한국산학기술학회논문지
Vol. 10, No. 1, pp. 122-127, 2009

항공통신 네트워크에서 보안구조 및 모델

홍진근[1*]

Security Architecture and Model in Aeronautical Communication Network

Jin-Keun Hong[1*]

요 약 본 본 논문은 항공 교통 체계에서 가장 중요하게 고려되는 안전한 항공체계에 대한 연구를 중심으로 보안구조를 검토하고 보안모델을 제시하였다. 분석된 내용은 항공서비스 분야 관련 보안기술을 기반으로 국제적인 기술 동향과 함께 국내의 항공체계에 대한 보안모델을 다루고 있다. 항공통신 네트워크의 보안 프레임워크에서는 항공과 지상 데이터링크 보안기술, 항공체계에 따른 보안구조를 분석하였고 U-information HUB 모델의 보안구조를 제시하였다. U-information HUB 보안구조는 항공사, 공항 네트워크, 항공기, 관련 정부기관 등과 연동범위를 포함하고 있다.

Abstract In this paper, it is reviewed security architecture and proposed security model about secure aeronautical system, which is considering in the cynical research topics out of aeronautical traffic system. The reviewed contents is treated about security model for domestic aeronautical system with international security technology trends in the basis of security technology related aeronautical services. In the security framework of aeronautical communication network, it is analyzed data link security technology between air and ground communication, and security architecture in according to aeronautical system, and presented security architecture of U information HUB model. The security architecture of U-information HUB includes the internetworking scope of airline, airport network, airplane network, and related government agency, etc.

Key Words : Aeronautical, Security

1. 서론

국내의 경우 항공 교통량은 2014년까지 승객이 2배, 화물이 2.5배 증가가 예상하며, 미국의 경우 교통량은 2006년 7억5천명에서 2012년에 10억명 이상을 예상하고 있다[1]. 우리 정부는 차세대 지능형 공항시스템 구축, 차세대 항행 안전기술 연구 개발 로드맵 수립, 항공관제용 통합 정보처리 시스템 개발 등을 추진 중에 있으며 이 사업이 완료되면, 2020년 까지 항공 물류 수송량 급증에 대처하고, 동북아 허브 공항으로서의 목표 달성과 국제 항공 안전의 감화에 따른 안전체계 마련의 기틀이 될 수 있다고 예측하고 있다[1-3].

유럽은 현재의 사용하고 있는 공항 환경과 기구축된 시스템을 사용할 경우, 2010년이 되면 유럽 상위 20개의 공항에서 정체가 예상되며, 공항과 항로의 포화와 함께 안전성의 저하, 정체, 지연이 발생할 가능성이 매우 높다고 판단하고 ICAO(International Civil Aviation Organization, 국제민항기구)에서 차세대 항행시스템 (CNS (communication, navigation, surveillance)/ ATM (Air traffic management)) 전환 계획을 추진하고 있는 실정이다[1]. 그런데 항공의 선진화와 함께 중요하게 고려되는 요소 가운데 하나가 보안대책 마련이다[1-7].

항공 체계의 보안 연구와 관련한 기존연구에서, 미국은 안전한 항공 데이터 서비스를 제공하기 위해 FAA와 국방성의 항공 네트워크 관련부서를 주축으로 보안성 및 안전성에 대한 연구가 수행되고 있다[4]. Mark 등이 발표한 ACP WGN05 WP10 발표에서는 ATN 보안 상호 운용성 시험과 상황 관리에 대한 내용을 주제로 하고 있으며, ICAO ATN 구현 3차 회의 AMHS IPS 개발에 관한 내용이 발표된 바 있다[6].

[*]백석대학교 정보통신학부
[*]교신저자: 홍진근(jkhong@bu.ac.kr)
접수일 08년 12월 12일 수정일 09년 01월 07일 게재확정일 09년 01월 16일

미국의 NASA GRC(Glen Research Center)에서는 secure aircraft for system information flow(SASIF) 취약성을 평가한 바 있으며, Secure Aircraft Data Network (SADN) 사이버 위협에 대한 보안 연구를 2005년과 2006년에 걸쳐 수행한 사례가 있다. 미 공군은 2006년과 2007년에 걸쳐 Airborne Network & CPSG(Cryptologic Protection Systems Group)에서 Phase1(Joint USAF/Civil AN에 관련하여 안전한 항공 네트워크를 위한 R&D 계획 수립)과 Phase 2(Joint AN의 IA 정보 요구와 관련된 워크샵 추진 및 공동 협력)을 추진해 오고 있는 실정이다.

