通信情報保護學會論文誌
第 10 券 第 3 號, 2000. 9

RMVD를 이용하는 동기식 스트림 암호 데이터 통신시 난수동기 이탈 검출 알고리듬

박 종 욱*, 황 인 호*, 홍 재 근**

Random sequence synchronization failure detection algorithm for synchronous stream cipher system using RMVD

Jong-wook Park*, In-ho Hwang*, Jae-keun Hong**

요 약

초기 동기 방식을 이용하는 동기식 스트림 암호 통신시 송수신 측에서 신속한 난수 동기 이탈 검출 및 난수 재동기는 통신 품질의 결정에 중요한 역할을 한다. 일반적으로 동기식 스트림 암호 통신 시스템은 난수 동기 이탈 검출을 위하여 송신측에서 난수 동기 이탈 여부를 판별할 수 있도록 부가 정보를 송신하게 된다. 그러나 채널 오류 보정을 위하여 RMVD(Running Majority Voting Detector)를 이용하여 송신하는 시스템의 경우 난수 동기 이탈 여부를 판별하기 위한 부가정보를 추가할 수 없다. 본 본문에서는 추가정보를 송신할 수 없는 RMVD를 이용하는 시스템의 수신 측에서 난수 동기 이탈을 검출할 수 있는 방안을 제안한다. 난수 동기의 이탈을 검출하기 위하여 수신된 암호화 데이터를 복호화한 후 복호된 데이터의 단위 시간 당 각 비트들의 천이 형태를 확률적으로 분석하고, 이 천이 확률을 이용하여 난수 동기 이탈 여부를 결정한다. 제안한 방법은 신속하고 높은 정확도를 가지며, 채널 잡음에 강하고, 하드웨어로 간단하게 구현이 가능하다.

ABSTRACT

It is very import role to increase communication quality that fast detection of random sequence synchronization fail in synchronous stream cipher system using initial synchronization mode. Generally, it sends additional information to detect random sequence synchronization fail. But we can't transmit additional informations to decide synchronization fail in a system using RMVD to correct channel error. In this paper we propose a method to detect synchronization fail in the receiver even though a system using RMVD has no margin to send additional information. For detecting random sequence synchronization fail we decipher received data, analyze probability of transition rate for pre-determined period and decide synchronization fail using calculated transition rate probability. This proposed method is fast, very reliable and robust in noisy channel and is easily implemented with hardware.

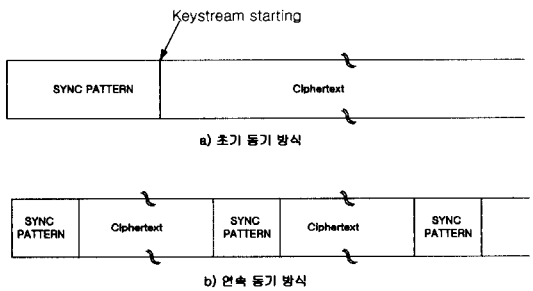
keyword : *synchronization fail, RMVD, EUROCOM D/I*

* 한국전자통신연구원 부설 국가보안기술연구소
** 경북대학교 전자전기공학부

Ⅰ. 서 론

스트림 암호는 동기 방식에 따라 자체 동기식(self-synchronization) 스트림 암호와 동기식 스트림 암호로 구분된다.[1] 자체 동기식 암호는 암호문을 입력에 궤환(feedback)시킴으로서 스트림 동기 이탈시 수신 단에서 자체적으로 동기를 복구시킬 수 있는 반면, 채널에서 단 한 비트의 오류가 발생하여도 이동 레지스터 단수 크기의 비트 오류가 확산되므로 채널 오류 대책이 마련된 통신망에서 적용된다. 자체 동기식 스트림 암호는 Vigenere 암호, 이동 레지스터 방안, 블록 암호화의 CFB(Cipher Feedback) 모드 등이 있다.[2] 동기식 스트림 암호 방식은 스트림 동기 이탈시 자체 복구가 불가능하므로 통신을 중단하고 재동기를 확립하여야 한다. 동기식 스트림 암호 방식에는 키 수열 발생기, Vernam 암호, Rotor 기계, 블록 암호의 OFB(Output Feedback) 모드, 블록 암호의 계수기 등이 있다.[2] 이 방식은 비트 삽입이나 소실과 같은 송수신간의 클락 슬립(clock slip) 발생시 동기가 이탈되는 문제점을 보완하여야 하지만 비트 오류의 확산이 없으므로 일반적으로 많이 사용된다.

