

비화 특성을 가진 RCNC(Random Connection Node Convolutional) 부호 기법의 설계

공형윤[†]·조상복[†]·이창희^{††}

요약

본 논문에서는 비화특성을 가진 새로운 FEC (Forward Error Correction) 부호기법으로 RCNC (Random Connection Node Convolutional) 부호화방식을 소개한다. 최근의 무선통신시스템은 다양한 멀티미디어 데이터 서비스를 하고 있다. 이러한 시스템은 전송 중 발생한 오류에 대한 정정 능력과 더불어 인증 사용자의 접근에 대한 비화 특성이 중요시된다. 이러한 문제를 해결하기 위한 방안으로 RCNC 부호화 방식은 전송 중 발생한 에러에 대한 오류 정정 기능을 가지면서, 전송데이터에 대한 비화성질을 부가하여 허용된 사용자 이외에는 접근이 불가능하도록 하는 암호화 특성을 가진다는 점이다. 본 논문에서는 RCNC 부호화 기법의 동작과 특성을 설명하고 있으며, 또한 컴퓨터 시뮬레이션을 이용하여 에러 정정 능력과 사용자 접근 허용정도를 검증하였다.

Design of RCNC(Random Connection Node Convolutional) Code with Security Property

Hyung-Yun Kong[†] · Sang-Bock Cho[†] · Chang-Hee Lee^{††}

ABSTRACT

In this paper, we propose the new FEC(Forward Error Correction) code method, so called RCNC (Random Connection Node Convolutional) code with security property. Recently, many wireless communication systems, which can provide integrated services of various media types and bit rates, are required to have the ability of secreting information and error correction. This code system is a kind of convolutional code, but it has various code formats as each node is connected differently. And systems by using RCNC codes have an ability of error correction as well as information protection. We describe the principle of operating RCNC codes, including operation examples. In this paper, we also show the performance of BER(Bit Error Rate) and verify authority of network system with computer simulation.

1. 서론

21세기 무선통신서비스는 많은 양의 멀티미디어를 전송할 수 있는 통신시스템이 요구된다. 이러한 무선을 이용한 데이터의 전송은 데이터의 올바른 수신에 관점에서 유선에 비해 많은 약점을 가지고 있어 전송

중 데이터의 손실이 우려된다. 이러한 문제에 대처하기 위한 전송기술에 관한 연구가 논의되어지고 있다. 또한 멀티미디어의 다양한 데이터를 전송하는데 있어서 인증 사용자에게 대한 접근의 허용에 관한 문제는 데이터 서비스의 관점에서 중요한 부분을 차지한다. 특히 군에서는 그 보안성이 중요시되며 보안을 유지하기 위한 방법으로 PN (Pseudo Random) code를 이용한 CDMA 방식을 사용하여 보안성을 유지하였다. 그리고 최근에 들어서는 CDMA 기술을 일반에 적용하여 Cel-

[†] 정 회 원 : 울산대학교 전기전자자동화공학부 교수
^{††} 준 회 원 : 울산대학교 대학원 전기전자자동화공학부 졸업
논문접수 : 2000년 3월 6일, 심사완료 : 2000년 11월 27일

