Review On Aircraft Security Monitoring System

Adarsh S S, Kavitha K V

M.Tech student, SCTCE, pappanamcode, Trivandrum, India; Assistant Professor, SCTCE, pappanamcode, Trivandrum, India.
Email: adarshto3@gmail.com

ABSTRACT: Passengers in aircraft must need high security. The incidents like aircraft hijacking or crash happens. To avoid these events, some security measures can be taken. Such type of three security measures are studied and compared here and among them, an efficient aircraft security method is identified. In first method, which is one of the old security measures, the Air Traffic Management (ATM) system is used to ensure security. Here the aircraft network is constantly monitored and checked for hacking is done. It is done through Network Activity Monitoring Tool, which is an Intrusion Detection System. So this method can prevent the attacks from hackers and virtual hijacking. In the second method, the implementation of a Smart Video Surveillance System (SVSS) is used. The video system is installed at the cockpit of the aircraft. In the video system, face recognition system is established. If anyone other than pilot entered in to the room, the system send emergency signals to the ground station. The SVSS architecture is also much simple than the previous method. The final method is the latest and one of the best aircraft security monitoring system. This system is invented and used in China. The security of aircraft and key agreement scheme is joined together to attain more security. The key agreement scheme authenticates the aircraft and airport software, so that to ensure either side is secure. The aircraft side makes high security by applying biometric systems so that only the pilots can fly the aircraft. Also there is secret video surveillance of passengers to ensure no passenger is a hijacker. This reviewwill provide a basic idea about aircraft security and it will be helpful for the future researches.

Keywords: ADN, SVSS, AAP, NKMU, Key Agreement, AFDX etc.

1 INTRODUCTION

SECURITY in an aircraft is as much essential as the security in airport. Providing security in airport is to provide security in aircraft too. In airport, there are many facilities for checking illegal materials that are prohibited in aircraft. The main threat to an aircraft is hijackers. They can enter into an aircraft in any appearance. So, to protect aircraft from hijackers, aircraft authorities can depend on many security methods. The first recorded aircraft hijack took place on February 21, 1931, in Arequipa, Peru. But it was not that much a fatal hijack. It was just a part of revolution. The pilot was approached by some armed revolutionaries and demanded to fly them somewhere. But the pilot refused to do so. After ten days, the pilot accepted their order and flies them to Lima. The world's first fatal hijacking occurred on 28 October 1939. After such an unfortunate incident, all illegal people understand that they have a chance to make money by capturing passengers and demand money for them. From 1948, the count of hijacking increased steeply. In 1969, 82 hijackings where happened. That was the largest number reported ever in a single year. Also, the famous incident on September 11, 2001, 19 al-Qaeda terrorists hijacked American Airlines Flight 11, United Airlines Flight 175, American Airlines Flight 77, and United Airlines Flight 93 and crashed them into the Twin Towers of the World Trade Center, the southwestern side of the Pentagon building, and Stonycreek Township near Shanksville, Pennsylvania in a terrorist attack. The 2,996 death toll makes the hijackings the most fatal in history. To avoid these incidents, Aviation Security Monitorin System is used. An Aviation Security Monitoring System has two phases. First phase consists of network phase. It controls the communication between aircraft and the airport systems. The aircraft analyze the route based on the signals provided from ground station. The Second phase consists of security measures taken inside aircraft to protect cockpit. The attackers can hack the aircraft and give wrong signals to cause land the aircraft at wrong airport or place. To avoid this situation, the network architecture must be well monitored. In this method, the solution for aircraft hijacking is not mentioned. Another method proposes Air Traffic Management (ATM) [1][2] system to ensure security. Also the implementation of Intelligent Video Surveillance system helps to monitor hijacking events in the aircraft. Also the use of Biometrics[9] in Aircraft Security systems makes more efficient Aircraft Monitoring System.

2 OBJECTIVES OF AIRCRAFT SECURITY

The basic security for an aircraft is provided on the airport. If any failure from the airport/ground station will cause problems on the security of the flying aircraft. Even though many security procedures are conducted on the airport, the security in the aircraft must also be provided. The security in aircraft is important because, if any chance a terrorist cleared the security clearance in airport, he must not break the security in aircraft. If the terrorist is successful in entering the pilot's cockpit, then he can change the route and easily hijack the aeroplane. So, it is important to any unauthorized person must not allow to enter to the cockpit region of the aircraft. The following sections discuss the different techniques that provide security for aircraft.

