論文 97-22-8-18

동기식 스트림 암호 통신에 적합한 사이클 슬립 보상 알고리즘

正會員 윤 장 홍*, 강 건 우*, 황 찬 식**

A Compensation Algorithm of Cycle Slip for Synchronous Stream Cipher

Jang Hong Yoon*, Ken Woo Kang*, Sik Chan Hwang** *Regular Members*

요 약

PLL을 사용하는 통신 시스템에서는 선로 잡음에 의해서 사이클 슬립 현상이 발생 할 수 있다. 이 사이클 슬립 현상이 동기식 스트림 암호 통신 시스템에 발생하면 난수 동기 이탈 현상을 발생시켜 통신을 할 수 없게된다. 이러한 난수 동기 이탈의 위험성을 줄이기 위하여 연속 재동기 방식을 사용하지만 이에 따른 문제점이 있다. 본 논문에서는 수신 클럭 복원시에 사용되는 수신 클럭 보상 알고리즘을 연속 재동기 방식에 적용하여 기존의 연속 재동기 방식의 문제점을 해결하는 방법을 제안하였다. 즉, 정해진 기준 시간 동안에 실제 수신 클럭 펄스 수를 계수하여 얻은 계수치와 동일 시간 동안에 사이클 슬립이 발생하지 않은 정상 상태에서의 수신 클럭 펄스 수인 정상치가 일치하지 않으면 사이클 슬립이 발생된 것으로 판단하여 훼손된 수신 클럭을 사이클 슬립의 발생 형태에 따라 클럭 펄스를 더해주거나 빼주는 방법을 연속 재동기 방식과 같이 사용하였다.

제안된 방법을 절대 클럭 동기를 요구하는 동기식 스트림 암호 통신 시스템에서 시험한 결과 기존의 연속 재동기 방법에 비하여 재동기 시간을 최대 20배까지 단축시켰는데 그것은 전송 데이터 량을 17.8% 감축하는 효과와 동일하다.

ABSTRACT

The communication systems which include PLL may have cycle clip problem because of channel noise. The cycle slip problem occurs the synchronization loss of communication system and it may be fatal to the synchronous stream cipher sytem.

While continuous resynchronization is used to lessen the risk of synchronization it has some problems. In this

*국방과학연구소
**경북대학교 전기전자공학부
論文番號:97033-0122
接受日字:1997年 1月 22日

paper, we propose the method which solve the problems by using continuous resynchronization with the clock recovery technique. If the counted value of real clock pulse in reference duration is not same as that of normal state, we decide the cycle slip has occurred. The damaged clock by cycle slip is compensated by adding or subtracting the clock pulse according to the type of cycle slip. It reduced the time for resynchronization by twenty times. It means that 17.8% of data for transmit is compressed.

Ⅰ. 서 론

컴퓨터 네트워크나 통신 네트워크를 통하여 중요 정보를 전송할 때 비인가자의 도용이나 도청 또는 정보 파괴 및 변조 등으로부터 정보를 보호하기 위하여 송신측에서는 암호기로 정보를 암호화하여 전송하고 수신측에서는 복호기로 이를 해독하여 인가자만이 원래의 정보를 얻도록 하는 방법을 사용한다. 그런데 암호기(encryptor)에서 전송한 암호문이 복호기(decryptor)에서 정상적으로 복호되기 위해서는 암호기에서 사용한 난수와 복호기에서 사용한 난수가 일치하여야 하나 여러가지 원인에 의하여 암호기의 난수와 복호기의 난수가 일치하지 않는 경우가 발생하는데 이를 흔히 난수 동기 이탈이라 한다. 동기식 스트림 방식을 사용하는 암호 시스템에서의 난수 동기 이탈은 주로 수신 클럭의 사이클 슬립에 의해서 발생되는데 난수 동기 이탈 현상이 발생하면 통신을 할 수 없을 뿐 아니라 복호된 데이터는 임의의 값을 가지므로 수신 시스템을 오동작시킬 수 있다[1-4]. 이러한 위험성을 줄이기 위하여 동기식 스트림 암호 체계에서는 암호문에 동기 패턴과 세션 키를 주기적으로 전송하여 암, 복호기의 난수열을 일치시키는 연속 재동기 방식을 흔히 사용하지만 몇가지 문제점들이 있다[5]. 첫째, 연속 재동기 방식은 주기적으로 재동기를 이루므로 한 주기 내에서 난수 동기 이탈이 발생하면 다음 동기 패턴과 세션 키를 수신할 때까지 동기 이탈 상태가 유지되어 통신을 할 수 없게 된다. 둘째, 연속 재동기 방식은 난수 동기 이탈의 발생과 무관하게 주기적으로 동기 패턴과 세션 키를 전송하여야 하므로 전송 효율이 떨어질 뿐아니라 매번 다른 세션 키를 발생하여 전송하여야 하는 부담이 있다. 셋째, 세션 키를 전송하는 과정에서 세션 키에 전송 오류가 발생하면 다음 동기 패턴과 세션 키를 수신할 때까지 동기 이탈된 상태가 유지되어 오류가 확산된다.