ular system이나 PCS system을 이용하고 차세대 이동통신시스템(IMT-2000)의 기술로 채택되어 있다[1]. CDMA 기술은 GPS(Global Positioning System)에 동기 되어 있는 PN code를 나누어 각각의 사용자에 변호를 부여하여 사용자 각각을 구분한다는 특징을 가진다. CDMA system은 랜덤 특성을 갖는 PN code를 이용하여 각각의 사용자에 대한 보안성을 유지시켜 주고 있다. 그러나 PN code의 사용은 그 사용형태가 국가적 차원이나 거대한 규모의 집단에서 운용하므로 소규모의 네트워크 시스템을 구성하는데 있어, 비화성을 요구되는 시스템을 설계할 때 PN code를 이용하는 데는 제약이 가지게 된다. 이러한 문제를 해결코자 본 논문에서는 소규모의 네트워크 시스템에 적용이 되어질 수 있는 새로운 코드를 소개한다. 유선이든 무선이든지 데이터를 전송하는데 있어서 송신 데이터가 전송 채널 상에서 다양한 형태를 갖는 잡음(noise, fading, multipath, ISI...)들에 의해서 변형되어 수신 될 때 본래의 송신 데이터를 제대로 복원할 수 없게 된다[2]. 이를 대비하여 송신할 때 정보데이터에 일정한 규칙을 갖는 여분의 비트를 첨가하여 보내게 된다. 수신 측에서는 수신된 데이터의 일정한 규칙에 따라 여분의 비트를 조사하여 수신데이터의 오류 유무를 판단하게 된다[3, 4]. 이러한 기술을 Forward Error Correction (FEC) 부호화 기법이라 한다. 1948년 Shannon에 의해 디지털 통신 시스템에 있어서 이와 같은 정보 이론에 대한 논문이 발표된 이후로 FEC 부호화 기법에 대한 논의가 시작되었으며[5], 이후 Gallager, Cover 그리고 Thomas 등에 의해 많은 발전을 이루게 되었다. 초창기 FEC 부호화 기법은 블록 부호로 주로 이용하게 되었다. 그러나 이 블록 부호는 정보 데이터를 Block으로 나누어 이에 일정한 규약을 갖는 여분의 비트들을 첨가하여 코드를 만드는 방법으로 데이터를 처리하는데 많은 시간이 소요되고, 또한 오류 검출 및 정정에 한계를 가지게 있다. 그래서 이러한 단점을 보완하기 위해, 이전과 이후 비트에 대한 정보를 가지는 연속적인 시퀀스에 대한 여분의 비트를 덧붙여서 코드를 만드는 콘볼루션 부호가 개발되었다. 이러한 콘볼루션 부호는 현재 대부분의 무선, 유선 통신시스템의 FEC 부호화방식으로 채택되어 사용되고 있다. 본 논문에서는 앞에서 언급한 비화성의 문제와 채널 상에서의 잡음에 대한 문제 모두를 만족시킬 수 있는 콘볼루션 부호를 응용한 RCNC 부호화 방식을 제시한다. 본 논문

의 구성은 아래와 같다. 1장에서는 RCNC 부호화기법에 대하여 설명하고, 2장에서는 부호기의 여러 가지 특성들과 그 동작의 원리에 관하여 설명한다. 그리고, 3장에서는 RCNC 부호기의 오류 정정능력과 인증자 접근에 따른 수신 데이터의 올바른 전송에 대한 성능을 논하고, 마지막으로 4장에서 본 논문의 결론을 내린다.

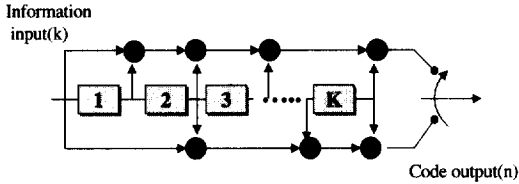
2. RCNC 부호화 기법

최근 대부분의 통신시스템은 멀티미디어의 다양한 데이터를 서비스하고 있고, 이러한 멀티미디어 데이터를 전송하는데 있어 많은 요구 사항들이 있다. 먼저 데이터 서비스는 서비스를 필요로 하는 사용자와 인증된 사용자에게만 접근이 가능하도록 하는 비화성을 가져야 한다. 멀티미디어 데이터의 전송은 그 자체적으로 방대한 양을 가지고 있을 뿐만 아니라 여러 사용자들에 대하여 Point to Multi-Point, Point-to-Point, Multi-Point to Multi-Point 방식의 다양한 방식의 서비스를 제공 해야한다. 이러한 관점에서 여러 사용자들 중에서 필요로 하는 사용자를 선택하고, 인증된 사용자에 대하여만 서비스를 제공할 수 있는 것은 서비스 사업자 및 소비자 모두에게 중요한 문제이다. 다음으로, 무선이든 유선이든 데이터의 전송시 발생할 수 있는 여러 가지 잡음, 간섭등에 대하여 강한 시스템이어야 한다. 멀티미디어의 데이터를 전송하는데 있어서 전송중 데이터의 소실은 재전송 요구에 의해 데이터 전송 지연 효과를 가져오게 됨으로써 전체적인 시스템의 부하를 크게 할 것이고, 특히 실시간 데이터 전송이 필요한 서비스의 경우에는 서비스의 질적 저하를 가져오게 된다. 이러한 문제점들을 개선하기 위한 효과적인 FEC 방식에 대한 연구는 과거, 현재뿐만 아니라 미래의 통신시스템에서 중요한 부분을 차지하게 될 것이다. 본 논문에서는 인증된 사용자에 대해서 접근 허용을 위한 비화성 문제와 전송중 오류에 대한 여러 정정 모두를 해결할 수 있는 RCNC 부호화 방식을 제안한다.

