論文 97-22-9-7

HDLC 프로토콜에서 운용되는 동기식 스트림 암호 통신에 적합한 적응 난수열 재동기 기법

正會員 윤 장 홍*, 황 찬 식**

An adaptive resynchronization technique for stream cipher system in HDLC protocol

Jang Hong Yoon*, Chan Sik Hwang** *Regular Members*

요 약

절대 클럭 동기를 요구하는 동기식 스트림 암호 통신 시스템에 사이클 슬립 현상이 발생하면 암,복호기간에 난수 동기가 이탈된다. 난수 동기 이탈 현상이 발생하면 통신을 할 수 없을 뿐아니라 수신 시스템을 오동작 시킬 수 있다. 이러한 위험성을 줄이기 위하여 암호문에 동기 패턴과 세션 키를 주기적으로 삽입하여 재동기를 이루는 연속 재동기 방법을 흔히 사용한다. 연속 재동기 방식을 사용하면 비교적 안정된 암호 통신을 할 수 있으나 몇 가지 문제점을 갖고 있다.

본 논문에서는 OSI 7계층중 링크 계층의 프로토콜로 HDLC방식을 사용하는 통신 체계에서 운용되는 동기식 스트림 암호 통신 시스템에 적합하고 연속 재동기 방식의 문제점들을 해결할 수 있는 적응 재동기 방식을 제안하였다. 제안된 적응 재동기 방식에서는 HDLC 프레임의 주소 체계 특성을 이용하여 난수 동기 이탈이 발생한 경우에만 재동기를 이루는 방법을 사용하였다. 즉, 각 단위 측정 시간 동안의 HDLC 프레임의 주소 영역 수신률을 측정하여 이것이 역치 보다 적은 경우에만 난수 동기 이탈이 발생한 것으로 판단하여 재동기를 이루는 방법을 사용하였다. 적응 재동기 방식은 연속 재동기 방식보다 효율적이며 주기적으로 동기 패턴과 세션 키를 전송하는 것에 따른 문제점을 해결하였다. 제안된 알고리즘을 HDLC 프로토콜을 사용하는 패킷 암호 통신에서 운용되는 동기식 스트림 암호 통신 시스템에 적용하여 시험한 결과, 연속 재동기에 비해 오 복호율 R_e와 오 복호된 데이터 비트수 D_e에서 훨씬 향상된 성능을 나타내는 것을 확인하였다.

ABSTRACT

The synchronous stream cipher which require absolute clock synchronization has the problem of synchronization

*국방과학연구소 근무
**경북대학교 전기전자공학부
論文番號:97217-0627
接受日字:1997年 6月 27日

loss by cycle slip. Synchronization loss makes the state which sender and receiver can't communicate with each other and it may break the receiving system. To lessen the risk, we usually use a continuous resynchronization method which achieve resynchronization at fixed timesteps by inserting synchronization pattern and session key. While we can get resynchronization effectively by continuous resynchronization, there are some problems. In this paper, we proposed an adaptive resynchronization algorithm for cipher system using HDLC protocol. It is able to solve the problem of the continuous resynchronization. The proposed adaptive algorithm make resynchronization only in the case that the resynchronization is occurred by analyzing the address field of HDLC. It measures the receiving rate of the address field in the decision duration. Because it make resynchronization only when the receiving rate is greater than the threshold value, it is able to solve the problems of continuous resynchronization method. When the proposed adaptive algorithm is applied to the synchronous stream cipher system in packet network, it has advanced the result in R_e and D_e.

Ⅰ. 서 론

최근 컴퓨터나 통신 네트워크의 발달로 정보 교환의 편리성은 극대화되어 가고 있으나 이에 따른 사회적 역기능 또한 늘어가고 있는 실정이므로 전송되는 정보의 보호 문제가 매우 중요한 문제로 부각되고있다. 이에 대한 대책으로 컴퓨터 네트워크나 통신 네트워크를 통하여 중요 정보를 전송 할 때 비인가자의 도용이나 도청 또는 정보 파괴 및 변조 등으로부터 보호하기 위하여 암호기로 암호화하여 전송하고 복호기에서 이를 해독하여 인가자만이 원래의 정보를 얻도록 하는 방법을 사용한다. 그런데 암호기에서 전송한 암호문이 복호기에서 정상적으로 복호되기 위해서는 암호기에서 사용한 난수와 복호기에서 사용한 난수가 일치하여야 하나 여러 가지 원인에 의하여 암호기의 난수와 복호기의 난수가 일치하지 않는 경우가 발생하는데 이를 흔히 난수 동기 이탈이라 한다. 난수 동기 이탈을 일으키는 주된 원인은 수신 측에서 복원한 클럭이 선로 잡음 때문에 송신 클럭에 비해 빠지거나 더해지는 사이클 슬립 또는 비트 슬립 현상이다. 사이클 슬립 현상이 스트림 암호 시스템에서 발생하면 암, 복호기간에 난수 동기 이탈을 일으켜[1-2] 통신을 할 수 없을 뿐 아니라 복호된 데이터는 임의의 값을 가지므로 수신 시스템을 오 동작시킬 수 있다[3-4]. 이러한 위험성을 줄이기 위하여 스트림 암호 통신에서는 난수 동기 이탈이 발생하면 암, 복호기간의 난수열을 다시 일치시켜 재동기를 이루는 방법을 사용하는데 주로 사용되는 방법은 연속 재동기 방식과 자체 동기 방식이다. 연속 재동기 방식은 동기식 스트림 시스템에서 주로 사용하는 재동기 방식으로서 암호문에 동기 신호와 세션 키를 주기적으로 삽입하여 전송하여 암, 복호기간에 주기적으로 재동기를 이루는 방법인데 한 주기 내에서 난수 동기 이탈이 발생하여도 다음 주기에서 재동기를 이루므로 비교적 안정된 암호 통신을 할 수 있는 장점이 있으나 몇 가지 문제점들이 있다[5]. 첫째, 연속 재동기 방식은 동기 이탈 현상의 발생 여부와 무관하게 일정 시간 간격으로 재동기를 이루므로 난수 동기 이탈이 발생하면 다음 동기 패턴과 세션 키를 수신 할 때까지 동기 이탈 상태가 유지되어 통신을 할 수 없게되고 난수 동기 이탈 시에 발생되는 임의의 데이터에 의해 수신 시스템을 오동작시킬 위험성이 존재한다 둘째, 연속 재동기 방식은 난수 동기 이탈의 발생과 무관하게 주기적으로 동기 패턴과 세션 키를 전송하여야 하므로 전송 효율이 떨어지고 매번 다른 세션 키를 발생하고 전송하여야 하는 부담이 있다. 셋째, 세션 키를 전송하는 과정에서 세션 키에 전송 오류가 발생하면 다음 동기 패턴과 세션 키를 수신 할 때까지 난수 동기 이탈된 상태가 유지되어 오류가 확산되는 문제점이 있다. 자체 동기 방식은, 암호문 자체를 암, 복호기의 세션 키로 사용하기 때문에 재동기를 위한 동기 신호와 세션 키를 따로 전송할 필요가 없을 뿐 아니라 암, 복호기 간에 난수열 불일치 현상이 발생하여도 일정 시간이 지나면 자동적으로 재동기를 이루는 장점이 있다. 그러나 이 방식은 암호문을 암, 복호기의 세션 키로 사용하는 구조적인 특성으로

인하여 암호문에 전송 도중 단순한 비트 오류가 발생되어도 복호기에서 여러 비트로 오류가 확산되는 문제점이 있어 열악한 선로 조건에서는 사용하기가 곤란할 뿐 아니라 사이클 슬립이 발생되면 강제적으로 초기화 시켜주지 않는 한 재동기를 이룰 수가 없는 단점이 있어 사이클 슬립이 있는 암호 통신 시스템에서는 효율적인 성능을 나타내지 못한다.

본 논문에서는 OSI(Open System Interconnection) 7계층 중 링크 계층의 프로토콜로 HDLC(High Level Data Link Control Procedure)를 사용하는 통신 체계에서 운용되는 링크 암호 통신 시스템에 적합하고 연속 재동기 방식의 문제점들을 해결 할 수 있는 적응 재동기 방식을 제안하였다. HDLC 주소 영역 부는 사용하는 길이에 따라 각 바이트의 첫 비트는 일정한 값을 갖는 특성이 있는데 제안된 방법에서는 이러한 주소 영역 특성을 이용하여 난수 동기 이탈의 발생 유, 무를 판단한 후 난수 동기 이탈이 발생한 경우에만 동기 패턴과 세션 키를 전송하여 재동기를 이루는 적응 재동기 방법을 사용하였다. 즉, 정상적으로 복호되는 경우는 HDLC 주소 영역부가 사용하는 주소 영역의 길이에 따라 일정한 값을 가질 것이나[6-8] 난수 동기 이탈이 발생된 경우는 임의의 값을 나타낼 것이므로 각 단위 측정 시간마다 HDLC 프레임의 주소 영역 수신률을 측정하여 이것이 역치(threshold)보다 적은 경우에만 난수 동기 이탈 현상이 발생된 것으로 판단하여 동기 패턴과 세션 키를 전송하여 재동기를 이루었다. 암호 통신 중에 난수 동기 이탈이 발생하는 기간은 정상적인 기간에 비하여 매우 적으므로 제안된 적응 재동기 방법을 사용하면 기존의 연속 재동기 방법에 비하여 재동기를 위하여 전송하는 동기 패턴과 세션 키의 수가 훨씬 줄어들어 통신 효율이 증가할 뿐 아니라 주기적으로 동기 패턴과 세션 키를 전송함으로서 발생되는 문제점들을 해결 할 수 있다. 또한 적응 재동기 방식에서의 단위 측정 시간은 연속 재동기 방식의 재동기 주기에 비하여 매우 짧으므로 적응 재동기 방식은 연속 재동기 방식에 비하여 난수 동기 이탈 상태를 훨씬 빠르게 찾아낼 수 있어 보다 안정된 암호 통신을 가능하게 한다. 제안된 방법의 성능을 평가하기 위하여 HDLC 프로토콜을 사용하는 패킷 통신망에서 운용되는 동기식 스트림 암호 통신 시스템에 적용하여 시험하였다. 시험은 전화선이나 음성 망을 이용하여 패킷 통신을 할 때 주로 사용하는 9,600-28,800bps급의 모뎀을 통하여 전송하였으며 사이클 슬립 발생기로 난수 동기 이탈을 인위적으로 발생시키면서 제안된 적응 재동기 방식이 얼마나 효과적으로 재동기를 이루는 가를 알아보았다.