본 논문에서는 수신 클럭에 사이클 슬립 현상이 발생하면 이를 보상하여 주는 방법을 연속 재동기 방식과 병행하여 사용하므로써 연속 재동기 방식의 문제점을 개선하는 방법을 제안하였다. 즉, 일정 기준 시간 동안 수신 클럭 펄스를 계수하여 구한 실계수치에서 동일 시간 동안에 사이클 슬립이 발생되지 않은 정상 상태에서의 수신 클럭 펄스의 갯수인 정상치를 뺀 차로서 사이클 슬립 현상의 발생 유무를 판단한 후 사이클 슬립 현상이 발생된 경우에는 사이클 슬립의 발생 형태에 따라 클럭 펄스를 수신 클럭에 가감하여 주는 사이클 슬립 보상 알고리즘을 연속 재동기 방식에 적용하여 흐트러진 암호 통신 시스템의 동기를 복원하였다. 제안된 방법을 사용하면 연속 재동기 방식만을 사용하는 경우보다 재동기를 위한 동기 패턴과 세션 키를 전송하는 주기를 길게 할 수 있으므로 연속 재동기 방식의 문제점을 개선할 수 있다. 제안된 방법의 성능 평가를 위한 시험은 전화망이나 음성용 통신망을 이용한 컴퓨터 통신이나 팩시밀리 통신 또는 무선 데이터 통신을 할 때 주로 사용하는 PLL이 내장된 9,600-28,800bps급 모뎀을 이용하였으며 사이클 슬립 발생기로 사이클 슬립을 인위적으로 발생시키면서 제안된 방법이 얼마나 효과적으로 난수 재동기를 이루는가를 알아보았다.

Ⅱ. 사이클 슬립 보상 알고리즘

사이클 슬립은 PLL이 선로 잡음 등의 영향으로 수신 클럭을 정상적으로 복원하지 못하는 현상을 말하는 것으로 수신 클럭 펄스를 빠뜨리거나 더하는 두 가지 형태로 발생된다. 본 논문에서는 암호 통신 시스템에서 사용하는 모뎀의 수신 클럭에 사이클 슬립 현상이 발생하였을 경우에 다음과 같은 방법으로 사이클 슬립에 의해 훼손된 수신 클럭을 보상하여 주었다.

