Journal of KIIT. Vol. 15, No. 12, pp. 109-115, Dec. 31, 2017. pISSN 1598-8619, eISSN 2093-7571 109
http://dx.doi.org/10.14801/jkiit.2017.15.12.109

쿨백-라이블러 발산을 이용한 인터리버 파라미터 추정

최창렬*, 윤동원**

Blind Interleaver Parameter Estimation Using Kullback-Leibler Divergence

Changryoul Choi*, Dongweon Yoon**

본 연구는 방위사업청 및 국방과학연구소에 의해 설립된 신호정보 특화연구센터의 지원을 받아 수행되었음.

요 약

본 논문에서는 랜덤 정방 행렬의 차원 분포와 쿨백-라이블러 발산을 이용하여, 인터리버의 파라미터들을 추정하는 알고리즘을 제안한다. 특정한 갈루아 필드 위의 랜덤 정방 행렬의 차원 분포는 항상 특정한 분포를 따른다. 오류 정정 부호화되고 인터리빙을 거친 데이터의 경우는 선형 의존성으로 인해서 인터리버 주기 l과 같은 크기의 $l \times l$ 정방 행렬을 만들었을 때, 랜덤한 정방 행렬의 차원과는 전혀 다른 차원 분포를 갖게 된다. 이 때, 랜덤 정방 행렬의 차원 분포와 가장 다른 차원 분포를 갖는 특정 길이를 찾기 위해서 쿨백-라이블러 발산을 활용한다. 모의 실험 결과를 통해서, 제안하는 방법이 기존의 방법보다 검출 성능 및 오경보 확률에서 월등히 좋은 결과를 나타냄을 확인하였다.

Abstract

In this paper, we propose a blind interleaver parameter estimation algorithm exploiting the distribution of the ranks of the random matrices and the Kullback-Leibler divergence. The distribution of the ranks of the random matrices over a Galois field follows the specific distribution. Since there is a linear dependence among data which are encoded by error-correcting codes and interleaved by some interleaver, if we construct square matrices whose size is the same as the true interleaver period using these data, the distribution of the ranks of these matrices is far different from that of the random square matrices. By calculating the Kullback-Leibler divergence between the distribution of the ranks of the random matrices and that of the constructed matrices, we can estimate the interleaver parameters effectively. Experimental results show that the proposed algorithm outperforms the previous algorithm in terms of the detection probability and the false alarm probability.

Keywords
blind estimation, interleaver, channel codes, Gaussian elimination

* 한양대학교 전자통신공학과
- ORCID: http://orcid.org/0000-0002-2616-8333
** 한양대학교 융합전자공학부(교신저자)
- ORCID: http://orcid.org/0000-0001-9631-3500

· Received: Aug. 29, 2017, Revised: Oct. 13, 2017, Accepted: Oct. 16, 2017
· Corresponding Author: Dongweon Yoon
Dept. of Electronic Engineering, Hanyang University, 222 Wangsimni-ro, Seongdong-gu, Seoul 04763, Korea
Tel.: +82-02-2220-0362, Email: dwyoon@hanyang.ac.kr

Ⅰ. 서 론

근래의 디지털 통신 시스템의 경우, 통신상에서 일어날 수 있는 다양한 오류 등에 대비한 안정적인 통신을 위해서 거의 항상 오류 정정 부호를 사용한다. 일반적으로 이러한 오류 정정 부호는 오류에 대응하기 위해서 부가 정보를 추가하며, 대부분의 오류 정정 부호는 랜덤 오류에 강인하게 디자인한다. 그러나 군집 오류가 발생했을 경우, 일반적인 오류 정정 부호의 오류 정정 능력은 급격히 떨어지게 되어 전체적인 시스템의 성능을 떨어뜨리게 된다. 이러한 문제를 해결하기 위해서, 군집 오류를 랜덤 오류로 바꾸어 줄 수 있는 기술인 인터리버를 사용하게 된다[1].

