논문 20-45-03-11 The Journal of Korean Institute of Communications and Information Sciences '20-03 Vol.45 No.03
https://doi.org/10.7840/kics.2020.45.3.537

터보 부호기의 RSC 파라미터 추정을 위한 전역 탐색 기법

고 선 재◆, 김 재 윤*, 김 선 교**, 최 병 조°

Parameter Estimation of RSC Turbo Codes with Full Search

Seon-Jae Ko◆, Jae-Yun Kim*, Seon-Kyo Kim**, Byoung-Jo Choi°

요 약

본 논문에서는 터보 부호화된 수신 신호로부터 송신기로부터 전송된 부가 정보 없이 터보 부호화에 사용된 RSC 파라미터를 추정하기 위한 전역 탐색 기법을 제안한다. 상용 시스템에 표준으로 채택된 터보 부호화기에 사용된 RSC의 구속장 길이가 컨볼루션 부호화기의 구속장과 비교하여 짧기 때문에 제안하는 전역 탐색 기법의 복잡도는 기존의 반복 최적화 기법과 비교하여 크게 증가하지 않는다. 또한 탐색 복잡도를 낮추기 위해 탐색 범위를 좁히기 위한 방안도 제시한다. 3GPP UMTS 터보 부화기 추정을 위한 모의 실험 결과 제안하는 방법은 기존의 추정 기법과 비교하여 AWGN 채널 환경에서 약 2.5dB의 SNR 이득을 나타내었다. 또한 채널 SNR이 0dB였을 때 기존 기법의 추정 오류 확률은 65%였지만, 제안하는 기법의 추정 오류 확률은 0.6%였다. 제안하는 기법의 계산 복잡도는 기존의 반복 최적화 기법과 비교하여 약 70% 정도였다.

키워드 : 터보 부호, RSC, 블라인드 파라미터추정, 전역 탐색, 탐색 영역 축소
Key Words : Turbo Code, RSC, Blind Parameter Estimation, Full search, search space reduction

ABSTRACT

A full search scheme for the blind RSC parameter estimation of a turbo encoder is proposed and its performance is explored by simulations over the AWGN channels. The constraint length of RSC encoder dictates the search space and, hence, the complexity of the full search scheme. Most commercial standards have turbo encoders with RSC sub-encoders with relatively short constraint length in comparison to non-systematic convolutional codes and the full search is a practical solution. It is shown that the search space can be further reduced using some properties of legitimate RSC encoders. Our simulation results for 3GPP UMTS scenario showed that the proposed full search scheme has about 2.5dB SNR gain over the wide range of SNR values when operating over AWGN channel, in comparison to the best scheme reported in the literature previously. In terms of the detection error rate, the previous scheme resulted in 65% at the channel SNR of 0dB, while the proposed scheme results in 0.6%. The corresponding complexity of our scheme was about 70% when compared to that of the previous scheme.

※ 본 연구는 국방과학연구소 광대역 저피탐 DSSS 신호 탐지 및 분석 시험장치대 과제 지원으로 수행되었습니다.
◆ First Author : Incheon National Univeristy, Department of Embedded Systems, dlem1277@inu.ac.kr, 학생회원
° Corresponding Author : Incheon National Univeristy, Department of Embedded Systems, bjc97r@inu.ac.kr, 종신회원
* LIGNex1, jykim0118@lignex1.com, 정회원
** Agency for Defense Development, seonkyo.kim@gmail.com, 정회원
논문번호 : 201912-328-0-SE, Received November 4, 2019; Revised January 31, 2020; Accepted January 31, 2020

Ⅰ. 서 론

디지털 통신 시스템은 채널 부호화 기법의 도움을 통해 오류 없이 정보를 전송할 수 있는 장점이 있다. 지금까지 디지털 전송 오류를 복구하기 위한 다양한 채널 부호화 기법이 제시되어왔다. 또한, 채널 부호화된 비트를 변조하기 위한 기법도 여러 종류가 있다. 이러한 다양한 기법과 구체적인 설정 파라미터는 송신기와 수신기 사이에 통신 규약을 통해 서로 약속이 되어 있거나, 가변적인 설정 파라미터의 경우에는 부가 정보를 전송하여 수신기에 구체적인 값을 알려주게 된다. 이러한 부가 정보를 전송하기 위해 일반적으로 추가적인 통신 자원을 사용하게 된다.

채널 부호화 기법 등 송신기에 사용된 구체적인 설정 파라미터를 송신기에서 전송하지 않거나, 비협력적 통신 환경과 같이 설정값을 수신하기 어려운 경우에는 이 설정 파라미터 값을 추정하여야 한다[1]. 이렇게 통신과 관련된 사전 정보 없이 설정 파라미터를 추정하여 데이터를 복호하는 수신기를 보통 블라인드 검출기(blind detector) 또는 블라인드 수신기라고 부른다.

터보 부호는 UMTS, LTE 등의 통신 표준에 널리 사용되는 채널 부호들 가운데 하나이다[2]. 부호율이 1/3인 터보 부호화기의 간략한 구조를 Fig. 1에 나타내었다. 이러한 터보 부호화기의 파라미터로는 인터리버(ILV)의 길이 N 및 구조, RSC (Recursive Systematic Convolutional) 부 부호화기(sub-encoder)의 구속장의 길이 K 및 생성 다항식 G가 있다. 이 가운데 인터리버의 길이 N을 제외한 K와 G는 보통 해당 통신 표준으로 정해져 있다. 그러나 비표준 통신 기법을 사용하는 경우나 어떠한 표준을 사용하는지 미리 알 수 없는 경우에는 구속장의 길이 K와 생성 다항식 G를 추정해야한다. 본 논문은 이 가운데 생성 다항식 G를 추정하는 기법에 관한 것이다.

