通信情報保護學會論文誌
第 8 卷 第 2 號, 1998. 6

프레임릴레이 프로토콜에서 주소비트를 이용한 키스트림 동기 보상 알고리즘

홍진근*, 윤장홍*, 윤정오**, 황찬식*

A Key Stream Synchronization Compensation Algorithm using Address Bits on Frame Relay Protocol

J.K.Hong*, J.H.Yoon*, J.O.Yun**, C.S.Hwang*

요 약

논문에서는 프레임릴레이 프로토콜을 사용하는 암호 통신 시스템에 적합한 키 스트림 동기 방식을 제안하였다. 제안된 주소영역의 확장 비트를 이용한 키 스트림 동기 방식은 단위 측정 시간 동안 측정된 프레임릴레이 프로토콜의 주소영역의 확장 비트 정보와 플래그 패턴의 수신률을 이용하여 문턱값보다 적은 경우에 동기 신호와 세션 키를 전송하므로써 종래의 주기적인 동기 방식에서 전송 효율성 저하와 주기적인 상이한 세션 키 발생, 다음 주기까지 동기 이탈 상태로 인한 오류 확산 등의 단점을 해결하였다. 제안된 알고리즘을 데이터 링크 계층의 처리기능을 최소화하여 패킷 망의 고속화가 가능하도록 설계된 프레임릴레이 프로토콜에서 서비스되는 동기식 스트림 암호 통신 시스템에 적용하여 slip rate 10^{-7}의 환경에서 주기가 1sec인 주기적인 동기 방식에서 요구되는 9.6×10^{6}비트에 비해 6.4×10^{5}비트가 소요됨으로써 전송율 측면에서의 성능 향상과 오복호율과 오복호 데이터 비트 측면에서 성능 향상을 얻었다.

Abstract

In this paper, we proposed a key stream synchronization algorithm for cipher system using frame-relay protocol. The proposed key stream synchronous algorithm using extended bits of address field solved the problem like the transmit session key and the incorrectness by continuing synchronization loss in next timestep. They are achieved by the transfer of synchronous signal and session key when it is less than the threshold value, using the receiving rate of extended bit information and flag patterns of the frame relay protcol in the decision duration. When the proposed algorithm is applied to the

* 경북대학교
** 한국산업대학교,

synchronous stream cipher system, using frame-relay protocol which is designed to provide the highest speed of packet network, minizing the process ability of data link level. it has advanced the result in Rerror and Derror, and in transmission rate, by the use of 6.4 × 10^5bits, not 9.6 ×10^6bits required in periodic synchronous method, having lsec time step, in slip rate 10^{-7}.

Keyword: *Correlator*, 키 수열 동기, 동기 패턴 발생, 동기 패턴 검출

Ⅰ. 서 론

최근 전세계적으로 초고속 정보 서비스를 목표로 하는 구축사업을 통해 다양하고 광범위한 매체가 등장하면서 이에 대한 전송되는 서비스의 보호 기술 문제가 매우 중요시 대두되고 있다. 통신망에서 정보 서비스를 보호하기 위해서는 정보를 전송할 때 비인가자의 도용이나 도청 또는 정보 파괴 및 변조 등으로부터 보호하기 위한 정보 변환 처리 기술이 요구된다. 정보를 변환하기 위해서는 먼저 정보를 긴 주기의 키 수열과 암호화하여 전송하고 복호기에서 이를 해독하여 인가자 만이 원래의 정보를 얻게 된다. 이때 암호기에서 전송한 암호문이 복호기에서 정상적으로 복호되기 위해서는 암/복호기에서 사용된 키 수열의 일치가 요구되지만 실제 망 환경에서는 여러 가지 원인으로 인해 암/복호기의 키 수열의 불일치성을 초래하게 되는데 이를 키 수열의 동기 이탈 현상이라 한다. 동기식 스트림 암호 통신 시스템에서는 수신 클럭의 사이클 슬립에 의한 키 수열의 동기 이탈 현상으로 인해 통신이 불능 상태가 발생하고[1-2] 이로 인해 키 수열의 동기 이탈이 발생하면 복호기는 정상적인 복호가 불가능하고 오복호된 데이터로 인해 수신 시스템을 오 동작을 일으킬 수 있다[3-4]. 이러한 위험성을 감소하기 위한 방안으로 동기식 스트림 암호 통신 시스템에서는 동기 패턴과 세션 키를 주기적으로 전송하여 암/복호기의 키 수열을 일치 시키는 주기적인 동기 방식을 사용하지만 이 또한 문제점이 있다[5]. 따라서 본 논문에서는 동기식 스트림 암호 통신에서 동기 이탈 상태를 유무를 판별하여 동기 이탈 상태일 때 동기 패턴과 세션 키를 전송하는 비주기적인 동기 방식을 제안하였다. 일반적으로 프레임릴레이는 낮은 에러율로 고품질의 전송 시스템의 잇점을 갖는 패킷 모드 서비스로서 ISDN(Integrated Services Digital Network) LAP-D(Link Access Procedure on the D channel (Q.291))에 사용되는 데이터 링크 계층 프로토콜을 근거로 하여 설계되었다. 이는 망의 부담을 최소화하여 데이터 전송에 필수적인 계층 2의 일부 기능만을 수행하고 종단 단말에서 데이터 링크 계층의 모든 기능을 수행하므로써 효율성을 증가시킨다. 본 논문에서는 프레임릴레이 프로토콜에 적합한 동기적인 스트림 암호 통신 시스템에서 효율적인 키 수열의 슬립 발생시 동기 보상 알고리즘을 제안하였다.