동기식 스트림 암호에서는 송수신 측의 난수열을 일치시키기 위해서 특정 패턴의 난수 동기 신호를 교환한다. 난수열 일치방식은 동기 패턴의 송신 횟수에 따라 그림 1과 같이 초기 동기방식과 연속 동기 방식으로 분류된다.[2] 연속 동기 방식은 통신 도중에 일정한 주기로 동기 패턴을 송신하므로 통신 도중 가입자(late entry)의 난수열 동기 확립이 가능하지만 통신 효율이 나쁘기 때문에 채널 상태가 극히 열악한 통신망에서 이용된다. 반면 초기 동기 방식은 암호 통신 시작 시점이나 난수 동기 이탈 시에만 동기 신호를 교환하기 때문에 통신 도중 가입자는 이용할 수 없지만 일대일 통신이나 전 이중 통신(full duplex)에 많이 사용된다.



〔그림 1〕 스트림 암호 통신시스템의 동기 방법

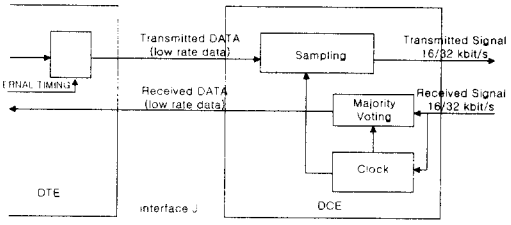
동기식 스트림 암호 시스템에서 초기 동기 방식을 이용하는 경우 가장 문제가 되는 부분은 암호화로 인한 통신 효율 감소 및 통신 신뢰도 저하를 들 수 있다. 이를 최대한 줄이기 위해 다음의 조건이 필요하다. 첫째는 신속하고 정확한 난수열 동기를 수립하여 통신 지연 요소를 줄여야 하고, 둘째는 채널에서 발생한 오류에 강하게 난수열 동기를 유지하여야 하며, 난수열 동기 이탈시 신속하게 동기 이탈 여부를 검출하여 난수 재동기를 수립하여야 한다. 신속하고 정확한 난수열 동기 일치를 위해서는 고 신뢰도의 동기 패턴 교환을 통한 방안[3,4]을 이용하여 구현할 수 있고, 난수 동기 이탈시 동기 이탈 여부의 신속한 검출을 위해서는 송신 데이터를 채널 속도로 변환 시 잉여 비트를 이용하여 일정 주기로 난수열 동기 이탈 여부를 판단할 수 있도록 특정 패턴을 삽입하는 방법이 있다. 그러나 잉여 비트가 없는 경우에는 송신 측에서 동기 유지 여부를 판단할 수 있도록 정보의 추가가 불가능하여 수신 측에서 수동으로 난수열 동기 이탈 여부를 판단하여야 한다.

본 논문에서는 군용 데이터 통신 시스템의 규격인 EUROCOM D/1[5]의 Class 2, 3에 동기식 스트림 암호를 적용한 경우 송신측에서 난수열 동기 유지 여부를 판단할 수 있도록 특정 패턴을 삽입할 여지가 전혀 없지만 수신측에서 난수 동기 이탈 여부를 신속하고 정확하게 검출 할 수 있는 방안을 제안하였다. 본 방안은 수신된 암호화 데이터를 복호화한 후 복호된 데이터의 단위 시간 당 각 비트들의 천이 형태를 확률적으로 분석하고, 이 천이 확률을 이용하여 난수 동기 이탈 여부를 결정한다. 제안한 방안은 신속, 정확할 뿐만 아니라 채널 잡음에 강하고, 특히 하드웨어 구현이 간단하다는 장점이 있다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 난수 동기 이탈 알고리듬의 적용 시스템인 EUROCOM D/1의 Class 2, 3 방식에 대해 살펴보고, Ⅲ장에서는 난수 동기 이탈 검출 방안을 제안한다. Ⅳ장에서는 제안한 방안을 확률적으로 분석하며, Ⅴ장에서는 시뮬레이션을 통해 제안한 방안을 검증하고, Ⅵ장에서 결론을 내린다.

Ⅱ. 적용 시스템

본 논문에서 적용하고자 하는 군용 데이터 및 음성 통신 시스템의 규격인 EUROCOM D/1에서는

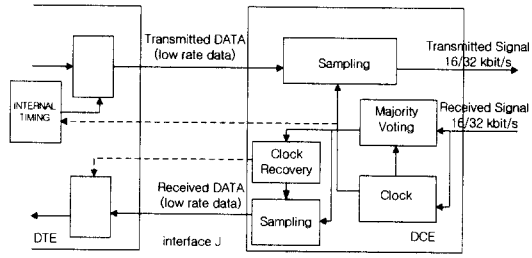


〔그림 2〕 EUROCOM D/1의 CLASS 2 통신시스템 블록도

여러 가지 데이터 통신 방안을 제시하고 있다. 이 중에서 전신기, 팩스와 같은 데이터 단말(DTE)과 DCE 간의 데이터 전송 방법은 5 가지가 있다. 본 논문에서는 5 가지 방법 중 채널 오류 보정을 위해 RMVD[6]를 사용하는 Class 2, Class 3 방법에 대해서 살펴본다.

