論文

항공전술 통신링크에서 암호통신을 위한 전송성능 분석

홍진근*, 박선춘**, 김성조**, 박종욱**

Transmission Performance Analysis for cipher communication in aerial tactical communication link

Jinkeun Hong*, Sunchun Park**, Sengjo Kim** and Jongwook Park**

ABSTRACT

LINK16 is a system which is designed to maximize performance in a particular tactical environment with high levels of jamming. In this paper, transmission performance of synchronization pattern for cipher communication in aerial tactical communication link is presented. Transmission architecture of operating mode (standard DP, P2SP, P2DP, P4mode) in LINK16 network is discussed, and an effect of synchronization pattern, a quality of degraded effect of transmission communication for collision probability between hopping frequencies and fading channel in crypto communication is analyzed.

초 록

LINK16은 고수준의 재밍을 갖는 전술네트워크 환경에서 성능 최대화를 위해 설계된 시스템이다. 본 논문에서는 항공통신 전술링크에 사용되는 암호통신에서 동기패턴의 전송성능을 분석하였다. 현재 LINK16 링크에서 운용되는 통신모드(표준 DP, P2SP, P2DP, P4mode)의 전송구조를 고찰하였으며, 암호통신과정에서 주파수간의 충돌확률 및 페이딩 채널에 대한 동기패턴의 영향, 전송성능 열화요인을 분석하였다.

Key Words: Tactical communication(전술통신), LINK16(링크16), Cipher(암호)

Ⅰ. 서 론

현재 전자, 컴퓨터, 통신기술의 발전과 함께 우주 항공분야에서도 유인항공분야, 무인항공분야, 위성분야에서 개선된 통신시스템 및 통신네트워크에 관한 연구가 지속적으로 이루어지고 있다[1-4].

미 해군은 LINK16[5] 항공통신 전술네트워크 기술의 성능개선을 위한 프로그램을 진행 중에 있으며, JTIDS(joint tactical information distribution system) 및 현재의 다양한 형태를 갖춘 MIDS(multi functional information distribution system)는 분해용 제어 메시지를 위한 무선 시스템으로 LINK16(TADIL J) 네트워크 기법 및 메시지 셋으로 구성하여 운용하고 있다. 이들 메시지는 감시트랙, 무기조정, 공중제어, 목표물 정보, PPLI (precise participant location and identification), 디지타이저된 음성 네트워크를 포함한다. JTIDS 및 다종의 MIDS는 항공기, 지상 함정, 잠수함 등 다양한 곳에 설치하여 운용되고 있으며 확대 보급될 예정이다. LINK16은 항공과 항공, 항공과 지상 전술네트워크를 구축

† 2004년 9월 14일 접수 ~ 2005년 1월 10일 심사완료
* 정회원, 천안대학교 정보통신학부
연락저자, E-mail : jkhong@cheonan.ac.kr
충남 천안시 안서동 115번지
** 국가보안기술연구소 응용기술연구부

하여 실시간에 준하는 데이터링크로서 C4I command, control, communications, computers, intelligence) 시스템간에 정보교환을 지원하는 통신, 항법, 식별 시스템으로, LINK16의 무선 송수신 컴포넌트는 JTIDS(joint tactical information distribution system) /MIDS (multifunctional information distribution system)이며, 이들 고용량 UHF, LOS, 주파수 호핑 데이터 통신을 지원하는 단말들은 안전하고, 안티 재밍의 음성 및 디지털 데이터 교환을 제공한다.

기존 연구에서는 Wilson J. W.가 LINK16 사례연구[6]에서 LINK16 계층구조에 대해 살펴본 바 있고, B. E. White는 논문[8]에서 전술 데이터링크, 항공트래픽 관리와 SDR(software programmable radios)에서 CADL(civil aviation data link)과 LINK16 통합방안을 언급하고 있다. 현재 EUROCONTROL에서는 ADS-B를 위한 MIDS의 민간용 버전에 대한 구현 가능성 연구[9]를 수행하고 있는 실정이다. 또한 LINK16은 현재 민간용 및 군사용이 통합 운용방안이 검토되고 있으며 선진국은 LINK16 및 통합운용방안[10][12]에 대한 연구가 활발하게 진행 중에 있으나 국내에서는 아직 이에 대한 연구가 미미한 실정이다. 특히 LINK16 보안체계는 MSEC (message security)과 TSEC(transmiss ion security)으로 구성된 보안기능을 제공하고 있으나 이에 대해 구체적으로 연구가 발표된 바는 없다. 이러한 차원에서LIKN16이 민간망과 연동되거나 자체 독립적으로 운용될 때 반드시 고려되어야 할 사항인 보안체계에 대한 연구가 필요하고, 본 논문은 LINK16의 메시지 보안과 전송보안을 위한 암호통신 환경에서 메시지를 전송할 때 암호 동기패턴이 전송보안을 위한 주파수 호핑 환경과 무선 채널의 페이딩 현상에서 어떠한 영향을 갖는지에 대해 분석하였다. 본 논문의 구성은 II장에서 LINK16의 특성에 대하여 살펴보았으며, III장에서 암호통신에서 성능을 분석하였고, IV장에서 주파수 호핑 패턴 및 무선 채널에서의 페이딩 현상이 통신에 미치는 영향을 시뮬레이션을 통해 살펴보았다. 그리고 마지막으로 V장에서 결론을 맺었다.