본 논문의 구성으로는 먼저 II장에서 종래의 주기적인 동기 방식으로 구성된 스트림 암호 통신 시스템을 살펴보고 III장에서 프레임릴레이 서비스 구조 전송을 위한 LAP-F 데이터 링크계층 프로토콜의 구조를 살펴보고 IV장에서 본 논문에서 제안한 LAP-F에서 주소영역의 확장 주소 비트를 이용한 슬립 보상 알고리즘을 살펴보고 V장에서 시뮬레이션 결과 및 고찰, VI장에서 결론을 맺고자한다.

Ⅱ. 주기적인 동기 방식으로 구성된 동기 스트림 암호 시스템

일반적으로 스트림 암호 시스템은 외부키가 키 스트림 발생기에 인가되고 이때 키스트림 발생기는 무한의 키 스트림을 발생시킨다. 그림1에서는 스트림 암호 시스템의 암/복호기가 주기적으로 동기 패턴과 세션 키를 송/수신하여 상호 동일한 세션 키를 사용하여 키 수열 발생기의 초기 상태값을 주기적으로 동일하게 생성하여 동기를 이루도록 한다.

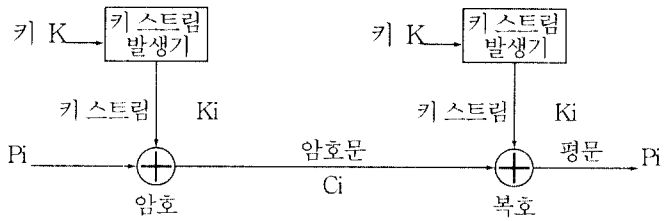


그림 1.스트림 암호 통신 시스템 구조

Fig. 1 The structure of stream cipher communication

주기적인 동기식 스트림 암호 통신 방식은 J. Daemen 등[5]에 의해 주기적인 동기 방식의 그 취약성이 연구되어 왔고 이에 대한 문제점은 다음과 같다. 먼저, 주기적인 동기 방식을 사용하므로써 동기 이탈 발생과 무관하게 일정 시간 간격으로 동기를 이루므로 키 수열의 동기 이탈이 발생하면 다음 동기 패턴과 세션 키를 수신시 까지 동기 이탈 상태가 유지되어 통신 불능 상태가 지속된다. 따라서 키 수열의 동기 이탈 시에 발생하는 임의의 데이터가 수신 시스템을 오동작 시킬 위험성이 존재한다. 다음으로, 주기적인 동기 방식은 키 수열의 동기 이탈 발생과 무관하게 주기적으로 동기 패턴과 세션 키의 전송이 요구되므로 전송 효율 저하와 주기적으로 다른 세션 키를 발생하고 전송하는 부담이 존재한다. 마지막으로, 세션 키를 전송하는 과정에서 세션 키에 전송 오류가 발생하면 다음 동기 패턴과 세션 키를 수신 할 때까지 동기 이탈 상태가 지속되어 오류 확산의 문제점이 존재한다. 그림 2에서는 주기적인 동기 방식에서 동기 이탈이 발생시 정상적인 복호 데이터와 비정상적인 오복호된 데이터에 대해 나타낸 것이다.

