http://dx.doi.org/10.14400/JDPM.2013.11.12.303

전술통신 환경에서 전송 성능 분석 및 보안 정책

홍진근*
백석대학교 정보통신학부*

The Transmission Performance Analysis and Security Policy in Tactical Communication Environment

Jinkeun Hong*
Division of Information and Communication, Baekseok University*

요 약 본 논문에서는 미군 전술통신 운용환경과 정책, 전술링크에서 보안정책 및 전달성능을 분석하였다. 운용환경에서는 운용통신 메시지와 반자동 전투력을 지원하는 프레임워크, 링크계층의 SINCGARS 사양을 살펴보았고, 전술 보안정책에서 COMSEC 정책과 응용계층 보안을 분석하였다. 또한 전술 통신환경에서 전송 성능 및 보안 동기 검출 측면에서 분석하였다. 전술링크와 COMSEC 보안정책은 AFKDMS, AKMS, RBECS, KIV-7/HSB 암호디바이스와 같은 측면에서 분석하였다.

주제어 : 보안정책, 전술통신, 전투 환경, 전송 성능

Abstract This paper analyzed about operation environment and policy for US military tactical communication, and security policy and transmission performance of tactical link. It is presented operation communication message and framework, which is supported semi automated force, SINCGARS specification of link layer in operation environment, and analyzed COMSEC policy and application layer security in tactical security policy. Also it analyzed in respect to transmission performance and crypto synchronization detection. Security policy of tactical link and COMSEC is analyzed in respect of crypto device such as AFKDMS, AKMS, RBECS, KIV-7/HSB.

Key Words : Security Policy, Tactical Communication, Combat Environment, transmission performance

1. 서론

미군은 일반 사이버 보안정책과 함께 군사 사이버 정책 또한 C&A 전환 목표, DoD 정보기술, 사이버 보안 어플리케이션 주기, 통제 결핍 수준과 위험 개념, 보안 상호관계성, 타임라인 측면에서 접근하고 있다. 미군의 정책은 상호의존성을 가지는데, NIST, DoD, NSS/IC가 그렇다. NIST에서 SP800-39(위험관리), -53(보안 통제), -37(위험관리 프레임워크), -137(연속 모니터링, RMF), -30(위험 평가), -53A(보안통제 평가)를 개발하며, 이 정책이 DoD의 DoDD 8500.1/2(보안통제 가이드, 엔터프라이즈 IA 거버넌스), 8510.01(위험관리 프레임워크 구현

Received 25 October 2013, Revised 27 November 2013
Accepted 20 December 2013
Corresponding Author: Jin-Keun Hong(Baekseok University)
Email: jkhong@bu.ac.kr

