주파수 도약 대역확산 다중접속 채널에서 내 부호 복호화 기법에 따른 쇄상부호의 성능 비교

이예훈* 정회원

Performance Comparison of Concatenated Codes with Different Inner Decoding Schemes in Frequency-Hopping Spread Spectrum Multiple-Access Channels

Ye Hoon Lee* *Regular Members*

요 약

본 논문에서는 내 부호의 복호화 방식에 따른 쇄상부호 시스템의 성능 변화를 분석한다. 내 부호의 복화화 방식으로는 오류 검출 방식과 오류 검출 및 정정 방식의 두 가지를 고려한다. 주파수 도약 대역확산 다중접속 통신시스템에 쇄상부호가 적용되었을 때 두 복호화 방식에 따른 성능을 비교하는데, 외 부호의 블록 길이가 유한한 경우와 무한한 경우에 그 성능을 분석하고 비교한다. 분석된 결과를 바탕으로 무한의 블록 길이의 경우에는 두 방식의 성능이 다중 접속자 수에 따라서 trade-off가 있음을 알 수 있고, 유한한 블록 길이의 경우에는 오류 검출 및 정정 방식의 성능이 더 우수함을 관찰하였다.

Key Words : Concatenated code; inner code; decoding scheme; frequency hopping; multiple access channel.

ABSTRACT

In this paper, we analyze the performance of a concatenated code with two different inner decoding schemes. One is the error-detecting inner decoding, and the other is the error-detecting-and-correcting inner decoding scheme. We compare the performances of the two decoding schemes for finite and infinite block length cases when the concatenated code is applied to slow frequency-hopping spread-spectrum multiple access (FH-SSMA) communication systems.

I. 서 론

쇄상부호(concatenated code)는 내 부호(inner code)와 외 부호(outer cde)의 결합에 의한 오류 정정 부호(eror cntrol cding)의 일종으로서 블록 길이를 증가시킴에 따라 지수적으로 감소하는 오류 확률을 가지면서 다항 시간(plynomial tme) 복호 복잡도를 만족하는 부호화 방식 중 하나이다[1]. 이러한 쇄상부호는 과거 1970년대 우주 통신부터 사용이 되기 시작하여 최근에는 디지털 TV 방송을 위한 오류 정정 부호 방식으로 채택이 되었다[2]. 쇄상부호 방식에서 가장 일반적으로 많이 사용되는 외 부호는 리드-솔로몬(Reed-Solomon) 부호인데, 그 이유는 리드-솔로몬 부호가 최대 거리 부호로서 redundancy를 효율적으로 잘 사용할 수 있고 연집 오류를 정정할 수 있는 능력이 있기 때문이다[3]. 본 논문에서도 외 부호로 리드-솔로몬 부호를 사용하기로 한다.

또한 본 논문에서는 내 부호로서 오류 검출 및 정정 능력이 있는 이진 블록 부호를 고려한다. 내 부호는 e_c개의 오류를 정정할 수 있고 e_d개의 오류를 검출할 수 있다고 가정한다. 단, 내 부호의 최소 거리(minimum distance)를 d_{mim}이라 할 때 $e_c+e_d < d_{mim}$을 만족하여야 한다. 오류가 검출될 경우, 모든 내 부호 심볼은 소거(erased)된다. 그러나, 내 부호에 의해서 오류가 검출되지 않거나 또는 정정되지 않는 경우는 내 부호의 복호화기 출력에 오류가 발생하게 되는데 외 부호는 이러한 내 부호에 의해 발생하는 소거 혹은 오류 심볼들을 정정하게 된다.

