항공 통신 시스템에 대한 보안 고찰 - 네트워크 보안 관점

*박진혁, **김현성
*경일대학교 사이버보안학과
**(교신저자)경일대학교 사이버보안학과
e-mail : vkqxkr@naver.com, kim@kiu.ac.kr

Remarks on Security of Aeronautical Communication System - A Network Security Concerns

*Jinhyuck Park, **Hyunsung Kim
*Dept. of Cyber Security, Kyungil University
**(Corresponding author)Dept. of Cyber Security, Kyungil University

Abstract

Due to the recent developing technology of civil aviation industry, data lost and stolen rates are increasing. Thereby, the purpose of this paper is to understand and overview the current state of art in security of aeronautical communication system focused on network security. This paper reviews aeronautical communication system configuration and security threats and solutions. Finally, this paper will provide research directions for the network security concerns.

I. 서론

오늘날, 항공 산업이 교통관리시스템의 발전으로 꾸준히 발전하고 있다. IT(Information Technology: 정보기술)이 발전하면서 항공통신기술이 아날로그보이스를 사용하는 쪽에서 디지털데이터를 사용하는 방향으로 이동하고 있다. 하지만 통신기술이 발달함에 따라 항공통신시스템에 공격 및 보안기술도 이슈화 되고 있다 [1-2]. 만약 공격자에 의하여 공격을 당하게 된다면, 도청공격, 서비스거부공격, 은폐공격, 반복공격, 메공격 등이 발생할 수 있다. 또한 안드로이드기기를 통해 항공기에 네비게이션 정보를 제공하는 시스템을 하이제킹하여 통제하는 문제점이 있다 [3].

본 논문에서는 항공 통신 시스템의 구성에 대해서 알아보고 데이터링크 네트워크에 대한 공격과 그에 대한 보안기법을 알아보고 해결책을 알아본다.

II. 항공 통신 시스템 구성

본 장에서는 항공 통신 시스템의 구성 요소 및 통신 방안에 대해서 기술한다. 그림 1은 본 논문에서 초점을 맞추고 있는 항공 통신 시스템의 개요도이다 [4].

초단파대(Very High Frequency, VHF) 전파를 이용하는 항공이동 무선통신은 항공교통관제 무선통신, 운항관리 통신 등에 사용되며 중요한 통신으로서 역할을 하고 있다. VHF대의 전파전달은 직접파에 의한 가시거리내의 통화이기 때문에 전달거리는 비행고도에 따라 달라지지만 약 400Km범위를 갖는다. 주파수 간격은 항공기가 증가함에 따라 통신량이 비약적으로 증가하는 것에 대비하기 위해 채널 수를 확보하기 위해서 단계적으로 좁혀왔으며, 현재는 25KHz를 이용한다. 따라서 118.000MHz ~ 136.975MHz의 760개 채널을 사용한다.

VHF주파수 대역을 사용하여 비행기와 지상 네트워

크간 데이터 통신을 VHF 데이터 통신이라고 한다. 그 대표적인 시스템이 ACARS (Aircraft Communication Addressing and Reporting System) 이다. ACARS를 통해 항공기는 항공기 Push Back시간, 출/도착 시간, 항공기 결항 사항, 항공기 위치 등 항공기에서 생성된 데이터를 지상으로 송신한다.

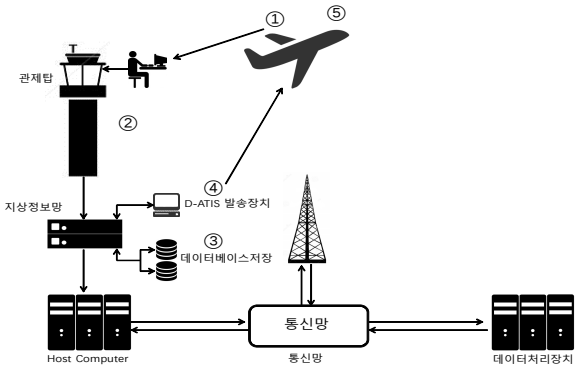

그림 1. 항공 통신 시스템 구성도

Ⅲ. 네트워크 보안의 잠재적 위협 및 해결책

보안 위협은 네트워크나 시스템 자산에 손실을 발생하는 잠재적인 행위로 정의할 수 있다. 네트워크 계층에 대한 공격을 위해 공격자는 무선 통신을 도청할 수 있다. 네트워크 상에서 공격자는 다음과 같은 능력을 가질 수 있다 [5].