먼저 Class 2의 경우 그림 2와 같이 4,800bps 이하의 비동기식 데이터 전송을 위해 사용된다. 송신의 경우 DTE에서 인터페이스 J를 통하여 전송되는 데이터는 DTE의 입력 데이터 속도와 무관하게 전달자(bearer)의 속도(16/32kbps)로 표본화되어 채널로 전송된다. 수신의 경우 수신측 전달자는 채널을 통하여 16/32kbps로 수신된 데이터를 RMVD 처리하여 원래의 전송속도인 4,800bps 이하로 변환 후 인터페이스 J를 통하여 DTE에 보낸다. EUROCOM D/1의 규격에서는 Class 2의 RMVD 처리를 하는 경우 채널의 오류율이 10^{-2} 이하일 때 단말 측 데이터의 오류율은 10^{-5} 이하가 되도록 보장하고 있고, 인터페이스 J에서의 데이터 펄스 폭 왜곡은 ±1%이하가 되도록 요구하고 있다.

Class 3의 경우는 그림 3과 같이 4,800bps 이하의 비동기식 또는 동기식 데이터 전송을 위해 사용되며, 비동기식의 경우 데이터 펄스 폭 왜곡은 데이터 전송 속도의 ±0.01% 를 넘어서는 안된다. DTE에서 전송되는 데이터는 비동기식의 경우 DCE의 시간과 무관하며 동기식의 경우 DTE 타이밍은 DCE측에서 제어하고, 이 타이밍은 전달자가 제공한다. 송신의 경우 Class 2와 동일하게 DTE에서 인터페이스 J를 통하여 전송되는 데이터는 DTE의 입력 데이터 속도와 무관하게 전달자의 속도로 표본화되어 채널로 전송된다. 수신의 경우 수신측 전달자는 채널을 통하여 16/32kbps로 수신된 데이터를 이용하여 DCE에서 타이밍 신호를 복구하고, 이를 송신 데이터 전달을 위한 표본화 클럭으로 사용한다. 또한 DCE에서는 RMVD 처리된 데이터를 이용하여 원래의 데이터 전송 속



〔그림 3〕 EUROCOM D/1의 CLASS 3 통신시스템 블록도

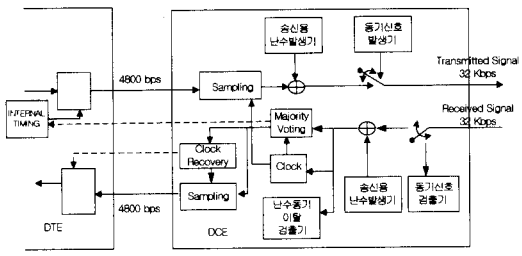
도 클럭을 복구하여 데이터 및 클럭을 DTE에 전송한다.

위에서 설명한 Class 2, 3 시스템은 유선 및 무선 채널에 모두 적용 가능하다. 따라서 이 시스템에 보안통신을 적용하기 위해서는 채널의 오류가 확산되는 블록 암호화보다는 동기식 스트림 암호가 적당하고, 동기 방식은 전송 시 여유 비트가 전혀 없기 때문에 동기 신호를 주기 적으로 송신하는 연속 동기 방식보다는 초기 동기 방식을 적용하는 것이 적당하다. 초기 동기 신호는 상관 특성이 우수한 패턴을 이용하여 구현이 가능하며,[4] 초기 동기가 수립된 후에는 난수 동기 이탈을 감시하고, 이탈 시 이를 재빨리 검출하여 난수 재동기를 수립하여야 한다. 일반적으로 수신측에서 난수 동기 이탈을 검출하기 위해서 송신 측에서 난수 동기 이탈을 검출할 수 있도록 정보 패턴을 삽입하여 송신하거나, 송신측 데이터에 동기 정보가 있는 경우 수신측에서 복호된 데이터의 동기 정보를 검사하여 동기 이탈 여부를 판단하는 방안이 일반적이다.

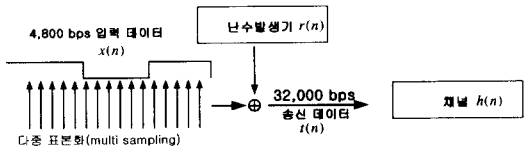
본 논문에서는 난수동기 이탈을 감시하기 위해서 송신측에서 난수열 동기 유지 여부를 판단할 수 있도록 특정 패턴을 삽입할 여지가 전혀 없는 EUROCOM D/1의 Class 2, 3 시스템의 수신측에서 난수 동기 이탈 여부를 신속하고 정확하게 검출 할 수 있는 방안을 제안하였다.