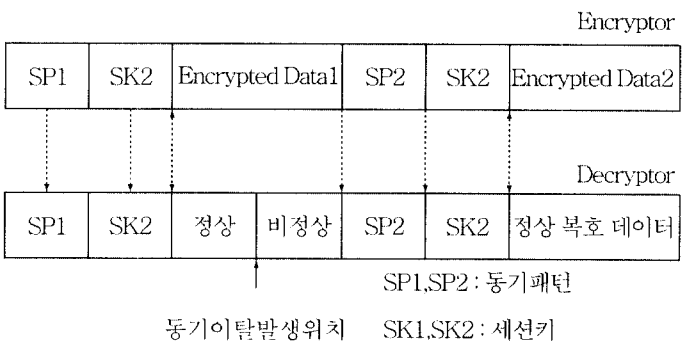


그림 2. 동기 이탈 발생시의 주기적인 동기 방식 구조

Fig. 2 The Structure of cyclic synchronization with synchronization loss

Ⅲ. LAP-F 데이터 링크계층 프로토콜의 구조

1. LAP-F 프레임의 구조와 전송 프로토콜

프레임릴레이의 데이터 전송 측면에서 망과 종단 단말의 전송 프로토콜 스택을 그림 3에서 제시하였다. LAP-F(*Link Access Procedures to Frame Mode Bearer Services*) 프로토콜은 Q.922에서 정의하고 있으며 LAP-F 프레임은 플래그, 헤더 필드, 정보 필드, FCS(*Frame Check Sequence*) 필드로 구성된다. 플래그는 프레임의 시작과 끝의 정보이며, "01111110"의 형태를 가지고 정보 필드에서 1이 연속 5개 이상 발생하면 송신측에서 강제적으로 0을 주소영역의 확장비트는 삽입한 후 수신측에서 다시 제거하여 데이터 투명성을 보장한다. 헤더 필드는 DLCI(*Data Link Connection, Identifier*), *EA*(*Extended Address*), FECN(*Forward Explicit Congestion Notification*), BECN(*Backward Explicit Congestion Notification*), DE(*Discard Eligibility*), C/R(*Command/Response*) 등으로 구성된다. 이때 DLCI 필드는 주소 기능으로 사용되며 EA 비트는 주소 필드 확장시 사용된다. 또한 FECN/BECN, DE 비트는 폭주 제어에 사용되고 C/R 비트는 명령/응답에 대한 사용자 장치에서 사용된다. FCS 필드는 ITU-T(CCITT) 16-CRC를 따르며 프레임의 에러 발생 유무를 검사한다. Q.922의 핵심 기능은 프레임의 투명성을 보장하고 DLCI를 이용한 다중화 및 역다중화 기능을 제공하고 프레임의 길이 검사, CRC를 통한 에러 검사, 폭주제어 등을 수행한다. 물리계층에서는 I.430/431에서 권고하고 있는 바와 같이 인터페이스가 제어 평면과 사용자 평면에 공통으로 적용되며 이를 통해 물리적인 제어 평면 및 사용자 평면 정보가 ISDN의 S/T 참조점을 통해 전송된다.

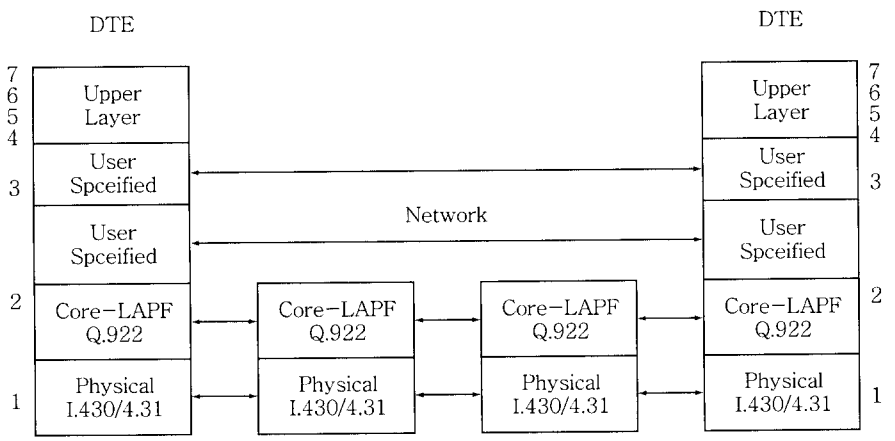


그림 3. 프레임릴레이 데이터 전송 프로토콜

Fig. 3 Data Transmission Protocol of Frame Relay

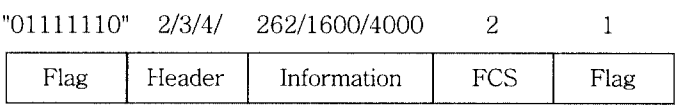


그림 4. LAP-F 프레임의 구조

Fig. 4 The structure of LAP-F Frame

프레임릴레이 서비스를 위한 LAP-F 프레임의 기본 구조는 그림 4에서 제시하고 있다. 제안된 프레임의 기본 구조는 2/3/4 옥텟으로 사용되는 프레임 헤더 즉, 주소 영역의 확장 주소 비트의 정보와 프레임의 시작과 끝을 나타내는 플래그의 수신률의 상태를 파악하여 슬립 상태 여부를 판별한다. 이때 파악된 수신률이 문턱치보다 클 경우 키 수열의 동기 이탈로 판단하고 동기 패턴과 세션 키를 전송하여 재동기 과정을 수행한다. 일반적으로 이때 사용되는 프레임릴레이 프레임 크기는 ISDN LAP-D 프로토콜과의 호환성을 고려하여 262 옥텟으로 설정하고, IEEE 802.3 LAN 또는 Ethernet간의 상호 접속을 지원하는 경우 라우터나 브릿지에서의 MAC 프레임을 처리하기 위해 소요되는 오버헤더를 감소하기 위해 최대 1600 옥텟까지 설정하며, 토큰 링 LAN 또는 FDDI간 상호 접속을 위해 4000 옥텟 이상을 지정하는 것이 바람직한 것으로 알려져 있다.

LAP-F 프레임의 주소 영역에서 확장 주소 비트가 정상적으로 복호되는 경우에는 일정한 값을 가지는데 반해 키 수열의 동기 이탈이 발생된 경우에는 임의의 값을 가지므로 단위 측정 시간 동안 복호된 LAP-F 프레임의 주소 영역의 확장 주소 비트의 분포를 이용하여 키 수열의 동기 이탈 현상을 파악하고 이때 발생된 키 수열의 동기 이탈 상태에서는 동기 패턴과 세션 키를 전송하므로써 재동기를 이루도록 한다. 암호 시스템의 암호 통신 중에 키 수열의 동기 이탈이 발생하는 기간은 정상적인 기간에 비하여 매우 적으므로 제안된 동기 방식은 주기적인 동기 방식에 비교하여 재동기를 위하여 요구되는 동기 패턴과 세션 키의 수를 감소시키므로써 통신 효율이 증가할 뿐 아니라 주기적으로 동기 패턴과 세션 키를 전송함으로서 발생되는 문제점들을 해결 할 수 있다. 또한, 제안한 동기 방식에서의 사용된 단위 측정 시간은 주기적인 동기 방식에서 사용된 재동기 주기에 비해 매우 짧아 키 수열의 동기 이탈 상태를 훨씬 빨리 검출이 가능하므로써 신뢰성있는 암호 통신이 가능하다.