3 AVIONICS DATA NETWORK

The security and Quality of service are main parameters while designing an Avionics Data Network (ADN)[1]. The total network is divided into three main components: control network, crew network and passenger network. So, a perfect ADN must control and monitor all the components effectively. In early days of ADN, there are many types of attacks (like MAC Flooding Attack, 802.1Q and ISL Tagging Attack, ARP Attack, Multicast Brute Force Attack etc.) were possible. So to avoid these attacks, an Intrusion Detection System (IDS) also integrated. Depending upon network activity and security status of the aviation data network[2], the ADN can reconfigure the active devices and facilitate control network traffic during emergency situations.To provide more security, ADN includes some more features like

- Download of Flight Critical Data in Real-time
- Real-Time Video Surveillance
- Remote Controlling
- Flight Location Tracking.

4 SVSS: SMART VIDEO SURVEILLANCE SYSTEM

Every thing done on ADN can also applicable for SVSS[4]. But the main feature here is to provide the security for pilot cockpit too. It is accomplished by an Image Database server, Sensors, Cameras, Image comparator, selection MUX and Transducer. An Image Database Server consists of the images of crew members and monitoring details.

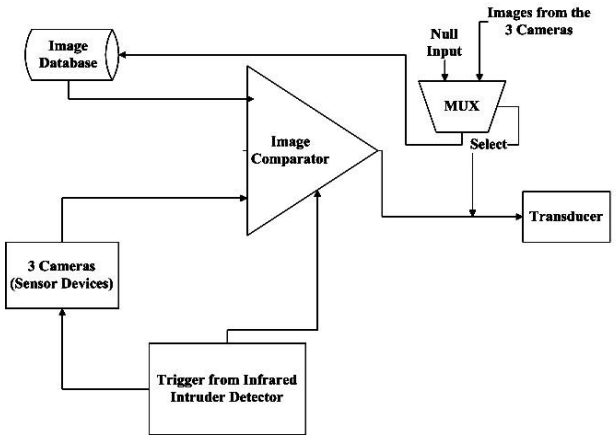

Fig. 1. *Block Diagram of the Control System*

The server also consists of the data of crew members based on the time of their shifts. The sensors are used to sense any type of Intrusion and activate the surveillance system. The high definition digital cameras are used to capture images of persons who enter the pilot cockpit. The system consists of three cameras.

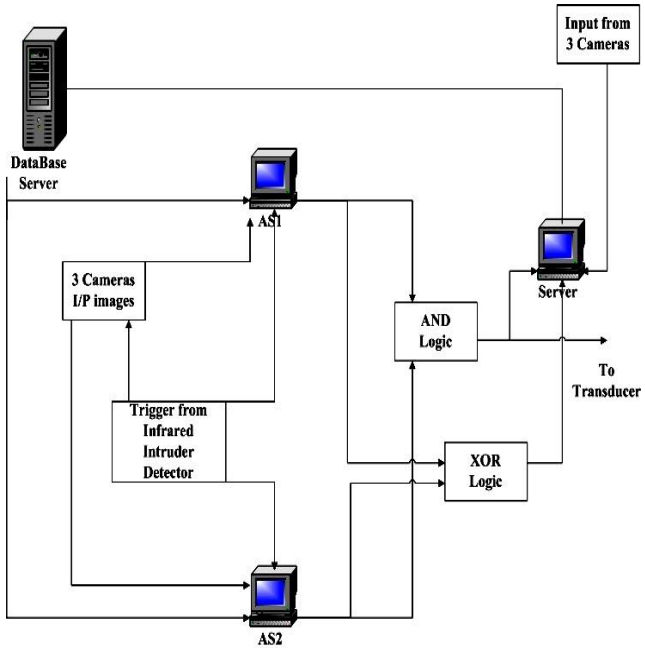

Fig. 2. *Comparator Diagram*

The Image Comparator runs a face detection algorithm[5][6] and tries to match the images available in the database server and the captured image. The output of the image comparator comes in binary form. The Selection MUX decides that the image should add to the database for future monitoring or not. The Transducer alerts the pilot by converting the output of the image comparator into multimedia form of data.