Ⅲ. 난수동기이탈 검출 방안

본 논문에서 제안한 난수 동기 이탈 검출 알고리듬을 적용하고자 하는 EUROCOM D/1의 class 2, class 3의 데이터 통신 시스템에서 입력 데이터 속도가 4,800bps이고, 채널 전송 속도가 32,000bps인 경우의 암호화 시스템은 그림 4와 같이 구현할 수 있다. 그림 4의 암호 통신 시스템의 난수 동기 이탈 검출 방안을 설명하면 다음과 같다.



〔그림 4〕 Class 2, 3 통신시스템의 암호 통신 블록도



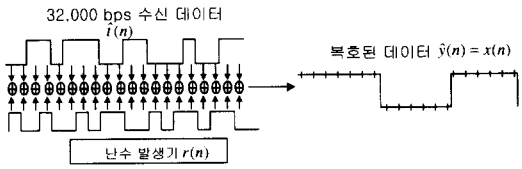
〔그림 5〕 데이터의 암호화 후 송신방법

그림 5와 같이 데이터 전송장치(DCE)에서 4,800bps 속도로 입력되는 데이터 $x(n)$을 32,000bps의 속도로 다중 표본화하고, 암호화를 위해 난수데이터 $r(n)$으로 배타적합을 수행한 후 32,000bps 속도로 암호화된 데이터 $t(n)$을 송신한다.

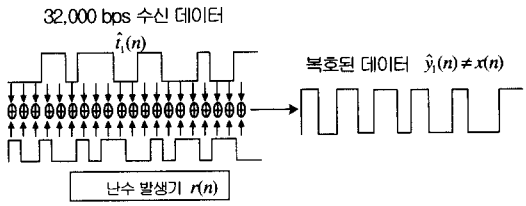
그림 5와 같이 송신된 데이터 $t(n)$이 채널 $h(n)$을 통과 시 전송 오류가 없다고 가정하면, 수신된 데이터 $\hat{t}(n)$을 그림 6과 같이 32,000bps의 속도로 난수 데이터 $r(n)$으로 배타적합(X-OR)을 수행하여 복호화하게 되는 데 이때 난수 동기가 유지되는 경우 복호된 데이터 $\hat{y}(n)$은 그림 5의 4,800bps 입력 데이터 $x(n)$과 동일한 데이터로 복원된다.

그러나 만약 채널 $h(n)$을 통과시 클럭 슬립 현상이 발생하는 경우 그림 7과 같이 수신 데이터 $\hat{y}_1(n)$은 그림 6의 $\hat{y}(n)$과 달리 난수 동기와 일치하지 않게 되며, 수신 데이터 $\hat{t}_1(n)$을 32,000bps의 속도로 난수 데이터 $r(n)$으로 배타적합을 수행하여 복호화 및 RMVD 처리된 데이터는 입력 데이터 $x(n)$과 전혀 다른 랜덤한 특성을 지닌 데이터 $\hat{y}_1(n)$으로 복호된다.

따라서 본 논문에서는 복원된 데이터의 단위 시간 당 0과 1의 천이 확률로부터 난수 동기 이탈 여부를 검출할 수 있다는 데 착안하였다. 난수 동기 이탈시 복호된 데이터는 그림 7과 같이 0 과 1이 랜덤하게 되며, 단위 시간 당 0 과 1의 천이 횟수가 난수 동기가 유지되고 있는 그림 6의 복호된 데이터 $\hat{y}(n)$의 천이 횟수 보다 훨씬 많은 것을 알 수 있다. 따라서 수신 측에서 복호된 데이터의 단위 시간 당 0과 1의 천이 확률을 이용하면 난수 동기 이탈 여부를 판단할 수 있음을 알 수 있다.