Ⅱ. OSI 참조 모델

1. 7계층의 구조

다른 기종간의 컴퓨터 통신을 가능하게 하기 위하여 ISO(International Standard Organization)에서 추진한 표준 네크워크 아키텍처를 개방형 시스템간의 상호 접속(OSI, Open System Interface)이라 하는데 이것은 7계층으로 구성되어 있으며 통상적으로 OSI 참조 모델이라 부른다. OSI 참조 모델은 각 계층의 프로토콜을 생산적이면서 서로 독립적으로 수행할 수 있도록 통신 개념과 그 기능에 대한 기준을 설정해 주는 것으로서 그림 1과 같은 구조를 갖는다. 그림 1에 표시되어 있는 것처럼 OSI 참조 모델에서는 통신 회선의 제어 기능에서부터 통신에 부수되는 일련의 통신처리 기능까지의 개방형 시스템에서 요구되는 통신 기능을 7개의 기능 계층으로 분리하고 있다. 이러한 7계층의 기능은 이미 잘 알려져 있으므로 7계층 전체에 대한 설명은 생략하기로 하고 본 논문에서 이용하는 제 2계층인 데이터 링크 계층의 기능과 HDLC 프로토콜의 프레임 구조에 대해서만 알아보기로 한다.

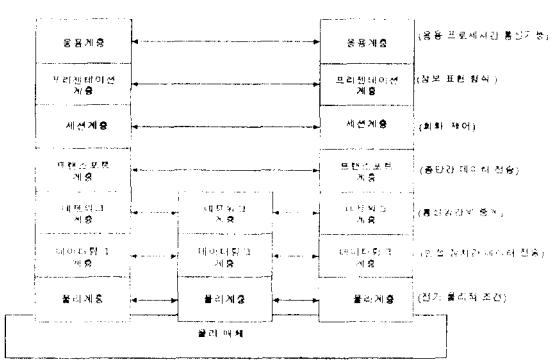

그림 1. OSI 참조 모델의 구조
Fig. 1 The structure of OSI reference model

2. 링크 계층의 기능과 HDLC 프레임의 구성

OSI 참조 모델 7계층 중 2번째 계층인 데이터 링크 계층은 DTE(Data Terminal Equipment)와 DCE(Data Circuit terminating Equipment)간의 원활한 데이터 전송이 이루어질 수 있도록 연속된 비트 열을 전송 단위로 분할하는 기능, 순서 제어 기능, 에러 검출 및 회복 기능, 흐름 제어 기능 등을 갖는다. 이 링크 계층의 프로토콜로는 ISO에 의해 1974년에 발표한 HDLC (High Level Data Link Control)와 1976년에 ITU-T에서 발표하여 X.25 권고 안에 사용되고 있는 LAPB가 있다. HDLC와 LAPB는 매우 유사하며 LAPB가 HDLC의 부분 집합이라 할 수 있는데 HDLC 프레임의 구성은 그림 2와 같다[6-8].

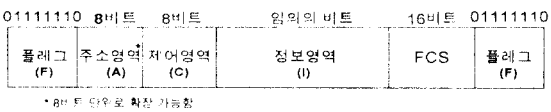

그림 2. HDLC 프레임의 구조
Fig. 2 The structure of HDLC frame

그림 2에 나타난 플래그(F)는 프레임의 개시 및 종결을 표시하는 특유의 형식으로서 프레임의 동기를 찾기 위해 사용된다. 개시 플래그와 종결 플래그 사이의 데이터에 플래그와 동일한 형식(01111110:1이 6개 연속)을 갖지 않도록 하기 위해서 송신 측에서는 전송하는 데이터의 '1' 비트가 5개 연속되면 다섯 번째 비트 다음에 '0' 비트를 하나 삽입하여 전송하고, 수신 측에서는 수신된 데이터의 '1' 비트가 5개 연속되면 그 다음의 '0' 비트를 제거하는 조작을 행하게 되는데 이러한 기법을 비트 스터핑(bit stuffing)이라 하며, 이 조작에 의하여 투과성(transparency)이 보장되어 자연스러운 비트 열의 데이터를 전송할 수 있다. 또한 플래그 패턴 사이가 32비트 미만인 프레임을 무효 프레임이라 하여 수신 국은 이 프레임을 무시한다. HDLC 프레임의 주소 영역 부는 기본적으로 1바이트이기 때문에 128가지 조합의 주소로 사용할 수 있으며 만일 이 조합으로 부족한 경우는 주소 부를 확장할 수 있다. 확장할 때는 미리 송, 수신간에 약속해 놓지 않으면 안된다. 그런데 HDLC의 주소 영역 부는 사용하는 길이에 따라 각 바이트의 첫 비트가 일정한 값을 갖는데 본 논문에서는 HDLC 주소 영역 부의 이러한 특성을 이용하여 난수 동기 이탈 현상을 판단하였다. 제어 영역(C)은 주소 영역에서 지정한 해당 국에 대해 동작을 명령하고 해당 국이 그 명령에 대한 응답을 하는데 사용된다. 정보 영역(I)은 사용자간에 교환되는 메시지와 제어 정보가 삽입되는 부분으로서 비트 열 및 비트 수에는 제한이 없다. 프레임 검사 순서(FCS)는 주소 영역과 정보 영역의 내용이 오류 없이 상대방에게 전송되어 지는 것을 확인하기 위해 사용된다.

Ⅲ. 암호화의 형태와 기존의 재동기 방식

1. 링크 암호 방식과 단대단 암호 방식

전송되는 데이터를 암호화하는 방법은 링크 암호화와 단대단 암호화로 구분 할 수 있다. 링크 암호화의 경우는 그림 3에서 보는 바와 같이 통신 링크 양단에 암호화 장치를 모두 설치하여 통신 링크 상의 모든 트래픽을 보호한다[9].

단대단 암호화 과정은 두 종단 시스템에서만 이루어지므로 두 종단 시스템에만 암호화 장치를 설치하면 된다. 이 두 가지 암호화 방식은 서로 상반된 장, 단점을 갖고 있다. 링크 암호화 방식은 링크 상의 모든 트래픽을 암호화하므로 전송 데이터의 보호 뿐 아니라 해당 데이터의 출처 및 목적지까지 보호되는 장점이 있으나 패킷 통신인 경우 패킷 교환기가 패킷을 전송하기 위해 패킷 헤더에 있는 주소를 읽어야 하므

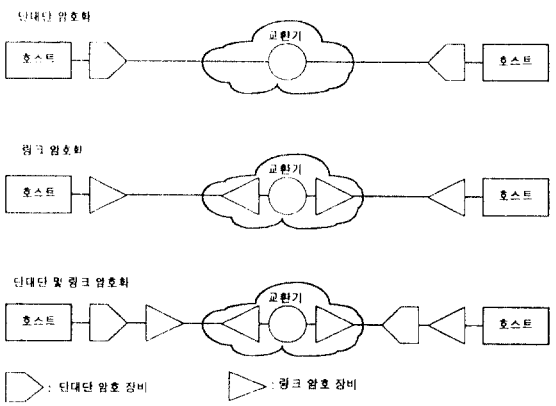

그림 3. 단대단 암호화와 링크 암호화
Fig. 3 End-to-End encrytion and Link encryption

로 암호화된 패킷 데이터가 패킷 교환기에 들어올 때마다 복호화 되어야 하는 단점이 있고 전송 데이터가 패킷 교환기에서 공격당할 우려가 있다. 반면 단대단 암호화 방식은 정보 영역을 선택하여 암호화하므로 전송되는 모든 과정에서 사용자 데이터는 안전하다는 장점이 있으나 패킷의 헤더 부분과 같은 트래픽 패턴은 암호화되지 않은 채 전송되기 때문에 해당 데이터의 출처 및 목적지가 노출되어 공격당할 우려가 있다. 이상과 같이 링크 암호 방식과 단대단 암호 방식은 서로 상반된 장, 단점을 가지므로 보다 높은 보안성을 유지하기 위해서는 그림 4에서 보는 바와 같이 링크 암호화 방식과 단대단 암호화 방식을 같이 사용하여야 한다. 링크 암호화 방식과 단대단 암호화 방식을 모두 사용하면 데이터의 출처 및 목적지의 노출을 막을 수 있을 뿐아니라 전송 데이터가 패킷 교환기에서 공격당할 우려도 없어지므로 완벽한 보안 체제를 구축 할 수 있다[9].

