논문 21-46-09-07 The Journal of Korean Institute of Communications and Information Sciences '21-09 Vol.46 No.09
https://doi.org/10.7840/kics.2021.46.9.1403

폴리블록 외부 근사 알고리즘을 이용한 무선 감시 통신 최적화

문 지 환◆

Optimization of Wireless Surveillance Systems with the Polyblock Outer Approximation Algorithm

Jihwan Moon◆

요 약

본 논문에서는 불법적인 용도로 통신을 활용할 것으로 의심되는 한 쌍의 송수신기를 감청하는 보안 통신 시스템을 다룬다. 하나의 중앙 감시 노드가 다수의 중계 노드를 통해 감청을 시도하며 각 중계 노드는 획득한 정보를 중앙 감시 노드에 전달하거나 의심스러운 송수신기가 사용하는 통신 속도가 감청 통신 링크가 수용할 수 있을 정도로 낮아질 수 있도록 재밍을 발생시킨다. 폴리블록 외부 근사 알고리즘을 활용하여 통해 감청 통신 속도를 최대화하는 방법을 제시하며 실험 결과를 통해 성능 이득을 확인한다.

Key Words : Physical layer security, proactive eavesdropping, wireless surveillance, cooperative jamming, node selection

ABSTRACT

In this paper, we study a wireless surveillance system on a pair of suspicious users. One central monitor eavesdrops on the suspicious users with the aid of multiple intermediate nodes. Each intermediate node either forwards intercepted messages to the central monitor or broadcasts jamming so that the suspicious users are induced to lower their data rate such that the eavesdropping link can tolerate. In this manner, the central monitor can successfully decode the information. The polyblock outer algorithm-based optimization method is proposed, and the simulation results verify its effectiveness.

Ⅰ. 서 론

무선 통신[1]을 안전하게 사용하기 위한 보안 기술이 학계 및 산업계로부터 큰 관심을 받고 있다. 특히 물리 계층에서의 보안 기술은 크게 두 가지 방향으로 개발되고 있다. 하나는 주변 도청자가 정상적으로 디코딩할 수 없도록 하는 보안 통신 기술[2]이고, 또 다른 방향은 바로 무선 감시 시스템이다[3]. 기존 보안 통신의 관점과 반대 목적을 가지고 있는데, 우리가 감청자가 되어 불법 또는 범죄를 일으킬 것으로 의심되는 사용자들이 서로 어떤 정보를 주고 받는지 감시하는 시스템을 일컫는다. 실제 미국 Terrorist Surveillance Program(TSP)과 같이 테러 및 공공 재난 예방을 위한 정부 차원의 전략에 유용하게 활용될 수 있다.

본 논문에서는 불법적인 용도로 통신을 활용할 것으로 의심되는 한 쌍의 송수신기를 감청하는 보안 통신 시스템을 다룬다. 하나의 중앙 감시 노드가 다수의 중계 노드를 통해 감청하며 각 중계 노드는 획득한 정보를 중앙 감시 노드에 전달하거나 의심스러운 송수신기가 사용하는 통신 속도가 감청 통신 링크가 수용할 수 있을 정도로 낮아질 수 있도록 재밍을 발생시킨다. 폴리블록 외부 근사 알고리즘을 통해 감청 통신 속도를 최대화하는 방법을 제시하며 실험 결과를 통해 성능 이득을 확인한다.

Ⅱ. 본 론

2.1 시스템 모델

그림 1은 본 논문에서 고려하는 시스템 모델을 도시한다. 모든 노드는 하나의 안테나를 가지고 있으며 의심되는 송신 노드 T가 수신 노드 R에게 정보를 전달한다. 이때 중앙 감시 노드 C는 T와 R로부터 존재를 감추기 위해 원거리에서 K개의 감청 중계 노드 E_1, ..., E_K를 통해 정보를 획득한다. 송신 노드 T와 중앙 감시 노드 C 사이에는 직접적인 통신 링크가 없음을 가정한다. 동시에 L개의 재밍 중계 노드 J_1, ...,