본 논문에서는 두 가지의 복호화 방식이 내 부호에 적용되었을 때 쇄상부호 시스템의 성능을 분석, 비교한다. 내 부호의 복호화 방식의 하나는 오류 검출 방식이며 또 다른 하

※ 이 연구는 서울과학기술대학교 교내 학술연구비 (일부)지원으로 수행되었습니다.
*서울과학기술대학교 전자IT미디어공학과 (y.lee@snut.ac.kr)
접수일자 : 2014년 5월 28일, 수정완료일자 : 2014년 6월 9일, 최종게재확정일자 : 2014년 6월 11일

나는 오류 검출 및 정정 방식이다. 오류 검출 방식에서는 내 부호가 단지 오류를 검출할 뿐이며 정정하지는 않는다. 내 부호에 의해서 검출된 오류는 소거되어 외 부호에 의해서 정정 될 수 있다. 오류 검출 및 정정 방식에서는 내 부호에 의해서 검출된 오류가 소거되기도 하고 또 내 부호에 의해서 정정되기도 한다. 전체 쇄상 부호의 부호율은 고정되어 있으므로 채널의 상태에 따라서 내 부호의 두 복호화 방식의 성능은 trade-off가 생길텐데, 본 논문에서는 이러한 쇄상부호가 주파수 도약 대역확산 다중접속 통신에 적용되었을 때 그 성능을 비교하기로 한다.

본 논문의 구성은 다음과 같다. 우선 Ⅱ절에서는 시스템과 채널 모델에 관하여 소개한다. Ⅲ절에서는 내 부호의 두 복화화 방식중에서 오류 검출 방식을 설명하고, Ⅳ절에서 오류 검출 및 정정 방식에 관하여 서술한다. Ⅴ절에서는 두 방식의 성능을 비교한 수치적 결과를 제시하고 분석하며, 마지막으로 Ⅵ절에서는 본 논문을 정리하고 마무리함으로써 끝맺는다.

Ⅱ. 시스템 및 채널 모델

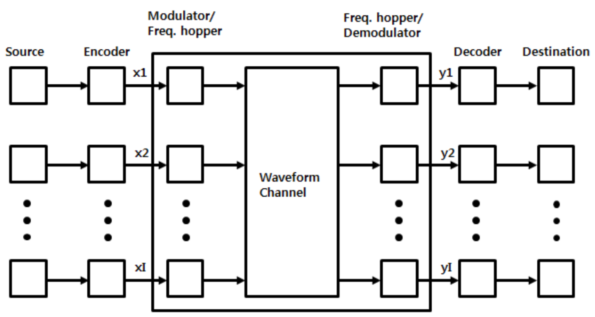


그림 1. I 명의 동시 사용자를 가진 주파수 도약 대역확산 다중 접속 채널 모델

본 논문에서는 그림 1에서 보는 바와 같이 I 명의 사용자가 동시에 동일한 채널을 통하여 주파수 도약 대역확산 다중접속 방식을 통하여 정보를 전송하는 시스템을 고려한다. 각 사용자의 소스는 전송하고자 하는 메시지를 발생시키는데, 각각 사용자들에 대하여 독립적이다. 전체적으로 I 개의 분리되어 있는 부호화기가 존재하며, j번째 부호화기는 j번째 소스로부터 메시지를 정보를 받아서 부호화된 코드워드 $(X_{j1}, X_{j2}, \cdots, X_{jn})$, $X_{ji} \in X$ 를 발생시키며, 여기서 X 는 입력 알파벳 집합이다. j번째 주파수 도약 패턴을 알고 있는 j번째 수신기에서는 주파수 도약된 신호를 수신하게 된다. 이 신호는 복조기를 거쳐서 벡터 $(Y_{j1}, Y_{j2}, \cdots, Y_{jn})$, $Y_{ji} \in Y$ 를 출력하게 되는데, 여기서 Y 는 출력 알파벳 집합이다. 복호화는 각 I 수신기에서 독립적으로 행해지므로 결국 전송 측과 수신 측은 어떠한 협력도 없게 된다. 그러면, 각 개별 채널은 채널에서의 천이 확률 $P(y_i|x_j)$, $i, j \in \{1,2,\cdots,\mathrm{I}-1\}$ 에 의해서 특징 지워지는데, 이 천이 확률은 모든 사용자에게 동일하게 된다.