II. LINK16 통신시스템

LINK16에서 사용되는 JTIDS 단말은 하나의 파형을 사용하고, 전체 24시간은 112.5 epochs로 나누어지며, 각 epochs는 12.8분을 유지하고, 각 epoch는 7.8125 msec 간격이며 타임 슬롯이 1

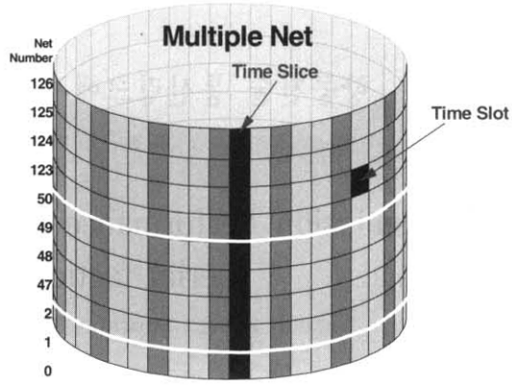

Fig. 1. Multi net operation of LINK16

epoch 당 98,304 타임 슬롯으로 구성된다.

각 셋에서 타임 슬롯은 셋 당 32,768 슬롯의 3개 셋(A, B, C)으로 조직되며, 각 셋 내의 슬롯은 0부터 32,767까지 번호가 주어지고 각 슬롯은 0A, 1A 등과 같은 슬롯 번호로 식별된다. 슬롯들은 각 epoch 내의 시간으로 분배되고, 셋 A의 타임 슬롯 n은 셋 C의 n-1 타임 슬롯을 따른다. 셋 B의 n을 앞서며, n은 0에서 32,767 시퀀스에서 정수 집합으로 정의하고 있다. 현재 LINK16 운용모드는 4개의 모드이며, 모드1에서는 암호화와 주파수 호핑을 사용하고 있으며, 모드2에서는 969MHz 대역의 단말 주파수와 암호화를 사용한다. 모드3에서는 클래스1(과거 버전) 단말과 호환성을 갖고 사용하고 있으며, 모드4에서는 969MHz 대역에서 단말 주파수에 암호화는 사용하지 않는다.

Table 1. Data rates of JTIDS/MIDS

메시지 유형	최대 처리율	TADIL J 워드/슬롯	P4SP와 비교할 때
표준DP	28.8Kbps	3	1/4×
P2SP	57.6Kbps	6	1/2×
P2DP	57.6Kbps	6	1/2×
P4SP	115.2Kbps	12	1×

III. 전송시스템 성능분석

3.1 무선채널 환경

항공 데이터통신의 서비스 요구에 발맞추어 선결해야 할 과제는 보안에 대한 위협요소들로부터 보호대책 수립이다[13-15]. 항공 데이터통신에서 고려되는 보안 위협요소에는 불법사용, 도청

(eavesdropping), 가로채기(interception), 전파교란(jamming), 정보유출, 파괴, 수정 등이 있다. 대부분의 무선채널에서는 전달거리가 제한적이고 전달거리내 신호대 잡음비가 유선에 비해 상당히 낮아서 전송채널에서 다량의 정보손실이 발생한다. 특히 항공통신을 포함한 무선채널에서 버스트 오류 발생 원인인 페이딩 현상[16-18]은 짧은 시간간격동안 신호세기의 급격한 변화, 다른 멀티패스 신호에서 변화하는 도플러 변이에 의한 랜덤 주파수 변조, 멀티패스 전송지연에 의한 시간 분산 등과 같은 요인으로 인해 발생한다. 라이시안 분포[16]는 직접파 성분과 분산이 σ^2인 독립적인 가우시안 성분을 포함하는 반사파 성분으로 구성되며 다른 페이딩 채널의 모델링이 가능하다. 라이시안 페이딩 모델은 직접파 성분과 반사파 성분이 복합된 수신신호로 K값이 다른 여러 전파환경에서 포락선 크기(r)의 제곱을γ로 정의하고 γ_0와 K를 파라메터로 하는 γ에 대한 확률밀도함수 $P_R(\gamma)$는 식1에서와 같다.

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

γ는 순시 수신반송파대 잡음전력비, $I_0(\cdot)$는 0차 변형베셀 함수, K는 직접파전력($\frac{a^2}{2}$)대 반사파전력 (σ^2)비로서 $K=\frac{a^2}{2\sigma^2}$ 의 값을 가진다. 라이시안 확률분포를 갖는 포락선 크기 r의 제곱평균 $E(r^2)=a^2+2\sigma^2$를 γ_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.

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

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

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

LINK16은 UHF에서 LOS 경로를 원칙으로 한다. 라이시안 페이딩 채널에서 DPSK (differential phase shift keying)기법을 적용하여 비트 오류율을 살펴보면 식4와 같이 나타낼 수 있다[17].

