 1 Kb/s or so. With these constraints, it seems to impossible to build up a quantum network. However, one could imagine about the using of a bunch of many single quantum links and of QKD Relays Network as described in the above section. By that, one could transmit secret bits between two arbitrary endpoints of an ordinary Internet network with an acceptable rate. The first QKD network, DARPA Quantum Network, has yet been constructed to test the robustness of such systems in real-world applications. This network links between Cambridge, Harvard, and Boston University and became fully operational on October 2003 ([23]).

Please note that quantum links could be confused with QKD links. In fact, quantum links also can be used for transmitting plaintext data. It means that we could obtain a true Quantum Network. In this network, we have a set of enclaves. Some of these enclaves are pair-wises connected by a bunch of quantum links. It is obvious that such a network would be more interesting. Security level is the same. And it would be a little more complex to build and to administrate with the gain of a wider usage.

VI. Applying QC to ATN

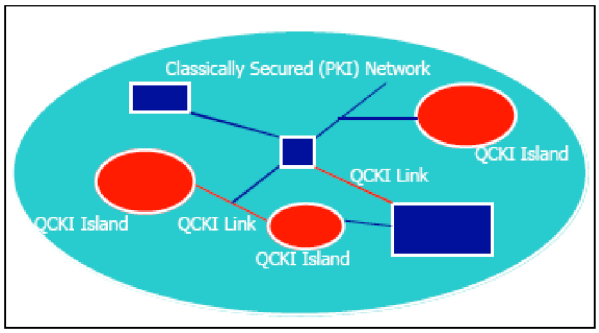

Fig. 5. Co-operation of QCKI and PKI

Quantum Confidentiality Key Infrastructure (QCKI) can be introduced locally to secure a sub-network of the ATN without altering the whole structure of the ATN or the existing PKI system. The sub-network is unconditionally secured and it communicates with the outer world with classical gateways. E.g., one can think of securing a big airport with optical fiber technology or securing an A380 aircraft with the same technology. We get QCKI Islands inside the ATN as shown in Figure 5.

QCKI can be introduced locally to secure links between ground entities of the ATN, provided that the constraints of distance are respected (now 150 km). For instance, we could secure the links between all airports of *Aéroports de Paris* (ADP) or between ground stations. If the distance is more than required, then one may think of using satellite-based QC although this technology is not yet ready. Otherwise, optical fiber unconditionally secured terrestrial QC dedicated networks can be used. This technology may be used to secure the ground part of the ATN and to incrementally replace PKI technology.

A developed concept is that of QBONE. One may think of a classically secured network such as the ATN or a bank network. Let us assume that this network must have *Access Points* (AP) located outside of its security zone. For instance, an ATM machine must be connected to the bank network but it may be located in an unprotected commercial center. For the ATN, the external AP could be aircrafts. Communication with an aircraft can easily be monitored, thus we cannot assume secrecy.

Let us consider aircraft as external AP to the classically secured ATN. *AGT Data Link* (DLK) provides numerical communications between ground stations and aircraft. They are used for many applications such as Graphical Position Reports, Contact Reports, etc. One may classify different threats:

- *Monitoring.* A third party may listen to DLK communications and gain information on the traffic. Current DLK communications do not guarantee privacy.
- *Spoofing.* A third party may listen to DLK communications and gain authentication information in order to impersonate one of the legal parties.
- *Modifying.* A third party may impersonate the second party with respect to the first party meanwhile he may also impersonate the first party with respect to the second party (man-in-the-middle attack). Integrity of the data is not preserved. Data may be corrupted.

It is very easy to monitor *Aircraft Communications Addressing And Reporting System* (ACARS) Data Link Messages ([24]). One needs a personal computer, a sound card, a *Radio Frequency* (RF) scanner and few software freely available on the WEB.

Thus, the need to secure aircraft communications with ground stations appears clearly. We consider aircraft as AP to the ATN. Free-space QCKI can be used to distribute encryption keys:

- To aircraft entering the European sky either from the ground if controllers oblige the aircraft to cruise at the vertical of one of some chosen points at the frontier of Europe; or from satellites otherwise (see Figure 6 on the following page)([25], [26]).
- To aircraft standing at airport, may be not wired to the airport terminal, the control tower could securely distribute a key to any aircraft standing on the tarmac using free space technology (see Figure 7 on the next page).