일반적인 통신 시스템의 경우, 송신단과 수신단은 통신 각 모듈에 대한 구체적인 파라미터를 알고 있어서 통신 자체에 어려움이 발생하지 않으나, 비협력적인 상황에서는 각 통신에 대한 구체적인 파라미터를 알 수 없으므로 통신 내용을 파악하기 위해서는 무엇보다 각 통신 모듈에 사용되는 파라미터를 파악하는 것이 무엇보다 중요하다. 본 논문에서는 이 중에서 인터리버 파라미터를 찾아내는 방법론에 대해서 제안하도록 한다.

기존의 인터리버 파라미터를 찾는 방법론은 기본적으로 오류 정정 부호가 갖고 있는 각 부호어내의 선형성을 이용하는 것이 일반적이다[2]-[8]. 이 방법론을 좀 더 세부적으로 구분해 보자면, 쌍대 부호를 사용하는 방법[2]-[6], 부호어내의 선형 의존성(Linear Dependence within a Codeword)을 이용하는 방법[7], 그리고 이 두가지 방법을 모두 다 차용하는 방법으로 나눌 수 있다[8]. 본 논문에서는 부호어내의 선형 의존성 뿐만 아니라 부호어간 선형 의존성(Linear Dependence Among Codewords)을 활용하여 인터리버 주기를 찾는 방법론을 확장하였고, 랜덤 정방 행렬의(Random Square Matrix) 차원 분포와 쿨백-라이블러 발산(Kullback-Leibler Divergence)을 이용하여 인터리버 주기를 찾는 방법론을 제안한다.

Ⅱ. 기존 연구

2.1 시스템 모델

C를 (n, k) 파라미터를 갖는 $GF(q)$ 위의 선형 부호라고 하자, 여기서 n은 부호의 길이를 나타내고, k는 부호의 차원을 나타내며, $GF(q)$는 원소의 개수가 q인 Galois field 혹은 유한체(Finite Field)를 나타낸다. 선형성으로 인해서, 임의의 부호어(Codeword) $c \in C$는 다음과 같이 표현할 수 있다[1].

$$c = mG \tag{1}$$

여기서 c는 $1 \times n$ 행벡터(Row Vector)를 나타내고, m은 $1 \times k$ 행벡터를 나타내며, G는 최대 차원(Full Rank)를 갖는 $k \times n$ 행렬을 나타낸다.

거의 모든 통신 시스템에서는 인터리버 사이즈 S는 부호어 길이의 정수배, 즉, $S = \beta_n$가 된다 (여기서 β는 자연수). t를 인터리빙된 데이터 스트림이라고 하고 z를 중간에 t를 캡쳐한 데이터이고 길이가 M이라고 하자. 이 데이터를 중간에 취하게 된 사람은 인터리버 파라미터에 대한 정보가 전혀 없으므로, 처음 몇몇 심볼 t_0개는 놓칠 수 있다. 일반성을 잃지 않고, $0 \le t_0 < S$라고 가정한다. 앞으로의 설명의 편의를 위해서 다음과 같은 데이터 스트림 z_d를 정의한다.

$$z_d(i) = t(i + t_0 + d) + e(i), 0 \le i < M - d \tag{2}$$

여기서 $e(i)$는 채널 오류를 나타낸다. 본 논문에서는 통신 채널로 오류 확률이 P_e인 이진 대칭 채널(Binary Symmetric Channel)을 가정한다. l을 예측된 인터리버 주기라고 가정하자. 이 경우, z_d를 사용해서 크기가 $D \times l$인 인터셉션 행렬(Interception Matrix) $Z_{l,d}$를 만들 수 있다. (여기서 $D = \left\lfloor \frac{M-d}{l} \right\rfloor$을 나타내며 $\lfloor x \rfloor$는 x를 넘지 않는 가장 큰 정수를 나타낸다.) 이때, 행렬은 캡쳐한 순서대로 왼쪽 맨 위부터 오른쪽 맨아래까지 래스터 스캔(Raster Scan) 순서로 쌓는다.