현재 일반적으로 사용되고 있는 모뎀의 송신 클럭

주파수는 ITU-T에서 ±0.01%, 즉 100ppm 이내의 오차를 갖도록 권고하고[6] 있으나 실제로 이것이 정확하게 지켜지지 않는 실정이며 지켜진다 하더라도 각 모뎀내의 수정 발진자(crystal oscillator)의 온도 특성 및 정밀도의 특성에 따라 송신 클럭의 오차가 조금씩 다르므로 이를 측정한 후 상대측에 전달하여 수신 클럭 펄스 계수용 기준 시간을 발생할 때 반영한다면 보다 정확하게 사이클 슬립 현상을 찾아낼 수 있을 것이다. 송신 클럭 오차를 측정하는 방법은 다음과 같다. 예를 들어, 통신 속도가 9,600bps인 경우, 송신 클럭의 동작 오차가 전혀 없다면 송신 클럭의 펄스 9,600개를 계수하는 동안에 측정된 시간은 정확히 1초를 나타낼 것이다. 그러나 송신 클럭이 오차를 갖는다면 송신 클럭의 펄스 9,600개를 계수하는 동안에 측정된 시간은 송신 클럭의 동작 오차에 해당되는 길이 δ만큼의 오차가 더해진 $(1\pm\delta)$초 일 것이다. 이 δ를 상대측으로 전송하여 주면 상대측에서는 이 δ를 반영한 기준 시간을 발생시키고 이 기준 시간 동안에 모뎀으로부터 공급되는 수신 클럭 펄스를 계수하는데 통신 속도가 9,600bps이고 기준 시간을 $(1\pm\delta)$초로 정하였다면, 사이클 슬립이 발생하지 않은 정상적인 경우에는 기준 시간 동안에 계수되는 수신 클럭 펄스의 갯수는 9,600개 이어야 한다. 만일, 계수된 수신 클럭 펄스의 갯수가 9,600이 아니라면 사이클 슬립이 발생한 것으로 판단하여 이를 보상하여 준다. 그림 1은 통신 속도가 9,600bps이고 기준 시간의 길이는 $(1+\delta)$초인 경우에 수신 클럭 펄스가 하나 빠지는 형태의 사이클

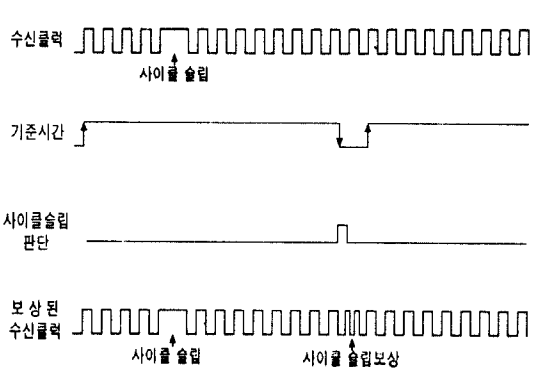
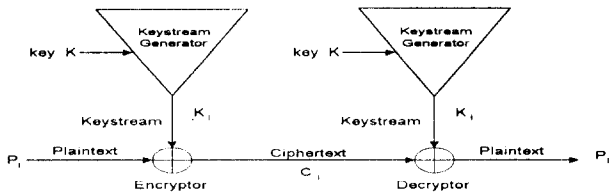


그림 1. 손상된 수신 클럭 보상 타이밍 다이아그램
Fig. 1 The timming diagram of compensation for damaged clock in receiver.

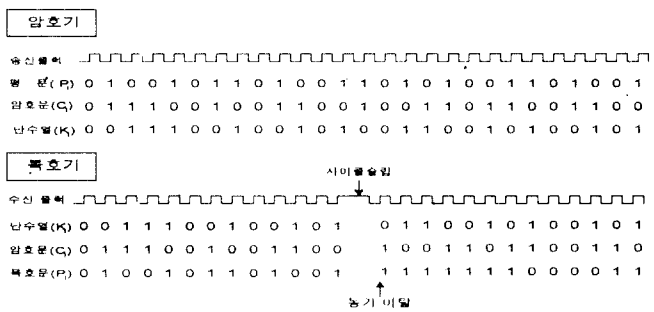
슬립이 발생하였을 때 수신 측에서 사이클 슬립을 감지하고 보상하는 과정을 나타낸다. 그림 1의 경우는 수신 클럭 펄스가 한 개 빠지는 형태의 사이클 슬립이 발생하였으므로, 기준 시간 동안에 모뎀을 통해서 공급되는 수신 클럭 펄스를 계수한 후 9,600을 빼면 결과 값은 −1이 될 것이다. 따라서 사이클 슬립에 의해서 빠진 수신 클럭을 보상하기 위해서 강제적으로 수신 클럭 펄스를 하나 더 만들어 DTE에 공급하여 주면 DTE는 공급되는 클럭의 rising egde 또는 falling edge만을 판단하여 데이터를 표본하기 때문에 사이클 슬립에 의해서 잠시 흐트러진 클럭 동기는 자연스럽게 회복된다.

