블록 페이딩 릴레이 채널에서의 저 피탐지 확률 통신 용량에 관한 연구

조강희, 이시현
한국과학기술원 전기 및 전자공학부

{kanghee, sihyeon}@kaist.ac.kr

요 약

본 논문은 송신단, 반이중 릴레이, 수신단이 존재하는 블록 페이딩 릴레이 네트워크에서의 저 피탐지 확률 통신 환경을 고려하였다. 통신 발생 유무를 탐지하고자 하는 악의적인 도청단으로부터 통신 발생 유무를 숨기고자 하며, 통신의 피탐지 확률을 도청단의 블라인드 테스트 성공 확률과 유사하게 하는 것을 목표로 한다. 본 네크워크에서 우수한 릴레이 기법인 decode-and-forward 협력 릴레이 기법에 기반한 릴레이 통신 전략과 송신파워, 부호화율을 동시에 최적화하는 기법을 제시한다. 복잡한 비볼록 목적함수와 제약함수를 다루기 위해 교차적으로 반복하는 저복잡도 최적화 기법을 활용한다. 이를 통해 다양한 릴레이 위치에서 네트워크의 저피탐 정전용량을 분석하고 점대점 통신 등 비교군과 성능을 비교한다.

Ⅰ. Introduction

저 피탐지 확률 통신 (covert communication, 저피탐 통신)은 합법적 송수신단의 통신 발생 유무를 악의적인 도청단이 알지 (탐지하지) 못하게 하는 보안 통신 기법의 일종이다. 이를 위해 통신 발생 시의 도청단 수신 신호가 도청단의 배경 잡음 신호와 유사할 수 있도록 송신 신호를 설계한다. 본 논문에서는 이러한 저피탐 통신의 성능을 정보이론적 관점에서 분석하고자 한다. 저피탐 통신에 대한 정보이론적 연구는 점대점 통신 환경에서 활발히 진행되었으며 [1,2], 다양한 네트워크 모델에서 확장, 연구되었다 [3,4].

본 논문에서는 반이중 릴레이가 존재하는 블록 페이딩 릴레이 네트워크에서의 저피탐 통신 정전 용량을 분석한다. 본 모델에서 도청단은 송신단과 릴레이의 신호를 함께 관찰하고 가설검증을 진행하는 결합 탐지를 수행한다. 이러한 상황하에서 decode-and-forward (DF) 릴레이를 운영하여 송신단과 릴레이의 파워, 부호화율을 복합적으로 최적화한다. 복잡한 최적화 문제를 해결하기 위해 교차적 반복 기반 저복잡도 최적화 기법을 활용하였으며, 다양한 릴레이 위치에서의 시뮬레이션을 통해 성능을 분석하였고, 성능을 점대점 기법과 비교하였다.

Ⅱ. System Model

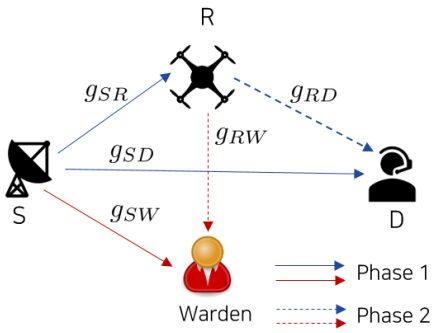

Figure 1 채널 모델

본 논문에서는 합법적 송신단 (S)과 수신단 (D), 반이중 릴레이 (R), 도청단 (W)가 있는 네트워크를 고려한다. 블록 페이딩 채널을 고려하였으며 coherence time 은 n 으로 둔다. 노드 i 와 j 의 거리를 d_{ij} , pathloss exponent 를 α로 두면 노드 i, j 사이의 channel gain g_{ij} 는 독립적인 complex white Gaussian 분포 $\mathrm{CN}(0, d_{ij}^{-\alpha})$ 를 따른다. 각 노드의 배경 잡음은 독립적인 $\mathrm{CN}(0,1)$ 를 따른다. 본 릴레이 네트워크는 decode-and-forward 기반 시분할 반이중 릴레이와 협력, 통신하며 통신 과정은 두 개의 phase 로 구성된다 (Figure 1). Phase 1 에서는 S 가 R 과 D 에게 신호 X_S를 전송하며, phase 2 에서는 릴레이가 신호를 복호화한 경우 송신 신호 X_R 을 생성하여 forwarding 하고, 복호화에 실패한 경우 phase 2 에서는 신호를 전송하지 않는다. 각 페이지의 길이는 $\mathrm{n}/2$ 로 둔다. 또한 합법적 노드들은 무한대 길이의 보안키를 공유하고 있다고 가정한다.