2.1 기존의 콘볼루션 부호

콘볼루션 부호는 1955년 Elias에 의해서 개발된 이후 1967년 Viterbi에 의해서 Viterbi 복호 알고리즘의 개발로 급격한 발전을 가져 왔다. (그림 1)은 구속장의

길이 K 이고 데이터율이 $1/2$ 인 콘볼루션 부호기 부분을 나타낸 것이다[6].



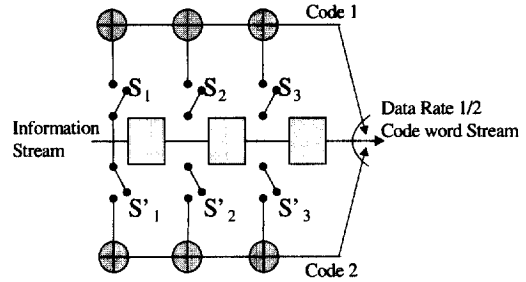
(그림 1) 콘볼루션 부호기의 구조

콘볼루션 부호기의 특징은 다음과 같이 설명할 수 있다. 콘볼루션 부호기는 입력 시퀀스에 대하여 연속적으로 부호화 작업을 실행하게 됨으로써 블록부호 방식에 비해 부호화 지연 시간을 줄일 수 있고, 또한 적은 비트를 추가함으로써 동일한 오류 정정 능력을 갖는 부호기를 설계할 수 있다는 장점을 가지고 있다. 그러나 연속적인 입력 시퀀스에 대해 부호화 작업을 함으로써 인하여 이전 비트에 대하여 그 연관성을 가지고 있으므로 버스트(burst) 에러에 약하다는 특성을 가지고 있다. 그리고, 콘볼루션 부호의 복호화 방식으로 최근 많은 연구가 이루어지고 있다. 전통적인 복호화 방식으로는 Viterbi 복호화 방식을 이용하고 있으며, 그 이후 Viterbi 복호화 방식을 개선시킨 MAP(Maximum A Posterior) 복호화 방식, SOVA(Soft-Output Viterbi Algorithm) 방식등 많은 발전을 이루었다. 이러한 콘볼루션 부호는 현재의 무선 이동 통신 시스템(PCS, IMT-2000..) 및 가입자망 서비스 시스템(WLL, LMDS..)등 통신 시스템의 FEC 부호화 방식으로 채택되어 이용되고 있다.

2.2 RCNC 부호화 기법

RCNC 부호기는 Convolutional code의 개선된 구조로 전송 데이터에 암호화 기법을 적용하여 부호화 함으로써 전송 데이터에 비화성질과 오류 정정 능력을 가지도록 부호화한 것이다. (그림 2)는 RCNC 부호기의 블록도를 나타내고 있다.

(그림 2)에서 보는 바와 같이 부호기는 shift register들과 각각의 node를 연결하기 위한 switch($S_1 \sim S_3$, $S'_1 \sim S'_3$)들로 구성된다. 여기서 switch의 ON/OFF(연결/미연결)에 따라서 부호화기의 특성은 달라진다. 예를 들어 S_1, S_3 , 그리고 S'_2, S'_3 가 연결된 상태라면 생성다항식 g_1 이 $1+x^2$ 이고, g_2 가 $x+x^2$ 인 일반적인 콘볼



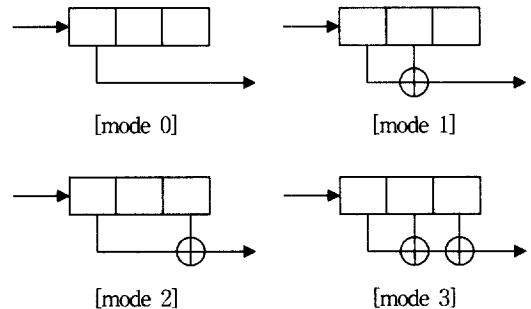
(그림 2) RCNC 부호기의 구조

루션 부호가 된다. 그리고 이러한 생성다항식들을 구분하기 위해서 본 논문에서는 MODE라는 개념을 사용한다. 즉, 생성다항식이 서로 다른 것들을 통칭하기 위한 것으로 부호기 설계자에 의해서 각각의 MODE를 정의하게 된다. 다음의 <표 1>은 구속장의 길이가 3인 경우의 MODE로 구분된 생성다항식의 한 예이다.