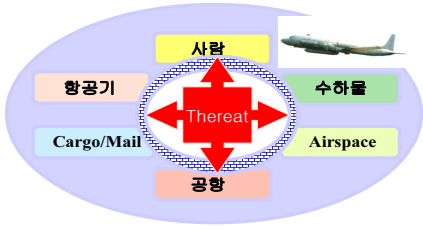
FAA 또한 보잉 B-787 SACO (Seattle Aircraft Certification Office)를 오픈하고 인증 관련 업무를 추진하고 있는 실정이다.

본 논문은 새로운 시대 새로운 환경의 항공 교통 체계에 대한 연구와 투자가 이루어지고 있는 환경에서 가장 중요하게 고려되는 안전한 항공체계에 대한 연구를 중심으로 보안구조를 분석하고 보안모델을 제시한다. 분석된 내용은 항공서비스 분야에서 세계적인 보안기술을 기반으로 국제적인 기술 추이와 함께 국내의 항공체계에 대한 보안모델을 제시하였다. 본 논문의 구성은 2장에서 항공네트워크 서비스와 보안기술을 소개하였고 3장에서 항공통신 네트워크의 보안 프레임워크를 기술하였으며 4장에서 결론을 맺었다.

2. 항공네트워크 서비스와 보안기술

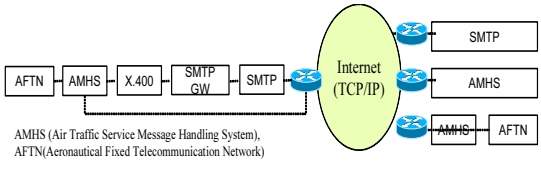
미래의 항공분야의 보안 기술은 새로운 수요량과 다양성을 수용할 수 있어야 하며 계획되지 않은 오퍼레이션 차원으로 확대되는 서비스에 대해서도 수용 가능하여야 한다. 이러한 차원에서 항공 보안 및 지원 계획이 국가적인 차원에서 마련되어야 하고 이를 기반으로 활동과 협력이 요구되고 있다. 차세대 넷 기반에서 요구되는 공유되는 상황 인식 기반 하의 운용에 대한 연구가 Catherine Bolczak 등에 의해 이루어진 바 있다[7]. 차세대 넷 중심의 보안프레임워크가 필요한 주요 서비스와 관련하여 그림1에서 제시하였다.

안전한 비행은 통합된 위험관리 측면에서 비행체와 리스크의 프로파일의 안전한 관리가 요구되며 인증된 오퍼레이션과 제약조건만이 제한된 비행 공간에 접근할 수 있도록 조치되어야 하며 검증되도록 하여야 한다. 즉 접근성이나 리스크 프로파일 요구조건 영향 측면에서 위치, 규모, 시간으로부터 제한 받도록 설계되어야 하며 항공기에 탑재된 인적 및 물적 요소가 보안 고려사항을 기반으로 관리되어야 한다. 이를 위해서는 항공기 트래픽 관리, 비행 계획이나 운용, 보안, 법률적인 강제사항 등의 측면에서 정보가 공유되어야 한다. 미국은 항공시스템 보안과 관련하여 WG-72에서 ADN 인증을 시작으로 2008년~2010년까지 WG-72와 SSDS 인증 프로젝트를 추진하고 있으며, FAA와 국방성은 항공데이터 망의 프로젝트 중복성을 정리하고, 안전한 ADN을 인증을 위한 SADN 도구 및 프로세스, 로드맵, 보안정책 수립을 하고 있다. 또한 항공보안과 관련된 연방정책 수립, 항공 네트워크 인증 요구사항 정의 (NIST 800-37, 800-2626), 보안 테스팅 기법, 침투 테스팅 프로세스나 테스팅 도구 (I&A, 감사, IDS 등) 개발, EUROCAE를 포함한 ADN용 국가 정책 명세서 개발, ADN용 FAA 인증을 위한 로드맵을 수립하고 있다.