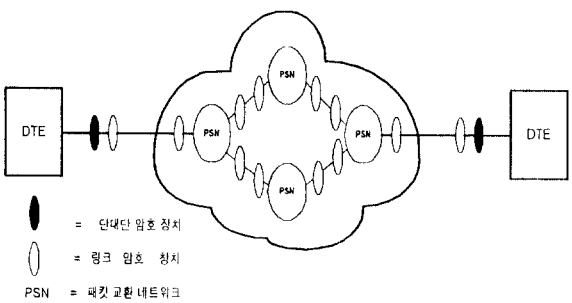

그림 4. 패킷 교환망 상의 암호화
Fig. 4 The encryption in packet network

2. 링크 암호 방식에서의 기존의 연속 재동기 방식

그림 5와 같이 표현되는 동기식 스트림 암호 통신은 암, 복호기에서 사용하는 난수열 K_i가 서로 일치하여야만 복호기에서 원래의 정보 P_i를 복원 할 수 있으나 선로 잡음에 의한 사이클 슬립 등이 발생하면 암, 복호기에서 사용하는 난수열 K_i가 서로 어긋나 그 이후부터 모든 암호문은 제대로 복원 할 수 없게 된다[4][10][11-12]. 이런 현상을 난수 동기 이탈이라 하며 난수 동기 이탈 후 다시 통신하기 위해서는 암, 복호기는 그들의 난수열 발생기를 재동기시켜야 하는데 여기서 재동기라는 것은 암, 복호기가 다시 동일한 난수열을 사용하여 정상적으로 암호문을 복호할 수 있도록 하는 것을 말한다. 흔히 사용하는 재동기 방법 중의 하나인 연속 재동기 방식은, 그림 6과 같이 암, 복호기가 주기적으로 동기 패턴과 세션 키를 주고받음으로서 서로 동일한 세션 키로서 난수열 발생기의 internal state 값을 주기적으로 동일하게 만들어 재동기를 이룬다[10]. 난수열 발생기의 내부 구조는 그림 7과 같이 표현되는데 난수열 발생기는 internal state의 값을 seed로 하여 난수열을 발생하므로 internal state 값이 동일하면 동일한 난수열이 발생된다. 따라서, 암, 복호기 난수열 발생기의 internal state의 값을

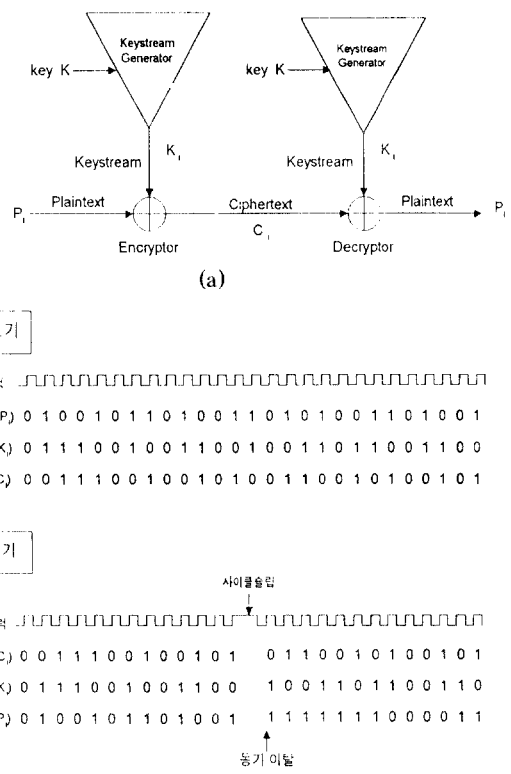

그림 5. 동기식 스트림 암호 통신 시스템의 구성과 사이클 슬립에의한 동기 이탈이 발생한 경우
(a) 동기식 스트림 암호 통신 시스템 구성
(b) 사이클 슬립에 의한 동기 이탈이 발생한 경우

Fig. 5. The structure of secure communication system using synchronous stream cipher and the case that have synchronization loss by cycle slip
(a) The structure of secure communication system using synchronous stream cipher
(b) the case that have synchronization loss by cycle slip

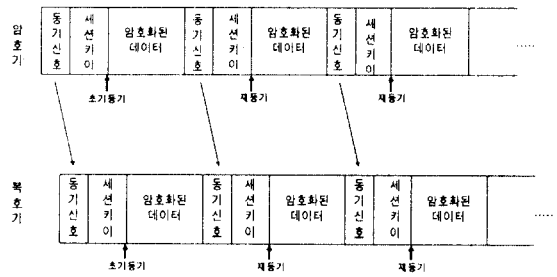

그림 6. 연속 재동기 방식의 구성도
Fig. 6. The structure of continuous resynchronization

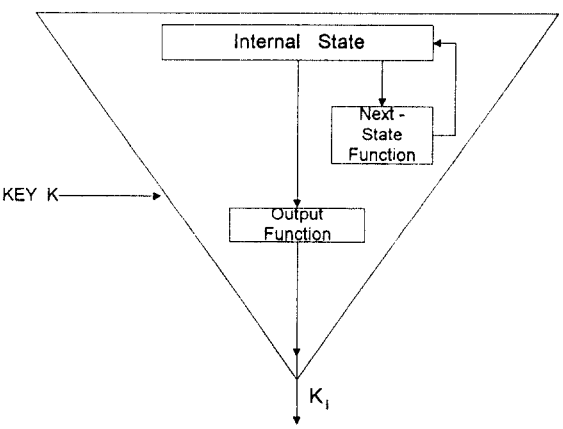

그림 7. keystream generator의 내부구조
Fig. 7 The internal structure of keystream generator

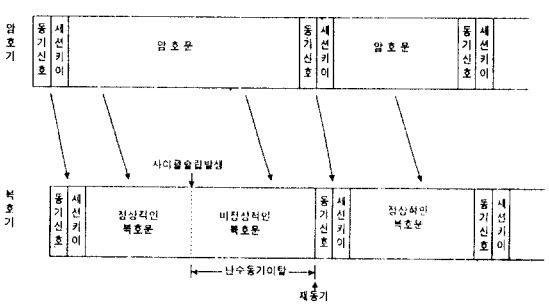

그림 8. 난수 동기 이탈 발생시의 연속 재동기 방식 구조
Fig. 8 The structure of continunous resynchronization with synchronization loss

동일한 시점에 서로 일치시키면 암, 복호기의 난수열 발생기의 출력이 서로 같아져 재동기가 가능하게 된다. 이러한 동기식 스트림 암호 체계에 연속 재동기 방식을 사용하면 난수 동기 이탈이 발생하여도 주기적으로 재동기를 이루므로 비교적 안정된 통신을 가능하게 하나 그림 8에 나타난 바와 같이 주기 내에서 동기 이탈이 발생하면 다음 재동기까지는 암호문을 정상적으로 복원 할 수 없는 단점이 있으므로 재동기 주기가 길어지면 정상적으로 복원하지 못하는 암호문의 양이 증가하여 전반적인 통신 품질을 저하시킨다. 반면에 재동기 주기를 짧게 하면 전송해야할 동기 패턴과 세션 키의 양이 증가하여 통신 효율을 떨어뜨린다.

Ⅳ. HDLC의 주소 특성을 이용한 링크 암호 통신에서의 적응 재동기 알고리즘

본 논문에서는 OSI 7계층 중 2번째 계층의 프로토콜로 HDLC를 사용하는 통신 체계에서 운용되는 링크 암호 통신 시스템에 적합하고 기존의 연속 재동기 방식의 단점을 해결할 수 있는 적응 재동기 알고리즘을 제안하였다. 제안된 알고리즘에서는 HDLC 프레임 구조 중 주소 영역의 특성을 이용하여 재동기를 이룬다.

1. 주소 영역 부의 구조 및 특성

HDLC 프레임의 주소 영역부는 기본적으로 1바이트이기 때문에 128가지의 조합의 주소를 사용할 수 있으나 이 조합으로 부족한 경우는 주소 부를 확장할 수 있다. 확장할 때는 미리 송, 수신간에 약속해 놓지 않으면 안된다[6-8]. 그림 9는 k 바이트까지 확장된 주소 영역을 각 비트 별로 나타낸 것인데 이때 각 비트는 a_{nm}으로 표시하였다. 이를 식으로 표시하면 식 (1)과 같다.

$$a_{nm}=\begin{cases}0 & \text{만일 } m=0\text{이고 } n\neq k-1\text{인 경우} \\ 1 & \text{만일 } m=0\text{이고 } n=k-1\text{인 경우} \\ 0 \text{ 또는 } 1 & \text{만일 } m\neq 0\text{이고 } n\neq k-1\text{인 경우}\end{cases} \quad (1)$$

여기서 n은 주소 영역의 바이트 순서를 나타내는 것으로 $n=0, 1, 2,\ldots, k-1$이고 m은 각 바이트 내의 비트 순서를 나타내는 것으로 $m=0, 1, 2, 3, 4, 5, 6, 7$이다.

만일, 주소 부를 8k 비트로 사용한다면 $n=0, 1, 2,\ldots, k-1$인 경우이므로 식(1)에서 $a_{00}, a_{10},\ldots, a_{(k-3)0}, a_{(k-2)0}$는 '0'이고 k번째 바이트의 최하위 비트인 $a_{(k-1)0}$

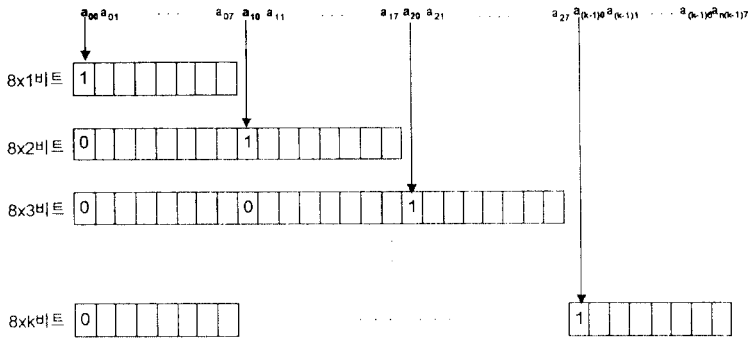

그림 9. HDLC 프레임에서의 주소 영역부의 구조
Fig. 9 The address field in HDLC frame

만 '1'로 하면 된다. 이때 사용할 수 있는 주소의 조합은 2^{7k}이다.

본 논문에서는 식 (1)에서 k=0, 1, 2인 경우 즉 주소 영역 부의 길이가 1바이트, 2바이트, 3바이트인 경우에 대해서 알아보기로 한다.

첫째, 그림 9와 같이 주소 부를 8비트 그대로 사용할 때는 k=1, n=0인 경우이므로 식 (1)에의하여 첫 번째 바이트의 최하위 비트인 a_{00}는 '1'이고 이때 사용할 수 있는 조합의 수는 27이다.

둘째, 그림 9와 같이 주소 부를 16비트로 사용할 때는 k=2, n=0, 1인 경우이므로 식 (1)에의하여 첫 번째 바이트의 최하위 비트인 a_{00}를 '0'으로 하고 두 번째 바이트의 최하위 비트인 a_{10}를 '1'로 한다. 이때 사용할 수 있는 조합의 수는 2^{14}이 된다.

셋째, 그림 9와 같이 주소 부를 24비트로 사용할 때는 k=3, n=0, 1, 2인 경우이므로 식 (1)에의하여 첫 번째 바이트의 최하위 비트인 a_{00}과 두 번째 바이트의 최하위 비트인 a_{10}를 '0'으로 하고 세 번째 바이트의 최하위 비트인 a_{20}를 '1'로 한다. 이때 사용할 수 있는 조합의 수는 2^{21}이 된다.

