논문 2008-5-22

물리 계층 보안시스템 MCC부호기 설계

Design of MCC Security System in Physical Layer

김건석*, 공형윤**

Gun-Seok Kim, Hyung-Yun Kong

요 약 본 논문은 빠르게 발전하고 있는 무선통신시스템에서 중요시되는 보안을 강화시키며 신뢰성 있는 통신을 가능하게 하는 MCC(M-sequence Convolution Code)채널부호기 설계를 제안한다. 제안한 부호기는 기존의 채널부호기가 가지는 오류 정정 특성뿐 아니라 정보데이터에 대한 비화성질을 부가하여 인증된 사용자만 접근할 수 있는 부호기이다. 제안한 부호기의 특성은 M부호열의 특성 중 평형특성을 이용함으로써 콘볼루션부호기의 출력부를 변화시켜 부호열을 얻는 물리계층의 보안 시스템이다. M부호열과 콘볼루션부호기를 사용함으로써 기존의 CDMA시스템에서 추가적인 부분 없이 간단하게 설계할 수 있으며 현재 사용되고 있는 콘볼루션부호기와 비교하였을 때 연집오류의 극복으로 약 0.1dB의 부호화 이득을 얻었고, 비화성능으로 인증된 사용자만이 송신된 데이터를 복구 가능한 것을 검증하였다. 비인증 사용자의 접근에 있어서는 SNR의 변화에 상관없이 50% 이상의 오류율을 보인다. 따라서 기존의 콘볼루션부호기 대신 제안한 MCC부호기를 사용함으로써 비화성능과 높은 BER성능을 얻을 수 있다.

Abstract Wireless data transmission is vulnerable to attackers and hackers. Recently, the fast development of wireless communication systems seamlessly increase the demand for security in this area. Moreover, error correction is especially important because various kinds of interferences among wireless devices. In order to solve two above problems, we propose to apply MCC (M-sequence Convolutional Code) in the system which is able to protect information and correct errors. The proposed system can obtain higher secure property by randomly changing the output connections by the proposed M-sequence. Performance of the system is analyzed according to BER (Bit Error Rate) and secure levels. The simulation results revealed that we can get the coding gain of 0.1 dB over conventional convolution coding technique. The proposed algorithm is installed in physical layer and easily implemented. Another advantage of our proposed (M-sequence and convolutional code) is that it can be applied to CDMA (Code Division Multiple Access) communication system.

Key Words : Convolution Code, PN-sequence, Security System

Ⅰ. 서 론

최근 무선통신 서비스는 방송, 멀티미디어 영상 및 음성, 모바일 서비스, 유비쿼터스 센서네트워크 등 많은 분야에서 활용되고 있다. 이러한 무선통신프로토콜은 데이터의 수신과정에서 유선에 비해 열악한 환경을 가지고 있기 때문에 전송 중 데이터의 손실이 발생한다. 손실 요인으로는 무선 통신채널환경의 잡음, 페이딩, 심볼간의 간섭 등이 대표적이며, 이러한 문제에 대처하기 위해 효과적인 전송기법에 관한 연구가 끊임없이 진행되고 있다.

또한, 최근 모바일 뱅킹, 인터넷 뱅킹, 멀티미디어 서비스 등의 다양한 서비스들이 사용자 개인정보를 전송하기 때문에 보안 문제가 끊임없이 야기되어지고 있다. 따라서 정보의 보안성능이 강화되어야 많은 사용자들이 안심하고 해당 서비스를 사용할 수 있게 된다. 현재 한국의 이동통신 망으로 채택되어 사용되고 있는 CDMA(Code Division Multiple Access) 방식을 이용한 통신 시스템은

*준회원, 울산대학교 전기전자정보시스템공학부
**정회원, 울산대학교 전기전자정보시스템공학부
접수일자 2008.9.9, 수정완료일자 2008.9.26

무작위 선택 특성을 갖는 PN 부호를 이용하여 각각의 사용자에 대한 보안특성을 부여하고 있다. 그 뿐만 아니라 데이터 신호를 PN부호를 이용하여 광대역의 전송신호로 만들어 전송함으로써 통신채널상의 다양한 잡음에 대하여 효과적으로 대처할 수 있는 특성을 가지고 있다. 그러나 최근 CDMA기술을 사용하는 휴대전화의 도청이 가능해짐에 따라 사회적문제로 대두되고 있다.

