RESEARCH ARTICLE OPEN ACCESS

Survey of Security Challenges in Aeronautical Data Communication Networks

Suman [1], Pinki Rani [2]
Department of Computer Science
Kurukshetra University, Kurukshetra
Thanesar, Haryana

ABSTRACT

This paper presents a comprehensive survey of network security issues and challenges in future data link networks. The paper gives an overview of the civil aviation industry efforts for securing the future Aeronautical Data Communications. The aviation communication technologies are progressively shifting towards the use of digital data instead of analog voice for traffic control, airline business, and passenger onboard entertainment systems. The open and wireless environment of data link networks makes it vulnerable to serious attacks. This paper discuss about enhancement of network to overcome the problems related to voice radio communication and to modernize the Air Traffic Management environment. Data link networks raise several security concerns for all users including pilots, air traffic controllers, airline staff, and even passengers. This survey can be used as a reference guide to first understand the factors that urge both the research community and the aviation industry to be concerned about network security in future Aeronautical Data Communications.

***Keywords*:-** Civil Aviation, Air Transport System, Network Security, Aeronautical data Communication, Data link

I. INTRODUCTION

Aeronautical communications are about to shift the paradigm of digital data in near future. A digital data link system was introduced, namely ACARS (Aircraft Communication Addressing and Reporting System), to essentially support radio voice systems, which were nearly running at their maximum capacity. The term "*data link*" is commonly used among the civil aviation community to represent digital communications between an aircraft and a ground station (i.e. an air traffic tower control, an airline operational control center). Data link networks raise several security concerns for all users including pilots, air traffic controllers, airline staff, and even passengers.

II. EVOLUTION OF AERONAUTICAL COMMUNICATION NETWORKS

A. Growth in Air Traffic Load

When an analog voice radio communication technology is used, all pilots in the same sector and communicating with an air traffic controller are tuned to the same frequency. This can be challenging, considering the expected air traffic growth. This growth is due to many factors such as an increased aircraft manufacturers market, more competitive low-cost airlines, an increased passenger demand and the greater need for companies to provide a better service to their customers.

B. Congestion of the Aviation Radio Frequency

A frequency saturation may delay the communication between the pilot and the controller and make them unreachable for a certain period of time. Many solutions have been provided in the past in order to address this frequency congestion issue such as optimizing frequency reuse, using a larger spectrum or even splitting the radio spectrum into narrower bandwidths (50 kHz to 25 kHz channels). Air traffic sector division cannot be considered as an efficient long-term solution for radio voice frequency saturation. In order to address the air traffic growth and subsequent frequency congestion issues, the industry is progressively leaving analog voice at the expense of digital data communications.

C. Modernization of Aviation Communication Technologies Using Data Link Systems

Many aircrafts are already equipped for data-based communications with data link systems such as the CPDLC (Controller to Pilot Data Link Communication) system, which is an ATN (Aeronautical Telecommunication Network) data link application that allows text-based message exchange between airline/air traffic ground facilities and the aircraft. Promising statistics showed that analog voice usage for operational services decreased in aircraft equipped for data-based ATS (Air Traffic Service) and AOC (Airline Operational Communication) applications

D. Future Aircraft Data Communication Services

Future Air communication services and their supporting systems will be based on data link technologies to provide both operational services and non-operational services.

- ATS services support ATC (Air Traffic Control) messages between the pilot and the traffic controller.
- AOC (Airline Operational Services) are required for efficient CNS and ATM operations. This service category supports operational voice and/or data messages between the aircraft and the airline or airport operational staff.
- ACD (Aircraft Control Domain) regroups all systems dedicated to the control of the aircraft and the flight.
- AISD (Airline Information Service Domain) regroups non safety-related systems dedicated to the maintenance and the crew.
- PIESD (Passenger Information and Entertainment Service Domain) contains all systems allowing the passengers to access IFE/IFC services.
- PODD (Passenger Owned Devices Domain) is relevant to passenger owned systems which need be connected to the network (e.g. tablets, smart phones, laptops).

III. NETWORK SECURITY CONSIDERATIONS

Security corresponds to the approaches and methods used to mitigate risks resulting from a malicious intent like an unauthorized intrusion on avionic systems. As a security attack may have some consequences on the regulation of the flight, security risks definitely imply safety risks in the aeronautical context. From a data link point of view, network security covers any attack or vulnerability in the air–ground communications.