주소 영역부의 길이가 1바이트, 2바이트, 3바이트 각 경우에 대한 a_{00}, a_{10}, a_{20}의 형태를 정리하면 표 1과 같다. 본 논문에서는 표 1에서 나타난 HDLC 프레임의 주소 영역에서 a_{00}, a_{10}, a_{20}의 특성을 이용하여 난수 동기 이탈이 발생한 경우에만 재동기를 이루는 적응 재동기 알고리즘을 제안하였다. HDLC 환경에서 사용하는 암호 통신 시스템의 복호기가 정상적으로 복호하는 경우에는 a_{00}, a_{10}, a_{20} 값이 거의 대부분 표 1에서 나타난 값을 가질 것이나 난수 동기 이탈이 발생된 경우에는 a_{00}, a_{10}, a_{20} 값이 표 1에서 나타난 값을 가지는 경우는 거의 없고 임의 값을 가지는 경우가 대부분일 것이다. 따라서, a_{00}, a_{10}, a_{20}의 특성을 이용하여 난수 동기 이탈이 발생한 경우에만 동기 패턴과 세션 키를 전송하여 재동기를 이루는 방법을 사용한다면 난수 동기 이탈과 무관하게 주기적으로 동기 패턴과 세션 키를 전송하여 난수 재동기를 이루는 연속 재동기 방식보다 훨씬 효율적일 것이다.

2. R_A(주소 영역 수신률)

본 논문에서는 HDLC의 주소 영역 중에서 a_{00}, a_{10}, a_{20}의 특성을 이용하여 난수 동기 이탈의 발생 여부를 판단하기 위한 척도로서 식(2)과 같이 표현되는 주소 영역 수신률 R_A을 사용하였다.

$$R_A = \frac{N_{FA}}{N_F} \tag{2}$$

여기서, N_F는 단위 측정 시간 T_u초 동안 복호된 데이터에서 감지된 프레그 패턴의 갯수이고, N_{FA}은 감지된 프레그 패턴 중에 a_{00}, a_{10}, a_{20}가 정상적인 HDLC 주소 영역 값을 갖는 경우의 수이다.

식(2)에서 보는 바와 같이 R_A는 단위 측정 시간으로 정의한 T_u초 동안에 수신된 모든 프레그 패턴 중에서 a_{00}, a_{10}, a_{20}가 정상적인 HDLC 주소 영역 패턴인 경우가 얼마나 되는가를 나타낸다. HDLC 프레임

표 1. a_{00}, a_{10}, a_{20}의 특성
Table 1. The characteristics of a_{00}, a_{10}, a_{20}

주소 비트위치 / 영역길이	a_{00}	a_{10}	a_{20}
8비트인 경우	1	–	–
16비트인 경우	0	1	–
24비트인 경우	0	0	1

의 주소 영역을 찾기 위해서는 복호된 데이터 열에서 HDLC 프레임을 구성하는 시작 프레그 패턴(F), 주소 영역(A), 정보 영역(I), 프레임 검사 순서(FCS)를 찾아 주소 영역에 해당되는 부분의 값을 읽는 방법도 있으나 이것은 복잡하고 계산 량도 많으므로 본 논문에서는 이러한 방법을 사용하지 않았다. 적응 재동기 방식에서는 HDLC 프레임 중에서 주소 영역만이 필요하므로 복호된 데이터 열에서 HDLC 프레임의 시작을 나타내는 프레그 패턴 값을 찾아낸 후 시작 프레임 다음의 값을 해당 주소 영역 바이트 수만큼 읽어 주소 영역으로 정하는 방법을 사용하였다. 예를 들어 주소 영역을 3바이트로 정하였다면 단위 측정시간 T_u초 동안 관찰된 총 프래그 패턴에서 프레그 패턴 다음 3바이트 값을 주소 영역부로 하였다. 이 주소 영역부 각 바이트중 최하위 비트인 a_{00}, a_{10}, a_{20}가 표 1과 같은 정상적인 HDLC 주소 영역 값을 갖는 경우가 얼마인가를 측정한 것이 R_A이다. 즉, R_A는 수신된 HDLC 프레임 중에서 정상적인 주소 영역을 갖는 프레임의 비율을 나타낸다. 그런데 정상적으로 복호되는 경우의 R_A와 난수 동기 이탈이 발생된 경우의 R_A는 많은 차이가 날 것이므로 R_A를 이용하여 난수 동기 이탈의 발생 유, 무를 판단할 수 있을 것이다. 본 논문에서는 매 T_u초 동안 R_A 값을 계산하여 그 값이 정해진 역치(threshold value)보다 크면 정상적인 경우로 판단하여 계속 암호 통신을 수행하고 반대의 경우에는 난수 동기 이탈이 발생된 것으로 판단하여 동기 패턴과 세션 키를 전송하여 재동기를 이루었다. 제안된 적응 재동기 방법의 흐름도는 그림 10에 나타나는데 이를 설명하면 다음과 같다. 먼저 복호된 비트 열에서 프레그 패턴이 찾아지면 HDLC 프레임의 시작이므로 프레그 패턴 다음의 해당 주소 영역 길이 만큼 데이터를 읽어 a_{00}, a_{10}, a_{20}가 정상적인 주소 영역 패턴인 가를 확인한다.

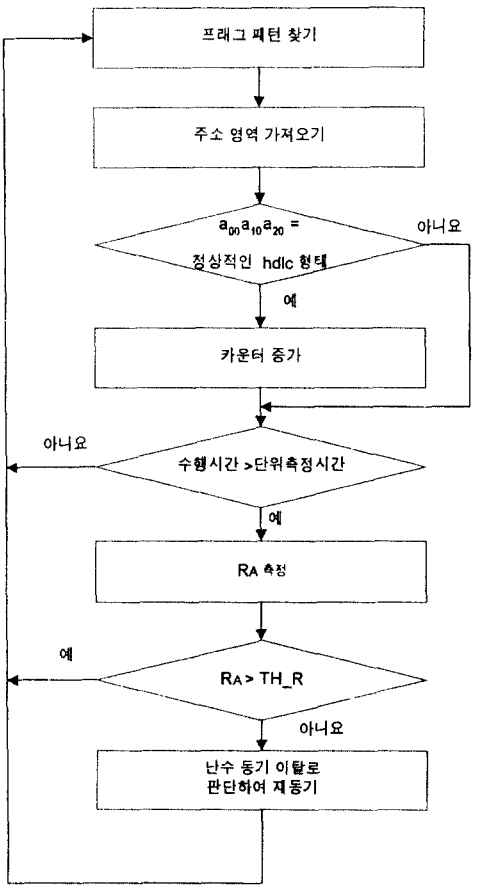

그림 10. 제안된 알고리즘의 흐름도
Fig. 10 The flow chart of proposed algorithm

a_{00}, a_{10}, a_{20}가 표 1에 나타난 HDLC 주소 영역 값을 갖는 경우에는 정상적으로 복호되는 것으로 판단하여 카운터 값을 증가시킨다. 이때, 프레그 패턴 다음에 연속적으로 프레그 패턴이 오는 경우는 동기를 위하여 프레그 패턴을 전송하는 경우로 간주하여 카운터 값을 증가시키지 않았다. 이러한 과정을 단위 측정 시간 T_u초 동안 수행한 후 계산된 R_A가 정해진 역치보다 크면 정상적인 경우로 판단하여 암호 통신을 계속 수행하고 반대의 경우는 난수 동기 이탈이 발생한 것으로 판단하여 동기 패턴과 세션 키를 송, 수신하여 난수 재동기를 취한다. 난수 동기 이탈이 발생된 것으로 판단되면 상대국에게 재동기를 요구하여

야하는데 재동기를 요구하는 방법은 해당 통신 시스템에따라 다를 수 있으나 흔히 데이터 패턴을 이용한다. 즉, 난수 동기 이탈을 감지한 국은 미리 약속된 데이터 패턴을 전송하여 재동기 요구를 하고 상대국에서는 이 데이터 패턴이 수신되면 상대국에서 재동기 요구가 있음을 알고 기존의 연속 재동기 방식에서 초기 동기를 이룰 때와 마찬가지로 동기 패턴과 세션 키를 주고 받아 재동기를 이루면 된다. 본 논문에서도 특정 데이터 패턴을 이용하여 재동기 요구를 하는 방법을 사용하였다.

적응 재동기 방식에서 난수 동기 이탈 발생 후 재동기를 이루는데 소요되는 시간은 단위 측정 시간 T_u의 길이에 의해서 결정되는데, T_u 값은 연속 재동기 방식의 재동기 주기 T_c 값보다 훨씬 적으므로 난수 동기 이탈 발생시 적응 재동기 방식이 연속 재동기 방식에 비해 빨리 재동기를 이룬다. 이것은 적응 재동기 방식을 적용하면 연속 재동기 방식에 비하여 통신을 할 수 없는 구간이 짧아지므로 보다 안정된 암호 통신을 할 수 있다는 것을 의미한다. 또한, 연속 재동기 방식은 난수 동기 이탈 발생과 무관하게 주기적으로 동기 패턴과 세션 키를 전송하여 재동기를 이루는데 반해 적응 재동기 방식은 난수 동기 이탈 현상이 발생한 경우에만 동기 패턴과 세션 키를 전송하여 재동기를 이루므로 동일한 정보를 전송하기 위하여 필요한 동기 패턴과 세션 키 수가 줄어들어 전송 효율을 향상시킬 뿐아니라 연속 재동기 방식에서 세션 키를 주기적으로 전송함으로서 발생되는 문제점도 해결 할 수 있다.

3. R_A의 분포

3.1 정상적인 암호 통신을 하는 경우

암호 통신 중에 발생될 수 있는 상황은 크게 나누어 정상적으로 통신하는 경우와 난수 동기 이탈이 발생하여 복호기에서 정상적으로 복호를 할 수 없는 경우인데 먼저 정상적으로 통신하는 경우의 R_A 값의 분포를 알아보자. 정상적으로 통신하는 경우에는 전송 오류를 무시한다면 $R_A=1$ 이어야 하나 실제로 선로 잡음에 의한 전송 오류는 항상 발생하므로 정상적인 경우에서도 $R_A<1$이다.