Ⅲ. 사이클 슬립 보상 알고리즘이 적용된 연속 재동기 방식

그림 2와 같이 표현되는 동기식 스트림 암호 통신은 암, 복호기에서 사용하는 난수열 K_i가 서로 일치하여야만 복호기에서 원래의 정보 P_i를 복원할 수 있으나 선로 잡음에 의한 사이클 슬립이 발생하면 암, 복호기에서 사용하는 난수열 K_i가 서로 어긋나 그 이후부터의 모든 암호문은 제대로 복원할 수 없게된다[4-5][7-9]. 이러한 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 3과 같이 암, 복호기가 주기적으로 동기 패턴과 세션키이를 주고 받음으로써 서로 동일한 세션 키이로 난수열 발생기의 internal state 값을 주기적으로 동일하게 만들어 재동기를 이룬다[5]. 이러한 연속 재동기 방식은 사이클 슬립이 일어나 난수 동기 이탈이 발생하여도 주기적으로 재동기를 이루므로 비교적 안정된 통신을 가능하게 하나, 그림 3에 나타난 바와 같이 주기 내에서 동기 이탈이 발생하면 다음 재동기까지는 암호문을 정상적으로 복원할 수 없는 단점이 있으므로 재동기 주기가 길어지면 정상적으로 복원하지 못하는 암호문의 양이 증가하여 전반적인 통신 품질을 저하시킨다. 반면에 재동기 주기를 짧게 하면 전송하여야할 동기



(a)



(b)

그림 2. 동기식 스트림 암호 통신 시스템의 구성과 사이클 슬립에의한 동기 이탈이 발생한 경우
(a) 동기식 스트림 암호 통신 시스템 구성
(b) 사이클 슬립에의한 동기 이탈이 발생한 경우

Fig. 2 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

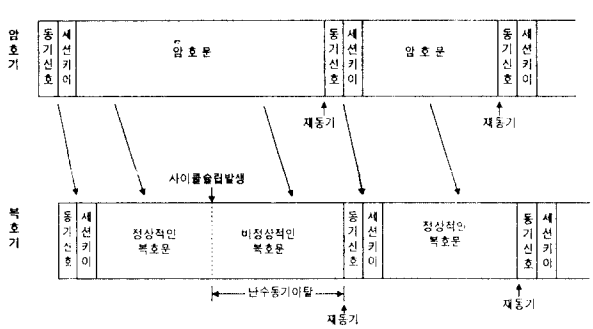


그림 3. 난수 동기 이탈 발생시의 연속 재동기 방식 구조

Fig. 3 The structure of continuous resynchronization with synchronization loss

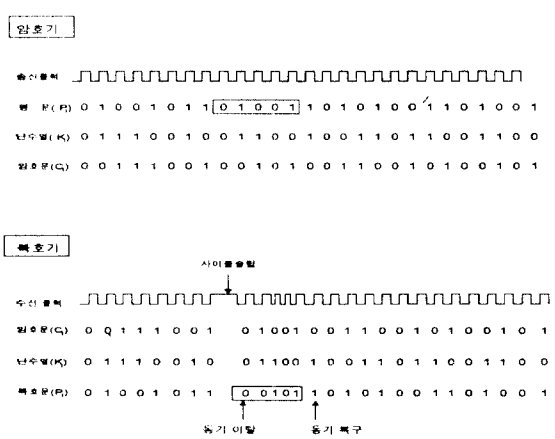


그림 4. 사이클 슬립 보상에 의한 재동기

Fig. 4 The resynchronization by cycle slip compensation

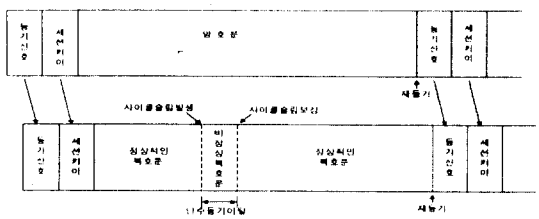


그림 5. 사이클 슬립 보상 알고리즘이 적용된 연속 재동기 방식의 구조

Fig. 5 The structure of continuous resynchronization with cycle slip compensation