2. LAP-F 프레임에서 주소 영역의 구조

LAP-F는 ISDN의 B-, D-, H-채널 인터페이스를 통한 프레임 모드 베어러 서비스를 이용하는 U-평면의 DL-서비스 이용자 사이에 데이터 링크 서비스 데이터 단위의 전송을 제공하고 하나 혹은 다수의 프레임 모드 베어러 접속의 통계적 다중화가 가능하다. 일반적으로 주소 필드는 최소한 2옥텟 이상으로 구성되고 필드 포맷은 다음 그림 5에서와 같이 주소 필드 확장 비트, 명령/응답 표시자, 순방향과 역방향 표시자와 폐기 적격 등을 위해 세트한 3개의 비트, 데이터 링크 접속 식별자(DLCI)필드와 3 또는 4옥텟 주소 필드의 마지막 옥텟이 하위 DLCI인가 아니면 DL-CORE 제어 정보인가 등을 표시하는 비트 등으로 구성된다. 이때 디폴트 주소 필드의 최소 길이는 2옥텟이거나 보다 많은 DLCI를 제공하거나 선택적 DL-

CORE 기능을 제공하기 위해 3옥텟 또는 4옥텟으로 확장이 가능하다. 주소 필드 범위는 주소 필드 옥텟 중의 처음 송출되는 비트를 셋팅하여 확장되고 주소 필드 옥텟의 첫 번째 비트가 0이 되는 것은 이 옥텟 다음에 오는 옥텟이 또다른 주소 필드의 옥텟임을 의미하고 주소 필드의 옥텟중 첫 번째 비트가 1이 되는 것은 이것이 주소필드의 최종 옥텟임을 표시한다. 그림 5.a에서 살펴 보듯이 2옥텟 주소 필드를 사용할 경우 첫 번째 옥텟 비트 1을 "0"으로 셋팅하고 두 번째 옥텟의 비트1을 "1"로 셋팅한다. 그림 5.b의 3옥텟 구조나 그림 5.c의 4옥텟 구조에서도 2옥텟 주소 필드와 동일한 방식으로 셋팅하게 된다.

그림 5. LAP-F 프레임의 주소 필드 구조

Fig. 5 The structure of LAP-F Frame Address Field

따라서 본 논문에서는 프레임의 주소 필드에서 각 옥텟의 확장 주소(EA)의 특성을 이용하여 확장 주소 비트의 수신률과 문턱치의 비교로부터 슬립 상태를 판별한다. 2옥텟 구조에서 주소부는 상위비트의 비트1이 "0" 이고 하위비트의 비트1이 "1" 일 때 사용가능한 조합의 수는 214이고 그 이외에 3옥텟 구조는 221, 4옥텟 구조는 224이 된다. 암호통신을 할 때 복호기가 정상적으로 복호를 수행하게 되면 다음 표 1에서 제시한바와 같은 정보를 갖게 되고 이것은 각 옥텟 구조에서 키 수열의 동기 이탈 현상이 발생하지 않은 것을 의미한다. 만일 키 수열에 동기 이탈이 발생하면 확장 주소 영역부의 정보는 임의의 값을 갖게 되고 측정 단위 시간내에 정상적으로 복호되는 수신 성공률로부터 동기 이탈 현상을 판단하게 된다.

〈표 1〉 확장 주소 영역부의 특성
〈Table 1〉 The characteristics of Extende Address Field

확장주소부 / 주소영역부	E_{A1}	E_{A2}	E_{A3}	E_{A4}
2옥텟	0	1	-	-
3옥텟	0	0	1	-
4옥텟	0	0	0	1

여기서 E_{A1}, E_{A2}, E_{A3}, E_{A4} 는 확장 주소 영역부에서 각 레벨의 비트 정보를 나타낸다. 확장 주소 영역부에서 각 옥텟에 대한 정보를 파악하여 키 수열의 동기 이탈 현상을 검출하고 이때 동기 이탈이 발생한 경우에 한해서 동기 패턴과 세션 키를 전송하므로써 재동기를 이루는 방식은 주기적으로 동기 패턴과 세션 키를 전송하여 재동기를 이루는 방식에 비해 오버헤더의 감소 측면이나 안전도 측면에서 효율적이다.

IV. 제안한 슬립 보상 알고리즘

1. 주소 영역의 확장 주소 비트를 이용한 수신률(R_{EA})

본 논문에서는 슬립 발생 유무를 판별하기 위해 LAP-F 주소 영역의 확장 주소 비트의 수신률을 사용하였고 이때 슬립 발생 유무에 관한 수신률을 $\mathbf{R}_{EA}$로 정의하였다.

$$R_{EA}=\frac{N_{EA}}{N_F} \qquad (1)$$

식(1)에서 N_F는 단위 측정 시간 T_u초 동안이나 단위 프래임내에서 플래그 패턴의 개수이고, N_{EA}는 주소 영역의 확장 주소 비트의 상태를 검출하여 판별한 비트 개수이다. 수신률 R_{EA}는 정상적으로 검출된 플래그 패턴으로부터 LAP-F 프레임 중에서 정상적으로 복호된 주소 영역의 슬립 판별용 검출 비트로 사용된 확장주소 비트(2("01")/3("001")/4("0001")옥텟 구조)에 의해 결정되고 이때 슬립의 상태 유무 판별을 결정하는 문턱치는 R_{EA}와 BER의 관계로부터 유도한다.