※ 이 논문은 조선대학교 학술연구비의 지원을 받아 연구되었음(2020)

◆ First Author : (ORCID:0000-0002-9812-7768)Department of Information and Communication Engineering, Chosun University, Gwangju 61452, South Korea, anschino@chosun.ac.kr, 조교수, 정회원

논문번호 : 202107-172-A-LU, Received July 20, 2021; Revised July 28, 2021; Accepted August 3, 2021

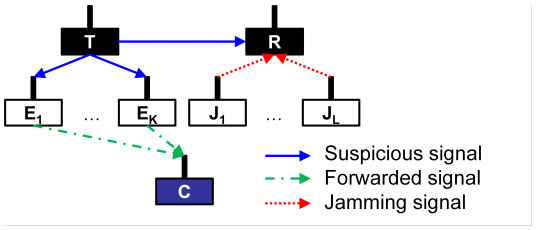


그림 1. 시스템 모델
Fig. 1. System model

J_L는 필요에 따라 의심스러운 송수신기의 통신 속도가 감청 통신 링크 최대 수용치 이하로 낮아지게끔 재밍을 수행한다.

2.1.1 감청 중계 노드와 중앙 감시 노드

본 논문에서는 [4]와 같이 협력 재밍을 가정한다. 즉, 중앙 감시 노드, 감청 중계 노드, 재밍 중계 노드 사이에는 재밍 신호 및 순서가 미리 약속되어 있어 수신 시 재밍 신호를 제거할 수 있음을 고려한다. 따라서 k 번째 감청 중계 노드의 수신 신호는

$$y_{E_k} = h_{TE_k} x_T + z_{E_k} \tag{1}$$

이며 h_{XY}는 노드 X와 노드 Y 사이 Rayleigh 무선 채널, $x_X \sim CN(0, P_T)$는 노드 X의 송신 정보, P_T는 의심되는 송신자의 송신 전력, $z_X \sim CN(0, \sigma_X^2)$는 노드 X에서 발생하는 잡음, σ_X^2는 잡음 z_X의 전력을 뜻한다.

한편 k 번째 감청 중계 노드가 중앙 감시 노드에게 보내는 정보를 $x_{E_k} \sim CN(0, P_{E_k})$라고 했을 때 중앙 감시 노드에 전달되는 신호는

$$y_C = \left(\sum_{k=1}^{K} h_{E_k C} x_{E_k} \right) + z_C \tag{2}$$

로 표현된다. 송신 노드 T와 중앙 감시 노드 C 사이에는 직접적인 통신 링크가 없다고 가정했기 때문에 x_T가 직접 수신되지 않는다. 하지만 수식 (2)를 바탕으로 감청 중계 노드 E_k와 중앙 감시 노드 C 사이 전달 링크에서 x_{E_k}를 정보 이론적으로 오류 없이 복구할 수 있는 최대 달성 가능 전송 속도는

$$\bar{r}_{E_k} = \log_2 \left(1 + \frac{P_{E_k} |h_{E_k C}|^2}{\left(\sum_{n \neq k}^{K} P_{E_n} |h_{E_n C}|^2 \right) + \sigma_C^2} \right) \tag{3}$$

로 제한된다. 따라서 [1]에서 소개된 압축 전달 기술을 사용하면 감청 중계 노드 E_k는 자신이 수신했던 y_{E_k}를 더 적은 비트로 압축하여 보냄으로써 수식 (3)의 제약 조건을 더 수월하게 만족시킬 수 있다. 다만 압축을 했기 때문에 중앙 감시 노드 C가 y_{E_k} 복구 시 필연적으로 추가적인 잡음 $q_{E_k} \sim CN(0, Q_{E_k})$을 겪게 되며 그에 따라 최종적으로 중앙 감시 노드 C가 압축 해제하는 신호는

$$\hat{y}_{E_k} = y_{E_k} + q_{E_k} = \left(h_{TE_k} x_T + z_{E_k} \right) + q_{E_k} \tag{4}$$

이다. 이때 y_{E_k}에 대한 전송 속도는

$$\log_2 \left(1 + \frac{E\left[|y_{E_k}|^2 \right]}{Q_{E_k}} \right) \tag{5}$$

으로 나타낼 수 있다.

