論文 96-21-3-14

CDMA 이동통신망에서의 데이타 비도에 관한 연구

正會員 김 지 홍*, 이 만 영**

A Study on Data Security in CDMA System

Ji Hong Kim*, Man Young Rhee** *Regular Members*

요 약

본 논문에서는 CDMA 방식에서 사용되는 PN 계열 확산에 의한 데이타 비도를 측정해 본다. [42/4]×4+[42/4]×4 비트의 출력계열을 알고 있다면, LFSR의 키에 해당되는 긴부호 마스크 비트(long code mask bit)를 구할 수 있고, 이를 이용하여 긴부호 계열을 생성하여 수신되는 직교 데이타와 이진합함으로서, 데이타를 찾을 수 있음을 밝힌다. 이러한 문제점을 통하여 CDMA 이동통신망에서의 암호 적용이 시급함을 보인다.

ABSTRACT

In this paper, we measure data security in CDMA system. If we know the [42/4]×4+[42/4]×4 bits of output sequences of key stream generator, we can find long code mask bits and orthogonal output sequences. So this paper showes us the necessity of data security algorithm in CDMA system.

Ⅰ. 서 론

1984년도 셀룰러 방식 서비스 개시이래 현재 국내에서 사용되는 이동통신 서비스는 FM 방식의 아날로그 AMPS(advanced mobile phone system) 방식을 사용하고 있다. 그러나 급증하는 수요의 증가와 통신 로상의 고품질화를 위하여, 디지탈 이동통신 방식으로 CDMA 방식을 국내 표준으로 선정하여 미국의 Qualcomm사와 공동으로 이동통신 시스템의 개발을 추진하고 있다. 이러한 디지탈 CDMA 이동통신방식은 대역확산(spread spectrum) 통신방식을 근간으로 한다. 대역확산 통신방식은 원래 군용통신에 널리 이용되어 왔지만 현재 디지탈 통신 기술과 반도체 기술의 발달에 힘입어 상용 디지탈 이동통신 분야에까지 그 응용영역을 확대하고 있다. 대역확산 통신방식은 다수의 사용자의 수용과 사용자 정보의 안전한 전달을 위하여 자신의 데이타 속도보다 훨씬 큰 대역폭을 사용하여 전송하고, 수신측에서는 이를 역확산 방식을 사용함으로서 전송로 상에서 발생될 수 있는 방해파(jamminig)의 효과를 제거할 수 있는 방식이다.

CDMA 방식은 기지국에서 이동국으로 전송되는 순방향채널(forward channel)과 이동국에서 기지국으

*세명대학교 전자공학과
**한양대학교 전자통신공학과
論文番號:95294-0828
接受日字:1995年 8月 28日

로 전송되는 역방향채널(reverse channel)로 구분된다. 순방향채널은 파이럿(pilot), 동기(sync), 호출(paging), 통화(traffic)채널로 구분되며, 역방향채널은 접속(access), 통화(traffic)채널로 구분된다. 이들 중에서 사용자의 통화 데이타 보호와 관련되는 부분은 역방향채널의 통화채널에 해당된다. 역방향 통화채널에서의 데이타 생성순서는 CRC 첨가, 8비트 첨가, 길쌈 부호기(convolutional encoder), 심볼 반복기(symbol repetition), 블럭 인터리버(block interleaver), 64진 직교변조기(orthogonal modulator), 데이타 난수기(data burst randomizer), 긴부호 발생기(long code generator), OQPSK 변조기의 순으로 구성된다. 이들 중 순수하게 데이타 보호와 관계되는 부분은 64진 직교변조의 출력에서 긴부호발생기의 출력과의 이진합으로 대역확산을 행하는 부분이다.

