論文 97-22-10-9

LAPB의 주소 영역을 이용한 적응 난수열 재동기 알고리즘

正會員 윤 장 홍*, 이 주 형*, 황 찬 식**, 양 상 운*

An adaptive keystream resynchronization algorithm by using address field of LAPB

Jang-Hong Yoon*, Joo-Heng Lee*, Chan-Sik Hwang**,
Sang Woon Yang* *Regular Members*

요 약

동기식 스트림 암호 통신 시스템은 수신 클럭의 사이클 슬립 등에 의하여 난수 동기 이탈을 발생하는 문제점을 갖고 있다. 난수 동기 이탈이 발생하면 통신을 할 수 없을 뿐 아니라 복호된 데이터는 임의의 값을 가지므로 수신 시스템을 오 동작시킬 수도 있다. 이러한 위험성을 줄이기 위하여 암호문에 동기 신호와 세션 키이를 일정 간격으로 삽입하여 주기적으로 재동기를 이루는 연속 재동기 방식을 사용한다. 연속 재동기 방식을 사용하면 비교적 안정된 암호 통신을 할 수 있으나 몇 가지 문제점을 갖고 있다. 본 논문에서는 LAPB 프로토콜을 사용하는 암호 통신 시스템에 적합하고 연속 재동기 방식의 문제점 들을 해결 할 수 있는 적응 재동기 방식을 제안하였다. 제안된 적응 재동기 방식은 단위 측정 시간 동안 측정된 LAPB 프레임의 주소 영역 수신률이 문턱 값보다 적은 경우에만 재동기를 이루는 방법을 사용하여 주기적으로 재동기를 이루는 기존의 연속 재동기 방식의 문제점들을 해결하였다. 제안된 알고리즘을 LAPB 프로토콜을 사용하는 X.25 패킷 암호 통신에서 운용되는 동기식 스트림 암호 통신 시스템에 적용하여 시험한 결과, 연속 재동기에 비해 오 복호율 E_rate와 오 복호된 데이터 비트 수 E_data에서 10배 향상시켰는데 이것은 전송하는 총 데이터 량을 약 11.3% 감축시키는 효과와 동일하다.

ABSTRACT

The synchronous stream cipher has the problem of synchronization loss by cycle slip. Synchronization loss make the state which sender and receiver can't communicate and it may make the receiving system disordered. To lessen the risk, we usually use a continuous resynchronization which achieve resynchronization at fixed timesteps by inserting synchronization pattern and session key. While we can get effectively resynchronization by continuous

*국방과학연구소
**경북대학교 전기전자공학부
論文番號:97191-0604
接受日字:1997年 6月 4日

resynchronization, there are some problems. In this paper, we proposed an adaptive resynchronization algorithm for cipher system using LAPB protocol. It is able to solve the problem of the continunous resynchronization. The proposed adaptive algorithm make resynchronization only in the case that the resynchronization is occurred by analyzing the address field of LAPB. It measure the receiving rate of the address field in the decesion duration. If the receiving rate is smaller than threshold value, it make resynchronization or not. By using adaptively resynchronization, it solves the problems of continunous resynchronization. When the proposed adaptive algorithm is applied to the synchronous stream cipher system which is used in X.25 packet network, it reduced the time for resynchronization by ten times. It means that 11.3% of total data for transmit is compressed.

Ⅰ. 서 론

최근 정보화 사회로 변화함에 따라 컴퓨터나 통신 매체 등을 이용한 정보 교환이 증가하면서 전송되는 정보의 보호 문제가 매우 중요시 되고 있다. 이에 대한 대책으로 컴퓨터 네트워크나 통신 네트워크를 통하여 중요 정보를 전송할 때 비인가자의 도용이나 도청 또는 정보 파괴 및 변조 등으로 부터 보호하기 위하여 암호기로 암호화하여 전송하고 복호기에서 이를 해독하여 인가자 만이 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. 동기식 스트림 암호 통신 시스템에서는 대부분 수신 클럭의 사이클 슬립에 의하여 난수 동기 이탈 현상이 발생되는데[1-2] 난수 동기 이탈이 발생되면 복호기는 정상적으로 복호하지 못하여 서로 통신하지 못할 뿐 아니라 복호된 데이터는 임의의 값을 가지므로 수신 시스템을 오 동작 시킬 수 있다[3-4]. 이러한 위험성을 줄이기 위하여 동기식 스트림 암호 통신 시스템에서는 동기 패턴과 세션 키를 주기적으로 전송하여 암, 복호기의 난수열을 일치 시키는 연속 재동기 방식을 사용하지만 몇가지 문제점 들이 있다[5].