ISSN: 1738-1916

가이드)에 반영된다. 또한 NSS/IC의 CNSSP 22(NSS용 IA 위험 관리 정책), 1253, DJSIG가 마찬가지로 DoDD에 반영된다. 전술보안 정책 또한 사이버 보안정책 측면에서 이해할 수 있다. 미군의 사이버 보안정책은 우선 임무 및 전투 중심이며, DoD CIO의 전략 및 우선순위, DCIO 사이버보안 우선순위, 개발되는 연방정책과 표준에서 리더십, 연방 정책과 표준에 초점을 맞추고 있다. 사이버보안 정책 개발은 NIST를 중심으로 연방정책, CNSS의 국가보안정책, DOD정책으로 이루어진다. 미 국방부의 경우 정보보안 정책과 관련하여, DoD CIO는 언터프레이즈 관점에서 IT 거버넌스 보드 재구조화, DoD IT 결정 전략 투자 측면에서 개선, 능률적인 컴플라이언스 프로세스, 네트워크화된 전투력, IT 가이드와 훈련의 현대화, 강화된 워크포스 등이 고려되고 있다. 기존 연구에서 Liu 등은 AHP를 기반으로 하는 전술 데이터링크 시스템의 효율성 평가라는 측면에서 연구한 바 있다[1]. Jongyon Kim 등은 MIL-STD- 188-220 네트워크에서 멀티 홉 방송을 위한 개선된 DAP-NAD 기법을 제안하고 각 지연요소에 대해 분석하고 있다[2]. Jajoon Lee 등은 MIL-STD-188-220 환경에서 음성 통신서비스에 품질 개선을 위한 적응적인 가상 슬롯방안에 대해 제안하고 있다. 이 연구에서는 음성메시지에서 패킨 지연을 중심으로 분석하고 있으며, 지터 허용시간에 대해서도 그 영향을 살피고 있다[3]. Gao Fei 등은 MIL-STD- 188-220 환경에서 패킷 라디오 망을 위한 보안 메커니즘을 제안하고 있다[4]. 이 연구에서는 DAP-NAD 기법에서 대기시간을 분석하고 있으며, 우선순위의 메시지 지연정도, 루틴 메시지의 지연정도 측면에서 분석한다. 이외 Gugun B 등의 전술 무선장비 환경에서 저속통신을 위한 프로세서 프로토타입 연구도 있다[5]. 본 논문은 전술 통신 운용환경에 대한 제반 통신 정책과 보안 정책, 반자동 전투력을 지원하는 계층 프레임워크에 대한 관점, 링크 계층 프레임구조와 COMSEC 보안 정책 연구에 대한 필요성을 인식하고, 전술링크 전송 성능과 보안 동기에 대한 연구 필요성에 따라 연구하였다. 먼저 미군이 전술 운용환경에 초점을 맞추어 정보보호 정책과 보안 문제에 초점을 맞추고 있다. 2장 전술통신 환경에서 운용환경과 정책, 메시지 구조와 유형, 반자동 전투력 계층별 프레임워크, 통신 링크 프레임 구조를 살펴보았고, 3장에서 전술 링크의 보안 정책을 기술하였다. 그리고 4장에서 전술 링크에서 전송성능을 전술통신 링크 측면과 보안 동기 검출 측면에서 구분하여 분석하였고, 5장에서 결론을 맺었다.

2. 전술통신의 운용환경과 정책

미군은 무선장비 측면에서 JTRS, EPLRS, AN PRC-117G가 2014-18년 기간에 WNW(Wideband Networking Waveform) 무선장비로 대체된다. 또한 SINCGARS와 AN PRC-117G가 SRW(Soldier Radion Waveform) 장비로 대체된다. 전술 에지(플랫폼, HH)의 경우 FBCB2, MTS가 2014-18년에 JCR - JBC-P로, 2019-27년에 플랫폼 COE로, 핸드헬드/ 종단 사용자 디바이스(Net Warrior, JBC-P 핸드헬드, AFATDS 핸드헬드, 로지스틱 핸드헬드, 인텔 핸드헬드) 가 미 장착용 COE로 진화된다. 소프트웨어 측면에서 Command Post COE와 엔터프라이즈 COE로 대체된다.

2.1 전술통신 운용 메시지

미군에서 사용하는 다중 전술 메시지 형식과 프로토콜에는 JVMF R5(Joint variable messaging formats, 6017), USMTF(United states message text format), FDL(FAAD data link), PASS(Publish and subscribe service) & DDS(Data distribution service) XML, JC3IEDM(Joint consultation, command and control info exchange data model), C2R(Command and control registry), OTH Gold(Over the Horizon gold), AFAPD(Aire Force Application program development) 등이 있다. 그 가운데 2045-47001 표준 규격을 준수하는 응용 메시지 전달구조는 table1에서와 같다. 응용계층 MIL-STD- 2045-47001, -17510 규격을 준수하는 규격은 비연결형 데이터 전송 응용계층의 표준으로 서브 네트워크와 점대점 링크 상에서 단일 메시지나 결합된 메시지를 처리 교환하기 위해 적용된다.

〈Table 1〉 Application message structure of variable message format

application header							
A		A+1		A+2		A+3	
2^0	2^7	2^0	2^7	2^0	2^7	2^0	2^7
message size						GPI	
00001110		00100000		11111010		00000010	

app header		variable message format			
50	51	52	53	54	55
2^0 2^7	2^0 2^7	2^0 2^7	2^0 2^7	2^0 2^7	2^0 2^7
min	sec	CF	GROUP		
00100000	00000000	00010011	00000101	00001111	00000011

