Journal of The Korea Society of Computer and Information
Vol. 22 No. 9, pp. 57-64, September 2017

www.ksci.re.kr
https://doi.org/10.9708/jksci.2017.22.09.057

A SES Alarmed Link Encryption Synchronization Method Having Optimized Threshold Value for High-Speed Video Data Encryption

Hyeong-Rag Kim*, Hoon-Jae Lee**, Ki-Hwan Kim***, Ju-Hyun Jung****

Abstract

CCSDS Standard is widely used in the international space telecommunication area. But standard recommendation of CCSDS is not restrictive, so, we can select an appropriate encryption protocol among the layer. For synchronization, encryption sync is attached in the beginning of the encrypted data. In the exceptional environmental condition, although the receiver can not decrypt the normal data, the sender have no conception of that situation.

In this paper, we propose a two-stage SES alarmed link encryption synchronization method having optimized threshold value necessary to decide whether the receiver has a correct decryption or not. first, through the experiment of mutual relations between error rate and encryption synchronization detection error, we can predict worst communication environment for the selected encryption synchronization pattern. second, through the experiment for finding what number of consecutive frame synchronization error is an appropriate reference value and analysis of that experiment, we suggest an optimized threshold value for resynchronization request. lastly, through the output images we can predict the probability error that should be guaranteed by channel coder.

▸Keyword: CCSDS, Link encryption, Encryption sync, SES Alarm

I. Introduction

우주 데이터 시스템 자문 위원회(Consultative Committee for Space Data Systems, CCSDS)가 우주 관련 정보의 상호 교환을 촉진할 목적으로 1982년 설립된 후 발표한 CCSDS의 패킷에 대한 표준 규격은 국제 우주 통신 분야에서 하나의 규격으로 폭넓게 사용되고 있다. CCSDS의 표준 권고안에는 우주 통신연결을 통해 송수신 되는 다양한 전송 기법이나 우주 통신 링크 프로토콜, OSI 참조 모델에 적합한 계층화된 모델들을 제시하고 있다[1-3]. CCSDS의 표준권고안은 구속력을 갖지 않으므로 암·복호화 및 무결성 알고리즘의 선택에는 제약이 없어서 CCSDS의 프로토콜 암호화는 계층별로 고유의 암호 프로토콜을 수행해 통신 채널에서 보안 요구사항을 만족하도록 하고 있다. 이때 여러 계층에서 수행하는 암호화 중에서 링크 암호화를 적용하면, 링크 암호화에 사용하는 장비가 데이터 동기화를 위해서 암호화 된 데이터의 시작부에 암호화 동기를 삽입하게 된다[4-6].

송수신 초기단계에서 암호화 동기가 이루어지면 수신부의 암호화 장비는 지속적으로 복호화를 수행하여 데이터를 수신하게 된다. 그런데 타이밍 지터링 등에 의한 비트 슬립이나 전원의 불안전성 등으로 인해 시스템이 비정상적으로 종료 되거나 채널의 불완전성으로 인해 문제가 발생하면 수신 장비는 데이터를 수신하더라도 암호화된 데이터의 복호화가 불가능하게 되어 정상적인 데이터 복원을 할 수 없게 된다[7-9]. 이를 개선하기 위하여 여러 가지

• First Author: Hyeong-Rag Kim, Corresponding Author: Hoon-Jae Lee
*Hyeong-Rag Kim (hrkim@pohang.ac.kr), Dept. of IT&Electronics, Pohang University
**Hoon-Jae Lee (hjlee@dongseo.ac.kr), Div. of Computer Engineering, Dongseo University
***Ki-Hwan Kim (ghksdl90@naver.com), Div. of Computer Engineering, Dongseo University
****Ju-Hyun Jung (jhyun@add.re.kr),ADD
• Received: 2017. 08. 18, Revised: 2017. 08. 25, Accepted: 2017. 09. 05.
• This work was supported by ADD.

원인들로 인해 송수신 도중에 문제가 발생할 경우 송신측에 Alarm 신호를 전송하여 정상적인 송수신이 이루어지도록 하는 링크 암호 동기 방식이 제시되기도 하였다[10].

본 논문에서는 수신측의 오류 확률이 허용범위를 벗어나 정상적인 데이터의 복원이 불가능한지 여부에 대한 판단을 두 단계로 진행하여 송신측으로 재동기 요청을 할 수 있게 하는 최적의 SES Alarmed 링크암호 동기 방식을 제안한다. 첫 번째 단계에서는 수신측에서 암호화 동기를 검출하지 못하여 송신측으로 재동기 요구를 하게 될 때 오류 확률과 암호동기 오류로 인한 재동기 요구 횟수 간 상호 관계의 실험을 통해 선택된 암호화 동기 패턴이 사용될 수 있는 최악의 통신 환경을 예측할 수 있게 한다. 두 번째 단계에서는 복호화 된 프레임 데이터의 프레임 동기 검출과정에서 연속된 프레임 동기 오류가 발생할 때 송신측으로 재동기 요구를 하기 위한 기준값을 오류 확률에 따라 몇 회의 연속 프레임 동기 오류로 설정하는 것이 가장 적정한 값인가를 찾는 실험을 통해 최적의 문턱값을 찾아내고 그 결과를 분석한다. 마지막으로 오류확률에 따른 최종 출력 결과를 통해 송수신 시스템 설계 시 채널코더에서 보장해야 할 오류확률을 예측할 수 있게 한다.

II. CCSDS Protocol and Link Encryption Synchronization Method

1. CCSDS Protocol and Security Structure

CCSDS의 프로토콜의 구조는 그림 1과 같다[1-3]. 계층별로 고유의 암호화 과정을 거쳐 통신 채널에서 보안 요구사항을 만족하도록 한다. 보안 요구사항의 수준은 고비도(high), 중비도(moderate), 저비도(minimal)로 구분된다.

