논문 22-47-08-06 The Journal of Korean Institute of Communications and Information Sciences '22-08 Vol.47 No.08
https://doi.org/10.7840/kics.2022.47.8.1063

비신뢰 중계망에서 물리계층 보안을 위한 중계기 선택의 다중사용자 다양성 분석

방 인 규◆, 김 태 훈*, 임 진 택°

Analysis of Relay Selection for Multiuser Diversity of Physical-Layer Security in Untrusted Relay Networks

Inkyu Bang◆, Taehoon Kim*,
Jin-Taek Lim°

요 약

본 논문에서는 다수의 비신뢰 중계기가 존재하는 중계망에서 중계 프로토콜과 중계기 선택에 따른 물리계층 보안 성능을 분석한다. 구체적으로 인공잡음(artificial noise) 전송 및 상쇄를 포함하는 보안 중계 상황에서 송신기-중계기 또는 중계기-수신기 사이의 무선 채널 상태에 따른 임계 값(threshold value) 기반의 중계기 선택 기법을 제안하고 보안 전송률(secrecy rate)에 미치는 영향을 모의실험을 통해 분석한다. 또한 각각의 중계기 선택 방법에서 인공잡음 생성 전력에 따른 보안 전송률을 분석한다.

Key Words : physical-layer security, multiuser diversity, untrusted relay, relay selection, artificial noise

ABSTRACT

In this paper, we investigate the secrecy rate of relay selection schemes in untrusted relay networks. We consider secure relaying protocol using artificial noise transmission with power control and propose a threshold-based relay selection scheme. Through simulations, we evaluate the secrecy rate of the proposed scheme compared with relay selection schemes considering channel state information of the transmitter-relay pair or relay-receiver pair.

Ⅰ. 서 론

물리계층 보안(physical-layer security)은 무선 채널의 임의성(randomness)을 물리계층 기술과 함께 활용하여 무선 신호에 대한 보안을 강화하는 연구 분야이다. 무선 통신 시스템의 진화·발전과 함께 무선네트워크 보안(wireless network security)은 더욱 중요해지고 있으며, 이러한 흐름 속에 물리계층 보안은 차세대 통신(예: 6G) 보안을 위한 하나의 후보기술로 논의되고 있다[1].

6G 등의 차세대 통신에서는 기지국 등의 인프라를 활용한 무선 통신 이외에도 단말 간 직접 통신(device-to-device: D2D), 단말 주변의 무선 기기를 활용한 중계 통신 등 다양한 형태의 무선 통신 시나리오를 고려하고 있다. 최근 물리계층 보안 연구 역시 단일 송·수신기 및 도청기가 존재하는 기본적인 도청 모델뿐만 아니라, 중계기가 존재하는 중계망(relay network)에서의 도청모델 등 다양한 시나리오를 가정하는 연구가 논의되고 있다. 예를 들어, 제한적인 통신환경으로 특정 기기가 D2D 통신을 통해 데이터를 전송할 때, 중계 역할을 하게 되는 기기는 악의적이지는 않지만 완전히 신뢰할 수는 없는(즉, 비신뢰) 기기로 간주할 수 있다. 실제로 물리계층 보안 연구에서는 중계망의 임의의 무선 기기가 중계기로 활용되는 경우 등을 고려하여 중계기를 비신뢰(untrusted) 노드로 간주하고 중계망의 보안성능을 분석하는 연구가 많이 논의되고 있다[2,3]. 그러나 기존 연구[2,3]는 단일 비신뢰 노드가 존재하는 상황을 고려하고 있다. 따라서 다중 비신뢰 노드 환경을 가정할 경우에 활용할 수 있는 다중사용자 다양성(multiuser diversity)의 효과에 대한 관찰이 미흡한 상황이다.