이때 R_A에 영향을 미치는 오류는 송신 측에서 프레그 패턴 다음에 전송한 a_{00}, a_{10}, a_{20}가 전송 도중 다른 값으로 변하는 경우인데 이것은 a_{00}, a_{10}, a_{20}에 한 비트 이상의 오류가 발생할 확률과 동일하다. 전송하는 동안 a_{00}, a_{10}, a_{20}에 한 비트 이상의 오류가 일어날 확률 P_E는 아래 식(3)-식(5)와 같이 나타난다. 식(3)-식(5)에서 b는 선로의 BER이다. 식(3)은 주소 영역을 1바이트로 한 경우의 P_E를 나타내는 것으로 a_{00}에 오류가 발생할 확률과 동일하다. 식(4)는 주소 영역을 2바이트로 한 경우의 P_E를 나타내는 것으로 a_{00}, a_{10}에 한 비트 이상의 오류가 발생할 확률과 동일하다. 식(5)는 주소 영역을 3바이트로 한 경우의 P_E를 나타내는 것으로 a_{00}, a_{10}, a_{20}에 한 비트 이상의 오류가 발생할 확률과 동일하다.

$$P_E = b \tag{3}$$

$$P_E = \sum_{i=1}^{2} {}_2C_i\, b^i (1-b)^{2-i} \tag{4}$$

$$P_E = \sum_{i=1}^{3} {}_3C_i\, b^i (1-b)^{3-i} \tag{5}$$

단위 측정 시간 T_u초 동안에 관찰된 프레그 패턴의 수를 N_F라하고, 프레그 패턴 다음의 a_{00}, a_{10}, a_{20}가 표1과 같은 정상적인 HDLC 주소 영역 값인 경우의 수를 N_{FA}라 한다면, N_{FA}는 N_F에 a_{00}, a_{10}, a_{20}가 정상적인 HDLC 주소 영역 값일 확률 P_H를 곱하면 된다. 그런데 P_H는 아래 식 (6)과 같으므로 N_{FA}는 식(7)과 같이 나타난다.

$$P_H = 1 - P_E \tag{6}$$

$$N_{FA} = N_F P_H \tag{7}$$

결과적으로, 난수 동기 이탈이 발생하지 않은 정상적 경우에 전송 오류를 고려한 R_A는 식(2)와 식(7)에 의해서, 주소 영역의 길이에 따라 식(8)-식(10)과 같이 구해진다. 식(8)은 주소 영역이 1바이트인 경우이고 식(9)은 2바이트인 경우 식(10)은 3바이트인 경우에 대한 R_A을 나타낸다.

$$R_A = P_H = 1 - P_E = 1 - b \tag{8}$$

$$R_A = P_H = 1 - P_E = 1 - \sum_{i=1}^{2} {}_2C_i\, b^i (1-b)^{2-i} \tag{9}$$

$$R_A = P_H = 1 - P_E = 1 - \sum_{i=1}^{3} {}_3C_i\, b^i (1-b)^{3-i} \qquad (10)$$

식(8)-식(10)에서 보는 바와 같이 RA는 선로의 BER에 따라 그 값이 변한다. 선로 상태가 나쁠수록 a_{00}, a_{10}, a_{20}에 전송 오류가 발생할 확률이 높아지고 이에 따라 R_A는 감소한다. 그림 11은 BER과 R_A의 관계를 나타내는 것으로 BER이 증가할수록 R_A는 감소함을 알 수 있다.

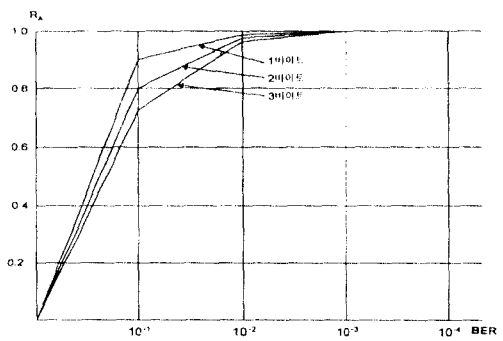

그림 11. BER의 변화에 따른 R_A
Fig 11. R_A for various BER

3.2 난수 동기 이탈이 발생한 경우

속도 v-bps로 암호 통신 중 난수 동기 이탈이 발생하면 복호된 데이터는 임의의 값을 가지므로 복호된 데이터에서 프레그 패턴 '01111110'은 256비트마다 한번씩 발생한다고 가정 할 수 있다. 즉, 난수 동기 이탈이 발생하였을 때 초당 발생할 수 있는 프레그 패턴 '01111110'의 수 n_f는 식 (11)과 같이 나타나므로 단위 측정 시간 T_u초 동안에 발생되는 프레그 패턴의 총 갯수 N_F는 식 (12)와 같다.

$$n_f = \frac{v}{256} \qquad (11)$$

$$N_F = T_u\, n_f \qquad (12)$$

여기서 난수 동기 이탈이 발생하였을 때 a_{00}, a_{10}, a_{20}가 정상적인 HDLC 주소 영역 패턴을 가질 확률을 P_H를 구해보자. 주소 영역을 1바이트로 정하였다면 표 1에 의하여 a_{00}만 '1'이면 된다. 난수 동기가 이탈한 경우에는 복호된 데이터는 임의의 값을 가지므로 '0'과 '1'의 발생 확률을 1/2로 가정할 수 있다. 따라서 a_{00}가 '1'일 확률은 1/2로 정할 수 있으므로 P_H는 1/2이다. 주소 영역을 2바이트를 정하였다면 정상적인 HDLC 주소 영역 패턴을 갖기 위해서는 표 1에 의하여 a_{00}는 '0', a_{10}는 '1'이어야 한다. 따라서, P_H는 a_{00}는 '0', a_{10}는 '1'일 확률과 동일하므로 $(1/2)^2$이다. 또한, 주소영역으로 3바이트를 정하였다면 표 1에 의하여 a_{00}는 0, a_{10}는 0, a_{10}는 1이어야 한다. 따라서, P_H는 a_{00}는 '0', a_{10}는 '0', a_{20}는 '1'일 확률과 동일하므로 $(1/2)^3$이다. 이상의 결과를 정리하면 표 2와 같이 나타난다.

표 2. 난수 동기 이탈이 발생하였을 때의 P_H와 R_A
Table 2. P_H and R_A in case of synchronization loss

주소 종류 / 영역길이	P_H	P_A
1 바이트	$(1/2)$	$(1/2)$
2 바이트	$(1/2)^2$	$(1/2)^2$
3 바이트	$(1/2)^3$	$(1/2)^3$

단위 측정 시간 T_u초 동안에 관찰된 프레그 패턴 N_F개 중에서 프레그 패턴 다음의 a_{00}, a_{10}, a_{20}가 표 1과 같이 정상적인 HDLC 패턴일 경우의 수를 N_{FA}라 한다면, N_{FA}는 N_F에 a_{00}, a_{10}, a_{20}가 정상적인 HDLC 패턴일 확률 P_H를 곱하면 된다. 그런데 P_H는 표 2와 같이 나타나므로 난수 동기 이탈이 발생한 경우의 R_A는 식(2)와 식(7)에 의하여 주소 영역의 길이에 따라 표 2와 같이 구해진다. 표 2에서 보는 바와 같이 난수 동기 이탈이 발생한 경우의 R_A는 선로의 BER에 무관하게 발생되며 주소 영역의 길이에 따라 일정한 값을 갖는다.

3.3 R_A의 역치 결정

링크 계층의 프로토콜로 HDLC를 사용하는 통신 체계에서 운용되는 동기식 스트림 암호 통신에서는 정상적인 경우의 R_A 값과 난수 동기 이탈이 발생된 경우의 R_A의 값은 차이가 많이 나므로 제안된 방법에서는 R_A을 이용하여 난수 동기 이탈 현상을 판단하였다. 즉, 암호 통신 중 매 T_u초 동안 측정한 R_A가 역치보다 크면 정상적인 경우로 간주하여 계속 통신

표 3. 단위 측정 시간 100msec인 경우 적응 재동기 방식의 파라미터 값

Table 3. The parameters in adaptive resynchronization method when Tu is 100msec.

BER	R_A	N_F	N_{FA}
1.0×10^{-1}	0.810	1.37	1.11
1.0×10^{-2}	0.980	2.95	2.89
1.0×10^{-3}	0.997	3.17	3.16
1.0×10^{-4}	1.000	3.19	3.19
1.0×10^{-5}	1.000	3.20	3.20
1.0×10^{-6}	1.000	3.20	3.20
1.0×10^{-7}	1.000	3.20	3.20
1.0×10^{-8}	1.000	3.20	3.20
1.0×10^{-9}	1.000	3.20	3.20

표 4. 단위 측정 시간 500msec인 경우 적응 재동기 방식의 파라미터 값

Table 4. The parameters in adaptive resynchronization method when T_u is 500msec.

BER	R_A	N_F	N_{FA}
1.0×10^{-1}	0.810	6.85	5.55
1.0×10^{-2}	0.980	14.75	14.45
1.0×10^{-3}	0.997	15.85	15.80
1.0×10^{-4}	1.000	15.95	15.95
1.0×10^{-5}	1.000	16.00	16.00
1.0×10^{-6}	1.000	16.00	16.00
1.0×10^{-7}	1.000	16.00	16.00
1.0×10^{-8}	1.000	16.00	16.00
1.0×10^{-9}	1.000	16.00	16.00

표 5. 단위 측정 시간 1sec인 경우 적응 재동기 방식의 파라미터 값

Table 5. The parameters in adaptive resynchronization method when T_u is 1sec.

BER	R_A	N_F	N_{FA}
1.0×10^{-1}	0.810	13.70	11.09
1.0×10^{-2}	0.980	29.51	28.90
1.0×10^{-3}	0.997	31.70	31.60
1.0×10^{-4}	1.000	31.91	31.91
1.0×10^{-5}	1.000	32.00	32.00
1.0×10^{-6}	1.000	32.00	32.00
1.0×10^{-7}	1.000	32.00	32.00
1.0×10^{-8}	1.000	32.00	32.00
1.0×10^{-9}	1.000	32.00	32.00

하고 반대의 경우는 난수 동기 이탈이 발생한 것으로 판단하여 재동기를 이루도록 하였다. 그런데 표 2에서 보는 바와 같이 난수 동기 이탈이 발생된 경우의 R_A는 선로 상태에 무관하게 거의 일정한 값을 갖지만 정상적인 경우는 식(8)-식(10)에서 보는 바와 같이 R_A가 선로의 BER에 영향을 받는다. 따라서 난수 동기 이탈 여부를 판단하기 위한 R_A의 역치는 해당 선로 조건에서 난수 동기 이탈이 발생한 경우와 발생하지 않은 경우를 명확히 구분할 수 있도록 정하여야 한다.