메시지 처리를 위한 C2 어댑터의 구조는 임무관리 도메인과 클라이언트 관리 도메인, 전투 확장 도메인으로 구분되고, 클라이언트 도메인은 전술 클라이언트, OneSAF 클라이언트, Warsim 클라이언트 등이 있다. 임무 관리 도메인은 결정(determine, 적용을 위해 특정한 파서를 결정) → Map(매핑으로 출입하는 메시지를 실행하고 수행) → address(항상 필요한 것은 아니나 나가는 메시지에 대해 요구됨) 단계로 구분된다. 결정 영역은 전투 확장 도메인에 포함된 CMP 파서/인코더, JC3IEDM 파서/인코더/플러그인, Warsim 파서/인코더/플러그인과 관련된 파서를 찾아 사용한다. OneSAF 클라이언트는 Map 영역에서 Mapper 엔진과 파일 처리를 수행한다. 반자동 전투력을 지원하기 위한 C2 체계에 적용되는 JVMF 메시지는 다음과 같다.

〈Table 2〉 C2 JVMF messages

Type	Message
FBCB2	K04.02(Land route) K05.01(position) k05.13(threat warning) k05.14(situation) k05.16(Minefield laying) k05.18(MOOP) k05.19(Logistics) k7.03 k07.04 k07.07 k07.09 k07.12 k07.01
OneSAF	K01.01(Free text) K01.03(progress Msn notification) K02.24 K02.37 K02.38 K05.11 K05.12 K05.15
JVMF - AFATDS & FBCB2	K02.01(Check fire) K02.04(Call for fire) K02.06 K02.11 K02.12 K02.14 K02.15 K02.16 K02.18 K02.22 K02.46 K03.02 K05.01
AFATDS	K02.01 K02.04 K02.06 K02.09 K02.11 K02.14 K02.16 K02.22 K02.51
AMDWS	F3(track)
MCS-WS	K04.02 K04.03 K04.09 K05.01 K05.02 K05.05 K05.06 K05.14
MCS-GW	K05.19 K05.01
ASAS-L	K05.17 K04.01 K05.19

2.2 반자동 전투력을 지원하는 계층 프레임워크

반자동 전투력을 지원하는 계층은 어플리케이션, product 계층, 컴포넌트 계층, 컴포넌트 지원 계층, 저장소 컴포넌트 계층, 공통 서비스 계층, 플랫폼 계층으로 구분된다. 플랫폼 계층은 하드웨어, OS, 네트워크로 이루어지며, 서비스 계층은 모니터 서비스, 타임 서비스, 네임 디렉토리 서비스, 메시징 서비스, 조정 서비스, 교환서비스 그리고 미들웨어 서비스로 이루어진다. 미들웨어 서비스에는 RTI, DIS, COE 서비스, JDBC/ODBC, ORB 등이 있다. 저장소 컴포넌트 지원 계층에는 주로 저장소와 관련된 계층으로 소프트웨어, 통합, 환경, 실행, 초기화, 시뮬레이션 등이 있다. 컴포넌트 지원 계층에는 GUI 서비스에서부터, 시뮬레이션, 환경 실행, 시뮬레이션 오브젝트 런타임 DB, 모델링 서비스 등이 있다. 컴포넌트 계층은 시스템 구성 도구, 군 시나리오 개발 환경, 환경DB 생성 환경, 단위 구성, 실체 구성, 행동 구성, 아이콘 도구, 전투 목록도구, 관리&통제 도구(SSDE), 데이터 수집 사양도구, 시뮬레이션 구성&자산 관리도구, 성능 모델링 도구, 네트워크 로더 도구, 벤치마킹 도구, 단위 모델, 실체 모델, 행동 모델, 물리적인 모델, 환경적인 모델, 관리&통제 도구, 합동 관리 도구, 스텔스 도구, 모니터&통제 서비스, 전환 서비스, 연결 서비스, AAR, ahepf 검증 도구, 데이터 관리 도구, 정보 메타 데이터 도구, 소프트웨어 공학 환경, CM도구, 소프트웨어 검증 도구, 소프트웨어 인스톨 도구, 시스템 분배 도구 등이다. Product 계층은 시스템 구성, 지식 공학 환경, 이벤트 계획, 모델 구성, 시뮬레이션 생성, 기술적인 관리, 시뮬레이션 코어, 시뮬레이션 제어기, C4I 어댑터, 분석과 검토, 저장소 관리, 유지보수 환경 등과 관련이 있다. 구조 차원에서 어플리케이션은 지휘관 및 스태프 훈련 시스템의 구성, 끈김이 없는 훈련 시스템 구성, 전투군과 조직 분석도구 시스템 구성, 시험 평가 시스템의 구성 및 기타 시스템으로 구성된다. 구성 툴킷의 운용시나리오 가운데 예를 들면, 먼저 군 시나리오를 개발하는 환경에서 시나리오를 구성하고, 이어 필요한 컴포넌트를 선택하여 시스템을 구성한다. 그리고 시스템 구성이 이루어지면 행동 구성, 단위 구성, 실체 구성을 통해 전투장을 구성할 수 있다.

