

# 항공전술 통신체계에서 TDMA STD DP 전송모드의 인터리빙 전송성능 분석

## Transmission Performance Analysis of Interleaving of TDMA STD DP transmission mode in Air Tactical Communication System

홍진근\*, 박선춘\*\*, 김성조\*\*, 박종욱\*\*

Hong jinkeun, Park sunchun, Kim sengjo, Park jongwook

**Abstract** - In this paper, we analyse transmission performance of interleaving for cipher communication in TDMA STD DP mode of aerial tactical communication link. In LINK16 link we present about transmission architecture of STD DP mode and study an effect of interleaving, the capability of crypto synchronization pattern, and a quality of degraded effect of transmission communication during crypto communication.

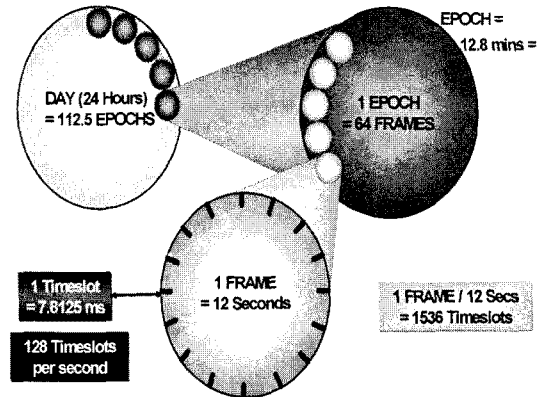
**Key Words** : LINK16, TDMA, interleaving, fading, JTIDS, MIDS

### 1. 서론

미 해군은 LINK16 전술 무선망 기술의 성능 개선을 위한 프로그램을 진행 중이다. JTIDS 및 현재의 다양한 형태를 갖춘 MIDS는 분배용 제어 메시지를 위한 무선 시스템으로 미 해군이 선택하였고, JTIDS/MIDS시스템은 LINK16 네트워크 기법 및 메시지 집합으로 구성되며, 전송되는 메시지는 감시 트랙, 무기 조정, 공중 제어, 목표물 정보, PPLI, 디지털화된 음성 네트워크를 포함하고 있다. JTIDS 및 다중의 MIDS는 항공기, 지상 함정, 잠수함 등 다양한 곳에 설치하여 운용하며, 항공전술 통신체계에 TDMA 방식으로 운용되고 타임 슬롯은 데이터 송신 및 수신을 위해 모든 LINK16 네트워크 참가자 가운데서 시간적으로 할당하여 사용하고 있다[1]. TDMA 구조의 기본적인 요소는 단독 통신 회선 또는 다수의 사용자에 의해 공유되는 네트워크로 구성되며, 넷(net)은 메시지 전송을 위해 JTIDS 개개 참가자들에게 할당 가능한 타임 슬롯으로 나누어진다. 통신 능력은 다수 개의 넷 상에서 동시 운용을 위해 확장이 가능하고, JU는 단지 특정시간에 단독 네트워크 상에서 운용하지만, 타임 슬롯을 기준으로 타임 슬롯 상에서 넷 교환이 가능한 구조로 이루어져 있다. 본 논문에서는 LINK16 통신시스템을 특징을 살펴보고, 전송정보에 대한 메시지 패킹 구조를 기준하여 암호통신을 수행할 때 인터리빙이 전송성능에 미치는 영향을 분석하였다. 2장에서는 LINK16의 특성에 대하여 살펴보고, 3장에서는 암호통신에서 인터리빙을 적용할 때 통신에 미치는 전송성능을 분석하였고, 4장에 결론을 맺었다.