본 논문에서는 송·수신기의 직접 통신이 불가능하

※ 이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2020R1G1A1101176).
※ 이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2020R1F1A1069934).
◆ First Author : (ORCID:0000-0001-7109-1999)Hanbat National University Department of Intelligence Media Engineering, ikbang@hanbat.ac.kr, 조교수, 정회원
° Corresponding Author : (ORCID:0000-0002-9649-0459)Agency for Defense Development, jtlim@add.re.kr, 선임연구원, 정회원
* (ORCID:0000-0002-9353-118X)Hanbat National University Department of Computer Engineering, thkim@hanbat.ac.kr, 조교수, 정회원
논문번호 : 202011-289-A-LU, Received June 6, 2022; Revised June 22, 2022; Accepted June 22, 2022

여 송·수신기 사이의 다수의 무선 기기를 비신뢰 중계기(untrusted relay)로 활용하는 중계망에서, 인공잡음의 생성 전력 및 채널 상태 정보에 따른 임계 값 기반의 중계기 선택 기법을 제안한다. 모의실험을 통해 제안 기법을 포함하여 다양한 중계기 선택 기법에 따른 다중사용자 다양성과 보안 전송률과의 관계를 분석한다.

Ⅱ. 시스템 모델

본 논문에서는 그림 1과 같이 직접(direct) 무선 링크는 존재하지 않는 한 쌍의 송·수신기와 N개의 비신뢰 중계기(untrusted relay)가 존재하는 중계망을 가정한다. 송신기와 수신기 사이의 임의의 무선 기기가 중계기가 될 수 있는 상황을 가정하고 있으며, 악의적인 목적이 없더라도 보안 관점에서 임의의 중계기를 완전히 신뢰할 수 없는 상황을 가정한다. 또한 임의의 기기는 중계기 선택 및 데이터 전송 전에 채널 추정을 위한 파일럿 신호 등을 전송할 수 있다고 가정한다[3]. 송신기는 매 시간 슬롯(time slot)마다 채널 상태 정보(channel state information)에 따라 하나의 중계기를 선택하여 데이터를 전송한다.[1] 여기서, 송신기와 수신기는 다음과 같이 총 두 단계로 구성되는 보안 중계 프로토콜을 사용한다.(n번째 중계기가 선택되었다고 가정)

1단계(data: source → n-th relay): 송신기는 n번째 중계기로 데이터 전송을 하며, 동시에 수신기는 비신뢰 중계기의 도청 가능성을 줄이기 위해 임의잡음(random noise) 형태의 인공잡음을 생성한다.

2단계(data: n-th relay → destination): n번째 중계기는 전달 받은 데이터를 증폭하여(amplifying) 수신기에게 전달한다. 수신기는 1단계에서 생성했던 인공잡음 정보를 이용하여 인공잡음의 효과를 상쇄하고 데이터를 복호한다.

여기서, h_n은 송신기와 n번째 중계기 사이의 채널 계수를 나타내며, g_n는 n번째 중계기와 수신기 사이의 채널 계수를 나타낸다. 각 채널 계수는 하나의 블록(block)에 해당하는 일정 시간 슬롯 동안에는 동일한 값을 유지하지만 블록마다는 독립적으로 변화하는 레일리 블록 페이딩(Rayleigh block fading) 채널 모델을 가정한다[4,5]. 따라서 각 채널 계수는 독립 가우시안 분포를 따르며, $h_n \sim CN(0,\sigma_h^2)$, $g_n \sim CN(0,\sigma_g^2)$이 된다. σ_h^2, σ_g^2는 각 무선링크의 평균 채널 이득 값을 나타내고 분석의 편의를 위해 송신기와 각 중계기(또는 각 중계기와 수신기)는 동일한 평균 채널 이득 값을 가정한다. 따라서 각 채널 이득(즉, $|h_n|^2$, $|g_n|^2$)은 지수 분포(exponential distribution)를 따르며, 확률 밀도 함수(probability density function: PDF)는 다음과 같다.