[그림 1] 차세대 넷 중심의 보안 프레임워크

AMHS 기반의 SMTP의 구현을 그림2에서 제시하였다. AFTN 형식의 헤더는 호스트 컴퓨터나 비행 데이터 입출력 등과 같은 프로세싱 시스템, 디스플레이, 비행 데이터 파일링과 호환되어야 하며 TCP/IP 기반으로 대체되어 가고 있다. 따라서 X.25를 기반으로 하는 AFTN의 경우 온라인 바이러스에 대한 대책과 악의적인 공격에 대한 보안과 네트워크 방어 개념이 제공되어야 하며, RFC1006의 AMHS 또한 공개된 인터넷 망으로부터 ATC TCP/IP 네트워크 분리를 강화할 수 있는 라우팅 정책과 네트워크 보호가 필요하다.



[그림 2] 항공 어플리케이션 서비스에 따른 TCP/IP 네트워크

공개된 인터넷에 사용되는 이메일 서비스의 경우 현재 민간 항공에서도 네트워크 방어대책과 보호에 대한 가이드라인이 요구되고 있다.

3. 항공 통신 네트워크의 보안 프레임워크

항공통신 시스템의 유형에는 VHF 데이터링크 시스템, 위성통신 시스템, 공항통신 시스템, 항공과 항공간 통신 시스템으로 구분되며, 지상과 항공간 통신시스템에 VDLM2/3, HFDL, 3G 등이 있으며, 위성통신 시스템으로 INMARSAT, SDLS, IRIDIUM, SATCOM 등이 있다.

또한 항공과 항공간 통신 시스템으로 1090 ES, UAT, VDLM4, P-25/-34 등이 있다. 공항 통신을 지원하는 시스템으로 ADL, IEEE802.11, IEEE 802.16, IEEE 802.20 등이 있다. IP 기반의 항공기 LAN 구조를 그림3에서 나타내었다.

3.1 항공과 지상 데이터링크 보안기술

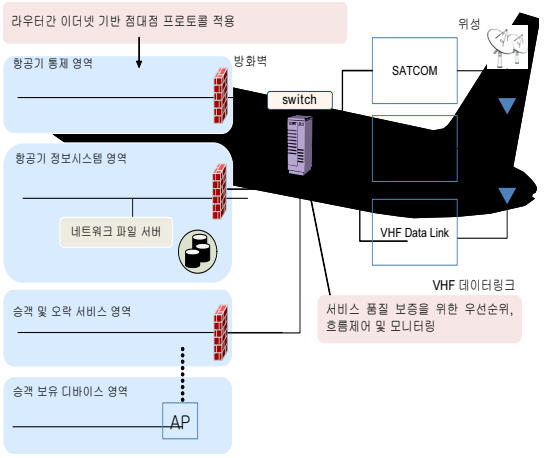
ACARS 메시지 보안을 위해 제공되는 비대칭키 크기는 공개키 및 개인키가 233비트를 적용하고 대칭키를 위해 128비트의 비밀키가 사용된다.

1) 대칭키 관리

NIST 권고(SP800-57)에 따르면 암호주기가 항공기와 지상 엔티티에 공유된 비밀키는 최대1년까지 사용가능하도록 설계되어야 한다.

2) 개인키와 공개키

항공기 엔티티와 지상 엔티티에는 개인키와 개인키를 운용하기 위해 최대 3년간 운용할 수 있도록 설계되어야 한다.



[그림 3] IP 기반의 항공기 LAN 보안 구조

3) 공개키 인증서 기반

NIST SP800-57, ATA DSWG AMS 인증서 정책에 따르면, 공개키 인증서를 기반으로 사용하는 경우 항공기에서 지상 CRL이나 인증서 승인 가능한 메커니즘에 접근할 수 있다면 최대 3년을 운용할 수 있도록 하고 접근이 어려울 경우 최대 8일까지 사용할 수 있도록 설계되어야 한다.

3.2 Airport 보안

1) RFID 구축망[8-11]

공항 내에서 사용자 정보는 강한 패스워드, ACL, 암호 및 백업 및 복구에 대한 전략을 수립해야 한다. 특히 다중 목적의 이동형 RFID 시스템은 항공사와 공항 네트워크 및 제작사 네트워크간 연계되어 있다. 에어 프랑스의 경우 샤를드골공항과 암스텔담 공항간 수하물에 대한 RFID 상호 연동시험을 수행한 바 있다. 또한 RFID 프로토콜에 SHA-256 설계 사례에 대한 연구가 이루어진 바 있으며, RFID 보안 프로토콜로 PRF, Hash, Hah+PRNG, AES+PRNG 등이 적용되고 있다.