### 2. LINK16 통신시스템

LINK16은 개개 JU에 데이터 전송을 위한 유일한 타임 슬롯을 할당하도록 네트워크를 설계함으로써 NCS에 대한 요구사항을 제거 시켰다. 이 TDMA 기법은 데이터 전송에 사용되는 1536개의 타임 슬롯으로 나누어진 12초 길이의 프레임들을 제공한다. 다중 넷 구조에서 동시성과 방해받지 않는 통신 능력을 제공하며 이는 많은 사용 가능한 넷에서 각자가 단일 JTIDS 네트워크 상에서 동일한 51개의 주파수를 사용하며, 통신을 위해 다른 주파수 호핑 패턴을 사용한다. LINK16에서 시간할당은 데이터 전송에 사용되는 1536개의 타임 슬롯으로 나누어진 12초 길이의 프레임들을 제공한다. 협대역 채널로부터 재밍을 방지하기 위해 단말의 송신 주파수는 각 펄스를 변경하여 사용하며 주파수 호핑 패턴은 하나의 net으로 정의하고 있다. 다중 넷 구조에서 동시성과 방해받지 않는 통신 능력을 제공한다.



<그림1> LINK16의 타임 구조

저자 소개

\* : 천안대학교 정보통신학부

\*\* : 국가보안기술연구소

### 3. LINK16 암호통신

#### 3.1 무선채널 환경

라이시안 페이딩 모델은 직접파 성분과 반사파 성분이 복합된 수신신호로  $K$ 값이 다른 여러 전파환경에서 포락선 크기( $r$ )의 제곱을  $\gamma$ 로 정의하고  $\gamma_0$ 와  $K$ 를 파라미터로 하는  $\gamma$ 에 대한 확률밀도함수  $P_R(\gamma)$ 는 다음 식1에서와 같다.

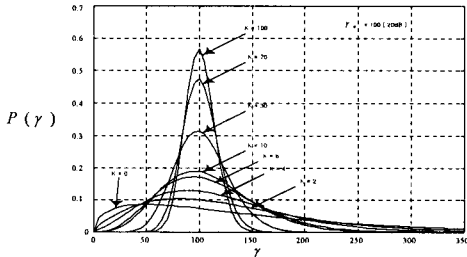
$$P_R(\gamma) = \frac{K+1}{\gamma_0} e^{[-K - \frac{\gamma(K+1)}{\gamma_0}]} \cdot I_0[2\sqrt{\frac{\gamma K(K+1)}{\gamma_0}}] \quad (1)$$

$\gamma$ 는 순시 수신반송파대 잡음전력비,  $I_0(\cdot)$ 는 0차 변형베셀 함수,  $K$ 는 직접파전력( $\frac{a^2}{2}$ ) 대 반사파 전력( $\sigma^2$ )비로서  $K = \frac{a^2}{2\sigma^2}$ 의 값을 가진다. 라이시안 확률분포를 갖는 포락선 크기  $r$ 의 제곱 평균  $E(r^2) = a^2 + 2\sigma^2$ 를  $\gamma_0$ 로 정의하고 평균 수신반송파대 잡음전력비를 나타낸다. 라이시안 확률분포로부터 페이딩 신호레벨과 진폭의 확률분포 관계인 CPD를 식2에서와 같이 구할 수 있다. 또한 라이시안 채널에서 오류율은 식3과 같다.

$$P(\gamma \leq L) = \int_{\gamma=0}^L P_R(\gamma) d\gamma \quad (2)$$

$$P_e = \int_{\gamma=0}^{\infty} P_b \cdot P_R(\gamma) d\gamma \quad (3)$$

이때  $P_b$ 는 잡음영향으로 인한 비트 오류율이고  $P_R(\gamma)$ 는 라이시안 채널의 확률밀도함수이다.



<그림2> PDF of rician fading channel( $\gamma_0=100$ )

$K=0$ 인 경우 레일리 페이딩 분포이고 페이딩이 매우 강한 전파환경에 해당한다. 이 환경은 직접파 성분이 없고 반사파만 수신하는 경우이고  $K=\infty$ 이면 페이딩이 거의 없는 전파환경으로 자유공간으로 볼 수 있다. 라이시안 페이딩은 다중경로와 LOS 경로가 동시에 존재하는 환경을 모델링 하는데 적합한 페이딩 채널이다. LINK16은 UHF에서 LOS 경로를 원칙으로 한다. 라이시안 페이딩 채널에서 Differential-Phase-Shift-Keying (DPSK) 기법을 적용하여 비트오류율을 살펴보면 식4와 같이 나타낼 수 있다.[10][11]

