論 文
54D-7-4

가변메시지형식체계에서 통신보안을 위한 비트동기 정보의 전송영향 분석

Analysis of Transmission Performance of Communication Security Bit Synchronization Information in VMF System

洪鎭根† · 朴稔美* · 孫暎昊* · 尹長鴻*
(Jinkeun Hong · Youngmi Park · Youngho Son · Janghong Yoon)

Abstract - In this paper, we analyses transmission performance of communication security(COMSEC) bit synchronization information over the single channel ground and airborne radion system in variable message format system. Experimental results demonstrate the robust characteristics of the COMSEC bit synchronization information in 10-1~10-5 of bit error channel and the relationship of time duration of bit synchronization and probability of synchronization detection.

Key Words : VMF, Cipher, Synchronizaiton

1 장 서 론

가변메시지 형식(variable message format, VMF) 체계는 미 육군과 해병대에서 선택한 전술통신체계의 데이터링크로 LINK16의 패밀리 멤버로 설계되었으며, 이탈리아, 네덜란드, 스페인, 싱가폴, 호주 등 세계 각국에서 관심을 가지고 있는 전술 메시지 형식 및 전송에 관련된 체계이다. VMF는 유연성, 상대적으로 간단한 구현성, 육군 및 해병대를 위해 구현 잠재성을 지닌 combat net radio(CNR) 환경에 적용 가능한 표준으로 자리 잡고 있다. TACFIRE의 경우 현재 사라져 가고 있는 실정이며 AH-64는 2005년에 일부 기종이 VMF를 적용할 수 없을 것으로 전망하고 노후화된 포병 유니트들은 AFTADS를 획득할 수 없을 것으로 파악하며 연합지역에서는 VMF를 획득할 수 있을 것으로 관측한다. US 아파치는 우리는 영국을 지원하기 위해 TACFIRE가 필요하고 영국 아파치 또는 미국을 지원하기 위해 TACFIRE가 필요하다는 견해를 가지고 있다. AFAPS는 F-16에서 오랫동안 존재하게 될 것이고 VMF로 가는 계획을 가지고 있지 않는 실정이다. 전장상황 정보를 실시간으로 주고받을 수 있는 진보된 전장 포병 전술 데이터 시스템인 advanced field artillery tactical data system(AFATDS)에 대한 시뮬레이션 연구가 일부 발표된바 있다[1].

Variable message format(VMF, Tadil K)는 singel channel ground and airborne radio system(SINCGARS)와 같은 전장 네트워크용 무선통신에 사용하기 위해 개발된 메시지 프로토콜로서 현재 미 전투기 F/A-18이나 EA-6B의 경우 Joint VMF 메시지를 구현하고 있다. VMF의 장점은 메시지가 쉽게 SINGARS로부터 기가 비트속도를 제공하는 인터넷으로 대상 매체에 의해 쉽게 전송이 가능하다는 점으로 메시지 형식이 다양한 미디어를 지원할 수 있으며, 가변적인 길이의 메시지가 처리율 요구사항을 감소시킴과 함께 유연성 있게 설계되었다.

VMF체계에 대한 관련 연구는 Douglas Dusseau와 Clinton Brock가 데이터링크를 베이스로 한 VMF 사용에 있어서 네트워크 중심의 상호 운용성에 대한 내용을 발표[2]한 바 있으나 아직까지 암호통신에 관련하여 구체적인 연구사례가 발표된 바는 없다. 본 논문에서는 VMF 체계 메시지를 SINCGARS환경에서 VMF 규격에서 제시하고 있는 형식체계를 기본으로 COMSEC 비트 동기의 암호통신을 수행할 때 주어진 암호통신 환경에 따른 비트동기의 전송영향을 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 데이터 암호통신 성능을 분석하였으며, 마지막 4장에서 결론을 맺었다.

2 장 가변 메시지 형식 체계

VMF에서 사용되는 TADIL K 가변적인 포맷은 사용자의 대역폭이 제한 받으며 지상과 지상간, 지상과 항공간, 항공과 지상간 데이터 링크를 제공하여 사용되고 있다. VMF 메시지는 전술 지휘관에 의해 사용되는 정보 형식을 표준화하기 위해 설계된 메시지로서 K05.15 "field orders" 메시지가 있다. 이 메시지의 경우 기본적으로 선택되는 메시지로 VMF 표준에 사용되는 것으로 전송되는 가장 크고 복잡한 메시지 가운데 하나이다. 게다가 전장에서 송신되는 메시지의 가장 중요하고 일상적인 유형 가운데 하나이다. 대규모 부대 및 소규모 부대 단위에서 매일 단위로 3개 또는 4개의 별개의 필드 order가 송수신 된다.