콘볼루션 코드는 현재 대부분의 유·무선 통신시스템의 채널코딩방식으로 채택되어 사용되고 있다. 본 논문에서는 PN부호와 콘볼루션 코드의 특성을 이용하여 보안과 잡음에 대한 문제 모두를 만족시킬 수 있는 코딩방식을 제안한다. 제안하는 시스템은 물리계층의 채널 부호기인 콘볼루션 코드의 출력방식을 PN부호열 중 하나인 M부호열을 이용한다. M부호열의 평형특성 때문에 0과 1의 개수는 0이 항상 1보다 하나가 작다. 따라서 M부호열의 앞이나 뒤에 0의 한 비트를 추가시킴으로써 같은 수를 얻을 수 있다. M부호열의 랜덤성을 이용하여 콘볼루션 코드에 비화성을 부여한다.

본 논문의 구성은 다음과 같다. 2장에서는 PN부호를 이용한 콘볼루션 코드기법에 대하여 설명하고, 제안한 시스템인 MCC를 설명한다. 3장에서는 제안한 MCC와 기존의 콘볼루션 코드의 오류정정능력을 비교하고 비인증 사용자의 데이터 복구율을 알아본다. 마지막으로 4장에서 본 논문의 결론을 내린다.

II. 제안한 콘볼루션 코드 기법

1. 콘볼루션 코드

그림 1은 구속장의 길이가 K이고 부호율이 1/2인콘볼루션 코드의 기본적인 형태를 나타낸 것이다.

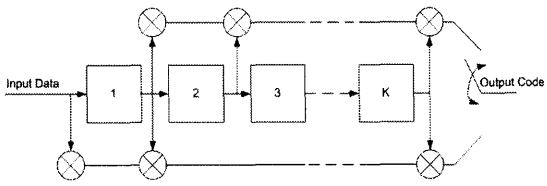


그림 1. 콘볼루션 코드
Fig. 1 Convolution Code

코드율이 1/2이고 구속장이 v=3인 콘볼루션 코드는 입력이 m(x)이면 하나의 출력에서 c0(x), 다른 하나의 출력에서 c1(x)가 합쳐져 C(x)로 나온다. 이 과정은 다음과 같은 다항식으로 표현 가능하다.

$$g_0(x) = 1 + x + x^2 \qquad (1)$$
$$g_1(x) = 1 + x^2$$

따라서 코드 다항식은

$$c_0(x) = m(x)g_0(x) \qquad (2)$$
$$c_1(x) = m(x)g_1(x)$$

코드C(x)는 다음과 같다.

$$C(x) = [c_0(x)c_1(x)] = m(x)[g_0(x)g_1(x)] = m(x)G(x) \qquad (3)$$

콘볼루션 코드의 복호 방식은 Viterbi 복호방식을 많이 이용하고 있으며, Viterbi 복호방식을 개선시킨 MAP(Maximum A Posterior) 복호화 방식, SOVA (Soft-Output Viterbi Algorithm) 방식 등 많은 방식이 있다. 현재 무선 이동통신시스템 및 가입자망 서비스 시스템 등 통신 시스템의 FEC 부호화 방식으로 채택되어 이용되고 있다.

2. PN부호-M부호열(M-sequence)

이상적인 PN 부호열은 +1과 -1이 완전히 무질서한 참된 난수로서 발생되는 것이다. 이러한 부호열 발생기로서 잘 알려진 것으로 M부호열 발생기가 있다.