Then the encryption keys are distributed to the ground stations possibly using the classically secured ground ATN.

VII. Free Space and Satellites

The very first demonstration of free-space QC system was a table-top experiment performed at the IBM Thomas J. Watson Research Center in 1989 over a distance of 32 cm. With the

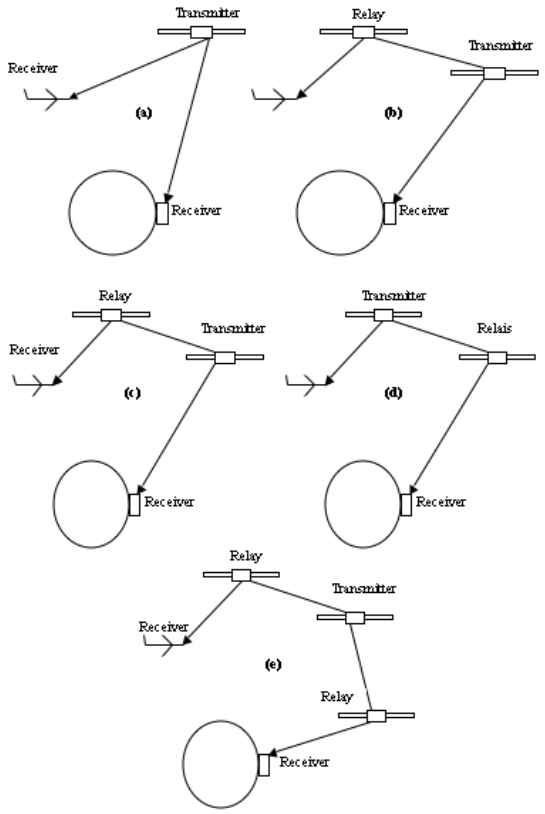

Fig. 6. Satellite-based QKD between aircraft and ground-station

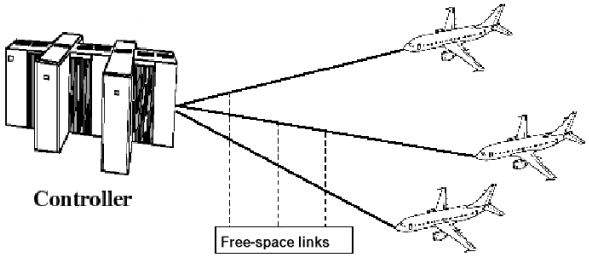

Fig. 7. QKD between the control tower and aircrafts

progress of technology, the most recent result of such a system has achieved a distance of 23.4 km.

Free-space links have been studied and already successfully implemented for several years for their application in quantum cryptography based on faint classical laser pulses. Free-space link is one of two solutions for quantum channel. Transmission over free-space links has some advantages compared to the use of fiber-based links. First of all, the atmosphere has a high transmission window at a wavelength of around 800 nm, where photons can easily be detected by using commercial high-efficiency photon detector. Furthermore, the atmosphere is only weakly dispersive and essentially isotropic at these wavelengths. It will thus not alter the polarization state of a photon.

However, there are some drawbacks concerning free-space links as well. In contrast to the signal transmitted in a optical fiber (guiding medium) where the energy is protected and remains localized in a small space, the energy transmitted via a free-space link spreads out, leading to higher and varying transmission losses. In addition, the background light such as ambient daylight or even moonlight at night can couple into the receiver, leading to dark-count errors. Finally, it is clear that the performance of free-space QC systems dramatically depends on atmospheric conditions.

From September 2001 to January 2002, P. Morris has tested a semi-portable free-space QC system between two mountain tops, Karwendelspitze (2244m) and Zugspitze (2960m), in Southern Germany, for the exchange of keys. The distance between the two locations is 23.4 km. The elevated beam path dramatically reduced the air turbulence effects experienced in previous low altitude tests, but also caused unprecedented requirements on stability against temperature changes, reliability under extreme weather conditions and ease of alignment.

