LINK16 통신체계에서 무선 키 갱신을 위한 전송성능 분석

Transmission Performance Analysis for OTAR in LINK16 communication system

홍진근
천안대학교

Hong Jin-Keun
Cheonan Univ.

요약

본 논문은 항공통신 전술링크 LINK16에서 무선 키 갱신을 위해 사용되는 동기신호가 주어진 통신환경에서 심볼오류율에 대해 전송속도를 기준으로 동기검출 확률, 오검출확률 측면에서 전송성능을 분석하였다.

Abstract

In this paper, we analyses transmission performance of synchronization pattern for over the air rekeying in aerial tactical link of LINK16, when it is given by symbol error rate, in respect of pattern detection probability and false alarm probability.

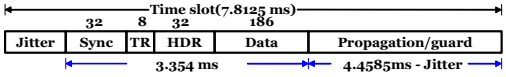
Ⅰ. 서 론

ISR체계에서 운용되는 LINK16은 각 체계 간에 상호 운용성을 제공하고, 실시간 정보를 교환하기 위한 전술 디지털 정보 링크로서, 단위부대, 전투부대, 지휘통제부간 고도로 긴밀한 통신을 보장하기 위해 개발되었다. LINK16 운용을 위한 MIDS 프로그램은 고속 정보 전송능력과 안티 재밍 능력, 보안 기능을 통한 안전한 디지털 통신이 가능하도록 개발되어 운용되고 있으며, 확산스펙트럼 주파수 호핑 통신과 항법 시스템을 제공한다. 메시지 표준은 TADIL J로 설계되었으며, 51개의 주파수 상에서 초당 77,000회 호핑이 이루어진다. LINK16에서는 암호 키를 사용한 전송파형에 대한 암호화와 TADIL J 메시지에 대한 암호화를 수행하는 이중 암호방식을 적용한다. 현재 구성된 LINK16은 TDMA 방식을 적용하여 1Mbps 용량을 지원하지만, 각 사용자는 NPG로 불리는 항공통제, 전자전, 음성 등과 같은 목적의 가상회선이 최대 54Kbps로 제한되고 있으며, LINK16에서 사용되는 JTIDS 단말은 하나의 파형을 사용하고, 전체 24시간은 112.5 epochs로 나누어지며, 각 epochs는 12.8분을 유지한다. 본 논문은 LINK16 통신에서 무선 키 갱신을 위하 사용되는 OTAR(over the air rekeying) 관리 메시지를 운용할 때 암호통신 성능을 분석한다. 2장에서는 LINK16 시스템 특성 및 구조를 설명하고, 3장에서 무선 키 갱신을 위한 암호동기신호 분석과 함께 4장에서 결론을 맺는다.

II. LINK16 시스템 특성 및 구조

TDMA 전송 데이터 메시지의 기본적인 전송구조는 지터(jitter), 동기(synchronization), TR(time refinement), Header(HDR), 데이터(data), Propagation/Guard 정보로 구성된다. 지터(jitter)는 타임 슬롯에서 전송 시작 시에 가변적인 시간 지연으로 통신 모드4에서 운용될 때 적용되지 않는다. 즉, RTT 메시지가 전송될 때나 또는 Packed-2 DP(double pulse)

또는 Packed-4 메시지 패킹 구조에서 메시지를 전송할 때 지터는 적용되지 않는다.