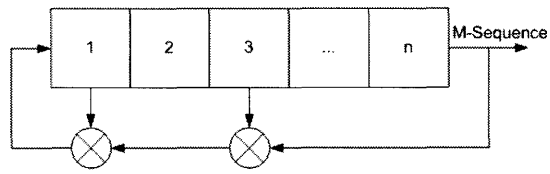


그림 2. M-부호열
Fig. 2 M-Sequence block diagram

M부호열 발생기는 그림2에 나타낸 것과 같이 0 또는 1의 상태를 저장하고 이동시킬 수 있는 쉬프트레지스터와 귀환 탭으로 구성되어 있다. 귀환 탭으로부터 발생되는 몇 개의 출력은 XOR을 취하여 쉬프트레지스터의 입력으로 돌아간다. 따라서 가장 오른쪽 레지스터의 값이 M부호열의 출력이 된다.

M부호열은 레지스터 개수를 m이라 하면 $2^m - 1$개가 주기가 되며, 그 이후에는 동일한 부호열의 데이터가 되풀이하여 출력된다. 본 논문에서는 PN부호열 중 M부호열을 선택하여 사용하였고 특성은 다음과 같다.

- 평형특성
  - 1의 개수: 2^{n-1}
  - 0의 개수: $2^{n-1} - 1$
- 런 특성
  - 부호열 가운데 0 또는 1이 연속하여 나타날 때, 그 연속의 길이
  - 길이 m의 런의 발생 빈도 : 2(m+1발생빈도)

3. 제안하는 MCC시스템

본 논문에서 제안하는 시스템은 콘볼루션부호기 출력을 M부호열로 스위칭시켜 코드를 만들어 내는 것이다. 이 때 c0(x)와 c1(x)의 비트 수를 같게 하는 M부호열의 특성을 컨볼루션부호기의 출력에 적용하여 그림 3과 같은 시스템 모델을 제안한다.

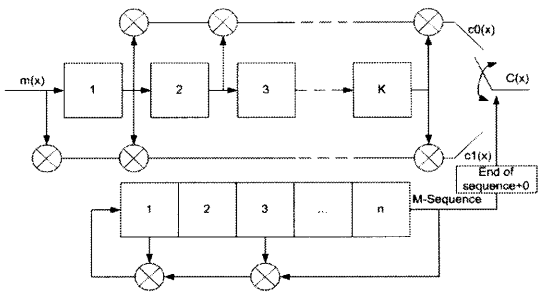


그림 3. 제안하는 MCC 시스템 모델
Fig. 3 Proposed MCC system model

그림 3에서와 같이 M부호열의 부호열이 콘볼루션 코드의 새로운 입력으로 들어가게 된다. 여기서 M부호열의 특징으로서 1이 0보다 항상 한 개의 비트가 많기 때문에 부호열 마지막에 0을 한 비트 추가(End of sequence+0)시켜 줌으로써 0과 1의 개수를 맞춰준다. 따라서 부호열의 개수는 다음과 같이 나타낼 수 있다.

$$\#\text{ of PN-sequence system} = 2^n - 1 + 1(0\text{ Bit}) = 2^n \quad (4)$$

여기서, #기호는 개수(number)를 나타내며, 0과 1의 개수는 다음과 같다.

$$\#\text{ of 0 and 1} = 2^{n-1} \quad (5)$$

제안한 콘볼루션 코드들을 전송한다면 비화성능으로 다음과 같은 조건이 성립된다.

첫 번째로 M부호열의 레지스터를 정확히 알아야 하고, M부호열의 탭을 정확히 알아야만 원래의 콘볼루션 코드를 알 수 있게 된다. 따라서 다음과 같은 확률을 얻을 수 있다.

$$P(find\,sequence) = \left(\frac{1}{2}\right)^n \times \frac{1}{n^2(n!)} \quad (6)$$

예를 들면, 다음 표 1에 나오는 데이터 흐름은 정보신호 [0 1 0 0]의 데이터와 레지스터 3개인 M부호열과, 구속장의 길이가 3이고 생성다항식이 $g_0(x) = x^2 + 1$, $g_1(x) = x^2 + x + 1$의 입력데이터에 대하여 코드 생성과정을 나타낸 것이다.

