JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 22, No. 1 : 202~210 Jan. 2018

T4급 링크 암호에 적합한 암호 동기방식 제안

이훈재[1*] · 김기환[2] · 강영진[2] · 이상곤[3] · 류영재[4]

A Proposal on Cryptographic Synchronization for T4 Link Encryption

HoonJae Lee[1*] · KiHwan Kim[2] · YongJin Kang[2] · Sang-Gon Lee[3] · Young-Jae Ryu[4]

[1*]Department of Information and Communication Engineering, Dongseo University, Busan 47011, Korea
[2]Department of Ubiquertous IT, Dongseo University, Busan 47011, Korea
[3]Department of Information and Communication Engineering, Dongseo University, Busan 47011, Korea
[4]ADD

요 약

현대 전장은 과학화 및 첨단화를 통해 빠른 현황 파악과 전력배치를 우선시하는 네트워크 중심 전으로 발전하고 있다. 이에 전술 데이터링크는 지속적으로 네트워크 속도 향상을 이루고 있으며, 최근 정찰용 무인기 및 각종 장비와의 무선통신을 위하여 보안 기술을 필요로 하고 있다. 또한 미래 정보전에서는 첨단 IT의 적극적인 활용이 필수적으로 요구되며, 다양한 시스템과 네트워크를 연동, 통합하기 위한 노력이 필요하다. 하지만 이러한 노력은 새롭게 변화하는 정보통신 환경에서 충분한 보안성을 전제 할 수 있어야 한다는 의미가 있다. 본 논문에서는 전술 데이터링크에 적합한 새로운 링크 암호동기방식을 제안한다. 제안한 암호 동기방식은 T4급 UAV 링크암호에 적합한 방식이며, 통신선로의 BER이 아주 낮은 경우에도 잘 견딜 수 있도록 설계하였고, 그 성능을 분석하였다.

ABSTRACT

The modern battlefield is being developed as a network-centric warfare where priority is given to rapid status grasp and power deployment through scientification and modernization. Therefore, tactical data link has been continuously improving the network speed, and recently, security technology is required for wireless communication with the UAV and various devices for reconnaissance. In addition, the future information warfare will utilize advanced IT technology positively. Efforts are needed to integrate various systems and networks. However, these efforts are meaningful only when they can assume sufficient security in a newly changing information and communication environment. In this paper, we propose a new cryptographic synchronization for link encryption suitable for tactical data links. The proposed cryptographic synchronization is useful for T4 UAV link encryption, and it is also adaptable for lower BER, then we analyze the performances analysis of that.

키워드 : 링크암호, 네트워크 중심전, 암호 시스템, 암호동기, T4 링크

Key word : link encryption, NCW, Encryption system, Cryptographic synchronization, T4 링크

Received 14 September 2017, **Revised** 19 November 2017, **Accepted** 09 January 2018

* **Corresponding Author** HoonJae Lee(E-mail:hjlee@dongseo.ac.kr, Tel:+82-51-320-1730)
Department of Information and Communication Engineering, Dongseo University, Busan 47011, Korea

Open Access http://doi.org/10.6109/jkiice.2018.22.1.202 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

과거 전장에서의 승패는 주로 전장 지휘 및 전투능력에 따라 승패가 갈렸다. 그러나 현대 전쟁에서의 승패는 전장 지휘 및 전투능력도 중요하지만, 얼마나 상대의 정보를 아느냐에 따라 승패가 좌우된다. 따라서 빠른 현황 파악과 전력배치를 위하여 네트워크 중심전(NCW: Network Centric Warfare)이 필수 요소로 자리잡고 있다[1,2]. 네트워크 중심전은 대량파괴 및 대량살상이 없이도 조기에 승리가 가능한 통합 합동전장을 목표로 변화되고 있다.

네트워크 중심전은 다양한 전력 요소들의 상호 유기적인 네트워크 환경을 보장하기 위한 목표를 가지고 있다. 첨단 IT 기술의 적극적인 활용으로 인해 다양한 시스템과 네트워크가 연동 및 통합되는 것은 빠른 의사소통 수단으로 활용될 수 있지만 반대로 정보가 누출되는 수단이 될 수 있다. 따라서 내부 네트워크에서 정보가 새어 나가지 않도록 보안할 필요가 있다.

현재 사용되고 있는 전술 데이터링크는 표적 정보, 교전 지시 명령 등과 같이 적은 양의 데이터와 짧은 지연시간 및 보안이 요구되지만, 감시 및 정찰 정보와 같이 영상정보를 다루는 데이터링크의 경우 수백 Mbps의 전송 속도와 넓은 주파수 대역을 필요로 한다. 대표적으로 무인정찰기와 공중 네트워크를 활용하는 항공기가 있다[3]. 무인정찰기의 경우 정찰에 필요한 장비를 탑재하여 목표지점 상공에서 촬영한 영상을 기지에 송신하는 목표를 주로 담당하고 있으며, 이러한 목표를 달성하기 위해서는 기존보다 더 고속전송을 위한 새로운 데이터링크가 필요하다.