일반적인 컨볼루션 부호화기 (Non-Systematic Convolutional code, NSC)의 파라미터 추정에 관한 연구는 1955년부터 문헌에 보고되어 왔다[1, 3]. Brushe는 컨볼루션 부호화기의 출력 비트로 구성된 한켈(Hankel) 행렬의 랭크(rank) 특징을 이용하여 구속장의 길이 K를 추정하고, 이 행렬의 널 벡터로부터 생성 다항식 G를 추정하는 기법을 제안하였다[3]. Filiol도 K와 G를 추정하기 위해 랭크 특징과 연립방정식의 해를 구하는 방법[4]을 적용하였다. 그러나 이 기법들은 수신 비트의 오류가 없는 경우에만 적용할 수 있다. AWGN 채널에서 얻어진 수신 심볼로부터 컨볼루션 부호화기의 파라미터를 추정하는 문제는 Dingel 등이 기댓값 최대화(Expectation Maximization; EM) 기법을 통해 해결책을 제시하기 시작했다[5].

한편 터보 부호화기를 구성하는 RSC의 파라미터 추정에 관한 문제는 2005년 Babier가 해결 방법을 제안하기 시작했다[6]. Barbier는 비트 오류가 없는 경우에 $1/n$의 부호율을 갖는 RSC의 생성 다항식 G는 Berlekamp-Massey 알고리즘을 이용하여 궤환 다항식(feedback polynomial)을 추정한 후 다항식 사이의 특징을 이용하여 나머지 다항식을 구하는 방법을 제안하였다. AWGN 채널을 통해 얻는 수신 심볼로부터 터보 부호화기의 파라미터를 추정하는 문제는 Debessu 등이 기댓값 최대화 기법을 적용하면서 활발하게 연구되기 시작했다[7]. 그러나 이 기법은 95%의 검출 확률을 얻기 위해 요구되는 채널 SNR이 12dB 정도였다. 그 후 RSC의 생성 다항식 G의 검출 확률을 향상 시키기 위해 목적 함수를 제시하고 최적화 방법을 적용하는 연구가 진행되어 왔다[8,9].

본 논문은 참고문헌 [8] 및 [9]에 적용된 목적 함수를 이용하여 전역 탐색을 통해 RSC 생성 다항식 G를 검출하는 기법을 제안하고, 탐색 영역을 좁히기 위한 방안을 제시하며, 시뮬레이션을 통해 제안하는 기법의 검출 성능을 고찰한다.

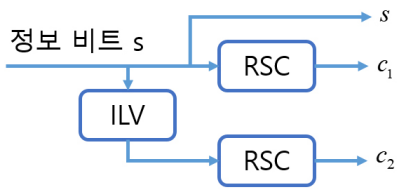

그림 1. 부호율이 1/3인 터보 부호화기 구조
Fig. 1. 1/3-rate turbo encoder

Ⅱ. 전역 탐색 기법

2.1 RSC 부호화기 모델

본 논문에서 고려하는 터보 부호화기는 그림 1에 나타낸 것과 같이 3GPP UMTS 및 LTE 등에 적용된 PCCC(Parallel Concatenated Convolutional Code) 구조를 가정한다. 이러한 터보 부호화기를 구성하는 RSC 컨볼루션 부호화기의 구조를 그림 2에 나타내었다. 이 구조는 부호율이 $1/2$이고 구속장의 길이가 $K=4$인 경우를 가정한 것이다.

구속장의 길이가 K인 RSC 부호화기는 $m=K-1$개의 지연 소자를 이용하여 구현할 수 있다. 이 부호

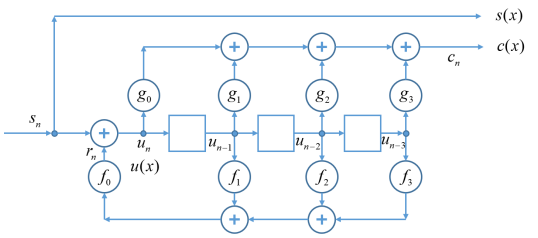

그림 2. 부호율이 1/2이고 구속장이 4인 RSC 부호화기
Fig. 2. A stylized diagram of a 1/2-rate RSC encoder with the constraint length of K=4

화기의 n-번째 패리티 출력 c_n은 다음과 같이 나타낼 수 있다.

$$c_n = g_0 u_n + g_1 u_{n-1} + \cdots + g_{n-m} u_{n-m} = \sum_{i=0}^{m} g_i u_{n-i} \quad (1)$$

식 (1)에서 g_i는 0 또는 1의 값을 갖는 연결 계수이며, u_{n-i}는 i-번째 지연 소자의 값을 나타낸다. 부호화기의 출력 비트열 $\{c_n\}$은 일반적으로 다음과 같이 다항식으로 표현할 수 있다[10].

$$c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n + \cdots \quad (2)$$

그림 2에서 관찰할 수 있는 것과 같이 c_n은 m개의 시프트 레지스터(shift register)에 u_n이 입력될 때의 출력에 해당하기 때문에 GF(2)에서 다음과 같이 다항식의 곱셈으로 표현할 수 있다[10].

$$c(x) = g(x)\,u(x) \quad (3)$$

여기서 $g(x) = g_0 + g_1 x + \ldots + g_m x^m$는 패리티 생성 다항식이다. 같은 방법을 사용하면 $u(x)$는 궤환 연결 계수로 구성된 다항식인 $f(x)$를 이용하여 다음과 같이 GF(2)에서의 나눗셈으로 나타낼 수 있다.

$$u(x) = \frac{s(x)}{f(x)} \quad (4)$$

위 식 (3)과 (4)로부터 다음과 같은 관계식을 얻을 수 있다[6].

$$c(x) = g(x)\frac{s(x)}{f(x)} \leftrightarrow s(x)g(x) + c(x)f(x) = 0 \quad (5)$$

위 식 (5)의 오른쪽 관계식의 항들을 다음과 같이 정의하기로 한다.

