간섭채널에서의 저 피탐지 확률 통신 용량에 관한 연구

조강희, 이시현
한국과학기술원 전기 및 전자공학부

{kanghee, sihyeon}@kaist.ac.kr

요 약

본 논문은 K 개의 송수신단으로 구성된 간섭채널에서의 저 피탐지 확률 통신 환경을 고려하였다. 통신을 관측하는 도청단은 수신값을 바탕으로 통신의 발생 유무를 판단하는 최적의 hypothesis testing 을 한다. 이때 저 피탐지 확률 통신은 이 테스트의 성능이 블라인드 테스트의 성능과 유사하게 나오는 것을 목표로 한다. 본 채널 환경에서의 저 피탐지 확률 통신 용량 및 이를 달성하는 최적 기법을 도출하였으며, 저 피탐지 확률 통신을 위한 최적의 암호키 길이 또한 분석하였다. 본 모델에서의 최적의 저 피탐지 확률 통신 방식으로는 단일 매체 통신 기반의 treating interference as noise 기법이 사용되었으며 암호키 길이에 대한 분석에는 채널 분해성 개념이 활용되었다.

Ⅰ. Introduction

저 피탐지 확률 통신은 합법적 송수신단의 통신 발생 유무가 적대적 도청단에 의하여 탐지되는 확률을 매우 낮은 수준으로 보장해주는 통신 기법이다. 이는 합법적 송수신단의 신호를 도청단 채널의 불확실성에 묻히게끔 설계함으로써 달성할 수 있다. 이러한 통신 기법에 대한 정보이론적 연구가 단일매체간 통신 환경에서 활발히 진행되었으며 [1-3], 여러 네트워크 상황에 대한 연구로 확장된 바 있다 [4, 5]. 일반적으로 저 피탐지 확률 통신 환경에서 n 번의 채널을 활용하여 $O(\sqrt{n})$ 비트의 정보를 전송할 수 있는 square-root law 가 성립한다.

본 논문에서는 간섭 채널에서의 저 피탐지 확률 통신 환경을 고려하였다. 저 피탐지 확률 통신 제약 조건이 없는 간섭채널에서는 일반적으로 통신 용량이 알려져 있지 않은데, 제약 조건하에서의 통신 용량을 본 논문에서 규명하였다. 최적 통신 기법으로는 단일 매체 통신 기반 treating interference as noise (TIN) 기법이 활용되었으며, 최적의 암호키 길이를 채널 분해성 (channel resolvability) 개념을 활용하여 분석하였다. 암호키는 다수의 코드북을 구성하여 도청단 채널의 관측값이 independent and identically distributed (IID) process 에 근접하게 만드는 것을 목표로 활용되었다.

Ⅱ. Problem Formulation

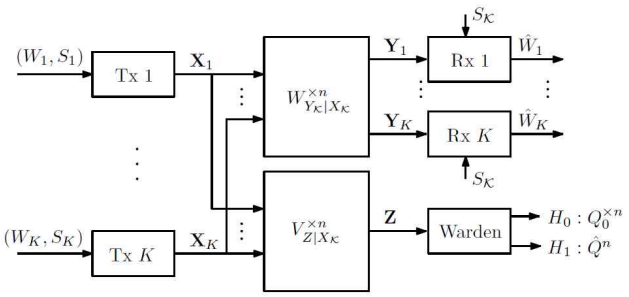

Figure 1 Channel Model

본 논문에서는 K 개의 송수신단으로 구성된 discrete memoryless interference channel (DM-IC)를 고려한다 (그림 1). 합법적 채널을 $(\chi_\kappa, W_{Y_k|X_\kappa}, \mathcal{Y}_\kappa)$ 로, 도청단이 관측하는 채널을 $(\chi_\kappa, V_{Z|X_\kappa}, \mathcal{Z})$ 로 표현하며, 이때 χ_κ 는 $(\chi_1, \dots, \chi_K)$ 를 나타낸다. 서술을 명료히 하기 위해, 입력 알파벳 χ_k 는 모든 k 에 대해 $\{0,1\}$로 가정한다. 통신이 발생하지 않을 때에는, 모든 송신단이 부호 0 을 전송한다고 가정하며, 통신 블록 길이는 n 으로 가정한다.