드론(Drone)이나 무인항공기 UAV(Unmanned Aerial Vehicle)와 같은 공중네트워크에서는 T3급(약 45Mbps)으로 사용하고 있는 장비들이 존재하고 있지만[4,5], 새로운 기술(무인정찰기, 공중 네트워크 등)을 도입하기 위해서는 적합하지 않기 때문에 더 높은 속도를 가진 새로운 고속 데이터링크인 T4급(약 274Mbps)을 적용해야 한다. 현재 T4급 장비를 개발하기 위하여 많은 연구를 진행하고 있다[6,7].

본 논문에서는 이미지 및 영상 데이터를 T4급 환경에서 데이터 링크 계층을 보안하기 위하여 프리엠블을 이용한 암호동기 방법과 HDLC Flag를 이용한 암호동기 방법을 제안 한다.

Ⅱ. T4 링크 암호화 방식 제안

T3의 속도는 45Mpbs정도이며, 이를 활용해 다중플랫폼 영상정보 및 공용데이터링크를 구성하여 사용한다. 앞으로 감시 정찰분야에서 중요한 역할을 하는 드론이나 UAV의 경우 실시간으로 대용량의 데이터(영상 및 정보)전송을 요구하기 때문에 이에 따른 전송 속도 및 넓은 주파수 대역이 필요하다. 따라서 새로운 고속 데이터링크인 T4(274Mbps)의 도입이 필요하다.

국제 암호표준에서 언급한 링크암호는 그림 1과 같이 영상부호장치 코덱(CODEC)과 T4급 모뎀 사이에 연결되고 코덱 장비로부터 영상신호를 전달 받아서 2계층 프레임 데이터에 결합된다[8]. 그림 1에서 보여준 암호단계(Phase)는 1단계(Phase I)에서 ID-기반 키 분배 및 인증을 거쳐서, 2단계(Phase II)인 링크 암호화로 이어지는데[9], 본 논문에서는 2단계에 대해서만 다루기로 한다.

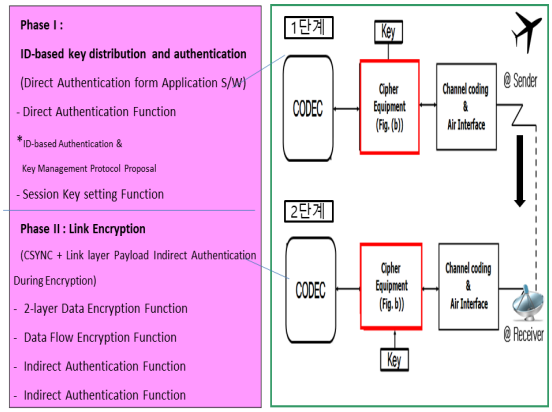


Fig. 1 A link encryption configuration and crypto system / crypto module location.

그림 2는 그림1의 암호장비(Cipher Equipment)부분을 세부 설계한 암호 시스템 구조를 보여주고 있으며, 각 블록의 역할은 다음과 같다.

블록 (1)은 코덱 인터페이스 및 프레임동기 신호 검출부(CODEC Interface and House Keeping: FEDET : Frame Error Detection)이다. 프레임동기신호 검출부(House Keeping)에서는 송신에서 암호화하여 발송한 HDLC 프레임의 플래그(Flag) 신호를 찾아서 암호동기가 정상적으로 작동되는지 아니면, 암호동기의 오류가

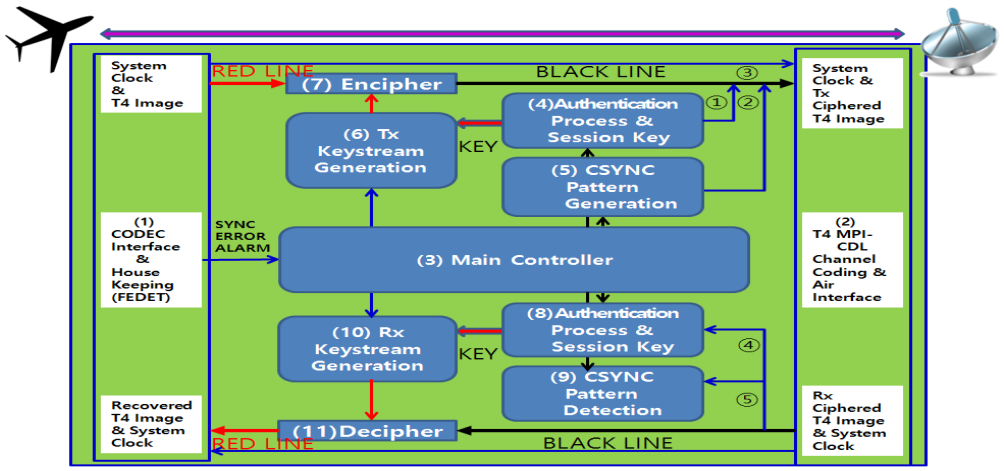


Fig. 2 Cryptographic system design(Cryptographic module).