2.2 쌍대 부호를 이용한 방법

C를 (n, k) 파라미터를 갖는 $GF(q)$ 위의 선형

부호라고 할 때, 쌍대 부호 $C^{\perp}$는 아래의 조건을 만족하는 길이가 n인 모든 벡터로 정의된다[2].

$$cy^{T}=0,\ \forall c\in G \tag{3}$$

여기서 T는 전치(Transpose)를 나타낸다. y를 쌍대 부호어(Dual Codewords)라 하자. 이 경우 다음의 식을 통해서 인터리버의 주기를 찾을 수 있다.

$$yZ_{l,d}=u \tag{4}$$

여기서 u는 $l\times D$ 행렬을 나타낸다. $d+t_0=S$ 이며 $l=S$라고 가정해 보자. 그리고 캡쳐된 데이터에 오류가 전혀 발생하지 않았다면, u의 해밍 무게(Hamming Weight)는 반드시 0이 될 것이다. 만약, 몇몇 오류가 발생했다면, u의 해밍 무게의 기대값은 아래와 같이 주어진다[2].

$$D\times\frac{1-(1-2P_e)^{w}}{2} \tag{5}$$

여기서 w는 쌍대 부호어 y의 해밍 무게를 나타낸다.

2.3 부호어내의 선형 의존성을 이용한 방법

식 (1)을 통해서 부호의 몇 몇 심볼의 경우는 다른 심볼의 선형 결합으로 표현될 수 있다는 것을 알 수 있다. 따라서 만약 추정된 주기 l이 실제 주기 S의 정수배라면, 우리는 행렬 $Z_{l,d}$의 차원을 계산함으로써 이러한 선형 의존성을 확인할 수 있게 된다[5].

2.4 쌍대 부호 특성 및 부호어내의 선형 특성을 이용한 방법

피봇팅을 이용한 가우스-조던 소거법(GJETP, Gauss-Jordan Elimination Through Pivoting)은 Sicot 등이 제안한 방식으로 쌍대 부호 특성과 부호어내의 선형 의존성을 동시에 이용하고 있다[8]. 이 방법은 가우스 소거법을 하는 과정에서 쌍대 부호어를 동시에 계산함으로써 기존의 방식을 확장하였다. 캡쳐된 데이터에 몇 몇 오류가 발생하였을 경우, 선형 의존인(Linear Dependence) 열이 생기지 않을 수 있다. GJETP 알고리즘은, 이 경우에 선형 의존인 행을 찾는 것이 아니라, 거의 선형 의존인(Almost Linear Dependence) 행을 찾도록 되어 있다. 이 경우, 가우스 소거법은 쌍대 부호어를 찾기 위해서 가로 방향(Horizontally)으로 연산이 이루어진다. GJETP가 끝난 후, 선형 독립인(Linearly Independent) 행들의 해밍 무게가 인터리버 주기를 찾는 일종의 메트릭(Metric) 역할을 한다.

III. 제안하는 블라인드 인터리버 파라미터 추정 알고리즘

3.1 부호어간의 선형 의존성

앞에서 살펴 본 모든 알고리즘들은 기본적으로 부호어내의 선형 의존성을 이용하고 있다. 그렇기 때문에, 행렬의 차원을 계산하기 위하여 가우스 소거법을 사용할 때 항상 가로 방향으로 연산을 하고 있다. (반대로 만약 부호어가 가로 방향으로 정렬되어 있으면, 이 경우의 가우스 소거법 연산은 세로 방향으로 진행된다.) 본 논문에서는, 이러한 부호어내의 선형 의존성뿐만 아니라, 부호어간의 선형 의존성을 이용하여 행렬의 차원을 예측하는 새로운 관점을 제시한다.