- 공격자가 타인의 통신 메시지 M_1과 M_2를 캡춰할 수 있다면, 이들 메시지로부터 새로운 메시지 $M_1||M_2$를 구성할 수 있다.
- 공격자가 메시지 M을 알 수 있다면, $\{M\}_k$를 위조하여 전송할 수 있다.
- 공격자가 해쉬함수 $h()$와 메시지M을 안다면, 메시지의 해쉬값 $h(M)$을 계산하고 이용할 수 있다.
- 공격자는 난수를 임의로 생성할 수 있다.
- K에 관한 정보를 알고 있다면, 공격자는 $\{M\}_K$로부터 M을 추론할 수 있다.
- K_i^+에 대한 정보를 알고 있다면 공격자는 $\{M\}_{Ki+}$로부터 M을 추론할 수 있다.
- 공격자는 $M_1||M_2$ 이나 $M_2||M_1$ 로부터 M_1을 추론할 수 있다.

3.1 보안 요구사항

일반적인 통신시스템은 다음과 같은 6가지의 보안 요구사항을 제시할 수 있어야 한다 [6].

-기밀성: 통신 회선에서 주고받는 정보는 시스템 참여자들이 그 데이터에 대해 알 수 있도록 권한이 제시되기 전에는 노출되면 안 된다. 기밀성은 의도된 수신자만 읽을 수 있게 하기 위해서 원본 메시지를 송신하기 전에 암호화함으로서 획득할 수 있다. 프라이버시가 기밀성 서비스로서 고려될 수도 있다.

-인증: 통신에 참여하는 송신자 및 수신자는 자신이 통신하고 있는 상대가 요구할 시 자신의 신원증명을 제공할 수 있어야 한다. 인증은 일방향 인증이나 상호인증 형식으로 제시될 수 있다. 인증이 완료될 시, 공격자는 적법한 사용자인체 가장할 수 없다.

-무결성: 데이터는 항상 허가받는 사용자에 의해서만 수정될 수 있어야 한다. 이러한 보안특징은 인가된 사용자가 받은 메시지가 그 메시지가 보내질 때의 상태와 동일한지에 대한 입증을 통해서 가능하다.

-부인방지: 통신 참여자들이 메시지의 송신여부나 수신여부를 부인하지 못하도록 한다. 일반적으로 부인방지는 디지털 인증서나 디지털 서명과 같은 몇몇 암호학적 기법에 의해 제시될 수 있다.

-유용성: 서비스제공자에 의해 제공되는 네트워크 서비스와 컴퓨터 자원들은 그들의 고객이 필요로 할 때 항상 접근하고 이용할 수 있어야 한다. 이 보안 특징은 분산서비스거부공격과 같은 공격에 대해 보증하기 매우 어렵다.

-인가: 인가는 한 개체가 시스템 자원에 대한 접근의 권한과 허용을 체크하는 절차이다. 일반적으로 시스템이나 네트워크의 어떤 동작을 수행하기 위해 인가되기 전에 인증이 먼저 수행되어야 한다.

보통 이러한 보안 요구사항들은 항공시스템의 보안을 휘해서도 동일하게 필요하다.

3.2 데이터링크 공격

일반적인 데이터 링크 공격자를 고려하면 다음의 다섯 가지 잠재적인 공격으로 분류할 수 있다.

-도청공격: 공격자나 비 인가된 사용자가 ACARS와 같은 특정한 디코더나 Wireshark와 같은 네트워크 프로토콜 분석기를 이용하여 데이터 트래픽을 권한 없이 도청하려고 하는 공격이다.

-서비스거부공격: 공격자는 서버를 다운시키기 위해서 연결요청, TCP SYN flooding같은 메시지를 반복하여 서버에 전송할 수 있다. 이렇게 함으로서 특정 시점에 서버가 서비스를 제공하지 못하도록

할 수 있다 [7].