발생되었는지를 확인할 수 있다. 만약, 이 모듈이 없을 경우 외부의 코덱 장치에서 프레임동기 오류가 검출되면, "SYNC ERROR ALARM"을 보안장비에 실시간으로 알려주어야 한다.

블록 (2)는 T4급 모뎀인 채널 코딩 및 공중망 인터페이스(T4 MPI-CDL Channel Coding and Air Interface)를 말하며, 모뎀회로에서는 274 Mbps급을 위한 LDPC (Low-Density Parity Checker) 오류정정기술이 적용되었다. 송신부에서는 영상데이터를 보안장비(암호모듈)에서 암호화하여 다른 T4급 모뎀으로 송신한다[10,11]. 이후 송신 받은 암호화정보를 보안장비(암호모듈)의 수신부로 전송하여 복호화 할 수 있도록 인터페이스를 제공하고 있다.

블록 (3)은 보안장비(암호모듈)를 전체 제어할 수 있는 주 제어장치(Main Controller)의 기능을 갖는다. 보안장비(암호모듈)의 인증 및 키 관리를 주관하고, 동기패턴을 수신부에 발송하게 지시하며, 또한 수신된 동기패턴을 검출하도록 명령하고, 암·복호 기능 전체를 제어하는 부분이다.

블록 (4)와 (8)은 인증과정 및 키 관리(Authentication Process & Session Key)를 담당하는 부분으로, 보안장비(암호모듈) 프로세서와 데이터에 대한 인증기능뿐만 아니라 장비를 사용하려는 사용자에 대하여 인증을 수행한다. 또한 세션키의 생성 및 관리 기능을 수행하는 부분이다. 블록 (5)는 160/192/224/256비트 크기의 암호동기 패턴을 발생하는 동기 패턴 발생기(CSYNC, Crypto-synchronization, pattern generator)로서 블록(9) 수신부의 동기 패턴 수신기(CSYNC Pattern Detection)와 상호 연동된다.

블록 (6)과 (10)은 고비도 특성의 송·수신 암호 알고리즘에 의한 키 수열 발생기로서 SEED, ARIA, AES 등과 같은 블록암호를 이용할 경우에는 OFB 모드로 전환하여 적용이 되거나, 스트림 암호로 적용된다. 위와 같이 블록암호의 OFB모드를 적용하거나 스트림 암호의 키 수열 발생기(Key stream Generator)로 적용되어야 하는 이유는 무선통신망에서 오류확산방지를 위함이다[12,13].

블록 (7)과 (11)는 송·수신 암호화/복호화 연산(XOR)을 수행하는 기능이다. 무선통신에서 오류확산을 방지하기 위해서는 블록암호를 적용할 수 없으며, 블록암호를 OFB 모드로 변환하여 스트림암호로 적용하여야 한다.

Ⅲ. 암호동기 방식 알고리즘 설계

본 논문에서 제안하는 암호동기 방식의 설계에서는 다음과 같은 사항을 고려하여 적용한다.

(1) 암호동기패턴인 CSYNC(Crypto-SYNC)의 패턴 길이는 160/192/224/256비트 패턴이 가능하다.

(2) 송·수신시 암호 지연은 최대 0.5초 이내로 한정한다. 설계 시스템에서는 인증 및 키 관리를 제외하고

이전 단계에서 세션키 합의 및 상호인증 완료시로 제한한 상태에서 수식 1과 같이 예상된다. 이때, CSYNC 송신에 사용되는 길이는 가변적으로 160~256비트로 나타낼 수 있다. 초기화(IV) 코드는 256비트이며, 총 7회 반복함으로서 수신에서 다수결 논리로 채널오류를 보정토록 설계한다. 초기화 소요시간은 최대 256비트를 처리하는 시간으로 가정하였으며, 이를 T4급 속도(274Mbps)로 나누었을 때 8.41 us 소요 예상된다.

$$\frac{CSYNC+IV*7\times pattern+IVloss\,time}{T4\,speed}=\frac{(128\sim256)+(256*7)+(\leq 256)}{274Mbps}=8.41us \quad (1)$$

(3) 암호 동기부 구성

동기패턴은 송신단에서 동기패턴 발생기, 수신단에서의 동기패턴 검출기와 프레임동기 에러 검출로 구성된다. 실제 적용에 있어서는 프리엠블(Preemble) 신호가 T4급 모뎀에 독립되어 있기 때문에 이 신호를 암호동기에 적용할 수가 없는 경우가 많지만, 영상장비(CODEC), 암호모듈(Cipher), 모뎀(Modem)이 통합된 장비의 경우에는 프리엠블 신호를 활용하여 암호장비의 동기를 추출할 수 있게 된다.