갈루아 필드 $GF(q)$ 위의 (n,k) 선형 부호는 전체가 n-차원인 벡터 공간의 k-차원의 부분공간(Subspace)이므로, k개의 기저(Basis)가 존재한다. 그러므로 만약 k+1개의 부호어가 존재한다면, 최소한 한 개 이상의 부호어는 다른 부호어들의 선형 결합으로 표현할 수 있다. 이렇게 부호어내의 선형의존성과는 별개로 부호어간의 선형 의존성을 활용하면 행렬의 차원 예측을 보다 더 정교하게 할 수 있다. 예를 들면, 만약 행렬 $Z_{l,d}$에서 같은 부호어가 2번 발생했다면, 부호어내의 선형 의존성을 이용한 방법은 실제로 나타나는 차원을 제대로 예측하지 못한다.

3.2 정방 랜덤 행렬의 차원 분포

$GF(q)$ 위의 원소들을 임의로 선택해서 (이때, 각 심볼의 발생 확률은 같다고 가정한다) $l \times l$ 정방 행렬(Square Matrices)을 만들었을 때, 이 행렬의 차원이 r이 될 확률 P_r은 아래와 같이 주어진다[9].

$$P_r = q^{-l^2} \frac{\left[\prod_{i=0}^{r-1}(q^l - q^i)\right]\left[\prod_{i=0}^{r-1}(q^l - q^i)\right]}{\prod_{i=0}^{r-1}(q^r - q^i)} \quad (6)$$

$GF(3)$ 및 $GF(2^2)$ 위에서 이 값을 계산해보면 아래와 같다. 이때, $l \rightarrow \infty$라고 가정한다.

표 1. $GF(3)$ 위의 정방 행렬의 차원 분포 P_r
Table 1. Distribution of the ranks of the random matrices over $GF(3)$ P_r

$l - r$	P_r
0	0.560126
1	0.420095
2	0.196919
3	8.73902×10^{-5}
4	4.09642×10^{-8}

표 2. $GF(2^2)$ 위의 정방 행렬의 차원 분포 P_r
Table 2. Distribution of the ranks of the random matrices over $GF(2^2)$ P_r

$l - r$	P_r
0	0.688538
1	0.306017
2	5.44030×10^{-3}
3	5.48279×10^{-6}
4	3.37227×10^{-10}

제안하는 알고리즘은 랜덤 정방 행렬의 차원만을 활용하므로, 제안하는 알고리즘의 심볼이 어떤 갈루아 필드 위에 있어도 적용이 가능하다. 따라서 표현의 편의를 위해서 이진 심볼을 이용하는 $GF(2)$ 위에서 설명을 이어가도록 한다. 또한, $l \times l$ 정방 행렬의 차원이 $l - s$이고 $l \rightarrow \infty$일 때의 확률을 P_s라고 하자. 이 값은 다음과 같이 계산할 수 있다[10].

$$P_s = 2^{-s^2}\left[\prod_{i=s+1}^{\infty}(1-2^{-i})\right]\left[\prod_{i=1}^{s}(1-2^{-i})^{-1}\right] \quad (7)$$

이때의 값을 계산해보면, 아래의 표로 나타낼 수 있다.

표 3. $GF(2)$ 위의 정방 행렬의 차원 분포 P_s
Table 3. Distribution of the ranks of the random matrices over $GF(2)$ P_s

s	P_s
0	0.288288
1	0.577576
2	0.128350
3	0.005238
4	4.65669×10^{-5}

일반적인 예상과는 다르게, 랜덤 이진 정방 행렬의 차원 분포에서의 최대값은 0이 아니라 1에서 나타난다.