$$h(x) = s(x)g(x) = \sum_{n=0} h_n x^n \quad (6)$$

$$v(x) = c(x)f(x) = \sum_{n=0} v_n x^n \quad (7)$$

위 식 (6)과 (7)에서 다항식 계수는 각각 $h_n = \sum_{i=0}^{m} s_{n-i} g_i$, $v_n = \sum_{i=0}^{m} c_{n-i} f_i$ 로 주어진다. 여기서 $s_k = 0, \forall k < 0$및 $c_k = 0, \forall k < 0$를 가정한다. 따라서 식 (5)의 오른쪽 관계식은 다음과 같이 F_n으로 정의하고 나타낼 수 있다.

$$F_n := h_n + v_n = \sum_{i=0}^{m} s_{n-i} g_i + \sum_{i=0}^{m} c_{n-i} f_i = 0 \quad (8)$$

이제 RSC 파라미터 추정은 $s(x)$와 $c(x)$에 해당하는 수신 심볼들로부터 식 (5) 및 (8)의 관계를 이용하여 $f(x)$와 $g(x)$를 찾아내는 문제로 정의할 수 있다.

2.2 무오류 채널에서의 RSC 파라미터 추정

위 식(5)의 왼쪽 식은 다음과 같이 나타낼 수 있다.

$$\frac{c(x)}{s(x)} = a(x) = \frac{g(x)}{f(x)} \quad (9)$$

만약 관찰된 $s(x)$가 0이 아니어서 나눗셈을 통해 $a(x) = c(x)/s(x)$를 구할 수 있다면, 식 (6)은 m-개의 시프트 레지스터로 구성된 LFSR (Linear Feedback Shift Register)의 초기값이 $g(x)$이고 궤환 연결 벡터로 구성된 다항식이 $f(x)$일 때의 출력을 나타내는 식에 해당한다[10, 11]. 어떤 LFSR의 출력 비트열을 $a(x)$로 나타냈을 때, 이 비트열을 생성하기 위한 최소개의 시프트 레지스터로 구성된 LFSR을 찾는 문제는 1969년에 Massey[11]가 Berlekamp의 알고리즘을 소개하며 그 해를 제시하였다. 이 기법은 Berlekamp-Massey (BM) 알고리즘으로 알려져 있으며 BCH 복호기에 활용되고 있다. Barbier[6]는 무오류 채널을 가정하고 BM 알고리즘을 이용하여 RSC 파라미터를 추정할 것을 제안했다.

2.3 AWGN 채널에서의 목적 함수

송신기는 0과 1로 표현되는 정보비트 s_n과 패리티 비트 c_n을 변조하여 AWGN 채널을 통해 전송한다. 본 논문에서는 BPSK 변조를 적용하여 0과 1이 각각 +1 및 -1로 매핑된다고 가정한다. 수신된 심볼들은 각각 $r_n^{(s)}=(-1)^{s_n}+\eta_n^{(s)}$ 및 $r_n^{(c)}=(-1)^{c_n}+\eta_n^{(c)}$로 나타낼 수 있으며 $\eta_n^{(*)}$은 평균이 0이고 분산이 σ^2인 가우시안 분포를 따른다고 가정한다. 따라서 수신 심볼의 확률 밀도 함수는 다음과 같다.

$$f_R(r)=\frac{1}{\sqrt{2\pi\sigma^2}}exp\left(-\frac{(r-(-1)^b)^2}{2\sigma^2}\right) \quad (10)$$

여기서 r은 수신 심볼 $r_n^{(s)}$이나 $r_n^{(c)}$를 나타내며, 2진 비트 b는 s_n, 또는 c_n을 나타낸다.

AWGN 채널을 통해 N 쌍의 심볼 $(r_n^{(s)}, r_n^{(c)})$을 수신하였을 때 전역 탐색을 통해 터보 부호의 RSC 파라미터를 추정하는 문제는 다음과 같이 정의할 수 있다[8,9].

$$\langle \hat{\boldsymbol{f}}, \hat{\boldsymbol{g}} \rangle = \arg\max_{\langle \boldsymbol{f},\boldsymbol{g} \rangle} P(F_n=0 \,\forall\, n | \langle \boldsymbol{f},\boldsymbol{g} \rangle) \quad (11)$$

식 (11)에서 $K\times 1$ 이진 벡터 $\boldsymbol{f}$와 $\boldsymbol{g}$는 RSC 생성 다항식의 후보에 해당한다. 따라서 식 (11)은 모든 가능한 $\boldsymbol{f}$와 $\boldsymbol{g}$의 조합에 대하여 $F_n=0$, $n=0,\ldots,N-1$을 만족할 확률이 가장 높은 조합을 찾는 문제에 해당한다.

한편 식 (8)에서 F_n은 GF(2)에서 $a+b$형태로 표현되어 있다. $P(a+b=1)$일 확률은 a와 b가운데 어느 하나만 1이어야 하므로, 이진 랜덤 변수 a와 b가 서로 독립이라고 가정하면 다음과 같이 나타낼 수 있다. 간략한 표현을 위해 $P_x=P(x=1)$의 의미로 나타내기로 한다.

$$P_{a+b}=(1-P_a)P_b+P_a(1-P_b) \quad (12)$$

이 관계식을 이용하면 다음과 같은 재귀적 확률 계산식을 유도할 수 있다[8,9,13].

$$\begin{aligned} 1-2P_{a+b} &= 1-2\times\{(1-P_a)P_b+P_a(1-P_b)\} \\ &= 1-2\times(P_a+P_b)+4P_aP_b \\ &= (1-2P_a)(1-2P_b) \end{aligned} \quad (13)$$

식 (13)을 이용하면 식 (8)에서 $F_n=0$일 확률을 직접 계산하는 것보다 $F_n=1$일 확률을 대상으로 다음과 같이 계산할 수 있다.