고비도 보안(high security)은 정부나 군에 적용된다. 위성체 제어시스템의 접근 보안은 임무 수행중이나 모든 환경 및 운용 조건하에 항상 요구된다. 지상국의 모든 데이터와 모든 원격명령 데이터는 기밀성, 무결성, 접근제어, 인증이 요구되며 모든 원격측정 데이터는 기밀성, 무결성, 인증과 같은 서비스 등이 이루어져야 한다. 중비도 보안(moderate security)는 상용통신, 기상업무, 원격감시, 위성항해 시스템 등에 적용되며 원격명령 데이터는 기밀성을 위한 요구사항, 무결성, 인증이 요구되며 일부 또는 모든 원격측정 데이터는 기밀성, 무결성 등이 이루어져야 한다. 저비도 보안(minimal security)은 기타 다른 시스템에 적용되며 원격명령 데이터는 기밀성을 위한 가능한 요구사항, 무결성, 인증이 요구되며, 일부 원격 측정 데이터와 지상국간의 일부 데이터는 기밀성이 요구된다[3].

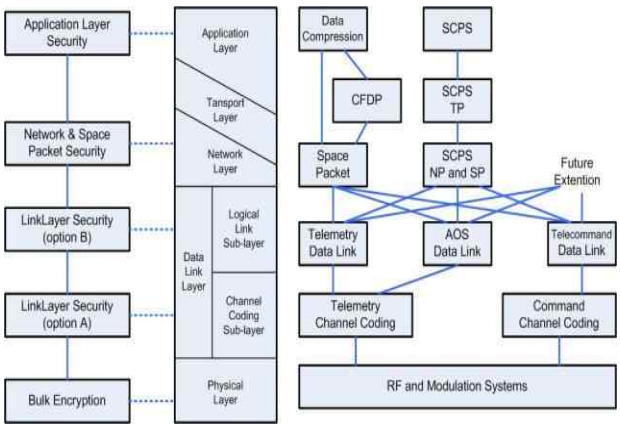


Fig. 1. CCSDS Protocol and Security architecture[3]

2. Link Encryption Synchronization Method in Accord with CCSDS

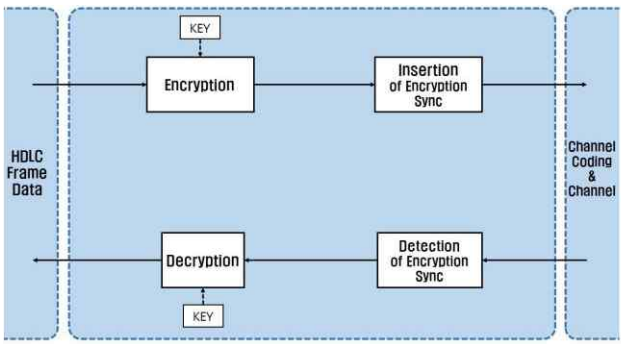


Fig. 2. A Detailed Block Diagram for Link Encryption Synchronization Method in Accord with CCSDS

그림 2는 CCSDS에서 규정하고 있는 링크 암호화 방식에서의 상세 구성도를 보여준다. 구성도에서 각각의 기능을 살펴보면 아래와 같다.

2.1 Encryption

암호화는 128비트 단위의 데이터를 128비트의 키로 암호화하는 AES[11] 알고리즘을 적용한다[12]. 링크 암호화를 위해 암호화기에 입력되는 데이터는 HDLC 프레임 구조를 가진다. 그림 3은 HDLC 프레임 구조를 보여준다. HDLC 프레임 구조는 8비트의 동기 플래그로 한 프레임의 시작을 나타내고, 8비트의 동기 플래그로 한 프레임의 끝을 나타내는 구조로 되어 있다. 정보부의 데이터는 8비트의 정수배 되는 길이로 제한이 없다. 따라서 고속의 영상데이터 전송을 위해서는 한 프레임 데이터의 길이가 제한된 이더넷 프레임 구조에 비해 HDLC 프레임 구조가 훨씬 효율적이다.

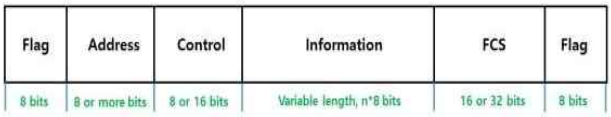


Fig. 3. HDLC Frame Structure

2.2 Insertion of Encryption Sync

송신측 암호화기에서 링크 암호화된 데이터는 수신측에서 동기화 할 수 있도록 그림 4와 같이 데이터 송신을 하기 전에 암호화 된 데이터 시작부에 암호동기 신호를 삽입한다. 이때 동기패턴은 잡음이 존재하는 채널에서 오류가 발생하더라도 수신 동기가 잘 이루어 질수 있도록 신뢰성이 높은 동기방식이 적용되어야 한다.

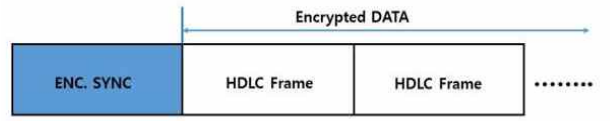


Fig. 4. Attachment of Encryption Synchronization

동기 패턴 검출기로는 자기 상관기(autocorrelator)를 일반적으로 많이 사용한다. Dixon[13]은 확산 대역 통신에서 의사난수 발생기를 초기화 하고자 자기 상관기를 이용하였다. Beker등[14]은 동기식 스트림 암호(synchronos stream ciphers)의 수신단에서 동기 패턴을 검출하고자 자기 상관기를 이용한 동기 방식을 제안하였다. 그러나 이들 방식은 고속 및 고신뢰도 통신이 요구되는 최근의 통신 회로에는 적용이 어렵다. 특히 잡음이 많은 무선 채널 등에서 통신 신뢰성 강화를 위하여 자기 상관기의 크기(이동 레지스터의 단수)를 늘릴 경우 하드웨어 복잡도가 크게 증가 되어 구현이 어렵게 된다. 왜냐하면 이동 레지스터의 단수(N)가 커질수록 구현 복잡도는 기하급수적으로 증가하기 때문이다. 또한, Leibowitz[15]는 TDM 다중화된 자기상관기(time-division multiplexed digital correlator)를 제안하여 k-배 만큼 속도를 개선시켰지만 고속처리에만 치중하여 하드웨어 복잡도는 기존 방식보다 k-배 이상 증가되었다.