CDMA 방식에서 사용중인 대역확산 방식은 LFSR (linear feedback shift register)의 출력으로 PN부호 확산을 이용한다. 일반적으로 N단 LFSR의 출력계열에서 출력을 얻는 경우, 출력계열중 2N비트를 알면 LFSR의 키(초기조건과 귀환계수)를 알수 있다[1, 4]. 그러나 CDMA 이동통신망의 경우에는 동기채널을 통하여, 기지국(base station)으로부터 42단의 LFSR의 현재상태값을 수신할 수 있다. 또한 42단 LFSR의 귀환결합계수는 EIA/TIA 표준안[7]을 통하여 이미 알고 있는 상태이다. 반면에 각각의 이동통신 사용자의 고유번호(ESN 혹은 MIN)를 포함한 42비트 긴부호 마스크(long code mask)를 사용하여 출력계열을 발생시키기 때문에, 긴부호 마스크가 LFSR의 키에 해당된다. 이러한 출력계열은 다시 4비트 단위로 1비트의 데이타와 확산되며, I, Q 채널확산과 OQPSK 변조방식에 의해 전송된다.

본 논문에서는 이러한 과정을 분석하고, 결과적으로 확산후 생성된 출력비트계열 중 $[42/4]\times4+[42/4]\times4$ 비트를 알면, 긴부호발생기의 키에 해당하는 긴부호 마스크 비트 패턴과 동일한 긴부호 계열을 생성할 수 있는 등가시스템을 구성할 수 있으며, 전송된 데이타의 일부를 알 수 있음을 보인다. 또한 이러한 이해을 돕기 위하여 $GF(2^6)$에 의해 생성되는 계열을 이용한다.

Ⅱ. 통화채널과 PN 부호 확산

일반적으로 CDMA 이동통신 가입자와 기지국간의 통화채널상의 데이타 비도(security)는 데이타 확산에 사용되는 긴부호 마스크에 의한다. 긴부호 마스크는 이동통신 전화기의 고유번호인 전자 일련번호(ESN : Electronic Serial Number)을 이용한 공용 긴부호 마스크(public long code mask) 방법과 사용자의 전화번호에 해당되는 이동국 식별번호(MIN : Mobile Identification Number)을 이용한 사용 긴부호 마스크(private long code mask) 방법이 있다. 이들 중 공용 긴부호 마스크 방법은 아래와 같은 마스크 비트를 사용한다.

41	32	31	0
1100011000		Permuted ESN ($E_0,E_{31},E_{22},E_{13},E_4,E_{26},E_{25},..$)	

처음 10 비트는 통화채널에 사용되는 통화채널용 긴부호 마스크패턴을 의미하며, 다음의 32비트는 순열 치환된 ESN(Electronic Serial Number)을 의미하며, ESN의 원래 형태는 다음과 같다[7].

31	23	17	0
MFR code	Reserved	Serial Number	

제조업자 고유의 MFR 부호(Manufacturer's code)와 향후 확장용으로 사용하기 위한 여분의 비트들과 제조업자들에 의해 할당된 18비트의 고유번호로 구성된다. 따라서 32개의 비트중에서 실질적으로 비밀데이타는 18비트에 불과하다. 따라서 최대 2^{18} 회의 연속공격(exhaustive attack)을 이용하여 긴부호 마스크를 찾는 방법도 있다.

그러나 본 논문에서는 LFSR의 근본적인 특성[1, 5]과 CDMA 시스템에서 전송 데이타 생성 과정[7]을 검토함으로서 긴부호 생성기의 키(긴부호 마스크 비트)를 찾는 방법을 분석한다. 통화채널의 전송데이타 생성과정에서, CRC 첨가, 8비트 첨가, 심볼 반복기등의 과정은 다양한 전송속도를 가진 데이타에 대하여 일정한 프레임 구조를 형성하기 위한 과정이며, 길쌈부호기, 블럭 인터리버는 전송과정에서 발생될 수 있는 오류에 대한 대비책에 해당되며, 특히 블럭 인터

리버는 연집오류(burst error)에 대한 대비책에 해당된다. 데이타난수기는 각각의 전송속도에 따라 효율적으로 출력전력을 제어하기 위하여 사용된다. 그러므로 64진 직교변조기의 출력에서 긴부호 생성기에 의한 확산과정만이 통화채널 데이타의 안전성과 관련된다.(참조: 그림 2-1)

