레터논문 (Letter Paper)
방송공학회논문지 제21권 제1호, 2016년 1월 (JBE Vol. 21, No. 1, January 2016)
http://dx.doi.org/10.5909/JBE.2016.21.1.105
ISSN 2287-9137 (Online) ISSN 1226-7953 (Print)

다수의 중계기와 도청자가 존재하는 협력 재밍 네트워크를 위한 중계기 선택 기법

최 용 윤[a)‡], 이 재 홍[a)]

Relay Selection for Two-hop Cooperative Jamming Network with Multiple Eavesdroppers

Yongyun Choi[a)‡] and Jae Hong Lee[a)]

요 약

본 논문에서는 다수의 중계기와 다수의 도청자가 존재하는 협력 재밍 네트워크를 다룬다. 다수의 중계기 중 하나의 중계기가 선택되어 증폭 후 재전송 기법으로 총 두 단계를 통해 수신기에 신호를 전송한다. 도청자의 신호 수신을 방해하기 위해 첫 번째 단계에서 수신기가 재밍 신호를 전송하며, 두 번째 단계에서 송신기가 재밍 신호를 전송한다. 이러한 시스템의 보안 전송률을 수식적으로 분석하며, 사용가능한 채널 정보에 따라 최적의 중계기 선택 기법을 각각 제시한다. 모의실험을 통해 제시한 중계기 선택 기법의 성능이 임의의 중계기 선택 기법에 비해 향상됨을 확인하였다.

Abstract

In this paper, a cooperative jamming network with multiple relays and multiple eavesdroppers is investigated. Among the relays, one best relay is selected to amplify and forward the signal to destination through two phases. To confuse eavesdroppers, the destination transmits a jamming signal in the first phase and the source transmits jamming signal in the second phase. Secrecy rate of this system is derived, and based on the available channel state information (CSI), relay selection schemes are proposed, respectively. Numerical results show that the performance of the proposed relay selection scheme outperforms than that of random relay selection scheme.

Keyword : physical layer security, cooperative jamming, eavesdropper, relay selection, secrecy rate

a) 서울대학교 전기정보공학부, 뉴미디어통신공동연구소(Department of Electrical and Computer Engineering and INMC, Seoul National Univ.)
‡ Corresponding Author : 최용윤(Yongyun Choi)
E-mail: yongyun@snu.ac.kr
Tel: +82-2-880-7045
ORCID: http://orcid.org/0000-0002-8984-0262
※이 논문은 2014, 2015년도 정부(미래창조과학부)의 재원으로 한국연구 재단의 지원을 받아 수행된 연구임(No. 2011-0017437, 2009-0083495, 2015R1D1A1A01057563).
Manuscript received Otober 23,2015; Revised January 21, 2016; Accepted January 21, 2016

Ⅰ. 서 론

물리 계층 보안 통신(physical layer security)은 별다른 암호화(encryption) 기법이 필요하지 않다는 점에서 장점이 있으며, 최근에 활발히 연구되고 있다[1]. 보안 통신을 달성하기 위한 여러 방법 중 협력 재밍(cooperative jamming)은 정보가 담긴 신호를 보내는 노드 외에 협력하는 노드가 존재하여 재밍 신호를 전송하는 기법이다[2]. 재밍 신호만을 전송하는 재머(jammer) 이외에도 중계기, 수신기 등이 협력하는 노드로 동작할 수 있으며, 이에 대한 연구가 활발히 진행되고 있다[3].

최근 중계기가 존재하는 협력 통신 네트워크에서 신호를 받는 수신기가 재밍 신호를 전송하는 방법에 대한 연구가 진행되고 있다[4]. [5]에서는 하나의 중계기와 하나의 도청자가 존재하는 시스템에서 수신기가 다수의 안테나를 이용해 재밍 신호를 빔포밍하는 기법을 제시하고 그 성능을 분석하였다. 하지만 수신기 뿐만 아니라 송신기에서도 재밍 신호를 전송하여 그 성능을 더욱 향상시키는 방법에 대한 연구 및 분석은 현재까지 이루어지지 않았다.