패턴과 세션 키이의 양이 증가하여 통신 효율을 떨어뜨린다. 이러한 연속 재동기 방식의 단점을 보완하기 위하여 본 논문에서는 사이클 슬립 보상 알고리즘을 연속 재동기 방식에 적용하여 동기 이탈되는 구간을 단축시켰다. 그림 4는 수신 클럭 펄스가 송신 클럭 펄스에 비해 한 개 빠지는 형태의 사이클 슬립 현상이 발생하여 난수 동기 이탈이 일어났을 경우에 사이클 슬립 보상 알고리즘을 적용하여 수신 클럭을 보상하여 줌으로써 난수 재동기를 이루는 과정을 나타낸다. 이러한 사이클 슬립 보상 알고리즘을 연속 재동기 방식에 적용하면 그림 5와 같이 난수 동기 이탈 구간이 감소하여 보다 안정된 암호 통신이 가능하다.

Ⅳ. 실험 및 고찰

1. 실험 방법

그림 6과 같이 구성된 동기식 스트림 암호 통신 시스템에 10^9 비트의 특정 패턴으로 구성된 데이터를 송, 수신할 때 의도적으로 사이클 슬립을 발생하면서 연속 재동기 방식에 사이클 슬립 보상 알고리즘을 적용한 경우와 적용하지 않은 경우의 성능을 비교하였다. 사이클 슬립 현상은 사이클 슬립 발생기를 이용하여 10^{-6}~10^{-8} 비트 비율로 사이클 슬립을 발생시켰는데 이 때, 사이클 슬립 현상은 그림 3의 연속 재동기 방식의 구성중 동기 패턴과 세션 키이 부분에서는 발생치 않고 암호문의 임의 부분에서만 발생하도록 하였다. 본 논문에서는 객관적 성능 평가를 위하여 식 (1)과 같이 표현되는 오복호율 R_{ed}와 수신측에서 잘못 복호된 데이터의 양 D_{err}을 사용하였는데 오복호율 R_{ed}는 전송된 총 데이터와 복호기에서 잘못 복호된 데이터의 비를 나타낸다. 즉, 이것은 동기 이탈이 발생된 후에 얼마나 빨리 재동기를 이루었나를 측정하는 척도이기도 하다.

$$R_{ed} = \frac{D_{err}}{D_t} \tag{1}$$

여기서 D_t는 암호기가 전송한 데이터 총 비트 수이며 D_{err}은 잘못 복호된 데이터 비트 수이다.

또한, 기준 시간의 길이와 통신 속도가 제안된 사이클 슬립 보상 알고리즘의 성능에 어떤 영향을 미치는가를 알아보기 위하여 9,600~28,800bps의 통신 속도에서 기준 시간의 길이를 변화시키면서 실험하였다.

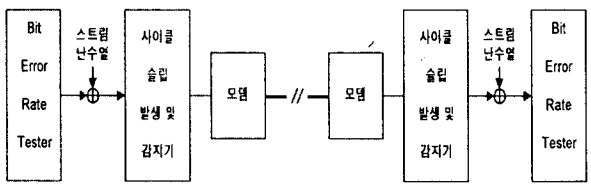


그림 6. 실험에 사용된 동기식 스트림 암호 통신 시스템

Fig. 6 The secure communication system be used in simulation.

2. 결과 및 고찰

표 1과 표 3은 연속 재동기 방식에 사이클 슬립 보상 알고리즘을 적용한 경우와 적용하지 않은 각 경우에 대하여 통신 속도 9,600bps인 경우는 10^9 bits 길이의 특정 데이터 패턴을, 통신 속도 28,800bps인 경우는 $3*10^9$ bits 길이의 특정 데이터 패턴을 암호화하여 전송한 후 복호기에서 복호하는 시험을 각 속도에 대하여 10회 실시한 후에 측정된 R_{ed}와 D_{err}의 평균값을 나타낸다. 이 때, 사이클 슬립 보상 알고리즘에 사용된 수신 기준 시간의 길이는 약 1초(9,600bps인 경우는 송신 클럭 9,600개 만큼의 시간, 28,800bps인 경우는 28,800개 만큼의 시간)와 0.5초(9,600bps인 경우는 송신 클럭 4,800개 만큼의 시간, 28,800bps인 경우는 14,400개 만큼의 시간)로 하였고, 연속 재동기 주기 T는 10초로 하여 실험하였다. 연속 재동기 주기는 통신 시스템의 특성에 따라 가변적일 수 있으나 너무 길게 하면 동기 이탈 시 재동기까지의 시간이 길어져