$$1-2P(F_n=1)=\{1-2P(h_n=1)\}\{1-2P(v_n=1)\} \quad (14)$$

식 (8)의 모든 항들에 대해 XOR 연산이 적용되어 있으므로 식 (14)에 식 (13)의 결과를 연속적으로 적용하면 다음과 같은 식으로 표현할 수 있다.

$$1-2P(F_n=1)=\prod_{i=0}^{m}\{1-2P_{s_{n-i}}g_i\}\prod_{i=0}^{m}\{1-2P_{c_{n-i}}f_i\} \quad (15)$$

식 (15)에서 P_{s_n}은 확률 $P(s_n=1)$을 나타낸다. 이 식을 AWGN 채널을 통해 수신된 심볼들에 적용하기 위해 식 (15)의 s_n과 c_n대신에 수신 심볼값으로부터 얻어진 사후 확률(A Posterior Probability, APP)을 사용한다. 예를 들어 수신기에서 $r_n^{(s)}$ 심볼 값을 수신하였을 때 송신기에서 $s_n=1$을 보냈을 확률은 사후 확률의 정의와 식 (10)을 이용하여 다음과 같이 나타낼 수 있다.

$$\begin{aligned} P(s_n=1|r_n^{(s)}) &= \frac{P(r_n^{(s)}|s_n=1)}{P(r_n^{(s)})}P(s_n=1) \\ &= \frac{f_R(r_n^{(s)}|s_n=1)}{f_R(r_n^{(s)}|s_n=1)+f_R(r_n^{(s)}|s_n=0)} \\ &= \frac{1}{1+e^{2r_n^{(s)}/\sigma^2}} \end{aligned} \quad 16$$

위 식의 전개 과정에서 r은 $r_n^{(s)}$을, $b=s_n$을 나타낸다. 식 (16)을 이용해 얻어지는 사후 확률을 각각 다음과 같이 나타내기로 한다.

$$P_n^{(s)}=\Pr[s_n=1|r_n^{(s)}],\ P_n^{(c)}=\Pr[c_n=1|r_n^{(c)}] \quad (17)$$

이제 식 (17)을 이용하여 식 (15)를 다음과 같이 목적 함수(objective function) 또는 비용함수 (cost function)를 나타내는 C_n으로 표현할 수 있다.

$$C_n=\prod_{i=0}^{m}\{1-2P_{n-i}^{(s)}g_i\}\prod_{i=0}^{m}\{1-2P_{n-i}^{(c)}f_i\} \quad (18)$$

식 (11)과 식 (15) 및 (18)로부터 다음 관계를 확인할 수 있다.

$$P(F_n = 0\ \forall n|\langle \boldsymbol{f},\boldsymbol{g}\rangle) \leftrightarrow P(C_n = 1\ \forall n|\langle \boldsymbol{f},\boldsymbol{g}\rangle) \tag{19}$$

따라서 전역 탐색을 통해 터보 부호의 RSC 파라미터를 추정하는 문제는 식 (19)의 오른쪽 확률을 최대화하는 $\langle \boldsymbol{f},\boldsymbol{g}\rangle$ 쌍을 찾는 문제가 된다.

2.4 탐색 영역 축소 기법

추정하여야 하는 터보 부호의 RSC에 적용된 구속장의 길이 K의 최대값을 $K_{\max}$라고 가정하자. RSC의 생성 다항식 $f(x)$와 $g(x)$ 의 계수는 각각 $K_{\max}$개이고, 각각의 계수는 0 또는 1의 값을 갖을 수 있으므로 $\langle \boldsymbol{f},\boldsymbol{g}\rangle$ 쌍의 탐색 영역은 $2^{2K_{\max}}$가 된다. 예를 들어 3GPP 터보 부호의 경우 구속장은 $K=4$이므로 $K_{\max}$를 4로 가정하더라도 탐색 영역은 256개가 된다. 이러한 넓은 탐색 영역에 대하여 식 (11) 및 식 (18)와 식 (19)를 계산하는 복잡도 때문에 참고문헌 [8]과 [9]는 각각 연속적 단일차원 탐색(iterative univariate search) 방법 및 연속적 기울기 상승(iterative gradient ascent) 탐색 기법을 적용하였다. 그러나 이러한 기법들은 모두 지역적 극소/극대 영역에서 수렴될 가능성이 있으며, 수렴 안정성이 떨어지고, 탐색 반복을 위한 최적의 계단 값 (step size), 반복 횟수(iteration numbers)가 추정 대상 파라미터에 따라 달라지는 문제를 가지고 있다. 따라서 탐색 영역을 축소시키고 전역 탐색을 하는 것이 효과적일 수 있다.

여기서는 $K_{\max} = K$라고 가정하자. RSC 부호의 구속장의 길이만을 추정하는 문제는 부호어의 선형 관계를 이용한 행렬의 랭크 추정 등을 통해 비교적 용이하게 얻을 수 있다[6]. 우선 RSC의 궤환 다항식 $f(x)$의 첫 항의 계수 f_0는 항상 1이어야 한다. 또한 체크 다항식 $g(x)$의 첫 계수 g_0 및 최고차 항의 계수들인 f_m과 g_m이 1이 아니면 구속장의 길이가 감소하기 때문에 RSC의 구속자의 길이를 K로 설정하는 의미가 없다. 결론적으로 f_0, f_m, g_0, g_m은 모두 1이어야 한다. 또한 식 (5)에서 $f(x) \equiv g(x)$인 경우 $c(x) = s(x)$가 되므로 반복 부호가 되므로 터보 코드의 부 부호로서 사용하기 힘들다. 이러한 제한 조건을 적용하면 $\langle \boldsymbol{f},\boldsymbol{g}\rangle$ 쌍의 탐색 영역은 $2^{2(K_{\max}-2)} - (K_{\max}-2)$개로 좁혀진다. 예를 들어 3GPP 터보 부호의 경우 $K_{\max}=4$로 가정하면 탐색 영역의 수는 14가 된다. 이것은 참고문헌 [8]의 방법이 약 50회의 반복 계산을, 참고문헌 [9]의 기법이 약 20회의 반복 계산을 필요로 하는 것과 비교하면 더 계산량이 적어지는 효과를 갖는다. 또한 RSC의 구속장의 길이에 대한 정보가 전형 없는 경우에도 터보부호에 적용하여 우수한 성능을 내는 RSC 코드들의 생성 다항식이 다양한 구속장의 길이에 대하여 연구되어 발표되었다[14]. 따라서 가능성이 높은 생성 다항식들의 테이블을 이용하여 탐색 영역을 축소하는 것이 가능하다.