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

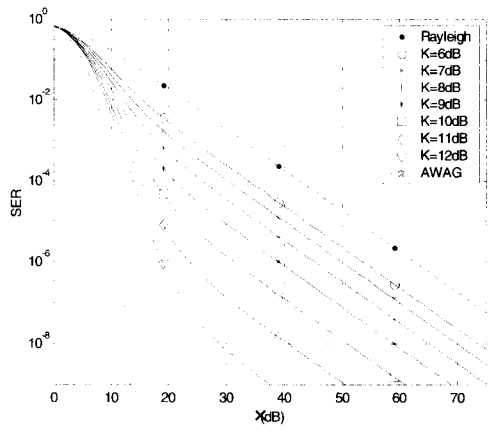

Fig. 2. S/N vs. word error rate in a Rician fading DPSK

ρ는 1비트 당 신호 에너지와 잡음간의 비율(E_b/N_o)로 나타낼 수 있으며, K는 식1에서 정의한 파라메타를 의미한다. 따라서 1개의 심볼에 오류가 발생할 확률(WER)은 식5와 같이 정의된다.

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

식5에 대하여 6dB에서부터 12dB로 K를 변화시켜가며 WER를 살펴본 결과를 Fig. 2에서 제시하였다.

3.2 LINK16 암호통신에서 동기신호의 주파수 호핑에 따른 WER 분석

TDMA 전송 데이터 메시지의 전송구조는 지터(jitter), 동기(synchronization), TR (time refinement), Header(HDR), 데이터, Propagation /Guard 정보로 구성된다. 지터(jitter)는 타임 슬롯에서 전송시작 시에 가변적인 시간지연으로 통신모드4에서 운용될 때 적용되지 않는다. 즉, RTT 메시지가 전송될 때, P2DP(packed 2 double pulse) 또는 P4모드 메시지 패킹 구조에서 메시지를 전송할 때 지터는 적용되지 않는다. 동기패턴은 DP 심볼 패턴이 수신되는 JUs에 동기화 용도로 허용된다. 패턴은 타임 슬롯에서부터 타임 슬롯으로 바뀌고, 하나의 타임 슬롯내의 패턴은 망 가운데 서로 다르다. TR은 4개의 DP 심볼 패킷의 고정된 패턴이 TR용으로 사용된다. HDR는 하나의 타임 슬롯내에 전송되는 메시지와 관련된 정보를 제공하며, 데이터는 타임슬롯내에 전송되는 메시지 정보를 제공하고, Propagation /Guard는 다음 타임 슬롯 전송을

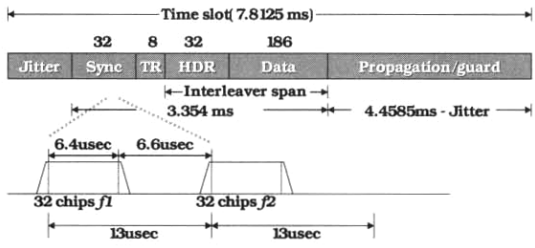

Fig. 3. Transmission architecture of STD DP

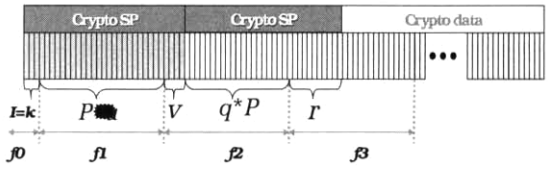

Fig. 4. Frequency hopping architecture of crypto SP(synchronization pattern)

위해 JUs에게 최대 범위 및 시간적인 허용을 위해 사용되는 시간주기이다. 이 경우 300nm (nautical miles, normal) 또는 500nm(extended)의 최대 영역까지 가능하도록 선택된다. LINK16은 7개의 계층구조로 이루어져 있으며, 임무계층, 응용계층, 서비스계층, 전달계층, 네트워크계층, 링크계층, 물리계층으로 구분하고 있다[6]. LINK16은 TDMA 프로토콜을 근거하고 있으며 타임 슬롯 내의 모든 통신이 초당 128개 타임 슬롯이며, 하나의 타임 슬롯내의 1개의 심볼은 주기적으로 32개의 값 가운데 하나에 의해 쉬프트되는 32개의 chip 시퀀스가 CCSK를 사용하여 부호화된다. 전송프레임은 각 15개의 심볼에 패리티 16개 심볼로 구성된 블록당 전체 31개의 심볼이 리드 솔로몬부호(RS(31,15), FEC)를 통해 전송된다. STD DP 모드에서는 3개의 블록이 전송되며, STD DP모드에서 심볼 패킷을 생성하기 위해 매 심볼은 다른 주파수상에서 2개의 연속되는 펄스가 맵핑되고, 이러한 반복과정은 페이딩이나 재밍과 같은 환경에 강인한 전송능력을 제공하기 위해서이다.