3.1. 프리엠블을 이용한 암호동기 : 모뎀과 보안장비가 통합된 경우

그림 3은 프레임에서 프리엠블(Preamble 1,2)을 이용한 암호화 동기 방법을 설계하고 있다. 단 이 기술은 보안장비의 암호 모듈에서 프리엠블 신호를 활용할 수 있을 경우에 제한적으로 적용 될 수 있다.

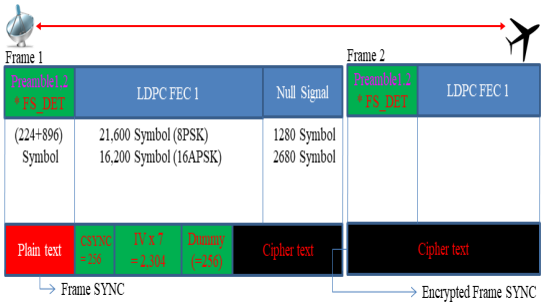


Fig. 3 Encryption synchronization method using preamble on Frame.

프리엠블을 이용한 프레임 동기 확인을 위하여 아래와 같이 동작한다.

초기 동기 시작 시 또는 동기에러 시(out-of-sync)에는 평문상태로 송, 수신 장비가 통신이 되고 있음을 확인할 수 있다.

정상적인 통신 상태에서 보안장비를 암호모드로 전환하여 프리엠블을 포함한 전체 데이터를 암호화 시킨다. 이때 보안장비에서는 CSYNC(Crypto-SYNC)를 출력하여 보안 장비 간에 정상 동기(In-Sync) 상태를 유지한 후, 이 후에 모든 데이터를 암호화시킨다.

송신단은 첫 번째 프레임에서 암호동기(CSYNC)+초기값+더미신호를 맨 먼저 전송하고, 다음 비트부터는 벌크 암호처럼 모든 데이터를 암호화 하여 보낸다. 이때 프리앰블(Preamble1,2)도 모두 암호화 되어 전송된다.

Preamble+Preamble2(224+896=1,120심볼x3비트/심볼=3,360비트)을 통하여 에러 유연성을 갖고 암호동기 이탈여부를 확인할 수 있는 House-Keeping (FS_DET)을 작동한다. 수신에서는 암호동기(CSYNC)신호를 검출한 시점부터 초기값을 복호하고, 이를 이용하여 키수열을 발생하며, 암호문에 대한 복호화를 시작한다.

House-Keeping(FS_DET)에서는 프리엠블의 3개 연속 오류가 검출될 경우에 보안장비의 프레임동기 오류로 판정하고 "SYNC-Error-Alarm"을 발송한다. 프리엠블의 1개 연속 오류이거나 2개 연속 오류일 경우에는 다음번의 프리엠블이 정상적으로 들어오는지 확인하여 3개 연속 오류가 발생할 때에만 비로소 보안장비 프레임 동기 오류로 판정하게 된다. (프레임 동기 에러 "SYNC-Error-Alarm"이 검출되면, 보안장비는 CSYNC 신호와 IV 신호를 보내어서 재동기를 진행한다.)

복호화 데이터에서부터 프리앰블 신호(Preamble1,2)를 확인하여, 연속적인 3개의 프리앰블 신호가 오류인지, 아닌지 검출한다. 3개 프레임 연속 오류가 될 경우에는 보안장비 암호동기 실패(Fail)로 판정하여 재동기 신호를 다시 송신한다.

3.2. HDLC 플래그를 이용한 암호동기 : 모뎀과 보안장비가 분리된 경우

그림 4는 HDLC 플래그를 이용한 암호동기 방법을 제시하며, HDLC 플래그를 이용한 암호동기 방법은 아

래와 같다.

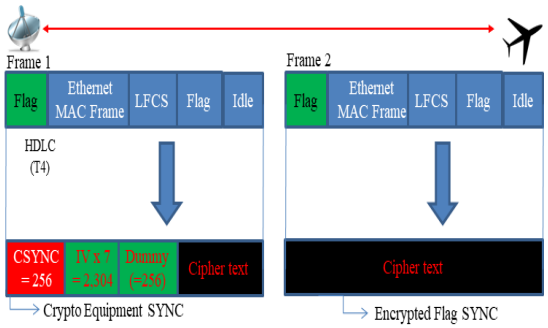


Fig. 4 Encryption synchronization(Tx) using flag signal of HDLC frame.