본 논문에서는 다수의 중계기와 다수의 도청자가 존재하는 협력 재밍 네트워크를 다룬다. 모든 채널 정보를 정확히 아는 경우와 도청자로의 채널 정보를 모르는 경우 각각에 대해 최적의 중계기 선택 기법을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 시스템 모델을 설정하고 시스템의 보안 전송률(secrecy rate)을 수식적으로 유도한다. 3장에서는 사용가능한 채널 정보에 따른 최적의 중계기 선택 기법을 각각 제시한다. 4장에서는 모의실험을 통해 제시한 중계기 선택 기법의 성능을 분석하며, 마지막으로 5장에서는 본 논문에 대한 결론을 맺는다.

Ⅱ. 시스템 모델 및 보안 전송률 분석

1. 시스템 모델

본 논문에서는 그림 1과 같은 협력 재밍 네트워크를 가정한다. 하나의 송신기(S)와 수신기(D)가 존재하고 K개의 중계기(R) 중 하나의 중계기가 증폭 후 재전송 기법을 사용하여 통신을 돕는다고 가정한다. 또한 L개의 도청자(E)가 존재하여 송신기와 중계기에서 보내는 신호를 도청한다고 가정한다. 모든 노드는 하나의 안테나를 가지고 있다고 가정하고, 송신기와 수신기 사이의 직접적인 통신은 일어나지 않는다고 가정한다. 그림 1에 표기한 것과 같이 h_{ij}는 i와 j 사이의 채널 계수를 나타내고, 모든 채널은 서로 독립적인 레일리 페이딩으로 모델링하였다.

신호 전송은 총 두 단계로 이루어진다. 첫 번째 단계에서 송신기는 중계기에게 데이터가 담긴 신호를 전송하며, 동시에 수신기는 도청자가 이 신호를 엿듣는 것을 막기 위해 재밍 신호를 전송한다. 첫 번째 단계에서 k번째 중계기와 l번째 도청자가 받는 신호는 각각 아래와 같다.

$$y_{R_k} = \sqrt{P_S^{(1)}} h_{SR_k} s + \sqrt{P_D} h_{DR_k} z_D + n_{R_k} \quad (1)$$

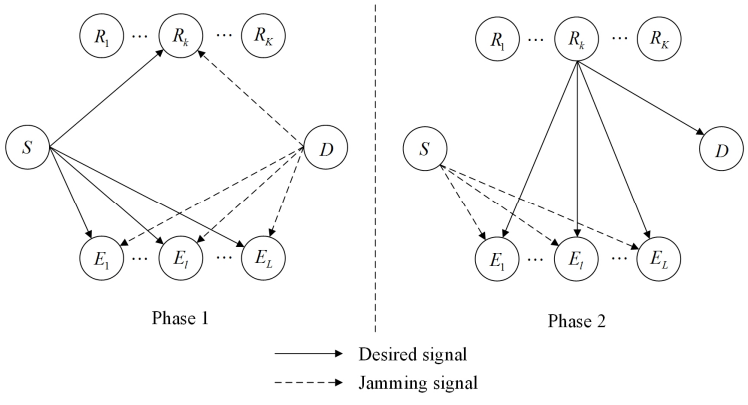

그림 1 . 협력 재밍 네트워크에서의 시스템 모델
Fig. 1. System model for cooperative jamming networks

$$y_{E_l}^{(1)} = \sqrt{P_S^{(1)}} h_{SE_l} s + \sqrt{P_D} h_{DE_l} z_D + n_{E_l}^{(1)} \quad (2)$$

여기서 $P_S^{(1)}$과 P_D는 각각 송신기와 수신기의 첫 번째 단계에서의 송신 전력이며, s는 단위 전력을 가지는 송신 신호, z_D는 수신기의 단위 전력 재밍 신호이다. n_{R_k}와 $n_{E_l}^{(1)}$은 각각 k번째 중계기와 l번째 도청자의 첫 번째 단계에서의 가산 백색 가우스 잡음(AWGN: additive white Gaussian noise)이다.