표 3-표 5는 9,600bps의 속도로 정상적인 암호 통신을 할 때 T_u와 BER을 변화시키면서 측정한 R_A, N_F, N_{FA}를 나타낸다. 이때, 주소 영역 길이는 2바이트로 하였다. N_F는 T_u초 동안 수신 측에서 감지된 프레그 패턴 '01111110'의 갯수를 의미하는데 이것은 T_u초 동안 송신 측에서 전송한 프레그 패턴 중에서 전송 오류없이 수신 측에 도착한 프레그 패턴 갯수와 동일하므로 평균적으로 식 (14)과 같이 구해진다. 여기서 P_C는 식 (13)과 같이 나타나는데 프레그 패턴 8비트가 BER이 b인 선로를 통하여 전송될 때 오류없이 전송될 확률을 의미한다. 따라서 N_F는 N_{avg}에 P_C와 T_u를 곱하면 된다. 식 (14)에서 N_{avg}는 송신 측에서 초당 발생하는 프레그 패턴의 평균 갯수를 말하는 것으로 본 논문에서는 32회로 정하였는데 이것은 HDLC 프로토콜을 사용하는 패킷 통신망에서 수집한 데이터를 분석한 결과이다. 이때, 연속적으로 프레그 패턴이 전송되는 경우에는 동기를 위한 프레그로 간주하여 계산에서 제외하였다.

$$P_C = 1 - \sum_{i=1}^{8} {}_8C_i\, b^i (1-b)^{8-i} \tag{13}$$

$$N_F \cong T_u\, N_{avg}\, P_C \tag{14}$$

표 3-표 5에 나타난 바와 같이 난수 동기 이탈이 발생하지 않은 정상적인 경우에 단위 측정 시간 길이를 변화시키면 N_F, N_{FA}는 차이가 있으나 R_A 값은 일정하다. 그런데, 동기 이탈이 발생한 경우의 RA 값은 표 2에 나타난 바와 같이 BER에 관계없이 일정할 뿐 아니라 정상적인 경우의 R_A 값과 차이가 많으므로 두 상태를 구분할 수 있도록 역치를 결정하는 것이 가능한데 이 역치를 TH R로 정의한다. 그림 12는 단

위 측정 시간 T_u를 0.5초로 설정한 경우의 R_A를 그린 것인데 굵은 선으로 표시된 것이 TH_R을 나타낸다. 제안된 적응 재동기 방식은 매 T_u초 동안 측정한 R_A가 TH_R 보다 큰 경우는 정상 상태로 판정하고 반대의 경우는 난수 동기 이탈 상태로 판정하여 동기 패턴과 세션 키를 전송하여 난수 재동기를 이룬다. 그런데 그림 12에서 TH_R 값을 크게 정할 수록 난수 동기 이탈이 발생하였는데 이를 감지 못하는 경우는 줄어들 것이나 정상적인 경우를 난수 동기 이탈로 잘못 판단하는 경우는 늘어날 것이다. 반면에, TH_R 값을 적게 정할 수록 정상적인 경우를 난수 동기 이탈로 잘못 판단하는 경우가 줄어들 것이나 난수 동기 이탈을 감지 못하는 경우는 늘어날 것이다. 따라서 TH_R은 해당 암호 시스템의 요구에 따라 적정하게 정하면 되나 본 논문에서는 TH_R 값을 0.4로 정하여 정상적인 경우를 난수 동기 이탈로 잘못 판단하는 경우를 줄이도록 하였다. 왜냐하면 난수 동기 이탈 현상이 발생하였을 때의 R_A 값은 표 2에서 보는 바와 같이 BER에 무관하게 일정한 반면에 정상적인 경우의 R_A 값은 선로의 BER에 따라 그 값이 변하므로 선로 상태가 감사기 악화되는 경우에는 정상적인 경우를 난수 동기 이탈이 발생한 것으로 잘못 판단할 확률이 증가하므로 이를 줄이기 위한 것이다. 본 논문에서는 그림 12의 굵은 선으로 나타난 것을 TH_R로 정하였는데 TH_R 값과 정상적인 경우의 R_A 곡선이 만나는 점 Q의 왼쪽 부분 즉 그림 12에서의 빗금친 부분은 정상적인 경우를 난수 동기 이탈이 발생한 것으로 잘못 판단할 경우이다. 그런데 그림 12에서 빗금친 부분에 해당되는 선로의 BER을 보면 0.35이상인데 이것은 10비트 전송하면 3비트 내지 4비트 이상의 오류를 일으키는 매우 열악한 상태이므로 이러한 상황이 통신 도중 발생할 확률은 매우 적으며 만일 발생하여도 이러한 열악한 상황에서 정상적인 암호 통신을 행할 수 없을 것으로 예상된다. 따라서 이 경우에는 비록 정상적인 경우라 하더라도 난수 동기 이탈이 발생한 경우로 판단하여 재동기를 이루는 것이 오히려 효율적일 수 있다.

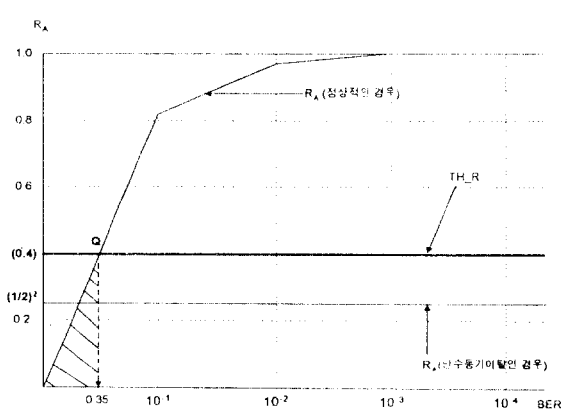

그림 12. T_u=0.5초인 경우 BER의 변화에 따른 R_A
Fig 12. R_A for various BER in case that T_u is 0.5sec.

V. 실험 결과 및 고찰

1. 실험 방법

기존의 연속 재동기 방식과 제안된 적응 재동기 방식의 성능을 비교하기 위하여 식 (15)와 같이 표시되는 오복호율 R_e와 복호기에서 잘못 복호된 데이터양 D_e, 그리고 재동기를 위하여 필요한 잉여 비트 전송량 D_r를 이용하였다.

$$R\_e = \frac{D\_e}{D\_t} \tag{15}$$

여기서 D_t는 암호기가 전송한 총 데이터의 비트 수이며 D_e은 잘못 복호된 데이터의 비트 수이다.

R_e는 전송한 총 데이터와 복호기에서 잘못 복호된 데이터 비를 나타내고 D_e는 잘못 복호된 데이터 비트 수를 나타내므로 R_e와 D_e가 낮을수록 난수 동기 이탈을 정확하고 신속하게 감지하여 재동기를 이룬다는 것을 의미한다. 따라서, 연속 재동기 방식과 적응 재동기 방식의 성능은 동일한 선로 조건과 난수 동기 이탈 조건에서 R_e와 D_e를 비교하면 알 수 있다. 또한, 동일한 양의 데이터를 암호 통신을 이용하여 전송할 때 재동기를 위하여 필요한 잉여 데이터 비트 수 D_r를 이용하여 두 방법의 통신 효율을 비교하였다. 이때, 재동기를 위하여 전송하는 동기 패턴은 128비트로 하였고 세션 키는 256비트를 (15, 4) 에러 정정 부호화 하여 전송하는 것으로 하였으며[13] HDLC 프레임의 주소 영역 부의 길이는 2바이트로 확장한 것으로 가정하였다. 그림 13과 같이 구성된 동기식 스트림 암호 통신 시스템에 10^9-3*10^9 비트의 특정

패턴으로 구성된 데이터를 송, 수신하면서 10^{-6}, 10^{-7}, 10^{-8} 비트의 발생률로 난수 동기 이탈을 발생시켰는데 난수 동기 이탈은 그림 6의 연속 재동기 방식의 구성 중에서 동기 패턴과 세션 키 부분에서는 발생치 않고 암호문의 임의의 부분에서만 발생하도록 하였다. 또한 선로의 BER, 통신 속도, 난수 동기 이탈 발생률 등이 제안된 적응 재동기 방법에 어떤 영향을 미치는 가를 알아보기 위하여 BER은 $10^{-4}-10^{-8}$ 비트, 통신 속도는 9,600-28,800bps, 난수 동기 이탈 율은 $10^{-6}-10^{-8}$비트의 범위에서 변화를 가하면서 실험하였다.

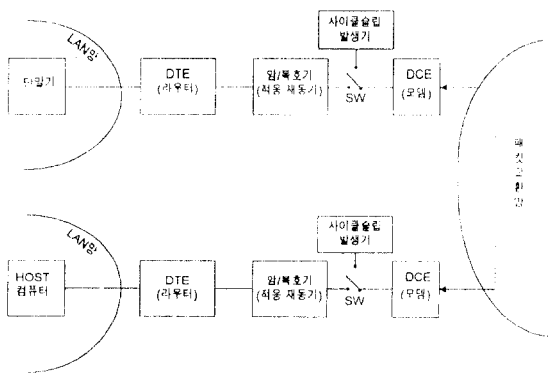

그림 13. 실험에 사용된 동기식 스트림 암호 통신 시스템
Fig. 13. The secure communication system be used in simulation.