본 논문에서 적용된 자기 상관기는 고 신뢰도를 보장하기 위하여 자기 상관기의 크기를 늘리더라도 그림 5와 같이 랜덤한 값으로 구성된 일반적인 동기 패턴을 단순 패턴으로 변환시켰다가 다시 역변환시키는 구조로 하드웨어 복잡도를 크게 줄일 수 있도록 함으로써, 고 신뢰도도 보장하면서 고속의 통신에도 적합한 방식이다. 다만, 단순 패턴 그 자체는 자기 상관성이 낮아서 동기 패턴으로 적합지 않으므로 자기 상관성이 우수한 동기 패턴을 생성 한 후 단순 패턴으로 변환시키는 과정이 별도로 필요하다. 또한 단순 패턴은 송신 시 선로 부호화 상에서 발생할 수 있는 연속 “0” 또는 연속 “1”로 인한 모뎀의 클럭 복구 문제 등을 방지할 수 있도록 스크램블러와 디스크램블러가 추가되어야 한다[16-17].

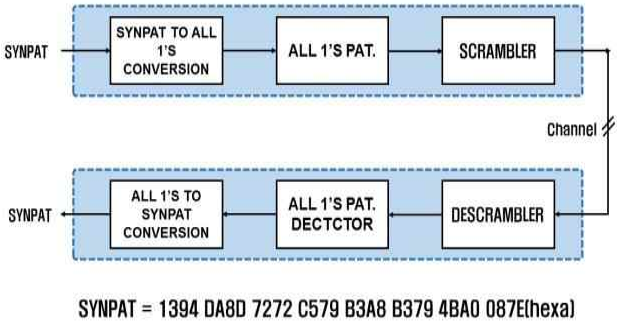


Fig. 5. Key Stream Synchronization Method using Simple Pattern

2.3 Detection of Encryption Sync

암호화된 데이터가 채널을 거쳐 수신되면 그림 2의 수신부 암호화 장비는 그림 2에서와 같이 먼저 암호화 동기를 검출한 후 복호화 과정을 거치게 된다.

2.4 Decryption

수신측에서 암호화 동기를 검출하게 되면 수신측 복호화기는 계속해서 이어지는 암호화된 데이터들에 대해 정상적으로 복호화를 수행한다. 그런데 송·수신측 간의 안정적인 암호 및 복호과정이 진행되는 도중에서도 여러 가지 환경적 요인으로 인해 복호화가 불가능한 상황이 발생할 수 있다.

III. SES Alarmed Link Encryption Synchronization Method

1. Environmental Causes of the Encryption System Error in the Receiver Side

실제 암호화 시스템을 운용할 경우 내·외부적인 요인으로 인하여 정상적인 복호화에 어려움을 가질 수 있다. 먼저 시스템의 내부적인 요인으로는 시스템에 주어지는 여러 가지 특성의 변화 - 온도, 습도 등의 환경적 요인- 에 따른 시스템의 불안정성 등으로 비트 슬립(bit slip) 이 발생하거나, 수신측 시스템의 전원차단, 셧다운 등이 발생하여 수신부의 동기화에 문제가 발생할 수 있고, 외부적인 요인으로는 번개 등에 의한 전자기적인 특성의 순간적인 변화나 이동체의 경우 특정 시점에서의 장애물에 의한 S/N비의 급격한 변화 등의 요인으로 인한 연집오류 등이 발생하여 암호동기를 탐지하지 못할 경우가 발생한다.

2. SES Alarmed Link Encryption Synchronization Method

CCSDS 프로토콜에 따른 링크 암호화의 문제점은 송수신이 진행되는 도중에 정상적인 복호화가 불가능한 상황이 발생하여 수신부의 데이터 획득이 불가능하게 되어도 송신측의 암호화

장비는 이 사실을 알지 못한다. 이와 같은 문제점을 해결하기 위한 방안이 SES Alarmed 링크 암호동기 방식이다. 이 방식은 그림 6과 같이 수신측에서 송신측으로 재동기 요구를 할 수 있는 방안이 제시 되었다[10]. 즉, 수신측에서 초기 암호화 동기를 탐지하는데 실패한다면 수신측에서 송신측으로 재동기 요청을 위한 신호를 전송하는 것과, 링크계층의 프레임 동기 오류가 연속적으로 탐지된다면 수신측에서 송신측으로 재동기 요청 할 수 있다는 것이다[10].

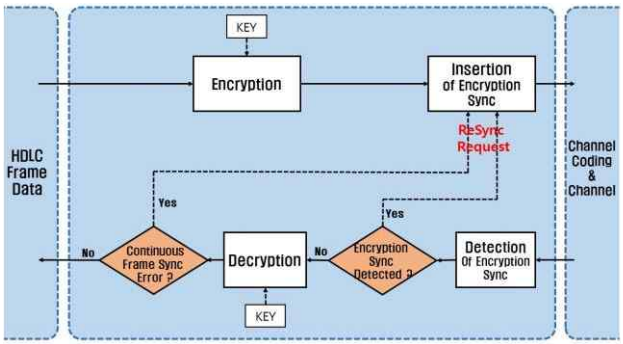


Fig. 6. A Detailed Block Diagram for SES Alarmed Encryption Synchronization Experiment

Ⅳ. Suggestion of Optimized SES Alarmed Link Encryption Synchronization Method

1. Optimized Two-stage Resynchronization Request

그림 7은 본 논문에서 제안된 최적의 SES Alarmed 링크 암호동기 방식 실험의 상세 구성도이다. 수신측에서 송신측으로의 재동기 요구는 2 단계에 걸쳐서 진행된다.

