CPDLC 통합정보 보호를 위한 키교환 매커니즘

홍진근*, 김기홍**
*천안대학교 정보통신학부
**국가보안기술연구소
e-mail:jkhong@cheonan.ac.kr

Key Exchange Mechanism for CPDLC Integrated Information Security

Jin-Keun Hong*, Ki-Hong Hong**
*Dept of Information & Commmunication, Cheonan University
**National Security Research Institute, ETRI.

요 약

본 논문에서는 CPDLC 통합정보 전송환경에서 보안서비스를 제공하기 위해 사용되는 키교환 매커니즘에 대해 살펴보았고, 키 핸드쉐이크를 위해 요구되는 전송되는 프레임 구조 및 소요시간을 분석하였다.

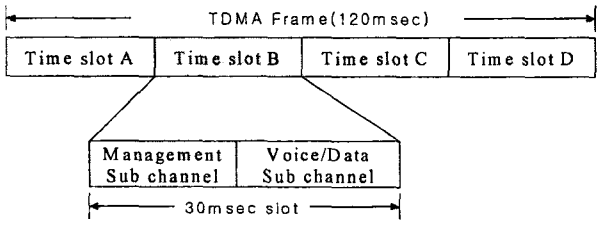
1. 서론

항공 트래픽 통제센터와 파일롯간 통신은 무선 음성 통신으로 이루어지며 2010년까지 지속적으로 매년 5% 항공 트래픽 증가가 예측되고 있다. 현재 IACO(international civil aviation ogranization) ATNP(ATN Panel)는 ATN을 위해 SARP (standard and recommend practices)에서 항공과 지상, 지상과 지상망에 무관한 단대단 프로토콜, 효과적인 데이터링크 사용을 위한 항공관련 어플리케이션 접속절차를 정의하고 있다[1]. LOS(line of sight) 데이터 링크에 관련하여 미 연방항공국(FAA)은 차세대 항공과 지상 통신 시스템(nexcom; next generation air ground communication)으로 새로운 디지털 음성 및 데이터 TDMA를 주창하고 있으며, 이에 대한 적용방식이 VHF 디지털 링크의 모드3(VDL Mode3)으로 알려져 있다. 1995년 ICAO는 VHF 항공통신 대역의 장기적인 솔루션으로 주창해오고 있으며, VDL Mode3은 31.5Kbps 전송속도와 25KHz 대역 및 종단간 지연은 250msec를 넘지 않도록 정해진다. 또 다른 방식으로 CSMA (carrier sense multiple access) 방식을 적용한 VDL Mode2로 AOC(aeronautical operational control)를 위해 매력적인 방식이다. ADS-B(automatic dependent surveillance broadcast)의 경우는 위치, 속도, 계획 정보의 LOS 방송통신을 위해 사용되며, ADS-B의 잠재적인 해결책으로 확장된 Squitter, S-TDMA (self-organizing TDMA; VDL-4), UAT (universal access transceiver)가 언급되고 있는 실정이다. Inmarsat 항공 위성통신 (SAT-COM)은 BLOS(beyond line of sight)의 ATC(air traffic control) 목적으로 사용하며, 많은 잠재적인 이용자들은 위성시스템 대신에 해양 ATC를 넘는 HFDL(HF data link)을 더 옹호하고 있는 실정이다. 본 논문은 CPDLC(controlled pilot data link communication) 통합정보 보호를 위해 제공되는 키 교환 매커니즘에 대해 살펴보았으며, VDL Mode3 링크를 통해 키 핸드쉐이크가 이루어질 때 전송구조 및 요구되는 소요시간에 대해 살펴보았다. 본 논문의 구성은 2장 VDL Mode3 링크에서 보안 매카니즘에 대해 살펴보고, 3장에서 CPDLC 통합정보를 보호하기 위한 키 핸드쉐이킹과정에서 키 교환

방안을 살펴보았으며, 4장에서 결론을 맺었다.

2. VDL Mode3 링크에서 보안 매카니즘

ATC(air traffic control)에서 CPDLC 사용은 향후 10년이상 ICNS (integrated communication, navigation and surveillance)을 위한 미래 항공통신의 한 부분으로 자리잡아가고 있다. VDL Mode3은 25KHz의 채널 대역폭과 43Kbps 전송속도, D8PSK 변조방식을 제공하며, 120msec의 TDMA로 구성되고 이때 각 TDMA 슬롯은 30 msec로 구성된다. 1개의 슬롯은 4개로 구성되며 1개의 슬롯에 496비트 데이터 또는 576비트의 음성이 실린다.