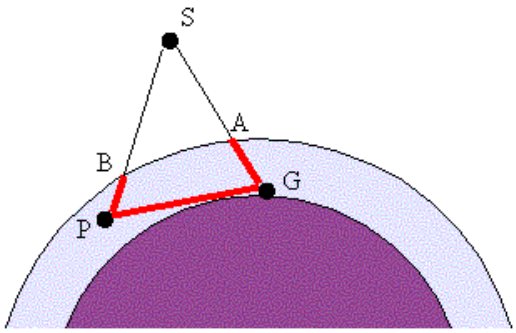

Fig. 8. Influence of atmosphere on the QKD

For the satellite free-space QC ([25], [26]), the transmission of photons is only hard in the first 1 km atmosphere, and then more easy because in space, atmospheric interference problems go away (see Figure 8). By theoretical calculations, one knows that 2 km Ground/Ground QC in the first 1 km atmosphere is equivalent to 300 km Ground/Space QC. The main difficulty would come from beam pointing and wandering induced by air turbulence. Then, minimizing the size and the weight of equipments is vital question as they are ever going to be installed on satellite. However, with the 2003's results, we could hope a free-space communication up to 1600 km, suitable for satellite-based key exchange.

The major design parameters for the transmission subsystem are laser wavelength, modulation format and data rate, and reception technique. Of equal importance is a sub-system required for beam pointing, link acquisition, and automatic mutual terminal tracking, named *Pointing Acquisition and Tracking* (PAT) QC. Because of the very narrow widths of the involved communication beams, PAT asks for highly sophisticated concepts and for electro-mechanic and electro-optic hardware meeting exceptional technological standards. Major parameters entering the link capacity are telescope size, optical transmit power, link distance, and receiver sensitivity. Other aspects are mass, volume, and power consumption of the terminal.

Examples for existing space laser communication links include *European Space Agency* (ESA)'s inter-satellite link

Semiconductor Laser Inter-satellite Link Experiment (SILEX) and a satellite ground link, which was only recently realized between the *Geostationnary Earth Orbit* (GEO) satellite ARTEMIS and ESA's optical ground station *Optical Ground Station* (OGS) at Tenerife.

Although space-to-space links have the attractive advantage of not being influenced by Earth's atmosphere, it is too much difficult at present due to the expected disproportionate technological and financial effort as compared to alternative schemes with at least one of the communication terminals on ground. Most envisioned quantum experiments require higher flexibility at the receiver due to active polarization control or data analysis, thus it is more reasonable to place the transmitter module in satellite, while the receiver modules stay in easily accessible ground-based laboratories.

We consider the exchange of key using LEO satellites (800 km). There are three options:

- The ground station transmits a key to the satellite.
- The satellite transmits a key to the ground station.
- The ground station transmits a key to another ground station by using the satellite as a mirror.

For all three models, it needs a classical channel that must be able to exchange digital data at high bit rates to allow interactive alignment, time synchronization, key sifting and error correction to be carried out in real time. Ethernet bandwidths, 10 Mbs, are needed for real-time operation. Lower classical bandwidth would require some time after optical key exchange for the protocol to be completed, thus limiting the number of key bits that could be exchanged on a typical pass. For the optical channel, we suggest telescopes like the following:

- A big telescope on the ground station with a diameter up to 30-100 cm which must be able to track the satellite
- A small telescope on the satellite (10 or 30 cm). With 10 cm optics the target of 3 kg may be reached but 30 cm optics will be difficult to build below 5 kg.

We propose models to create a satellite QC network (see Figure 9). There are two choices:

- Ground-Based transmitter terminal: key is transmitted from ground to satellite.
- Space-Based transmitter terminal: key is transmitted from satellite to ground or to another satellite.

Normally, with a satellite at the altitude a of 800 km and its maximum range d, one can calculate the surface covered on the ground with a diameter $2r$ where $r^2 = d^2 - a^2$ (see Figure 10)([27], [28]). However, when one forms a satellite network to cover an enormous surface, one cannot install the satellites with the distance of $2r$ because there is a small uncovered area.

Therefore, the appropriate distance between two satellites is l where $l^2 = 3.r^2$. The radius of the Earth is 6378 km and the altitude of LEO satellite is 800 km. Therefore, the radius of satellite orbit is 7178 km and it needs n satellites to cover a surface with the width of l km: $n = 2.\pi.7178/l \sim 45100/l$.