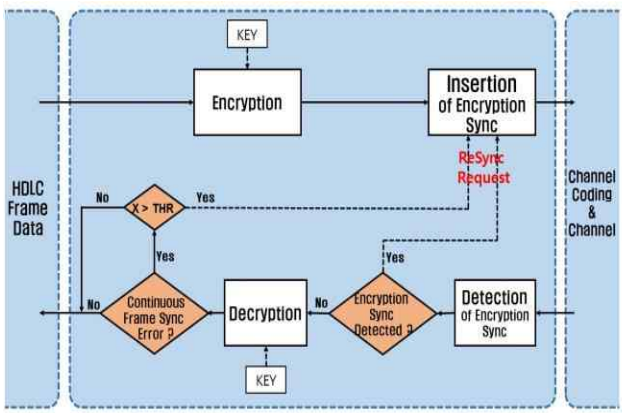


Fig. 7. A Detailed Block Diagram for Optimized SES Alarmed Encryption Synchronization Experiment

첫 번째 단계는 수신측의 암호동기 탐지과정에서 암호동기 오류가 발생하여 탐지를 하지 못할 경우 송신측에 재동기 요구를 하는 것이고, 두 번째 단계는 복호화 된 HDLC 프레임 데이터에서 프레임동기 오류를 검출할 때 연속된 프레임동기 오류의 횟수가 문턱값을 비교하여 오류 횟수가 문턱값을 초과할 경우 송신측에 재동기 요구를 하는 방식으로, 오류 확률에 따라 최적의 문턱값을 찾는 것이 중요하다.

2. Resynchronization Request Depending on Encryption Sync Detection

암호화된 데이터가 채널을 거쳐 수신되면 수신부의 암호화 장비는 먼저 암호화 동기를 검출한 후 복호화 과정을 거치게 된다. 그런데 채널에서 발생하는 여러 가지의 환경적 요인으로 인해 수신부에서 암호화 동기 패턴을 탐지하지 못하면 수신측은 송신측에 재동기 요청을 하게 되고, 송신측은 암호화된 데이터 앞부분에 암호화 동기를 다시 삽입하여 전송하게 된다.

본 논문에서는 그림 5에서 도출된 암호화 동기 패턴(SYNPAT)이 채널의 오류 확률 증가로 인하여 수신측에서 검출하지 못할 경우 수신측에서 송신측으로 재동기 요구를 하게되는데, [10]에서 오류가 발생하면 단순히 재동기 요구를 할 수 있다는 선언적 의미를 구체화 하여 오류 확률과 재동기 요구 횟수 간의 상호 관계를 실험하고 분석하여 선택된 암호화 동기 패턴이 사용될 수 있는 최악의 통신환경을 예측할 수 있게 한다.

3. Optimized Resynchronization Request Depending on Dectction of Frame Synchronization

그림 7의 실험 상세 구성도에서 두 번째 단계의 재동기 요구의 절차를 살펴보면 다음과 같다.

수신측의 복호화 된 데이터는 HDLC 프레임 구조를 가지게 되는데, 이때 각 프레임 데이터를 추출하기 위해서는 프레임 동기를 찾는 것이 우선된다. 채널을 거치는 과정에서 채널코딩/디코딩부에서 통상적으로 1×10^{-5} ~ 1×10^{-6}이하의 오류확률이 보장 되도록 설계되지만, 확률적으로 일정한 수의 프레임의 동기에서 오류가 발생할 수 있고, 이때 해당 프레임 데이터는 손실되게 된다. 그런데 3장 1절과 같은 특수한 환경적 요인으로 인해 허용범위를 초과한 연집오류가 발생하면 연속된 프레임 동기 오류가 발생하고, 이때 각각의 해당 프레임의 데이터들은 모두 손실되게 된다. 이와 같이 수신측에서 연속된 프레임 데이터의 오류가 발생하면 수신측은 암호화 된 데이터가 정상적으로 복호화 되지 못한다고 판단하게 된다.

본 논문에서는 먼저 수신측에서 연속적인 프레임 동기 오류가 발생하더라도 시스템은 정상적인 복호화가 진행하고 있는지의 여부를 판단하기 위한 판단의 기준값인 문턱값(THR)을 오류 확률에 따라 시뮬레이션을 통해 실험적으로 구한다. 다음으로 수신측에서 복호화 된 HDLC 프레임 데이터에서 계속적으로 프레임 동기 오류를 검출할 때 연속된 프레임 동기 오류가 발생할 경우 연속된 횟수를 x라 하면 수신 시스템은 x와

THR을 계속 비교하는 과정이 진행되도록 한다.

계속된 비교과정에서 $x \geq THR$ 이면 수신측 암호화기가 암호화 된 데이터를 복호화 하는데 실패한 것으로 판단하고 송신측에 재동기 요구를 하도록 설계한다. 다만 $x < THR$ 이면 프레임동기의 연속된 오류가 일시적인 현상인 것으로 판단하여 계속적인 송수신 과정이 진행되도록 한다. 따라서 본 논문에서는 시뮬레이션을 통하여 채널의 오류 확률에 따른 문턱값(THR)을 구하여 최적의 SES Alarm 신호를 발생하는 암호동기 방식을 제안한다.