초기 동기 시작 시 또는 동기 에러시(out-of-sync)에는 평문상태로 송·수신 장비가 통신이 되고 있음을 확인한 후 정상적인 통신 상태에서 보안장비를 암호모드로 전환하여 HDLC 플래그를 포함한 전체 데이터를 암호화 시킨다. 이때 보안장비에서는 CSYNC를 출력하여 보안 장비간에 정상 동기(In-Sync) 상태를 유지한 후, 이 후에 모든 데이터를 암호화시킨다.

송신에서는 첫 번째 프레임에서 암호동기(CSYNC)+초기값+더미신호를 맨 먼저 전송하고, 다음 비트부터는 벌크 암호처럼 모든 데이터를 암호화 하여 보낸다. 이때 플래그(Flag)도 모두 암호화 되어 전송된다.

HDLC 플래그를 에러 유연성을 갖고 암호동기 이탈 여부를 확인할 수 있는 House-Keeping(FS_DET)을 작동한다. 수신에서는 암호동기(CSYNC)신호를 검출한 시점부터 초기값을 복호하고, 이를 이용하여 키수열을 발생하며, 암호문에 대한 복호화를 시작한다.

House-Keeping(FS_DET)에서는 HDLC 플래그의 3개 연속 오류가 검출될 경우에 보안장비의 프레임동기 오류로 판정하고 "SYNC-Error-Alarm"을 발송한다. HDLC 플래그의 1개 연속 오류이거나 2개 연속 오류일 경우에는 다음번의 HDLC 플래그가 정상적으로 들어오는지 확인하여 3개 연속 오류가 발생할 때에만 비로소 보안장비 프레임 동기 오류로 판정하게 된다. 이때, 프레임 동기 에러 "SYNC-Error-Alarm"이 검출되면, 보안장비는 CSYNC 신호와 IV 신호를 보내어서 재동기를 진행한다.

복호화 데이터에서부터 프레임 신호(Flag)를 확인하여, 연속적인 3개의 프레임 플래그가 오류인지, 아닌지 검출한다. 3개 프레임 연속 오류가 될 경우에는 보안장비 암호동기 실패(Fail)로 판정하여 재동기 신호를 다시 송신한다.

그림 4에서는 HDLC 프레임의 플래그를 이용한 암호동기 방식을 보여주고 있다. 그림 4에서는 송신 보안장비(Tx)의 HDLC 플래그를 이용하여 암호화 시키는 방법을 보여준다. 암호 장비의 동기를 위하여 256비트 CSYNC와 키 수열 발생기의 256비트 초기값(IV, Initial Value)을 7회 반복하는 오류정정부호(repetition coding)신호, 그리고 송·수신 키 수열 발생기(Tx/Rx Keystream Generation)의 정상적인 초기화 시간 동안에 전송하는 랜덤한 256비트 더미값(Dummy)을 주고받은 보안장비는 정상적인 암호문을 출력하게 된다. 이후부터는 모든 HDLC 플래그와 프레임 데이터를 모두 암호화시켜서 전송하게 된다.

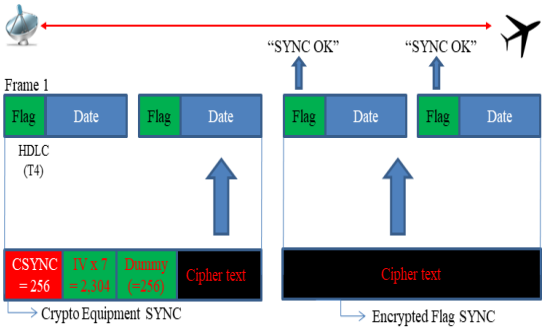


Fig. 5 When frame synchronization of Rx receiving equipment is normal.

그림 5에서는 수신 보안장비(Rx)에서의 HDLC 플래그를 이용한 프레임 동기 탐색방법을 보여주고 있다. 보안장비에서 CSYNC + IV(7회 repetition) + DUMMY를 정상적으로 수신하여 키 수열 발생기가 초기화되고(물론 이때 세션 비밀키에 의하여 암호 초기화 과정이 진행됨), 정상적인 키 수열 발생이 시작되면 HDLC 플래그를 정상적으로 복호해낼 수 있게 된다. 수신 프레임 동기반(House-Keeping, FS_DET)에서는 HDLC 플래그를 지속적으로 확인하면서 프레임 동기가 정상 상태("SYNC OK")임을 확인하게 된다. 즉, 보안장비의 암호동기가 잘 맞고 있음을 확인하게 된다.