If we assume *ground-based key transmitter terminal*, the photon source of QKD is easily accessible but there is a high attenuation due to atmospheric effects. The range d of

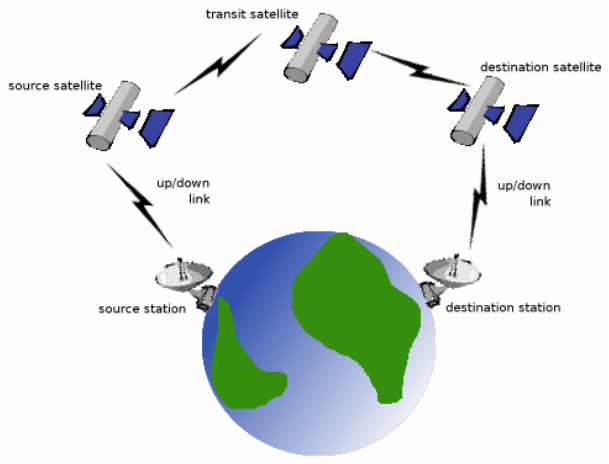

Fig. 9. Satellite-aided QC network

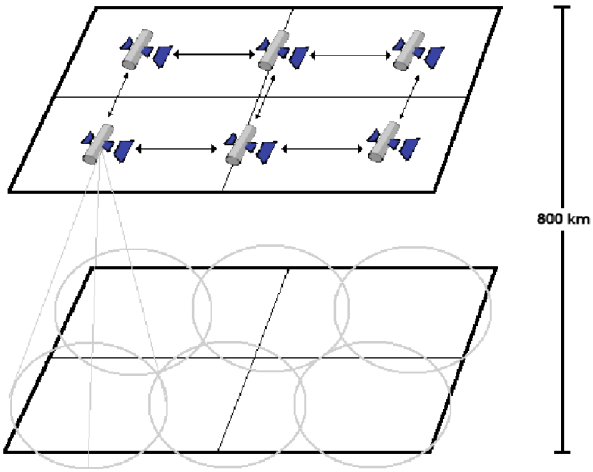

Fig. 10. Covered areas by Satellites

a receiver satellite is 1000 km. The optics on satellite is 10 cm diameter. The covered radius is 600 km. One can compute that the distance between two satellites must be about 1000 km and 43 satellites are required. If we use 30 cm diameter optics on satellites than 9 satellites are required.

If we assume *space-based key transmitter terminal*, the system is more complex but also more flexible and it allows individual distribution of keys from any satellite. It is a global system. If we use 50 cm optics at ground stations, the maximum range is 2000 km. The distance between two satellites is 3174 km and 14 satellites are required. With enormous 100 cm optics at ground stations, then only 7 satellites are required.

The distance of optical channel is really limited. There is always a big problem to send photons through a long distance in free space. Thus, the scenario of distributing key from the satellite to the ground station is the best choice because it is easier and less expensive to install a large telescope at ground station than on satellite.

VIII. PERSPECTIVES

The perspectives of our work performed could be a coupling of *Air Identification Tag* (AIT) ([29]) developed by the university of Graz and Eurocontrol with QKD. AIT is the watermarking insertion of flight identification in VHF ground-pilot communication. Any party duly equipped can see the other party identification on a special visual device or, in the case of controller; it can be used to highlight the speaking aircraft on the radar screen. AIT did not intend to guarantee authentication of the parties. AIT has been designed to reduce the workload and the stress of controller. Authentication and integrity can be obtained by cryptographic signature technology provided that the two parties share a key. Free space QKD is used from the control tower to distribute a key to aircraft standing at the airport. The AIT message could include the flight identification, the current GMT Time and a signature of both provided by one of the hash functions of the classical cryptography cookbook.

Our work also describes more ambitious scenarios based on different QKD techniques to secure the whole ATN while respecting the criteria of the incremental insertion of QKD inside PKI-based system and the criteria of complementarities of the two techniques. The most ambitious plan would be to use satellites-based key distribution. The required number of satellites varies from 7 to 43 depending on technology evolution. It is a costly solution that may be used only if PKI is broken one day by Quantum Computers or mathematical progress.

