가변메시지형식체계에서 COMSEC 프레임 동기정보의 전송영향 분석

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

Analysis of transmission effect of communication security frame synchronization information in variable message format

Jin-Keun Hong*, Sun-Chun Park**, Ki-Hong Kim**, Seng-Jo Kim**, Jang-Hong Yoon**
*Div. of Information and Communication, Cheonan University
**NSRI.

요 약

본 논문에서는 가변형식메시지체계에서 COMSEC 프레임동기 정보의 전송영향을 분석하였다. 실험결과 비트오류율 10^{-1}~10^{-5} 환경에서 COMSEC 프레임 동기 정보의 강인한 특성을 고찰하였으며 암호통신을 위해 사용되는 프레임 동기정보가 동기검출 및 오검출 측면에서 영향정도를 분석하였다.

1. 서 론

가변메시지형식(variable message format, VMF)체계는 미 육군과 해병대에서 선택한 데이터 링크로 LINK16의 패밀리 멤버로 설계되었으며, 가변메시지형식체계 실제 운용에 관련하여 이탈리아, 네덜란드, 스페인, 싱가폴, 호주 등이 많은 관심을 보이고 있는 실정이다[1][2]. 미 육군은 하나의 특정 파형에 제한되지 않고 모든 전장의 기능적인 영역에 적용 가능한 메시지 표준을 갖는 전장을 디지타이저화 하기로 결정하였다. JTIDS/MIDS 및 다른 데이터 링크 구조가 적절한 서비스 요구 조건을 제공하지만, 사이즈, 전력 요구조건 등이 모든 전투 환경에 사용하기에 추천되지 않는 상황에서 VMF는 유연성, 상대적으로 간단한 구현성, 육군 및 해병대를 위해 구현 잠재성을 지닌 CNR(combat net radios) 환경에 적용 가능한 표준으로 자리 잡고 있다. 또한 대역폭이 제약되어 있는 전장 환경에서 거의 실시간으로 데이터 교환이 가능한 가변적인 길이의 메시지로 구성된 비트 지향형 디지털 정보 표준이며, 어떤 특정 라디오나 프로세서 환경에 묶여있지 않고, 공통 데이터 요소 정도를 공유하며, 지상군의 운용 및 기능적인 요구사항을 만족해야 한다. LINK16과 다른 TDL 간 갭, MTF(메시지 텍스트 표준)의 기능을 해결하고 있으나, 현재까지 LINK16 타입의 실시간으로 연속적인 상황인식 능력을 포함하고 있지 않다. MTF와 달리 VMF 메시지를 읽기 위한 단말 처리 능력이 요구되고, JTIDS LINK16은 고정형 및 가변형 워드 형식 메시지를 포함하고 있으며, 지상 공중 방어 정보를 교환할 목적으로 LINK16의 가변적인 서브셋으로 설계되었다.

VMF체계 관련 연구는 Douglas Dusseau와 Clinton Brock가 데이터링크를 베이스로 한 VMF 사용에 있어서 네트워크 중심의 상호 운용성에 대한 연구를 발표한 바 있으나[1] 아직까지 가변형식 메시지 체계를 근거로 한 보안 서비스에 대한 구체적

인 연구사례가 제시된 바 없으며, 디지털 메시지 운용 및 전송을 위한 메시지 형식의 정의 및 인터페이스 표준이 MIL-STD-2045-47001C와 MIL-STD-188-220B 규격에서 정의되고 있다[3][4]. 본 논문은 VMF 메시지를 SINCGARS 환경에서 전송할 때 주어진 채널환경에 따른 COMSEC 프레임 동기 영향을 살펴봄으로써 비트오류환경에 대한 정상적인 동기검출확률, 오검출확률 등을 분석함으로써 프레임 동기와 비트오류율, 암호통신 서비스 영향 등을 분석하고자 한다. 본 논문의 구성은 다음과 같다. 먼저, 2장에서는 가변메시지형식의 체계 구성을 소개하였고, 3장에서 가변메시지형식 체계가 SINCGARS 베어러 환경에서 서비스 될 때 서비스 프레임워크와 데이터 암호통신을 수행할 때 채널환경에서의 프레임 동기 정보의 전송 성능을 분석하였으며, 마지막 4장에서 결론을 맺었다.