본 논문에서는 OSI(Open System Interconnection) 7계층 중 LINK 계층의 프로토콜로 LAPB(Link Access Procedure Balanced)를 사용하는 암호 통신 시스템에 적합하고 연속 재동기 방식의 문제점 들을 해결할 수 있는 적응 재동기 방식을 제안하였다. 제안된 방법에서는 LAPB 프레임의 주소 영역의 특성을 이용하여 난수 동기 이탈이 발생된 경우에만 동기 패턴과 세션 키를 전송하여 재동기를 이루는 방법을 사용하였다. LAPB 프레임의 주소 영역은 정상적으로 복호되는 경우는 DTE(Data Terminal Equipment)와 DCE(Data Circuit Equipment)를 구분하여 주는 일정한 값을 가지나[6] 난수 동기 이탈이 발생된 경우는 임의의 값을 나타낼 것이므로 단위 측정 시간 동안 복호된 LAPB 프레임의 주소 영역 값의 분포를 구하여 난수 동기 이탈 현상이 발생된 것으로 판단된 경우에만 동기 패턴과 세션 키를 전송하여 재동기를 이루는 방법을 사용하였다. 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 안정된 암호 통신을 할 수 있다. 제안된 방법의 성능을 평가하기위하여 LAPB 프로토콜을 사용하는 X.25 패킷 통신망에서 운용되는 동기식 스트림 암호 통신 시스템에 적용하여 시험하였다. 시험은 전화선이나 음성망을 이용하여 데이터 통신 할 때 주로 사용하는 9,600 28,800bps 급의 모뎀을 통하여 전송하면서 사이클 슬립 발생기로 난수 동기 이탈을 인위적으로 발생시키면서 제안된 적응 재동기 방식이 얼마나 효과적으로 재동기를 이루는 가를 알아보았다.

Ⅱ. 동기식 스트림 암호 방식에서의 기존의 연속 재동기 방식

동기식 스트림 암호 방식에서 사용되는 재동기 방법 중의 하나인 연속 재동기 방식은, 그림 1과 같이 암, 복호기가 주기적으로 동기 패턴과 세션 키를 주고 받아 서로 동일한 세션 키로 난수열 발생기의 internal state 값을 주기적으로 동일하게 만들어 재동기를 이룬다[5]. 이러한 연속 재동기 방식은 난수 동기 이탈이 발생하여도 주기적으로 재동기를 이루므로 비교적 안정된 통신을 가능하게 하지만 몇가지 문제점 들이 있다. 첫째, 그림 1에서 보는 바와 같이 연속 재동기 방식은 동기 이탈 현상의 발생 여부와 무관하게 일정 시간 간격으로 재동기를 이루므로 난수 동기 이탈이 발생하면 다음 동기 패턴과 세션 키를 수신할 때 까지 동기 이탈 상태가 유지되어 통신을 할 수 없게될 뿐아니라 난수 동기 이탈 시에 발생되는 임의의 데이터에 의해 수신 시스템을 오동작 시킬 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 동기 이탈된 상태가 유지 되어 오류가 확산되는 문제점이 있다.

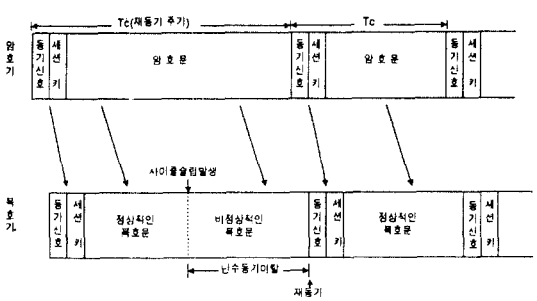


그림 1. 난수 동기 이탈 발생시의 연속 재동기 방식 구조
Fig. 1 The structure of continunous resynchronization with synchronization loss

Ⅲ. LAPB의 주소 특성을 이용한 적응 재동기 알고리즘

1. Link 계층의 기능과 LAPB 프레임의 구성

OSI 참조 모델 7계층 중 2번째 계층인 데이터 링크 계층의 프로토콜로는 ISO에 의해 1974년에 발표한 HDLC(High Level Data Link Control)와 1976년에 ITU-T에서 발표하여 X.25 권고안에 사용되고 있는 LAPB가 있다. LAPB와 HDLC는 매우 유사하며 LAPB가 HDLC의 부분 집합이라 할 수 있는데 LAPB 프레임의 구성은 그림 2와 같다[6].