Ⅳ. Experiment and Analysis

본 실험은 첫째, 채널의 오류 확률이 증가함에 따라 암호동기의 오류가 발생하게 되고, 이때 송신측으로 재동기 요구를 하는 것이 바람직하다고 제시한 [10]의 방안을 컴퓨터 시뮬레이션을 통해 구체적으로 오류 확률과 재동기 요구 횟수 간의 상호관계를 실험 및 분석하고자 한다. 둘째, 복호화 된 프레임 데이터의 프레임 동기 검출과정에서 연속된 프레임 동기 오류가 발생하면 송신측으로 재동기 요구를 할 수 있다는 방법의 제시에만 그친[10]을 개선하여 수신측에서 송신측으로 재동기 요구를 하기 위한 기준값을 오류 확률에 따라 몇 회의 연속 프레임 동기 오류로 설정하는 것이 최적의 문턱값인지를 찾기 위한 실험을 진행한다. 즉, 오류 확률에 비례해서 발생하는 통상적인 프레임 동기 오류인지 아니면 수신측 암호화기에 입력되는 암호화 된 데이터가 채널의 환경적 요인에 의해 허용범위를 초과한 연집오류의 발생으로 암호화기가 정상적으로 복호화를 하지 못해서 발생하는 프레임 동기 오류인지를 판단하기 위한 문턱값을 탐색하고자 하는 실험이다. 셋째, 오류확률에 따른 최종 출력 결과를 실험을 통하여 확인함으로써 송수신 시스템 설계 시 수용할 수 있는 출력 결과를 기준으로 채널코더에서 보장해야 할 오류확률을 예측할 수 있게 한다.

1. Experiment and Analysis for Resynchronization Request Depending on Error Rate of Encryption Synchronization

표 1은 암호화 된 데이터에 그림 5에서 생성된 128비트 암호화 동기 패턴을 삽입하였을 때 채널의 오류 확률에 따라 수신측 암호화기에서 송신측으로 재동기 요구를 하는 평균 횟수를 나타낸다. 이때 표 1의 결과 값은 재동기 요구 횟수를 계산하는 시뮬레이션에서 각 오류확률에 대해 각각 100회의 실험을 실시하고, 그 값을 평균하여 구하였다. 일반적인 채널 환경에서는 표 1과 같은 오류 확률이 발생할 가능성이 낮지만, 3장 1절에서 언급한 것과 같은 채널의 특수한 환경적 요인에 해당할 경우 수신측의 오류 확률은 표 1에서 나타낸 것과 같은 아주 낮은 상태에서 암호 동기를 탐지해야 하고, 그 결과 암호 동기 탐지 오류가 발생할 확률이 아주 높아져서 송신측으로 재동기 요구 횟수가 증가할 수 있다.

Table 1. Number of ReSync Request Depending on Error Rate

Error Rate	No. of ReSync Request
1×10^{-1}	0
2×10^{-1}	0.8
2.5×10^{-1}	1.7
3×10^{-1}	8.5
3.5×10^{-1}	76.3
4×10^{-1}	653.4

그림 8은 그 결과를 그래프로 보여주고 있다. 그림 8을 보면 오류 확률이 3.0×10^{-1}이하가 되면 재동기 요구 횟수가 급격하게 증가하는 것을 볼 수 있다. 따라서 정상적으로 암호화 동기가 탐지되려면 채널이 최악의 상황이라고 해도 수신측의 오류 확률이 3.0×10^{-1}이하가 될 수 있도록 채널 코더를 설계하거나, 그렇지 않으면 암호화 동기의 비트 수를 더 크게 하여 더 낮은 오류 확률에서도 암호동기의 오류가 발생하지 않도록 보장하여야 할 필요가 있다.

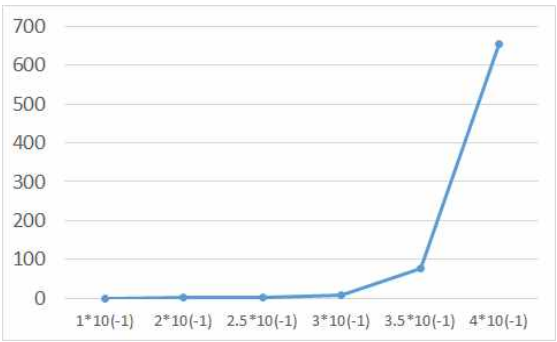


Fig. 8. Number of ReSync Request Depending on Error Rate

2. Threshold Detection and Analysis for Optimized Resynchronization Request

오류 확률이 증가하면 HDLC 프레임의 프레임동기 검출 오류 확률도 증가하게 된다. 그런데 이러한 오류가 수신측의 암호화기에서 암호화 된 데이터가 정상적으로 복호화 된 후 오류 확률의 증가에 비례해서 발생한 프레임 동기 오류라고 하면 이는 단지 채널의 환경에 따른 일시적인 현상으로 볼 수 있다. 그러나 3장 1절에서 언급한 것과 같은 환경적 요인으로 인해 허용 범위를 초과한 연집오류의 발생으로 수신측 암호화기가 정상적인 복호화를 하지 못해서 프레임 동기 오류가 연속해서 발생한 것이라면 송신측에서는 알 수가 없기 때문에 수신측에서 송신측으로 재동기 요구를 하는 과정이 있어야 한다.