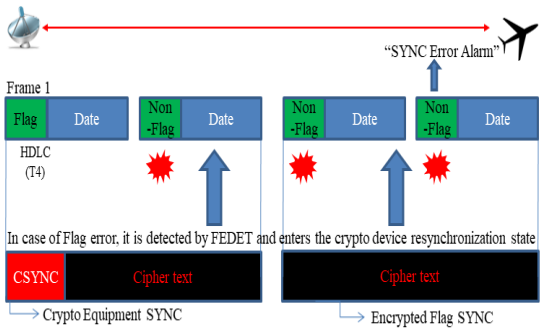


Fig. 6 When frame synchronization of Rx receiving equipment is in error state.

만일 그림 6과 같이 여러 가지 환경에 의하여 프레임 동기가 맞지 않을 경우에는 보안장비에서 자체적으로 이를 감지해낼 수 있어야 하는데, 본 연구에서는 수신 프레임 동기반(House-Keeping, FS_DET)에서 이를 확인하기 위하여 HDLC 플래그의 연속 3개 오류가 발생되면 암호동기 오류 상태(SYNC-ERROR-ALARM)임을 판단할 수 있도록 설계하였다. 이를 수신한 보안장비의 주제어 장치(Main Controller)에서는 즉시 암호 재동기 절차로 전환하여 CSYNC+IV(7회 repetition)+DUMMY 신호를 다시 전송하게 된다. 수신에서는 CSYNC를 검출하고 키 수열 발생기를 다시 작동시키는 재초기화 과정을 거쳐서 정상적인 암·복호화 단계에 이를 수 있게 된다.

3.3. 성능분석

본 논문에서 제안한 링크 암호의 동기 코드를 160~256비트까지 32비트 단위로 늘려가면서 각각의 성능을 분석하였다.

CSYNC신호에 대하여 송신된 동기 신호가 수신에서 정확히 검출해내는 검출 확률(detection probability) PD, 동기 신호를 놓치게 되는 미검출 확률(missing probability) PM, 랜덤하게 수신된 데이터로부터 동기 신호를 오판하여 잘못 검출해 내는 오검출 확률(false detection probability) PF, 그리고 오검출 (평균)시간 TF 등이 동기 검출기의 주요 성능을 나타내는 값이다. 검출 window N, 채널 비트 오류율 B, 전송속도 R bps하에서 N비트 동기 신호 송출시 문턱 값 NT($0 \le NT \le N$)에 따라 이들 동기 확률을 계산 한다. 즉, 수신되는 신호는 랜덤 특성이 좋은 암호문으로 "0"과 "1" 균일 분포를 가지며, 전송로의 BER이 B에서 1 비트를 한번 전송할 때 틀릴 수 있는 확률이 B이고 옳을 수 있는 확률은 1-B가 된다. 만약 N 비트로 구성된 동기 신호를 전송하면 전송로의 BER에 의해서 수신단에서는 0에서 N까지 에러가 발생될 수 있으며, 에러 개수 i 에 대한 동기검출 확률밀도함수 pDi와 동기 검출 확률 PD, 그리고 미검출 확률 PM은 다음과 같다.

$$p_{Di} = {}_NC_i\, B^i\, (1-B)^{N-i},\ i=0,1,\ldots,N \quad (1)$$

$$P_D = \sum_{i=0}^{N_T} p_{Di} = \sum_{i=0}^{N_T} ({}_NC_i\, B^i\, (1-B)^{N-i}) \quad (2)$$

$$P_M = 1-P_D \quad (3)$$

한편 동기 신호를 전송하지 않아도 채널에서의 랜덤 잡음에 의해서 동기신호는 검출될 수 있으므로 이를 오검출(false detection)이라 하며, 에러 수 i 에 대한 오검출 확률 밀도 함수 pFi와 오검출 확률 PF, 그리고 평균 오검출 시간 TF는 아래와 같다.

$$p_{Fi} = {}_NC_i\, 0.5^i\, (1-0.5)^{N-i} = {}_NC_i\, 2^{-N} \quad (4)$$

$$P_F = 2^{-N} \sum_{i=0}^{N_T} {}_NC_i \quad (5)$$

$$T_F = \frac{1}{P_F \cdot R} \quad (6)$$

이와 같은 자료를 바탕으로 표 1은 160비트에서 256비트까지 파라메터에 따라서 정의된 암호시스템 동기 확율을 시뮬레이션한 결과이다.

실험환경에 사용된 컴퓨터는 i5-2500, 8GB RAM, Windows10을 사용하였으며, 분석을 위해 사용된 툴은 Visual Studio 2015 이다.