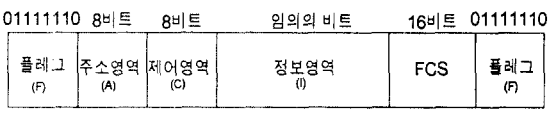


그림 2. LAPB 프레임의 구조
Fig. 2 The structure of LAPB frame

그림 2와 같이 표현되는 LAPB 프레임에서는 단일 링크로 동작하는 경우에는 주소 영역이 DCE인 경우는 '01', DTE인 경우는 '03'으로 고정되고 다중 링크인 경우에는 DCE인 경우는 '0F(h)', DTE인 경우는 '07'으로 고정되어 있는데 그림 3은 단일 링크에서의 주소 영역의 사용 방법을 설명하여 준다[7]. 본 논문에서는 LAPB의 단일 링크에서의 고정된 주소 영역 특성을 이용하여 난수 동기 이탈 현상을 판단하였으나 다중 링크인 경우는 번지 값만 변경하여 단일 링크에서와 동일한 방법으로 판단하면 된다.

2. 주소 영역 수신률(R_{CR})

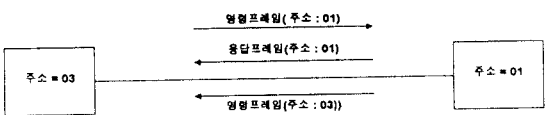
본 논문에서는 LAPB의 주소 영역 특성을 이용하여 난수 동기 이탈의 발생 여부를 판단하기 위한 척도로서 식 (1)과 같이 표현되는 주소 영역 수신률 ,R_{CR}, 을 사용하였다.

$$R_{CR} = \frac{N_{F01,\,03}}{N_F} \tag{1}$$

여기서, N_F는 단위 측정 시간 T_u초 동안 수신측에서 감지된 프래그 패턴의 갯수 이고, $N_{F01,\,03}$은 프레그 패턴 다음의 주소 영역이 '01' 혹은 '03'인 경우의 수

이다.

식 (1)에서 보는 바와 같이 R_{CR}은 단위 측정 시간으로 불리는 T_u초 동안에 수신된 모든 프레그 패턴 중에서 프레그 패턴 다음의 1바이트가 '01' 또는 '03'인 경우가 얼마나 되는가를 나타낸다. LAPB 프레임의 주소 영역을 찾기 위해서는 복호된 데이터 열에서 LAPB 프레임을 구성하는 시작 프레그 패턴(F), 주소 영역(A), 정보 영역(I), 프레임 검사 순서(FCS)를 모두 찾아 주소 영역에 해당되는 부분의 값을 읽는 방법도 있으나 이것은 복잡하고 계산량도 많다. 본 논문에서는 LAPB 프레임 중에서 주소 영역만이 필요하므로 복호된 데이터 열에서 LAPB 프레임의 시작과 끝을 나타내는 프레그 패턴 값을 찾아낸 후 프레그 다음의 1바이트 값을 주소 영역으로 정하는 방법을 사용하였다. 즉, 그림 2에서 나타난 바와같이 LAPB 프레임의 주소 영역은 프레그 패턴 다음의 1 바이트로 표시되므로, 단위 측정시간 Tu초 동안 관찰된 프래그 패턴중에서 다음 1바이트 값이 '01' 또는 '03'인 경우가 얼마인가를 측정한 것이 R_{CR}이다. 정상적으로 암호 통신하는 경우와 난수 동기 이탈이 발생된 경우의 R_{CR} 값의 특성은 다음과 같다.



주소	비트 8	비트 7	비트 6	비트 5	비트 4	비트 3	비트 2	비트 1	
DCE	0	0	0	0	0	0	0	1	01
DTE	0	0	0	0	0	0	1	1	03

그림 3. LAPB 프레임에서의 주소 영역
Fig. 3 The address field in LAPB frame

2.1 정상적인 경우의 R_{CR}

채널의 BER이 b인 경우에 송신 측에서 전송한 주소 영역의 값인 '01' 또는 '03'이 오류없이 수신측에 도착할 확률 P_{CH}은 아래 식 (2)와 같이 나타난다.

$$P_{CH} = (1-b)^8 \tag{2}$$

여기서 b는 채널의 BER(Bit Error Rate)이다.

단위 측정 시간 T_u초 동안에 관찰된 프레그 패턴의 수를 N_F라 하고, 프레그 패턴 다음의 1바이트가 '01' 또는 '03'일 경우의 수를 $N_{F01,\,03}$이라 한다면, $N_{F01,\,03}$은 N_F에 P_{CH}를 곱하면 되므로 아래 식 (3)과 같이 나타난다.

$$N_{F01,\,03} = N_F \cdot P_{CH} \tag{3}$$

결과적으로, 난수 동기 이탈이 발생하지 않은 정상적인 경우에 전송 오류를 고려한 R_{CR}은 다음 식 (4)와 같이 구해진다.

$$R_{CR} = P_{CH} = (1-b)^8 \tag{4}$$

식 (4)에서 보는 바와 같이 R_{CR}은 선로의 BER에 따라 그 값이 변하므로 선로 상태가 나쁠수록 LAPB의 주소 영역에 전송 오류가 발생할 확률이 높아지고 이에 따라RCR은 감소한다. 그림 4는 BER과 R_{CR}의 관계를 나타내는 것으로 BER이 증가 할수록 R_{CR}은 감소함을 알 수 있다.