Table 1
Output of the Image Comparator

Output from AS1	Output from AS2	Match/No Match	Logic Operations
0	0	No Match	Both the AND and EXOR gates consider the output as'0'
0	1	No Match	AND, OR gates consider the output as 0 but EX-OR gates consider the output as 1
1	0	No Match	AND, OR gates consider the output as 0 but EX-OR gates consider the output as 1
1	1	Match	AND, OR gates consider the output as 1 but EX-OR gates consider the output as 0

5 KEY AGREEMENT SCHEME

Here, the concepts of AAP (Avionics Application Process)[3], NKMU (Network Key Management Unit) and AFDX (Avionics Full Duplex Ethernet)[8] are introduced. Using NKMU, all AAPs are controlled by its session key Agreement. The NKMU controls all communication devices of the aircraft. So that anyone can interfere in the secure communication devices. This results in the reduction of hijacking by impersonating the aircraft by false messages. So no more false messages can be received by the aircraft and the aircraft route cannot be changed. But the main disadvantage of this method is that, the system gives main control to the pilot. If the pilot is a wrong person, then nothing can be done. So the pilot must be honest.

5.1 Aircraft Security

The key agreement scheme will stop to hacking into aircraft-network. Now the aircraft also got secured by a series of biometric systems. Only the pilots can enter into the cockpit. The fingerprint and iris scan is done there. Also inside cockpit, the systems work only if the pilots authentication done through fingerprint and a video surveillance system to recognize the-face of the pilot. The face can be recognized at any direction by using the 3D object recognition technique[7]. Also there is a sensor at all passenger seats to sense any weapons. Any

weapon enter into the aircraft, it will give alarms to the pilots. Also a high surveillance system is done at the passage of cockpit and the passenger/crew area. Only pilot can enter in that area and some special powered crew members. Any other person on that area causes activation of alarms. So this technique gives a high security to the aircraft.

6 COMPARISON

The most secure Aircraft Security Monitoring System can find out by comparing the three techniques.

Table 2
Comparison Table

Parameters	Avionics Data Network	Smart Video-Surveillance System	Key Agreement Scheme
Network Architecture	Good	Good	Better than SVSS
Video surveillance	Time 2-3 hours only	Complete duration of flight	Complete duration of flight
Face Recognition Algorithm	None	Principle Component Analysis and Linear Discriminant Analysis	3D object recognition algorithm
Network hacking	Difficult to do, but possible	Difficult to do, but possible	Almost impossible
Security mechanism	IPSec and SSL/TLS	IPSec and SSL/TLS	AAP, NKMU and AFDX
Aircraft hijacking	Reduce the number very much	Very less possibility	Very less possibility
Security rate	50%	80%	90%

7 CONCLUSION

The Aircraft Security Monitoring System reduced the hijacking rate very much. But from the three techniques discussed above Smart Video Surveillance System and Key Agreement Schemes are much better techniques. Comparing both techniques, the Key Agreement Scheme is more secure. But the main disadvantage of all these techniques is that, if the pilot turns into a hijacker, nothing can be done. So, in future, a better technology is needed to avoid that kind of hijacking. For that, a technology which can give alert to nearby airport stations or air force/military stations when an aircraft turned to a wrong direction. Then a remote control facility is needed to control the aircraft from the ground station. Thus hijacking by the pilot can also be reduced.

REFERENCES

[1] N. THANTBRY and R. PENDSE, “Aviation data networks: Security issues and network architecture,” IEEE A&E SYSTEMS MAGAZINE, JUNE 2005.

[2] P. TINGEY and P.PARKINSON, “Secure networking for avionics systems,” DEFENSE PROCUREMENT ANALYSIS, 2003.

[3] M. S. A. N. THANTBRY and R. PENDSE, “Security, internet connectivity and aircraft data networks,” in IEEE CONFERENCE PAPER, 2005.

[4] A. S. K. N. NAGARAJA THANTHRY, INDIRA P EMMADI and R. PENDSE, “Svss: An intelligent video surveillance system for aircraft,” in IEEE CONFERENCE PAPER, 2007.

[5] D. Y. Y. GUANG DAI and Y. T. QIAN, “Face recognition using kernel-step discriminant analysis algorithm,” PATTERN RECOGNITION, vol. 40, pp. 229–243, 2007.

[6] M. G. KRESIMIR DELAC and S. GRGIC, “Independent comparative study of pca, ica and lda on the feret data set,” UNSKA 3/XII, 2006.

[7] R. C. W. ZHAO and J. PHILLIPS, “Face recognition in still and video images: A literature survey,” ACM COMPUTING SURVEYS, vol. 35, pp. 399–458, DECEMBER 2003.

[8] Q. L. DAHAI DU and Z. LI, “A key agreement scheme for avionics communications security,” in IEEE CONFERENCE PAPER, 2012.

[9] Z. C. SHENGBAO WANG and K.-K. R. CHOO, “Provably secure identity-based authenticated key agreement protocols without random oracles,” CRYPTOGRAPHY ePRINT ARCHIVE, pp. 1–16, 2006.