<표 1> 구속장의 길이가 3인 경우 RCNC 부호기의 MODE 예

| MODE | 생성다항식 | 연결 |
|------|--------------|-------------|
| 0 | $1, x, x^2$ | 100,010,001 |
| 1 | $1+x, x+x^2$ | 110,011 |
| 2 | $1+x^2$ | 101 |
| 3 | $1+x+x^2$ | 111 |

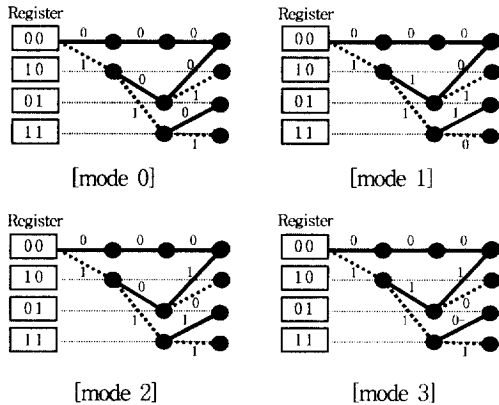
(그림 3)과 (그림 4)는 MODE에 따른 RCNC 부호기와 그에 따른 격자도를 나타낸 것으로 구속장의 길이를 3으로 하여 간략하게 표현한 것이다. 구속장의 길이가 길어질수록 MODE에 따른 부호기의 종류가 많아지고, 격자도의 복잡도는 증가하게 된다.



(그림 3) MODE에 따른 RCNC 부호기

(그림 4)에 나타낸 격자도는 기존의 콘볼루션 부호

기를 해석하기 위한 격자도와 동일하며, 부호기의 입력 데이터에 따른 출력 데이터를 나타낸 것이다. RCNC 부호기는 하나의 입력에 대하여 다수(n)의 부호를 출력하기 때문에 임의의 데이터 율 1/n을 구성할 수 있다. 그러므로 개별적인 MODE에 따른 격자도를 나타냄으로써 RCNC 부호기의 해석 및 설계가 용이하게 된다.



(그림 4) MODE에 따른 RCNC 부호의 격자도

이러한 RCNC 부호기는 비화성질을 부여하기 위해서 정해진 시간에 따라 MODE는 변하게 된다. 만약 입력 데이터의 1비트마다 MODE가 변하게 된다면 각각의 입력 비트에 따라 서로 다른 방식의 부호화기로 부호화가 생성되게 된다. MODE가 바뀌는 시간은 적절히 구성되어질 수 있는데 1 byte, 1 word나 1 frame 등 설계자의 선택에 따라 달라질 수 있다. 짧은 시간에 MODE의 변화를 가지게 되면 입력데이터에 따른 부호화 과정보다 MODE의 변화에 따른 시간이 많은 부하를 가져오게 되어 적절한 MODE 변화 간격을 가지는 것이 중요하다.

3. RCNC 부호화 기법의 특성 및 동작원리

3.1 RCNC 부호화 기법의 생성다항식과 MODE의 수

RCNC의 MODE는 부호기 구축장의 길이에 따라서 변하게 되는데 구축장의 길이가 길어질 수록 MODE의 수는 증가하게 된다. 식 (1)은 RCNC 부호기의 MODE의 수를 나타낸 것이다.

$$N = (2^{k-1})^{c-1} \tag{1}$$

여기서 N은 생성 가능한 MODE의 수이고, k는 shift register의 수(구축장의 길이)이고, c는 데이터 율에 해당한다. 같은 길이의 구축장을 갖는 콘볼루션 부호를 사용하여 N명의 사용자가 서로 다른 코드를 만들어 전송할 수 있다. 위의 식에서 알 수 있듯이 구축장의 길이가 길어질수록 부호화 MODE의 수가 많아져 많은 종류의 RCNC 부호화를 설계할 수 있다. 하나 RCNC 부호기의 MODE 수가 많아지면 인증된 사용자 이외의 접근은 그 만큼 어려워지게 되고, 이렇게 됨으로써 부호기의 비화성질은 높아진다고 할 수 있다. 이에 반하여 콘볼루션 부호기는 특정 생성연결 다항식에서는 급격하게 BER 성능이 떨어지는 현상이 생기게 된다. 이러한 현상은 RCNC 부호기의 특성을 저하시키는 요인이 됨으로 충분한 실험으로 RCNC 부호기의 MODE에서 제외시켜 전체적인 부호기의 BER 성능을 유지하여야 할 것이다.