(1) 160비트 CSYNC를 Nt=30, BER=10-1을 선택할 때 동기신호의 검출확률(PD)은 0.999보다 크고 우려되는 오검출확율(PFA)은 $0.243*10^{-15}$보다 작게되며, 오검출평균시간(TFA)은 약 173.83일로 계산되어 안전하다.

(2) 192-비트 CSYNC를 Nt=38, BER=10-1을 선택할 때 동기신호의 검출확률은 0.9999보다 크고 우려되는 오검출확율은 $0.462*10^{-17}$보다 작고 오검출평균

시간은 약 25년으로 안전하다.

(3) 224-비트 CSYNC를 Nt=48, BER=10-1을 선택할 때 동기신호의 검출확률은 0.999999보다 크고 우려되는 오검출확율은 $0.12*10^{-17}$보다 작고 오검출평균시간 약 96.4년으로 안전하다.

(4) 256-비트 CSYNC를 Nt=58, BER=10-1을 선택할 때 동기신호의 검출확률은 0.999999999보다 크고 우려되는 오검출확율은 $0.223*10^{-18}$보다 작고 오검출평균시간은 약 516년으로 안전하다.

Table. 1 Comparison of CSYNC detection probability, miss probability, false-detection probability

bits	P_{FA}	P_D	P_M
160	0.2430807677813 6381536D-15	0.9997443879970 1859093D+00	0.2556120029814 0906995D-03
192	0.4620836290099 5583032D-17	0.9999851712039 3515256D+00	0.1482879606484 7438174D-04
224	0.1155410806758 6362911D-17	0.9999998696459 0115157D+00	0.1303540988484 2863448D-06
256	0.2236627445132 1557792D-18	0.9999999990645 6937814D+00	0.9354306218511 9651980D-09

Ⅳ. 결 론

본 논문에서는 전술 데이터링크에 적합한 새로운 링크 암호동기방식을 제안하였다. 제안 방식은 T4급 UAV 링크암호에 적합한 방식이며, 통신선로의 BER이 아주 낮은 경우에도 잘 견딜 수 있도록 설계되었고, 그 성능을 분석하였다.

성능분석은 160/192/224/256비트를 시뮬레이션 하여 결과 값을 통해 분석하였으며, 동기신호의 검출확률(0.999~0.999999999)과 오검출확률($0.243*10^{-15}$~$0.223*10^{-18}$)의 결과 값을 통해 160/192/224/256비트다 안전한 결과가 나왔다. 하지만 오검출평균시간을 볼 때 160비트(173.83일), 192비트(25년), 224비트(94.6년), 256비트(516년) 각 비트별로 차이가 있음을 확인할 수 있었다.

이전 연구[14,15]에서는 스트림 암호화 시스템을 제안하고 있다. 이 연구에서도 다양한 비트(Ping Pong 128/192/256)의 암호동기방식을 적용시켰지만, 속도는 T1급(약 1.544Mbps)라는 제한이 있다.

본 논문에서 제안한 암호동기방식은 다양한 채널 환경에 맞출 수 있도록 CSYNC 값을 160~256비트로 설계하였으며, 설계된 CSYNC 패턴은 그 길이에 따라 다르게 표현하였다. 또한 무선 노이즈 환경(BER)에 따른 오검출 확률(False-detection) 및 보안장비 생명주기(life-cycle) 등을 고려하여, 256비트 CSYNC 값을 선택하는 것이 가장 좋은 방법이라 판단된다. 또한 제안한 암호동기를 활용하여 T3급보다 6배 이상 고속화된 T4급 암호 동기가 가능하며, 영상정보가 고화질로 전송할 수 있어 정밀도가 높은 고속 암호시스템에 적용될 수 있다.

ACKNOWLEDGEMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (NRF-2016R1D1A1B01011908). And it also supported by ADD project.

REFERENCES

[1] P. T. Mitchell, *Network Centric Warfare: Coalition operations in the age of US military primacy*, 1th ed. New York, NY: Routledge, 2013.

[2] D. S. Alberts and R.E. Hayes, *Power to the Edge: Command and Control in the Information Age*, 1th ed. Washington DC, WA: CCRP Publication Series, 2003.

[3] G. C. Wang, B. S. Lee, K. J. Lim and J. Y. Ahn, “Technical Trends on Security of Control and Non-payload Communications Network for Unmanned Aircraft Systems,” *International Journal of Electronics and Telecommunications Research Institute*, vol. 32, no. 1, pp. 82-92, Feb. 2017.

[4] Weatherington, Dyke, and U. Deputy, "Unmanned aircraft systems roadmap, 2005-2030." United States, Office of the Secretary of Defense, Technical Report, 2005.