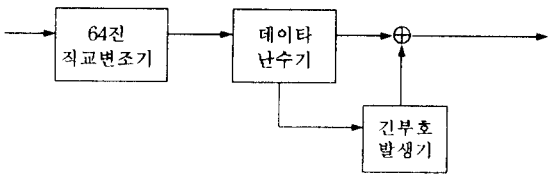


그림 2-1. 데이타 확산과정
Fig 2-1. The process of data scranbling

Ⅲ. CDMA 긴부호 발생기 분석

3.1 긴부호 마스크 비트 효과

CDMA 이동통신의 통화채널에서 데이타 확산에 사용되는 긴부호 생성기는 그림(3-1)과 같은 구조로서, 42단의 LFSR로 구성되며 생성다항식은 다음과 같다.

$$g(x)=1+x+x^2+x^3+x^5+x^6+x^7+x^{10}+x^{16}+x^{17}+x^{18}+x^{19}+x^{21}+x^{22}+x^{25}+x^{26}+x^{27}+x^{31}+x^{33}+x^{35}+x^{42}$$

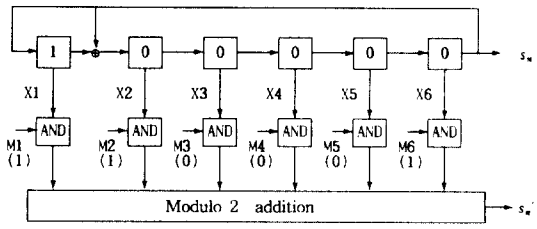


그림 3-1. 긴부호 생성기
Fig 3-1. Long code generater

LFSR의 기본 출력계열을 s_n이라 하고, 마스크 비트에 의해 마스크 절차와 이진합을 수행한 후의 출력계열을 s_n'이라 하면, 두 계열간에는 다음의 관계식이 성립된다.

$$s_n' = x^d s_n \tag{1}$$

즉 마스크 비트들에 의해 마스크된 후의 출력계열 s_n'는 원래의 출력계열 s_n를 d번 천이된 결과와 같으며, N단 LFSR의 초기치에 의해 결정되는 A_i와 $GF(2^N)$상의 N개의 서로 다른 근 α_i를 이용하여, 출력계열을 표시할 수 있다[2].

$$s_n = \sum_{i=0}^{N-1} A_i (\alpha_i)^n \tag{2}$$

식(2)에서 N차 생성다항식 $g(x)$를 귀환결합 방정식으로 사용하는 N단 LFSR 시스템에서 서로 다른 근 α_i는 α^{2^i}으로서, i=0에서 N-1에 해당하는 근이다. 그러므로 $GF(2^N)$상의 N개의 근은 $\alpha, \alpha^2, \alpha^4, \alpha^8 .. \alpha^{2^{N-1}}$이다. 만약 $A_0=A_1=\cdots=A_{N-1}=1$인 초기상태를 식(2)에 적용하면, trace 함수를 이용한 식(3)과 같이 표시될 수 있다.

$$s_n = \sum_{i=0}^{N-1} (\alpha^{2^i})^n = tr(\alpha^n) \tag{3}$$

이러한 초기상태로 부터 d번 천이된 후의 LFSR의 출력계열은 다음과 같다.

$$s_{n+d} = \sum_{i=0}^{N-1} (\alpha^{2^i})^{n+d} = tr(\alpha^{n+d}) \tag{4}$$

예로서 N=6인 6단 LFSR 시스템에 대하여, $A_0=A_1=\cdots=A_5=1$인 초기상태를 적용하고, 식(3)에 의하여 출력계열을 구하면 다음과 같다.

s_n=(000001000011000101001111101000...)

출력계열 s_n은 LFSR의 초기상태가 "100000"에서의 출력계열과 동일하며, $tr(\alpha^{n+d})$는 $A_0=(\alpha)^d$, $A_1=(\alpha^2)^d$ ... $A_{N-1}=(\alpha^{2^{N-1}})^d$로서, "100000"에서 d번 천이된 초기상태에서의 출력계열 s_{n+d}를 의미한다[2, 4]. 마스크 효과를 분석하기 위하여 그림 3-1과 같은 구조의 6단 LFSR에 대하여 초기조건("100000")과 마스

크 비트("110001")를 가정하고, 마스크된 후의 출력 계열 s_n'를 구하면 다음과 같다.