따라서 1개의 타임 슬롯내에서는 186 (=2×3×31)개의 정보펄스가 있으며, 32개의 동기펄스, 8개의 TR(time refinement) 펄스, 32개의 헤더 펄스가 추가된다. 1개의 표준 DP 슬롯내에서는 258개의 전체 펄스 수를 가지게 된다. 각 헤더는 5비트 심볼이 7개인 35비트의 정보로 구성되며, 헤더정보는 RS(16,7) 부호화에 의해 보호되고, 헤더는 항상 32개의 펄스인 DP형식으로 전송된다. P2DP와 P4SP모드에서 펄스의 수는 444개이고, 이 경우 지터는 제거되며, 데이터 레이블된 블록의 크기는 2배가 된다. LINK16의 순간적인 대역폭은 채널 여유 공간을 고려하여 3MHz로 고려할 수 있으며, P4모드의 정보효율은 115.2Kbps이다.

3.3 전송성능 분석

LINK16에서 데이터 메시지는 75비트 워드로 구성되고, 각각 RS(31,15) 부호화되어 전송된다. RS(31,15) 코드워드는 31개 심볼 가운데 15개 심볼이 데이터에 해당하고, 16개 심볼이 패리티 정보이다. RS(31,15)와 RS(16,7) 코드워드는 동일한 로직에 의해 부호화 및 복호화 된다.

일반적으로 주파수 호핑이 평균 초당 2000회가 일어난다면, 암호통신 동기신호와 암호화된 데이터 영역에서 평균 4회에서 5회 정도 발생한다고 볼 수 있다. 만일 주파수 호핑 과정에 암호통신 동기신호를 정확하게 검출하지 못한다면, 1주기 동안 암호화된 데이터를 손실하게 된다. 암호통신에서 동기패턴 검출능력은 암호통신의 성능을 결정하는 중요한 요소이다. 따라서 전송보안에 사용되는 주파수 호핑에 따른 암호통신을 위한 동기신호의 오류율 정도를 살펴보고자 한다. 동기신호가 1회에 주파수 호핑 동안 전송되는 문자의 수를 P라 정의(P = 1, 2, 3, ... 문자/호핑)하고, 동기신호에서 호핑이 이루어질 확률은 평균 1~2회가 발생한다고 가정한다.

동기패턴의 앞부분의 일부는 f_0, f_1 주파수이고 뒷부분의 일부는 f_2 주파수로 전송될 때 정상적인 동기패턴을 검출하기 위해서는 f_0, f_1, f_2로 호핑되어 전송된 동기패턴이 모두 오류없이 전송되어야 정상적인 검출이 가능하다. 주파수 f_0로 호핑되어 전송되는 문자가 k개일 확률은 식 6과 같고, 이때 전송되는 문자의 개수는 P 보다 작으며 유니폼 분포를 따른다고 가정한다.

$$P(I=k)=\frac{1}{P} \qquad 0 \le k \le P-1 \qquad (6)$$

P(N)을 N개의 단말이 전송 중에 있을 때 단말간에 같은 주파수를 선택하여 충돌이 발생할 확률로 정의하면, 식7과 같다.

$$P(N)=\sum_{k=1}^{N-1}\binom{N-1}{k}\left(\frac{1}{51}\right)^{k}\left(\frac{50}{51}\right)^{N-1-k}=1-\left(\frac{50}{51}\right)^{N-1} \qquad (7)$$

따라서 N개의 단말이 동시에 전송하고 있을 때 충돌이 일어나지 않을 확률은 식8과 같다.

$$P_S(N)=\left(\frac{50}{51}\right)^{N-1} \qquad (8)$$

f_0 주파수로 호핑되어 전송되는 동기패턴의 수를 I라 정의하고, l을 $31-k$로 두면, $I=k$ 일 때 u, v, q, r를 식9~12와 같이 나타낼 수 있다.

$$u = \frac{l}{P}\ , \tag{9}$$

$$v = l - u \cdot P \tag{10}$$

$$q = \frac{31-v}{P} \tag{11}$$

$$r = (31-v) - q \cdot P \tag{12}$$

u는 f_1 주파수로 호핑되어 전송되는 동기패턴을 나타내고, v는 f_2 주파수로 호핑되어 전송되는 동기패턴을 의미한다. 주파수간 호핑 시 충돌이 발생하면 해당 주파수를 통해 전송되고 있는 문자는 모두 손실되는 것으로 가정한다. $F0$은 f_0 주파수로 전송되는 문자들 중 성공적으로 전송되는 동기패턴 수, $F1$은 f_1 주파수로 전송되는 문자들 가운데 성공적으로 전송되는 동기패턴 수, $F2$는 f_2 주파수 전송되는 문자들 중 성공적으로 전송되는 동기패턴 수, $F3$은 f_3 f_1 주파수로 전송되는 문자들 중 성공적으로 전송되는 동기패턴 수를 나타낸다.

$$[F0 \mid I=k] = \begin{cases} k & with\ probability\ of\ P_S \\ 0 & with\ probability\ of\ (1-P_S) \end{cases} \tag{13}$$

$$[F1 \mid I=k] = P \times i$$
$$with\ probability\ of \begin{pmatrix} u \\ i \end{pmatrix} (P_S)^i (1-P_S)^{u-i} \tag{14}$$