만약 $l \times l$ 이진 정방 행렬의 차원이 $l - s (s \geq 3)$이라고 가정해 보자. 이렇게 낮은 차원을 가진 경우에 대한 설명은 크게 보면 두가지 정도가 있을 수 있다. 첫 번째는 순전히 운에 의존해서 이렇게 낮은 확률을 갖는 경우이다. 예를 들면, 만약 s = 4라고 가정해 보자. 이런 사건이 발생할 확률은 4.65669×10^{-5}이며, 극단적으로 낮은 값으로 100만번 정도 실험을 하면면 47번쯤 나올 수 있는 확률이다. 또 하나의 가능한 설명은 $l \times l$ 이진 정방 행렬 내부에 어떤 규칙성이 존재하는 경우이다. 즉, 본 논문에서 해결하려고 하는 문제인 인터리버 파라미터를 찾는 문제를 생각해 보면, 이진 정방 행렬이 오류 정정 부호화되어 있고, 이 후에 인터리버를 거친 데이터라고 하면 부호어간의 선형 의존성으로 인해서 행렬의 차원이 낮은 값을 가질 수 있을 것이다. 보다 더 정확히 말하자면, 만약 l = S라면, $l \times l$ 이진 정방 행렬의 차원 분포는 표 3과는 전혀 다른 분포를 가질 것이고, $l \neq$ S라면 표 3의 분포를 따르게 될 것이다.

3.3 제안하는 인터리버 파라미터 추정 방법

3.2절에서 설명했듯이, 캡쳐된 데이터를 특정 주

기를 단위로 정방 행렬로 만든 후에, 그 데이터의 차원 분포를 이용하면 인터리버의 파라미터를 쉽게 추정할 수 있다. 그러나 일반적으로 캡쳐 된 데이터는 적을 수도 있고, 빠른 계산을 위해서는 데이터양이 적은 경우에도 이러한 방법론을 사용할 수 있어야 한다. 그러나 캡쳐하는 데이터를 정방 행렬로 순서대로 만들어서 차원 분포를 계산하게 되면, 실제로 만들 수 있는 정방 행렬의 개수가 심하게 제한된다. 예를 들면, 길이 1,000인 데이터를 캡쳐 했다고 가정해 보자. 이 경우, 10×10인 정방 행렬을 만든다고 가정하면, 우리가 만들 수 있는 최대치는 10개 정도가 되며, 이 경우는 행렬의 차원 분포를 보기에 심각하게 미흡한 숫자가 되게된다. 여기서, 선형 부호어간의 의존성은 부호어의 순서와는 아무런 관련이 없으므로 다음과 같이 정방 행렬의 개수를 늘릴 수 있다. 길이가 1,000인 데이터를 각각 길이가 10인 시퀀스로 중복되지 않도록 쪼갠다(Partition). 이 경우, 총 시퀀스의 개수는 100이 된다. 이렇게 쪼개진 100개의 시퀀스 중에서 임의로 10개의 시퀀스를 선택한다. 이렇게 하면, 이론상 다음과 같은 조합이 가능하다.

$$\binom{100}{10} \approx 1.731 \times 10^{13} \tag{8}$$

즉, 약 10^{12} 정도 가지수가 늘어나게 되어 정방 행렬의 차원 분포를 보는데 아무런 문제가 발생하지 않는다. 물론, 이 경우 중복되는 행들이 발생할 수 있으나, 전체적으로 보면 정방 행렬의 차원 분포를 왜곡시키지는 않는다. 캡쳐되고 이동된 데이터 $Z_{l,d}$를 특정한 길이 l로 쪼갠 시퀀스들을 $w_i\ (j)$ ($0 \le i < D$, $0 \le j < l$)라 하자. 이러한 방법을 통해서, 정방 행렬의 분포를 계산한 후, 그 분포가 표 3과 크게 다른 l을 찾게 된다. 분포가 표 3과 다른 분포를 찾기 위해서 아래와 같은 쿨백-라이블러 발산(Kullback-Leibler Divergence)값을 이용한다[11].

$$D_{KL,l} = \sum_i P(i) \log \frac{P(i)}{Q_l(i)} \tag{9}$$

식 (9)에서 $P(i)$는 표 3의 확률값을 나타내고, $Q_l(i)$는 $l \times l$ 정방 행렬의 차원 분포를 나타낸다.