2) 심층방어 개념의 보안 적용[12-13]

공항 네트워크는 DiD 개념을 기반으로 송신기 전력 통제, MAC 주소 접근통제, 라디우스 인증 서버 지원, LEAP (lightweight extensible authentication protocol)을 지원하며 WPA (Wi Fi protected Access) 기반으로 한다. WPA & WPA2 기업을 위해서는 TKIP, 802.1x, MIC, EAP를 지원하며, 802.1x/EAP 인증 메커니즘(TLS, TTLS, PEAP)를 적용하고, WPA personal을 위해서는 128비트 TKIP를 적용되도록 설계한다. WIPS는 무선 랜 넷 상에서 보안 위협에 대한 탐지 및 방해, 차단 및 방어 해법으로 사용되고, TKIP는 사용자별, 세션별, 시간별, 프레임별로 동적으로 변하는 암복호 키를 재생성하고 변경하여 사용한다.

3.3 항공체계에 따른 보안구조

1) ACARS 체계

ACARS 체계는 어플리케이션 계층 보안을 위한 방안이 마련되지 않고 있으나 ATN 보안 서비스를 기반으로 적용할 수 있다. 별도의 네트워크 보안 방안이 제공되지 않으며 항공기내 LAN 보안 또한 마련되지 않고 있으나 제한된 물리적인 영역에 한하여 적용되고 있다.

2) ATN (CLIP) 체계

ATN 체계는 어플리케이션 계층을 위한 보안 서비스를 제공하고 있으며 네트워크 계층을 위한 별도의 보안 서비스가 제공되지 않으나 선택적으로 링크 인증과 암호를

적용할 수 있다. 항공기내 LAN 보안을 위해 보안서비스를 제공하지 않으나 제한된 물리적인 영역에 대해 접근할 수 있도록 하고 있다. ATN 메시지 보안 관점에서는 메시지 보안을 위해 ATN 인증 프로토콜이 제공되어야 하고 HMAC-SHA 같은 안전한 해쉬 알고리즘을 적용하여야 하며 IPSec을 적용한다. IKEv2를 적용하고 ATN 키 수립 상황인식 정보는 상황인식 단계에서 키를 수립하고 그렇지 않으면 사전에 고유된 항공용 보안 키 수립을 진행한다. 보편적으로 항공용 키 수립은 사전에 공유된 방식을 많이 이용한다. CPDLC를 사용하는 ATN 보안 인증 절차는 다음과 같다. 1단계에서 ATN 디지털 서명기법을 사용하여 CM 로그온 메시지를 서명하고, 2단계로 지상 CM은 항공기와 지상 CPDLC 공개키 인증서를 검색하며, ATN 디지털 서명 기법을 사용하여 CM 로그온 메시지를 검증한다. 3단계에서 지상 CM은 ATN 키 일치 기법을 사용하여 CM 세션키를 유도하며, 4단계에서 지상 CM이 ATN MAC 기법을 사용하여 태그된 CM 응답 메시지 내에 지상 CPDLC 어플리케이션의 공개키와 공개키 인증서를 전송한다. 5단계로 항공기는 ATN 키 일치 기법을 사용하여 CM 세션키를 유도하며, 6단계로 항공기가 ATN MAC 기법을 사용하여 CM 응답 메시지 상에 테그를 체크한다. 7단계에서 지상 CPDLC가 항공기 공개키를 획득하고 8단계에서 지상 CPDLC가 ATN 키 수립 기법을 사용하여 CPDLC 세션키를 도출한다. 9단계에서 항공기는 ATN 키 수립 기법을 사용하여 CPDLC 세션키를 도출하고, 마지막 10단계에서 연속적인 CPDLC 메시지가 ATN MAC 기법을 적용하여 태그되고 체크된다. ATN 보안서비스를 위한 주요 알고리즘을 표1에서 나타내었다.

[표 1] ATN 보안 서비스를 위한 보안알고리즘

용도	적용 보안 알고리즘
데이터 출처 인증/무결성	HMAC-SHA-160 HMAC-RIPEMD-160
데이터 암호	AES(128, 192, 256) Triple DES(112) IDEA(128), RC5(≥128), CAST-128, Blo wfish (≥128)
사용자 인증용 공개키알고리즘	IPSec IKE지원 사전공유 비밀키 공개키 디지털 서명

3) IP Near Term 체계

미국의 경우 어플리케이션 계층을 위해 제한적으로 SWIM 보안 서비스를 제공하는데 ATN 보안 서비스를 기반으로 한다. 네트워크 보안을 위해라우터간 IPSec을 적용하며 선택적으로 링크 인증과 암호를 지원한다. 항공기내 LAN 보안은 적용하고 있지 않으나 제한적으로 물리적인 접근을 적용하고 있다.