2. 결과 및 고찰

표 6-표 11은 동기식 스트림 암호 통신 시스템에 기존의 연속 재동기 방식을 적용한 경우와 제안된 적응 재동기 방식을 적용한 경우에 대하여, 통신 속도 9.600bps에서는 10^9 비트의 특정 데이터 패턴을, 통신 속도 28,800bps에서는 $3*10^9$ 비트의 특정 데이터 패턴을 암호화하여 전송한 후 복호기에서 복호하는 시험을 각 속도에 대하여 10회 실시한 후에 측정된 Re와 De의 평균값을 나타낸다. 이때, 연속 재동기 방식에서 사용한 재동기 주기 T_c는 10초로 하였는데 T_c를 너무 길게 하면 동기 이탈시 재동기까지의 시간이 길어져 복호율이 떨어지고, 너무 짧게 하면 동기 신호와 세션 키를 자주 전송하여야 하므로 부가 정보가 많아져 통신 효율이 떨어지는 단점이 있으므로 시스템 설계시 주기 T_c는 해당 통신 시스템의 특성에 따라 적절히 결정하여야 한다. 표 6-표 11은 선로의 평균 BER이 10^{-6}인 경우에 측정한 결과이며 이때 사용한 적응 재동기 방식에서의 RA의 역치 TH_R는 그림 12에서 0.4로 하였다. 표 6-표 11에서 보는 바와 같이 적응 재동기 방법이 연속 재동기 방식에 비해 난수 동기 이탈 율에 무관하게 R_e와 D_e가 훨씬 감소됨을 알 수 있는데 이것은 적응 재동기 방법이 동기 이탈 후 재동기를 이루는데 소요되는 시간이 훨씬 짧기 때문이다. 즉, 연속 재동기 방식을 사용한 경우에는 동기 이탈이 발생하여 재동기를 이루는데 소요되는 시간은 평균적으로 $T_c/2$이나 적응 재동기 방식을 적용한 경우는 평균적으로 단위 측정 시간 T_u가 경과하면 재동기를 이룬다고 볼 수 있다. 그런데 T_u는 T_c보다 훨씬 적게 정하였으므로 적응 재동기 방식을 적용하였을 때가 훨씬 빠르다. 이 두 경우의 재동기 소요 시간 비 T_rate를 식으로 나타내면 식 (16)와 같다.

$$T\_rate \cong \frac{T_c}{2T_u} \tag{16}$$

여기서 T_c는 연속 재동기 주기이고 T_u는 적응 재동기의 단위 측정 시간이다.

식 (16)에서 보는 바와 같이 T_c를 10초로 하고 T_u를 약 0.5초로 하였을 경우에는 T_rate=10이다. 즉, 적응 재동기 방식이 기존의 연속 재동기 방식에 비하여 재동기를 이루는데 소요되는 시간이 10배나 빠르다는 것을 나타낸다. 이것은 표 6-표 11에서 나타나는 것과 같이 동일한 사이클 슬립 발생률에서 오복호율 R_e와 오복호된 데이터 비트 수 D_e를 10배 감소시켜 수신 측에서 훨씬 정확한 데이터를 얻을 수 있다는 것을 말한다.

표 12와 표 14에서 보는 바와 같이 연속 재동기 방식은 재동기 주기 T_c에 따라 요구되는 총 잉여 비트 수인 D_r이 달라진다. 재동기 주기 T_c를 길게 하면 D_r은 줄어드나 난수 동기 이탈 기간이 길어지고 재동기 주기 T_c를 짧게 하면 D_r은 증가하지만 난수 동기 이탈 기간은 짧아진다. 표 12와 표 14의 결과를 보면 연속 재동기 주기 T_c가 10초인 경우는 0.5초인 경우에 비하여 약 2.15x108 비트의 잉여 비트 감축 효과가 있다. 반면에, 표 13과 표 15에서 나타난 바와 같이 적응 재동기 방식에서의 재동기를 위한 잉여 비트 수는 난수 동기 이탈 율에만 영향을 받는다. 적응 재

표 6. 통신 속도 9,600bps일 때 제안된 적응 재동기 방식에서의 단위 측정 시간 T_u의 변화에 따른 D_e와 R_e의 비교
Table 6. The comparison of D_e and R_e in case that speed is 9,600bps and period of resynchronization, T_u, is various in adaptive resynchronization method.

사이클 슬립발생률	제안된 적응 재동기 방식 (단위측정시간 = 100mesc)		제안된 적응 재동기 방식 (단위측정시간 = 500mesc)		제안된 적응 재동기 방식 (단위측정시간 = 1sec)	
	D_e (bits)	R_e (%)	D_e (bits)	R_e (%)	D_e (bits)	R_e (%)
10^{-6}	9.6×10^{5}	9.6×10^{-2}	4.8×10^{6}	4.8×10^{-1}	9.6×10^{6}	9.6×10^{-1}
10^{-7}	9.6×10^{4}	9.6×10^{-3}	4.8×10^{5}	4.8×10^{-2}	9.6×10^{5}	9.6×10^{-2}
10^{-8}	9.6×10^{3}	9.6×10^{-4}	4.8×10^{4}	4.8×10^{-3}	9.6×10^{4}	9.6×10^{-3}

표 7. 통신 속도 9,600bps일 때 연속 재동기 방식에서 재동기 주기 T_u의 변화에 따른 D_e와 R_e의 비교
Table 7. The comparison of D_e and R_e in case that speed is 9,600bps and period of resynchronization, T_u, is various in continuous resynchronization method.

사이클 슬립발생률	연속 재동기 방식 (T = 1초)		연속 재동기 방식 (T = 5초)		연속 재동기 방식 (T = 1초)	
	D_e (bits)	R_e (%)	D_e (bits)	R_e (%)	D_e (bits)	R_e (%)
10^{-6}	4.8×10^{7}	4.8×10^{0}	2.4×10^{7}	2.4×10^{-0}	4.8×10^{6}	4.8×10^{-1}
10^{-7}	4.8×10^{6}	4.8×10^{-1}	2.4×10^{5}	2.4×10^{-1}	4.8×10^{5}	4.8×10^{-2}
10^{-8}	4.8×10^{5}	4.8×10^{-2}	2.4×10^{5}	2.4×10^{-2}	4.8×10^{4}	4.8×10^{-3}

표 8. 통신 속도 9,600bps일 때 연속 재동기 방식과 제안된 적응 재동기 방식의 D_e과 R_e의 비교
Table 8. The comparison of D_e and R_e in case of 9,600bps for adaptive resynchronization and continuous resynchronization method.

사이클 슬립발생률	연속 재동기 방식 (재동기주기 = 10초)		제안된 적응 재동기 방식 (단위측정시간 = 0.5초)		제안된 적응 재동기 방식 (단위측정시간 = 1초)	
	D_e (bits)	R_e (%)	D_e (bits)	R_e (%)	D_e (bits)	R_e (%)
10^{-6}	4.8×10^{7}	4.8×10^{0}	4.8×10^{6}	4.8×10^{-1}	9.6×10^{6}	9.6×10^{-1}
10^{-7}	4.8×10^{6}	4.8×10^{-1}	4.8×10^{5}	4.8×10^{-2}	9.6×10^{5}	9.6×10^{-2}
10^{-8}	4.8×10^{5}	4.8×10^{-2}	4.8×10^{4}	4.8×10^{-3}	9.6×10^{4}	9.6×10^{-3}

동기 방식은 난수 동기 이탈이 발생된 경우에만 동기 패턴과 세션 키를 전송하여 재동기를 이루므로, 적응 재동기 방식의 재동기 주기는 해당 선로의 난수 동기 이탈 발생 주기와 거의 일치 할 것이다. 난수 동기 이탈 주기가 연속 재동기 방식의 재동기 주기보다 훨씬 길므로 적응 재동기 방식이 연속 재동기 방식보다 재동기를 위하여 필요한 잉여 비트 수가 훨씬 적다. 표 6와 표 7에서 보면 단위 측정 시간 0.5초인 적응 재동기 방식과 재동기 주기 1초인 연속 재동기 방식이 동일한 D_e와 R_e를 나타내는 것으로 나타낸다. 그런데, 표 12와 표 13에서 보면 10^{9} 비트의 데이터를 9,600bps로 재동기 주기 1초인 연속 재동기 방식으로 전송하는데 소요되는 총 잉여 비트 수는 1.13×10^{8} 비트이나 단위 측정 시간 0.5초인 적응 재동기 방식으로 전송 할 때는 난수 동기 이탈 율이 10^{-7} 비트라 가정한다면 1.09×10^{5} 비트만 있으면 된다. 즉, 동일한

표 9. 통신 속도 28,800bps인 경우의 제안된 적응 재동기 방식에서의 단위 측정 시간 T_u의 변화에 따른 D_e와 R_e의 비교

Table 9. The comparison of D_e and R_e in case that speed is 28,800bps and period of resynchronization, T_u, is various in adaptive resynchronization method.

사이클 슬립발생률	제안된 적응 재동기 방식 (단위측정시간 = 200msec)		제안된 적응 재동기 방식 (단위측정시간 = 500msec)		제안된 적응 재동기 방식 (단위측정시간 = 1sec)	
	D_e (bits)	R_e (%)	D_e (bits)	R_e (%)	D_e (bits)	R_e (%)
10^{-6}	1.8×10^{7}	6.0×10^{-1}	4.4×10^{5}	1.4×10^{-0}	8.7×10^{7}	2.9×10^{-0}
10^{-7}	1.8×10^{6}	6.0×10^{-2}	4.4×10^{6}	1.4×10^{-1}	8.7×10^{6}	2.9×10^{-1}
10^{-8}	1.8×10^{5}	6.0×10^{-3}	4.4×10^{5}	1.4×10^{-2}	8.7×10^{5}	2.9×10^{-2}

표 10. 통신 속도 28,800bps인 경우의 연속 재동기 방식에서 재동기 주기 T_u의 변화에 따른 R_e와 D_e의 비교

Table 10. The comparison of D_e and R_e in case that speed is 28,800bps and period of resynchronization, T_u, is various in continuous resynchronization method.

사이클 슬립발생률	연속 재동기 방식 (T = 5초)		연속 재동기 방식 (T = 0.5초)		연속 재동기 방식 (T = 0.5초)	
	D_e (bits)	R_e (%)	D_e (bits)	R_e (%)	D_e (bits)	R_e (%)
10^{-6}	4.3×10^{8}	1.4×10^{2}	2.1×10^{8}	7.0×10^{0}	2.1×10^{7}	7.0×10^{-1}
10^{-7}	4.3×10^{7}	1.4×10^{1}	2.1×10^{7}	7.0×10^{-1}	2.1×10^{6}	7.0×10^{-2}
10^{-8}	4.3×10^{6}	1.4×10^{-1}	2.1×10^{6}	7.0×10^{-2}	2.1×10^{5}	7.0×10^{-3}

표 11. 통신 속도 28,800bps일 때 연속 재동기 방식과 제안된 적응 재동기 방식의 D_e와 R_e의 비교

Table 11. The comparison of D_e and R_e in case of 28,800bps for adaptive resynchronization and continuous resynchronization method.