2.3 링크계층 SINGARS 디바이스

링크계층에 사용되는 SINCGARS 디바이스의 경우 table2에서 제시된 유형을 중심으로 서비스가 이루어져 오고 있다.

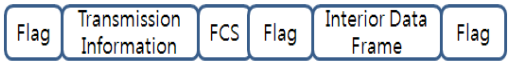
〈Table 3〉 SINCGARS VHF device category

Type	contents
RT-1702	Tx Rx(display unit selection)
AN/PRC-119	5W Manpack
AN/VRC-87	Vehicle(V), short range
AN/VRC-89	V, short range
AN/VRC-91	V, long range, short range
AN/VRC-90	V, long range, short range
Spearhead	Handheld, SINCGRAS ITT Compatible(C)
RT-1478E	Airborne(A), SINCGARS ITT C
AN/ARC-201	A, SINCGARS ITT C
AN/VRC-92	V, 50W, dual long range

Spearhead는 MIL-STD-188-22(데이터 모뎀 표준)을 수용하고, STANAG 4285(HF용 싱글톤 모델), 4415(저속 직렬 tone 모드)를 지원한다.

2.4 링크계층 MIL-STD-188-220 전달 구조

데이터 링크의 경우 MIL-STD-188-220 규격을 준수하고 있다(Fig.1). 디지털 메시지 디바이스 버스 시스템을 위한 상호 운용 표준으로 단말과 단말간 정보 교환을 목적으로 하는 전술 통신 체계에서 적용된다.



[Fig. 1] Frame Structure

3. 전술 링크 보안정책

3.1 어플리케이션 환경에서 보안메시지 구성

어플리케이션에 적용되는 보안 메시지 유형에는 보안파라미터, 키 재료 ID길이 정보, 암호 초기화 길이 정보, 암호 초기화 정보, 키 토큰 길이정보, 키 토큰 정보, 인증 데이터 길이 정보, 인증 데이터 정보, 서명된 ACK 요청 식별자 정보, 메시지 보안 패딩 길이 정보, 메시지 보안 패딩 정보로 구성된다.

보안파라미터 정보는 4비트로 구성하며, 데이터 출처 인증기능, 비연결형 무결성 기능, 메시지 서명을 기반으로 송신지 인증을 하는 부인방지 기능을 갖는다. 인증을 위해 미군은 SHA-1과 DA를 적용해 오고 있다.

SPI필드 크기는 키재료 ID용으로 0-64, 암호 초기화용으로 0-128, 키 토큰용으로 0-512, 인증데이터용으로 320-1024, 메시지 보안 패딩용으로 0-128이 사용된다.