1.1 정상적인 스트림 암호 통신일 경우

채널의 BER(Bit Error Rate)가 b인 경우 송신측에서 전송한 확장 주소 영역의 값이 2옥텟 구조에서는 상위 비트의 비트1이 "0" 이고 하위 비트의 비트1이 "1"이다. 이때 오류없이 수신측에 도착할 확률 Pr은 식 (2)로부터 얻을 수 있다.

$$Pr = (1\text{-}BER)^{16} \qquad (2)$$

이때 BER은 전송 채널의 Bit Error Rate이다. 상기 식으로부터 키 수열의 동기 이탈 현상이 발생하지 않는 정상상태의 암호 통신에서 전송 오류 R_{EA}는 식 (3)으로 결정된다.

$$R_{EA} = Pr = (1\text{-}BER)^{16} \qquad (3)$$

통신 채널의 상태가 나쁠수록 LAP-F의 슬립 검출 비트에 대한 채널 오류가 증가하고 이에 따라R_{EA}은 감소한다. BER과 R_{EA}의 관계를 그림6를 통해 살펴 보면 BER이 증가 할수록 R_{EA}은 감소함을 알 수 있다. 이는 통신 채널 환경이 채널 전송시 발생하는 오류와의 상관관계를 잘 설명해 준다.

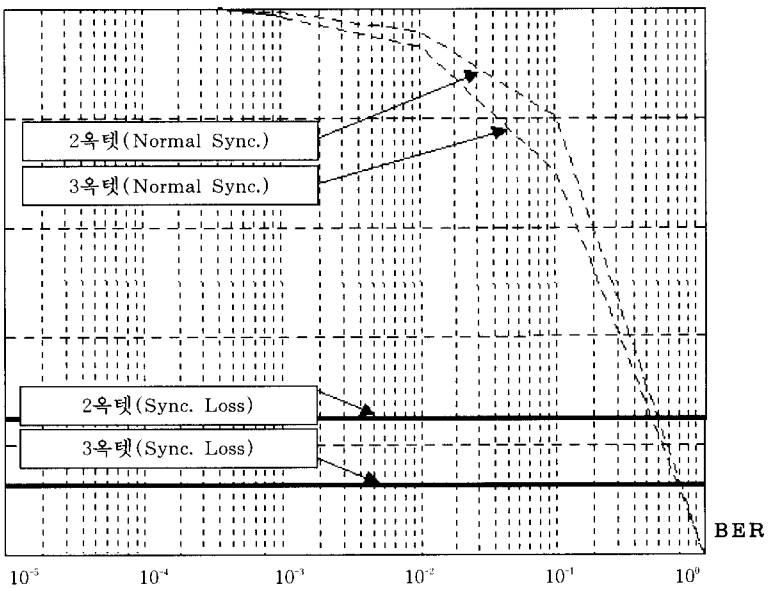


그림 6. T_u = 0.1초인 경우 BER의 변화에 따른 R_{EA}

Fig 6 R_{EA} for various BER in case that T_u is 0.1sec.

1.2 동기 이탈한 스트림 암호 통신일 경우

암호 통신 중 키 수열의 동기 이탈 현상이 발생하면 암호된 데이터의 복호시 2옥텟 구조의 주소 영역부에서 확장 주소 영역의 정보 오류 발생 확률은 $1/2^{16}$(비트)로 가정할 수 있고 T_u초 동안에 복호된 데이터에서 발생할 N_{EA}는 식(4)에서와 같이 얻을 수 있다. 이때 키 수열의 동기 이탈 현상이 발생하면 R_{EA} 값은 식 (5)에서 얻을 수 있고 일정한 값 $1/2^{16}$으로 결정된다.

$$N_{EA} = N_F \left(\frac{1}{2^{16}}\right) = \frac{1}{2^{16}} N_F \qquad (4)$$

$$R_{EA} = \frac{N_{EA}}{N_F} = \frac{1}{2^{16}} \qquad (5)$$

2. 수신률(REA)을 이용한 문턱치 결정

2.1 흐름도

키 수열의 동기 이탈이 발생한 경우 재동기를 이루는 제안된 방식은 그림 7에서 나타낸 흐름도와 같다. 먼저 복호된 비트열을 검색하여 플래그 패턴을 찾게 되면 플래그 패턴 다음 주소 영역에서 옥텟 2의 경우 상위 비트의 비트1이 "0", 하위 비트의 비트1이 "1"인지를 확인한다. 이때 옥텟 2의 경우 "01", 옥텟 3의 경우"001", 옥텟4의 경우"0001"이 검출되면 정상적으로 복호된 것으로 판단하여 계수를 증가시킨다.