2. 가변메시지형식체계의 메시지 구조

VMF 메시지 패킷은 최소의 시간으로 전송하기 위해 패킷의 크기를 최적화하는 것이 필요하며, 데이터 구조는 하위 부대 단위의 임무 수행을 위해 부가 정보의 반복을 필요로 한다. MIL-STD-2045-47001 표준[4]에서는 응용계층의 헤더 표준(VMF message header)을 정의하고 있으며, MIL-STD-188-220B 표준에서는 디지털 메시지 디바이스 서브 시스템을 위한 상호운용성 표준을 제시하고 있다. 47001 상호 운용성 표준은 비연결형 데이터 전송 응용계층 표준으로서 서브 네트워크 및 점대점 링크 상에서 단일 메시지 또는 결합된 메시지의 취급 및 교환을 지원하기 위해 필요한 최소의 필수적인 데이터 통신 파라미터와 프로토콜을 정의한다. 220B 표준은 디지털 메시지 전술을 위한 상호운용성 표준으로 DMTD와 DMTD간 정보교환을 수행하는 C4I 시스템을 위한 사양에 적용되어야할 절차, 프로토콜, 파라미터를 정의한다. 또한 방송용 무선 서브네트워크 및 점대점 링크 상에서 단일 또는 다중 세그먼트 메시지의 전송을 위한 계층화된 프로토콜을 정의하며, 다른 데이터 단말 디바이스와 통신에 요구되는 최소의 필수 데이터 통신 파라미터와 프로토콜 스택을 제공한다. 가변형식의 메시지는 하부 SINCGARS 또는 EPLRS와 같은 무선장비를 통해 전송되며 이때 데이터 보호 기능이 제공된다. 전송 링크의 데이터 보호방안이 적용될 때 정상적인 암호통신을 위해 COMSEC 프레임 동기 정보가 요구된다.

3. VMF체계 SINCGARS환경에서 COMSEC 프레임 동기정보의 전송영향 분석

VMF 체계에 운용 가능한 무선장비는 SINGARS와 ehnanced position location reporting system(EPLRS)가 있고, SINGARS는 1초당 100홉수를 가지며, VHF/FM(30MHz~88MHz) 대역의 장비로 음성과 데이터 통신기능을 지원한다.

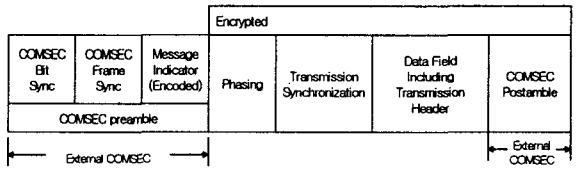

Fig.1. 가변메시지형식 암호통신 전송 프레임 구조

VMF 메시지를 전송하는 베어러 서비스인 SINCGARS 베어러 서비스 환경의 경우 서비스 전송율은 1200bps에서부터 최대 9600bps 전송속도를 제공한다. COMSEC 시스템을 통해 이루어지는 암호통신 전송 프레임 구조를 Fig.1에서 제시하였다. COMSEC 비트 동기부 필드는 비트 동기를 이루기 위한 신호를 제공하기 위해 사용되며 이 COMSEC 비트 동기를 이루기 위해 65msec에서 1.5sec로 선택가능하다. 프레임 동기 부 필드는 수신 단말에 부호화된 MI의 시작을 나타내는 프레임 신호를 제공하기 위해 사용된다. COMSEC 프레임 동기 부 필드 구조를 Fig.2에서 제시하였다.

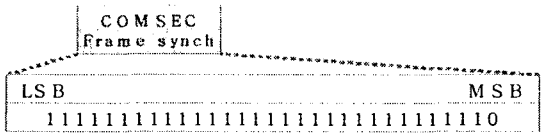

Fig.2. Phi 부호화를 위한 COMSEC 프레임 동기 패턴

이 부 필드는 465비트의 길이로 31Phi 부호화 비트로 구성된다. 이 Phi 패턴은 여분의 부호화 데이터 비트의 방법으로 논리적으로 "1" 데이터 비트는 Phi(1)로 111101011001000(15)비트 특성을 가지며, "0" 데이터 비트는 Phi(0)로서 000010100110111(15)로 부호화된다. COMSEC 프레임 동기에 사용되는 1개의 Phi(1) 또는 Phi(0)에 오류가 발생할 확률은 eq(1)과 같이 정의된다.

$$P_f = 1 - (1 - P_e)^{15} \quad (1)$$

스트림 암호통신에서 동기능력은 전송채널조건에서 동기신호검출에 대한 정확성 여부와 유사신호에 대한 정확한

검출능력에 의해 결정되며, 송신신호에 대한 수신신호의 검출확률 P_D, 동기신호의 미검출 확률 P_M, 송신측에서 미전송시에 수신측의 송신한 것으로 판단하는 오검출 확률 P_F 등에 의해 결정된다. 무선채널 구간이 갖는 평균 비트 오류율(BER, bit error rate) P_e는 1비트를 1회 전송시 오류가 발생할 확률로 나타낼 수 있다. 암호기에서 n비트의 동기 신호를 송신할 때 복호기에서는 $0 \sim n$개의 오류를 가진 동기 신호가 수신된다. 이때 n비트 가운데 i 비트 오류 개수가 검출될 동기 검출 확률 P_{Di}는 식 1을 통해 얻을 수 있고 동기를 놓칠 확률 P_{Mi}는 eq(3)에서와 같다.

$$P_{Di} = n C_i P_e^{\,i} (1 - P_e)^{n-i} \quad (2)$$

$$P_{Mi} = 1 - P_{Di} \quad (3)$$

이때 i는 $0, 1, \ldots, n$이다. 따라서 m개까지의 오류가 발생했을 때의 동기 검출 확률 P_{TD}는 eq(4)와 같다.