만일 P≤1이면 식15와 같이 얻을 수 있고,

$$[F2 \mid I=k] = \begin{cases} v+q & with\ probability\ of\ P_S \\ 0 & with\ probability\ of\ (1-P_S) \end{cases} \tag{15}$$

P>1이면 식16과 같이 얻을 수 있다.

$$[F2 \mid I=k] = P \times i$$
$$with\ probability\ of \begin{pmatrix} q \\ i \end{pmatrix} (P_S)^i (1-P_S)^{q-i} \tag{16}$$

또한 $F3$는 식17과 같이 나타낼 수 있다.

$$[F3 \mid I=k] = \begin{cases} r & with\ probability\ of\ P_S \\ 0 & with\ probability\ of\ (1-P_S) \end{cases} \tag{17}$$

주어진 식13~17로부터, 충돌 없이 성공적으로 전송된 동기패턴 $F1$, $F2$, $F3$에 대한 probability mass function(pmf)의 Generating Function은 식18~22와 같이 나타낼 수 있다.

$$P_S z^k + (1-P_S) \tag{18}$$

$$[P_S z^p + (1-P_S)]^u \tag{19}$$

$$P_S z^{(v+q)} + (1-P_S) \quad (\mathrm{P} \le 1\text{일 경우}) \tag{20}$$

$$[P_S z^p + (1-P_S)]^q \quad (\mathrm{P}>1\text{일 경우}) \tag{21}$$

$$P_S z^r + (1-P_S) \tag{22}$$

동기패턴은 RS(31,15) 2개의 코드워드로 구성되며, 1개의 코드워드가 반드시 충돌없이 전송되어야 정상적으로 검출이 가능하다. 따라서 구성된 RS(31,15) 코드워드의 동기패턴 가운데 주파수간 충돌 없이 성공적으로 전송된 동기패턴 수(S_H)에 대한 pmf는 식23, 24와 같이 곱의 함수로 구할 수 있다.

$$G_{S_H}(z) = \sum_{k=0}^{P-1} [P_S z^k + (1-P_S)] \cdot [P_S z^p + (1-P_S)]^u \cdot [P_S z^{u+q} + (1-P_S)] \cdot [P_s z^r + (1-P_s)] \cdot [\frac{1}{P}] \quad (\mathrm{P} \le 1\text{일 경우}) \tag{23}$$

$$G_{S_H}(z) = \sum_{k=0}^{P-1} [P_S z^k + (1-P_S)] \cdot [P_S z^p + (1-P_S)]^u \cdot [P_S z^p + (1-P_S)]^q \cdot [P_s z^r + (1-P_s)] \cdot [\frac{1}{P}] \quad (\mathrm{P}>1\text{일 경우}) \tag{24}$$

또한 라이시안 페이딩으로부터 동기패턴이 손실되지 않고 성공적으로 전송될 확률 P_f는 식5로부터 유도할 수 있다.

$$P_f = 1 - WER(\rho.K) \tag{25}$$

2개의 RS(31,15)로부터 전송되는 동기패턴은 n개의 심볼 가운데 여유마진이 m개까지 오류가 발생하여도 정상적으로 검출이 가능하므로 비트 오류환경에서 동기패턴이 검출될 확률은 식26과 같이 나타낼 수 있다.

$$P_{fm} = \sum_{i=0}^{m} {}_nC_i P_f^i (1-P_f)^{n-i} \tag{26}$$

따라서 전송되는 2개의 RS(31,15) 동기패턴 가운데 주파수 간 호핑에서 충돌이 없고 페이딩으로도 오류가 없이 정상적으로 동기패턴(S)이 검출될 개수가 n일 확률은 다음과 같이 구해 질수 있다.

$$P(S=n) = \sum_{l=n}^{62} P(S_H = l) \begin{pmatrix} l \\ n \end{pmatrix} P_{fm}^n (1-P_{fm})^{l-n} \tag{27}$$

식 27에 대한 Generating function은 다음과 같이 구해 질 수 있다.

$$[G_S(z) \mid S_H = l] = [P_{fm} z + (1-P_{fm})]^l \tag{28}$$

$$G_S(z) = \sum_{l=0}^{62} [P_{fm} z + (1-P_{fm})]^l P(S_H = l) = G_{S_H}[P_{fm} z + (1-P_{fm})] \tag{29}$$

따라서 주파수 간 충돌이 없고 페이딩으로 인한 오류도 없이 성공적으로 전송된 문자 수에 대한

pmf는 $P_{fm}z+(1-P_{fm})$를 대입하면 식30, 31을 얻을 수 있다.

$$\sum_{k=0}^{P-1} \frac{1}{P}[P_S(P_{fm}z+(1-P_{fm}))^k+(1-P_S)] \cdot [P_S(P_{fm}z+(1-P_{fm}))^p+(1-P_S)]^u \cdot [P_S(P_{fm}z+(1-P_{fm}))^{(v+q)}+(1-P_S)] \cdot [Ps(P_{fm}z+(1-P_{fm}))^r+(1-Ps)]$$