[Fig.1] VDL Mode3 채널 구조

항공 통신 트래픽은 변조, replay 및 변조 공격의 위험성과 함께 항공 CNS 및 ATM의 모든 영역에 서비스 거부 공격 등이 일어날 수 있다. VDL Mode3채널구조는 [Fig.1]에서 제시하였으며, Mode3 링크는 CPDLC 데이터가 로딩될 때 섹터에 의해 동등하게 공유가 가능한데, 이때 각 섹터에 부담해야 할 부하가 43Kbps peak/23 data channels 이면 각 채널당 1.9Kbps 최대 부하를 갖게 되고, 데이터 채널에서 최대 데이터 용량은 4.8Kbps, 가용한 용량은 4Kbps이다. 최악의 경우, 400기 항공기 가운데 60기가 단일 Mode3 채널에 위치해 있고, 이때 공유 가능한 최대 부하량은 43Kbps×60기/400기로 가정할 경우 6.45Kbps를 가지며 이 부하량은 단일 데이터 Mode3의 용량을 넘어서나 2개의 데이터 채널에 의해 쉽게 관리가 가능하다. CPDLC 정보보호를 위해 제공되는 서비스로는 항공과 지상간 메시지 인증, 데이터 무결성, 접근통제, 데이터 비밀성 기능이 있다. 적용되는 암호기법에는 대칭형 및 비대칭형 암호기법을 적용하며 이 기법들은 디지틀 서명, 키교환, 메시지 인증 등에 사용되며 알고리즘 설계를 위해 사용되는 암호 키의 길이는 해당년도에 만족할 만한 안전성을 제공하는 대칭형, RSA와 EC 비대칭형 키 길이를 비교한 내용을 [Table1]에서 제시하였다. 보안 프레임워크는 ISO/IEC 표준에 근거하며, ISO/ IEC 10181-1에서는 개방형시스템의 보안프레임워크[2]를, ISO/IEC 10181-2[3], 10181-3[4], 10181-6[5]에서는 인증, 접근제어, 데이터 무결성 기능을 정의하고 있다.

[Table1] 비도기준한 암호알고리즘 키 길이 비교

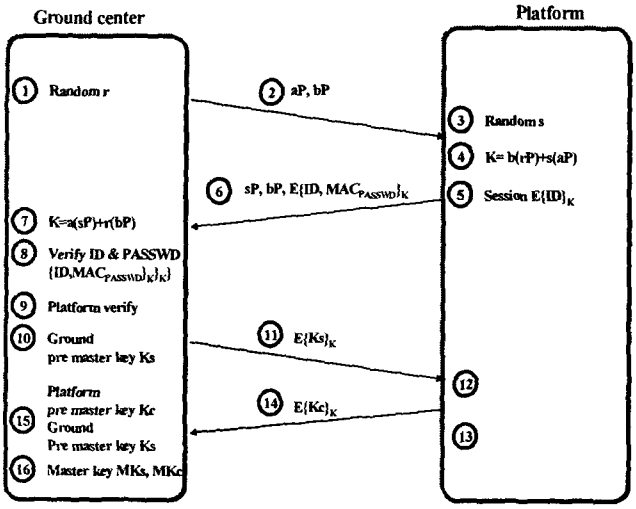
년도	대칭형 (bits)	비대칭형RSA (bits)	비대칭형 타원곡선(bits)
2010	78	1369	146
2020	86	1881	161
2030	93	2493	176
2040	101	3214	191
2050	109	4047	206

CPDLC 보호를 위해 제공되는 보안 매카니즘은 신뢰가 존재하는 엔티티간에 PKI(public key infrastructure)를 명시하고 있으며, ISO/IEC 9594-8[6]과 ITU-T X.509에서 PKI와 공개키 인증서 형식을 정의하고 있다. 2020년도에 최소한 보안 운용에서 디지털 서명이나 키 교환을 위해 사용가능한 키 길이는 타원곡선 알고리즘에서 161비트 키 길이는 만족되어야 한다. 이것은 좁은 대역폭을 제공하는 항공 지상간 데이터 링크 환경에서 종래의 RSA 방식의 1881비트 키 길이에 비하면 오버헤드를 줄임과 동시에 안전성을 강화하는 고무적인 일이다. 현재 MAC길이로 32비트를 명시하며, 사용되는 인증서는 ITU-T X.509 인증서를 표준으로 하되 ATN 압축된 인증서를 사용하고 이때 압축된 인증서에는 인증서 시리얼 번호, CA명, 유효기간, 소유주명, 소유주 공개키와 CA 서명이 포함된다. 압축된 인증서는 ISO/IEC 8825-2 형식에서 정의된 PER (packed encoding rules)에 의해 부호화되어 전송된다.