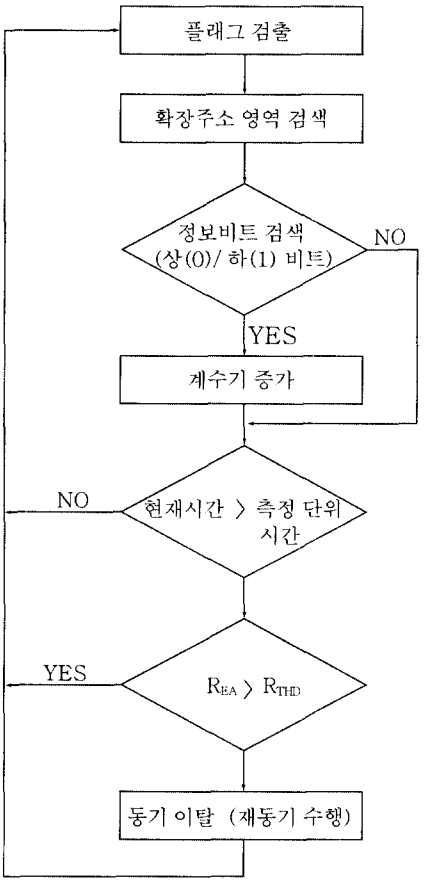


그림 7. 제안된 알고리즘의 흐름도

Fig. 7 The flow chart of proposed algorithm

이와 같은 과정을 주어진 측정 단위시간 동안 수행하고 수행된 단위 시간동안의 정상적으로 수신된 수신률을 문턱치와 비교하여 문턱치보다 크면 정상적으로 키 수열의 동기 이탈이 발생하지 않은 것으로 판단하고, 동기 이탈 발생 여부를 계속적으로 감시하다가 문턱치보다 작은 경우가 발생하면 동기 이탈이 발생한 것으로 판단하여 재동기 과정 즉, 동기 패턴과 세션 키를 전송하여 신뢰성있는 통신이 가능하도록 한다.

2.2 R_{EA}의 결정

R_{EA}의 결정은 채널의 BER에 영향을 받으므로 채널의 조건으로부터 키 수열의 동기 이탈 현상이 존재하는 경우와 존재하지 않는 경우로 구분하여 결정하여야 한다. R_{EA}는 단위 측정 시간 Tu에 따라 문턱치를 구분하여 그림 6을 통해 나타내었다. 문턱치의 값을 큰 값으로 결정하게 되면 키 수열의 동기 이탈 상태를 검출 하지 못하는 현상이 감소하게 되지만 이에 반해 정상적으로 통신하는 경우를 키 수열의 동기 이탈로 잘못 판단하는 현상이 증가할 것이다. 또한 문턱치의 값을 적게할 수록 정상적인 통신을 키 수열의 동기 이탈 현상으로 잘못 판단하는 경우가 감소하게 될 것이나 키 수열의 동기 이탈 현상을 감지하지 못하는 현상이 증가할 것이다. 따라서 문턱치는 제안되는 동기식 암호 시스템에 따라 적합한 위치에서의 결정이 요구되므로 본 논문에서는 그림 6에서 나타난바와 같이 옥텟에 따라 달리 결정하였다.

V. 실험 결과 및 고찰

1. 실험 방법

종래의 주기적인 재동기 방식과 제안된 비주기적인 재동기 방식의 성능 평가는 오복호율 R_{Error}와 재동기를 위해 요구되는 비트 전송량 R_D비율을 통해 판별하였다.

$$R_{Error} = \frac{D_{Error}}{D_t} \qquad (6)$$

여기서 D_t 는 암호기에서 전송된 전체 데이터의 비트 수이며 D_{Error}는 오복호된 데이터의 비트 수이다.

R_{Error}는 전송한 전체 데이터로부터 복호기에서 오복호된 데이터 비를 나타내며 D_{Error}가 낮을수록 키 수열의 동기 이탈 현상을 정확하고 신속하게 검출하여 재동기 과정을 수행하게

된다. 동일 채널 환경과 키 수열 동기 이탈 환경으로부터 성능 분석은 R_{Error}을 통해 파악할 수 있다.

또한, 재동기를 위해 요구되는 데이터 비트수 R_D는 암호화된 데이터에 재동기를 위한 동기 패턴(128비트)과 세션 키 비트(128비트를 (15,4) 최대길이 부호화)로 구성하였다. 구성된 동기식 암스트림 암호 통신 시스템을 이용하여 64Kbps환경에서 10^6비트의 특정 데이터 패턴을 암호화 및 복호화 수행을 10회 반복 실시하여 측정된 데이터 R_{Error}와 D_{Error}의 평균 값을 측정하였다. 이때 송,수신 수행 과정에서 10^{-6}, 10^{-7}, 10^{-8}비트의 발생율로 키 수열의 동기 이탈을 유발하고 발생된 동기 이탈은 동기 패턴과 세션 키 부분에서는 발생하지 않고 암호문의 임의의 부분에서만 발생시켰다. 이때 전송 채널에서의 평균 BER은 10^{-6}비트로 실험을 수행하였다.

2. 오복호율

동기적인 스트림 암호 통신에서 동기 패턴 검출을 위해 주기적인 동기 패턴을 전송방식과 제안된 비주기적인 동기 패턴 전송방식으로 전송하여 얻은 결과를 표2~표6을 통해 제시하고 있다. 주기적인 동기 방식에서 재동기 주기를 T_c로 정하고 동기 이탈이 발생한 이후 재동기를 이루기 위해 소요되는 평균 시간은 $T_c/2$에 해당하지만 비주기적인 동기 방식에서는 재동기를 이루기 위해 소요되는 평균 시간은 단위 측정 시간 T_u이 소요된다. 이와 같은 경우 T_u가 T_c보다 훨씬 짧은 시간으로 결정되므로 비주기적인 재동기 방식을 이용하므로써 보다 짧은 시간에 동기를 이룰수 있다. 상기 두 방식을 통해 재동기를 수행할 때 소요되는 소요 시간비(R_{Time})를 다음 식에서 제시하고 있다.

$$R_{time} \cong \frac{T_c}{2T_u} \qquad (7)$$

여기서 T_c는 주기적인 재동기 주기이고 T_u는 비주기적인 재동기의 단위 측정 시간이다.