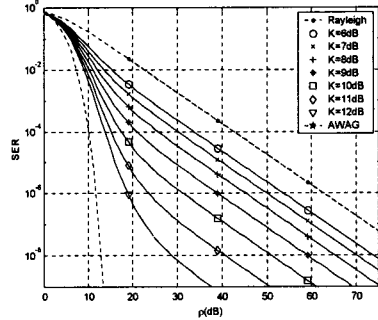
$$BER(\rho, K) = \frac{1+K}{2(\rho+1+K)} \exp\left(\frac{-K\rho}{\rho+1+K}\right) \quad (4)$$

$\rho$ 는 1비트 당 신호 에너지와 잡음간의 비율( $E_b/N_0$ )로 나타낼

수 있으며,  $K$ 는 식1에서 정의한 파라미터를 의미한다. 따라서 1개의 심볼(5비트로 구성)에 오류가 발생할 확률(SER)은 식5와 같이 정의된다.

$$SER(\rho, K) = 1 - (1 - BER)^5 \quad (5)$$

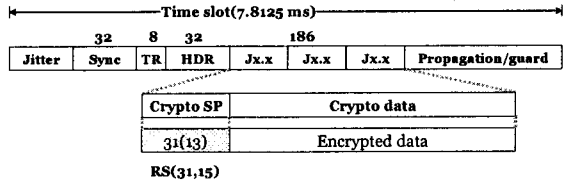
식5에 대하여 6dB에서부터 12dB로  $K$ 를 변화시켜가며 SER를 살펴본 결과를 그림3에서 제시하였다.



<그림3> S/N vs. word error rate in a Rician fading DPSK

#### 3.2 LINK16 표준 DP 전송프레임 구조

표준 DP구조에서는 심볼 패킷을 생성하기 위해 매 5비트의 심볼이 별개의 주파수상에서 2개의 연속되는 펄스가 맵핑된다. 이러한 처리를 통해 페이딩이나 재밍과 같은 환경에 강인한 전송능력을 제공할 수 있다. 따라서 하나의 타임 슬롯내에서는 186(=2×3×31)개의 정보 펄스가 존재하며, 표준 DP구조에서는 32개의 동기 펄스, 8개의 TR(time refinement) 펄스, 32개의 헤더 펄스가 추가된다. 하나의 표준 DP 슬롯에서 전체 펄스 수는 258개를 가지게 된다. 매 헤더에는 5비트 심볼이 7개인 35비트의 정보로 구성되고, 헤더정보는 RS(16,7) 부호화에 의해 보호된다. 헤더는 항상 32개의 펄스인 DP형식으로 전송되며, 암호화를 위해 사용되는 동기 패킷길이를 63비트로 선택하여 RS(31,15)를 적용할 수 있다.



<그림4> 표준 DP 패키징 구조를 적용한 암호프레임 구조

무선채널 구간이 갖는 평균 비트오류율(BER)  $P_e$ 는 1비트를 1회 전송시 오류가 발생할 확률로 나타낼 수 있다. 암호기에서  $n$ 비트의 동기 신호를 송신할 때 복호기에서는  $0 \sim n$ 개의 오류를 가진 동기 신호가 수신된다. 이때  $n$ 비트 가운데  $i$ 비트 오류 개수가 검출될 동기 검출 확률  $P_{Di}$ 는 식5에서와 같다.

$$P_{Di} = n C_i P_e^i (1 - P_e)^{n-i} \quad (5)$$

이때  $i$ 는  $0, 1, \dots, n$ 이다. 따라서  $m$ 개까지의 오류가 발생했을 때의 동기 검출 확률  $P_{Dm}$ 는 식6과 같다.

$$P_{TD} = \sum_{i=0}^m P_{Di} \quad (6)$$

각 오류개수에 대한 false alarm 확률  $P_{Fi}$ 는 채널의 오류로 인해 동기 신호를 잘못 검출할 수 있는 오검출 확률로 식7과 같이 계산된다.

$$P_{Fi} = n C_i 0.5^i (1-0.5)^{n-i} = n C_i 0.5^n \quad (7)$$

이때  $n$ 은 0, 1, ...,  $m$ 까지이다.  $m$ 개까지의 오류가 발생했을 때의 false alarm 확률  $P_{TF}$ 는 식8과 같다.