3.2 Non-Recursive/Recursive Convolutional code를 이용한 RCNC 부호화 기법

콘볼루션 부호기는 Non-recursive와 Recursive convolutional code로 나누어 질 수 있다. Non-recursive convolutional code의 구성은 (그림 3)과 같고 그에 해당하는 격자도는 (그림 5)에 해당한다



(그림 5) $g = x^3 + x^2 + 1$ 인 Non-recursive Convolutional encoder

Non-recursive convolutional code의 코드어에서는 동일한 길이의 구축장을 갖는 부호기는 동일한 경로를 가지고 코드어가 생성되게 된다. 각 생성다항식간에 시간의 지연만을 가지고 동일한 코드를 가지는 경우가 있으므로 전체 연결 가능한 생성코드의 길이가 2^{k-1} 이 되는 것이다. Non-recursive code 생성식은 식 (2)와 같이 표현할 수 있다.

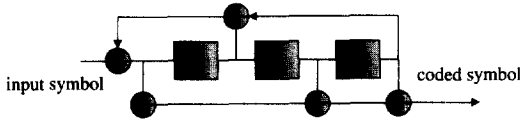
$$g(x) = g_1(x) \tag{2}$$

여기에서 $g_1(x)$ 는 각 shift register node의 연결을 나타내는 식이다.

Recursive code 생성식은 식 (3)과 같이 표현할 수

있으며 (그림 6)는 이에 대한 블록도를 나타내고 있다.

$$g(x) = \frac{g_1(x)}{g_2(x)} \quad (3)$$



(그림 6) Recursive Convolutional encoder

식 (3)에서 $g_1(x)$ 는 출력의 각 shift register node에 연결되는 식이고, $g_2(x)$ 는 귀환이 각 shift register node에 연결되는 식을 나타낸다. Recursive convolutional code를 이용할 경우에는 생성 다항식의 연결에 따라 격자도의 경로 자체가 변하게 된다. 그렇기 때문에 비화성에 있어 보다 좋은 성능을 가지게 되지만 부호기의 복잡도가 증가하게 된다.

<표 2>는 구속장의 길이가 4인 Non-recursive convolutional code의 MODE 표를 나타낸 것이다. 여기에서, MODE는 RCNC 부호기를 구성하는데 있어 서로 다른 생성다항식을 구분하기 위한 표시이며, 이러한 Mode는 부호어가 생성되는데 있어 각각의 시간에 따라 변화하게 된다. 간단한 예를 들면 Mode가 0, 3, 4, 2.의 순으로 변화면서 부호어를 만들어 낸다면, 그 때의 생성 다항식은 다음과 같다. (x^3 or x^2 or x or 1), (x^3+x^2+x or x^2+x+1), (x^3+1), (x^3+x or x^2+1)...

<표 2> 구속장의 길이가 4인 경우의 MODE에 따른 생성 다항식

| MODE | 생성 다항식 |
|------|-----------------------|
| 0 | $x^3, x^2, x, 1$ |
| 1 | $x^3+x^2, x^2+x, x+1$ |
| 2 | x^3+x, x^2+1 |
| 3 | x^3+x^2+x, x^2+x+1 |
| 4 | x^3+1 |
| 5 | x^3+x^2+1 |
| 6 | x^3+x+1 |
| 7 | x^3+x^2+x+1 |

Non-recursive convolutional code와 Recursive convolutional code와의 차이는 생성코드의 격자도에서 쉽게 찾아 볼 수 있다. 전자의 경우에는 생성코드의 가치가 입력의 데이터에 대하여 동일한 경로를 따라서

생기게 되고 단지 코드화되는 코드어만 달라지게 된다. 그러나 Recursive convolutional code를 이용하게 된다면 코드어 뿐만 아니라 가치의 경로도 바뀌게 되고 더욱 복잡한 시스템이 되겠지만 비화성에 있어서 그 만큼 더 우수한 성능을 가질 수 있다. Recursive convolutional 부호기와 Non-Recursive convolutional 부호기의 RCNC 부호기 구성에 따른 특성을 보면 <표 3>과 같다.