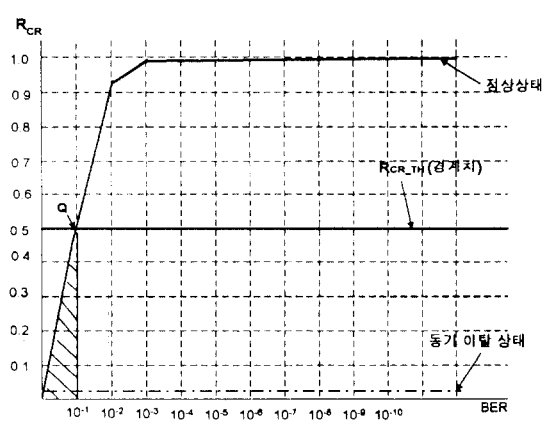


그림 4. T_u = 0.5초인 경우 BER의 변화에 따른 R_{CR}
Fig 4 R_{CR} for various BER in case that T_u is 0.5sec.

2.2 난수 동기 이탈한 경우의 R_{CR}

암호 통신 중 난수 동기 이탈이 발생하면 복호된 데이터는 임의의 값을 갖으므로 복호된 데이터에서 '01' 과 '03'이 발생할 확률은 각각 1/256(비트)로 가정

할 수 있다. 따라서, T_u초 동안에 복호된 데이터에서 프레그 패턴 다음의 1 바이트 값인 주소 영역이 '01' 또는 '03'일 경우의 수인 $N_{F01,03}$은 식 (5)와 같이 나타난다. 결과적으로, 난수 동기 이탈 시의 RCR 값은 식 (6)과 같이 구해지는데 난수 동기 이탈이 발생하였을 때의 R_{CR}은 2/256의 일정한 값을 갖는다.

$$N_{F01,03} = N_F\left(\frac{1}{256} + \frac{1}{256}\right) = \frac{2}{256} N_F \quad (5)$$

$$R_{CR} = \frac{N_{F01,03}}{N_F} = \frac{2}{256} \quad (6)$$

3. R_{CR}을 이용한 적응 재동기 방식

3.1 적응 재동기 방식의 흐름도

그림 4에서 보는 바와 같이 정상적인 경우의 R_{CR} 값과 난수 동기 이탈이 발생한 경우의 R_{CR} 값은 차이가 많이나므로 본 논문에서는 R_{CR}을 이용하여 난수 동기 이탈이 발생된 경우에만 재동기를 이루는 방법을 제안하였다. 그림 5는 제안된 적응 재동기 방식의 흐름도이다. 먼저 복호된 비트열에서 프레그 패턴이 찾아지면 LAPB 프레임의 시작이므로 프레그 패턴 다음의 1바이트 값이 '01' 또는 '03' 인가를 확인한다. 프레그 패턴 다음의 1바이트는 주소 영역이므로 그

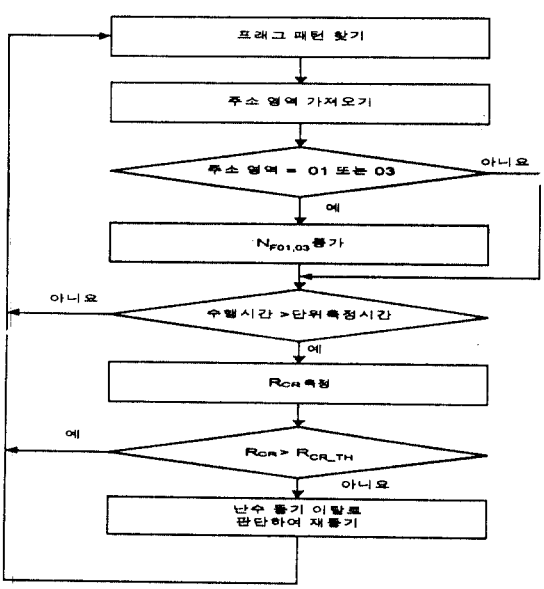


그림 5. 제안된 알고리즘의 흐름도
Fig. 5 The flow chart of proposed algorithm

표 1. 적응 재동기 방식에서의 R_{CR}에 따른 상태 판단법
Table 1. State-decision-rule by RCR in adaptive resynchronization

조건	상태	조치
R_{CR} > 역치	정상상태	계속 통신
R_{CR} > 역치	난수 동기 이탈	재동기

값이 '01' 또는 '03'이면 정상적으로 복호되는 것으로 판단하여 $N_{F01,03}$를 증가시킨다. 이러한 과정을 단위 측정 시간 T_u초 동안 수행한 후 계산된 R_{CR}이 정해진 역치보다 크면 정상적인 경우로 판단하여 난수 동기 이탈 감시를 계속 수행하고 반대의 경우는 난수 동기 이탈이 발생한 것으로 판단하여, 동기 패턴과 세션 키를 송, 수신하여 난수 재동기를 취하여 통신을 다시 가능하도록 하였다. 이것을 정리하면 표 1과 같다.

