

Aviation Data Networks

R. Volner

Department of Air Transport, Faculty of Transportation Sciences, Czech Technical University in Prague, Horská 3,128 03 Prague 2, phone/fax: +420 2 2435 9183, e-mail: volner@fd.cvut.cz

P. Boreš

Department of Theory Circuit, Faculty of Electrical Engineering, Czech Technical University in Prague, Technická 3,166 00 Prague 6, phone/fax: +420 2 2435 2098, e-mail: bores@feld.cvut.cz

Introduction

In the recent past, there has been an enormous amount of development in internet technology. There has been significant development both in internet access methodology and applications using internet. With the development of high speed wireless access devices, mobile internet access is fast becoming popular.

An airplane could be considered as a network that is on the move. While the basic mobile IP suit can support single host mobility, this basic form cannot support the network mobility. In order to support network mobility, the mobile network should be equipped with a mobile router (MR). The MR is similar to the mobile node except that the MR should also perform the routing functionality. The extensions to the basic mobile IP to support network mobility also propose using two tunnels, one for the MR itself and the second one for the nodes attached to the MR. While mobile IP offers basic mobility support, it does not guarantee any form of security and quality of service for mobile node/network traffic. Security and quality of service can be provided by using additional protocols that are external to mobile IP (Fig. 1).

The aircraft can use many different communication mechanisms like terrestrial links, wireless links or satellite

links to provide internet connectivity when in flight. Using satellite links is the most viable mechanism because of its high reliability, bandwidth availability and large geographic area coverage. Using satellite links reduces the number of handoffs required by the aircraft data network (ADN) when the aircraft is in the air.

Over the past decade, there has been a tremendous growth in the communication field. From the initial communication systems based on radio technology that were mainly used for communication between the pilot and the ground station, today aircrafts use satellite based communication systems that could be used for advanced flight control and passenger benefits. The current broadband communication systems (satellite communication systems) provide a bandwidth to the order of 8 Mb/s to 10Mb/s.

Communication networks within the airplanes bring out a lot of new possibilities. Along with providing Internet access to the passengers, the communication network could also be used to enhance flight safety and flight control. Some airline manufacturers have gone one step further and are planning to use data networks to connect the flight components. While this enables an easier control system, it involves some possible security and safety issues.