$s_n' = (11000101001111010001110010010...)$

결국, 마스크 비트에 의해 마스크된 후에 생성된 s_n' 계열과 원래의 LFSR 출력계열 s_n을 비교하면, 10번 천이한 것과 같다. 따라서 초기상태 "100000"에 의해 생성되는 LFSR 출력계열에 마스크 비트 "110001"을 이용하여 마스크 시키면 10번 천이된 후의 상태인 "000011" 상태에서 시작되어 생성되는 계열과 동일하게 나타난다.

s_n = 00000100001100010100111110100 01...
s_n' = ---------1100010100111101000111001 0010...

그러므로 그림 3-1의 출력계열과 동일한 출력계열을 생성할 수 있는 등가 시스템은 초기상태 "000011"를 갖는 그림 3-2와 같은 LFSR 시스템으로 구성될 수 있다.

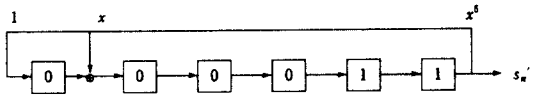


그림 3-2. 등가 LFSR 시스템
Fig 3-2. The equivalent LFSR system

또한 그림 3-1의 LFSR 의 각 단에서 생성되는 출력계열을 x_1, x_2, x_3, x_4, x_5, x_6라 하면, 아래와 같은 초기조건을 갖는 각각의 등가 LFSR 시스템으로 구성할 수 있다.

x_1 : 초기조건 "100001" → 출력계열 : "1000001000011..",
x_2 : 초기조건 "010000" → 출력계열 : "0100001100010..",
x_3 : 초기조건 "001000" → 출력계열 : "0010000110001..",
x_4 : 초기조건 "000100" → 출력계열 : "0001000011000..",
x_5 : 초기조건 "000010" → 출력계열 : "0000100001100..",
x_6 : 초기조건 "000001" → 출력계열 : "0000010000110..",

이 들 중에서 $x_1 \oplus x_2 \oplus x_6$를 하면 초기조건 "110000"에서 생성되는 출력계열은 s_n'과 동일한 계열을 얻을 수 있다. 이러한 특성은 최대장 계열의 천이와 합의 특성(shift and add property)[6]에 해당한다. 따라서 초기조건 "100000"에서 마스크 비트 "110001"를 이용하여 얻은 출력계열 s_n'는 초기조건 "110000"을 이용한 등가시스템으로 구성할 수 있으며, 또한 이때 사용된 마스크 비트는 $M_1 = M_2 = M_6 = 1$로 나타나는 것을 알 수 있다.

3.2 긴부호 계열과의 이진합 효과 분석

제 2장에서 설명된 그림 2-1와 같이, 긴부호 생성기의 PN부호 출력은 64진 직교변조기와 데이타 난수기를 통과한 데이타와 이진합된다. CDMA 시스템에서 사용되는 프레임의 단위는 20 msec 이다. 표 3-1은 CDMA 역방향 통화채널 데이타 생성 순서에 따라, 프레임당 비트 갯수를 표시한 것이다. 가장 흔히 사용되는 9600 bps 데이타의 경우에 대해서는 반복과 데이타 난수기 과정이 생략되며, 직교변조기의 출력과 긴부호 출력을 비교하면 직교변조기를 통과한 데이타 1비트당 긴부호 출력계열이 4비트와 이진합된다는 것을 알 수 있다.

표 3-1. 역방향 통화채널에서의 파라메터
Table 3-1. Revese traffic channel modulation parameter

	9600 bps	4800 bps	2400 bps	1200 bps
비트갯수(20msec)	192	96	48	24
길쌈 부호기	576	288	144	72
심볼 반복기	-	1 번	3 번	7 번
블럭 인터리버	576	576	576	576
직교 변조기	6,144	6,144	6,144	6,144
데이타 난수기	-	1/2	1/4	1/8
긴부호 출력	24,576	24,576	24,576	24,576

예로서 6단 LFSR 시스템으로 생성되는 긴부호 출력계열과 임의로 설정된 직교 변조기의 출력을 사용하여, 위에서 설명된 바와 같이 긴부호 출력 4비트당 1비트의 직교변조기 출력과 이진합되는 과정을 분석하기로 한다.

긴부호 출력 Z : 1100 0101 0011 1101..
직교변조기 출력 D : 0 1 0 1..
출력 계열 Z` : 1100 1010 0011 0010..