〈표 2〉 채널 속도 64Kbps 환경에서 제한된 비주기적인 동기 방식의 단위측정시간 T_u 변화에 따른 R_{Error}과 D_{Error}의 비교

〈Table 2〉 The comparison of R_{Error} and D_{Error} of a non-periodic synchronization method for various T_u at 64Kbps.

64Kbps 채널속도										
T_u / Slip Rate	50msec		100msec		200msec		500msec		1sec	
	D_{Error}	R_{Error}	D_{Error}	R_{Error}	D_{Error}	R_{Error}	D_{Error}	R_{Error}	D_{Error}	R_{Error}
10^{-6}	1.8×10^{6}	1.8×10^{-3}	3.4×10^{6}	3.4×10^{-3}	6.6×10^{6}	6.6×10^{-3}	1.8×10^{7}	1.8×10^{-2}	3.4×10^{7}	3.4×10^{-2}
10^{-7}	1.8×10^{5}	1.8×10^{-4}	3.4×10^{5}	3.4×10^{-4}	6.6×10^{5}	6.6×10^{-4}	1.8×10^{6}	1.8×10^{-3}	3.4×10^{6}	3.4×10^{-3}
10^{-8}	1.9×10^{6}	1.9×10^{-5}	3.6×10^{4}	3.6×10^{-5}	6.7×10^{4}	6.7×10^{-5}	1.9×10^{5}	1.9×10^{-4}	3.6×10^{5}	3.6×10^{-4}

〈표 3〉 채널 속도 64Kbps 환경에서 주기적인 동기 방식으로 109비트 데이터 전송시 T_C변화에 따른 R_{Error}과 D_{Error}의 비교

〈Table 3〉 The comparison of R_{Error} and D_{Error} of a periodic synchronization method for various T_C at 64Kbps.

64Kbps 채널속도										
T_u / Slip Rate	500msec		1sec		2sec		5sec		10sec	
	D_{Error}	R_{Error}	D_{Error}	R_{Error}	D_{Error}	R_{Error}	D_{Error}	R_{Error}	D_{Error}	R_{Error}
10^{-6}	9×10^{6}	9×10^{-3}	1.8×10^{7}	1.8×10^{-2}	3.6×10^{7}	3.6×10^{-2}	9×10^{7}	9×10^{-2}	3.6×10^{8}	3.6×10^{-4}
10^{-7}	9×10^{5}	9×10^{-4}	1.8×10^{6}	1.8×10^{-3}	3.6×10^{6}	3.6×10^{-3}	9×10^{6}	9×10^{-3}	3.6×10^{7}	3.6×10^{-2}
10^{-8}	1.0×10^{5}	1.0×10^{-4}	2.0×10^{4}	2.0×10^{-4}	4.0×10^{-4}	4.0×10^{-4}	1.0×10^{6}	1.0×10^{-3}	4.0×10^{6}	4.0×10^{-3}

〈표 4〉 채널 속도 64Kbps 환경에서 109 비트의 데이터 전송시 요구되는 오버헤더 비트 수의 비교.

〈Table 4〉 The comparison of overhead bits, channel rate = 64Kbps and slip rate = 10^{-7}bits.

동기방식 / Slip Rate	주기적인 동기 방식 (bits)/(T_C=1sec)	비주기적인 동기 방식 (bits)/(T_u=1sec)
10^{-7}	9.6×10^{6}	6.4×10^{5}

〈표 5〉 채널 속도 384Kbps 환경에서 제안된 비주기적인 동기 방식의 단위 측정 시간 T_u 변화에 따른 R_{Error}과 D_{Error}의 비교

〈Table 5〉 The comparison of R_{Error} and D_{Error} of a non-periodic synchronization method for various T_u at 384Kbps.

384Kbps 채널속도										
T_u / Slip Rate	50msec		100msec		200msec		500msec		1sec	
	D_{Error}	R_{Error}	D_{Error}	R_{Error}	D_{Error}	R_{Error}	D_{Error}	R_{Error}	D_{Error}	R_{Error}
10^{-6}	4.9×10^{6}	4.9×10^{-3}	9.7×10^{6}	9.7×10^{-3}	2.0×10^{7}	2.0×10^{-2}	4.9×10^{7}	4.9×10^{-2}	9.7×10^{7}	9.7×10^{-2}
10^{-7}	4.9×10^{5}	4.9×10^{-4}	9.8×10^{5}	9.8×10^{-4}	2.0×10^{6}	2.0×10^{-3}	4.9×10^{6}	4.9×10^{-3}	9.7×10^{6}	9.7×10^{-3}
10^{-8}	5.0×10^{4}	5.0×10^{-5}	1.0×10^{5}	1.0×10^{-4}	2.1×10^{5}	2.1×10^{-4}	5.0×10^{5}	5.0×10^{-4}	9.8×10^{5}	9.8×10^{-4}

〈표 6〉 채널 속도 384Kbps 환경에서 주기적인 동기 방식으로 3x109비트 데이터 전송시 T_C변화에 따른 R_{Error}과 D_{Error}의 비교

〈Table 6〉 The comparison of R_{Error} and D_{Error} of a periodic synchronization method for various T_C at 384Kbps.