$$P_{TD} = \sum_{i=0}^{m} P_{Di} \quad (4)$$

각 오류개수에 대한 *false alarm* 확률 P_{Fi}는 채널의 오류로 인해 동기 신호를 잘못 검출할 수 있는 오검출 확률로 eq(5)와 같이 계산된다.

$$P_{Fi} = n C_i 0.5^{\,i} (1 - 0.5)^{n-i} = n C_i 0.5^{\,n} \quad (5)$$

이때 i는 $0, 1, \ldots, n$까지이다. m개까지의 오류가 발생했을 때의 *false alarm* 확률 P_{TF}는 eq(6)과 같다.

$$P_{TF} = \sum_{i=0}^{m} n C_i 0.5^{\,n} \quad (6)$$

비트오류율이 $10^{-1} \sim 10^{-5}$ 환경에서 COMSEC 프레임 동기 패턴이 전송될 때 비트오류채널별 정상적인 동기 검출 능력을 Fig.3에서 제시하였다. 제시된 결과를 통해 정상적인 암호통신이 이루어지기 위한 COMSEC 프레임 정보필드의 검출능력을 고려할 때 10^{-1}채널에서는 정상적인 검출이 불가능하다고 볼 수 있으나 동기검출 여유비트가 증가할 때 99.99%로 수렴하는 것을 볼 수 있다.

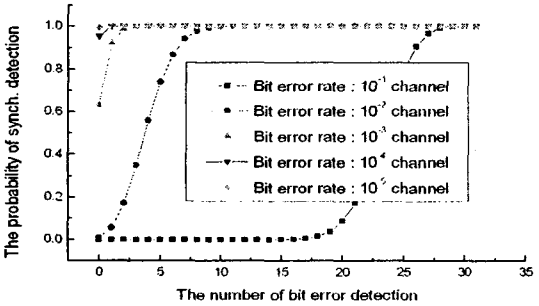

Fig.3. COMSEC 프레임 동기 정보의 검출능력

또한 10^{-2} 채널에서는 10비트 정도 수준에서 99.99% 동기검출 능력을, 10^{-3} 채널에서는 3비트 정도 수준에서 99.99% 동기검출능력을, 10^{-4} 채널에서는 1비트 정도 수준에서 99.99% 동기검출능력을 제공하며, 10^{-5} 채널에서는 100% 정확한 동기검출능력을 제공한다. 그러므로 COMSEC 프레임 동기는 정상적인 암호통신이 이루어지기 위한 채널환경 10^{-3}이상, 데이터 암호통신 10^{-5} 이상의 채널환경을 고려할 때 COMSEC 프레임 동기 검출이 가능하다고 판단할 수 있다. 또한 Fig.4에서 제시된 오검출 확률도 주어진 COMSEC 프레임 동기정보 환경에서 오검출로 인한 문제 없이 정상적으로 적용 가능한 것으로 판단할 수 있다.

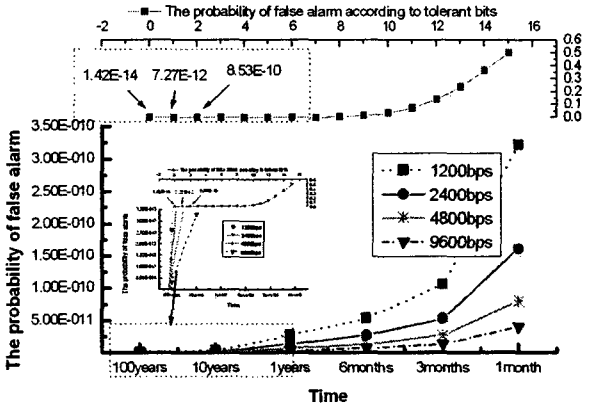

Fig.4. COMSEC 프레임 동기정보의 오검출 능력

4. 결 론

본 논문은 가변형식메시지체계에서 COMSEC 프레임동기 정보의 전송영향을 분석하였다. 실험결과 비트오류율 $10^{-1} \sim 10^{-5}$ 환경에서 COMSEC 프레임 동기 정보의 강인한 특성을 고찰하였으며 암호통신을 위해 사용되는 프레임 동기정보가 동기검출 및 오검출 측면에서 어떤 영향을 갖는지를 분석하였다.

참고문헌

[1] Dusseau D. and Brock C, "Network centric interoperability - using a variable message format(VMF) based data-link to improve situational awareness and close air support(CAS)," Aerospace and Electronic Systems Magazine, IEEE, Vol.19, Issue 9, Sept. 2004 pp.8-13.

[2] Thuente D. et al., "The design andanalysis of the AFATDS communication networks using simulation," tactical communications conference, 1996, Proceedings of the 1996, 30 April, pp.267-279.

[3] MIL-STD-2045-47001C.

[4] MIL-STD-188-220C.