[5] J. M. Chung, K. C. Park, T. Y. Won, U. H. Oh, D. C. Ko, S. J. Hong, C. B. Yoon, H. Kim and U. Y. Pak,

"Standardization Strategy for the Image and Intelligence Common Datalink," *International Journal of the Korean Information and Communication Magazine*, vol. 28, no. 4, pp.41-50, Apr. 2011.

[6] E. Burak, E. C. A. Nail, T. Craig and M. Ken, "A 275 Gbps AES encryption accelerator using ROM-based S-boxes in 65nm," in *Proceeding of the Custom Integrated Circuits Conference*, California: CA, pp. 1-4, 2015.

[7] Y. J. Ryu and J. M. Ahn, "Research on Performance Analysis for the Long Distance Air-Ground Wideband Common Data Link," *International Journal of Korean Institute of Communications and Information Sciences*, vol. 42, no. 04, pp. 703-715, Apr. 2017.

[8] F. H. Myers, "A Data Link Encryption System," in *Proceeding of National Telecommunications Conference*, Washington: WA, pp. 27-29, 1979.

[9] D. H. Lim, S. J. Lee, "Public Key Authentication using Secret Sharing and ECC for Tactical Communication Networks," *Journal of Security Engineering*, vol. 13, no. 6 pp. 421-438, Dec. 2016.

[10] D. J. C. MacKay, *Information theory, Inference and Learning Algorithms*, 1th ed. Cambridge, CBG: Cambridge University Press, 2003.

[11] T. K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms*, 1th ed. New Jersey, NY : John Wiley & Sons, 2005.

[12] N. Bruce, Y. S. Lee, W. T. Jang and H. J. Lee, "Next Generation Encryption of Enhanced Light-weight Stream Cipher for Communication Systems," *International Journal of Wireless Devices and Engineering*, vol. 1, no. 1, pp. 27-32, 2017.

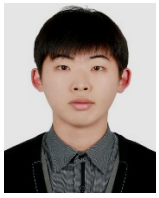
[13] A. Kahate, *Cryptography and network security*, 3th ed, New Delhi, IN: Tata McGraw-Hill Education, 2013.

[14] H. J. Lee, I. S. Ko (Franz Ko), "An Intelligent Security Agent for Reliable Cipher System using PingPong," *Cybernetics and Systems*, vol. 39, no. 7, pp.705-718, Oct. 2008.

[15] H. R. Kim, H. J. Lee, D. H. Kwon, U. Y. Pak, "A SES Alarmed Link Encryption Synchronization Method for High-speed Video Data Encryption," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 17, no. 12, pp.2891-2898, Dec. 2013.

이훈재(HoonJae Lee)

1985년 경북대학교 전자공학과 졸업(학사)
1987년 경북대학교 전자공학과 졸업(석사)
1998년 경북대학교 전자공학과 졸업(박사)
1987년 ~ 1998년 국방과학연구소 선임연구원/팀장
1998년 ~ 2002년 경운대학교 조교수
2002년 ~ 현재 동서대학교 컴퓨터정보공학부 교수
※관심분야 : 암호이론, 네트워크보안, 부채널공격, 정보통신/정보네트워크



김기환(KiHwan Kim)

2015년 동서대학교 정보통신공학과 졸업(학사)
2017년 동서대학교 유비쿼터스IT학과 졸업(석사)
2017년 ~ 현재 동서대학교 유비쿼터스IT학과 박사과정
※관심분야 : 암호이론, 네트워크 보안, 인공지능

강영진(YongJin King)

2013년 동서대학교 정보통신학과 졸업(학사)
2015년 동서대학교 유비쿼터스IT학과 졸업(석사)
2015년 ~ 현재 동서대학교 유비쿼터스IT학과 박사과정
※관심분야 : 부채널공격, 네트워크 보안

이상곤(Sang-Gon Lee)

1986년 경북대학교 전자공학과 졸업(학사)
1988년 경북대학교 전자공학과 졸업(석사)
1993년 경북대학교 전자공학과 졸업(박사)
1991년 ~ 1997년 창신대학교 전자통신학과 조교수
1997년 ~ 현재 동서대학교 컴퓨터공학부 교수
※관심분야 : 암호이론, 암호프로토콜 및 네트워크 응용, 소프트웨어정의 네트워크, 블록체인

류영재(Young-Jae Ryu)

2000년 2월: 경북대학교 전자 전기공학부 졸업
2002년 2월: 경북대학교 전자 공학과 석사
2017년 8월: 충남대학교 전파 정보통신공학과 박사
2002년~현재 : 국방과학연구소 선임연구원
※관심분야 : 영상정보용 데이터링크, 디지털 통신신호처리