오직 i 번째 송신단만 부호 1 을 전송할 때, k 번째 수신단의 채널 출력 분포를 $W_i^{(k)}$ 로 정의하며, 모든 송신단이 0 을 전송할 때에는 $W_0^{(k)}$ 으로 정의한다. 이와 유사하게, i 번째 송신단만 1 을 전송할 때 도청단의 채널 출력 분포를 Q_i, 모든 송신단이 0 을 전송할 때의 출력 분포를 Q_0 으로 정의한다. 본 논문에서는 피탐지 확률 척도로 상대 엔트로피를 사용하며, 저 피탐지 확률 통신의 조건을 다음과 같이 설정한다 [1].

$$\lim_{n\to\infty} D(Q^n || Q_0^{\times n}) = 0$$

임의의 채널 입력에 대한 도청단의 채널 출력값의 support set 은 Q_0의 support set 에 포함되며 (반대시 상대 엔트로피 값이 무한대가 되어 저 피탐지 확률 통신이 불가능하다), 임의의 채널 출력 분포의 convex combination 으로 Q_0를 구성할 수 없음 (반대시 square-root law 가 성립하지 않음)을 가정한다.

각 송수신단 k 는 메시지 $W_k \sim Unif[1:M_k]$ 를 암호키 $S_k \sim Unif[1:J_k]$ 를 이용하여 주고받는다. 이때, 저 피탐지 확률 통신 채널 용량 영역은 다음과 같이 정의된다.

Definition 1) 본 저 피탐지 확률 통신 환경에서 투플 쌍 $(R_\kappa, L_\kappa) \in \mathbb{R}_+^{2K}$ 는 다음을 만족하는 코드열이 존재할 때 달성 가능하다고 한다.

$$\liminf_{n\to\infty} \frac{\log M_k}{\sqrt{nD(Q^n||Q_0^{\times n})}} \geq R_k, \qquad \forall k,$$

$$\limsup_{n\to\infty} \frac{\log J_k}{\sqrt{nD(Q^n||Q_0^{\times n})}} \leq L_k, \qquad \forall k,$$

$$\lim_{n\to\infty} P_e^n = 0 \text{ and } \lim_{n\to\infty} D(Q^n||Q_0^{\times n}).$$

이때, 저 피탐지 확률 통신 용량 영역은 집합 $\{R_\kappa \in \mathbb{R}_+^K$: (R_κ, L_κ)가 어떤 L_κ에 대해 달성 가능$\}$의 closure 로 정의된다.

Ⅲ. Main Results

본 Section 에서는 K 개의 송수신단으로 구성된 간섭채널에서의 저 피탐지 확률 통신 용량 영역을 제시하고, 주요 핵심 내용들을 요약한다.

Theorem 1) 저 피탐지 확률 통신 채널 용량 영역
본 통신 환경에서의 채널 용량 영역은 $\sum_k \alpha_k = 1$ 을 만족하는 어떤 $\boldsymbol{\alpha} \triangleq \{\alpha_k\}_{k\in\kappa} \in [0,1]^K$ 에 대해서 다음을 만족하는 통신량 투플 R_κ의 집합으로 나타난다:

$$R_k \leq \frac{\alpha_k D(W_k^{(k)}||W_0^{(k)})}{\sqrt{\frac{\chi^2(\boldsymbol{\alpha})}{2}}}, \quad \forall k$$

이때, $\chi^2(\boldsymbol{\alpha})$는 다음과 같이 정의된다.

$$\chi^2(\boldsymbol{\alpha}) \triangleq \sum_z \frac{(\sum_k \alpha_k Q_k(z) - Q_0(z))^2}{Q_0(z)}$$

위 부등식에서의 등식을 만족하는 투플 R_k에 대해서 (즉, 채널 용량 영역의 경계선에서) (R_κ, L_κ)가 달성 가능할 필요충분조건은 다음과 같다.

$$L_k \geq \frac{\alpha_k[D(Q_k||Q_o) - D(W_k^{(k)}||W_0^{(k)})]^+}{\sqrt{\frac{\chi^2(\boldsymbol{\alpha})}{2}}}, \quad \forall k$$

따라서 어떤 k에 대하여 $D(Q_k||Q_o) \leq D(W_k^{(k)}||W_0^{(k)})$ 라면, k 번째 송수신단은 암호키를 필요로 하지 않는다.

Achievability 로는, 일반적 방식인 random codebook 과 joint typicality decoding 이 활용되었다. 인코딩을 할 때에는 각 송신단에서 n 번의 채널 사용동안 $\sqrt{n}$ order 개의 1 을 전송하며, 디코딩에는 TIN 기법이 활용된다. 다음으로는 몇가지 주요한 분석결과를 정리하였다.