내 부호화에 의해서 오류가 검출될 때, 내 부호화기에 의해서 형성되는 수퍼 채널(super channel)은 그림 2와 같은 M진 소거 및 오류 채널(M-ary erasures and errors channel)로 모델링 할 수 있다. 외 부호의 목적은 내 부호에 의한 소거 심볼 및 오류 심볼을 정정하는 것이다. 최소 거리 성질(minimum distance property)로 부터 (n,k) 리드-솔로몬 부호는 $e=n-k$ 개의 소거 심볼 혹은 그 절반인 $t=(n-k)/2$ 개의 오류 심볼을 정정할 수 있다[3]. 일반적으로 말하면 (n,k) 리드-솔로몬 부호는 $2t+e$ 의 값이 $n-k$를 넘지 않는 범위 내에서 e개의 소거 심볼과 t개의 오류 심볼의 어떠한 조합도 정정할 수 있는 것이다. 그러므로 외 부호 코드워드의 블록 오류 확률 P_E는 다음과 같이 주어진다.

$$P_E = \sum_{2t+e>n-k} \binom{n}{t,e} P_d^e P_{ud}^t (1-P_d-P_{ud})^{n-t-e} \tag{1}$$

(1)에서

$$\binom{n}{t,e} = \frac{n!}{t!e!(n-t-e)!} \tag{2}$$

이다.

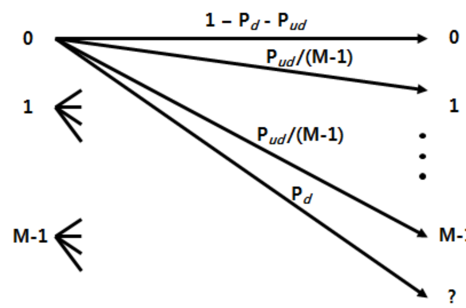


그림 2. M진 소거 및 오류 채널

본 논문에서는 모든 주파수 도약 송신기가 그들의 도약 시간을 동시에 조정하는 동기식(synchronous) 주파수 도약과 한 도약 홉 동안 하나의 내 부호 심볼이 전송되는 빠른(fast) 주파수 도약 방식을 고려한다. 그러므로, 한 홉 동안의 다중 사용자 간섭도 일정하게 유지된다. 또한 본 논문에서는 도약 홉핑 패턴이 랜덤하다고 가정하는데, 이는 한 홉 동안의 다중 사용자 간섭이 다른 홉 구간과 독립적으로 여겨질 수 있다.

I 명의 사용자가 각자의 패킷을 동시에 전송할 때 최대 $i+1$, $i \in \{0,1,\cdots,\mathrm{I}-1\}$ 명의 사용자가 동시에 특정 주파수를 같이 사용할 수 있다. 만약 특정 주파수 슬럿이 $i+1$ 명의 사용자에 의해서 공유되고 있다면 그 슬럿은 다음의 천이 확률을 p_i를 갖는 이진 대칭 채널(binary symmetric channel) Δ_i로 모델링 된다.

$$p_i = \frac{2^i - 1}{2^{i+1}} \tag{3}$$

이다. 반면에 채널 Δ_i가 선택될 확률, 즉 $i+1$ 명의 사용자가

동시에 같은 주파수 슬럿을 공유할 확률, $P_{h,I}(i)$, 은 다음과 같이 주어진다.

$$P_{h,I}(i) = \binom{I-1}{i}\left(\frac{1}{q}\right)^i\left(1-\frac{1}{q}\right)^{I-1-i},\ i \in \{0, 1, \cdots, \mathrm{I}-1\} \tag{4}$$

Ⅲ. 내 부호의 오류 검출 복호화 방식

내 부호가 오류 검출로만 사용되어 질 때, 채널에서의 오류 패턴이 제로가 아닌 코드워드와 동일할 경우에만 수신기에서 복호화 오류가 발생하게 된다[5]. 이진 대칭 채널의 경우 채널의 오류 패턴이 부호 길이 N을 가진 내 부호의 특정한 코드워드와 일치할 확률은 $p^i(1-p)^{N-i}$ 인데, 여기서 p는 채널의 천이 확률이다. 그래서, 미검출 오류 확률(undetected error probability) P_{ud}는 다음과 같이 주어진다.