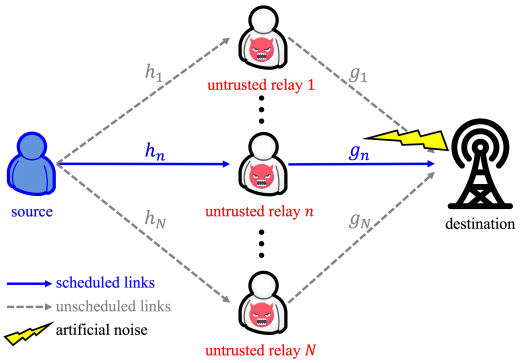

그림 1. 다수의 비신뢰 중계기가 존재하는 중계망 모델
Fig. 1. A relay network consists of multiple untrusted relays and a single transmitter-receiver pair

$$f_{|h_n|^2}(x)=\frac{1}{\sigma_h^2}exp\left(-\frac{x}{\sigma_h^2}\right), \quad (1\text{-}1)$$

$$f_{|g_n|^2}(y)=\frac{1}{\sigma_g^2}exp\left(-\frac{y}{\sigma_g^2}\right). \quad (1\text{-}2)$$

각 채널계수(h_n, g_n)는 두 시간 슬롯 동안은 변하지 않으며 매 데이터 전송마다 독립적으로 변한다.(즉, 한 블록은 두 시간 슬롯으로 구성된다.) n번째 중계기가 선택된다고 가정할 경우, 중계 프로토콜의 1단계와 2단계에서 중계기와 수신기의 수신 신호 대 간섭 및 잡음비(signal-to-interference plus noise ratio: SINR)는 각각 다음과 같이 계산할 수 있다[2].

$$\Gamma_{R,n}(\phi)=\frac{|h_n|^2P_S}{\phi|g_n|^2P_D+\sigma_n^2}, \quad (2\text{-}1)$$

$$\Gamma_{D,n}(\phi)=\frac{G^2|g_n|^2|h_n|^2P_S}{(G^2|g_n|^2+1)\sigma_n^2}, \quad (2\text{-}2)$$

여기서, $\phi\in[0,1]$은 수신기가 생성하는 인공잡음의 전력 비율을 나타내고, σ_n^2은 가산 백색 가우시안 잡음(additive white Gaussian noise: AWGN)의 평균

1) 중계기 선택 방법은 다음 장에서 구체적으로 논의한다.

전력 값을 나타낸다. P는 각 노드의 전송 전력, 아래 첨자 S, R, D는 source, relay, destination을 의미한다. G는 중계기의 증폭 전송에 따른 중계 이득을 나타내며 다음과 같이 계산된다.

$$G=\sqrt{\frac{P_R}{|h_n|^2P_S+\phi|g_n|^2P_D+\sigma_n^2}}. \quad (3)$$

Ⅲ. 중계기 선택 기법 및 인공잡음 생성 전력 비율

본 장에서는 중계망에서 채널 상태 정보에 따른 임계 값 기반의 중계기 선택 기법을 제안하고 모의실험을 통해 그 성능을 분석한다.

3.1 보안 전송률

주어진 블록에서 각 채널계수(h_n, g_n), 선택된 중계기 인덱스(index) n 및 인공잡음 생성 전력 비율 ϕ이 주어졌을 때, 보안 전송률은 수식 (2-1)과 (2-2)를 이용하여 다음과 같이 계산할 수 있다.

$$R_n^{\mathrm{sec}}(\phi)=\left[\frac{\log_2(1+\Gamma_{D,n}(\phi))}{\log_2(1+\Gamma_{R,n}(\phi))}\right]^+, \quad (4)$$

여기서 $[x]^+=\max\{x,0\}$을 나타낸다.

수식 (1-1)과 수식 (1-2)를 활용하여 평균 보안 전송률을 다음과 같이 계산할 수 있다.

$$\overline{R}_n^{\mathrm{sec}}(\phi)=\int_0^{INF}\int_0^{INF}R_n^{\mathrm{sec}}(\phi)f_{|h_n|^2}(x)f_{|g_n|^2}(y)dxdy, \quad (5)$$

수식 (5)의 평균 보안 전송률 값은 모의실험을 통해 수치적으로 계산할 수 있다. 본 논문에서는 중계망에서 보안 전송률을 향상 시킬 수 있는 중계기 선택 기법을 제안하고 분석하는데 초점을 맞추고 있다.[2)]

중계기 선택 방법에 따라 수식 (4)의 보안 전송률 값이 달라진다. 여기서, 송신기와 중계기 또는 중계기와 수신기 사이의 채널 상태 정보(h_n 또는 g_n)를 단순히 활용하는 경우에는 다음의 두 가지 중계기 선택 방법을 생각해 볼 수 있다.

$$n_{SR}^*=\arg\max_{n\in\{1,\cdots,N\}}\left\{|h_n|^2\right\}, \quad (6\text{-}1)$$

$$n_{RD}^*=\arg\max_{n\in\{1,\cdots,N\}}\left\{|g_n|^2\right\}. \quad (6\text{-}2)$$

여기서 수식 (6-1)의 $|h_n|^2$와 수식 (6-2)의 $|g_n|^2$을 최대화 시키는 중계기 선택 방법을 각각 max SR (Source-Relay), max RD (Relay-Destination)으로 명명한다.