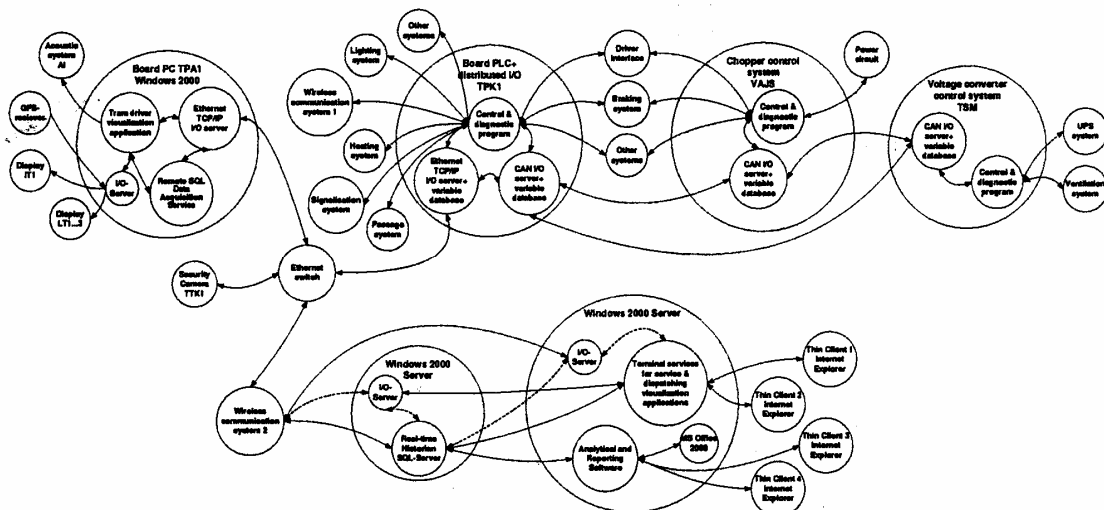


Fig. 1. Information system data flow diagram

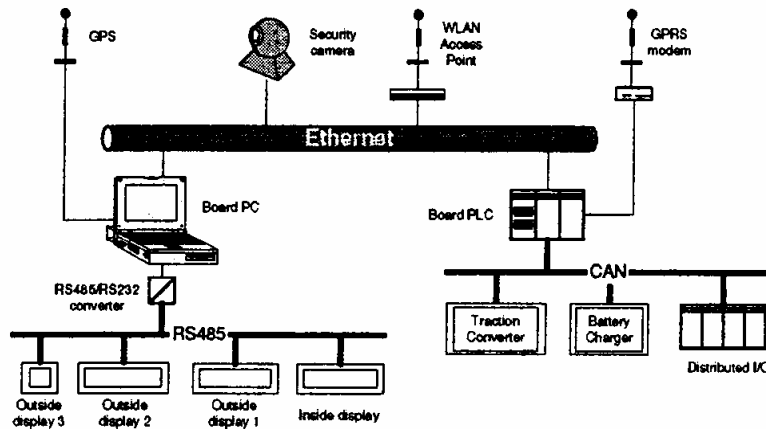


Fig. 2. Public air transport onboard control and diagnostics system

Safety enhancements

Providing internet access to airplanes when they are airborne opens up many possible service opportunities. Some of them are related to flight security and some are of commercial in nature. Below is a list of some of the possible service features that can be deployed in an internet enabled airplane (Fig. 2):

- using the internet access gateway as a beacon device – when an airplane is airborne, it is very important for the administration to keep a track of the position of the airplane. Typically, air traffic control keeps track of the flight position using transponders that detect a radio signal from the air route traffic control center or terminal radar control centers and respond with an amplified signal specifying crucial flight data including flight speed and height information. Although this system works efficiently, it is possible to turn off the transponder with the existing implementation. In fact, the pilot activates the transponder once the flight is airborne. This poses serious security threats as a hijacker, knowing the mechanism, can turn off the transponder and break the communication between the ground station and the airborne flight,
- download of flight critical data in real-time – the black box plays an important role in retrieving important data from a crashed airplane. A black box constitutes two parts:
 - cockpit voice recorder (CVR),
 - flight data recorder (FDR).

As the name suggests, the CVR unit records the voice activity inside the cockpit and the FDR records the trivial data (like flight speed, altitude, temperature, etc.) related to the flight. Most of the black boxes that are used in today's airplane are either made of magnetic tapes or solid-state memory boards. The magnetic tape based black boxes are being phased out and most of the solid-state memory board based black boxes. With the existing computer hardware technology, it is possible to use a high capacity storage device within the airplane. This storage device can be connected to a server and also to the traditional black

box/sensor network. One of the main advantages of using a server with the storage device attached is that the server can mirror all the flight data to the ground station in real-time. This helps the ground station to monitor the flight status/health and assist the flight crew in disaster situations,

- real-time video surveillance – flight safety is one of the most widely discussed topics in the aviation industry today. With the existing video compression standards, it is possible to transmit the video signals to the ground station in real-time. This enables the ground station to monitor the in-flight activities during abnormal situations and make appropriate decisions. This also helps the ground crew to be prepared in the case of medical emergencies,
- remote controlling – in remote situations where the flight crew is compromised or is unable to control the flight due to some unforeseen reasons, the ground station could enable remote controlling of the flight so that flight could be landed safely on the ground. This feature will be helpful in the event of hijacks or medical emergency.

Aviation security requirements

Along with safety, the avionics subsystem must also possess sufficient security provisioning for a successful deployment. Adoption of open standards for data networks has further increased the security concerns. In addition, care must be taken about security requirements while achieving interoperability between various systems within the airplane (Fig. 3).