$$P_{TF} = \sum_{i=0}^m n C_i 0.5^n \quad (8)$$

주어진 상기 식들로부터 동기길이 63비트에 대한 동기검출확률은  $10^{-1}$ 채널에서 현실적으로 통신이 어렵다고 판단되고,  $10^{-2}$ 채널에서는 적어도 동기검출확률이 99%를 보장하려면 7비트 정도의 여유비트를 허용해야 가능하다.  $10^{-3}$ 이상 채널에서는 99%이상의 동기검출 능력을 가지고 있다고 볼 수 있다. 만일 전송속도가 57.6 Kbps를 제공하는 환경에서 적어도 1년간 동기 오검출이 일어나지 않는 확률을 보장하고자 한다면  $5.5 \times 10^{-13}$  확률을 가지므로 이 경우 63비트 패턴을 사용하여 암호 동기를 검출할 때 4~5비트의 여유비트를 허용해도 정상적인 암호동기를 판단할 수 있다. 즉 63비트 비트 가운데 4~5비트가 오류가 발생할 경우에 정상적으로 암호 동기를 찾을 수 있는 경우가 된다. 만일  $K=0$ 인 페이딩 채널에서 LINK16 주파수 969MHz 대역, 이동속도가 24Km/h, 전송속도가 57.6Kbps 환경에서 평균 전력변이(-25dB, -10dB, 0dB)가 일어날 때, 발생할 수 있는 최대 버스트의 길이는 50, 360, 1980 비트 길이를 갖는다. 만일 인터리빙 depth를 52, 360, 1980 값으로 정하면, 인터리빙 구조는  $52 \times 1090$ ,  $360 \times 1090$ ,  $1980 \times 1090$  구조를 정할 수 있다. 인터리빙 depth에 따라 지연시간은 50일 경우 1sec, 360일 경우 7sec, 1980의 경우 38sec가 소요되며, depth를 증가시킬수록 지연시간이 상대적으로 증가한다.

<표1> 인터리빙 depth에 따른 지연시간 비교

	$52 \times 1090$	$360 \times 1090$	$1980 \times 1090$
57.6Kbps	≈1sec	≈7sec	≈38sec

300회를 인터리빙 하여 전송하고 최대 버스트 길이는 52, 360, 1980에서 균일한 분포로 발생한다고 하면, 전송을 위해 1시간 16분이 소요되며, 인터리빙 depth 52, 260, 1980에 따라 정상적으로 복호된 데이터양과 손실된 데이터양을 나타내었다.

<표2> 전력변이와 인터리빙 depth에 따른 복호 데이터양 비교

	정상적인 데이터양	손실된 데이터양
인터리빙 ×	0	2.60E+8
depth= 52	5.67E+6	2.55E+8
depth= 360	4.49E+7	2.16E+8
depth=1980	2.60E+8	0

LINK16 통신체계에서 전력변이에 달라지는 최대 버스트

길이를 갖는 최악의 통신환경을 고려하여 암호통신을 수행할 때, 암호통신의 전송능력과 인터리빙 영향을 분석하였다.

#### 4. 결론

본 논문에서는 항공 전술통신체계에서 사용되는 LINK16시스템의 통신특성을 살펴보았으며, 제시된 표준DP 메시지 패킹 구조를 이용하여 암호통신을 수행할 때, 전송되는 암호동기의 영향을 살펴보았으며, 인터리빙을 적용할 때 인터리빙 구조에 따른 암호통신 능력을 분석하였다.

#### 참 고 문 헌

- [1] MIL-STD-6016A, "TADIL(tactical digital information link) J message standard," 1997. Feb.
- [2] <http://www.nap.edu/openbook/0306074266/html/151.html>
- [3] European 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/NS401\\_old/introduction/html/indexintro.html](http://prodevweb.prodev.usna.edu/SeaNav/NS40x/NS401_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 Tilborg, 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. 592-596, 1996. Feb.
- [11] Roberts, J.A., Abeyasinghe, 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.