(P≤1일 경우) (30)

$$\sum_{k=0}^{P-1} \frac{1}{P}[P_S(P_{fm}z+(1-P_{fm}))^k+(1-P_S)] \cdot [P_S(P_{fm}z+(1-P_{fm}))^p+(1-P_S)]^u \cdot [P_S(P_{fm}z+(1-P_{fm}))^p+(1-P_S)]^q \cdot [Ps(P_{fm}z+(1-P_{fm}))^r+(1-Ps)]$$

(P>1일 경우) (31)

식30, 31의 결과를 전개하면 z^n항 계수는 62개 심볼로 구성되는 동기패턴 가운데 n개의 심볼이 성공적으로 전송될 확률을 의미한다. 만일 n개의 심볼이 일정 동기패턴 검출을 위해 요구되는 여유 마진을 넘어설 경우 동기검출은 실패로 판정된다. 만일 전송모드가 표준 DP방식으로 전송될 경우, 동일한 펄스가 2회 반복됨으로 확률적으로 2배의 검출능력을 제공한다고 볼 수 있으며, 식 32, 33과 같이 나타낼 수 있다.

$$2\cdot\sum_{k=0}^{P-1} \frac{1}{P}[P_S(P_{fm}z+(1-P_{fm}))^k+(1-P_S)] \cdot [P_S(P_{fm}z+(1-P_{fm}))^p+(1-P_S)]^u \cdot [P_S(P_{fm}z+(1-P_{fm}))^{(v+q)}+(1-P_S)] \cdot [Ps(P_{fm}z+(1-P_{fm}))^r+(1-Ps)]$$

(P≤1일 경우) (32)

$$2\cdot\sum_{k=0}^{P-1} \frac{1}{P}[P_S(P_{fm}z+(1-P_{fm}))^k+(1-P_S)] \cdot [P_S(P_{fm}z+(1-P_{fm}))^p+(1-P_S)]^u \cdot [P_S(P_{fm}z+(1-P_{fm}))^p+(1-P_S)]^q \cdot [Ps(P_{fm}z+(1-P_{fm}))^r+(1-Ps)]$$

(P>1일 경우) (33)

IV. 시뮬레이션 환경 및 결과

LINK16 암호통신에서 암호동기 패턴이 전송보안을 위한 주파수 호핑, 페이딩 채널에서 영향을 분석하기 위한 실험 모델을 Fig. 5에서 제시하였다. 실험환경에서 암호통신을 위해 전송되는 동기패턴이 1회 주파수 호핑을 할 때 전송되는 호핑 패턴 심볼의 수를 P, 한 비트 당 신호 에너지와 잡음간의 비율(E_b/N_o)를 ρ, LOS 경로와 다중 경로의 비를 K를 전송성능 분석을 위한 파라메타로 설정하였다. 실험모델은 암호통신을 수행

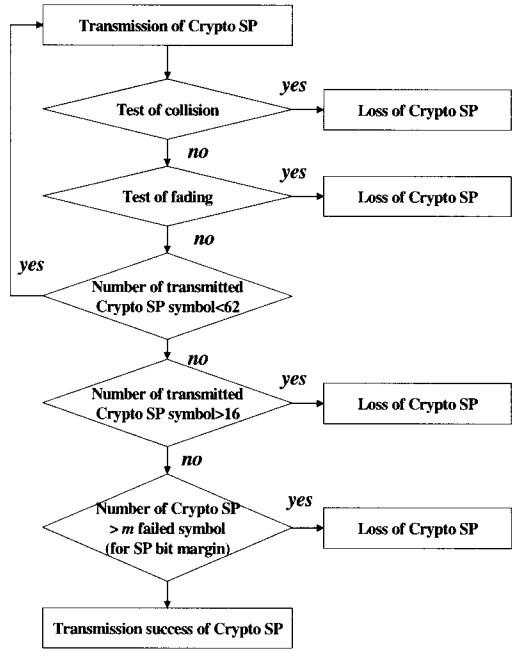

Fig. 5. Experimental model for transmission performance analysis of crypto SP

할 때 암호동기 패턴이 페이딩이 존재하는 무선 채널에서 주파수 호핑이 이루어질 때 각 가입자 단말과 암호동기 패턴에서 발생하는 심볼오류의 상관관계를 분석하였다. 가입자 단말이 1회 호핑 시에 P개의 심볼을 전송한다고 가정하고 사용중인 주파수가 다른 단말 가입자에 의해서 동시에 사용되고 있다면 해당 주파수를 통해 전송되고 있는 P개의 동기패턴 심볼은 충돌에 의해 손실된다. 암호통신을 위해 동기패턴을 전송할 때 주파수 간 충돌이 발생여부를 판단하고 P개의 심볼에 대한 페이딩 오류 영향에 따른 손실 여부를 판단하며, 워드오류율(WER)은 ρ 및 K에 따라 식5로부터 얻을 수 있다. Fig. 5에서 암호동기가 전송될 때 충돌이 일어나면 암호 동기패턴은 손실되고, 암호 동기패턴의 충돌이 일어나지 않는 페이딩 환경에서 채널 오류부호 능력에 의해 제공된 암호동기가 정상적으로 전송되었는가를 판단한다. RS 부호화에 의해 정상적으로 암호동기 패턴이 정정될 수 없을 경우 이를 암호동기 손실로 판단하며, 정상적인 RS 부호화에 의해 전송된 암호 동기패턴은 허용여유비트 이내일 경우 정상적인 암호동기를 검출한 것으로 판단하고 그렇지 않을 경우 암호동기 전송이 실패한 것으로 판단한다.