3.2 R_{CR}의 역치

식 (4)에서 보는 바와 같이 R_{CR}은 선로의 BER에 영향을 받으므로 R_{CR}의 역치인 R_{C_TH}를 정할 때는 해당 선로 조건에서 난수 동기 이탈이 발생한 경우와 발생하지 않은 경우를 명확히 구분할 수 있도록 하여야한다. 그림 4는 단위 측정 시간 T_u를 0.5초로 설정한 경우의 R_{CR}를 그린 것인데 굵은 선으로 표시된 것이 정상 상태와 난수 동기 이탈 상태를 구분하는 경계치인 R_{CR_TH}을 나타낸다. 그림 4에서 R_{CR_TH} 값을 크게 정할 수록 난수 동기 이탈 상태를 감지 못하는 경우는 줄어들 것이나 정상적인 경우를 난수 동기 이탈로 잘못 판단하는 경우는 늘어날 것이다. 반면에, R_{CR_TH} 값을 적게 정할 수록 정상적인 경우를 난수 동기 이탈로 잘못 판단하는 경우가 줄어들 것이나 난수 동기 이탈을 감지 못하는 경우는 늘어날 것이다. 따라서 R_{CR_TH}은 해당 암호 시스템의 요구에 따라 적정하게 정하면 되나 본 논문에서는 그림 4에서 나타난바와 같이 R_{CR_TH} 값을 0.5로 정하여 정상적인 경우를 난수 동기 이탈로 잘못 판단하는 경우를 줄이도록 하였다. 이 경우 R_{CR_TH} 값과 정상적인 경우의 R_{CR} 곡선이 만나는 점 Q의 왼쪽 부분 즉, 그림 4에서의 빗금친 부분은 정상적인 경우를 난수 동기 이탈이 발생한 것으로 잘못 판단할 경우이다. 그런데 그

림 4에서 빗금친 부분은 T_u초 동안의 평균 BER이 약 0.1 이상인데 이것은 10비트 전송하면 1비트 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.

4. 적응 재동기 방식의 응용

LAPB를 채택하고 있는 대표적인 망은 X.25 망인데 이것은 DTE나 DCE 로 구축되는 사설망이나 광역 유, 무선 공중망에 많이 사용되고 있으며 현재 국내의 5대 기간 전산망에서도 중요 기간망은 대부분 X.25로 구성되어 있다. 중요 기간망을 통하여 중요 정보를 전송할 때 트래픽과 데이터의 보호를 위하여 링크용 암, 복호기를 사용하지만 선로 상에 존재하는 잡음에의해서 난수열 동기가 흐트러져 원활한 암호 통신을 할 수 없을 때가 많이 발생한다. 이러한 경우에 제안된 적응 재동기 방식을 사용한다면 보다 안정된 암호 통신을 가능하게 할 것이다.

Ⅳ. 실험 결과 및 고찰

1. 실험 방법

기존의 연속 재동기 방식과 제안된 적응 재동기 방식의 성능을 비교하기 위하여 식 (7)과 같이 표시되는 오복호율 E rate와 재동기를 위하여 필요한 잉여 비트 전송량 D red를 이용하였다.

$$E\_rate = \frac{E\_data}{D_t} \tag{7}$$

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

E_rate는 전송한 총 데이터와 복호기에서 잘못 복호된 데이터 비를 나타내므로 E_rate가 낮을수록 난수 동기 이탈을 정확하고 신속하게 감지하여 재동기를 이룬다는 것을 의미한다. 따라서, 동일한 선로 조건과 난수 동기 이탈 조건에서 연속 재동기 방식과 적응 재동기 방식의 성능은 E_rate를 비교하면 알 수 있다. 또한, 동일한 양의 데이터를 암호 통신을 이용하여 전송할 때 재동기를 위하여 필요한 잉여 데이터 비트 수 D red를 이용하여 두 방법의 통신 효율을 비교하였다. 재동기를 위하여 전송하는 동기 패턴은 128비트로 하였고 세션 키는 256비트로 하였다. 전송 도중 세션 키에 오류가 발생하면 난수 동기가 흐트러지므로 3비트의 오류 정정 능력을 갖는 (15, 4) ML (Maximum-length) 코드로 에러 정정 부호화하여 전송하는 것으로 하였다[8]. 동기식 스트림 암호 통신 시스템에 10^9과 $3*10^9$ 비트의 특정 패턴으로 구성된 데이터를 송, 수신하면서 10^{-6}, 10^{-7}, 10^{-8} 비트의 발생율로 난수 동기 이탈을 발생시켰는데 난수 동기 이탈은 그림 1의 연속 재동기 방식의 구성중 동기 패턴과 세션 키 부분에서는 발생치 않고 암호문의 임의의 부분에서만 발생하도록 하였다. 선로의 평균 BER은 10^{-6} 비트로 하였으며 통신 속도는 9,600bps와 28,800bps에서 통신 시험을 하였다.