▶▶ 그림 1. 표준 DP 전송 프레임 구조

동기(synchronization) 패턴은 DP 심볼 패턴이 수신되는 JUs에 동기화 용도로 허용된다. 패턴은 타임 슬롯에서부터 타임 슬롯으로 바뀌고, 하나의 타임 슬롯내의 패턴은 넷 가운데 서로 다르다. TR(time refinement)은 4개의 DP 심볼 패킷의 고정된 패턴이 TR용으로 사용된다. HDR(header)는 하나의 타임 슬롯내에 전송되는 메시지와 관련된 정보를 제공한다. 데이터(data)는 타임 슬롯내에 전송되는 메시지를 말한다. Propagation/Guard는 다음 타임 슬롯 전송을 위해, JUs에게 최대 범위 및 시간이 허용되는 시간 주기이다. 이 경우 300nm (nautical miles,normal)/500nm,extended) 최대 영역까지 가능하도록 선택된다. LINK16은 TDMA 프로토콜을 근거하고 있으며 타임 슬롯 내의 모든 통신이 초당 128 타임 슬롯 즉, 7.8125msec가 소요되며, 하나의 타임 슬롯내의 정보는 5비트로 구성된 펄스열로 전송된다. 각 타임 슬롯내의 정보는 각 75비트 단위의 블록 수로 반송되며 이는 5비트로 구성된 심볼이 15개에 해당된다. 또한 이 블록은 각 15개의 심볼에 패리티 16개 심볼로 구성된 블록당 전체 31개의 심볼이 리드 솔로몬부호화(RS(31,15), FEC(forward error code))를 통해 전송된다. 시스템 환경에 의존하여, 타임 슬롯당 전송되는 블록의 수는 3, 6, 또는 12개 이다. STD DP(standard double pulse) 모드에서는 3개의 블록이 전송되며, STD DP모드에서 심볼 패킷을 생성하기 위해 매 5비트의 심볼은 다른 주파수상에서 2개의 연속되는 펄스가 맵핑되고, 이러한 반복과정은 페이딩이나 재밍과 같은 환경에 강인한 전송능력을 제공하기 위해서이다. 그러므로 1개의 타임 슬롯내에서는 186(=2×3×31)개의 정보 펄스가 있으며, 32개의 동기 펄스, 8개의 TR(time refinement) 펄스, 32개의 헤더 펄스가 추가된다. 그러므로 1개의 표준 DP 슬롯 내에서는 258개의 전체 펄스 수를 가지게 된다. 매 헤더는 5비트 심볼이 7개인 35비트의 정보로 구성되고, 헤더정보는 RS(16,7) 부호화에 의해 보호된다. 헤더는 항상 32개의 펄스인 DP 형식으로 전송된다. 1개의 슬롯내에 P2DP (packed-2 double pulse) 또는 P2SP (packed- 2 single pulse)모드를 사용하여, 6개의 RS 블록으로 전송하는 것이 가능하다.

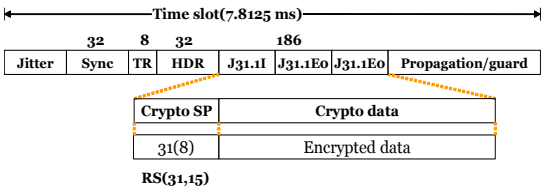
III. 무선 키 갱신(OTAR)을 위한 암호 동기신호 분석

LINK16에서 무선 키 갱신은 OTAR 관리메시지를 위한 J31.0메시지와 J31.1메시지가 있다. J31.0메시지는 관리를 위해 사용되고, J31.1메시지는 키 갱신을 위해 사용된다. 관리메시지와 갱신 메시지는 초기워드(Initial word), 연속워드(continuous word), 확장워드(extended word)로 구성된다. OTAR 관리를 위해 사용되는 39비트의 키 동기는 J31.1 송신/수신 규칙의 암호 동기를 위해 사용되는 39비트이며, J31.0 관리 메시지 확장워드를 통해 전송된다.

Spare (5)	CPD Synch (1)	Key locial Label synch (7)	Key synch bits (39)	CPD Rekey (1)	Key Logical Label, rekey (7)	Memory Loc, rekey (3)	Continuation Word label (5)	Word Format (2)

▶▶ 그림 2. OTAR J31.0 확장워드 형식

본 논문에서는 무선전송환경에서 동기 39비트가 전송환경에 받는 영향을 분석하여 전송성능을 분석한다. 스트림 암호통신에서 동기능력은 전송채널조건에서 동기신호검출에 대한 정확성 여부와 유사신호에 대한 정확한 검출능력에 의해 결정되며, 송신신호에 대한 수신신호의 검출확률 P_D, 동기신호의 미검출확률 P_M, 송신측에서 미 전송시에 수신측의 송신한 것으로 판단하는 오검출 확률 P_F 등에 의해 결정된다.



▶▶ 그림 3. OTAR 메시지 암호통신시 전송구조

무선채널 구간이 갖는 평균 비트오류율(BER) 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.