In any network system, there are three basic security requirements that need to be addressed. They are confidentiality, authentication and integrity. Data confidentiality ensures the privacy of the end users and protects their data from spoofing. Similarly data integrity ensures that the data sent by the end user is not modified by any malicious element in the network. Authentication is one of the most important factors in network security as it controls access to the network resources. Authentication ensures that only valid users have access to the network resources.

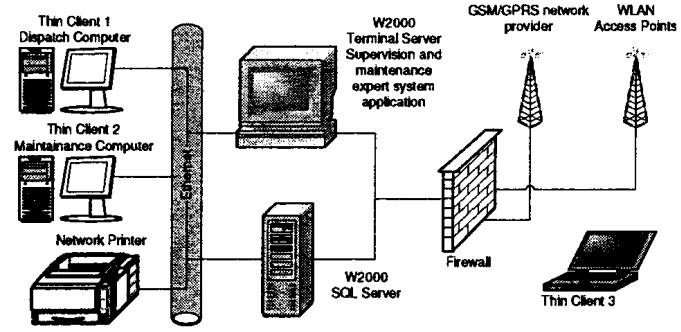


Fig. 3. Structure of dispatching center

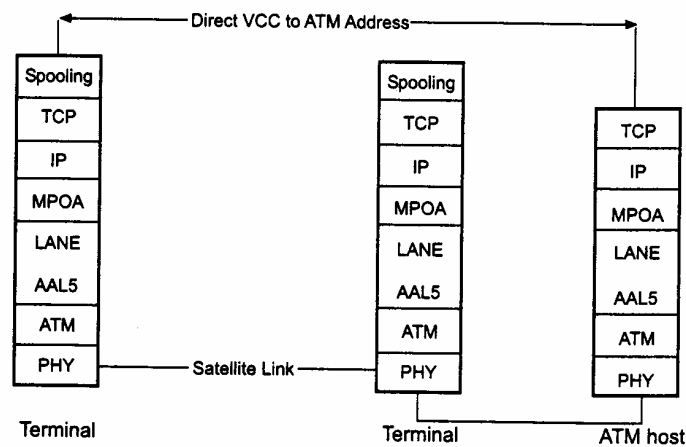


Fig. 4. Multiprotocol over ATM solution for IP/ATM over satellite/terrestrial networks

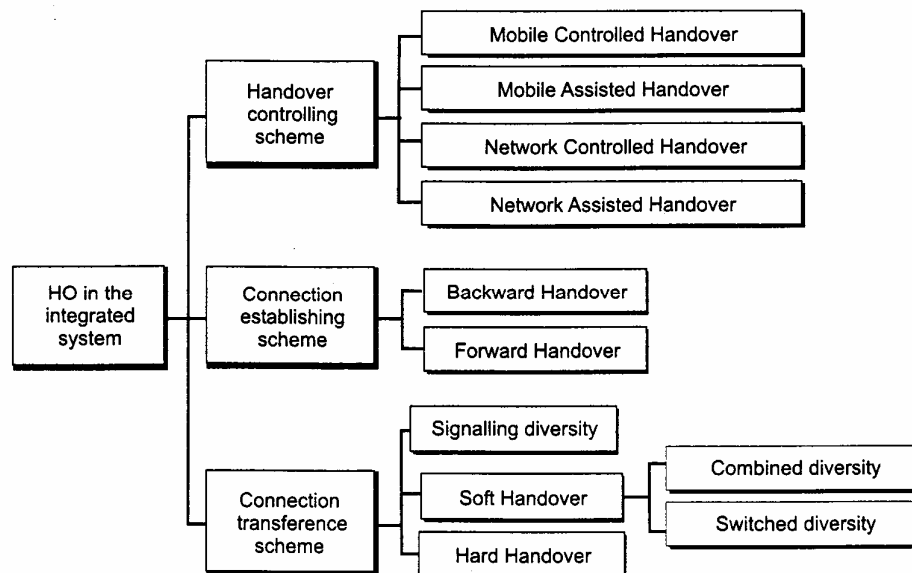


Fig. 5. Handover taxonomy for satellite/terrestrial network architecture

In addition to the above requirements, an airplane network needs additional security in terms of separation between various network segments. The control network has to be protected from unauthorized access. This requires the control network to be separated from the passenger network. Also the passenger network resource usage needs to be monitored and controlled. This requires the passenger network to be connected to a gateway that performs both the monitoring and controlling function in addition to providing Internet access.