2. 오복호율(E rate)

표 2~표 5는 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 복호기

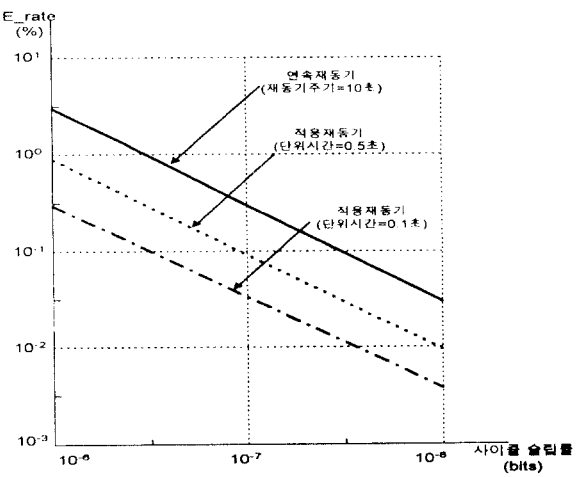


그림 6 통신 속도 9,600bps에서의 오복호율 비교
Fig. 6 The comparison of E_rate in 9,600bps

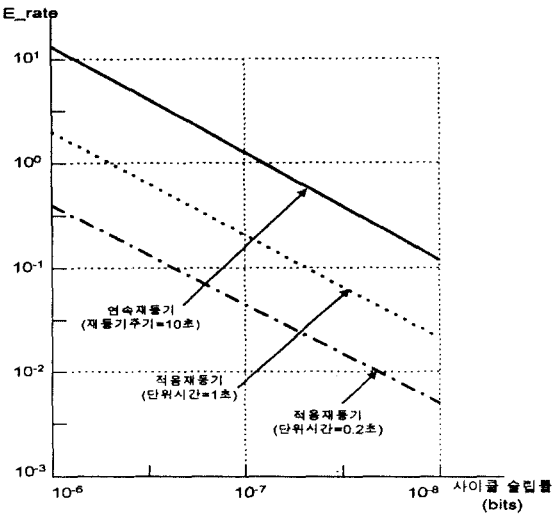


그림 7 통신 속도 28,800bps에서의 오복호율 비교
Fig. 7 The comparison of E_rate in 28,800bps

에서 복호하는 시험을 10회 실시한 후에 측정된 E_rate와 E_data의 평균값을 나타낸다. 또한, 그림 6과 그림 7은 통신 속도 9,600bps와 28,800bps에서 연속 재동기 방식과 적응 재동기 방식의 E_rate를 그림으로 나타낸 것이다.

표 2 표 5와 그림 6 그림 7에서 보는 바와 같이 적응 재동기 방법이 연속 재동기 방식에 비해 난수 동기 이탈 율에 무관하게 오복호률 E_rate와 잘못 복호된 데이터 비트 수를 나타내는 E_data가 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 연속 재동기 주기를 T_c라 할 때 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 이룬다

표 2. 통신 속도 9,600bps일 때 제안된 적응 재동기 방식에서의 단위 측정 시간 T_u의 변화에 따른 E_data와 E_rate의 비교

Table 2. The comparison of E_data and E_rate in case that speed is 9,600bps and period of resynchronization ,T_u, is various in adaptive resynchronization.

사이클 슬립발생률	제안된 적응 재동기 방식 ($T_u=0.1$초)		제안된 적응 재동기 방식 ($T_u=0.5$초)		제안된 적응 재동기 방식 ($T_u=1$초)	
	E_data (bits)	E_rate (%)	E_data (bits)	E_rate (%)	E_data (bits)	E_rate (%)
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 3. 통신 속도 9,600bps일 때 연속 재동기 방식에서 재동기 주기 T_c의 변화에 따른 E_data와 E_rate의 비교

Table 3. The comparison of E_data and E_rate in case that speed is 9,600bps and period of resynchronization ,T_u, is various in continuous resynchronization.