표 1. 통신 속도 9,600bps, 재동기 주기 T = 10초 일 때 D_{err}과 R_{ed}의 비교

Table 1. The comparison of D_{err} and R_{ed} in case that the period of resynchronization, T, is 10sec and speed is 9,600bps

	연속 재동기 방식 (재동기주기 = 10초)		연속 재동기 방식 + 사이클 슬립 보상 (p = 1초)		연속 재동기 방식 + 사이클 슬립 보상 (p = 0.5초)	
사이클 슬립발생률	D_{err}(bits)	R_{ed}(%)	D_{err}(bits)	R_{ed}(%)	D_{err}(bits)	R_{ed}(%)
10^{-6}	4.8×10^{7}	4.800	4.8×10^{6}	0.480	2.4×10^{6}	0.240
10^{-7}	4.8×10^{6}	0.480	4.8×10^{5}	0.048	2.4×10^{5}	0.024
10^{-8}	4.8×10^{5}	0.048	4.8×10^{4}	0.004	2.4×10^{4}	0.002

표 2. 통신 속도 9,600bps인 연속 재동기 방식에서 재동기 주기 T의 변화에 따른 D_{err}와 R_{ed}의 비교

Table 2. The comparison of D_{err} and R_{ed} for various period of resynchronization, T, in 9,600bps.

	연속 재동기 방식 (재동기주기 = 10초)		연속 재동기 방식 (재동기주기 = 5초)		연속 재동기 방식 (재동기주기 = 0.5)	
사이클 슬립발생률	D_{err}(bits)	R_{ed}(%)	D_{err}(bits)	R_{ed}(%)	D_{err}(bits)	R_{ed}(%)
10^{-6}	4.8×10^{7}	4.800	2.4×10^{7}	2.400	2.4×10^{6}	0.240
10^{-7}	4.8×10^{6}	0.480	2.4×10^{5}	0.240	2.4×10^{5}	0.024
10^{-8}	4.8×10^{5}	0.048	2.4×10^{5}	0.024	2.4×10^{4}	0.002

표 3. 통신 속도 28,800bps, 재동기 주기 T = 10초 일 때 D_{err}과 R_{ed}의 비교

Table 3. The comparison of D_{err} and R_{ed} in case that the period of resynchronization, T, is 10sec and speed is 28,800bps.

	연속 재동기 방식 (재동기주기 = 10초)		연속 재동기 방식 + 사이클 슬립 보상 (p = 1초)		연속 재동기 방식 + 사이클 보상 (p = 0.5초)	
사이클 슬립발생률	D_{err}(bits)	R_{ed}(%)	D_{err}(bits)	R_{ed}(%)	D_{err}(bits)	R_{ed}(%)
10^{-6}	4.2×10^{8}	14.00	4.2×10^{7}	1.400	2.1×10^{7}	0.700
10^{-7}	4.2×10^{7}	1.400	4.2×10^{6}	0.140	2.1×10^{6}	0.070
10^{-8}	4.2×10^{6}	0.140	4.2×10^{5}	0.014	2.1×10^{5}	0.007

표 4. 통신 속도 28,800bps인 연속 재동기 방식에서 재동기 주기 T의 변화에 따른 D_{err}와 R_{ed}의 비교

Table 4. The comparison of D_{err} and R_{ed} for various period of resynchronization, T, in 9,600bps.

	연속 재동기 방식 (재동기주기 = 10초)		연속 재동기 방식 (재동기주기 = 5초)		연속 재동기 방식 (재동기주기 = 0.5초)	
사이클 슬립발생률	D_{err}(bits)	R_{ed}(%)	D_{err}(bits)	R_{ed}(%)	D_{err}(bits)	R_{ed}(%)
10^{-6}	4.2×10^{8}	14.00	2.1×10^{8}	7.00	2.1×10^{7}	0.700
10^{-7}	4.2×10^{7}	1.40	2.1×10^{7}	0.70	2.1×10^{6}	0.070
10^{-8}	4.2×10^{6}	0.14	2.1×10^{6}	0.07	2.1×10^{5}	0.007

표 5. 통신 속도 9,600bps인 연속 재동기 방식으로 10^9 비트의 데이터 전송시에 요구되는 잉여 비트 수의 비교.
Table 5. The comparison of total dummy bits in 9,600bps when 10^9 bits is transmitted by continuous resynchronization method.