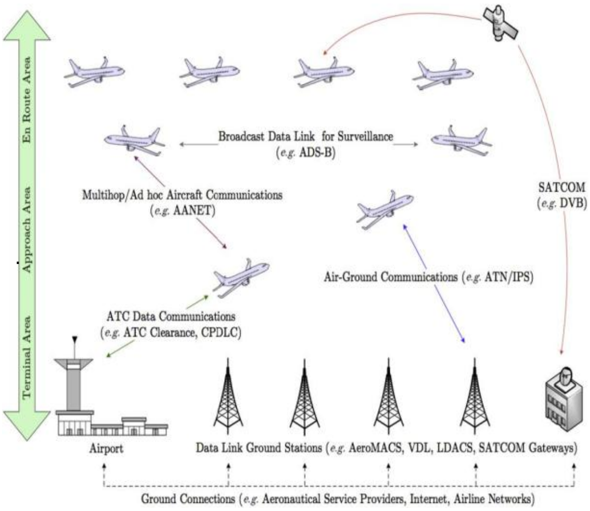
En Route Area
Approach Area
Terminal Area
Broadcast Data Link for Surveillance
(e.g. ADS-B)
Multihop/Ad hoc Aircraft Communications
(e.g. AANET)
SATCOM
(e.g. DVB)
Air-Ground Communications (e.g. ATN/IPS)
ATC Data Communications
(e.g. ATC Clearance, CPDLC)
Airport
Data Link Ground Stations (e.g. AeroMACS, VDL, LDACS, SATCOM Gateways)
Ground Connections (e.g. Aeronautical Service Providers, Internet, Airline Networks)

Fig. 1: Data Link Communications in the Future Airspace System

The opportunity to take advantage of safety-related service aggregation with airline and passenger services will require appropriate security countermeasures to protect the operational services from new threats. ATS traffic requires high priority and full availability, whereas AOC NG services may have restricting QoS (Quality of Service) requirements to be satisfied. While it is important for the aircraft to maintain continuous network connectivity with operational ground stations, availability becomes an important aspect of the overall network architecture, specially when considering the usage of a single satellite link for all the aeronautical services. Security requirements for the communication system will be more complex to fulfill due to additional factors such as traffic heterogeneity, aircraft mobility or scaling issues. Providing IFC services for passengers may be an open invitation for hacking the air–ground connectivity as the Internet is an open network where anyone can connect anywhere no matter where they are.

IV. SECURITY CHALLANGES IN DATA LINK NETWORKS

This section summarizes what should be the main points of interest regarding cyber security in next generation aeronautical communications.

A. Data flow Logical Separation

Currently, ATS communications have to be strictly separated from other types of communications, because of safety and regulation policies, as required by ICAO SARPs (Standards and Recommended Practices). ICAO SARPs define a set of end-to-end protocols and operational access procedures that allow both safety and non-safety aeronautical applications to use data link technologies independently of air-ground and ground-ground sub networks. In the perspective of a network architecture which allows the coexistence of all aeronautical services in the same infrastructure, an exciting challenge from a security point of view emerges.

B. *Heterogeneity of Security Requirements*

In operational aeronautical communications, some security properties are more or less required than others. One security mechanism would probably not be able to cover all the security requirements for all traffic classes, unless the strongest security mechanism is deployed. For instance, if IPsec is configured to use the AH (Authentication Header) mode for all traffic classes, onboard users would likely hesitate (even refuse) to access passenger services provided by the airline (which could have an impact on the business plan of the company). Indeed, AH does not provide data confidentiality, which is actually an issue if a passenger is entering some kind of confidential data (e.g. passwords, credit card ID).

C. *Defense in Depth*

The idea behind defense in depth is to use multiple security strategies at several layers, so that if one security layer falls down, there will be always a security backup layer to prevent a full breach into the communication system. Consequently, having a security framework that takes the advantages of each security layer and uses them to deal with the drawbacks of other security layers will be perfect.