〔그림 6〕 난수동기 유지시 복호된 수신 데이터

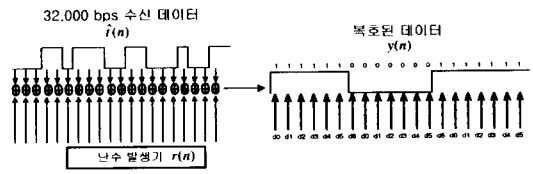


〔그림 7〕 난수 동기 이탈시 복호된 수신 데이터

이를 수학적으로 접근하기 위해 예를 들어 설명하면 다음과 같다. 그림 5와 같이 4,800bps의 입력 데이터 $x(n)$을 32,000bps 속도로 다중 표본화 후 난수 발생기 $r(n)$으로 암호화한 데이터 $t(n)$을 송신하여 채널의 오류가 없다고 가정하면, 수신 측은 그림 8과 같이 수신 데이터 $\hat{t}(n)$을 난수 발생기 $r(n)$으로 복호화하고, 이를 32,000bps의 속도로 샘플링한다. 이때 4,800bps의 데이터 1비트는 32,000bps의 데이터 6.7 비트(32,000/4,800)에 해당된다. 따라서 난수동기가 유지된다고 가정하면 32,000bps의 복호된 데이터는 항상 6 비트 이상씩 같은 데이터가 반복된다. 즉 32,000bps의 속도로 샘플링된 임의의 연속된 7비트의 데이터에서 2번 이상의 데이터 천이(0에서 1, 혹은 1에서 0)가 발생할 수 없다. 따라서 그림 8과 같이 복호된 32,000bps의 7비트 구간을 기본 단위로 하여 임의의 7 비트를 취한 후 다음과 같이 데이터 천이 횟수를 계산할 수 있다.

$$N = \sum_{i=0}^{6} (d_i \oplus d_{i+1})$$

여기서 $\oplus$ 는 배타적합을 의미한다. 이 천이 횟수가 2 이상이면 채널 오류가 없는 경우 난수 동기가 이탈되었다고 판단할 수 있다.



〔그림 8〕 난수동기 이탈 검출방법

그러나 채널에서 오류가 발생하는 경우 단위 시간당 0 과 1의 천이 횟수는 훨씬 증가하게 된다. 따라서 채널 오류가 있는 경우 단위 시간을 7 비트로 고정하면 실제로 동기가 유지되고 있어도 동기 이탈이 검출되는 오검출(false alarm)이 발생하며, 단위 시간을 너무 길게 하면 동기 이탈이 발생했을 경우 즉시 검출되지 않고 검출 지연이 발생하게 된다. 즉 동기 이탈 검출 확률을 높이고, 오검출 확률을 낮추며, 검출 지연 시간을 최소로 하기 위해서 0 과 1의 천이 횟수를 측정하는 단위 시간의 최적화가 필요하며, 또한 난수 동기가 이탈되었다고 판정 할 수 있는 0 과 1의 단위 시간 당 천이 횟수의 문턱값(threshold value)도 결정하여야 한다. 다음 절에서는 확률적 접근을 통해 이를 결정한다.

Ⅳ. 확률적 접근

채널오류율에 강인한 난수동기 검출 확률을 얻기 위하여 난수동기가 이탈되었다고 판단하는 단위시간 및 문턱값을 다음과 같이 구할 수 있다.

먼저 난수동기가 유지되는 경우 채널오류율을 BER, 32,000bps의 연속되는 7비트의 샘플링 데이터가 4,800bps 데이터의 천이영역에 있을 확률을 P_{tr}, 천이영역이 아닐 확률을 P_{ntr} 이라 두고, 송신 데이터의 통계적 특성이 랜덤하다고 가정하면, 2번 이상의 천이가 발생할 확률 P_{N2}는 식 (1)과 같다.

$$
\begin{aligned}
P_{N_2} &= 1-[\{probability\ of\ no\ transition\}+\{probability\ of\ one\ transition\}] \\
&= 1-[\{P_{ntr}\times((1-BER)^7+BER^7)+P_{tr}\times 0.5\times((1-BER)^7+BER^7) \\
&\quad + P_{tr}\times 2\times 0.5\times\left\langle\begin{matrix}(1-BER)\cdot BER^6)+(1-BER)^2\cdot BER^5+(1-BER)^3\cdot BER^4+\\ (1-BER)^4\cdot BER^3+(1-BER)^5\cdot BER^2+(1-BER)^6\cdot BER\end{matrix}\right\rangle\} \\
&\quad + \{P_{ntr}\times 2\left\langle\begin{matrix}(1-BER)\cdot BER^6)+(1-BER)^2\cdot BER^5+(1-BER)^3\cdot BER^4+\\ (1-BER)^4\cdot BER^3+(1-BER)^5\cdot BER^2+(1-BER)^6\cdot BER\end{matrix}\right\rangle \\
&\quad + P_{tr}\times 0.5\times\frac{10}{12}\times\left\langle\begin{matrix}(1-BER)\cdot BER^6)+(1-BER)^2\cdot BER^5+(1-BER)^3\cdot BER^4\\ +(1-BER)^4\cdot BER^3+(1-BER)^5\cdot BER^2+(1-BER)^6\cdot BER\end{matrix}\right\rangle \\
&\quad + P_{tr}\times 0.5\times\left\langle BER^7+(1-BER)^7\right\rangle\}
\end{aligned}
$$

$$
P_{ntr}=\frac{no\_tran\_length}{totallength},\quad P_{tr}=1-P_{ntr},\quad no\_tran\_length=\left(\frac{1}{4800}-\frac{6}{3200}\right),
$$

$$
totallength=\left(\frac{1}{4800}+\frac{6}{3200}\right) \qquad (1)
$$

다음으로 난수동기가 이탈된 경우 복호된 데이터는 랜덤한 특성을 나타내며, 7비트의 데이터에서 x 번의 천이가 발생할 확률을 P'_{Nx}라고 할때 P'_{Nx}는 식 (2)와 같이 표현된다.