$$P_{ud} = \sum_{i=1}^{N} A_i\, p^i (1-p)^{N-i} \tag{5}$$

(5)에서 A_i는 내 부호의 무게 분포(weight distribution)이다. 그러므로, 본 논문에서 고려하는 전체 주파수 도약 다중접속 채널 모델에서 채널 천이 확률은 다음과 같이 주어진다.

$$p = \sum_{i=0}^{I-1} p_i P_{h,I}(i) = \sum_{i=0}^{I-1}\binom{I-1}{i}\left(\frac{2^i-1}{2^{i+1}}\right)\left(\frac{1}{q}\right)^i\left(1-\frac{1}{q}\right)^{I-1-i} \tag{6}$$

내 부호 심볼에 오류가 발생하지 않을 확률, 즉 오류 미발생 확률(corrected error probability)은 다음과 같다.

$$P_c = (1-p)^N \tag{7}$$

그러므로, 오류 검출 확률(probability of detected error)는 다음과 같이 주어진다.

$$P_d = 1 - P_{ud} - P_c \tag{8}$$

Ⅳ. 내 부호의 오류 검출 및 정정 복호화 방식

이번 절에서는 e_c개의 오류를 정정할 수 있고, 동시에 e_d개의 오류를 검출할 수 있는 내 부호의 복호화 방식을 고려한다. 이때 내 부호의 최소 거리(minimum distance)를 d_{mim}이라 할 때, $2e_c + e_d < d_{mim}$ 을 만족하여야 한다. 내 부호의 코드워드가 바르게 복호될 확률은 다음과 같다.

$$P_c = \sum_{j=0}^{e_c} p^j (1-p)^{N-j} \tag{9}$$

이때, 미검출 오류 확률 P_{ud}는 다음과 같이 근사화 될 수 있다.

$$P_{ud} \approx \sum_{i=e_d+1}^{N}\binom{N}{i} p^i (1-p)^{N-i}\left(\frac{2^K-1}{2^N}\right)\sum_{j=0}^{e_c}\binom{N}{j}. \tag{10}$$

그러므로 오류 패턴이 검출될 확률은 식 (8)과 동일하게 된다.

Ⅴ. 실험 결과 및 토의

극한에서 외 부호의 부호율 $r = k/n$ 은 고정된 채로 n과 k값이 무한대로 접근할 때, *중심 극한 정리* (central limit theorem)로부터[6] 아래의 사실을 증명할 수 있다.

$$\lim_{n,k\to\infty} P_E = \begin{cases} 0, & r < 1 - P_d - 2P_{ud} \\ 1/2, & r = 1 - P_d - 2P_{ud} \\ 1, & r > 1 - P_d - 2P_{ud} \end{cases} \tag{11}$$

다시 말해서, 점근적으로(asymptotically) 만약 내 부호의 부호율이 $r < 1 - P_d - 2P_{ud}$ 를 만족한다면 오류 없는 통신이 가능하다는 것이다. 그렇다면 $1 - P_d - 2P_{ud}$ 의 값이 가능한 최대화 되어야만 하겠다. 이것은 곧 점근적 관점에서 $P_d + 2P_{ud}$ 의 값이 최소화 되는 내 부호를 선택하는 것이 바람직하다는 것을 의미한다.

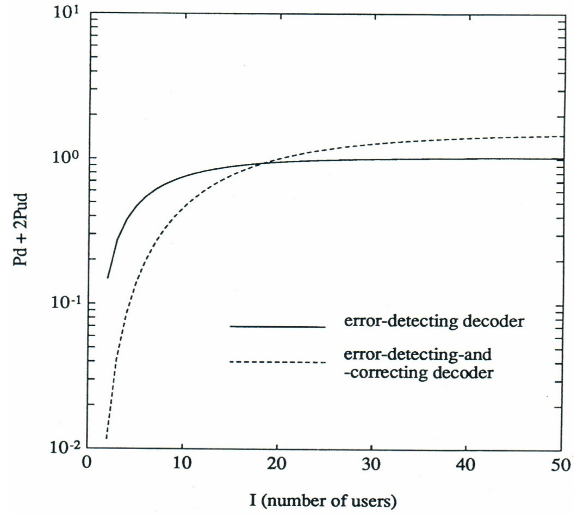


그림 3. 다중 사용자 수 I 에 따른 두 복호화 방식의 $P_d + 2P_{ud}$ 값의 비교
($n = 2048$, $N = 16$, $K = 11$, $q = 25$)