2.5 부분 전역 탐색 기법

본 논문에서는 기존 논문에 제시된 파라미터 추정 최적화를 위한 비용함수들을 그대로 이용하거나 수정하고 수치적 최적화 기법을 적용하는 대신, 축소된 영역에서의 전역 탐색 기법을 적용한 기법들을 소개한다.

2.5.1 코사인 비용함수 기반 부분 전역 탐색

문헌에 발표된 RSC 파라미터 추정 기법 가운데 가장 성능이 우수한 기법은 코사인 비용함수를 최대화하는 문제를 반복적 기울기 상승 기법(gradient ascent)으로 최적화 하는 것이다[9]. 이 방법은 식 (18)에서 g_i 및 f_i를 0과 1사이의 값을 갖는 확률값으로 설정하고, $P_n g_i$가 $0 \sim 1$의 값을 갖을 때 $\cos(\pi P_n g_i)$를 적용하여 식 (18)과 같이 $+1 \sim -1$사이의 범위로 변환한 비용함수를 기반으로 수치적 최적화 기법을 적용한 것이다. 이렇게 구한 비용함수를 동일하게 사용하되 Ⅱ-4절과 같이 탐색 영역을 축소 시킨 후 전역 탐색 기법을 사용할 것을 제안한다. 이 방법은 Ⅲ절의 모의 실험 결과에서 "MC-cosin, full search"로 표시하였다. 한편, 식 (16)을 계산하는 과정에서 지수 함수 연산이 포함되기 때문에 다음과 같이 간단한 선형 계산식을 적용하는 기법을 "MC-linear, full search"로 나타내었다.

$$P_n^{(s)} = \begin{cases} 1 & \text{if} \quad r_n^{(s)} < 1 \\ -0.5 r_n^{(s)} + 0.5 & \text{elseif} -1 \le r_n^{(s)} \le 1 \\ 0 & \text{else} \end{cases} \tag{20}$$

2.5.2 최소 자승 비용함수 기반 부분 전역 탐색

식 (19)에서 모든 n에 대하여 $C_n = 1$일 확률을 구하는 것은 쉽지 않다. 왜냐하면 서로 다른 n과 m에 대하여 $C_n = 1$인 확률과 $C_m = 1$인 확률이 서로 독립적인 사건에 대한 확률과 같이 곱으로 나타내기 힘들기 때문이다. 식 (18)을 관찰해 보면 C_n을 계산하기 위해 $m+1$개의 수신 값들이 사용되는 것을 알 수 있다. 따라서 C_n과 C_{n+1}은 동일한 m개의 수신 값을

이용하여 계산되므로 서로 확률적으로 독립 변수라고 보기 힘들다. 참고문헌 [8]은 식 (19) 대신에 모든 n에 대하여 $(C_n-1)^2$의 합을 구하여 최적화를 위한 목적함수로 사용하였다. 여기서는 이와 동일한 목적함수를 사용하되 참고문헌 [8]과 같이 연속적 단일차원 최적화 기법을 적용하는 대신에 Ⅱ-4절과 같이 탐색 영역을 축소 시킨 후 전역 탐색 기법을 사용할 것을 제안한다. 이 방법은 Ⅲ절의 모의 실험 결과에서 "LS, full search"로 나타내었다. 한편, 이 방법도 식 (16)을 계산하는 과정에서 AWGN 채널의 잡음 분산값인 σ^2 값의 추정이 필요하다. 정확한 SNR의 추정이 쉽지 않은 경우 이 값을 SNR이 0dB에 해당하는 $\sigma^2=1$값으로 고정하여도 성능이 크게 열화되지 않는다는 것을 모의실험을 통해 확인하였다. 이 방법은 모의 실험에서 "LS, full search, SNR=0dB"로 나타내었다.

Ⅲ. 모의 실험 결과

지금까지 문헌에 보고된 RSC 추정 기법들 가운데 가장 높은 추정 성공 확률을 나타내는 참고문헌 [9]의 코사인 비용함수 최대화 (MC) 기법과 본 논문에서 제안하는 부분 전역 탐색 기법들의 성능을 고찰하기 위해 모의 실험을 진행하였다. 우선 3GPP 터보 부호화기[15]를 대상으로 G=[013, 015]인 터보 부호화 블록의 크기가 $N=1{,}000$ 비트 일 때 AWGN 채널에서 10^4회 독립적인 전송 및 추정 시도를 진행한 결과를 그림 3과 4에 나타내었다. 추정 성공 확률(detection rate)은 그림 3에 나타내었으며, 추정 실패 확률은 로

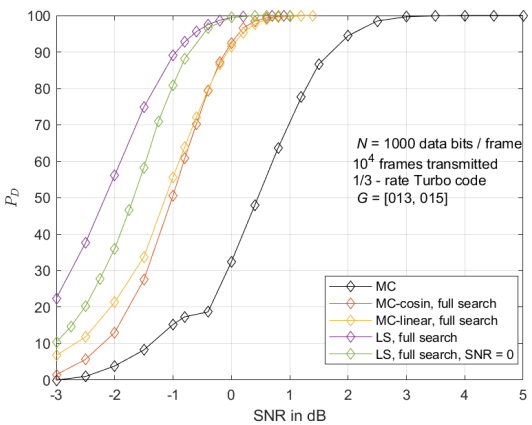

그림 3. 터보 부호화기의 RSC 생성 다항식 G 추정 확률; K=4, G=[013, 015], N=1,000
Fig. 3. Detection probability of RSC generator polynomial, G, in Turbo code; K=4, G=[013, 015], N=1,000