384Kbps 채널속도										
T_u / Slip Rate	500msec		1sec		2sec		5sec		10sec	
	D_{Error}	R_{Error}	D_{Error}	R_{Error}	D_{Error}	R_{Error}	D_{Error}	R_{Error}	D_{Error}	R_{Error}
10^{-6}	4.9×10^{7}	4.9×10^{-2}	9.7×10^{7}	9.7×10^{-2}	2.2×10^{8}	2.2×10^{-1}	4.9×10^{8}	4.9×10^{-1}	9.7×10^{8}	9.7×10^{-1}
10^{-7}	4.9×10^{6}	4.9×10^{-3}	9.7×10^{6}	9.7×10^{-3}	2.2×10^{7}	2.2×10^{-2}	4.9×10^{7}	4.9×10^{-2}	9.7×10^{7}	9.7×10^{-2}
10^{-8}	5.0×10^{5}	5.0×10^{-4}	9.9×10^{5}	9.9×10^{-4}	2.3×10^{6}	2.3×10^{-3}	5.0×10^{6}	5.0×10^{-3}	9.8×10^{6}	9.8×10^{-3}

T_c를 1sec로 하고 T_u를 약 0.2sec라 가정하면 이때 소요 시간비는 5이다. 이것은 주기적인 재동기 방식에 비해 비주기적인 재동기 방식이 재동기를 이루기 위해 소요되는 시간이 5배가 빠르다는 것을 의미한다. 109 비트의 데이터를 1초 단위로 동기 패턴과 세션키를 삽입하여 주기적으로 암호화하여 전송할 경우 요구되는 총 오버헤드 비트 수는 9.6×10^{6} 비트가 요구된다. 이에 반해 단위 측정 시간이 0.1sec이고 동기 이탈률이 10^{-7}비트인 비주기적인 동기 전송의 암호 통신에서 요구되는 총 오버헤드 비트 수는 6.41×10^{5} 비트가 필요하다.

VI. 결 론

본 논문은 프레임릴레이 프로토콜 환경에서 암호 통신 시스템에 적합한 비주기적 재동기 알고리즘을 제안하였다. 제안된 주소영역의 확장 비트를 이용한 키 스트림 동기 방식은 단위 측정 시간 동안 측정된 프레임릴레이 프로토콜의 주소영역의 확장 비트 정보와 플래그 패턴의 수신률을 이용하여 문턱 값보다 작은 경우에 동기 신호와 세션 키를 전송하므로써 종래의 주기적인 동기 방식에서 전송 효율성 저하와 주기적인 상이한 세션 키 발생, 다음 주기까지 동기 이탈 상태로 인한 오류 확산 등의 단점을 해결하였다. 제안된 알고리즘을 적용하여 시험한 결과 주기적인 동기 방식에 비해 오복호율을 감소하면서, 빠른 시간에 동기화가 가능하다.

참고문헌

[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, Oct. 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] ITU-T Rec. X.25, pp.113 - pp.116, 1984.

[7] ITU-T Rec. X.25, pp.126 - pp.127, 1984.

[8] M. Y. Lee, " Error-Correcting Coding Theory ", McGraw-Hill, 1989.

[9] ITU-T Rec. I.222, Framework for Providing Additional Packet Mode Bearer Services.

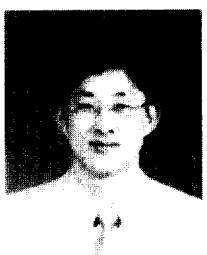
[10] ITU-T Rec. I.233, Service Architecture for Frame Mode Bearer Services.

[11] ITU-T Rec. Q.921, ISDN User Network Interface, Data Link Layer Specification.

[12] ITU-T Rec. Q.922, ISDN Data Link Layer Specification for Frame Mode Bearer Services.

[13] D. B. Grossman, "An overview of frame relay technology", Proceedings of INFOCOM '91, pp.539- 545,1991.

□ 著者紹介



홍 진 근

1991년 2월 경북대학교 전자공학과 졸업(공학사)
1994년 2월 경북대학교 전자공학과 졸업(공학석사)
1996년 3월 - 현재 경북대학교 전자공학과 박사과정

윤 장 홍

1983년 2월 경북대학교 전자공학과 졸업(공학사)
1987년 2월 경북대학교 전자공학과 졸업(공학석사)
1998년 2월 경북대학교 전자공학과 졸업(공학박사)

윤 정 오

1989년 2월 경북대학교 전자공학과 졸업(공학사)
1991년 2월 경북대학교 전자공학과 졸업(공학석사)
1996년 3월 - 현재 경북대학교 전자공학과 박사과정
1998년 7월 - 현재 한국산업대학교 정보통신공학과 전임강사

황 찬 식

1977년 2월 서강대학교 전자공학과 졸업(공학사)
1979년 8월 한국과학기술원 전기전자공학과 졸업(공학석사)
1996년 2월 한국과학기술원 전기전자공학과 졸업(공학박사)
1991년 8월 - 1992년 8월 UTA 방문교수
1979년 9월 - 현재 경북대학교 전자전기공학부 교수