실험의 방법은 표 2와 같이 오류 확률이 증가에 따라 2회 연속, 3회 연속, 5회 연속 및 7회 연속 프레임동기 오류가 발생할

경우를 미리 문턱값으로 설정하고 각각의 오류 확률에서의 누적된 오류 프레임 수를 구하는 실험을 하였다. 예를 들어 문턱값을 5회 연속 프레임동기 오류로 설정하고 채널의 오류확률을 계속 증가시켜 가면서 프레임의 동기 오류로 인해 누적된 오류 프레임의 수를 구하는 실험을 해보면, 채널의 오류 확률이 5×10^{-2} 이 되었을 때 누적 오류 프레임 수가 급격하게 증가하는 것을 볼 수 있다. 이때 누적 오류 프레임의 수를 급격하게 증가시키는 요인은 수신측 암호화 시스템의 복호화가 정상적으로 이루어지지 않을 가능성이 크다. 따라서 그림 7의 실험을 위한 상세 구성도에서 나타낸 것과 같이 수신측의 암호화기에서 복화화를 거친 후 1 차적으로 연속된 프레임 동기 오류를 판단하고, 연속된 프레임 동기 오류가 발생한다면 2 차적으로 문턱값과 비교해서 판단하게 되는데, 5×10^{-2}범위 내로 오류확률이 보장되는 좋은 채널환경에서는 문턱값을 5($THR = 5$)로 설정하는 것이 최적의 값이라는 것을 보여준다. 부연해서 설명하면 수신측에서는 2 차적인 판단과정에서 계속해서 검출되는 연속된 프레임동기 오류의 수 x와 문턱값을 비교해서 $x \geq THR$ 조건이 충족되면 수신측에서는 송신측으로 재동기 요청을 진행하게 된다. 같은 방식으로 진행한 실험에서 오류 확률이 1.5×10^{-2}범위 내의 값으로 보장될 수 있는 채널이라면 수신측에서 송신측으로 재동기 요청을 위한 판단의 기준 값인 연속된 프레임동기 오류에 대한 문턱값을 2회로 설정하는 것이 최적의 값이라는 것을 알 수 있고, 오류 확률이 3×10^{-2} 범위 내의 값으로 보장될 수 있는 채널이라면 수신측에서 송신측으로 재동기 요청을 위한 판단의 기준 값인 연속된 프레임동기 오류에 대한 문턱값을 3회로 설정하는 것이 최적의 값이라는 것을 알 수 있다. 또한 오류 확률이 7×10^{-2}범위 내의 값으로 보장될 수 있는 채널이라면 수신측에서 송신측으로 재동기 요청을 위한 판단의 기준 값인 연속된 프레임동기 오류에 대한 문턱값을 7회로 설정하는 것이 최적의 값이라는 것을 알 수 있다.

Table 2. Number of Accumulated Error Frame Depending on Error Rate

classification	2-consecutive error	3-consecutive error	5-consecutive error	7-consecutive error
1×10^{-3}	2.1	1.9	2.3	1.7
5×10^{-3}	11.4	8.7	7.3	6.8
1×10^{-2}	33.9	19.5	14.7	15.2
1.5×10^{-2}	188.0	35.2	23.2	22.8
1.8×10^{-2}	746.7	43.2	28.8	29.6
3×10^{-2}	-	358.7	47.3	40.6
3.5×10^{-2}	-	1085.2	63.5	47.1
5×10^{-2}	-	-	175.7	76.4
7×10^{-2}	-	-	2430.5	173.7
1×10^{-1}	-	-	-	2537.2

표 2의 결과값은 누적 오류 프레임의 수를 계산하는 시뮬레이션에서 각 오류 확률에 대해 각각 100회의 시뮬레이션을 실시하고, 그 값을 평균하여 각각의 오류 확률에서의 값을 구하였다. 그림 9는 그 결과를 그래프로 보여주고 있다. 그래프에서 보면 2-연속된 프레임 동기 오류의 문턱값의 경우 오류 확률이 1.5×10^{-2}에서부터 수신측에서 송신측으로 재동기 요구 횟수가 급격하게 증가하기 시작하는 것을 알 수 있다. 3-연속된 프레임 동기 오류의 문턱값의 경우 오류 확률이 3×10^{-2}에서부터 수신측에서 송신측으로 재동기 요구 횟수가 급격하게 증가하기 시작하는 것을 알 수 있고, 5-연속된 프레임 동기 오류의 문턱값에서는 오류 확률이 5×10^{-2}에서 재동기 요구 횟수가 급격하게 증가하는 것으로 나타난다. 문턱값을 7-연속 프레임 동기 오류로 설정한 그래프의 경우 오류 확률이 7×10^{-2}에서 재동기 요구 횟수가 크게 증가하는 것을 보여준다. 이와 같은 방법으로 실험을 하면 수신측 오류 환경에 따라 연속 프레임 동기 오류에 대한 최적의 문턱값을 구할 수 있게 되어 송·수신측 간에 일시적인 현상으로 인한 연속 프레임 동기 오류에 대해서는 불필요한 재동기 요구가 없이 안정적으로 송·수신 할 수 있게 된다.