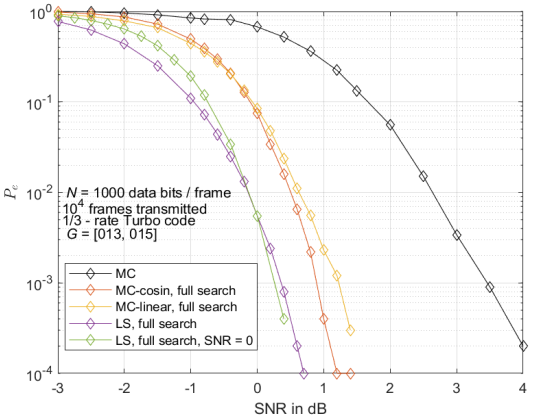

그림 4. 터보 부호화기의 RSC 생성 다항식 G 추정 오류 확률; K=4, G=[013, 015], N=1,000
Fig. 4. Detection error probability of RSC generator polynomial, G, in Turbo code; K=4, G=[013, 015], N=1,000

그 단위로 그림 4에 나타내었다. 그림 3과 그림 4의 그래프를 관찰해보면 거의 모든 SNR영역에서 Ⅱ-5절에서 제안한 4가지 부분 전역 탐색 기법이 기존의 MC[9]과 비교하여 1.5dB 이상의 SNR 이득을 보이는 것을 알 수 있다. 채널 SNR이 0dB일 때, MC 기법은 약 35%의 추정 정확도를, 제안하는 기법들은 90% 이상을 나타내고 있다.

참고문헌 [9]와 같이 코사인 비용함수를 이용하는 것보다 참고문헌 [8]에 사용되었던 최소 자승 비용함수(LS)를 이용하는 경우 부분 전역 탐색에서는 더 우수한 추정 정확도를 나타내는 것도 관찰할 수 있다. 한편 MC 비용함수를 적용하는 경우 계산량을 줄이기 위한 MC-linear 기법의 추정 성능이 MC-cosine 방법과 비교하여 추정 오류 확률이 10^{-2}일 때 약 0.15dB 정도의 성능 열화를 나타낸 것을 알 수 있다. 또 LS 비용함수를 이용하는 경우 SNR을 0dB로 고정하면, -3dB ~ 0dB의 SNR 범위에서는 추정 정확도가 10% 이상 낮아지지만, 0dB 이상의 SNR 범위에서는 그 정도가 거의 없거나 미미하게 향상되는 것이 관찰되었다. 터보 부호화기의 성능은 부호화 블록 길이가 길 때 오류 정정 능력이 향상되고, 짧은 경우에는 반대로 오류 정정능력이 감소된다. 터보 부호화 블록 길이가 추정 성능에 미치는 영향을 고찰하기 위해 $N=100$으로 감소시킨 후 동일한 모의 실험을 진행하였다.

그림 5와 그림 6은 터보 부호 블록 길이가 $N=100$인 경우 수행한 모의 실험결과를 통해 얻은 추정 성능을 나타낸 것이다. 그림 3 및 그림 4의 결과와 비교할 때 식 (18)로 주어지는 비용 함수의 개수가 1,000에서 100으로 감소하였기 때문에 잡음의 영향을

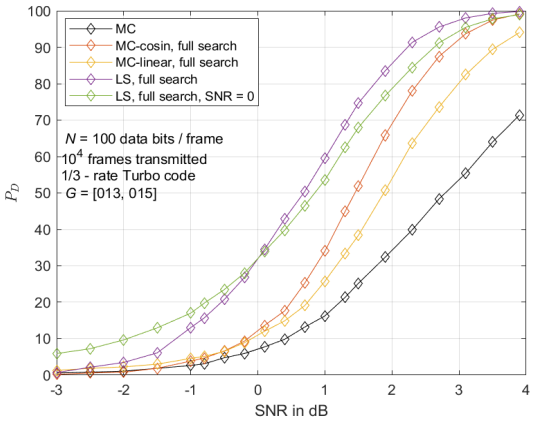

그림 5. 터보 부호화기의 RSC 생성 다항식 G 추정 확률; K=4, G=[013, 015], N=100
Fig. 5. Detection probability of RSC generator polynomial, G, in Turbo code; K=4, G=[013, 015], N=100

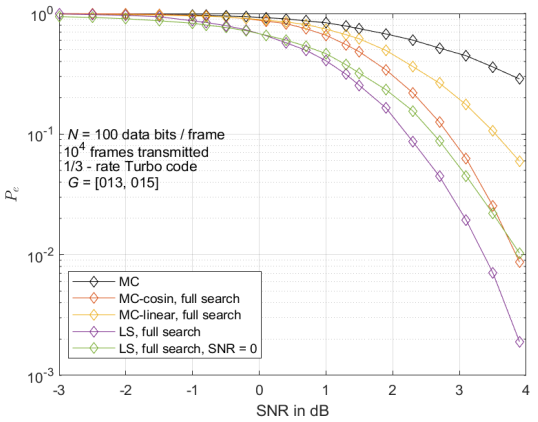

그림 6. 터보 부호화기의 RSC 생성 다항식 G 추정 오류 확률; K=4, G=[013, 015], N=100
Fig. 6. Detection error probability of RSC generator polynomial, G, in Turbo code; K=4, G=[013, 015], N=100

더 많이 받아 추정 성능이 감소되는 것을 알 수 있다. 기존 MC 기법의 경우, 채널 SNR을 4dB까지 증가시켜도 추정 정확도가 70% 정도였다. 그러나 제안하는 부분 전역 탐색 기법들의 경우 동일한 SNR 값에서 추정 정확도가 94%~99.8%였다. 한편, 3GPP 터보 부호화기의 동작 범위로 추정되는 -1dB~0dB의 채널 SNR에서는 모든 기법의 추정 정확도가 35% 이하였다.