만일 위와 같은 이진합 과정을 거친 확산된 출력계

열 Z' 의 일부를 알고 있다고 가정하면, 이를 이용하여 간부호 출력계열과 데이타 출력계열을 찾을 수 있다. 왜냐하면 이진합 과정을 거친 출력계열의 특징은 4비트 단위로 "0000" 혹은 "1111"과 이진합되었기 때문에 추정이 가능해 진다는 특성을 가진다. 만일 이진합된 출력계열 중 8비트(1100 1010..)를 알고 있다고 가정하자. 이때 이진합된 출력계열에 대하여 가능한 데이타 비트계열은 "00", "01", "10", "11"의 4가지 경우만 존재하며, 이들에 대하여 타당성을 조사하기로 한다.

(1) 직교변조기 출력 "00" 라면, 간부호 출력 = 1100 1010
(2) 직교변조기 출력 "01" 라면, 간부호 출력 = 1100 0101
(3) 직교변조기 출력 "10" 라면, 간부호 출력 = 0011 1010
(4) 직교변조기 출력 "11" 라면, 간부호 출력 = 0011 0101

위의 4가지 경우의 수에 대하여 합당한 것을 찾아보기 위하여, 먼저 (1)의 경우에 가능한 간부호 출력은 "1100 1010..."이며, 이와같은 초기조건 "110010"인 LFSR로 생성할 수 있는 계열(1100 1001..)에 해당되지 않는다. 다음으로 (2)의 경우에는 LFSR로 생성할 수 있는 계열(1100 0101 0011..)과 일치하고, (3)의 경우에는 LFSR로 생성할 수 있는 계열(0011 1001 0010..)과 일치하지 않으며, 마지막 (4)의 경우에는 LFSR로 생성할 수 있는 계열(0011 0101 0110..)과 일치한다. 초기의 4가지 경우가 2가지 경우의 수로 줄어들었다. 따라서 추가적으로 4비트를 이용하여 최종적인 결과를 얻을 수 있다. 결과적으로 위의 2가지 경우(2번과 4번)에 대하여 다시 수행한다.

(1) 직교변조기 출력 "010" 라면, 간부호 출력 = 1100 0101 0011
(2) 직교변조기 출력 "011" 라면, 간부호 출력 = 1100 0101 1100
(3) 직교변조기 출력 "110" 라면, 간부호 출력 = 0011 0101 0011
(4) 직교변조기 출력 "111" 라면, 간부호 출력 = 0011 0101 1100

위의 4가지 경우중에서 (1)번의 경우만이 6단 LFSR에 의해 생성될 수 있는 계열임을 알 수 있다. 결과적으로 데이타 비트를 "010"로 가정한 (1)의 경우만이 간부호 계열을 생성할 수 있으며 나머지 64비트의 간부호 출력계열을 추정할 수 있다.

Z'' = 1100 0101 0011 1101 0001 1100 1001 0110 ..

이와 함께 가지의 가지의 출력 Z'를 추정된 간부호 출력계열 Z''와 이진합을 행하면, 다음과 같이 직교변조기의 출력 계열을 찾아낼 수 있다.

추정된 출력 Z''
= 1100 0101 0011 1101 0001 1100 1001 0110 ..
가지의 출력 Z'
= 1100 1010 0011 ..
직교변조기 출력
= 0000 1111 0000

결과적으로 이진합의 결과로 구해진 직교변조기의 출력계열은 010...이 된다. 이와같이 L = 6인 경우, [6/4]×4 + [6/4]×4 (= 12)비트의 확산된 출력계열을 알면 실제로 동작중인 LFSR 시스템의 등가 시스템을 구성할 수 있을 뿐 아니라, 직교변조기의 출력계열의 일부도 함께 추정할 수 있다. [6/4]×4는 LFSR 출력계열을 4비트 단위로 마스크시키기 위한 비트수이며, [6/4]×4는 간부호 출력계열을 파악하기 위한 추가적인 비트갯수에 해당한다. 따라서 4비트 단위로 추가함에 따라, 합당한 간부호 계열을 생성할 수 있는 경우의 수는 1/2씩 감소함을 알 수 있다.