All project information and report are available from the CARE INO web site at the following URL:

`http://www.eurocontrol.int/care-innov/public/standard_page/innov2_quantum.html`

A full description of the possible applications of QKD to ATN may be found in the report mentioned above.

REFERENCES

[1] ICAO, "Manual of technical provisions for the aeronautical telecommunications network (atn) - standard and recommended practices (sarps)," Mars 2001.

[2] B. Witulski, "Key management," in *Presentation at DLK Users Forum*, Brussels, Belgium, June 1995.

[3] J. McMath, "Aeronautical telecommunication network(atn): Security, key management and distribution security, key management and distribution," in *AEEC Data Link Users Forum and ESC/GAD, Titan Corporation, Public Release: 03-0052 edition*, Hanscom, MA, USA, February 2003.

[4] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, 1984, pp. 175–179.

[5] C. Bennett, F. Bessettee, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," September 1991.

[6] N. Gisin and al, "Quantum cryptography," *Reviews Modern Physics*, vol. 74, pp. 145–195, January 2002.

[7] C. Elliott, "Building the quantum network," *BBN Technologies (USA)*, June 2002.

[8] M. D. Dang and M. Riguldel, "Usage of secure networks built using quantum technology," 2004.

[9] T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura, "Single-photon interference over 150-km transmission using silica-based integrated-optic interferometers for quantum cryptography criterion," *Submitted to Electronics Letters*, 2004.

[10] W. T. Buttler and al, "Practical free-space quantum key distribution over 1km," *Phys. Rev. Lett.*, vol. 81, pp. 3283–3286, 1998.

[11] ——, "Daylight quantum key distribution over 1.6 km," *Phys. Rev. Lett.*, vol. 84, pp. 5652–5655, June 2000.

[12] P. M. Gorman, P. R. Tapster, and J. G. Rarity, "Secure free-space key exchange to 1.9 km and beyond," *J. Mod. Opt. of Physics*, vol. 48, pp. 1887–1901, 2001.

[13] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New Journal of Physics*, vol. 4, pp. 43.1–43.14, 2002.

[14] C. Kurtsiefer, P. Zarda, M. Halder, P. Gorman, P. Tapster, J. Rarity, and H. Weinfurter, "Long distance free-space quantum cryptography," *In New Journal of Physics*, vol. 4, pp. 43.1–43.14, 2002.

[15] D. Gottesman and H.-K. Lo, "Proof of security of quantum key distribution with two-way classical communications," September 2002.

[16] D. Mayers, "Unconditional security in quantum cryptography," *JACM*, vol. 48, no. 3, pp. 351–406, May 2001.

[17] H. Inamori, N. Lütkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," July 2001.

[18] H.-K. Lo, "Communication complexity and security of quantum key distribution," April 2004.

[19] H.-K. Lo and H. Chau, "Unconditional security of quantum key distribution over abitrarily long distance," *Science*, pp. 2050–2056, 1999.

[20] P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," April 2004.

[21] C. Guenther, "The relevance of quantum cryptography in modern cryptographic systems," December 2003.

[22] P. Bellot, M. D. Dang, and H. Q. Nguyen, "A new authentication scheme for quantum key distribution," 2004.

[23] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the darpa quantum network," Mars 2005.

[24] D. L. A. H. Committee, "Ad hoc meeting on security, executive summary for aeec general session 2002 membership," *ESC/GAD, Titan Corporation (Hanscom, MA, USA)*, May 2002.

[25] M. Pfennigbauer, W. R. Leeb, M. Aspelmeyer, T. Jennewein, and A. Zeilinger, "Free-space optical quantum key distribution using intersatellite link," November 2003.

[26] G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," *New J. Phys.*, vol. 4, no. 82, October 2002.

[27] B. R. Elbert, "The satellite communication applications handbook," *Artech House, Inc, MA*, 2002.

[28] J. Lee and S. Kang, "Satellite over satellite (sos) network: A novel architecture for satellite network."

[29] H. Hering, M. Hagmüller, and G. Kubin, "Safety and security increase for atm through unnoticeable watermark aircraft identification tag transmitted with the vhf voice communication," in *Proceedings of the 22nd Digital Avionics Systems Conference (DASC)*, Indianapolis,USA, October 2003.