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

$$P_{Mi} = 1 - P_{Di} \quad (2)$$

이때 i는 0, 1, ..., n이다. 따라서 m개까지의 오류가 발생했을 때의 동기 검출 확률 P_{TD}는 식3과 같다.

$$P_{TD} = \sum_{i=0}^{m} P_{Di} \quad (3)$$

각 오류개수에 대한 *false alarm* 확률 PFi는 채널의 오류로 인해 동기 신호를 잘못 검출할 수 있는 오검출 확률로 식4과 같이 계산된다.

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

이때 i는 0, 1, ..., n까지이다. m개까지의 오류가 발생했을 때의 *false alarm* 확률 P_{TF}는 식5과 같다.

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

비트오류율이 10^{-1}의 채널환경은 현실적으로 통신이 이루어지기 매우 어려운 환경이다.

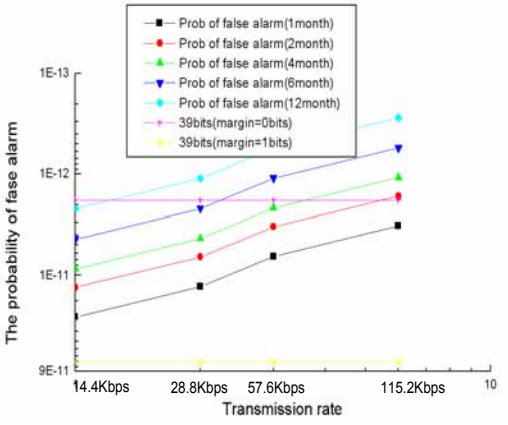
[표 1] 비트오류율, 동기길이에 따른 동기검출 확률

동기 패턴	동기길이 39bits				
	10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}
P_{D0}	1.19E-9	0.140884	0.822755	0.980684	0.998052
P_{D1}	3.35E-8	0.424046	0.983674	0.999817	0.999998
P_{D2}	4.59E-7	0.701313	0.999007	0.999999	1
P_{D3}	4.1E-6	0.877546	0.999956	1	1
P_{D4}	2.68E-5	0.959287	0.999998	1	1
P_{D5}	0.000137	0.988775	1	1	1
P_{D6}	0.000571	0.997386	1	1	1
P_{D7}	0.001989	0.999478	1	1	1
P_{D8}	0.005922	0.99991	1	1	1
P_{D9}	0.015317	0.999986	1	1	1
P_{D10}	0.034865	0.999998	1	1	1
P_{D11}	0.070605	1	1	1	1
P_{D12}	0.128438	1	1	1	1
P_{D13}	0.211739	1	1	1	1
P_{D14}	0.319026	1	1	1	1
P_{D15}	0.443034	1	1	1	1
P_{D16}	0.572034	1	1	1	1
P_{D17}	0.693073	1	1	1	1
P_{D18}	0.795667	1	1	1	1
P_{D19}	0.874307	1	1	1	1
P_{D20}	0.928845	1	1	1	1
P_{D21}	0.963065	1	1	1	1
P_{D22}	0.982482	1	1	1	1
P_{D23}	0.992435	1	1	1	1
P_{D24}	0.997036	1	1	1	1
P_{D25}	0.998951	1	1	1	1

비트 오류율이 10^{-2} 이상의 채널환경은 동기패턴 검출능력이 100%이상을 제공하기 위해서는 여유비트가 11비트가 허용되어야 하며 정상적인 암호통신이 가능하다. 검출확률은 식3과 식5를 이용하여 P_{TD}와 P_{TF}을 얻을 수 있다. 전송속도가 v이고 *false alarm*이 발생할 시간간격이 T시간이면 *false alarm*이 발생할 확률 $P_{v\cdot T}$은 식6과 같다.

$$P_{v\cdot T} = \frac{1}{v\cdot T} \quad (6)$$

그림 4를 통해 살펴볼 때, 동기패턴 길이가 39비트 환경에서 동기검출확률이 100% 성공적으로 검출되기 위해서는 이론적으로 여유비트가 0비트도 허용하지 않는다. 그림에서 전송속도와 1년/6개월/4개월/2개월/1개월에 1회 false alarm이 발생할 확률간의 상관관계를 살펴볼 때 1비트의 오류를 허용하지 않으며, 39비트가 모두 정상적으로 전송되어야 동기검출 능력이 100% 보장받음을 의미한다. 그러나 현실적으로 동기신호는 RS(31,15)의 채널부호화를 통해 전송되므로 평균 4비트의 오류가 발생하더라도 정상적인 동기신호 검출로 판단할 수 있는 허용여유를 제공한다.