3.2 COMSEC 보안 정책

CNSS의 경우 COMSEC 규격과 관련하여, CNSSI No.4033(COMSEC 재료 명칭), 4003(COMSEC 사고 평가 및 리포팅), 4000(COMSEC 장비 유지보수 및 교육), 4006(이전 COMSEC 키 재료를 위한 통제기관)에서 정의하고 있다. 미 국방부 규격에서도 DoDI s-5200.1(COMSEC), 5200.16(NC2 통신에서 사용되는 COMSEC 수단), 8560.01(미 국방부 정보시스템의 COMSEC 모니터링 및 IA 가독성 테스트), 8530.01(컴퓨터 네트워크 방어), 8530.aa(컴퓨터 네트워크 방어를 위한 지원), 8530.01-M(국방망 서비스 제공자 인증 및 인가 프로세스), 8520.02(PKI 및 PK), 8520.03(정보시스템용 식별 인증), 8540.aa(크로스 도메인 솔루션), 8551.01(포트, 프로토콜, 서비스 관리), 8140.aa(사이버 공간 워크 포스 관리), 8570.01(IA 훈련, 인승 및 워크 포스 관리), 8570.01-M(IA 워크 포스 개선 프로그램), 8580.01(방어획득 시스템의 IA), 8581.01(국방부에 의해 사용되는 우주 시스템용 IA 정책), 5200.mm(신뢰시스템과 망), 8582.01(비 국방성 정보시스템 상에서 개방된 국방 정보 보안), 5205.13(DIB CS/IA 활동), DoDM O-5205.13(DoD DIB CS/IA 보안 통제 매뉴얼), 5505.13E(DC3용 DoD EA), 8500.01(정보보증), 8500.02(정보보증 구현), 8510.01(DIACP)를 다루고 있다. MIL-STD-6017 메시지 규격을 수용할 수 있는 하위 디바이스에 적용 가능한 보안 디바이스는 ERF, AKMS, AFKMDS, RBECS 등이 있다.

1) AKMS

암호관리, 전자보호, 암호 키생성 및 분배시스템, 키 감사 추적 기록을 통합한다.

2) AFKDMS(air force key data management syste)

공군에서 사용하며 키정보 관리 단말과 DTD로 구성된다. 공군 전자 키 관리시스템(AFEKMS)는 암호 재료 생성, 관리, 분배 및 감사한다.

3) RBECS

미 해군에서 연합작전 수행을 위해 구성품인 소프트웨어, 단말, RDG, DTD를 사용한다. RDG는 TRANSEC 변수 생성하는데 사용하고 DTD는 ECCM (electronic counter countermeasures)과 TRANSEC 키 로드를 위해 사용하도록 정책을 제시한다. ANCD/DTD는 KYK-15/15A로 대체하도록 권고된다. NKMS는 자동화된 암호 키 관리 및 분배 시스템으로 ANCRS (automated navy COMSEC reporting system), CARS (COMSEC automated reporting system) S/W, STU-III, AN/CYZ-10으로 구성된다.

〈Table 4〉 Key insertion security device for Radio equipment

Type	Security device for key insertion
COMSEC(KY-57/58)	AN/CYZ-10, KYK-13, KYX-15
FH information	AN/CYZ-10, MX-18290, MX-10579
Synchronous time data	AN/CYZ-10, AN/PSN-11 (PLGR)
COMSEC/FH (KY-57/58)	AN/CYZ-10
COMSEC/FH data/ synchronous time data	AN/CYZ-10

4) KIV-7/HSB 암호 디바이스

임베디드 KG-84 COMSEC 모듈(KIV-7HSB)은 컴팩트하고 실용적이며 고성능에 사용자 위주의 통신 보안 디바이스로 개발되었다. 개인용 컴퓨터, 워크스테이션, 팩스 장비 사용자 가운데 안전하게 통신할 수 있도록 설계되었다. KIV-7HSB는 비밀로 분류된 곳이나 민감한 디지털 데이터 전송 보호를 위해 제공되며, 1.544Mbps급 통신에 주로 사용된다. KIV-7HSB는 안전한 데이터 제공과 OTAR 모드에서 적용 가능한 정부표준 KG-84, KG-84A 및 KG-84C 데이터 암호 장비와 호환 가능하다. KG-84 장비와 사용운용 가능하기 위해 KIV-7HSB가 허용되며, KIV-7HSB는 사용자 어플리케이션의 폭넓은 범위를 지원하는 능력이 제공된다. 점대점이나 네트워크화, 브로드캐스트 데이터링크용에 적합한 보호를 제공하며, 시스템 재설정 요구 없이 평문 헤더 바이패스 기능이 있어 트래픽 운용을 안전하게 하도록 초기 모뎀을 설정한다. 통합된 원격 제어 인터페이스가 독립된 안전한 링크를 경유 싱글 KIV-7HSB에 의해 30개 원격 유니트에 이르도록 관리를 수행한다. 사용자 중심의 운용자 인터페이스의 메뉴 구성은 모든 운용자에게 편리하도록 제공하고 있다.