-가장공격: 공격자는 신뢰된 토신 참여자들을 속이기 위해서 인가된 사용자의 신원으로 속일 수 있다. 즉, 이 공격을 통해 중간자 공격 (Man in the middle attack)이 가능할 수 있다.

-재전송공격: 공격자는 두 명의 인가된 사용자간에 주고받는 데이터 링크 메시지를 캡춰해서 공격자가 필요할 때 이들 메시지를 재전송할 수 있다. 예를 들어 Needham등의 공개키 인증 프로토콜에서 공격자는 한 통신 세션에 참가한 두 명의 사용자간 주고 받는 메시지를 캡춰해서 뒤따르는 다음 세션에 이용할 수 있다 [9]. 이러한 공격은 데이터 링크 프로토콜이 보호되지 않아서 가능하다 [8].

-메시지변경공격: 공격자는 합법적인 사용자 간 주고받는 메시지를 지연, 변경, 재전송할 수 있다. 또한 공격자는 메시지 프로토콜 형식을 고려하여 위조된 메시지를 삽입할 수도 있다. 예를 들어 공격자는 항공 소프트웨어 데이터의 내용을 수정할 수 있다.

3.3 데이터링크 보안 기법

본 절에서는 데이터링크 공격에 대한 해결책으로서 관련 연구를 살펴본다.

-ACARS 메세지 보안: 연구에서는 항공 무선 통신 데이터 보안을 제공하기 위한 ACARS를 위한 AMS 프레임워크를 제안하였다. AMS는 존재하는 ACARS 기반구조를 사용한다. 상호호환성 때문에 ACARS 보안 솔루션은 응용계층에서 구현되어 왔다. 이 연구의 안전한 ACARS 관리자 응용은 통신 참여자들 간 안전한 연결을 설립하고 유지하기 위해 요구되는 모든 보안 특징을 제공한다. AMS는 통신 참여자들 간에 안전한 연결을 설립하기 위해타원곡선암호화 알고리즘 (Elliptic curve cryptosystem, ECC)에 기반 한 세션 키 설립 알고리즘을 이용한다 [9-10].

-안전한 CPDLC: Getachew등은 관제탑과 파일럿간 데이터 링크 통신 (Controller to pilot data link communication, CPDLC) 통신 시스템을 위한 ECC기반 인증 프로토콜을 제안하였다 [8]. 파일럿과 ATC 관제 시스템 간 상호인증이 가장공격과 스푸핑 공격 (Spoofing attack)을 피하기 위해 제공된다. 관제탑과 파일럿 간 CPDLC 데이터 통신을 설립하기 위해서 연결 관리자 (Connection management, CM)가 요구된다. CM은 로긴 서비스를 통해서 파일럿이 데이터 링크 서비스를 시작하고 각 데이터 링크 어플리케이션을 통해 정보를 제공할 수 있도록 해준다. CM은 로긴이 성공할 때만 관제탑이 CM이 제공하는 어떤 데이터 링크를 통해 통신할 수 있는지 정보를 제공한다. 메시지 인증을 위해서 HMAC (Hashed message authentication code)가 사용되고 PKI (Public key infrastructure) 또한 필요하다 [8-11].

-AADS와 EDS 보안: Robinson등은 EDS (Electronic distribution of software)라고 불리는 특별한 항공 네트워크 어플리케이션을 위한 보안 프레임워크를 제안하였다 [12]. EDS 어플리케이션은 항공기가 유지보수에 들어갈 때 소프트웨어나 데이터와 같은 정보를 분배하기 위한 목적에서 개발되었다. 이들 소프트웨어는 비행기가 착륙한 후에 사용되기 때문에 적재할 정보의 무결성과 신뢰성이 특히 보증되어야 한다. 그래서 Robinson등은 EDS 응용에 타겟된 보안 위협을 분석하고 EDS시스템의 안전을 위한 AADS (Airplane assets distribution system)을 개발하였다. AADS 시스템은 디지털 서명과 키 관리 및 분배 기법을 이용한다. 이 연구의 확장 연구로서 Robinson등은 AADS 시스템을 위한 두 가지 보안 기법을 제안하였다 [12-14].