Ⅳ. 결 론

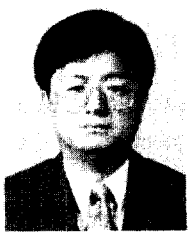
전 장에서 6단 LFSR 시스템으로 설명한 바와 같이, CDMA 방식에서 사용되는 42단 LFSR 시스템으로 생성되는 간부호 계열도 마찬가지 방법으로 데이타 비트계열과 이진합된 42단 간부호 출력계열에 대하여 적용된다. 즉 4의 정수배인 44비트에 대한 데이타 11비트를 가정한 상태에서 타당성을 조사하면 2^{11}개의 경우의 수가 존재한다. 초기의 44비트에서 42비트에 부가되는 2비트를 이용하여 경우의 수는 2^{10}개로 되며, 추가되는 4비트마다, 경우의 수는 1/2로 줄기 때문에, 결국 간부호 계열을 생성하는 42단 LFSR의 경우에는 [42/4]×4 + [42/4]×4 = 84비트를 알면 간부호 출력계열을 추정할 수 있다. 이러한 관점에서 CDMA 방식에서 사용되는 PN계열 확산방식을 정리

하면 다음과 같다.

공용 긴부호 마스크에 의한 마스크 효과는 단지 현재 사용중인 LFSR 시스템의 초기상태를 변환시킴으로서, 마스크가 사용치 않았을 경우에 비하여 시간적으로 치환된 상태의 출력계열을 생성한다. 또한 직교 변조기를 통과한 데이타 비트에 대하여 각각 4 비트씩 긴부호 출력계열과 이진합하는 것은 데이타 확산의 효과는 있지만, 데이타 보호에는 효과가 없음을 알았다. 즉 만약 직교 변조기를 통과한 데이타 비트에 대하여 각각 1비트씩의 긴부호 출력계열과 이진합을 행하면, 출력계열을 이용하여 등가 LFSR 시스템을 찾는 것은 데이타 비트의 불규칙성으로 인하여 거의 불가능할 것이지만, 각각 4비트 씩의 긴부호 출력계열과 이진합을 행하면 각 4비트씩 동안 출력의 규칙성으로 인하여, [42/4]×4+[42/4]×4 비트를 알면 등가 LFSR 시스템을 구성할 수 있게 되었다. 이러한 결론은 현재 상용화가 실시되고 있는 CDMA 이동통신 시스템에 대하여 적절한 암호 알고리즘의 적용이 시급함을 보인다.

참 고 문 헌

1. Golomb, S.W, *Shift Register Sequences*. Holden-Day, San Francisco, CA, 1967.
2. Key, E.L, "An Analysis of the Structure and Complexity of Non-Linear Binary Sequence Generators", *IEEE Trans. Inf. Theory*. vol. IT-22, pp. 732-736, 1976.
3. Rhee, M.Y, *Cryptography and Secure Communication*. McGraw-Hill, New York, 1993.
4. Rueppel, R.A, *Analysis and Design of Stream Ciphers*. Springer-Verlag, Berlin, Germany, 1986.
5. Lidl, R. and Niedereiter, H, *Finite Fields (Encyclopedia of Mathematics and its Application)*. Addison-Wesley, New York, Vol. 20, 1983.
6. Sarwate, D.V. and Pursley, M.B, "Crosscorrelation Properties of Pseudoran dom and Related Sequences", *Proceedings of the IEEE*. Vol. 68, No. 5, May 1980.
7. TIA/EIA/IS-95, *Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System*. July 1993.



김 지 홍(Ji Hong Kim) 정회원

1982년 : 한양대학교 전자공학과 공학사

1984년 : 한양대학교 전자통신과 공학석사

1996년 : 한양대학교 전자통신과 공학박사

1984년~1990년 : 금성전선 연구소

1991년~현재 : 세명대학교 전자공학과 조교수

이 만 영(Man Young Rhee) 정회원

서울대학교 전기공학과 공학사

미국 Colorado 대학교 공학석사 및 공학박사

미국 Virginia 주립대 공과대학 교수

국방과학연구소 제1부소장/한국전자통신 사장/삼성반도체 사장

한양대학교부총장/ 명예교수/한국통신보호학회장

제 31권 A편 제8호 참조

현재 : 한양대학교 전자통신과 명예교수

통신정보 보호학회 회장