<표 3> 부호기의 구성에 따른 RCNC 부호기의 특성

| | Non-Recursive convolutional code | Recursive convolutional code |
|-------------|----------------------------------|---|
| 생성 다항식 | $c(x) = d(x) \cdot g(x)$ | $c(x) = d(x) \cdot \frac{g_1(x)}{g_2(x)}$ |
| 가능한 MODE의 수 | $(2^{k-1}) C_n$ | $(2^{k-1}) \cdot (2^n) C_n$ |
| 복잡도 | Low | High |
| 비화성 | Low | High |

3.3 RCNC 부호화 기법의 오류 검출 및 정정 능력

RCNC 부호는 기존의 콘볼루션 부호와 크게 다른 부분이 없이 코드어를 만들어 내고 그 코드어를 찾아 낼 수 있다. 즉, 기존의 격자도를 이용하여 코드어를 만들어내고 Viterbi 복호 알고리즘 와 MAP 복호 알고리즘[7]을 이용하여 그 복호가 가능하다. 그 복호방식은 기존의 방식을 그대로 이용이 가능하며 시뮬레이션 결과에서도 알 수 있듯이 최적의 콘볼루션 부호를 구성한 경우보다는 BER(bit error rate) 성능이 좋지 않다. BER 10^{-3} 의 성능이 요구될 때 약 7dB의 SNR이 요구된다. 그러므로 위의 경우에 기존의 성능을 그대로 유지하면서 비화성의 성질을 가미한 콘볼루션 부호를 구성할 수 있다.

3.4 RCNC 부호화 기법의 Bi-Orthogonal 신호적 특성

생성된 부호어의 성질을 보면 같은 입력 데이터에 대해 출력되는 코드어의 성질은 Bi-orthogonal한 성질을 가지고 있다. 즉, 부호어간의 상관성(z_{ij})을 구하려면 식 (4)를 이용하면 된다.

$$z_{ij} = \frac{\text{일치하는 bit 수} - \text{일치하지 않는 bit 수}}{\text{전체 bit 수}} \quad (4)$$

생성식은 $c(x) = d(x)g(x)$ 로 나타내어 질 수 있다. 위의 식을 이용하여 구속장의 길이가 4인 콘볼루션 부

호를 예로 들면 다음과 같이 간단하게 표현된다.

MODE 1에 대한 생성 코드 ($k=4$)

$$d(x) = x^7 + x^4 + x^3 + x^2 + 1, \quad g(x) = x^3 + x^2 \text{ 일 때}$$

$$c(x) = x^{10} + x^7 + x^6 + x^5 + x^3 + x^9 + x^6 + x^5 + x^4 + x^2$$

$$= x^{10} + x^9 + x^7 + x^4 + x^3 + x^2$$

$$\therefore c: 11010001110$$

즉, 부호화되는 코드는 c 와 같게 된다. 여기서, 입력 데이터 1001,1101에 대하여 각 MODE에 따라 출력되는 부호어를 표시하면 <표 4>를 만들 수 있다.

<표 4> 입력 코드에 따른 생성 코드의 예

| 입력 데이터 | 1001,1101 |
|--------|-----------|
| MODE | 생성되는 코드어 |
| 0 | 1001,1101 |
| 1 | 1101,0011 |
| 2 | 1011,1010 |
| 3 | 1111,0100 |
| 4 | 1000,1110 |
| 5 | 1100,0000 |
| 6 | 1010,1001 |
| 7 | 1110,0111 |

여기서, 생성 부호어의 상관계수를 찾아보면 식 (5)를 만족한다.

$$z_{ij} = \begin{cases} 1, & i=j \\ 2/M, 0, 2/M, & i \neq j \end{cases} \quad (5)$$

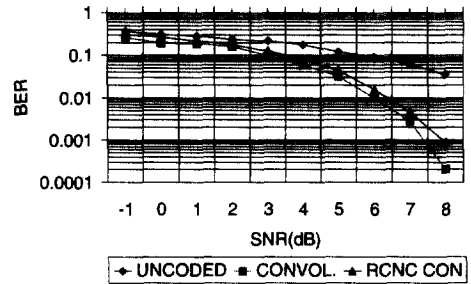
식 (5)는 부호어의 Bi-orthogonal한 신호의 특성을 나타냄을 보여주고 있다.