3.2 임계 값 기반의 중계기 선택 기법

수식 (6-1)의 max SR 기법과 수식 (6-2)의 max RD 기법은 중계망의 채널 계수를 직관적으로 비교하여 중계기를 선택하는 기법이다. 본 절에서는 중계기 선택에 있어 $|h_n|^2$과 $|g_n|^2$을 종합적으로 고려하는 중계기 선택 기법을 새롭게 제안한다. 제안 기법은 총 두 단계로 구성된다.

1단계($|h_n|^2$ 후보 선별): 송신기는 최적화된 임계 값 η^*을 이용하여 $|h_n|^2\geq\eta^*$ 조건을 만족하는 중계기 인덱스 후보 집합 $\mathcal{N}(\eta^*)$을 선별한다. 1단계 과정은 송신기와 비신뢰 중계기 간의 채널 품질을 보장하기 위한 단계이다. $|h_n|^2$의 값이 클 경우, 송신기의 데이터가 잘 전송될 수 있지만 반대로 비신뢰 중계기로의 데이터 유출 가능성도 커지기 때문에 최적화된 임계 값 η^*을 사용해야 한다.

2단계($|g_n|^2$ 최대화): 1단계를 통해 얻은 중계기 후보 인덱스 집합 $\mathcal{N}(\eta^*)$ 안에서 $|g_n|^2$이 가장 큰 중계기 인덱스를 최종 선택한다. $|g_n|^2$의 값이 클 경우, 최종적으로 중계기를 통해 전달되는 데이터 신호의 수신 이득이 커지기 때문에 보안 성능이 향상된다.

제안 기법에서 사용되는 임계 값은 $[0,4\sigma_h^2]$ 범위를 $\sigma_h^2/100$ 간격으로 나눈 후에 η 값과 이에 대응되는 후보 집합 $\mathcal{N}(\eta)$을 순차적으로 대입하여 중계기를 선택하고 수식 (5)의 평균 보안 전송률 값을 수치적으로 계산하는 방식으로 최적화된 임계 값 η^*를 계산할 수 있다.

또한 수식 (4)의 보안 전송률 값은 중계기 선택 방법이 정해졌을 때, 인공잡음 생성 전력 비율 ϕ 값에 따라 달라지며 최적의 ϕ^* 값은 다음과 같이 계산할 수 있다.

$$\phi^*=\arg\max_{\phi\in[0,1]}\left\{R_n^{\mathrm{sec}}(\phi)\right\}. \quad (7)$$

2) 수식 (5)의 닫힌 형태(closed-form) 표현을 분석하는 것은 본 연구를 확장하는 새로운 연구주제가 될 수 있다.

3.3 성능 평가

중계기 선택에 따른 보안 전송률 향상에 있어 제안 기법과 수식 (6-1), (6-2)의 중계기 선택 기법 그리고 수식 (7)의 인공잡음 최적화의 효과를 분석하기 위해 모의실험을 진행하였다. 모의실험 결과에서 제안 기법은 'proposed'으로 표시하였고 성능비교 및 참고를 위하여 중계기를 임의로 선택하는 방법('random'으로 명명)을 추가로 고려하였다.