† 교신저자, 正會員 : 천안대학교 정보통신부 교수
E-mail : jkhong@cheonan.ac.kr
* 正 會 員 : 국가 보안기술 연구소
接受日字 : 2005年 5月 16日
最終完了 : 2005年 5月 27日

4093	007	Plan/Order Type	2
4014	002	FPI	1
4003	007	Operation Identification	14
....			
4014	001	GPI	1
4045	001	GRI	1
4014	002	FPI	1
4004	012	Unit Reference Number (URN)	24
4014	002	FPI	1
4045	002	FRI	1
4075	005	Para 1. Situation	1400
4014	002	FPI	1
4045	002	FRI	1
4075	006	Para 2. Mission	1400
....			

그림 1. KO5.15 필드 order 메시지 형식
Fig. 1. Message format of KO5.15 field order

메시지 형식은 K05.15내에 GPIs, GRIs, FPIs, FRIs가 49개의 단일 비트 필드로 구성되고, 메시지내에 132 전체 필드라 할 수 있다. 지시자 필드는 해당 그룹 또는 필드의 존재 유무를 나타난다. 각 VMF 메시지 패킷의 길이는 가변으로 정의되기 때문에, 고정된 패킷 크기에 근거하여 높은 차원에서의 오류 검출 및 정정하는 것이 어렵고, 1개 또는 2개의 누락된 비트는 쉽게 오류 체킹 프로토콜에 의해 누락될 수 있으며 MIL-STD-188-220C[3] 전송 프로토콜에 상대적으로 강인한 순방향 오류정정 기능이 포함되어 있다. 비연결형 데이터 전달 응용 계층 표준을 위한 상호운용성 표준을 MIL-STD-2045-47001[4]에서 제시한다.

3 장 VMF체계 SINCGARS환경에서 COMSEC 비트동기 정보의 암호통신 영향분석

전술 인터넷에 주로 사용되는 무선장비는 SINGARS와 ehnanced position location reporting system(EPLRS)가 있고, SINGARS는 저가형 주파수 호핑(100hops/sec) VHF/FM (30MHz~88MHz)장비로 음성과 데이터 통신기능을 지원하며, 데이터 모드에서 처리율은 2400bps를 지원한다.

VMF 메시지를 전송하는 베어러 서비스로는 크게 SINCGARS와 EPLRS를 둘 수 있으며, SINCGARS 베어러 서비스 환경의 경우 서비스 전송율은 1200bps에서부터 최대 9600bps 전송속도를 제공한다.

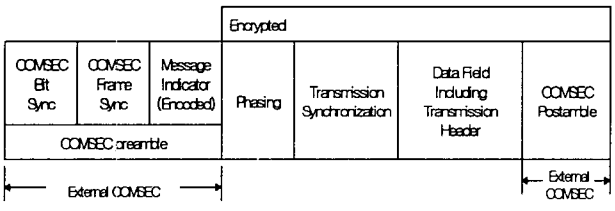

그림 2. 가변메시지형식 암호통신 전송 프레임 구조
Fig. 2. Structure of COMSEC transmission frame in VMF

COMSEC 시스템을 통해 이루어지는 암호통신 전송 프레임 구조를 그림1에서 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.

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 0000101001 10111(15)로 부호화된다.

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 미 전송시에 수신측의 송신한 것으로 판단하는 오검출 확률 P_F 등에 의해 결정된다.

무선채널 구간이 갖는 평균 비트오류율(BER, bit error rate) P_e는 1비트를 1회 전송시 오류가 발생할 확률로 나타낼 수 있다.

암호기에서 n비트의 동기 신호를 송신할 때 복호기에서는 0~n개의 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 식2에서와 같다.

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

$$P_{Mi} = 1 - P_{Di} \tag{2}$$

이때 i는 $0, 1, \ldots, n$이다. 따라서 m개까지의 오류가 발생했을 때의 동기 검출 확률 P_{TD}는 식3과 같다.

$$P_{TD} = \sum_{i=0}^{m} P_{Di} \tag{3}$$

각 오류개수에 대한 *false alarm* 확률 P_{Fi}는 채널의 오류로 인해 송신측에서 비트동기정보를 전송하지 않았으나 수신측에서 비트 동기정보로 잘못 오인하여 검출되는 오검출 확률로 식4와 같이 계산된다. 이 경우 가정된 오검출 확률은 일정 수준의 threshold level 이상의 수신환경에서 0.5(50%)의 값으로 정하였다.