내 부호의 두 가지 복호화 방식에 따른 성능을 비교하기 위하여 그림 3에서는 다중 사용자 수 I 에 변화에 따른 $P_d + 2P_{ud}$ 의 값을 도시하였다. 무한대의 블록 길이를 실험적으로 나타내기 위하여 n 의 값은 충분히 큰 2048로 정하였다. 내 부호로는 확장된(extended) Hamming 부호를 사용하여서 내 부호의 $d_{\min} = 4$ 를 사용하였다[7]. 그러므로, 오류 검출 복호화 방식으로 사용될 때는 $e_d = 3$ 을 충족하며, 오류 검출 및 정정 복호화 방식으로 사용될 때는 $e_c = 1, e_d = 2$ 를 만족하게 된다. 그림 3으로부터 두 복호화 방식의 성능이 전환되는 점이 존재하는 것을 알 수 있다. 다중접속 채널의 사용자 수가 적을 때에는 오류 검출 및 정정 복호화 방식이 오류 검출 복호화 방식에 비하여 성능이 더 좋으며, 채널의 사용자 수가 많아질수록 오류 검출 방식의 성능이 더 좋아짐을 관찰할 수 있다.

그림 4와 그림 5에서는 유한의 블록 길이에서 두 복호화 방식의 성능을 비교하기 위하여 최대 다중 사용자의 수 I 가 5와 25의 경우에 블록 오류 확률 P_E 대 k 의 값을 그린 것이다. 대부분의 영역에서 오류 검출 및 정정 복호화 방식이 오류 검출 복호화 방식에 비하여 성능이 우수함을 알 수 있다. 이것으로 미루어 유한한 블록 길이의 경우 내 부호를 오류 검출 및 정정 복호화 방식으로 사용하는 것이 전체 쇄상부호 시스템의 성능을 향상시키는 방법임을 알 수 있다.

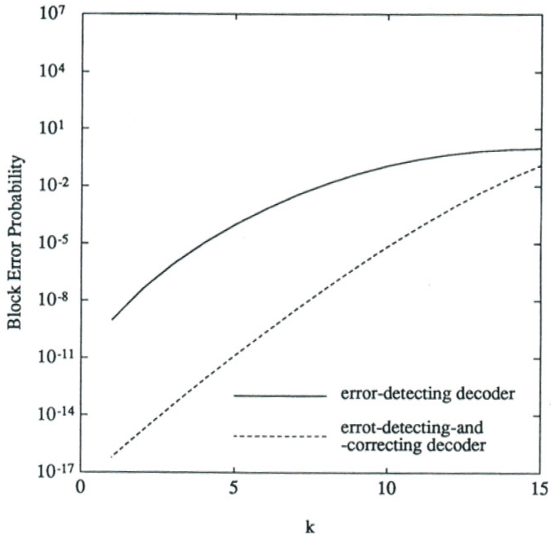


그림 4. k값의 변화에 따른 블록 오류 확률 P_E값의 비교
$(I=5,\ q=25,\ n=16,\ N=8,\ K=4)$

그림 4와 그림 5에서는 유한의 블록 길이에서 두 복호화 방식의 성능을 비교하기 위하여 최대 다중 사용자의 수 I 가 5와 25의 경우에 블록 오류 확률 P_E 대 k 의 값을 그린 것이다. 대부분의 영역에서 오류 검출 및 정정 복호화 방식이 오류 검출 복호화 방식에 비하여 성능이 우수함을 알 수 있다. 이것으로 미루어 유한한 블록 길이의 경우 내 부호를 오류 검출 및 정정 복호화 방식으로 사용하는 것이 전체 쇄상부호 시스템의 성능을 향상시키는 방법임을 알 수 있다.