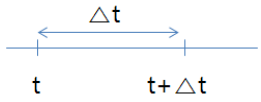
4. 전술 링크에서 전달성능 분석

4.1 링크계층 전달 성능 분석

링크계층에서 데이터 통신 전달 구조를 확률적으로 분석하고자 한다.

1) 전송 프레임 도달율 분석

링크계층 데이터 통신 전달구조에서 도달율에 대한 모델은 포아송 분포를 많이 사용한다. 랜덤 프로세스 N(t)가 주어진 시간 t까지 발생한 이벤트의 수라고 가정하고, 서로 다른 시간 구간 내에서 발생하는 이벤트의 수가 독립일 때, 특정 시간 구간 내에서 발생한 이벤트수가 시간 구간의 크기에 제한하여 결정되고 발생 시간과 무관할 때 이를 stationary increment 프로세스로 정의할 수 있다. Fig.2는 주어진 시간t에 시간 구간(△t)을 나타낸 것이다.



[Fig. 2] time interval(△t)

전체 시간(T)을 작은 단위의 시간 구간(△t)로 나눌 때 개수 n = △t/T 로 표현 할 수 있고 이때 작은 단위 구간 내에서 일어날 수 있는 확률 p는 도착률(λ)•△로 나타낼 수 있다. 데이터나 음성 프레임 도착 프로세스를 포아송 분포로 모델링 할 때, 주어진 n 개의 구간 가운데 k 개 구간에서 일어날 수 있는 확률 $P_k(T)$로 확장하면, 다음 식 (1)과 같이 나타낼 수 있다.

$$P_k(T) = e^{-\lambda T}\frac{(\lambda T)^k}{k!} \quad (1)$$

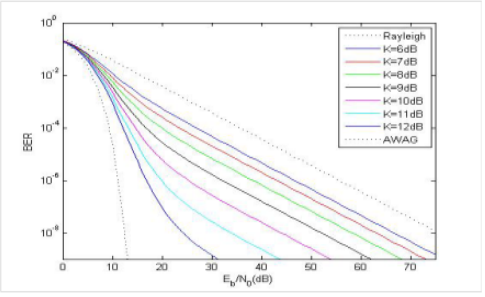
여기서 k는 0, 1, 2, ...이다.

또한 주어진 시간 t 이내에 새로운 프레임이 도착할 확률은 다음 식(2)와 같이 나타낼 수 있다.

$$P[T \le t + t_0 | T > t_0] = 1 - e^{-\lambda t} \quad (2)$$

2) 무선채널 특성

만일 채널 환경이 라이시안 페이딩 채널이라고 가정하고, 라이시안 페이딩 채널에서 DPSK (differential phase shift keying)기법을 적용하여 비트 오류율을 살펴보면, 다음 Fig.3에서 나타내었다.

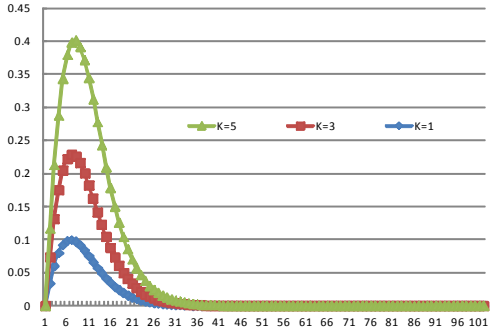


[Fig. 3] S/N rate in Rician fading channel (ρ =variable, k=variable)

$$BER(\rho, K) = \frac{1+K}{2(\rho+1+K)} \exp\left(\frac{-K\rho}{\rho+1+K}\right) \quad (3)$$

ρ는 1비트 당 신호 에너지와 잡음간의 비율(E_b/N_o)로 나타낼 수 있으며, K는 식1에서 정의한 파라메타를 의미한다. 주어진 t시간 내에서 프레임이 성공적으로 도착할 확률은 다음 식(4)과 Fig.4에서와 같이 나타낼 수 있다.

$$P_{frame}[T \le t] = (1 - e^{-\lambda t}) \bullet BER(\rho, k) \quad (4)$$



[Fig. 4] Frame arrival probability(P_{frame}) in Rician fading channel (ρ =variable, k=1/3/5)