$$
P'_{Nx}={}_6C_x\times 0.5^6 \quad ; \quad x=0,1,2,\cdots,6 \qquad (2)
$$

이때 2번 이상의 천이가 발생할 확률 P'_{N2}은 식 (3)과 같다.

$$
\begin{aligned}
P'_{N2} &= 1-[(prob.of\ no\ transition)+(prob.of\ one\ transition)] \\
&= 1-[{}_6C_0\times 0.5^6+{}_6C_1\times 0.5^6] \qquad (3)
\end{aligned}
$$

식 (1)에서 식 (3)까지의 확률을 이용하여 단위 시간 T_{det} msec 이내에 난수 동기 이탈을 검출하기 위한 문턱값을 구해야 한다. 이때 샘플링 속도가 32,000bps인 경우 T_{det} msec 동안 $32\cdot T_{det}$ 비트의 데이터를 취할 수 있고 $32\cdot T_{det}$ 비트의 데이터에서 7비트씩 취하여 2번 이상의 천이가 발생하는 횟수에 대한 문턱값을 D_{th}라 두면 D_{th}는 0에서 $32/7\cdot T_{det}$ 사이의 값으로 설정할 수 있다. 이하에서는 $32/7\cdot T_{det}$를 D_{max}라 표현한다.

난수 동기가 이탈되지 않았는데 채널에서의 랜덤 잡음에 의해 난수 동기가 이탈되었다고 판단할 수 있으며, 이를 오검출(false alarm)이라 하며, 오검출 확률 P_{fa}[6]은 식 (4)와 같이 문턱값의 함수로 표현할 수 있다.

$$
P_{fa}(D_{th})=\sum_{i=D_{th}}^{D_{max}} {}_{D_{max}}C_i\times P_{N_2}{}^i(1-P_{N_2})^{D_{max}-i} \quad ; D_{th}=0,1,2,\cdots,D_{max} \qquad (4)
$$

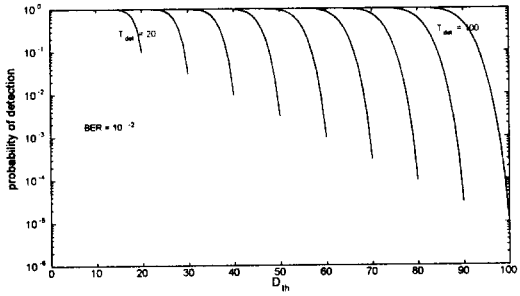
난수 동기가 이탈된 경우 수신측에서 난수 동기 이탈을 정확히 검출할 확률 P_{det}[6]을 문턱값의 함수로 표현하면 식 (5)와 같다.

$$
P_{det}(D_{th})=\sum_{i=D_{th}}^{D_{max}} {}_{D_{max}}C_i\times P'_{N_2}{}^i(1-P'_{N_2})^{D_{max}-i} \quad ; D_{th}=0,1,2,\cdots,D_{max} \qquad (5)
$$

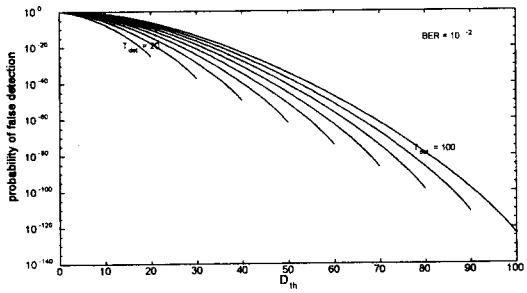
또한 난수 동기 이탈이 발생하였지만 수신측에서 이를 검출하지 못할 미검출 확률 P_{miss}[6]도 식 (6)과 같이 문턱값의 함수로 나타낼 수 있다..

$$
P_{miss}(D_{th})=1-P_{det}(D_{th}) \quad ; \quad D_{th}=0,1,2,\cdots,D_{max} \qquad (6)
$$

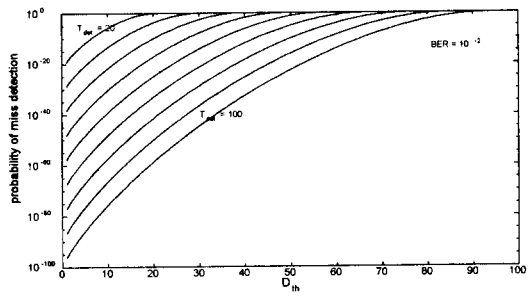
위에서 구한 식을 이용하여 동기 검출 확률의 정확성을 알아보기 위해 난수 동기 이탈 검출주기 T_{det}를 가변하고, 채널오류를 10^{-2} 으로 가정하면, 문턱값 D_{th}에 따른 난수 동기 이탈을 정확히 검출할 확률 P_{det}, 난수 동기가 이탈되지 않았는데 이탈되었다고 판단할 오검출 확률 P_{fa}, 난수 동기 이탈이 발생하였지만 이를 검출하지 못할 미검출 확률 P_{miss}는