사이클 슬립발생률	연속 재동기 방식 ($T_u=10$초)		연속 재동기 방식 ($T_c=5$초)		연속 재동기 방식 ($T_c=1$초)	
	E_data (bits)	E_rate (%)	E_data (bits)	E_rate (%)	E_data (bits)	E_rate (%)
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 4. 통신 속도 28,800bps인 경우의 제안된 적응 재동기 방식에서의 단위 측정 시간 T_u의 변화에 따른 E_data과 E_rate의 비교

Table 4. The comparison of E_data and E_rate in case that speed is 28,800bps and period of resynchronization ,T_u, is various in adaptive resynchronization.

사이클 슬립발생률	제안된 적응 재동기 방식 ($T_u=0.2$초)		제안된 적응 재동기 방식 ($T_u=0.5$초)		제안된 적응 재동기 방식 ($T_u=1$초)	
	E_data (bits)	E_rate (%)	E_data (bits)	E rate (%)	E_data (bits)	E_rate (%)
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 5. 통신 속도 28,800bps인 경우의 연속 재동기 방식에서 재동기 주기 T_c의 변화에 따른 E_rate와 E_data의 비교

Table 5. The comparison of E_data and E rate in case that speed is 28,800bps and period of resynchronization ,T_c, is various in continuous resynchronization.

사이클 슬립발생률	연속 재동기 방식 ($T_u=10$초)		연속 재동기 방식 ($T_c=5$초)		연속 재동기 방식 ($T_c=0.5$초)	
	E_data (bits)	E rate (%)	E_data (bits)	E_rate (%)	E_data (bits)	E_rate (%)
10^{-6}	4.3×10^{8}	1.4×10^{1}	2.1×10^{8}	7.0×10^{0}	2.1×10^{7}	4.8×10^{-1}
10^{-7}	4.3×10^{7}	1.4×10^{0}	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 6. 통신 속도 9,600bps 일 陜 연속 재동기 방식으로 10^9 비트의 데이터 전송시에 요구되는 잉여 비트 수의 비교.

Table 6. The comparison of total dummy bits in 9,600bps when 10^9 bits is transmitted by continuous resynchronization.

연속재동기방식 ($T_c=1$초)	적응재동기방식 ($T_u=0.5$초, 난수동기이탈 $=10^{-7}$)
1.13×10^{8}(bits)	1.09×10^{5}(bits)

표 7. 통신 속도 28,800bps일 때 적응 재동기 방식으로 $3*10^9$ 비트의 데이터 전송시에 요구되는 잉여 비트 수의 비교.

Table 7. The comparison of total dummy bits in 28,800bps when $3*10^9$ bits is tansmitted by adaptive resynchronization.

연속재동기방식 ($T_c=1$초)	적응재동기방식 ($T_u=0.2$초, 난수동기이탈률 $=10^{-7}$)
2.27×10^{8}(bits)	3.27×10^{5}(bits)

고 볼 수 있다. 그런데 T_u는 T_c 보다 훨씬 적게 정할 수 있으므로 적응 재동기 방식을 적용하였을 때가 훨씬 빠르다. 이 두 경우의 재동기 소요 시간 비 T_rate를 식으로 나타내면 식 (8)과 같다.

$$T\_rate \cong \frac{T_c}{2T_u} \tag{8}$$

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

식 (8)에서 보는 바와같이 T_c를 10초로 하고 T_u를 약 0.5초로 하였을 경우에는 T_rate=10 이다. 즉, 적응 재동기 방식이 기존의 연속 재동기 방식에 비하여 재동기를 이루는데 소요되는 시간이 10배나 빠르다는 것을 나타낸다. 이것은 표 2 표 5에서 나타나는 것과 같이 동일한 사이클 슬립 발생 확률에서 오복호율 E_rate와 오복호된 데이터 비트 수 E_data를 약 10배 감소시켜 수신측에서 훨씬 정확한 데이터를 얻을 수

있다는 것을 말한다.

3. 잉여 비트수(D_red)