터보 부호화기의 RSC에 적용된 구속장 K가 5이고 G=[023, 033]인 경우에도 동일한 조건으로 모의 실험을 진행하여 그 추정 성능을 고찰하였으며, 터보 부호화 블록의 크기가 $N=1{,}000$일 때의 결과를 그림 7과 그림 8에 나타내었으며, $N=100$일 때의 결과를 그림 9와 그림 10에 나타내었다. 탐색 범위는 2^{2K}에 비례하기 때문에 구속장 K 값이 3에서 4로 증가하게 되면 탐색 범위가 4배 증가하게 된다. 탐색 범위가 넓어지면 잡음에 의해 우연히 바르지 않는 RSC 생성 다항식 후보에 해당하는 목적함수가 바른 후보의 값보다 더 커질 가능성이 증가한다. 따라서 추정 성능의 열화가 예상된다. 그림 3 및 그림 4와 그림 7 및 그림 8을 비교해 보면 동일한 터보 부호 블록 길이 $N=1{,}000$에 대하여 구속장 K 값이 3에서 4로 증가하였을 때, 제안하는 전역 탐색 기법들은 추정 오류 확률 10^{-2}에서 요구되는 SNR값이 약 0.2dB 증가한 것을 알 수 있다. 한편 기존의 MC 기법은 동일한 추정 오류 확률을 얻기 위해 K값이 1증가할 때 약 2dB 더 높은 SNR을 필요로 하고 있다. 제안하는 LS 기반 전역 탐색과 기존의 MC 기법을 비교하면 추정 오류 확률 10^{-2}를 기준

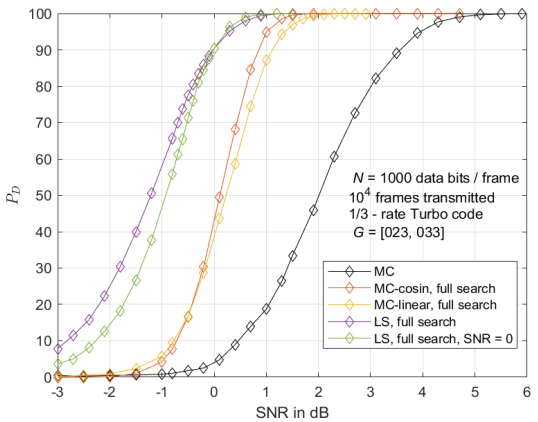

그림 7. 터보 부호화기의 RSC 생성 다항식 G 추정 확률; K=5, G=[023, 033], N=1,000
Fig. 7. Detection probability of RSC generator polynomial, G, in Turbo code; K=5, G=[023, 033], N=1,000

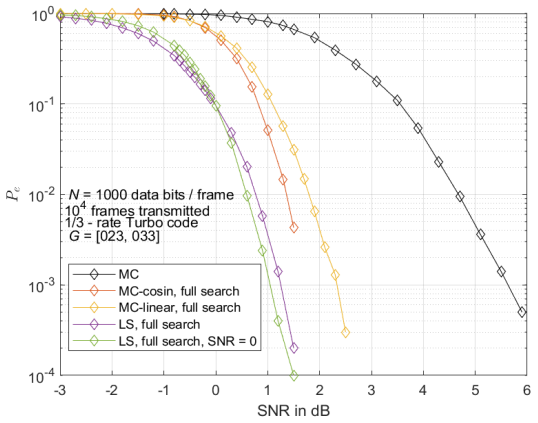

그림 8. 터보 부호화기의 RSC 생성 다항식 G 추정 오류 확률; K=5, G=[023, 033], N=1,000
Fig. 8. Detection error probability of RSC generator polynomial, G, in Turbo code; K=5, G=[023, 033], N=1,000

으로 할 때 제안하는 기법이 약 4dB의 채널 SNR 이득을 보이고 있는 것을 관찰 할 수 있다. 터보 부호 블록 크기를 N=100으로 감소시켰을 때는 그림 9 및 그림 10과 같이 RSC 생성 다항식 추정 성능이 N=1,000에 해당하는 그림 7 및 그림 8과 비교하여 현저히 열화되는 것을 관찰 할 수 있다. 제안하는 기법 가운데 가장 우수한 LS 기반 전역 탐색의 경우 10^{-2}의 추정 오류 확률을 얻기 위한 SNR은 약 4.5dB 증가하였다. 기존의 MC 기법은 SNR을 4dB까지 증가시켰을 때 추정 정확도가 30%에 도달했다.

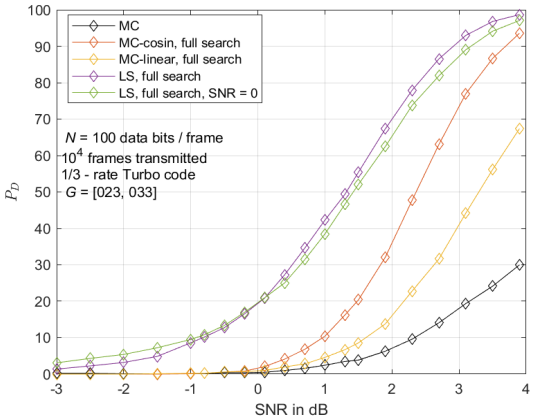

그림 9. 터보 부호화기의 RSC 생성 다항식 G 추정 확률; K=5, G=[023, 033], N=100
Fig. 9. Detection probability of RSC generator polynomial, G, in Turbo code; K=5, G=[023, 033], N=100