이 때 기존의 콘볼루션 코드의 성능은 그대로 유지되며 콘볼루션 코드의 단점인 연집오류에도 인터리빙 효과로 인해 강해졌음을 코드신호로부터 알 수 있다.

표 1. 입력데이터에 대하여 MCC 코드생성과정
Table 1. MCC code generating process

구분	Digit value
데이터 M부호열(+0)	0 1 0 0 1 1 1 0 1 0 0 (0)
c0(x) c1(x)	0 0 1 1 0 1 1 1
C(x)	0 1 1 0 1 0 1 1

4. 제안하는 MCC시스템

MCC의 복호는 기존의 콘볼루션 코드의 복호 방식인 Viterbi 알고리즘을 그대로 사용할 수 있다. Viterbi 복호 알고리즘은 ML(Maximum Likelihood) 방식으로 수신된 데이터 값과 코딩 특성을 비교하여 근사도가 가장 큰 값을 판정하여 복구하는 것이다.

그림 4는 구속장의 길이가 3인 경우의 콘볼루션 코드의 트렐리스 다이어그램을 나타낸 것으로 좌측의 상자안에 표시된 내용은 레지스터가 가지는 값으로 상태를 나타낸 것이고 각 시간에 따른 변화를 보여주고 있다. 각 시간의 이동에 따른 점선과 실선은 코드를 생성하기 위해 거쳐나가는 경로를 나타내며, 각 선의 중간에 표시된

값은 경로를 거친 코드를 나타낸다. 그리고 점선과 실선은 입력데이터인 0과 1을 나타낸다. 예를 들어 입력데이터가 1 0 1 …로 입력이 되면, 출력은 101 011 001 …이 생성된다.

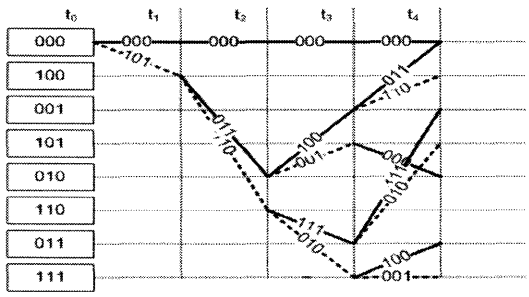


그림 4. 콘볼루션 코드의 트렐리스 다이어그램
Fig. 4 Trellis diagram to decode convolution code

따라서 수신된 데이터의 복구는 표 2와 같이 진행된다. 데이터가 송신되면 수신측에서는 모든 경로에 대한 해밍거리(Hamming Distance)를 구하고 최소거리를 갖는 경로가 최대근사 경로로 결정하여 복호하게 된다. 따라서 송신상의 오류에 대하여 오류를 정정할 수 있다.

표 2. 수신데이터에 대하여 MCC 코드복호과정
Table 2. MCC code decoding process

구분	Digit value
RC(x) M부호열(+0)	0 1 1 0 1 0 1 1 1 1 1 0 1 0 0 (0)
Rc0(x) Rc1(x)	0 0 1 1 0 1 1 1
데이터	0 1 0 0

Ⅳ. 실험 및 결과

본 논문에서는 두 가지로 나눠 모의실험을 하였다. 첫 번째는 기존의 콘볼루션 코드와 성능을 비교하기 위한 컴퓨터 모의실험이고, 두 번째는 비화성능을 검증하기 위한 모의실험이다. 컴퓨터 모의실험 환경으로 무선 통신환경은 가우시안채널(AWGN)을 사용하였고 하나의 데이터 프레임 그룹은 8비트이며, 콘볼루션 코드의 생성다항식은 $g_0(x) = x^2 + x + 1$, $g_1 = x^2 + 1$이다. M부호열의 초기 레지스터 값은 [0 0 0 1]로 설정하였고, 귀환 탭은 첫 번째 레지스터와 마지막 레지스터에 연결하였으며 다음과 같은 결과를 얻었다.