4. 모의실험 결과

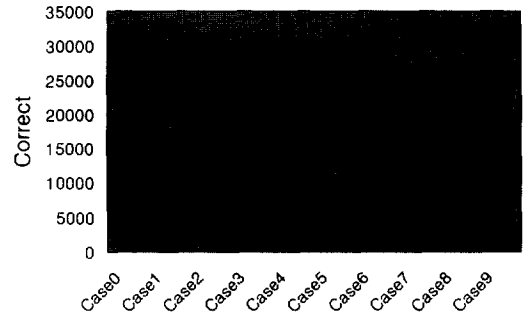
본 논문에서는 무선 전송 환경을 가우시안 채널로 가정하여 모의실험[8] 하였으며, (그림 7)은 RCNC 부호의 오류 정정 능력에 대한 BER 성능을 나타내고 있다. 여기서 볼 수 있듯이 BER 10^{-3} 에서 약 -0.3 dB의 코딩 이득을 보이고 있다. 최적의 콘볼루션 부호기를 설계한 상황에서보다, BER특성이 저하되게 된다.

(그림 8)은 인증된 사용자와 비 인증 사용자간의 올바른 수신 데이터를 얼마나 수용하는지에 대한 시뮬레이션 결과 그래프이다. 여기서 사용된 신호의 Block은 30000이다. 또한, 사용한 MODE의 수는 3개이다. 즉,

30000개의 데이터를 하나의 정보 Block으로 하여 30000개에 대한 인증접근 허용이 어느 정도인지를 검증하였다. 여기서 보는 것 같이 Case0에 해당하는 인증 사용자의 경우에는 100%의 인증접근이 가능하지만, 인증되지 않은 사용자의 경우(Case1-Case9)에는 모두 30% 이하의 낮은 접근허용을 나타내고 있다.



(그림 7) RCNC 부호화기의 BER 성능 분석



(그림 8) 사용자 접근 허용도

각 비트 당 비인증 사용자 접근허용 가능성 ($P_b(x)$)은 식 (6)과 같이 표현된다.

$$P_b(x) = \frac{1}{M} \quad (6)$$

여기서 M 은 시스템에 사용된 MODE의 수이다. MODE의 수가 증가할수록 비인증 사용자의 접근허용 가능성은 줄어들게 되어 시스템의 비화성질은 높아지게 된다. 그리고, MODE 수에 따른 비인증 사용자의 접근허용은 식 (7)과 같이 표현이 가능하다.

$$P(x) = \left(\frac{1}{M}\right)^B \quad (7)$$

여기서, $P(x)$ 는 비인증 사용자가 올바르게 접근할 수 있는 가능성을 나타내고 있다. B는 정보 Block의 길이에 해당한다. 마찬가지로 정보 Block의 길이가 길어질수록 접근허용가능성이 줄어들게 된다. (그림 7), (그림 8)의 모의실험 결과에서도 알 수 있듯이 RCNC 부호화 기법은 전송중의 오류에 대한 정정 능력과 더불어 사용자간의 인증 성능도 가지고 있어 통신시스템을 구성하는데 있어 보다 효과적인 부호화 기법이라 할 수 있다.