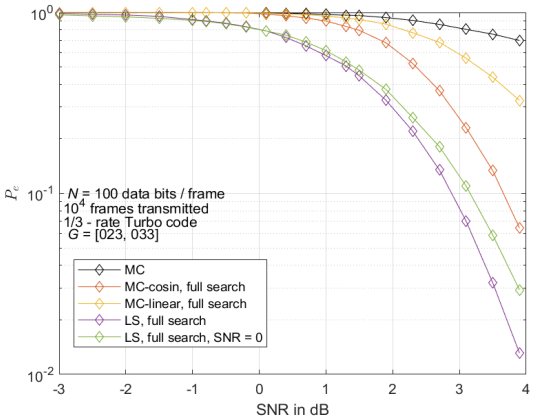

그림 10. 터보 부호화기의 RSC 생성 다항식 G 추정 오류 확률; K=5, G=[023, 033], N=1,000
Fig. 10. Detection error probability of RSC generator polynomial, G, in Turbo code; K=5, G=[023, 033], N=1,000

Ⅳ. 결 론

본 논문에서는 블라인드 송수신 환경에서의 수신된 메시지를 통해 터보 부호기의 RSC 파라미터 추정 문제를 고찰하고 기존의 수치적 최적화 방법 대신 탐색 범위를 좁힌 전역 탐색 기법을 제안하고, 그 추정 성능을 모의 실험을 통해 고찰하였다. 제안하는 기법은 터보 부호 블록 크기가 N=1,000 일 경우 추정 정확도 99%를 기준으로 K=4인 경우 기존의 MC 기법보다 2.7dB, K=5인 경우는 4dB의 SNR 이득을 나타내었다.

References

[1] M. Teimouri and H. K. Motlagh, "Reverse engineering of communications networks: evolution and challenges," arXiv: 1704.05432, 2017.

[2] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo codes," in *Proc. IEEE ICC '93*, pp. 1064-1070, Geneva, Switzerland, May 1993.

[3] G. D. Brushe, et al., "Determining the constraint length and generating polynomials of rate 1/L convolutional coded signals," *IEEE Signal Process. Lett.*, vol. 2, pp. 160-162, 1995.

[4] E. Filiol, "Reconstruction of convolutional encoders over GF(q)," *IMA Intl. Conf. on Cryptography and Coding*, pp. 101-109, 1997.

[5] J. Dingel and J. Hagenauer, "Parameter estimation of a convolutional encoder from noisy observations," *IEEE Int. Symp. Inf. Theory*, pp. 1776-1780, Nice, 2007.

[6] J. Barbier, "Reconstruction of turbo-code encoder," in *Proc. SPIE, Secur. Defence Symp.*, vol. 5819, pp. 463-473, Mar. 2005.

[7] Y. G. Debessu, et al., "Novel blind encoder parameter estimation for turbo codes," *IEEE Commun. Lett.*, vol. 16, pp. 1917-1920, 2012.

[8] P. Yu, J. Li, and H. Peng, "A least square method for parameter estimation of RSC sub-codes of turbo codes," *IEEE Commun. Lett.*, vol. 18, no. 4, pp. 644-647, Apr. 2014.

[9] Z. Wu, "A maximum cosinoidal cost function

method for parameter estimation of RSC turbo codes," *IEEE Commun. Lett.*, vol. 23, no. 3, pp. 390-393, Mar. 2019.

[10] R. L. Peterson, et al., *Intro. to Spread-Spectrum Communications*, Prentice-Hall, 1995.

[11] J. Massey, "Shift-Register synthesis and BCH decoding," *IEEE Trans. Info. Theory*, vol. 15, no. 1, pp. 122-127, Jan. 1969.

[12] T. K. Moon, "Maximum-likelihood binary shift-register synthesis from noisy observations," *IEEE Trans. Info. Theory*, vol. 48, no. 7, pp. 2096-2104, Jul. 2002.

[13] J. Hagenauer, et al., "Iterative decoding of binary block and convolutional codes," *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 429-445, Feb. 1996.

[14] M. S. C. Ho, S. S. Pietrobon, and T. Giles, "Improving the constituent codes of turbo encoders," *IEEE Globecom*, pp. 3525-3529, 1998.

[15] H. J. Oh, et al., "3GPP GERAN evolution system employing high order modulation and turbo coding : Symbol mapping based on priority," *J. KICS*, vol. 33, no. 6, pp. 607-613, 2008.

고 선 재 (Seon-Jae Ko)

2018년 2월 : 국립인천대학교 임베디드시스템공학과 공학사

2018년 3월~현재 : 인천대학교 임베디드시스템공학과 석사과정 재학중

<관심분야> 인터넷기술, 유비쿼터스네트워크, 임베디드시스템, 검출 및 추정이론

[ORCID:0000-0001-9473-8644]

김 재 윤 (Jae-Yun Kim)

2002년 2월 : 한양대학교 전자공학과 학사 졸업

2004년 2월 : 한양대학교 전자전기제어 계측공학과 석사 졸업

2004년~현재 : LIG넥스원 전자전연구소 수석연구원

<관심분야> 통신 및 전자전 신호처리

[ORCID:0000-0002-4692-8467]

김 선 교 (Seon-Kyo Kim)

2010년 8월 : 연세대학교 컴퓨터공학과(공학사)

2013년 2월 : 연세대학교 컴퓨터과학과(공학석사)

2013년~현재 : 국방과학연구소 선임연구원

<관심분야> ES 신호분석 SW

[ORCID:0000-0001-8714-2404]

최 병 조 (Byoung-Jo Choi)

1990년 2월 : KAIST 전기및전자공학과 졸업

1992년 2월 : KAIST 전기및전자공학과 석사

2002년 5월 : 영국 Southampton 대학 공학박사

1992년 1월~2005년 2월 : LG 전자 중앙연구소 책임연구원

2005년 3월~현재 : 국립인천대학교 임베디드시스템공학과 교수

<관심분야> 무선 통신, 무선 제어, 임베디드시스템

[ORCID:0000-0002-2570-0308]