본 논문에서 암호동기패턴 전송은 주파수 호핑 과정에서 일어나는 충돌, 페이딩 오류에 의한

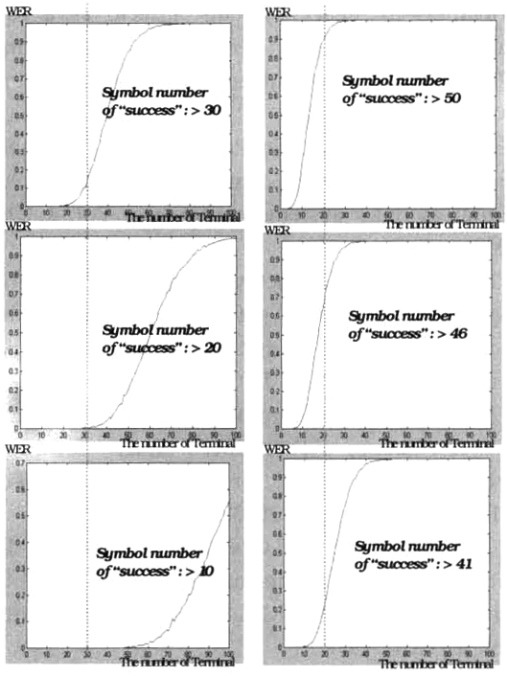

Fig. 6. The relation of the number of terminal and WER according to the number of crypto SP(p(Eb/No)=15dB, K=10dB)

실패, 채널 오류정정에서 실패와 허용 여유비트 이상의 암호 동기패턴에서 오류가 발생할 경우를 실패로 구분하여 판단하고 이에 대한 시뮬레이션을 수행하였다. 암호통신을 위해 사용된 암호동기패턴은 117비트(39비트,3회,majority voting)를 가지며 이는 2개의 RS(31,15)로 구성되고, 이때 1개의 RS(31,15)가 정상적으로 채널 오류정정이 가능하려면 8개 이하의 오류가 발생하였을 때 성공적으로 수신할 수 있으므로, 전체 동기패턴이 정상적으로 검출되기 위해서는 16개 이하의 심볼 오류가 발생하여야 한다.

만일 통신을 시도하는 가입자 단말이 적을 경우 주파수 호핑이 많을수록 낮은 심볼 비트오류율을 나타나고, LINK16에서 사용되는 통신모드에 따라 처리율이 달라진다. 가입자 단말이 사용하는 초당 주파수간 호핑 수는 이론적으로 최대 77,000번까지 가능하나 보통 2,000회 미만이며, 통신 중인 가입자 단말의 수와 전송되는 심볼 수 P간의 관계에서 P 값의 변화가 암호통신 전송성능에 영향을 미치며, 암호통신 전송성능을 보장하기 위해서는 수신신호 전력의 일정 전력레벨 이상의 유지가 요구된다. 암호 동기패턴을 전송하는 가입자 단말에 대해서 p(Eb/No) 값이 15dB, K값이 10dB로 정할 때 전송되는 암호 동기패턴의 심볼 수에 따라 가입자 단말 수와 암호 동기패턴의 심볼 오류간의 관계를 Fig. 6에서 제시하였다. 주어진 채널환경에서 SP모드로 암호 동기패턴이 주파수 호핑 충돌 없이 정상적으로 전송되기 위해 전체 62개의 심볼을 갖는 암호 동기패턴(2개의 RS(31,15))의 수가 50개 이상이 성공할 조건에서 가입자 단말 수가 매우 감소하여야 한다. 예를 들면 가입자 단말의 수 20개가 동시에 가입하고 있을 경우 심볼 오류율은 매우 높게 나타난다. 그러나 강인한 리드 솔로몬 부호화 방식, 인터리빙 기법, 추가적인 동기패턴 검출을 위한 허용 여유비트를 제공할 경우 가입자 단말의 동시 가입자 수를 증가시키고, 암호 동기패턴의 심볼 오류율을 낮출 수가 있다. 성공적인 암호 동기패턴의 심볼 수를 30개 이상을 암호 동기 전송이 성공한 것으로 판단하려면 가입자 단말 40개가 동시에 가입할 경우 심볼 오류율은 50% 정도이다. 반면 가입자 단말 수가 30개로 감소하면 암호 동기패턴의 충돌확률이 10% 수준, 단말 가입자 수가 20개로 감소하면 암호동기의 100% 전송이 보장된다. DP모드의 경우 암호동기 성능은 현재 분석된 SP모드에 비해 동일한 환경에서 2배의 암호동기 통신 성공이 보장된다. Fig. 7은