〔그림 9〕 난수 동기 이탈 검출주기 T_{det} 및 문턱값 D_{th}에 따른 검출 확률



〔그림 10〕 난수 동기 이탈 검출주기 T_{det} 및 문턱값 D_{th}에 따른 오검출 확률

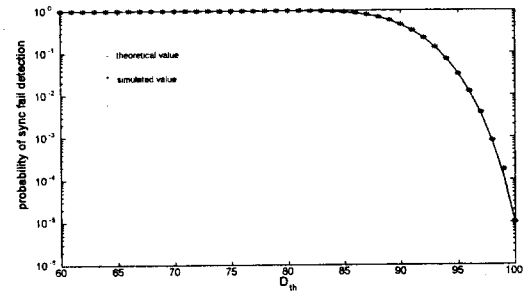


〔그림 11〕 난수 동기 이탈 검출주기 T_{det} 및 문턱값 D_{th}에 따른 미검출 확률

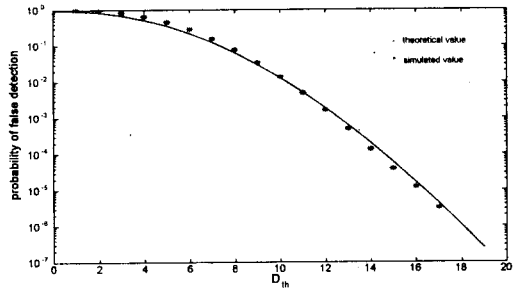
그림 9, 10, 11과 같이 구할 수 있다. 채널 오류율이 10^{-2} 이하인 경우에도 같은 방법으로 구할 수 있고, 채널 오류율이 10^{-2}일 경우의 결과를 그대로 적용할 수 있다. 다음 절에서는 이를 시뮬레이션을 통해 알아보고 하드웨어 구현 방안도 살펴본다.

V. 시뮬레이션 결과 및 구현

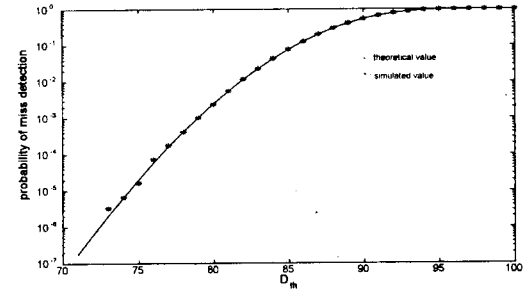
채널의 오류율이 10^{-2}이고 난수 동기 이탈 검출 주기 T_{det}을 20msec로 두고, 문턱값 D_{th}에 따른 동기 이탈 검출 확률, 오검출 확률 및 미검출 확률을