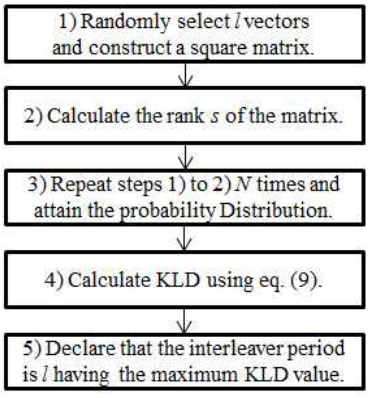

그림 1. 제안하는 블라인드 인터리버 파라미터 추정 방법
Fig. 1. Proposed blind interleaver parameter estimation

만약 l이 인터리버 주기와 다르다면, 이 값 $D_{KL,i}$는 0에 수렴할 것이고, 그렇지 않을 경우는 다른 값을 갖게 될 것이다. 제안하는 블라인드 인터리버 파라미터 추정 방법을 정리하면 그림 1과 같다.

Ⅳ. 성능 분석

제안하는 알고리즘을 검증하기 위해서 다양한 실험을 진행하였다. 제안하는 방법은 기본적으로 선형 부호의 선형성만을 활용함으로, 모든 선형 부호에 적용 가능하다. 본 논문에서는 가장 간단한 부호인 (7, 4) 해밍 부호를 활용하여 실험을 진행하였다. 그리고, 계산의 편의성을 위해서, KLD 계산 과정에서 표 3의 모든 값을 사용하지 않고, s가 3일때까지의 값만을 활용하였다. 이 경우, P_s는 0.005238에서 1 - 0.288788 - 0.577576 - 0.128350 = 0.005286이 된다.

우선, 제안하는 방법에서 검출 오경보 확률(False Alarm Probability)을 조절하기 위해서, 관련한 실험을 진행하였다. 이 경우 최대 KLD 값이 특정한 문턱값(Threshold) 아래인 경우는 검출 실패로 간주하였고, 최대 KLD 값이 문턱값 보다는 크지만, 추정한 인터리버 주기가 실제 인터리버 주기와 다른 경우를 오경보로 판단하였다.

그림 2는 인터리버 주기가 28일 때, 각 문턱값에 따른 검출 확률을 채널 오류 확률 BER(Bit Error Rate)에 따라서 나타낸다. 그림에서 볼 수 있듯이 문턱값을 높일수록 전반적인 검출 성능이 약간씩 떨어지는 결과를 알 수 있다.