-지상간의 보안: Karmakar등은 ANSP(Air Navigation Service Provider, 항공 네비게이션 서비스제공자) 도메인 외부의 지상 네트워크 상의 잠재적인 분산 네트워크 공격들을 해결하기 위한 몇 가지 가이드라인을 제시했다. 예를 들어 CSP(Communication service provider, 통신 서비스제공자)와 non-ASPN 인터페이스를 통한 네트워크 공격에 대응하기 위하여 원격지 기반이나 목적지 기반의 미터링 기법의 사용을 제안하였다 [12].

Ⅳ. 결론 및 향후 연구 방향

본 논문에서는 항공 산업이 발달함에 따라 항공 통신 시스템에 네트워크 보안이 이슈화되고 그것에 관한 공격 기법과 보안 기법에 관하여 알아보았다.

현재 ATS 통신은 안전성과 규제 정책으로 인해서 다른 형태의 통신과 엄격히 분리되어 운영되고 있다. 하지만, 증가되는 네트워크 통합의 요구로 인해서 네트워크 효율성을 향상시키고 유용한 자원의 사용의 효용성과 저비용성을 제공하기 위한 노력이 제시되고 있다 [15-16].

사사(Acknowledgement)

본 연구는 2010년 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 연구임(한국연구재단2010-0021575).

참고문헌

[1] 김명동, 박기식 "항공통신용 VDL(VHF Digital Link) Mode 3 시스템의 개요", *전자공학회지*, pp. 1043-1049, 2013.

[2] 김태식, 장재원, 김수홍, 강석엽 "다변측정감시(Multilateration) 시스템 국내개발 현황", *전자공학회지*, pp. 36-42, 2013.

[3] http://dailysecu.com/news_view.php?article_id=4179.

[4] http://blog.naver.com/tycheksh?Redirect=Log&logNo=40128931791.

[5] D. Dolev, A.C. Yao, "On the security of public key protocols," *Proc. of 22nd Annual Symp. on Foundations of Computer Science SFCS* '81, pp. 350-357, 1981.

[6] R. Shirey, Internet security glossary, Version 2, RFC 4949(Informational), 2007. http://www.ieth.org/rfc/rfc4949.txt.

[7] Ainoline,http://www.ainonline.com/aviation-news/ainalerts/2011-01-25/newark-airport-gbas-vulnerable-truckers-gpsjammers, 2013.

[8] D. Getachew, J. H. Griner, "An elliptic curve based authentication protocol for controller-pilot data link communications," *Proc. of ICNS Conference & Workshop*, 2005.

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

[10] ARINC, Draft 04 (strawman) of aeec project paper 823 datalink security, part 2: key management, 2007.

[9] R . M. Needham, M. D. Schroeder, "Using encryption for authentication in large networks of computers," *Commun. ACM*, vol. 21, pp. 993-999, 1978.

[10] G. Lowe, "An attack on the Needham-Schroeder public key authentication protocol," *Inform. Process. Lett.*, vol. 56, pp. 131-133, 1995.

[11] H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-Hashingfor message authentication," *RFC 2104*, http://www.ietf.org /rfc/rfc2104.txt 1997.

[12] R. Robinson, M. Li, S. Lintelman, K. Sampigethaya, R. Poovendran, D. v. Oheimb, J. U. Buauer, J. Cuellar, "Electronic distribution of airplane software and the impact of information security on airplane safety," *Proc. of International Conference on Computer Safety, Reliability and Security(Safecomp)*, pp. 28-39, 2007.

[13] R. Robinson, M. Li, S. A. Lintelman, K. Sampigethaya, R. Poovendran, D. v. Oheimb, J. U. Buauer, "Impact of public key enabled applications on the operation and maintenance of commercial airplanes," *Proc. of AIAA Aviation Technology, Integration and Operations Conference*, 2007.

[14] ISO, ISO/IEC 15408: Common criteria for information technology security evaluation, 1999.

[15] ICAO, ICAO Manual on required communications performance, Appendix N (Manual on RCP) to the Report, Technical Report Version 5.1, 2005.

[16] B. Mahmoud, M. Slim, P. Alain, L. Nicolas, "Aeronautical communication transition from analog to digital data: A network security survey," *Computer Science Review*, vol. 11, no. 12, pp. 1574-0137, 2014.