4) IP Long Term 체계

어플리케이션 계층 보안을 위해 제한적으로 SWIM 보안 서비스가 적용되는데 ATN 보안 서비스를 기반으로 한다. 네트워크 계층의 보안 서비스는 비용을 고려하여 DiD 수준의 IPSec이 적용되어야 하며 선택적으로 링크 인증과 암호를 제공한다. 항공기내 LAN 보안을 위해 항공기 통제나 방화벽 등이 적용될 수 있다. ATN 보안 메커니즘별 적용하고 있는 알고리즘을 표2에서 제시하였다.

[표 2] ATN 보안 메커니즘별 적용 보안알고리즘

보안 서비스	메커니즘	보안 알고리즘		
		DoD class3	ATN SARPs & secure ACARS	항공 망(SWIM)
데이터 무결성 /인증	디지털 서명	RSA PKCS#1	ECDSA FIPS186-2	ECDSA FIPS186-2
	메시지 인증	HMAC SHA-1 (RFC 2104)	HMAC SHA-1 (RFC 2104)	HMAC SHA-1 (RFC 2104)
	해쉬	SHA-1 FIPS180-1	SHA-1 FIPS180-1	SHA-1 FIPS180-1
기밀성	암호	Triple DES FIPS 46-3	AES FIPS-197	AES FIPS-197
키 설정	키 동의	RSA PKCS#1	ECDH ANSI X9.63	ECDH ANSI X6.63
	공개키 인증	ITU-T X.509	ITU-T X.509	ITU-T X.509
메시징		비사용	특정 어플리케이션 계층	IPSec/TLS/특정 어플리케이션 계층
적용 영역		비사용	항공과 지상간	모든 네트워크

3.4 항공기 자산 환경에서 보안 요구사항

항공기 설계 및 운용과 관련하여, AEEC ADN (ARINC664), AEEC Security 위원회(ARINC811), AEEC 소프트웨어 분배(ARINC666), AEEC 데이터링크 보안, EUROCAE WG72(항공 시스템 보안) 등에서 정의하고 있다. 항공기 제조, 운용, 유지 보수에 관련된 주요 프로세스를 네트워크 기반으로 처리함으로써 효율성을 강화하고 있다. 그러나 네트워크 기반의 항공기 소프트웨어 및 관련 정보의 안전성에 영향을 미칠 수 있으며 이에 대한 연구가 이루어지고 있다. 항공기 자산을 분배하는 체계를 고려할 때 CC 보호 프로파일로 무결성을 위해서는 EAL 7등급을, 인증을 위해서는 EAL 6등급이 최소사양으로 요구되고 있다. 또한 항공기 상태에 대한 모니터링 관리를 지원하는 보안 프레임워크 마련이 요구되고 단대단, 실체와 실체간 무결성 보호와 함께 운용 및 유지 보수 측면에서 PKI를 적용하는 문제가 고려되고 있다.

3.5 U-information HUB 모델의 보안구조

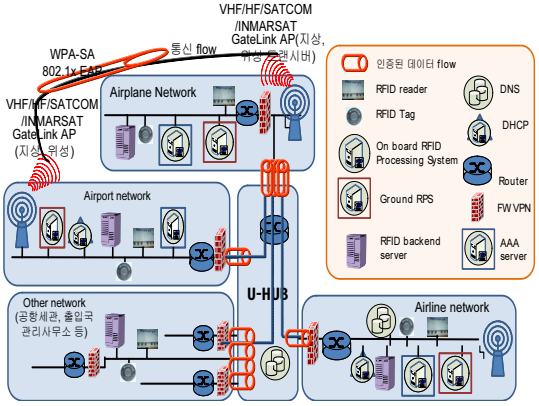
국내에서 추진하고 있는 U-information HUB 모델의 개념을 기초로 하여 요구되는 보안 구조를 제안하고자 하며 그림4에서 나타내었다.

1) 항공사 네트워크

항공사 네트워크는 VPN 방화벽을 갖는 시스템, 라우터 장비, DHCP 서버, DNS 서버, AAA 인증서버, 어플리케이션 서버 등이 기본시스템으로 구성되며 공항 네트워크와 선택적으로 인증 접속이 가능한 체계가 필요하다. 또한 항공기 네트워크와도 SSL SA 보안접속이 형성되도록 U- information HUB를 구성하는 것이 필요하다.