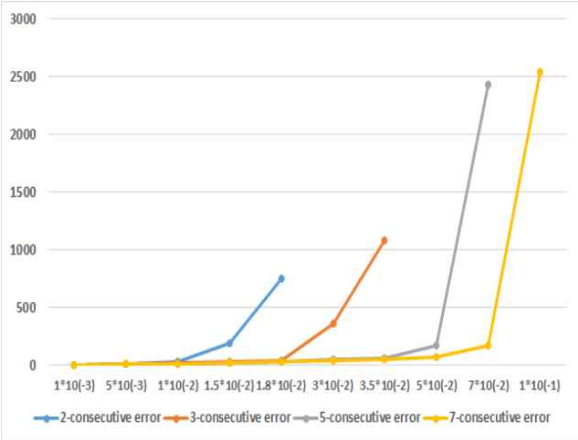


Fig. 9. Number of Accumulated Error Frame Depending on Error Rate

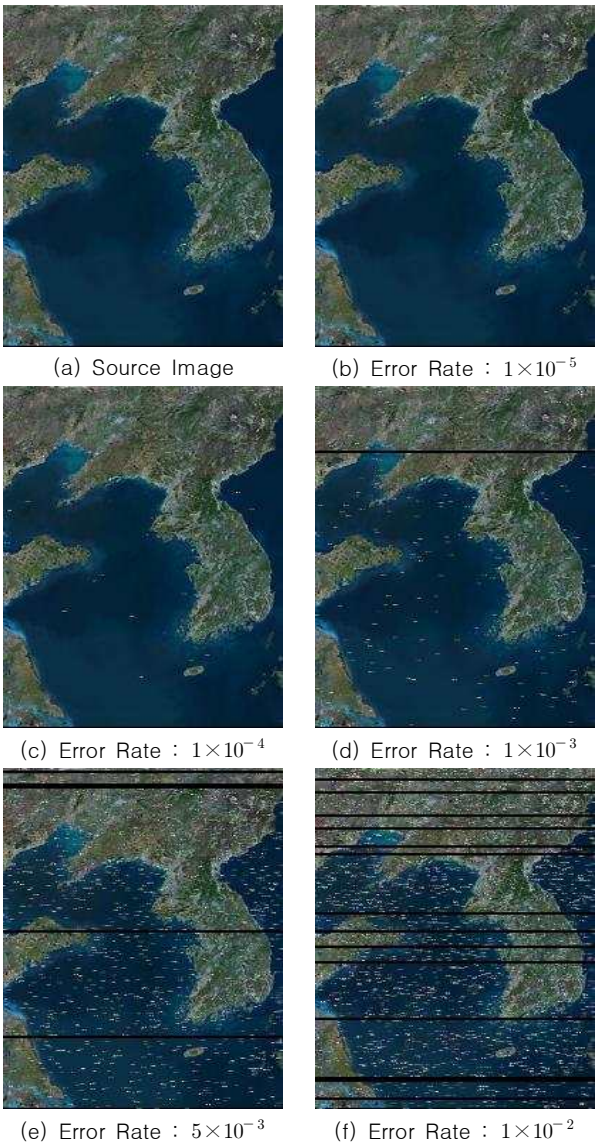
3. Decrypted Output Results Depending on Error Rate

그림 7의 수신측 암호화기에서 수신된 데이터를 복호화하면 HDLC 프레임 구조를 얻게 되는데, 이때 각 HDLC 프레임의 페이로드 데이터를 추출하려면 프레임 동기 검출이 선행되어야 한다. 만약 프레임 동기에 오류가 발생하여 프레임의 동기가 검출이 되지 않으면 해당 프레임의 데이터는 모두 손실되게 된다.

일반적인 통신환경에서는 채널코딩을 통해 1×10^{-6} 또는 1×10^{-5} 이하의 오류 확률을 보장하게 되고, 이 경우 HDLC 프레임 동기 오류는 거의 발생하지 않는 것으로 알려져 있다.

실제 실험에서도 그림 10과 같이 일반적인 오류 확률에서는 깨끗한 출력 이미지를 얻을 수 있다. 그러나 오류 확률이 낮아짐에 따라 점차 페이로드 데이터의 랜덤 오류가 발생하기 시작하다가 오류 확률이 기준 레벨보다 더 낮아지게 되면 프레임 동기 오류로 인해 한 프레임 전체 데이터의 손실도 발생하기 시작한

다. 그림 10(a)는 원본 이미지를 보여 주고 있고, 그림 10(b)는 오류 확률이 1×10^{-5}일 때의 결과이다. 이때의 결과 이미지는 그림 10(a)의 원본 이미지와 마찬가지로 랜덤 오류나 프레임 동기오류가 발생하지 않은 깨끗한 출력 결과를 보여준다.



(a) Source Image (b) Error Rate : 1×10^{-5}

(c) Error Rate : 1×10^{-4} (d) Error Rate : 1×10^{-3}

(e) Error Rate : 5×10^{-3} (f) Error Rate : 1×10^{-2}

Fig. 10. Decrypted Output Image Depending on Error Rate

그림 10(c)의 경우 오류 확률이 1×10^{-4}에서는 페이로드 데이터에서의 랜덤 오류로 인한 이미지 손상은 극히 드물게 나타남을 볼 수 있지만 프레임 동기 오류는 발생하지 않음을 알 수 있다. 그림 10(d)와 같이 오류 확률이 1×10^{-3}으로 떨어지면 페이로드 데이터의 랜덤 오류로 인한 이미지 손상뿐만 아니라 프레임 동기 오류로 인해 한 개의 프레임 전체의 데이터가 손실되었음을 확인할 수도 있다. 그림 10(e)와 같이 오류 확률이 5×10^{-3} 가 되면 랜덤 오류로 인한 이미지 손상도 많이 나타나고, 프레임 동기 오류로 인한 프레임 데이터 손상도 많이 나타나기 시작한다. 그림 10(f)에서 오류 확률이 1×10^{-2} 가 되면 페이로드 데이터의 랜덤 오류로 인한 이미지 품질의 열화도 크게 나타나지만, 프레임 동기 오류도 많이 발생하는 것을 확인 할 수 있다. 따라서 수신측 오류 확률이 최소한 1×10^{-3} 이하는 되어야 수신측에서 수용할 수 있을 정도의 이미지의 품질을 보장할 수 있음을 알 수 있다.

Ⅴ. Conclusion

CCSDS 프로토콜에 따라 설계된 암호화 장비는 송신측과 수신측 간에 데이터의 동기화를 위해 송신측에서 암호화된 데이터의 앞단에 암호화 동기를 삽입하여 전송함으로써 송수신 시스템 간에 초기 동기를 설정하도록 한다. 그러나 실제 시스템 운영 과정에서는 3장 1절에서 언급한 여러 가지의 환경적 요인들 때문에 수신측 암호화 장비에서 정상적인 데이터의 복호화를 하지 못하는 경우도 발생한다. 이 경우에도 송신측에서는 수신측의 상황을 알 수 있는 방법이 없다. 따라서 수신측에서 암호화 동기를 탐지하는데 실패하거나 복호화 된 HDLC 프레임의 프레임동기 검출 실패가 연속적으로 발생한다면 송신측에 재동기를 위한 피드백 과정이 필요하다.