$$P_{Fi} = n\,C_i\,0.5^{\,i}(1-0.5)^{n-i} = n\,C_i\,0.5^{\,n} \tag{4}$$

이때 i는 $0, 1, \ldots, n$까지이다. m개까지의 오류가 발생했을 때의 *false alarm* 확률 P_{TF}는 식5에서와 같다.

$$P_{TF} = \sum_{i=0}^{m} n\,C_i\,0.5^{\,n} \tag{5}$$

비트오류율이 10^{-2}이고, 전송속도가 1200bps의 열악한 암호통신 채널환경에서 COMSEC 비트 동기의 검출능력을 그림3에서 제시하였다. 암호통신 채널환경(BER)이 10^{-2}환경일 경우 COMSEC 비트 동기 전송시간을 65msec, 83msec, 200msec, 400msec 수준에서 전송하면 각각 99.999% 수준의 동기검출능력을 제공하지만 동기검출을 위한 여유 비트에 따라 상대적으로 수렴하는 정도가 다르게 나타난다.

비트 동기정보를 65msec를 사용하는 경우와 400msec를 사용하는 경우, 65msec를 사용할 때 보다 동기검출 확률이 3비트 정도의 여유를 두고 99.99% 동기검출 능력을 제공하며, 400msec 동기정보를 전송할 경우 15비트 정도의 여유를 두어야 99.999% 동기검출 능력을 제공

한다. 동기정보를 전송하는 시간이 증가할수록 동기비트 검출이 100% 수렴하기 위해서는 상대적으로 비트여유 또한 증가한다.

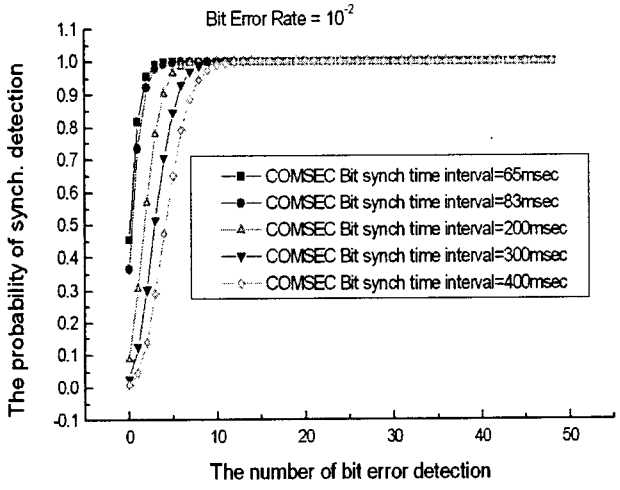

그림 3. COMSEC 비트동기정보의 전송시간에 따른 동기검출 능력

Fig. 3. Synchronization detection capability ccording to COMSEC bit synchronization nformation

그림4에서 암호통신 채널환경(BER)에서 고려하면, 암호통신이 거의 불가능한 10^{-1}환경일 경우 거의 COMSEC 암호 비트 동기는 검출이 불가능하다고 판단되며, 그 이외의 환경에서는 비트동기 일치는 99.999%이상 가능하게 나타난다.

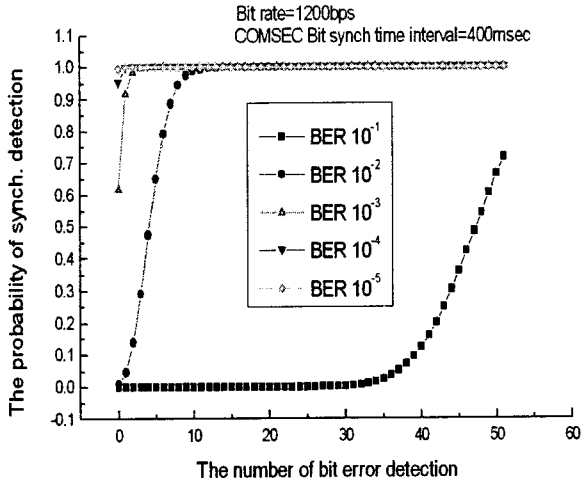

그림 4. COMSEC 비트동기정보의 비트 오류율에 따른 동기 검출능력(전송속도 1200bps 환경에서)

Fig. 4. Synchronization detection capability ccording to BER of COMSEC bit ynchronization information(at 1200bps)

데이터 전송을 위한 2400bps 암호통신 채널환경에서 비트 오류율이 10^{-3} 조건일 경우 COMSEC 암호 비트동기 일치는 100% 검출이 가능하며 사용된 동기 정보의 시간에 따라 100%의 수렴시간이 다소 차이가 날 수 있으나 시간 차이 또는 근소하며 이에 대해 그림4에서 제시하였다.