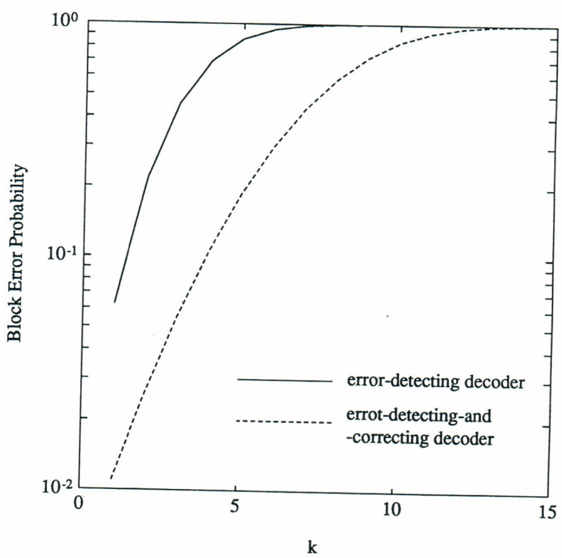


그림 5. k값의 변화에 따른 블록 오류 확률 P_E값의 비교
$(I=25,\ q=25,\ n=16,\ N=8,\ K=4)$

VI. 결 론

본 논문에서는 쇄상부호에서 내 부호의 두 가지 복호화 방식에 따른 성능 분석 및 비교를 행하였다. 하나는 내 부호에서 오류 검출만 하고 검출하여 소거된 심볼을 외 부호가 전적으로 정정하는 방식이며, 또 다른 하나는 내 부호에서 오류 검출 및 정정을 행하고 외 부호에서는 남아있는 오류만을 추가로 정정하는 방식이다. 본 연구에서 하나의 내 부호 심볼이 한 홉의 주파수 도약 대역확산 방식에 의해서 전송되는 빠른 홉핑을 고려하였다. 유한한 블록 길이의 경우 오류 검출 및 정정 방식이 오류 검출만 하는 방식에 비하여 성능이 우수함을 보였고, 무한의 블록 길이를 갖는 점근적 해석에서는 두 방식간의 trade-off가 있음을 분석하였다.

참 고 문 헌

[1] G. D. Forney, Concatenated Codes, MIT Press, Cambridge, MA, 1966.

[2] Z. Yang, M. Han, C. Pan, A. Men, and L. Yang, “A novel scheme of coding and modulation for digital television terrestrial broadcasting,”Proc. of IEEE PIMRC, pp. 376-379, 2003.

[3] T. Blahut, Theory and Practice of Error Control Codes, Addison Wesley Pub. Co, 1983.

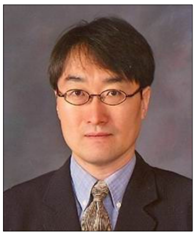
[4] H. Sato, Two-user communication channels,” IEEE Trans. on Inform. Theory, vol. 23, pp. 295-304, May 1977.

[5] E. R. Berlekamp, Algebraic Coding Theory, Aegean Park

Press, 1984.
[6] A. Papoulis, Probability, Ramdom Variables, and Stochastic Processes, McGrawHill Inc, Kogakusha, Ltd., 1965.
[7] J. H. Wolf, et. All, On the probability of undetected error for linear block codes," IEEE trans. on Communications, vol. 30, pp. 317-324, Feb. 1982.

저자

이 예 훈 (Ye Hoon Lee) **정회원**



· 1990년 2월 : KAIST 전기 및 전자공학과 학사졸업
· 1992년 2월 : KAIST 전기 및 전자공학과 공학석사
· 2000년 2월 : KAIST 전기 및 전자공학과 공학박사
· 2000년~2001년 : LG전자 차세대 단말연구소 선임연구원
· 2001~2003년 : Research Associate, New Jersey Institute of Technology, U.S.A.
· 2003~2005년 : 삼성종합기술원 i-Networking Lab, 전문연구원
· 2005년~현재 : 서울과학기술대학교 전자IT미디어공학 부교수
<관심분야> : 통신이론, 이동통신, 위성통신 등