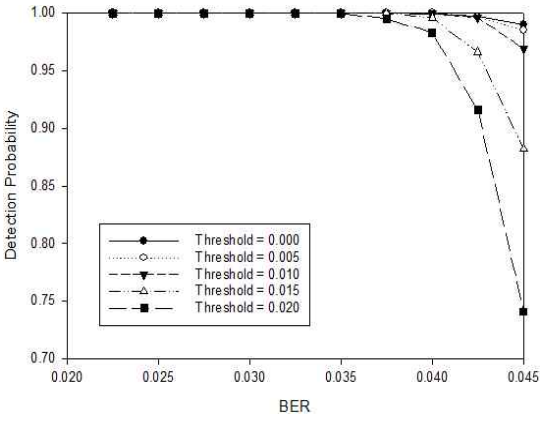

그림 2. 문턱값에 따른 검출 확률
Fig. 2. Detection probability for varying thresholds

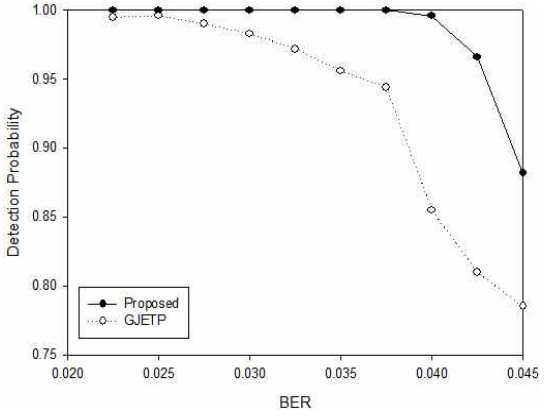

그림 3. 인터리버 주기가 28일 때 검출 확률
Fig. 3. Detection probability when the interleaver period is 28

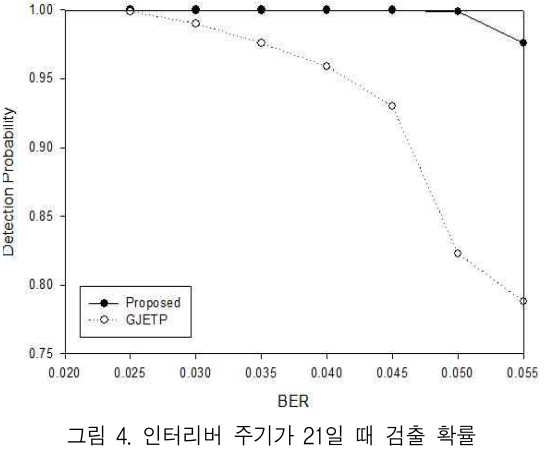

그림 4. 인터리버 주기가 21일 때 검출 확률
Fig. 4. Detection probability when the interleaver period is 21

그리고 각 알고리즘의 오경보 확률은 각각, 0.14%, 0.18%, 0.12%, 0.03%, 그리고 0%로 문턱값이 커짐에 따라서 전반적으로 오경보 확률이 작아지는 결과를 보여준다. 여기서 나온 실험 결과를 통해서, 문턱값이 0.015일 때가 검출 성능과 오경보 확률 사이에서 균형 잡힌 결과를 난다고 판단된다. 따라서 이후의 실험 결과는 문턱값을 0.015로 고정하였다.

그림 3은 제안하는 알고리즘과 GJETP 알고리즘(GJETP로 표시)의 성능을 비교한 그림이다. 이 경우 인터리버 주기는 28이다. 그림에서 볼 수 있듯이 제안하는 알고리즘이 전반적으로 좋은 검출 성능을 나타내는 것을 알 수 있다. 또한, 실제 필드 환경에서 안정적인 통신을 위한 타켓 BER 이 0.001 정도인 것을 감안하면, 제안하는 알고리즘은 항상 100%의 검출 성능을 나타냄을 알 수 있다. 이 경우, 제안하는 알고리즘의 오경보 확률은 0.03%이고, GJETP 알고리즘의 오경보 확률은 0.2%로, 제안하는 알고리즘이 안정성 측면에서도 월등한 결과를 나타냄을 알 수 있다.

그림 4 역시 GJETP 알고리즘과 제안하는 알고리즘의 비교를 나타내는데, 이 경우의 인터리버 주기는 21이다. 역시 그림에서 볼 수 있듯히 제안하는 알고리즘이 훨씬 나은 성능을 나타내고 있다. 이 경우의 오경보 확률은 제안하는 알고리즘은 0%, GJETP 알고리즘은 0.06%를 나타낸다.