4.2 보안 통신환경에서 전달성능 분석

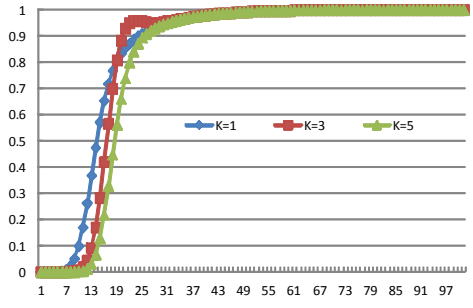
만일 주어진 시간 t내에서 도착하는 프레임이 성공할 확률을 가진, 보안 동기를 검출할 확률은 다음 식(5)과 같이 나타낼 수 있다.

$$P_{crypto\,sync}[T \le t] = (1 - e^{-\lambda t}) \bullet \sum_{i=o}^{m} {}_nC_i \bullet BER(\rho, k)^i \bullet (1 - BER(\rho, k)^{n-i}) \quad (5)$$

그러므로 주어진 페이딩 채널 환경에서 정상적으로 도착하는 프레임 가운데 보안 동기(31비트 사용)를 성공적으로 검출할 확률은 다음 식(6)과 같이 나타낼 수 있다.

$$P_{crypto\,sync}[T \le t] = (1 - e^{-\lambda t}) \bullet \sum_{l=n}^{31} {}_{31}C_l \bullet BER(\rho, k)^n \bullet (1 - BER(\rho, k)^{31-n}) \quad (6)$$

보안통신을 위해 31비트 동기 정보 가운데 2비트까지 오류가 발생하여도 정상적으로 검출 가능하다고 판단하고, 이때 주어진 시간 내에 도달하는 프레임의 보안 동기를 검출할 확률을 다음 Fig.5에서 나타내었다.



[Fig. 5] Crypto Detection Probability(P_{crypto}) in Rician fading channel (ρ =variable, k=1/3/5)

5. 결 론

본 논문에서는 미군 전술통신에서 운용환경과 운용

정책, 전술링크에서 보안정책 및 보안 동기의 전달성능을 중심으로 분석하였다. 운용환경의 경우 운용통신 메시지와 반자동 전투력을 지원하는 각 계층별 프레임워크를 분석하였으며, 링크계층의 경우 SINCGARS 사양을 살펴보았다. 전술 보안정책에서는 COMSEC 정책과 응용계층 보안을 일부 살펴보았다. 또한 전술 통신환경에서 전송 성능 및 보안 동기 검출 측면에서 그 영향 정도를 분석하였다. 연구결과는 국내 전술 통신 환경에서 제반 통신 성능 및 보안 정책 수립에 도움이 될 것으로 사료된다.

참 고 문 헌

[1] Liu Hongbo, Gao Jun, Liu Qin-tao, Zhao Ming, Research of weight coefficient in efficiency evaluation of Tactical Data Link system based on AHP, CCC2013, pp.6349-6352, 2013.

[2] Jongyon Kim, Bosung Kim, Byeonghee Roh, An enhanced DAP-NAD scheme for multi-hop broadcast based on MIL-STD-188-220 networks, ICACT2013, pp.552-557, 2013.

[3] JaeJoon Lee, Dongwon Kim, Jaesung LIM, Adaptive virtual slot for enhancing QoS of voice communication in MIL-STD-188-220, MILCOM 2012, pp.1-6, 2012.

[4] Gao Fei, Zhi Ruxin, Yang Jie, Study of the Security Mechanism for Packet Radio Network Based on MIL-STD 188-220C, WiCom2009, pp.1-4, 2009.

[5] Gugun B Maruhum, Harry Chandra, Sinta Amanda, Erwin, Yoanes Bandung, Baseband Processor Prototype for Low Bit Rate Communication in Tactical Radio, ICISS2013, pp.1-7, 2013.

홍 진 근(HONG, JINKEUN)

- 1991년 2월 : 경북대학교 전자공학과(공학사)
- 2000년 2월 : 경북대학교 전자공학과(공학박사)
- 2004년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
- 관심분야 : 정보보호정책, 통신네트워크보안
- E-Mail : jkhong@bu.ac.kr