2) 공항 네트워크

공항 네트워크는 AAA 인증서버, DHCP, DNS, 라우터, 방화벽 시스템, GateLink AP 등이 기본시스템으로 구성되며, 통신 flow는 U- information HUB를 통해 항공사 네트워크와 연동되고 항공기 네트워크와 지상 및 위성 트랜시버를 통해 접속되도록 구성한다. 또한 WPA SA 기반으로 보안 접속이 이루어지도록 구성하며 802.1x 포트 기반 EAP 인증 방안 등을 적용한다. 항공기 내에서도 항공사와 항공기 내 VPN 채널을 기반으로 접속이 가능하도록 구성한다.



[그림 4] U-Information HUB 모델 기반의 보안구조 제시 예

3) 항공기 네트워크

항공기 네트워크는 주로 지상통신과 비행중 무선장비를 활용한 통신, 위성을 활용한 통신 등으로 구분된다. 항공기 통제 영역은 VHF/HF /SAT COM 링크장비를 기반으로 지상과 통신이 이루어지며 항공기 정보 서비스를 위해 GateLink 등을 활용하고, WLAN 접속 서비스를 제공하도록 구성한다. 또한 승객 정보나 오락 서비스 등을 위해서는 지상과 INMARSAT 등 위성을 활용한 광대역 서비스가 이루어진다.

4. 결 론

본 논문은 항공교통 체계에서 고려되는 안전한 항공체계를 위한 보안구조를 분석하고 보안모델을 제시하였다. 분석된 내용은 항공서비스 분야에서 보안기술을 기반으로 국제적인 기술 동향 및 국내의 항공체계에 대한 보안 모델을 제시하였다.

참고문헌

[1] 건설기술평가원, “차세대 지능형 공항 시스템 개발 기획 연구보고서,” 2007. 10.

[2] 건설기술평가원, “항공관제시스템 개발 기회 연구보고서,” 2007. 10.

[3] 교통개발연구원, “항공안전 중장기 종합계획 수립을 위한 기초연구,” 2007. 3.

[4] Kevin Harnett, "Cyber Security Research Plans for a Secure Aircraft Data Network(SADN)," The proceeding of NASA ICNS2006 Conference & Workshop, May 2006.

[5] Mark Brown and Frederic Picard, "Aeronautical Communication Panel: WG N-Networking, WGN4-Security : Context Management and ATN Security Interoperability Testing between ENRI and STNA," Report of ACP WGN05 WP10, 2005.

[6] Hoang N. Trans, "Review ATN related developments in the Aeronautical Communication Panel: AMHS IPS development," Report of 3th meeting of ATN implementation co ordination group of APANPRIG, May 2008.

[7] Catherine Bolczak, Chih Chia Vanessa Fong, "Shared Situational Awareness to Meet future Airspace Security Mission Needs," The proceeding of ICNS2008 Conference, May 2008.

[8] 인천국제공항공사, “항공화물 국가경쟁력 강화를 위한 공통RFID 인프라 구축자료,” 2007. 2.

[9] 한국전자통신연구원, “RFID/USN 산업동향 및 발전전망,” 2005. 6.

[10] 아시아나IDT, "RFID 적용사례 및 향후 전망,“ 2008. 2.

[11] 장윤석, 정상효, 류재신, “차세대 지능형 공항 시스템 개발 - 실시간 화물지원 자원 추적관리 연구,” 한국

항공경영학회 2008 춘계학술대회 자료집, 2008. 5.
[12] Richard V, Robinson, Mingyan Li, Scott A. Lintelman, Krishna Sampigethaya, Radha Poovendran, David von Oheimb, jens-Uwe Buber, "Impact of Public Key Enabled Applications on the Operation and Maintenance of Commercial Airplanes," AIAA Aviation Technology Integration, and Operations (ATIO) conference, Belfast, Northern Ireland, 18-20, September 2007.
[13] Bob Eichler, "6 steps to information security at an Airline," ATA e-Business Forum, October 17-19, 2007 Miami Beach, FL.

홍 진 근(Jin-Keun Hong) **[정회원]**

- 2008년 12월 현재 : 백석대학교 정보통신학부 교수

<관심분야>
전술통신, 센서넷, RFID, 무선랜 보안