두 번째 단계에서 중계기는 증폭 후 재전송(amplify and forward) 방법을 통해 첫 번째 단계에서 받은 신호를 전송하며, 송신기는 재밍 신호를 전송한다. 두 번째 단계에서 수신기와 l번째 도청자가 받는 신호는 각각 아래와 같다.

$$y_D = g_k h_{R_k D}\left(\sqrt{P_S^{(1)}} h_{SR_k} s + \sqrt{P_D} h_{DR_k} z_D + n_{R_k}\right) + n_D \quad (3)$$

$$y_{E_l}^{(2)} = g_k h_{R_k E_l}\left(\sqrt{P_S^{(1)}} h_{SR_k} s + \sqrt{P_D} h_{DR_k} z_D + n_{R_k}\right) + \sqrt{P_S^{(2)}} h_{SE_l} z_S + n_{E_l}^{(2)} \quad (4)$$

여기서 $P_S^{(2)}$는 송신기의 두 번째 단계에서의 송신 전력이며, z_S는 송신기의 단위 전력 재밍 신호, n_D와 $n_{E_l}^{(2)}$은 수신기와 l번째 도청자의 두 번째 단계에서의 가산 백색 가우스 잡음이다. g_k는 k번째 중계기의 증폭계수이며 그 값은 아래와 같다.

$$g_k = \sqrt{\frac{P_{R_k}}{P_S^{(1)}\left|h_{SR_k}\right|^2 + P_D\left|h_{DR_k}\right|^2 + N_0}} \quad (5)$$

여기서 P_{R_k}는 k번째 중계기의 송신 전력이다. 수신기는 두 번째 단계에서 받은 신호에서 자신이 보낸 재밍 신호를 제거하며, 제거한 후의 신호는 다음과 같다.

$$y_D' = g_k h_{R_k D}\left(\sqrt{P_S^{(1)}} h_{SR_k} s + n_{R_k}\right) + n_D \quad (6)$$

이러한 시스템 모델에 대하여 secrecy rate를 구해 본다.

2. 보안 전송률 분석

수식 (6)을 통해 계산한 수신기의 신호대 잡음비(SNR)는 아래와 같다.

$$\gamma_{D,k} = \frac{P_S^{(1)} P_{R_k}\left|h_{SR_k}\right|^2\left|h_{R_k D}\right|^2}{N_0\left\{\left(P_{R_k} + P_D\right)\left|h_{R_k D}\right|^2 + P_S^{(1)}\left|h_{SR_k}\right|^2 + N_0\right\}} \quad (7)$$

수식 (2)와 (4)를 통해 계산한 l번째 도청자의 각 단계에서의 신호대 잡음비는 아래와 같다.

$$\gamma_{E_l}^{(1)} = \frac{P_S^{(1)}\left|h_{SE_l}\right|^2}{P_D\left|h_{DE_l}\right|^2 + N_0} \quad (8)$$

$$\gamma_{E_l}^{(2)} = \frac{\dfrac{P_S^{(1)} P_{R_k}\left|h_{SR_k}\right|^2\left|h_{R_k E_l}\right|^2}{P_D\left|h_{DR_k}\right|^2 + P_S^{(1)}\left|h_{SR_k}\right|^2 + N_0}}{\dfrac{P_{R_k}\left|h_{R_k E_l}\right|^2\left(P_D\left|h_{DR_k}\right|^2 + N_0\right)}{P_D\left|h_{DR_k}\right|^2 + P_S^{(1)}\left|h_{SR_k}\right|^2 + N_0} + P_S^{(2)}\left|h_{SE_l}\right|^2 + N_0} \quad (9)$$

각 도청자가 최대비 합성(maximal ratio combining)을 사용한다고 가정하면, l번째 도청자의 신호대 잡음비는 아래와 같이 정의할 수 있다.

$$\gamma_{E_l} = \gamma_{E_l}^{(1)} + \gamma_{E_l}^{(2)} \quad (10)$$

식 (7)과 (10)를 통해 이 시스템의 보안 전송률은 아래와 같이 구할 수 있다.

$$R = \left[\frac{1}{2} log_2\left(\frac{1+\gamma_{D,k}}{1+\max(\gamma_{E_1},\cdots,\gamma_{E_L})}\right)\right]^+ \quad (11)$$

여기서 $[x]^+ = \max(0, x)$이다.

Ⅲ. 중계기 선택 기법

사용가능한 채널 정보의 양에 따라 두 가지의 경우를 다룬다. 첫 번째 경우는 모든 채널 정보가 사용가능한 경우이며, 두 번째 경우는 전체 채널 정보 중 도청자로의 채널 정보를 모르는 경우이다. 본 논문에서는 이러한 두 경우에 대한 중계기 선택 기법을 각각 제시한다.