V. 결론 및 향후 과제

본 논문에서는 비협력적 상황에서 정방 랜덤 행렬의 차원 분포와 쿨백-라이블러 발산값을 활용하여 수신 신호의 복원을 위한 인터리버 파라미터 추정 방법을 제안하였다. 오류 정정 부호 및 인터리빙된 데이터의 경우, 인터리버 주기 l과 동일한 크기로 $l \times l$ 정방 행렬을 만들었을 때, 이 행렬들의 차원 분포는 랜덤 정방 행렬의 차원 분포와는 완전히 다르게 된다. 이 특성을 활용해서, 캡쳐된 데이터를 특정 단위로 잘라서 정방 행렬을 만든 후에, 그 정방 행렬들의 차원 분포를 계산하였다. 이 후, 이 분포와 랜덤 정방 행렬의 차원 분포를 이용하여 쿨백-라이블러 발산값을 계산한 후, 가장 큰 값을 갖는 특정 단위를 인터리버 주기로 선언하였다. 모의 실

험 결과를 통해서 제안하는 방법이 기존의 방법보다 검출 성능 뿐 아니라 오경보 확률에서 월등히 좋은 성능을 나타냄을 알 수 있었다. 제안한 알고리즘에서는 오경보 확률을 조절할 수 있는 문턱값을 실험에 의존하여 결정하였으나, 추후 연구를 통해서 오경보 확률에 따른 문턱값을 결정하도록 할 예정이다.

References

[1] S. B. Wicker, "Error control systems for digital communications and storage", Englewood Cliffs, NJ, USA: Prentice-Hall, pp. 424-427, 1995.

[2] A. Valembois, "Detection and recognition of a binary linear code", Discrete Applied Mathematics, Vol. 111, No. 1-2, pp. 199-218, Jul. 2001.

[3] A. Canteaut and F. Chabaud, "A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511", IEEE Trans. Inf. Theory, Vol. 44, No. 1, pp. 367-378, Jan. 1998..

[4] M. Cluzeau and M. Finiasz, "Recovering code's length and synchronization from a noisy intercepted bitstream", in Proc. of ISIT, Seoul, Korea, pp. 2737-2741, Jun./Jul. 2009.

[5] Swaminathan R, A. S. Madhukumar, N. W. Teck, and C. M. S. See, "Parameter estimation of convolutional and helical interleavers in a noisy environment", IEEE Access, Vol. 5, pp. 6151-6167, Mar. 2017.

[6] J. Jeong, J. Oh, H. Lim, and D. Yoon, "Estimation of Interleaver Parameters for Punctured Channel Coded Signals in Noisy Channels", Journal of KIIT, Vol. 14, No. 11, pp. 49-57, Nov. 2016.

[7] G. Burel and R. Gautier, "Blind estimation of encoder and interleaver characteristics in a non cooperative context", in Proc. of IASTED, Scottsdale, AZ, USA, Nov. 2003.

[8] G. Sicot, S. Houcke, and J. Barbier, "Blind detection of interleaver parameters", Signal Processing, Vol. 89, No. 4, pp. 450-462, Apr. 2009.

[9] E. M. Gabidulin, "Theory of codes with maximum rank distance", Problems of Information Transmission, Vol. 21, No. 1, pp. 1-12, Jan. 1985.

[10] V. F. Kolchin, "Random graphs", New York: Cambridge University Press, pp. 126-135, 1999.

[11] T. M. Cover and Joy A. Thomas, "Elements of Information Theory", New York: Wiley, pp. 12-49, 1991.

저자소개

최 창 렬 (Changryoul Choi)

1997년 2월 : 한양대학교 전파공학과(공학사)
1999년 2월 : 한양대학교 전자통신공학과(공학석사)
2010년 8월 : 한양대학교 전자통신전파공학과(공학박사)
2017년 10월 현재 : 한양대학교 신호정보특화연구센터 연구 교수
관심 분야 : 비디오 코딩, 데이터 은닉, 채널 코딩

윤 동 원 (Dongweon Yoon)

1989년 2월 : 한양대학교 전자통신공학과(공학사)
1992년 2월 : 한양대학교 전자통신공학과(공학석사)
1995년 8월 : 한양대학교 전자통신공학과(공학박사)
2017년 10월 현재 : 한양대학교 융합전자공학부 교수
관심분야 : 무선통신, 위성 및 우주통신, 신호정보