1) 저 피탐지 확률 조건은 송신단들이 전송할 수 있는 1 의 총 개수를 제한한다. Theorem 1 의 $\boldsymbol{\alpha}$는 총 1 의 개수를 각 송신단이 나눠 갖는 비율을 나타낸다. 각 송수신단 간의 채널 환경이 다르고, 각 송신단의 전송이 피탐지 확률에 함께 영향을 미치기 때문에, 총 1 의 개수는 $\boldsymbol{\alpha}$와 각 송수신단의 marginal 채널에 의해 결정되며, 파라미터 $\chi^2(\boldsymbol{\alpha})$에서 나타난다.
2) 각 송신단이 전송할 수 있는 1 의 개수가 크게 제한되 있기 때문에, 1 의 전송이 채널 불확실성에 추가하는 영향은 모든 송신단이 0 을 전송할 때의 채널 불확실성에 비해 근사적으로 무시할 수 있다. 따라서 각 송신단은 분배받은 만큼의 1 를 활용하여 서로에게 무시할만한 간섭을 끼치며 단일 매체간 통신에서의 최적 용량을 달성할 수 있다.
3) 각 송신단에서 도청단으로 가는 marginal 채널이 동일할 경우, $\chi^2(\boldsymbol{\alpha})$는 $\boldsymbol{\alpha}$값에 상관없이 일정하다. 따라서 채널 용량 영역이 선형적으로 나타나게 되며 시분할 통신 기법이 TIN 기법과 동일한 성능을 내며 최적의 기법이 된다.

IV. Proof

본 Section 에서는 증명의 대략적인 흐름을 제공한다. 상세한 증명은 [6]에서 확인할 수 있다.

A. Achievability Proof

1) Channel Reliability

간섭채널에서의 저 피탐지 확률 통신 채널 용량을 달성하는 방식으로는 각 송신단이 $\sqrt{n}$ order 개수의 부호 1 을 전송하는 것과 동시에, TIN 디코딩 방식이 있다. 증명에서는 통신 중에 각 송수신단이 겪는 marginal 채널을 다른 모든 송수신단이 0 을 전송하는 상황에서 하나의 송수신단만 통신을 하는 채널로 근사를 하는 방식이 활용되었으며, 이를 바탕으로 단일 매체간 저 피탐지 확률 통신의 분석을 적용하였다.

2) Channel Resolvability

저 피탐지 확률 통신 조건을 만족하기 위하여 도청단의 채널 출력 분포를 통신이 발생하지 않을 때의 출력 분포와 유사하게 해주는 것이 필요하다. 이를 위해 적은 수의 부호 1 을 전송하는 것과 동시에 암호키를 활용하여 충분히 많은 수의 코드북을 만들고, 이를 바탕으로 도청단의 채널 출력이 근사적으로 IID process 를 따르게 만드는 채널 분해성 접근 방식이 사용되었다. 도청단의 채널 출력을 근사적으로 IID process 로 만들기 위하여 다음이 요구된다.

$$R_k + L_k \geq \frac{\alpha_k D(Q_k||Q_0)}{\sqrt{\frac{\chi^2(\boldsymbol{\alpha})}{2}}}, \quad \forall k$$

위 결과와 channel reliability 에서의 결과를 통합하여 Theroem 1 의 achievability 를 증명할 수 있다.

B. Converse Proof

Converse 증명으로는 Fano's inequality 를 활용한 일반적 전개 방식과 더불어, 각 송수신단의 최대 전송량에 대한 상한값을 다른 송수신단이 통신을 하지 않고 하나의 송수신단만 통신을 할 때의 최대 전송량에 대한 상한값으로 치환하고, 이를 바탕으로 증명을 전개하였다. 자세한 증명은 [6]에서 확인할 수 있다.

V. 결론

본 논문에서는 K 개의 송수신단으로 구성된 간섭채널에서의 저 피탐지 확률 통신의 전송 용량을 규명하였으며, 채널 분해성 이론을 활용하여 암호키를 필요로하지 않는 채널 조건을 분석하였다. 최적의 통신 기법으로는 단일 매체간 통신 기법 기반의 TIN 기법이 활용되었다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터지원사업의 연구결과로 수행되었음 (IITP-2020-0-01787).

참 고 문 헌

[1] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," IEEE JSAC., vol. 31, no. 9, pp. 1921-1930, Sep. 2013.

[2] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," IEEE Tran. Info. Theory, vol. 62, no. 5, pp. 2334-2354, May 2016.

[3] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," IEEE Tran. Info. Theory, vol. 62, no. 6, pp. 3493-3503, June 2016.

[4] K. S. K. Arumugam and M. R. Bloch, "Covert communication over a k -user multiple-access channel," IEEE Tran. Info. Theory, vol. 65, no. 11, pp. 7020-7044, Nov 2019.

[5] V. Y. F. Tan and S.-H. Lee, "Time-division is optimal for covert communication over some broadcast channels," IEEE Transactions on Information Forensics and Security, vol. 14, no. 5, pp. 1377-1389, May 2019.

[6] K.-H. Cho and S.-H. Lee, "Treating interference as noise is optimal for covert communication over interference channels," IEEE Transactions on Information Forensics and Security, submitted for publication. [Online]. https://arxiv.org/abs/2003.04531.