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

표 6. 통신 속도 28,800bps인 연속 재동기 방식으로 $3*10^9$ 비트의 데이터 전송시에 요구되는 잉여 비트 수의 비교.
Table 6. The comparison of total dummy bits in 28,800bps when $3*10^9$ bits is transmitted by continuous resynchronization method.

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

복호율이 떨어지고, 너무 짧게 하면 동기 신호와 세션 키이를 자주 전송하여야 하므로 부가 정보가 많아져 통신 효율이 떨어지는 단점이 있으므로 시스템 설계시 주기 T는 해당 통신 시스템의 특성에 따라 적절히 결정하여야 한다. 표 1~표 6에서 보는 바와 같이 사이클 슬립 보상 알고리즘을 연속 재동기 방식에 적용하였을 경우가 그렇치 않은 경우보다 사이클 슬립의 발생률에 무관하게 R_{ed}와 D_{err}가 훨씬 감소됨을 알 수 있는데 이것은 사이클 슬립 보상 알고리즘을 적용하면 동기 이탈 후 재동기를 이루는데 소요되는 시간이 훨씬 짧기 때문이다. 즉, 연속 재동기 방식만을 사용한 경우에는 동기 이탈이 발생하여 재동기를 이루는데 소요되는 시간은 평균적으로 T/2이나 사이클 슬립 보상 알고리즘을 적용한 경우는 평균적으로 P/2이다. P는 T보다 훨씬 적게 정하였으므로 사이클 슬립 보상 알고리즘을 적용하였을 때가 훨씬 빠르다. 이 두 경우의 재동기 소요 시간 비 R_{time}를 식으로 나타내면 식 (2)와 같다.

$$R_{time} \cong \frac{T}{P} \tag{2}$$

여기서 T는 연속 재동기 주기이고 P는 기준 시간 길이이다.

식 (2)에서 보는 바와 같이 연속 재동기 주기를 10초로 하고 수신 기준 시간을 약 0.5초로 하였을 경우에는 $R_{time} = 20$ 이다. 즉, 사이클 슬립 보상 알고리즘을 적용하면 그렇지 않은 경우보다 재동기를 이루는데 소요되는 시간이 20배나 빠르다는 것을 나타낸다. 이것은 표 1~표 6에서 나타나는 것과 같이 동일한 사이클 슬립 발생 확률에서 오복호율 R_{ed}와 오복호된 데이터 비트 수 D_{err}이 20배 감소하여 수신측에서 훨씬 정확한 데이터를 얻을 수 있다는 것을 말한다. 표 1에서 보는 바와 같이 통신 속도 9,600bps에서 오복호율 $R_{ed} = 0.24\%$의 결과를 얻기 위해서는 사이클 슬립 보상 알고리즘을 적용하였을 경우는 연속 재동기 주기 T를 10초, 기준 시간 P를 0.5초로 하면 되나, 표 2에서 나타난 것처럼 제안된 알고리즘을 적용하지 않은 경우는 연속 재동기 주기 T를 0.5초로 하여야 한다. 이러한 결과는 통신 속도 28,800bps에서 실험한 결과인 표 3과 표 4에서도 동일하게 나타난다. 즉, 동일한 R_{ed}을 얻기 위해서, 사이클 슬립 보상 알고리즘을 적용하지 않은 경우는 적용한 경우에 비하여 재동기 주기 T를 20배 짧게 하여야 하는데 이것은 20배의 잉여 데이터를 더 전송하여야 하는 것과 동일한 의미이다. 연속 재동기 방식에서 T가 짧다는 것은 재동기를 위한 동기 패턴을 자주 전송한다는 것을 의미하므로 전송 효율을 떨어뜨리는 불이익을 감수하여야 한다. 따라서 연속 재동기 방식에 사이클슬립 보상 알고리즘을 적용한다면 T값을 길게 할 수 있어 전송 효율을 향상시키는 이익을 얻을 수 있다. 128비트의 동기 패턴을 사용하고, 256비트의 세션 키이를 (15, 4) 에러 정정 부호화하여[10] 10^9 bits의 데이터는 9,600bps로 전송하고, $3*10^9$ bits의 데이터는 28,800bps의 속도로 모두 전송할 경우에 연속 재동기 방식의 각 T