Security Issues

The security issues involved with airplane network can be broadly classified into two categories (Fig. 4):

- external,
- internal.

The external security issues are mostly related to the external link connecting the airplane network with the ground station and to the protocol used to provide mobility support. The airplane network could be connected to the ground station by either satellite links or wireless links, depending on the location of the airplane. While the airplane is airborne, it could use either a satellite link or terrestrial link to connect to the ground station. If the airplane is within the range of a wireless access point, it could even use wireless media to connect to the external world. Each of these media has security issues associated with it.

Avionics subsystem design

The main requirements of the avionics subsystem are high determinism and low response time. Different layer 2 technologies like Ethernet, ATM, fibre channel could be considered to provide such a high determinism and low response time. Ethernet is one of the strongest contenders for connections between various flight sub systems and is also mentioned in standard.

Avionics data network design

Security and quality of service are the two important parameters that need to be considered while designing the aviation data networks. The quality of service here does not reflect the quality of service requirements of the end-user applications, but it represents the requirements of the avionics subsystem itself (Fig. 5).

One of the major security requirements of aviation data networks is the separation of different network subsystems. An aviation data network could possibly contain three major network segments namely a control network, crew network and passenger network. As the names suggest, the control network predominantly consists of avionics components. The crew network is used by the flight crew for monitoring purposes and the passenger network enables internet connectivity for the passengers.

In order to protect the control network from unauthorized access and security attacks, it is necessary that the control network is separated from rest of the

aviation data networks. The separation can either be logical or physical.

The network activity monitoring/controlling server could be built in line with an intrusion detection system (IDS). However, unlike normal IDS, the network activity monitoring/controlling server can make decisions based on the data feed from many sources including the cabin voice recorder and surveillance equipment placed at strategic locations within the flight. The server could potentially control all the active forwarding devices. Depending upon the network activity and the security status of the aviation data network, the server can reconfigure the active devices and facilitate control network traffic during emergency situations.

Conclusion

Data network enabled aircrafts have opened up a new set of service opportunities. At the same time, they have also introduced several security threats that need to be addressed. These security threats can originate from outside the airplane or from within the plane.

This paper and research has been supported by MSMT grant N^o. CEZ: 6840770014.

References

1. **Volner R.** Modeling Air Mobile Multimedia Services, Cofax, // 10. medzinárodná vedecká konferencia „Telekomunikácie 2004“, Bratislava, April 2004. – ISBN 80-967019-6-7. – P. 233 - 234. – Poster (in English)
2. **Volner R.** Future Broadband Radio Access Systéme for Integrated Services with Flexible Ressource Management, Cofax, 10. medzinárodná vedecká konferencia „Telekomunikácie 2004. – Bratislava, April 2004. – ISBN 80-967019-6-7. – P. 235 – 236. – Poster (in English)
3. **Volner R.** Informatika v leteckej doprave // medzinárodná konferencia Informatika '2003. – Bratislava, November 2003. – (in Slovak)
4. **Volner R.** ATN network – Basic traffic models for services // Konference k 10. výročí založení fakulty dopravní ČVUT Praha „Doprava a telekomunikace pro 3. tisíciletí“. – Praha, máj 2003. – ISBN 80-01-02741-4. – P. 321 – 326 (in English)

Pateikta spaudai 2005 05 23

R. Volner, P. Boreš. Duomenų perdavimo tinklai aviacijoje // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2005. – Nr. 6(62). – P. 22–26.