도청단 W 는 두 phase 를 모두 관측하여 얻은 길이 n의 수신신호 벡터 Z 를 이용해 통신을 탐지한다. 본 논문에서는 저피탐 통신 척도로 통신 발생시의 도청단 수신 신호 Z의 결합분포 Q_Z와 배경 잡음 분포 Q_{N_W}의 n-fold product 사이의 상대 엔트로피 $\mathrm{D}(Q_Z||Q_{N_W}^{\times n})$를 활용한다. 채널의 random 성으로 인해 아래와 같이 양의 상수 δ에 대해 상대 엔트로피의 평균을 척도로 삼는다:

$$\mathrm{E}[\mathrm{D}(Q_Z||Q_{N_W}^{\times n})] \leq \delta$$

이 상대 엔트로피가 작아질수록 도청단의 탐지 실패 확률이 높아지며, 0 에 수렴할 경우 탐지 성공률은 블라인드 테스트 성공률과 같아진다. 따라서 도청단의 수신신호의 분포가 배경잡음 신호의 분포와 유사할 수 있도록 송신 신호를 설계한다.

Ⅲ. Communication Baseline

DF 릴레이 시스템의 동작을 서술하기에 앞서, 송수신단 간의 점대점 저피탐 통신 기법 및 성능을 분석 한다. 블록길이는 n이다. [2]에 따르면 평균 송신파워 $\bar{P}$에 대해 아래와 같은 필요조건식을 얻을 수 있다.

$$\mathrm{D}(Q_Z||Q_{N_W}^{\times n}) \geq n|g_{SW}|^4\bar{P}^2/2$$

양변에 평균을 취하면 다음과 같은 저피탐 척도 및 송신 평균 파워의 상한값을 필요조건으로 얻을 수 있다.

$$\mathrm{E}[\mathrm{D}(Q_Z||Q_{N_W}^{\times n})] \geq n d_{SW}^{-2\alpha}\bar{P}^2$$
$$\bar{P} \leq d_{SW}^{\alpha}\sqrt{\delta/n}.$$

이 필요조건을 만족하는 최적의 코딩 기법은 Gaussian 랜덤 코딩이며 파워를 $d_{SW}^{\alpha}\sqrt{\delta/n}$로 둔다. 부호화율이 γ일 때 정전 확률은 $p_{out}^{P2P} = \Pr(|g_{SD}|^2 P \leq \gamma)$이며, 정전 용량 $\gamma(1-p_{out}^{P2P})$ 을 최대화 하는 부호화율 γ^*는 미분을 통해 $d_{SD}^{-\alpha}P$ 임을 확인할 수 있다. 최종적으로 점대점 저피탐 통신 정전용량은 $(d_{SD}^{-\alpha}/d_{SW}^{-\alpha})\sqrt{\delta/n}\cdot\exp(-1)$이 된다.

S, R 간의 통신은 위와 같이 진행된다. 두 개의 phase 가 끝난 뒤 D 는 각 phase 의 신호를 maximum ratio combining (MRC)를 이용해 결합하고 복호화를 수행한다. 이때의 수신 SNR 은 $|g_{SD}|^2 P_S + |g_{RD}|^2 P_R$이다.

IV. Covertness analysis & Optimization

릴레이 통신의 정전 사건은 R 과 D 가 모두 복호화에 실패하는 경우와 R 이 복호화하여 forwarding 하였으나 D 에서 MRC 복호가 실패하는 경우로 구성된다. 따라서 정전 확률은 다음과 같다.

$$p_{out}^{DF} = p_e^{SR} p_e^{SD} + (1 - p_e^{SR}) p_e^{MRC}$$

다음으로, 저피탐 통신 제약 조건의 closed-form 식을 얻기 위해 제약 조건을 만족하는 충분 조건을 유도하여 자원 최적화의 제약함수로 삼고자 한다. Gaussian 랜덤 코딩을 활용했을 경우, phase 1 에서 도청단의 수신 신호 분포는 Gaussian 분포이다. Phase 2 에서는 R 이 복호화에 성공하여 forwarding 할 수도, 안 할 수도 있으므로 도청단의 수신 신호 분포는 두 Gaussian 분포의 mixture 이다. Gaussian mixture 분포와 Gaussian 분포 간의 상대 엔트로피는 정확히 구하기 어려우므로, 상대 엔트로피의 concavity 를 이용하여 그 상한값을 구하고 그 값을 제한하는 충분조건을 활용한다. 이를 반영한 최적화 문제는 다음과 같이 정의된다.