3. CPDLC 통합정보를 위한 키교환 방안

CPDLC를 위한 항공 트래픽 관리 응용을 구현하기 위해 항공 플랫폼과 지상에 종단시스템(ES)이 구현되고, 이때 PKI구현이 어려운 환경에서 항공과 지상간 통신보호를 위해 키 핸드쉐이크 과정은 [Fig.2]에서 제시하였다. 항공과 지상간 암호통신을 수행하기 위해서는 사전에 키 협상 및 교환에 관련된 핸드쉐이크 과정이 요구된다. 먼저 플랫폼이 지상센터로부터 인증받기 위해 ID, PASSWD 인증과정이 필요하고, 이로부터 플랫폼과 지상 센터간에 통신을 위한 공유 키 생성 과정과 생성된 공유키를 이용하여 메시지 암호용도에 사용될 pre master

key 생성 및 분배과정이 수행된다. 이때 pre master key는 사전에 양자가 랜덤 값으로부터 생성된 공통키를 통해 암호화되어 분배된다. CPDLC 보호구간은 채널대역폭이 제한되므로 이를 고려한 간략화된 인증과정과 감소된 키 교환 과정이 이루어진다.



[Fig.2] 항공과 지상간 핸드쉐이크 과정 블록도

이때 항공 플랫폼에서 지상 센터에 공통키를 생성하기 위해 사용되는 랜덤 값, 프레임 체크 시퀀스로 구성된 프레임이 먼저 전송되고, 지상 센터에서 항공 플랫폼으로 랜덤 값, ID, 패스워드에 대한 MAC 값, 프레임 체크 시퀀스 정보로 구성된 프레임이 전송된다. 또한 다음 과정으로 메시지 보호를 위해 사용되는 예비키인 pre master key가 공통키로 암호화되어 전송되고, 플랫폼과 지상센터에서 이 키를 수신하여 키 일치를 수행후 암호통신을 수행한다.

SP(16bits)	aP(161bits)	bP(161bits)	ID(48bits) MAC_PWD(48bits)	FCS(16bits)
SP(16bits)	352bits RS(31,15)	352bits RS(31,15)	ID, MAC_PWD(224bits)	FCS(32bits)

[Fig.3] ID/PWD인증을 위한 전송 프레임 구성

VDL Mode3에서 단일채널을 이용할 때, 채널이 밀집되지 않는 환경에서 보호 메시지가 4Kbps의 전송속도를 제공받는다고 가정한다. 항공 플랫폼 1기가 지상센터와 ID/PWD 인증 및 키 일치를 위해 요구되는 시간은 [Fig.2]에서 제시한 핸드쉐이크 과정을 기준으로 할 때, 평균 소요되는 시간을 [Table2]에서 제시하였다. [Table2]를 통해 VDL Mode3의 4Kbps 환경에서는 최소한 항공과 지상간 핸드쉐이크를 위해 요구되는 시간이 3sec가 필요하며, 이외에 인증서 요청 및 응답에 관련된 인증서 교환 과정이 추가되면 추가적인 시간이 요구된다.

[Table2] 키 핸드쉐이크 과정에서 소요시간 비교

전송 과정	전송 회수에 따른 전송 소요시간	
	1회	3회
과정②	0.364sec	1.092sec
과정⑥	0.42sec	1.26sec
과정⑪	0.06sec	0.18sec
과정⑫	0.06sec	0.18sec
전 체	0.904sec	2.712sec

그러나 항공통신에 사용되는 PER을 고려하여 전송되는 키 교환정보가 50% 정도 감소된다고 가정하더라도 키 핸드쉐이크 과정에 소요되는 1.5~2sec이 필요하다.

4. 결론

본 논문에서는 항공과 지상간 CPDLC 정보를 교환할 때, VDL Mode3에서 운용되는 무선환경에서 메시지의 비밀성, 무결성, ID인증을 보장하기 위해 키 교환 매커니즘을 적용할 때 소요되는 정보량과 시간 측면에서 영향을 분석하였다.

참고문헌

[1] Blake-Wilson, Simon, E.F.C. LaBerge, Michael Olive, Aloke Roy, 2000, Overview of the Security Concept and Architecture for the Aeronautical Telecommunications Network (ATN), Version 0.5(Draft), Columbia, Maryland, Honeywell.

[2] ISO/IEC Joint Technical Committee 1, 1996, Information technology-open systems inter connection-security frameworks for open systems: overview, ISO/IEC 10181-1:1996, Geneva, Switzerland, ISO/IEC.

[3] ISO/IEC Joint Technical Committee 1, 1996, Information technology-open systems inter connection-security frameworks for open systems: overview, ISO/IEC 10181-2:1996, Geneva, Switzerland, ISO/IEC.

[4] ISO/IEC Joint Technical Committee 1, 1996, Information technology-open systems inter connection-security frameworks for open systems: overview, ISO/IEC 10181-3:1996, Geneva, Switzerland, ISO/IEC.

[5] ISO/IEC Joint Technical Committee 1, 1996, Information technology-open systems inter-conn ection security frameworks for open systems: overview, ISO/IEC 10181-6:1996, Geneva, Switzerland, ISO/IEC.

[6] ISO/IEC Joint Technical Committee 1 Subcommittee 6, 1998, Information technology- open systems interconnection- Directory: authentication framework, ISO/IEC 9594-8:1998, Geneva, Switzerland, ISO/IEC.