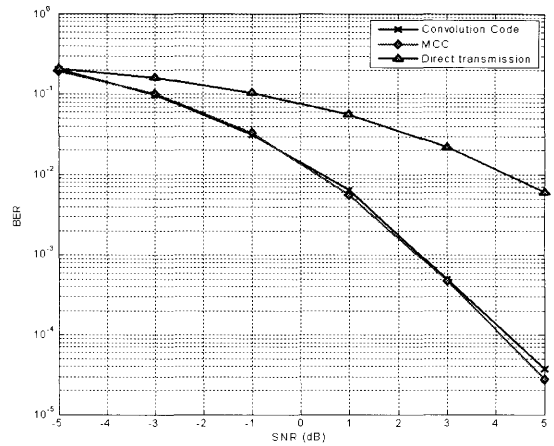


그림 5. 제안한 시스템의 BER 성능
Fig. 5 BER performance of proposed system

직접전송과 기존의 콘볼루션부호기와 제안한 MCC부호기의 성능을 비교하면 10-2에서 채널 부호화를 하지 않은 직접전송보다 콘볼루션부호기는 약 4dB이득을 보이고, 제안한 MCC부호기는 콘볼루션부호기보다 0.1dB 정도의 이득이 있다. 따라서 제안한 부호기는 출력부의 스위칭의 효과로 인하여 콘볼루션부호기의 연집오류를 극복하기 때문에 기존의 콘볼루션 부호보다 좋은 성능을 보인다. 따라서 콘볼루션부호기의 특징으로 인하여 데이터 프레임의 길이가 길수록 MCC부호기는 더 많은 연집오류를 극복하여 더욱 좋은 성능을 얻을 수 있게 된다.

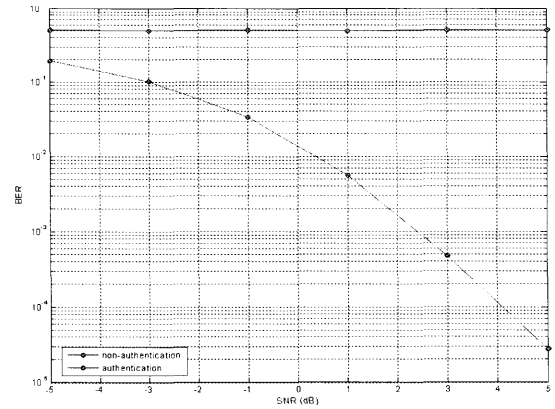


그림 6. 사용자 접근 허용도에 관한 성능
Fig. 6 Security performance of proposed system(Unit: Bit)

그림 6에서는 제안한 시스템의 장점인 비화성능에 관한 성능곡선을 나타낸다. 그림에서 두 가지 곡선은 인증된 사용자(authenticator)와 비인증 사용자(non-authenticator)의 데이터 복구율에 대한 그래프이다. SNR에따라 변화하지 않는 곡선은 랜덤하게 M부호열을 만들어 내어 송신된 신호를 검출하여 복호하는 비인증 사용자를 나타낸다. 비인증 사용자의 복호율은 SNR의 값의 변화와 상관없이 50%의 데이터가 오류를 나타내고 있다. 50%의 오류는 복구할 때 0과 1의 데이터를 랜덤하게 생성한 결과와 같다고 볼 수 있다. 인증사용자의 시스템의 경우 송신단의 M부호열을 정확히 만들 수 있기 때문에 SNR이 증가함에 따라 지수적으로 오류율이 감소함을 알 수 있다.