D. *ATM Scalability*

In order to manage all the security primitives that might be needed by aircraft, passengers, or avionic systems, a PKI has to be deployed. PKI is usually defined as a set of practices, technologies, and policies involved in several process such as deployment, management, storage, and revocation of certificates when cryptography is used. Because different aviation organizations may have different security policies in their own PKIs, interworking and roaming schemes between aircraft, end entities, or airlines are required. In such conditions, deploying a PKI regardless of these considerations becomes a tough task. Thus, a great challenge lies in finding adequate mechanisms and a well-suited PKI for data link communications under such constraints.

E. *Impact of Security on Air–Ground Resources*

Security has an undeniable impact on the network performances. Experimental studies have been carried out in the past and demonstrated the performance impact due to security protocols such as IPSec or SSL (Secure Socket Layer). Generally, security should be optimized, otherwise it may induce heavy overhead to data transmission and could deteriorate the system performances. Finding the best trade-off between required security services and system performances may be an interesting challenge to meet.

F. *Vulnerability and Risk Assessment*

Having assessed the risks, security measures (which could be technical or operational) are identified then implemented in order to mitigate those risks. In the data link context, the risk resulting from interconnection between nodes and different networks has to be mitigated because of the future SWIM (System Wide Information Management) paradigm.

V. IMPROVEMENT DIRECTIONS FOR AIRCRAFT COMMUNICATION SECURITY

Three solutions are given in order to address these data link security issues and challenges.

A. *Adaptive Security*

Adaptive security should provide enough flexibility and accuracy to deal with many of the security issues previously depicted. For instance, a security manager module could be installed onboard the aircraft to manage all the secure communications between the air and the ground. As one infrastructure is meant to deal with several traffic flows coming from different network domains, such a security manager module could be deployed on a proxy that intercepts the clients requests and establishes a secure communication with the ground entity.

B. Enhanced Vulnerability and Risk Assessment

In order to estimate the security risk, the following expression is usually used :

$$\boldsymbol{Risk = Likelihood * Impact}$$

Where likelihood is the probability of occurrence of a threat and impact is the potential damage resulting from the exploit of the associated vulnerabilities.

1. **The risk per node** is computed for each node depending on its own vulnerabilities and its connections with correlated nodes. As a node is connected to other nodes in the network, the total risk for a given node *i* is evaluated as the product of node value $Value_i$ and the sum of its individual and propagated risks (respectively denoted $Risk^{+}_{i}$ and $Risk^{-}_{i}$). The risk for the node *i* is then computed as:

$$Risk_i = Value_i * (Risk^{+}_{i} + Risk^{-}_{i}).$$

2. **The individual risk** is the intrinsic risk computed for each node, meaning it takes into account only the vulnerabilities associated with the node itself. The individual risk $Risk^{+}_{i}$ is computed as the sum on the number of existing vulnerabilities T_i of the product between the likelihood of occurrence of a threat $P_t(i)$ and its impact $I_t(i)$, which is fully compliant with the basic expression of the risk:

$$T_i$$

$$Risk^{-}_{i} = P_t(i) * I_t(i).$$

$$t=0$$

3. **The propagated risk** is the risk inherited from the de-pendency between correlated nodes (e.g. data flow exchanges, client–server architectures, etc.). The propagated risk $Risk^{+}_{i}$, is estimated as the following:

$$n_i \;\; T_j$$

$$Risk^{+}_{i} = \qquad P_t(i, j) * I_t(i, j).$$

$$j=0 \;\; t=0$$

Compared to the individual risk expression, the idea is quite the same except the difference that the propagated likelihood $P_t(i, j)$ and the propagated impact $I_t(i, j)$ are induced by all the vulnerable nodes connected with node *i* (and denoted n_i).

4. **The network risk** is the total risk computed for all the nodes composing the network. It is calculated as the sum of all the risks relevant to each node in the network (where *n* denotes the total number of hosts on the network):

$$n$$

$$Risk_{net} = \; i=0 \;\; Risk_i.$$

C. Scalable public key infrastructure and key management

A performance-aware PKI should provide an efficient and scalable key management for the future E-enabled aircraft. This ATM dedicated PKI must provide three fundamental properties:

1. **Scalability** is probably the most important criteria as it should help in decreasing the amount of security overhead. When a PKI is used, several security-related procedures take place aside the effective secure exchange of data flows: registration of end entities to the CA, key generation, certificate distribution/revocation/ verification, etc. As these procedures require the use of several signaling messages (e.g. request for a CRL—Certificate Revocation List), they should be minimized and optimized.