가변메시지 형식체계에서 SINCGARS 베어러 서비스를 제공할 때 COMSEC 비트 동기정보는 암호통신 뿐만아니라 일반통신도 불가능한 비트 오류율이 10^{-1}채널의 경우에는 그림5에서와 같이 정상적인 비트 동기 정보 검출은 거의 불가능하며, 비트 오류율이 10^{-2}채널 환경의 경우 비트동기 검출을 위해 제공되는 가변적인 시간 구간이 증가할수록 동기검출을 위한 수렴시간은 증가하나 수렴정도가 거의 근소한 차이를 나타낸다.

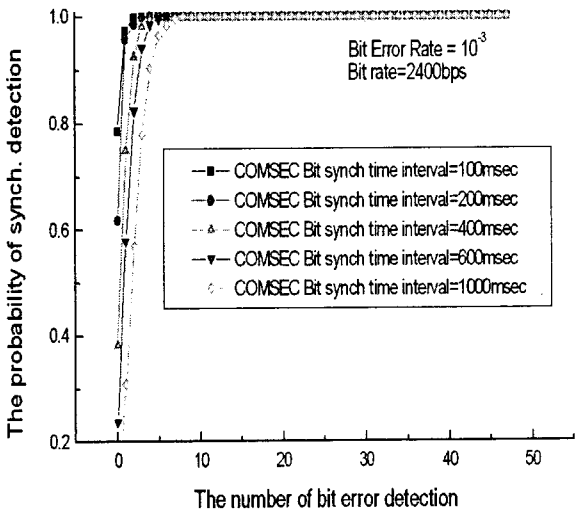

그림 5. COMSEC 비트동기정보의 전송시간에 따른 동기 검출능력(전송속도 2400bps 환경에서)

Fig. 5. Synchronization detection capability ccording to BER of COMSEC bit ynchronization information(at 2400bps)

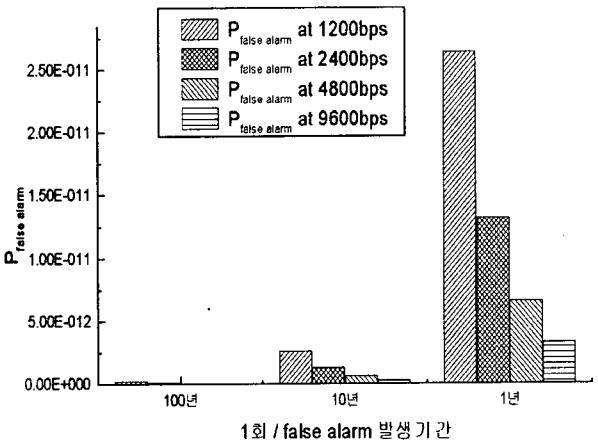

그림 6. COMSEC 비트동기정보의 오검출 발생기간과 오검출 확률간의 관계

Fig. 6. The relationship of time interval of false alarm in COMSEC bit synchronization information and probability of false alarm

그림6에서 주어진 전송속도가 1200bps(2400bps)환경에서 1년에 오검출이 1회 일어날 경우 오검출 확률은 2.64×10^{-16}(1.32×10^{-16})이며 이때 암호통신을 위한 비트동기 길이를 65msec로

설정할 경우 12비트(38비트)의 여유비트를 가지고 1년에 1회 오검출이 발생한다. 또한 1200bps환경에서 동기길이를 100msec로 설정하면 26비트의 여유비트를, 200msec로 설정하면 71비트의 여유비트를 제공한다. 즉, 71비트에 비트오류가 발생하더라도 1년에 1회 오검출 확률을 제외하고는 정상적인 비트 동기 검출이 가능하다. 또한 SINCGARC 베어러 서비스 환경에서 제공되는 COMSEC 비트 동기i정보는 주어진 구간 1200bps환경의 경우 100msec, 2400bps환경의 경우 200msec, 4800bps환경의 경우 400msec, 9600bps 환경의 경우 400msec 동기 길이 전송성능이 적합한 것으로 판단된다.

4 장 결 론

본 논문에서는 가변메시지 형식체계를 위해 제공되는 SINCGARS 베어러 서비스환경에서 COMSEC 비트동기 정보를 전송할 때 채널상태와 전송속도에 따른 동기검출 능력을 분석하였다. 오검출 발생기간에 따른 오검출 확률범위를 살펴보았고, 주어진 전송속도 1200bps, 2400bps환경에서 계산된 오검출 확률로부터 적합한 여유비트와 비트동기정보의 길이에 따른 영향을 분석하였다.

참 고 문 헌

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

[2] 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.

[3] MIL-STD-188-220C specification.

[4] MIL-STD-2045-47001C specification.