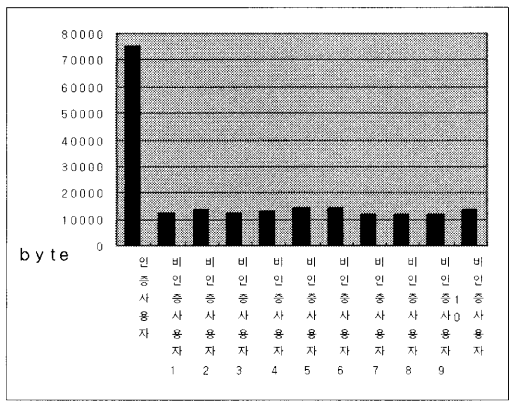


그림 7. Packet단위 접근 허용도
Fig. 7 Security performance of proposed system(Unit: packet)

그림 6에서는 비트 단위로 송·수신 데이터를 비교한 것이고 그림 7은 60만 비트에 대하여 바이트단위로 송신 데이터와 수신 데이터를 비교한 것이다. 세로축은 올바르게 찾아낸 바이트의 수를 나타내고, 가로축은 첫 번째는 인증사용자이고 나머지 1~10은 비인증 사용자를 나타낸다. 인증 사용자는 송신 측과 같은 M-sequence 초기값을 사용하였고 비인증 사용자는 다른 초기 값을 갖는 것으로 설정하였다. 이 결과 역시 인증 사용자의 경우 모든 데이터를 정확히 수신했으나 비인증 사용자의 경우 다른 스위칭을 가짐으로서 정확한 데이터를 얻을 수 없다. 따라서 그래프에서 나타나듯이 비인증사용자가 랜덤하게 찾아낸 바이트는 1200바이트 내외이다.

V. 결 론

제안한 MCC는 최근 활발하게 이용되는 무선통신 시스템에서 물리계층 채널부호화 기법으로 에러정정이 가능한 동시에 비화성능을 가진다. 기존의 CDMA통신 시스템에서 표준화되어있는 채널부호기인 콘볼루션 코드와 M부호열을 사용함으로써 추가적인 부분 없이 구현이 가능하다. 또한 콘볼루션 코드 대신 MCC를 사용함으로써 기존의 콘볼루션 코드의 약점인 연집오류를 스위칭 효과로 인하여 극복할 수 있다. 따라서 본 논문에서 제안된 프로토콜이 네트워크 계층의 암호화와 함께 진행한다면 높은 시너지효과를 기대할 수 있다.

참 고 문 헌

[1] Stephen B. Wicker, "Error Control Systems for Digital Communication and Storage", School of Electrical and Computer Engineering Georgia Institute of Technology, pp. 246-355, 1995

[2] Floyd M. Fardner, John D. Baker, "Models of Communication Signals and Process", JOHN WILEY & SONS. Inc, pp. 261-273

[3] G. D. Forney, Jr., "Cnvolutional codes I : Algebraic structure", IEEE Trans. Inform. theory, vol. IT-16, pp. 720-738, Nov. 1970

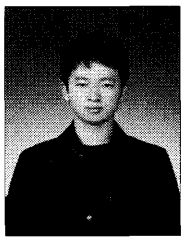
[4] A. J. Viterbi and J. K. Omura, "Principle of Digital Communication and Coding", NY: McGraw-Hill, 1979

[5] Proakis, "Digital Communications", pp. 471-514, McGraw-Hill 1989

※ Acknowledgement : 이 논문은 2007년도 정부(과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(No. R01-2007-000-20400-0)

저자 소개

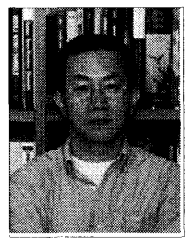
김 건 석(준회원)



- 2007년 2월 울산대학교 전기전자정보시스템공학부 학사
- 2007년 3월~현재 울산대학교 전기전자정보시스템공학부 석사과정

<주관심분야 : OFDM, MC-CDMA, QAM, 멀티코드, 협력통신>

공 형 윤(정회원)



- 1989년 2월 미국 New York Institute of Technology 전자공학과 학사
- 1991년 2월 미국 Polytechnic University 전자공학과 석사
- 1996년 2월 미국 Polytechnic University 전자공학과 박사
- 1996년~1996년 LG전자 PCS 팀장
- 1996년~1998년 LG전자 회장실 전략 사업단
- 1998년~현재 울산대학교 전기전자정보시스템공학부 교수

<주관심분야 : 모듈레이션, 채널 부호화, 검파 및 추정 기술, 협력통신, 센서 네트워크>