▶▶ 그림 4. 동기신호 오검출 확률

IV. 결론

본 논문에서는 항공통신 전술 데이터링크로 사용되는 LINK16 시스템이 무선 키 갱신을 위해 사용되는 동기신호에 대한 전송성능을 분석하였다. 동기신호가 무선 심볼오류율 환경에서 동기검출 확률과 전송속도, 오검출 확률이 주어진 시간동안에 갖는 전송 영향 정도를 분석하였다. 이론적으로 39비트 동기신호는 정상적으로 100% 동기검출이 보장되기 위해서는 1비트의 허용 여유비트도 존재하지 않으며, 동기신호가 RS(31,13)에 의한 채널부호화를 통해 4비트정도의 허용 여유는 보장받을 수 있다.

▌참고문헌▐

[1] MIL-STD-6016A,"TADIL(tactical digital informatio n link) J message standard," 1997. Feb.

[2] http://www.nap.edu/openbook/0306074266/html /151 .html

[3] Europenan organisation for the safety of air navigation,"Feasibility study for civil aviation data link for ADS-B based on MIDS/Link16," 2003. Aug.

[4] http://prodevweb.prodev.usna.edu/SeaNav/NS40x /NS 401_old /introduction/html/indexintro.html

[5] Air land Sea Application Center,"Introduction to Tactical Digital Information Link J and Quick Reference Guide," 2000. June

[6] Van Til borg, H. C. A.,*An Introduction to Cryptology*, KLUWER Academic Pub., Boston, 1988.

[7] H. J. Beker and F. C. Piper, Cipher Systems : *The Protection of Communications*, Northwood Books, London, 1982.

[8] B. Schneier, *Applied Cryptography 2nd ed. : Protocols, Algorithm, and Source code in C*, John Willy & Son, New York, 1996.

[9] William Stallings, "Wireless Communications and network," Prentice Hall, pp.110-123, 2001.

[10] J. A. Roberts and J. M. Bargallo,"DPSK Performance for Indoor Wireless Rician Fading Channels," *IEEE Trans. Commun.*, Vol. COM-42, pp. pp.592-596, 1996. Feb.

[11] Roberts, J.A., Abeysinghe, J.R."A two-state Rician model for predicting indoor wireless communication performance," *IEEE Intern.* Conf., Commun. Seattle, vol.1, pp.40-43, 1995. June

[12] Yao, Y.-D., Sheikh, A.U.H.,"Outage probability analysis for microcell mobile radio systems with cochannel interferers in Rician/Rayleigh fading environment," *IEE*, Electronics Letters, vol.26, pp.864-866, 1990. June

[13] Prasad, R., Liu, C.-Y.,"Throughput analysis of some mobile packet radio protocols in Rician fading channels," *in Proc. IEE*, Commun.,

vol.139, pp.297-302, 1992. June

[14] Muammar, R.H.,"Co-channel interference in microcellular mobile radio system," *41st IEEE,* Veh. Technol. Conf., pp.198-203, 1991. May

[15] Hassan, A., Chennakeshu, S., Anderson, J.,"Performance of coded slow-frequency-hopped TDMA cellular systems," *IEEE 43rd*, Veh. Technol. Conf., pp.289-292, 1993. May

[16] Chennakeshu, S., Hassan, A.A., Anderson, J.B., Gudmundson, B.,"Capacity analysis of a TDMA-based slow-frequency-hopped cellular system," *IEEE Trans*., Veh. Technol., vol.45, pp.531-542, 1996. Aug.

[17] Kostic, Z., Maric, I., Wang, X.,"Fundamentals of dynamic frequency hopping in cellular systems," *IEEE J*., Select. Areas Commun., vol.19, pp.2254-2266, 2001. Nov.

[18] Alberto Leon-Garcia,"Probability and Random Processes for Electrical Engineering," Addison Wesley, 1994.