값에 따라 요구되는 총 잉여 비트 수는 표 5와 표 6에 나타난다. 표 5와 표 6에서 보는 바와 같이 연속 재동기 주기 T가 10초인 경우는 T가 0.5초인 경우에 비하여 약 $2.15*10^8$ 비트의 감축 효과가 있음을 알 수 있다. 즉, 동일한 오복호율 R_{ed}와 오복호된 데이터 비트 수 D_{err}을 얻는 것을 목표로 했을 때 연속 재동기 방식에 사이클 슬립 보상 알고리즘을 적용하면 적용하지 않았을 경우에 비하여 9600bps인 경우에는 전송하여야 할 총 데이터 량 10^9bits의 약 17.8%, 28,800bps인 경우에는 $3*10^9$ bits의 약 6.8%의 감축 효과를 얻을 수 있다. 본 논문에서는 속도의 변화에 관계없이 P의 값을 일정하게 하였으나 통신 속도가 증가할수록 P의 값을 짧게 하면 데이터 감축 효과는 더욱 증가하고 오복호율 R_{ed}와 오복호된 데이터 비트 수 D_{err}는 더욱 감소할 것으로 예측된다.

V. 결 론

본 논문에서는 동기식 스트림 암호 시스템에서 사용되는 연속 재동기 방식에 사이클 슬립 보상 알고리즘을 적용하여 성능을 개선하였다. 사이클 슬립 보상 알고리즘은 송신 클럭의 동작 오차를 고려한 기준 시간 동안 수신 클럭 펄스를 계수한 후 동일 시간 동안에 사이클 슬립이 일어나지 않은 정상 상태에서의 수신 클럭 펄스의 갯수인 정상치와 비교하여 사이클 슬립 현상을 찾아내는 방법을 사용하였다. 사이클 슬립 보상 알고리즘을 동기식 스트림 암호 통신 시스템의 연속 재동기 방식에 적용하여 시험한 결과 사이클 슬립 보상 알고리즘을 적용하지 않은 연속 재동기 방식에 비해 오복호율 R_{ed}와 오복호된 데이터 비트 수 D_{err}를 20배 감소시켰는데 이것은 전송하여야 할 데이터의 총량을 최대 17.8% 감축하는 효과를 나타낸다.

사이클 슬립 보상 알고리즘이 적용된 연속 재동기 방식을 동기식 스트림 암호 방식을 사용하고 일악한 채널 상태에서 PLL을 이용하여 수신 클럭을 복원하는 무선 암호 데이터 통신 시스템에 제안된 방식을 적용한다면 효율적으로 난수 동기를 유지할 것이다.

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. CCITT Rec. v.29, pp. 206, 1984.
4. B. Schneier, "Applied Cryptography: protocols, algorithm, and source code in C", John Willy & Son, 1993.
5. D. J. Torrieri, "Principles of Secure Communication Systems", Artech House, 1992.
6. R. A. Rueppel, "Analysis and Design of Stream Ciphers", Springer-Verlag, 1986.
7. M. Y. Lee, "Cryptography and Secure Communications", McGraw-Hill, 1994.
8. D. W. Davies, W. L. Price, "Security for Computer Networks", John Wiley & Sons, 1989.
9. J. Daemen, R. Govaerts, J. Vandewalle, "Resynchronization Weaknesses in Synchronous Stream ciphers," Pre-proceedings of EUROCRYPT'93, pp. T9-T17, 1993.
10. 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

강 건 우(Ken Woo Kang)정회원

1973년 2월 : 연세대학교 전자공학과 졸업(공학사)
1987년 2월 : 한국과학기술원 전기전자공학과 졸업(공학석사)
1996년 2월 : 한국과학기술원 전기전자공학과 졸업(공학박사)
1973년 1월~1981년 11월 : 한국과학기술연구소
1981년 12월~현재 : 국방과학연구소 근무
※주관심분야 : OFDM, 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.