$$\begin{aligned} \max_{P_S, P_r, \gamma} \quad & \frac{\gamma}{2}(1 - p_{out}^{DF}) \\ \text{s.t.} \quad & d_{SW}^{-2\alpha} P_S^2 + \exp\left(-\frac{\gamma}{d_{SR}^{-\alpha} P_S}\right) d_{SW}^{-2\alpha} P_R^2 \le \frac{\delta}{n} \\ & P_S, P_R, \gamma \ge 0 \end{aligned}$$

위 최적화 문제의 목적함수와 제약함수는 복잡한 비볼록 구조를 가진다. 이 문제를 해결하기 위해 먼저 부호화율을 고정한 뒤 송신 파워쌍을 최적화하고 (step 1), 그 다음 파워쌍 값을 고정한 후 부호화율을 최적화하는 것 (step 2)을 목적함수가 수렴할 때까지 반복한다. Step 1 에서 파워쌍을 최적화할 때, 임의의 P_S에 대해서 P_R 은 제약함수의 등호를 만족하는 P_S 에 대한 함수값으로 잡을 수 있으므로 P_S 에 대한 선탐색만을 진행하면 되고, step 2 에서는 부호화율에 대한 선탐색을 하면 된다. 따라서 선탐색을 반복하는 저복잡도 알고리즘으로 비볼록 문제를 해결할 수 있다.

V. Simulation Results

이 장에서는 이전 장에서 정의한 최적화 문제를 해결한 몇가지 시뮬레이션 결과를 제시한다. 시뮬레이션 환경으로는 이차원 좌표계를 고려하였으며 S, D, W 의 위치는 각각 (-11, 0), (11, 0), (-0, -11)이다. 네 꼭지점이 (-11, 11), (11, 11), (11, -11), (-11, -11)인 사각형 안에서 릴레이의 위치를 바꾸어가며 통신 성능을 분석하였다. Figure 2 는 저피탐 통신의 성능을 2 차원 그래프로 나타낸 것이며, Figure 3 은 릴레이 통신과 점대점 통신의 성능을 비교한 그래프이다. Figure 3 에서 파란색 영역은 DF 릴레이 기법이 점대점 통신보다 성능이 더 좋은 영역이며, 붉은색 영역은 점대점 통신의 성능이 더 좋은 영역이다. 릴레이 기법과 점대점 통신 기법은 서로 경쟁적인 성능을 가지며, 해당 시뮬레이션 결과를 통해 릴레이의 사용 유무와 활용 위치 등을 전략적으로 고려할 수 있다.

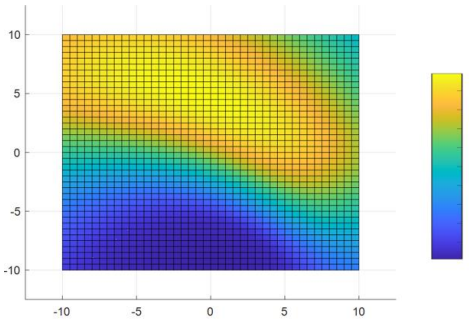

Figure 2 정전 채널 용량

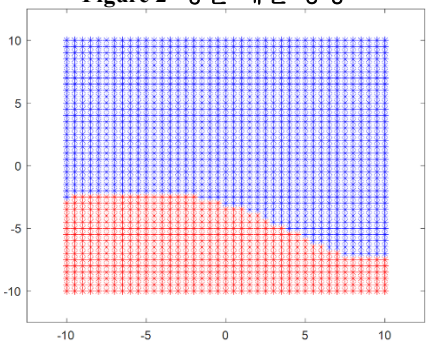

Figure 3 릴레이 기법 우수 (파란색), 점대점 기법 우수 (빨간색)

VI. Conclusion

본 논문에서는 반이중 릴레이가 존재하는 블록 페이딩 릴레이 채널에서의 저 피탐지 확률 통신 기법을 분석하였다. DF 릴레이를 기반으로 하여 자원 분배를 최적화하는 문제를 저복잡도 알고리즘을 제안하여 해결하였다. 또한 다양한 릴레이 위치에 대해서 시뮬레이션을 통해 성능을 분석하고 이를 점대점 통신 기법과 비교하였다.

ACKNOWLEDGMENT

본 연구는 정부 (과학기술정보통신부)의 재원으로 한국연구재단의 지원 (No, 2022R1A2C2092151) 및 정부 (과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원 (No, 00229524)을 받아 수행된 연구임.

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

[3] K.-H. Cho and S.-H. Lee, “Treating interference as noise is optimal for covert communication over interference channels,” IEEE Tran. on Information Forensics and Security, vol. 16, pp. 322-332, 2021.

[4] K. S. Kumar Arumugam, M. R. Bloch, and L. Wang, “Covert communication over a physically degraded relay channel with non-colluding wardens,” in 2018 IEEE ISIT, June 2018, pp. 766-770.