1. 모든 채널 정보가 사용가능한 경우

모든 채널 정보가 사용가능한 경우, 시스템의 보안 전송률을 정확하게 알 수 있으므로, 이 경우의 중계기 선택 기법은 다음과 같이 구할 수 있다.

$$k^* = \arg\max \left[\frac{1}{2} log_2 \left(\frac{1+\gamma_{D,k}}{1+\max(\gamma_{E_1},\cdots,\gamma_{E_L})} \right) \right]^+ \quad (12)$$

2. 도청자로의 채널 정보를 모르는 경우

도청자로의 채널 정보를 모르는 경우, 시스템의 보안 전송률을 정확히 알 수 없다. 따라서 이 경우의 최적의 중계기 선택 기법은 수신기의 신호대 잡음비를 최대로 하는 기법이며, 이는 다음과 같이 구할 수 있다.

$$k^* = \arg\max \gamma_{D,k} \quad (13)$$

Ⅳ. 모의실험

모의실험에서는 모든 채널 계수의 분산을 1로 가정하였다.

그림 2는 다양한 K 값에 대한 각 중계기 선택 기법의 보안 전송률을 비교하고 있다. 이 때의 도청자 수는 3으로 설정하였으며, 성능 비교를 위해 임의선택(random selection) 기법에 대한 보안 전송률을 함께 나타내었다. 그림을 보면 알 수 있듯이, 본 논문에서 제시한 두 기법이 임의 선택 기법에 비해 높은 보안 전송률을 달성함을 볼 수 있다. 또한, 모든 채널 정보가 사용가능한 경우가 도청자로의 채널 정보를 모르는 경우에 비해 더 높은 보안 전송률을 달성하지만 그 차이가 미비함을 확인할 수 있다. 또한, 중계기의 수가 더 많을수록 높은 보안 전송률을 달성함을 볼 수 있다.

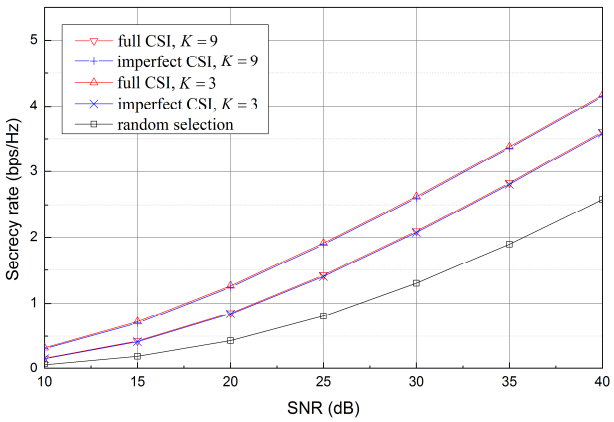

그림 2. 다양한 K 값에 대한 각 기법의 보안 전송률 비교, $L=3$
Fig. 2. Secrecy rate of various schemes versus SNR using different K, $L=3$

Ⅳ. 결 론

본 논문에서는 증폭 및 재전송 기법을 사용하는 다수의 중계기와 다수의 도청자가 존재하는 협력 재밍 네트워크에서 송신기 및 수신기가 도청자의 신호 수신을 막기 위해 재밍 신호를 전송할 때의 성능 분석을 하였다. 시스템의 보안 전송률을 수식적으로 분석하였으며, 사용 가능한 CSI에 따라 최적의 중계기 선택 기법을 각각 제시하였다. 또한 모의실험을 통해 제시한 중계기 선택 기법의 성능을 확인하였다.

참 고 문 헌 (Reference)

[1] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” IEEE Trans. Inf. Theory., vol. 54, no. 6, pp. 2470 - 2492, June 2008.

[2] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” IEEE Trans. Wireless Commun., vol. 7, no. 6, pp. 2180-2189, June 2008.

[3] J. Huang and A. Swindlehurst, “Cooperative jamming for secure communications in MIMO relay networks,” IEEE Trans. Signal Process., vol. 59, no. 10, pp. 4871 - 4884, Oct. 2011.

[4] Y. Liu, A. P. Petropulu, and H. V. Poor, “Joint decode-and-forward and jamming for wireless physical layer security with destination assistance,” in Proc. Asilomar Conference on Signals, Systems and Computer (ASILOMAR’11), Pacific Grove, USA, Nov. 2011.

[5] J. Huang and A. L. Swindlehurst, “Cooperative jamming for secure communications in MIMO relay networks,” IEEE J. Sel. Areas Commun., vol. 59, no. 10, pp. 4871 - 4884, Oct. 2011.