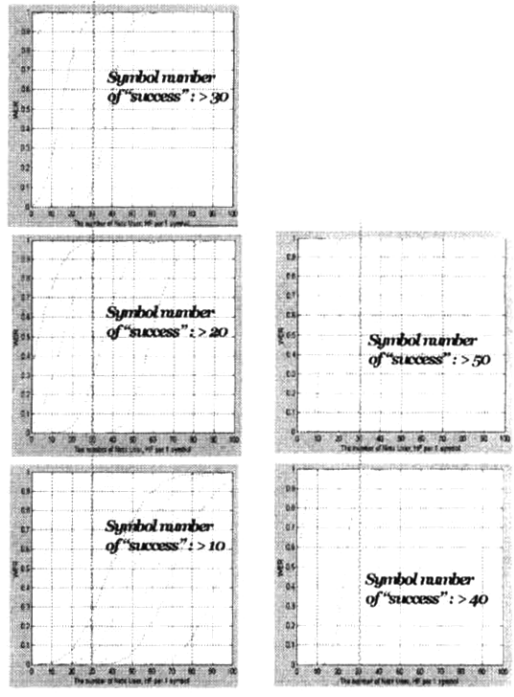

Fig. 7. The relation of the number of terminal and WER according to the number of crypto SP(according to vary K value)

페이딩 채널 K값을 고정시킨 상태에서, 단말 가입자 수와 암호 동기패턴의 심볼 오류율에 대한 관계를 나타내었는데, 신호전력의 변동에 따라 암호 동기패턴의 심볼 오류율이 영향을 받는 것을 알 수 있다. 암호동기가 30개 이상의 심볼을 검출하기 위해 30개의 가입자 단말 수가 동시 가입할 때, 수신 신호전력 변동율에 따라 암호 동기패턴의 심볼오류 변동이 크게 나타나므로 일정 수준이상의 신호전력 레벨 유지가 요구된다.

V. 결 론

LINK16은 항공과 항공간, 항공과 지상간, 항공과 함정간 실시간에 준하는 통신능력을 제공하며, 주요 정보 즉 감시 트랙, 무기 조정, 공중 제어, 디지털화된 음성 네트워크를 포함한 중요한 전술 통신 네트워크이다. 현재 LINK16은 민간망과 LINK16간의 연동 및 동합에 관한 연구가 현재 진행중에 있으나, LINK16 보안체계에 대한 연구 발표는 거의 전무하다.

본 논문에서는 LINK16 네트워크에서 암호통신을 제공할 때 주파수 호핑 및 페이딩 영향으로 암호 동기의 전송성능을 분석하였다. 본 연구결과는 향후 민간망과 LINK16의 연동 및 보안체계 구축과정에서 기초자료로 활용가능하며, 덧붙여 향후 현재 EUROCONTROL을 중심으로 활발하게 논의되고 있는 LINK16과 민간망 연동체계에서 보안체계에 대한 연구 및 효율적인 연동방안 등에 관련한 추가적인 연구가 필요하다.

참고문헌

1) 김중표, 구철회, 최재동, "정지궤도 통신위성의 CCSDS 원격명령 암호복호기 구현", 한국항공우주학회지, 제31권, 제10호, 2003년 12월.

2) 김주년, 이상래, 김성완, 임유철, 이재득, "해외발사체의 TT&C 시스템 분석", 한국항공우주학회지, 제32권, 제8호, 2004년 10월.

3) 임철호 외7인, "스마트무인기기술개발사업의 추진현황 및 향후 계획", 한국항공우주학회지 제32권, 제4호, 2004년 5월.

4) MIL-STD-6016A, "TADIL(tactical digital information link) J message standard", Feb. 1997.

5) http://www.nap.edu/openbook/0306074266/html/151.html.

6) Wilson, W. J, "Applying layering principles to legacy systems: Link16 as a case study", MICOM2001 Conference Proceeding, IEEE creating the information force, Vol. 1, Oct. 2001.

7) Farr, D. B., "Digital messaging on the comanche helicopter", Proceedings DASC, 19th, digital avionics systems conference, Vol. 1, Oct. 2000.

8) White, B. E., "Tactical data links, air traffic management, and software programmable radios", Digital Avionics Systems Conference Proceeding 18th, Vol. 1, Oct. 1991.

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

10) Davis, B. W., Graham, C., Stamm, D., "Tactical digital information link(TADIL) J range extension", MIL-COM97 Proceedings, Vol. 1, Nov. 1997.

11)http://prodevweb.prodev.usna.edu/SeaNav/NS40x/NS401_old/introduction/html/indexintro.html.

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

13) Van Til borg, H. C. A.,*An Introduction to Cryptology*, KLUWER Academic Pub., Boston, 1988.

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

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

16) William Stallings, "Wireless Communi -cations and network", Prentice Hall, pp. 110-123, 2001.

17) J. A. Roberts and J. M. Bargallo, "DPSK Performance for Indoor Wireless Rician Fading Channels", *IEEE Trans. Commun.*, Vol. COM42, pp.592-596, Feb. 1996.

18) Roberts, J.A., Abeysinghe, J.R. "A two-state Rician model for predicting indoor wireless communication perfor -mance", *IEEE Intern.* Conf., Commun. Seattle, vol.1, pp.40-43, June 1995.