본 논문에서는 첫째, 오류 확률과 암호동기오류로 인한 재동기 요구 횟수 간 상호 관계의 실험을 통해 선택된 암호화 동기 패턴이 사용가능한 통신환경을 예측할 수 있게 하였다. 둘째, 복호화 된 HDLC 프레임 데이터에서 프레임 동기의 연속 오류로 인한 재동기 요구 시 오류 확률 별 판단의 기준값인 최적의 문턱값을 찾아내고 분석하였다. 마지막으로 오류 확률에 따른 출력 결과를 통해 시스템 설계 시 채널 코더에서 보장해야 할

본 논문에서 제안하고, 계산한 최적의 SES Alarm 신호 방식을 적용하면 이동체 들 간에 암호화 된 고속 영상데이터를 안전하게 송수신할 수 있다.

REFERENCES

[1] CCSDS Satellite Recommended Standard , http:// public.ccsds.org/ publications/BlueBooks.aspx

[2] Procedure Manual for the Consultative Committee for Space Data Systems, CCSDS A00.0-Y-9, Yellow Book, Issue 9, Washington, D.C.:CCSDS, November 2003.

[3] The Application of CCSDS Protocols to Secure Ssystems, CCSDS 350.0-G-1, Green Book, Issue 1, Washington, D.C.:CCSDS, March 1999.

[4] Telecommand Part 1 : Channel Service, Recommendation for Space Data Systems Standards, CCSDS 201.0-B-3,

Blue Book, Issue 3, Washington, D.C. : CCSDS, June 2000.
[5] TC Synchronization and Channel Coding, Recommendation for Space Data Systems Standard, CCSDS 231.0-B-1, Blue Book, Issue 1, Washington, D.C. : CCSDS, September 2003.
[6] Space Assigned Numbers Authorith(SANA) - Role, Responsibilityes, Policies, and Procedures, CCSDS 313.0-Y-1, Yellow Book, Washington, D.C. : CCSDS, July 2011
[7] J. H. Yoon, C. S. Hwang, "A Resynchronization Technique by Time-Synchronization for Secure Communication using Stream Cipher," Proceeding of ICICS'97 , pp.1129-1133, Singapore, 9-12 September 1997.
[8] Ashraf D. Elbayoumy, Simon J.Shepherd, "Stream or Block Cipher for Securing VoIP?," International Journal of Network Security, Vol.5, No.2, pp.128-133, September 2007
[9] H. J. Beker and F. C. Piper, Cipher System : The Protection of Communications, Orthwood Books, London
[10] HyeongRag Kim, HoonJae Lee, DaeHoon Kwon, UiYoung Pak, "A SES Alarmeded 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, December 2013.
[11] NIST, "Announcing the Advanced Encryption Standard (AES)" (PDF). 《Federal Information Processing Standards Publication 197》. United States National Institute of Standards and Technology (NIST)., November 2001.
[12] Procedure Manual for the Consultative Committee for Space Data Systems, CCSDS A00.0-Y-9, Yellow Book, Issue 9, Washington, D.C. : CCSDS, November 2003.
[13] Dixon, R. C. (1976), Spread Spectrum Systems, Wiley, New York.
[14] Beker, H. J. and Piper, F. C. (1985), Secure Speech Communications, London Academic Press.
[15] Leibowitz, L. M. (1985), "Multiplexing Techniques for Digital Correlator Speed Improvement," IEEE Trans. on Comm, 33(6), pp.579-588.
[16] HoonJae Lee, Il Seok Ko, "An Intelligent Security Agent for Reliable Cipher System using PingPong," Cybernetics and Systems , Vol. 39, No. 7, pp.705-718, October 2008.
[17] Joan Daeman, Rene Govaerts and Joos Vandewalle, "Resynchronization Weaknesses in Synchronous Stream Cipher," Pre-Proceedings of EUROCRYPT'93. 1993.

ACKNOWLEDGMENTS

This work was supported by the "T4(274Mbps) class wideband common datalink" project of the Agency for Defense Development (ADD), Korea.

Authors

Hyeong-Rag Kim received the B.S., M.S. and Ph.D. degrees in Electronics Engineering from Kyungpook National University, Korea, in 1992, 1994 and 2010, respectively Dr. Kim joined the faculty of the Department of Information& Telecommunications at Pohang University, Pohang, Korea, in 1996. He is currently a Professor in the Department of IT&Electronics, Pohang University. He is interested in channel coding, cryptography and network security.

Hoon-Jae Lee received the B.S., M.S. and Ph.D. degree in Electrical Engineering from Kyungpook national university in 1985, 1987 and 1998, respectively. Dr. Lee had been engaged in the research on cryptography and network security at Agency for Defense Development from 1987 to 1998. Since 2002 he has been working for Department of Computer Engineering of Dongseo University as an associate professor, and now he is a full professor. His current research interests are in security communication system, side-channel attack, USN & RFID security. He is a member of the Korea institute of Information security and cryptology, IEEE Computer Society, IEEE Information Theory Society and etc

Ki-Hwan Kim received the B.S., M.S. degree in Computer Networking from Dongseo University, Republic of Korea in 2015. He current research interests are in Cryptography, Information Security and Network Security. Mr. Kim is now a Ph.D. student in the ubiquitous IT department at Dongseo Graduate School in 2017. He research interests are cryptography, Information security and network security.

Ju-Hyun Jung received the B.S degree in Computer Engineering from Konyang University in 2000 and M.S. degree in Computer Engineering from Chungnam National University in 2011.Ms. Jung Joined the Agency for Defense Development, Republic of Korea, in 2011 and is currently working as a researcher. Her current research interests are tactical networks, wireless network routing, Common data link(CDL).