사이클 슬립발생률	연속 재동기 방식 (재동기주기 = 10초)		제안된 적응 재동기 방식 (단위측정시간 = 0.2초)		제안된 적응 재동기 방식 (단위측정시간 = 1초)	
	D_e (bits)	R_e (%)	D_e (bits)	R_e (%)	D_e (bits)	R_e (%)
10^{-6}	4.8×10^{8}	1.4×10^{1}	1.8×10^{7}	6.0×10^{-1}	8.7×10^{7}	2.9×10^{0}
10^{-7}	4.8×10^{7}	1.4×10^{0}	1.8×10^{6}	6.0×10^{-2}	8.7×10^{6}	2.9×10^{-1}
10^{-8}	4.8×10^{6}	1.4×10^{-1}	1.8×10^{5}	6.0×10^{-3}	8.7×10^{5}	2.9×10^{-2}

표 12. 통신 속도 9,600bps 일 때 연속 재동기 방식으로 10^9 비트의 데이터 전송 시에 요구되는 잉여 비트 수의 비교.

Table 12. The comparison of total dummy bits in 9,600bps when 10^9 bits is transmitted by continuous resynchronization method.

연속재동기방식 (재동기주기 = 10초)	연속재동기방식 (재동기주기 = 5초)	연속재동기방식 (재동기주기 = 1초)	연속재동기방식 (재동기주기 = 0.5초)
1.13×10^{7} (bits)	2.27×10^{7} (bits)	1.13×10^{8} (bits)	2.27×10^{8} (bits)

표 13. 통신 속도 9,600bps 일 때 적응 재동기 방식으로 10^9 비트의 데이터 전송 시에 요구되는 잉여 비트 수의 비교.
Table 13. The comparison of total dummy bits in 9,600bps when 10^9 bits is transmitted by adaptive resynchronization method.

적응 재동기 방식 (난수동기이탈율 = 10^{-6})	적응 재동기 방식 (난수동기이탈율 = 10^{-7})	적응 재동기 방식 (난수동기이탈율 = 10^{-8})
1.09 x 10^6 비트	1.09 x 10^5 비트	1.09 x 10^4 비트

표 14. 통신 속도 28,800bps일 때 연속 재동기 방식으로 $3*10^9$ 비트의 데이터 전송 시에 요구되는 잉여 비트 수의 비교.
Table 14. The comparison of total dummy bits in 28,800bps when $3*10^9$ bits is transmitted by continunous resynchronization method.

연속재동기방식 (재동기주기 = 10초)	연속재동기방식 (재동기주기 = 5초)	연속재동기방식 (재동기주기 = 1초)	연속재동기방식 (재동기주기 = 0.5초)
1.13×10^7(bits)	2.27×10^7(bits)	1.13×10^8(bits)	2.27×10^8(bits)

표 15. 통신 속도 28,800bps일 때 적응 재동기 방식으로 $3*10^9$ 비트의 데이터 전송시에 요구되는 잉여 비트 수의 비교.
Table 15. The comparison of total dummy bits in 9,600bps when $3*10^9$ bits is tansmitted by adaptive resynchronization method.

적응 재동기 방식 (난수동기이탈율 = 10^{-6})	적응 재동기 방식 (난수동기이탈율 = 10^{-7})	적응 재동기 방식 (난수동기이탈율 = 10^{-8})
3.27 x 10^6 비트	3.27 x 10^5 비트	3.27 x 10^4 비트

D_e와 R_e를 목표로 할 때, 적응 재동기 방식을 사용하면 연속 재동기 방식에 비해 10^9 비트의 데이터를 전송하는 경우에 약 1.13×10^8의 잉여 비트를 줄일 수 있다. 또한, 28,800bps로 전송하는 경우에도 마찬가지의 결과가 나타난다. 표 10과 표 11에서 나타난 것처럼 단위 측정 시간 0.2초인 적응 재동기 방식과 재동기 주기 0.5초인 연속 재동기 방식이 비슷한 D_e와 R_e를 나타내지만 표 14와 표 15에서 보면 3×10^9 비트의 데이터를 28,800bps로 재동기 주기 0.5초인 연속 재동기 방식으로 전송하는데 소요되는 총 잉여 비트 수는 2.27×10^8 비트이나 단위 측정 시간 0.2초인 적응 재동기 방식으로 전송 할 때는 난수 동기 이탈 율이 10^{-7} 비트라 가정한다면 3.27×10^5 비트 만 있으면 된다. 즉, 동일한 D_e와 R_e를 목표로 하였을 때, 적응 재동기 방식을 사용하면 연속 재동기 방식에 비해 3×10^9 비트의 데이터를 전송 할 때 약 2.27×10^8 비트의 잉여 비트 수를 줄일 수 있다. 이것은 전송하여야 할 총 데이터 량에서도 10^9 비트의 데이터를 9,600bps로 전송하는 경우에는 약 11.3%의 감축 효과를 얻을 수 있고 3×10^9 비트의 데이터를 28,800bps로 전송할 경우에는 약 7.6%의 감축 효과를 얻을 수 있는 것을 의미한다. 본 논문에서는 속도의 변화에 관계없이 연속 재동기 방식의 재동기 주기 T_c의 값을 일정하게 하였으나 속도가 증가할수록 연속 재동기 방식의 재동기 주기 T_c는 짧게 하여야 하므로 데이터 감축 효과는 더욱 증가할 것으로 예측된다.

Ⅵ. 결 론

본 논문에서는 OSI 7계층 중 링크 계층의 프로토콜로 HDLC를 사용하는 통신 체계에서 운용되는 동기식 스트림 암호 통신 시스템에 적합하고 연속 재동기 방식의 문제점들을 해결 할 수 있는 적응 재동기 알고리즘을 제안하였다. 제안된 방법에서는 각 단위 측정 시간마다 HDLC 프레임의 주소 영역 수신률을 측정하여 난수 동기 이탈이 발생된 경우에만 동기 패턴과 세션 키를 전송하여 재동기를 이루는 적응 재동기 방법을 사용하였다. 적응 재동기 방법을 적용하면, 난수 동기 이탈이 발생된 후 재동기까지의 소요 기간이 줄어들어 통신을 할 수 없는 기간이 감소되어 보다

안정된 암호 통신을 가능하게 하였다. 또한, 적응 재동기 방법은 난수 동기 이탈이 발생한 경우에만 동기 패턴과 세션 키를 전송하므로 전송 효율을 향상시키고 주기적으로 세션 키를 발생하는 부담을 줄일 수 있다. 제안된 알고리즘을 HDLC 프로토콜을 사용하는 동기식 스트림 암호 통신 시스템에 적용하여 시험한 결과 연속 재동기에 비해 오복호율 R_e와 오복호된 데이터 비트 수 D_e를 평균적으로 10배 감소시켰는데 이것은 전송하여야 할 데이터의 총량을 최대 11.3%까지 감축하는 효과를 나타낸다. 제안된 적응 재동기 알고리즘을 HDLC 프로토콜 또는 이와 유사한 주소 체계의 링크 프로토콜을 사용하는 유, 무선 암호 통신에 적용한다면 보다 안정되고 효율적인 암호 통신을 할 수 있을 것으로 예상된다.

참 고 문 헌

1. B. Schneier, "Applied Cryptography: protocols, algorithm, and source code in C", John Willy & Son, 1993.
2. G. Ascheid and H. Meyr, "Cycle slips in Phase-Locked Loops: A Tutorial Survey", IEEE Transactions on Communications, vol. 30, No. 10, pp. 2228-2241, October 1982.
3. H. Meyr and G. Ascheid, "Synchronization in Digital Communications vol.1", John Wieley & Sons, 1990.
4. R. A. Rueppel, "Analysis and Design of Stream Ciphers", Springer-Verlag, 1986.
5. J. Daemen, R. Govaerts, J. Vandewalle, "Resynchronization Weaknesses in Synchronous Stream ciphers," Pre-proceedings of EUROCRYPT'93, pp. T9-T17 1993.
6. W. Stallings, "Data and Computer Communications", Macmillan Publishing Company, 1994.
7. ISO 3309 High-level Data Link Control(HDLC)-Frame Structure, fourth edition, 1991.
8. B. N. Jain, A. K. Agrawala, "Open Systems Interconnection", McGraw-Hill, 1993.
9. W. Stallings, "Network and Internetwork Security Principles and Practice", Prentice-Hall, 1995.
10. M. Y. Lee, "Cryptography and Secure Communications", McGraw-Hill, 1994.
11. D. W. Davies, W. L. Price, "Security for Computer Networks", John Wiley & Sons, 1989.
12. D. J. Torrieri, "Principles of Secure Communication Systems", Artech House, 1992.
13. M. Y. Lee, "Error-Correcting Coding Theory", McGraw-Hill, 1989.

윤 장 홍(Jang Hong Yoon)정회원

1982년 2월 : 경북대학교 전자공학과 졸업(공학사)

1987년 2월 : 경북대학교 전자공학과 대학원 졸업(공학석사)

1993년 3월~현재 : 경북대학교 전자공학과 박사과정

1987년 2월~현재 : 국방과학연구소 근무

※주관심분야 : 컴퓨터 통신, 암호 통신

황 찬 식(Chan Sik Hwang)정회원

1977년 2월 : 서강대학교 전자공학과 졸업(공학사)

1979년 8월 : 한국과학기술원 전기전자공학과 졸업(공학석사)

1996년 2월 : 한국과학기술원 전기전자공학과 졸업(공학박사)

1979년 9월~현재 : 경북대학교 전기전자공학부 교수

1991년 8월~1992년 8월 : Univ. of Texas 전기전자공학부 Visiting Prof.

※주관심분야 : 데이터 통신, 초고속 통신, 암호 통신