표 2와 표 3에서 보면 통신 속도 9,600bps에서, 재동기 주기 T_c가 1초인 연속 재동기 방식과 단위 측정 시간 T_u가 0.5초인 적응 재동기 방식의 성능은 거의 동일하게 나타지만 표 8에서 보면 10^9 비트의 데이터를 연속 재동기 방식으로 전송하는데 필요한 총 잉여 비트 수는 약 1.13×10^8 비트이나 적응 재동기 방식으로 전송할 때는 난수 동기 이탈률을 10^{-7} 비트로 가정한다면 1.09×10^5 비트만 있으면 된다. 즉 동일한 E_data와 E_rate를 목표로 하였을 때, 적응 재동기 방식을 사용하면 연속 재동기 방식에 비해 약 1.13×10^8 비트의 잉여 비트 수를 줄일 수 있다. 또한, 표 5와 표 6에서 나타난 것처럼 28,800bps로 전송하는 경우에도 마찬가지의 결과가 나타난다. 단위 측정 시간 0.2초인 적응 재동기 방식과 재동기 주기 0.5초인 연속 재동기 방식이 비슷한 E_data와 E_rate를 나타내는 것으로 나타내지만 표 7에서 보면 3×10^9 비트의 데이터를 28,800bps로 연속 재동기 방식을 사용하여 전송하는데 소요되는 총 잉여 비트 수는 2.27×10^8 비트 이나 적응 재동기 방식으로 전송 할 때는 난수 동기 이탈율이 10^{-7} 비트라 가정한다면 3.27×10^5 비트 만 있으면 된다. 즉, 동일한 E_data와 E_rate를 목표로 하였을 때, 적응 재동기 방식을 사용하면 연속 재동기 방식에 비해 약 2.27×10^8 비트의 잉여 비트 수를 줄일 수 있다. 이러한 결과는 적응 재동기 방식을 사용하면 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 있다는 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 짧게하여야 하므로 데이터 감축 효과는 더욱 증가할 것으로 예측된다.

V. 결 론

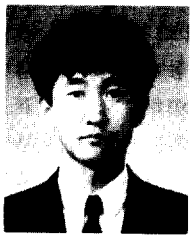
본 논문에서는 LINK 계층의 프로토콜로 LAPB를 사용하는 암호 통신 시스템에 적합하고 연속 재동기 방식의 문제점 들을 해결 할 수 있는 적응 재동기 알고리즘을 제안하였다. 제안된 방법에서는 LAPB 프레임의 주소 영역 특성을 이용하여 난수 동기 이탈이 발생된 경우에만 동기 패턴과 세션 키를 전송하여 재동기를 이루는 적응 재동기 방법을 사용하였다. 적응 재동기 방법을 사용하면 난수 동기 이탈 발생 후 재동기까지의 소요 기간이 줄어들므로 통신을 할 수 없는 기간이 감소될 뿐아니라 난수 동기 이탈이 발생한 경우만 동기 패턴과 세션 키를 전송하므로 전송 효율을 향상시키고 세션 키를 주기적으로 발생하는 부담을 줄일 수 있다. 제안된 알고리즘을 LAPB 환경에서 운용되는 동기식 스트림 암호 통신 시스템에 적용하여 시험한 결과 연속 재동기에 비해 오복호율 E_rate와 오복호된 데이터 비트 수 E_data를 10배 감소시켰는데 이것은 전송하여야 할 데이터의 총량을 최대 11.3%까지 감축하는 효과를 나타낸다. 제안된 적응 재동기 알고리즘을 LAPB 프로토콜을 사용하는 X.25 유, 무선 패킷 암호 통신에 적용한다면 보다 안정된 통신을 할 수 있을 것으로 예측된다.

참 고 문 헌

1. 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.
2. H. Meyr and G. Ascheid, "Synchronization in Digital Communications vol. 1", John Wieley & Sons, 1990.
3. R. A. Rueppel, "Analysis and Design of Stream Ciphers", Springer-Verlag, 1986.
4. B. Schneier, "Applied Cryptography:protocols,algorithm,and source code in C", John Willy & Son, 1993.
5. J. Daemen, R. Govaerts, J. Vandewalle, "Resynchronization Weaknesses in Synchronous Stream ciphers", Pre-proceedings of EUROCRYPT'93, pp. T9-T17 1993.
6. CCITT Rec. X.25, pp.113-pp.116, 1984.
7. CCITT Rec. X.25, pp.126-pp.127, 1984.
8. M. Y. Lee, "Error-Correcting Coding Theory",

McGraw-Hill, 1989.

윤 장 홍(Jang-Hong Yoon) 정회원
국방과학연구소 재직
한국통신학회논문지 제22권 8호 참조



이 주 형(Joo-Heng Lee) 정회원
1989년 2월 : 경북대학교 전자공학과 졸업(학사)
1992년 2월 : 경북대학교 대학원 전자공학과 졸업(석사)
1992년 3월~현재 : 국방과학연구소 재직
※주관심분야 : 데이터 통신, 음성신호처리, ASIC 설계

양 상 운(Sang-Woon Yang) 정회원
1992년 2월 : 충북대학교 정보통신공학과 졸업(학사)
1992년 3월~현재 : 국방과학연구소 재직
※주관심분야 : 데이터통신, ASIC 설계

황 찬 식(Chan-Sik Hwang) 정회원
경북대학교 전기전자공학부 교수
한국통신학회논문지 제22권 8호 참조