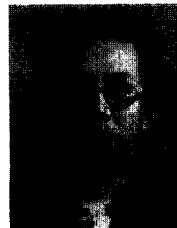
5. 결 론

RCNC 부호는 FEC 방식에 추가적으로 비화성을 얻을 수 있게 한 부호화의 한 방법이다. 소규모의 네트워크 시스템에서 비화성이 요구되는 경우 RCNC 부호를 사용하게 된다면 2^{k-1} 명의 사용자가 서로 비화성을 얻을 수 있고 여기에 덧붙여 여러 검출 및 정정이 가능하다. 시뮬레이션 결과에서 알 수 있듯이 BER이 10^{-3} 이 요구되는 시스템에서 RCNC 부호와 콘볼루션 부호는 0.3dB의 SNR 차이를 보이고 있어 기존의 FEC 부호화 방식을 대체하기에 충분한 부호화 방식이다. 또한, 콘볼루션 부호의 경우 자체적으로 비인증 사용자의 접근을 막을 수는 없지만 RCNC 부호화는 부호화 과정에서 인증된 사용자에 대해 암호화 방식을 적용함으로써 비인증 사용자의 접근에 대해 3배 이상의 비화성을 가지고 있다. 결과적으로 RCNC 부호는 기존의 콘볼루션 부호와 동일한 성능을 가지며 추가적으로 비화성이라는 성질을 가지게 됨으로써 앞으로 많은 분야에서 응용이 가능하리라 예상된다. 그리고 지금까지 RCNC 부호화 방식의 출력 데이터에 대한 성질이 충분히 고찰되지 않았기 때문에 출력 데이터에 대한 특성 해석의 방향으로 지속적인 연구가 필요할 것이다.

참 고 문 헌

[1] Neeli R. Prasad, "GSM Evolution towards Third Generation UMTS/IMT2000," Proceedings, IEEE, ICPWC'99, pp.50-54, 1999.
 [2] Stephen B. Wicker, "Error Control Systems for Digital Communication and Storage," School of E-

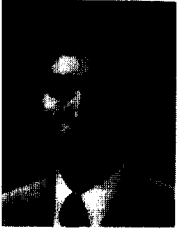
lectrical and Computer Engineering Georgia Institute of Technology, pp.264-355, 1995.
 [3] J. H. Yuen, et. al., Modulation and Coding for Satellite and Space Communications, Proceedings IEEE, Vol.78, No.7, pp.1250-1265, July 1990.
 [4] Floyd M. Fardner, John D. Baker, "Models of Communication Signals and Process," JOHN WILEY & SONS, Inc, pp.261-273.
 [5] C. E. Shannon, "A Mathematical Theory of Communication," Bell System Technical Journal, Vol. 27, pp.379-428, July. 1948.
 [6] G. Robert Redinbo, "Decoding Real-Number Convolutional Codes : Change Detection, Kalman Estimation," IEEE Trans. On Information Theory, Vol.43, No.6, pp.1864-1876, November 1997.
 [7] P. Robertson E. Vilebrun, and P. Hoher, "A Comparison of optimal and sub-optimal MAP decoding algorithm operating in the log domain," ICC pp.1009-1013, IEEE, 1995.
 [8] Rodney F. W. Coates, Gareth J. Janacek, "Monte Carlo Simulation and Random Number Generation," IEEE Journal on Selected Areas in Communications, Vol.6, No.1, pp.58-66, January, 1988.



공 형 운

e-mail : hkong@uou.ulsan.ac.kr
 1989년 미국 New York Institute of Technology 졸업(학사)
 1991년 미국 New York Polytechnic University 졸업(공학 석사)

1996년 미국 New York Polytechnic University 졸업 (공학박사)
 1996년~1996년 LG 전자 PCS 팀장
 1996년~1998년 LG 그룹 회장실 전략사업단
 1998년~현재 울산대학교 조교수
 관심분야 : 무선통신시스템(IMT-2000/LMDS/위성통신), 무선통신전송기술(Channel Coding, Multi-Carrier/Multi-Code, Equalizer...)



조 상 복

e-mail : sbcho@uou.ulsan.ac.kr

1979년 한양대학교 전자공학과
졸업(학사)

1981년 한양대학교 전자공학과
졸업(공학석사)

1985년 한양대학교 대학원 전자
공학과 졸업(공학박사)

1994년~1995년 University of Texas, Austin, Visiting
Scholar

1998년~2000년 울산대학교 전기, 전자 및 자동화
공학부 학부장

1986년~현재 울산대학교 전기, 전자 및 자동화 공학
부교수

관심분야 : 무선통신시스템(B-WLL), 프로세서 및 시스
템 설계 고집적회로/고집적 메모리 설계 및
테스트



이 창 희

e-mail : lee_chee@hanmail.net

1999년 울산대학교 전자공학과
졸업 (학사)

2001년 울산대학교 전기전자 및
자동화공학부 졸업(공학
석사)

관심분야 : 무선통신시스템, 전송기술(Channel Coding...)