〔그림 12〕 문턱값(D_{th})에 따른 난수 동기 이탈 검출 확률

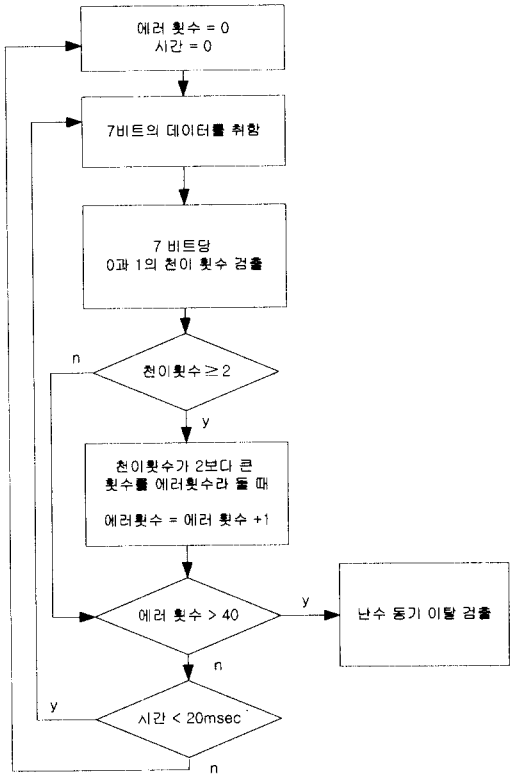


〔그림 13〕 문턱값(D_{th})에 따른 난수 동기 이탈 오검출 확률



〔그림 14〕 문턱값(D_{th})에 따른 난수 동기 이탈 미검출 확률

시뮬레이션을 통해 구해본 결과 그림 12, 13, 14와 같이 이론치와 거의 일치함을 알 수 있다. 문턱값이 30 이상인 경우 난수 동기 이탈 검출 확률은 100%이고, 난수 동기 이탈 미검출 확률은 9.37×10^{-43}, 난수 동기 이탈 오검출 확률은 4.02×10^{-14} 이며, 이 확률은 32,000bps의 속도로 1년 동안 연속 송신시 난수 동기 이탈시 이를 100% 검출하고, 미검출이나 오검출은 한번도 발생하지 않는 정도의 정확도를 가진다. 난수 동기 이탈 검출 주기를 20msec 두고, 문턱값이 40 이상인 경우 난수 동기가 이탈했다고 판단하는 하드웨어를 그림 15의 흐름도를 이용하여 구현할 수 있다.



〔그림 15〕 난수 동기 이탈 검출 알고리듬 흐름도

Ⅵ. 결 론

본 논문에서는 RMVD를 이용하는 시스템에 데이터 암호 통신을 위하여 동기식 스트림 암호방식을, 난수열 동기 방식으로 초기 동기 방식을 적용하는 경우 암호화로 인한 통신 효율 감소 및 통신 신뢰도 저하를 최소화하기 위해 필요한 난수 동기 이탈 알고리듬을 제안하고 분석하였다. 본 알고리듬은 수신측에서 난수 동기 이탈 검출을 위한 정보를 송신측에서 전송할 필요가 없고, 열악한 무선 환경에서도 성능이 우수하며, 난수 동기 이탈시 신속하게 검출이 가능하다. 본 알고리듬의 분석 결과 채널 오류율이 10^{-2} 이하인 경우 난수 동기 이탈시 검출 확률이100%이고, 오검출 확률이 10^{-14} 이하인 고신뢰도 방식임을 알 수 있었고, 소프트웨어와 하드웨어를 이용하여 쉽게 구현이 가능하다. 또한 제안된 방안을 이용하여 군 전술 통신 체계에 적용하여 시험한 결과 성능이 우수함을 알 수 있었다.

참 고 문 헌

〔1〕 R. A. Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag, 1986.

〔2〕 D. E. R. Denning, *Cryptography and Data Security*, Addison-Wesley Publishing Co., California, 1982.

〔3〕 이훈재, 문상재, "고신뢰도 동기식 스트림 암호 시스템", *통신정보보호학회 논문지*, 8(1), Mar. 1998.

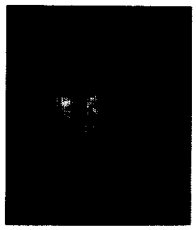
〔4〕 이훈재, "*링크 암호에 적합한 개선된 동기식 스트림 암호 시스템*", 경북대학교 박사학위 논문, 1997년 12월.

〔5〕 EUROCOM 규격, *Tactical Communications Systems Basic Parameters(D/1)*, Sep. 1982.

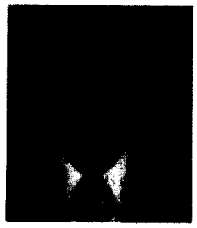
〔6〕 최성남, "*무전기 접속부의 RMVD 회로 성능 개선 구현*", 삼성전자 사내 논문지, Apr. 1997.

〔7〕 H. J. Beker and F. C. Piper, *Secure Speech Comminications*, Academic Press, London, 1985.

〈著者紹介〉



박 종 욱 (Jong-wook Park) 정회원
1986년 2월 : 경북대학교 전자공학과 졸업
1988년 2월 : 경북대학교 전자공학과 석사
1994년 3월~현재 : 경북대학교 전자공학과 박사과정
1988년 2월~2000년 1월 : 국방과학연구소 근무
2000년 2월~현재 : 국가보안기술연구소 선임연구원
〈관심분야〉 정보보호, 네트워크통신



황 인 호 (In-ho Hwnag)
1980년 2월 : 한양대학교 전자통신공학과 졸업
1982년 2월 : 중앙대학교 전자공학과 석사
1999년 2월 : 한국과학기술원 정보 및 통신공학과 박사
1986년 2월~2000년 1월 : 국방과학연구소 근무
2000년 2월~현재 : 국가보안기술연구소 책임연구원
〈관심분야〉 통신신호처리, 정보보호

홍 재 근 (Jae-keun Hong)
1975년 2월 : 경북대학교 전자공학과 졸업
1979년 2월 : 경북대학교 전자공학과 석사
1985년 2월 : 경북대학교 전자공학과 박사
1979년~1982년 : 경북산업대학교 조교수
1983년~현재 : 경북대학교 전자전기공학부 교수
〈관심분야〉 음성인식, 음성신호처리