2. **Interoperability** is needed, first to provide a smooth aircraft mobility (transition from an airline domain to another for instance) and a seamless service to passengers and users onboard the aircraft.

3. **Robustness** is critical as the PKI should avoid a single point of failure (e.g. single CA) and provide a chain of trust between its different components.

In order to guarantee all three properties, a multi-rooted hierarchical PKI model with cross certification between trusted CAs may be used. In order to have a trusted relationship between third party authorities with end entities, and cost-effective communications in a large scale ATM system, it is suitable for CA to manage a limited number of PKI operations. Following Table shows a mapping between the improvement security solutions provided in this paper and the data link security challenges.

Data link security challenges	Adaptive security	Enhanced vulnerability and risk assessment	Scalable PKI and key Management
Data flow logical separation	✓		
Heterogeneity of security requirements	✓		
Defense in depth	✓	✓	✓
ATM scalability			✓
Impact of security on air–ground resources	✓		✓
Vulnerability and risk assessment		✓	

Table : Mapping between challanges and improvement directions in data link security

VI. CONCLUSION

Since many years, the aviation industry is evolving in every aspect. Data communications will be soon widely used and network security must be addressed to avoid unwanted side effects. This paper is a survey of network security in the future aircraft data communications. It explains why network security should be a central point of interest in the future aircraft data communication systems and provides an overview of the efforts undertaken in order to accommodate a safe and secure air traffic environment. Finally, main security challenges are discussed then likely improvement directions are presented. These enhancement directions could be used as a starting point to provide a secure environment for data link communications.

REFERENCES

[1] H. Hering, K. Haufdauer, From analogue broadcast radio towards end-to-end communication, in: 26th Congress of the International Council of the Aeronautical Sciences ICAS 2008, 2008.

[2] ICAO, Aeronautical communications panel (acp) wgf, need for spectrum for future aeronautical air/ground communication systems, 2006.

[3] ARINC, Arinc report 811, commercial aircraft information security concepts of operation and process framework, 2005.

[4] W.H. Jones, M. de La Chapelle, Connexion by boeing-broadband satellite communication system for mobile platforms, in: Proc. Communications for Network-Centric Operations: Creating the Information Force. IEEE Mili-tary Communications Conf. MILCOM 2001, vol. 2,2001,Pp 755–758. http://dx.doi.org/10.1109/MILCOM.2001.985939

[5] C. Douligeris, D. Serpanos, Pki systems, in: Network Security:Current Status and Future Directions, IEEE, 2007, pp 409–418.

[6] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (1978) 120–126.

[7] FAA, Review of web applications security and intrusion detection in air traffic control systems. Report Number: FI-2009-049, Technical Report, 2009.

[8] ARINC, Draft 1 of ARINC project paper 823 datalink security, part 1: ACARS message security, 2007.

[9] M.L. Olive, Efficient datalink security in a bandwidth-limited mobile environment—an overview of the aeronautical telecommuni-cations network (atn) security concept, in: Proc. DASC Digital Avionics Systems The 20th Conf, vol. 2, 2001. http:// dx.doi.org/ 10.1109/DASC.2001.964255.

[10] R. Robinson, M. Li, S. Lintelman, K. Sampigethaya, R. Poovendran, D. von Oheimb, J.-U. Buauer, J. Cuellar, Electronic distribution of airplane software and the impact of information security on airplane safety, International Conference on Comp. Safety, Reliability and Security(Safecomp)4680 (2007) 28–39.

[11] R. Jain, F. Templin, K.-S. Yin, Analysis of l-band digital aeronautical communication systems: L-dacs1 and l-dacs2, in: Proc. IEEE Aerospace Conf, 2011, pp. 1–10. http :// dx.doi.org/10.1109/AERO.2011.5747378.

[12] K. Sampigethaya, R. Poovendran, S. Shetty, T. Davis, C. Royalty, Future e-enabled aircraft communications and security: the next 20 years and beyond, Proceedings of the IEEE 99 (2011) 2040–2055.