마지막으로 중앙 감시 노드 C가 압축 해제한 신호 $\hat{y}_{E_1}, \ldots, \hat{y}_{E_K}$를 한 번에 복구하게 되면

$$\begin{bmatrix} \hat{y}_{E_1} \\ \vdots \\ \hat{y}_{E_K} \end{bmatrix} = \begin{bmatrix} h_{TE_1} \\ \vdots \\ h_{TE_K} \end{bmatrix} x_T + \begin{bmatrix} z_{E_1} \\ \vdots \\ z_{E_K} \end{bmatrix} + \begin{bmatrix} q_{E_1} \\ \vdots \\ q_{E_K} \end{bmatrix} = h_{TE} x_T + z_E + q_E \tag{6}$$

이고 전체 정보 x_T에 대한 달성 가능 전송 속도는

$$r_C = \log_2 \left| I + P_T Z^{-1} h_{TE} h_{TE}^H \right| \tag{7}$$

이며 $Z = diag(\sigma_{E_1}^2 + Q_{E_1}, \ldots, \sigma_{E_K}^2 + Q_{E_K})$이다.

2.1.2 의심되는 수신 노드

의심되는 수신 노드에 수신되는 신호는

$$y_R = h_{TR} x_T + \left(\sum_{l=1}^{L} h_{J_l R} x_{J_l} \right) + Z_R \tag{9}$$

이고 달성 가능 전송 속도는

$$r_R = \log_2 \left(1 + \frac{|h_{TR}|^2 P_T}{\left(\sum_{l=1}^{L} |h_{J_l R}|^2 P_{J_l} \right) + \sigma_R^2} \right) \tag{10}$$

로 쓸 수 있다.

2.2 감청 통신 속도 최대화

위를 바탕으로 감청 통신 속도 최대화 문제는

$$\begin{aligned}\max_{K_E,K_J,\{Q_{E_k}\},\{P_{J_l}\},\{P_{E_k}\}} \quad & r_R,\\ s.t. \quad & r_C \ge r_R,\\ & (5) \le (3), 0 \le P_{E_k} \le \overline{P}_{E_k}, \forall k \in K_E,\\ & 0 \le P_{J_l} \le \overline{P}_{J_l}, \forall l \in K_J\end{aligned}$$

으로 정립된다. 목적 함수가 중앙 감시 노드의 전송 속도 r_C가 아닌 의심되는 송수신 노드의 전송 속도인 r_R인 이유는 실질적으로 감청되는 정보는 의심되는 송수신 노드 간 전송되는 정보이고 이는 r_R을 따르기 때문이다. 따라서 중앙 감시 노드 C는 첫 번째 제약 조건처럼 r_C를 r_R보다 높게 유지하여 의심되는 송수신 노드의 전송 속도를 수용할 수 있으면 충분하다. 나아가 K_E와 K_J는 집합 변수로서 각각 감청 중계 노드로 사용할 노드와 또는 재밍 중계 노드로 사용할 노드를 포함한다.

2.3 폴리블록 외부 근사 알고리즘

감청 통신 속도 최대화 문제는 비볼록 문제이지만 P_{E_k}와 P_{J_l}가 서로 독립적이기 때문에 고정된 집합 K_E, K_J에 대해 두 단계 풀이로 접근할 수 있다. 먼저 중앙 감시 노드 C에서의 r_C를 최대화하는 문제 (P1)을 해결하고 구해진 최적의 P_{E_k} 값에 대해 감청 통신 속도 r_R을 최대화하는 문제 (P2)를 풂으로써 원래 문제의 목표를 해결할 수 있다.