Duomenų perdavimo tinklai plačiau taikomi aviacijoje lėktuvo judėjimui sekti ir pagalbai suteikti. Ryšiui, taip pat ir ryšiui su keleiviais, užtikrinti daugelis aviacijos priemonių kūrėjų stengiasi optimaliai lėktuve išdėstyti tinklus. Duomenų tinklas lėktuve ir galimybė keleiviams juo naudotis įpareigoja imtis tam tikrų saugos priemonių ir kartu padidina saugumo tikimybę. Turint internetinį ryšį lėktuve, veiksmai jame gali būti kontroliuojami ir valdomi realiu skrydžio laiku iš žemės stoties. Tai pat, naudojant bangos pločio palydovinių ryšių, kritiniai skrydžio duomenys gali būti perduodami į tarnybinę stotį žemėje realiu skrydžio laiku ar periodiškai, ir tai leidžia kontroliuoti skrydžio eigą.

Informacinių technologijų (IT) laimėjimai, taip pat su vartotojų poreikius gauti greitą informaciją nulėmė didelę internetinių tinklų plėtrą pastarajame dešimtmetyje.

Integruotos saugos sistemų struktūra reikalauja griežtai laikytis į ryšio saugumo lėktuve reikalavimų. Paprastai lėktuve būna trijų tipų ryšys: keleivių tinklas, įgulos tinklas ir kontrolinis tinklas. Saugos taisyklės reikalauja, kad šios trys ryšio grupės būtų atskirtos ir kad šių reikalavimų būtų laikomasi. Il. 5, bibl. 4 (anglų kalba; santraukos lietuvių, anglų ir rusų k.).

R. Volner, P. Boreš. Aviation Data Networks // Electronics and Electrical Engineering. – Kaunas: Technologija, 2005. – No. 7(63). – P. 22–26.

Aircraft data networks are fast becoming more of a necessity due to their support for user mobility. Many aircraft manufacturers are planning to deploy data networks within their airplanes and provide internet connectivity to their passengers. While a data network within the aircraft and passenger access to it causes some security concerns, it opens up some safety enhancement opportunities. With internet connectivity within the airplane, the activity within the airplane can be monitored in real-time from the ground station. Also, using the high bandwidth satellite links, the flight critical data could be downloaded to a server in the ground station in real-time flight or periodically, thereby enabling real-time flight status monitoring.

The information technology (IT) revolution, combined with people's need to access information quickly, has resulted in the explosive growth of the Internet in the past decade. An integrated security framework requires a careful consideration of the security features of the network within an airplane. Potentially, the aircraft could consist of three kinds of networks namely passenger network, crew network and control network. The security protocol implemented must ensure a proper separation of these networks and also watch for any security protocol violations. Il. 5, bibl. 4 (in English; summaries in Lithuanian, English and Russian).

Р. Волнер, П. Бореш. Авиационные сети передачи данных // Электроника и электротехника. – Каунас: Технология, 2005. – № 7(63). – С. 22–26.

В последнее время сети передачи данных в авиации приобретают все большую значимость для слежения передвижения и оказания помощи потребителю. Чтобы гарантировать связь, в том числе и с пассажирами, многие конструкторы стараются оптимально распределить сети связи в самолетах. Эти сети в самолете и возможность пассажирам ими пользоваться обязывают обратиться к некоторым охранным мерам и тем самым увеличивают саму безопасность полета. При наличии интернетной связи в самолете, действия в нем могут подвергаться контролю и управлению с земли. С помощью спутниковой связи, критические данные полета могут быть переданы в земной сервер в реальное время полета или периодически, тем самым создавая возможность контролировать ход полета.

Достижения в области информационных технологий (ИТ), вместе с потребностью получить срочную информацию, предприняли быстрое развитие интернетных сетей в последнее десятилетие.

Интегрированные охранные сети требуют серьезного отношения к безопасности полета. Обычно в самолете находится связь трех типов: связь с пассажирами, связь между членами экипажа и контрольная связь с землей. Правила охраны требуют, чтобы эти типы были разделены и не нарушались. Ил. 5, библи. 4 (на английском языке; рефераты на литовском, английском и русском яз.).