$$\begin{aligned}&(P1):\\ &\max_{\{P_{E_k}\}} \quad r_C\left(\{P_{E_k}\}\right)\\ &s.t. \quad P_{E_k} \le \overline{P}_{E_k}, \forall k \in K_E\\ &(P2):\\ &\max_{\{P_{J_l}\}} \quad r_R\left(\{P_{J_l}\}\right)\\ &s.t. \quad r_C\left(\{P_{E_k}\}\right) \ge r_R\left(\{P_{J_l}\}\right)\\ &\qquad 0 \le P_{J_l} \le \overline{P}_{J_l}, \forall l \in K_J\end{aligned}$$

한편 (P1)의 r_C는 (7)에 의해 각 전달 링크의 신호 대 잡음비에 대해 단조 증가 함수이며 각 신호 대 잡음비는 표준 집합(normal set)이기에 폴리블록 외부 근사 알고리즘[5]으로 최적화될 수 있다. 또한 (P2)는 이분법(bisection) 알고리즘에 의해 해를 찾을 수 있다.

2.4 저복잡도 감청/재밍 선택 알고리즘

K_E와 K_J를 위한 전역 탐색은 복잡도가 높다. 재밍 중계 노드는 최소한으로 유지하는 것이 감청 속도에 유리함을 이용해 다음의 알고리즘을 제시한다.

초기화: $K_J = \oslash$

반복:

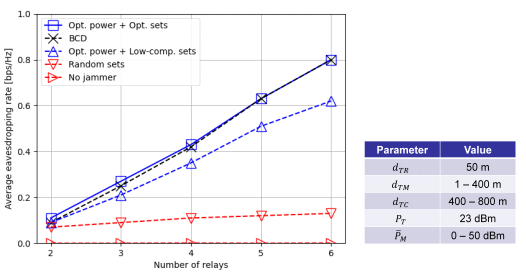
(P1)과 (P2)를 시도하여 해 존재 시 종료.

그렇지 않으면 감청 중계 노드 중 수신 노드와의 채널 이득이 가장 큰 노드를 K_J에 편입.

Ⅲ. 실험 결과 및 결론

그림 2는 중계 노드 개수에 따른 평균 감청 통신 속도 성능을 나타낸다.

"Opt. power + Opt. sets"는 II-3절에서 기술한 두 단계 풀이 방법과 전역 탐색 K_E, K_J를 이용한 성능이고 "BCD"는 기존 잘 알려진 반복성 알고리즘 Block coordinate descent를 $\{P_{E_k}\}$, $\{P_{J_l}\}$에 대해 사용했을 때의 성능이다. 또한 "Low-comp. sets"는 II-4절에서 제안한 저복잡도 감청/재밍 선택 알고리즘의 성능이다. 같은 성능이지만 "BCD"는 여러 번 반복하고 제안하는 "Opt. power + Opt. sets"는 두 단계만을 필요로 하기에 복잡도 측면에서 장점이 크다. 또한 중계 노드의 개수가 늘어날수록 감청 통신 속도가 증가하고 있음을 알 수 있다.



Parameter	Value
d_{TR}	50 m
d_{TM}	1 – 400 m
d_{TC}	400 – 800 m
P_T	23 dBm
$\bar{P}_M$	0 – 50 dBm

그림 2. 중계 노드 개수에 따른 평균 감청 통신 속도
Fig. 2. Average eavesdropping rate versus relays

References

[1] Y. Jeon, S.-H. Park, C. Song, J. Moon, S.

Maeng, and I. Lee, "Fronthaul designs with self-interference mitigation for full-duplex cloud radio access networks," *2017 Winter Conf. KICS*, Jan. 2017.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[3] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over Rayleigh fading channels," *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 80-83, Feb. 2016.

[4] J. Moon, H. Lee, C. Song, S. Kang, M. Kim, and I. Lee, "Full-duplex spoofing relays for wireless surveillance with inter-relay interference suppression," *VTC2020-Spring*, 2020.

[5] L. Liu, R. Zhang, and K. Chua, "Achieving global optimality for weighted sum-rate maximization in the k-user gaussian interference channel with multiple antennas," in *IEEE Trans. Wireless Commun.*, vol. 11, no. 5, pp. 1933-1945, May 2012.