그림 2는 $\frac{P_S}{\sigma_n^2}$으로 정의되는 송신기와 중계기 사이의 SNR (signal-to-noise ratio: SNR) 값 변화에 따른 각 중계기 선택 기법의 보안 전송률을 나타낸다. 다중사용자 다양성(multiuser diversity)의 효과를 관찰하기 위하여 중계기의 수가 10인 경우와 100인 경우를 각각 도시화하였으며, $\frac{P_R}{\sigma_n^2}$으로 정의되는 중계기와 수신기의 SNR 값은 15 dB 그리고 $\phi=1$으로 설정하였다. 모든 중계기 선택 기법에 대해서 비신뢰 중계기를 고려하기 때문에 일반적인 중계망에서와는 다르게 보안 전송률이 SNR 값이 증가하더라도 감소하는 것을 확인할 수 있다. 그러나 중계기 수가 10에서 100으로 증가하는 경우 중계기 선택 기법에 따라 다중사용자 다양성의 효과로 얻을 수 있는 성능 이득이 달라지는 것을 확인할 수 있다. 특히 제안 기법은 $|h_n|^2$과 $|g_n|^2$을 종합적으로 고려하기 때문에 $|h_n|^2$과 $|g_n|^2$을 단순히 활용하는 max SR 및 max RD 기법 대비 전 SNR 영역에서 보안 전송률이 우수한 것을 확인할 수 있다.

그림 3는 중계기 수가 100인 상황에서 송신기와 중

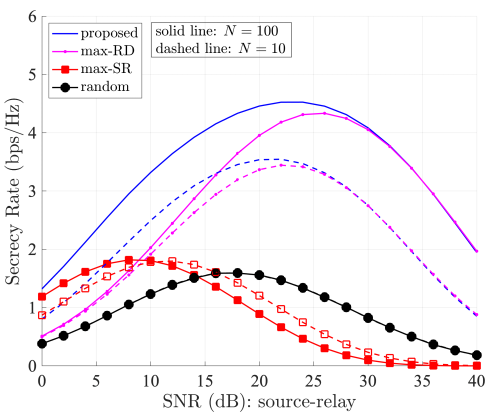

그림 2. 중계기 수와 중계기 선택 기법에 따른 보안 전송률
Fig. 2. Secrecy rate with the number of relays and relay selection schemes

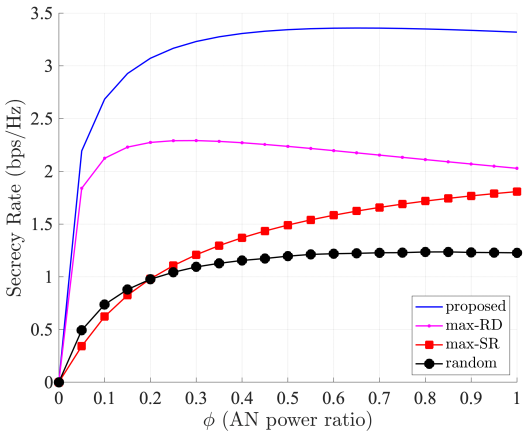

그림 3. 중계기 선택 기법의 인공잡음 생성 전력에 따른 보안 전송률
Fig. 3. Secrecy rate with artificial noise power generation ratio for relay selection schemes

계기, 중계기와 수신기의 SNR 값을 각각 10 dB, 15 dB로 설정했을 때, ϕ값에 따른 각 중계기 선택 기법의 보안 전송률을 나타낸다. 각 중계기 선택 기법에 따라 최적의 인공잡음 생성 전력 비율이 달라지는 것을 확인할 수 있다.[3] 또한 제안 기법의 보안 전송률이 상대적으로 매우 우수한 것을 확인할 수 있다.

Ⅳ. 결 론

본 논문에서는 비신뢰 중계망에서 임계 값 기반의 중계기 선택 기법을 제안하고 중계기 선택 기준과 인공잡음 생성 전력 비율이 보안 전송률에 미치는 영향을 분석하였다. 중계기 선택 기법에 따라 다중사용자 다양성의 활용 정도가 달라지며 이에 따라 보안 전송률의 개선 폭이 달라지는 것을 확인할 수 있었다.

References

[1] P. Porambage, et al., "The roadmap to 6G security and privacy," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094-1122, May 2021. (https://doi.org/10.1109/OJCOMS.2021.3078081)

[2] I. Bang, et al., "Performance analysis of secure relaying protocol against an untrusted

3) 분량 제한으로 송신기와 중계기, 중계기와 수신기의 SNR 값이 10 dB, 15 dB인 경우만 도시하였으나, 다른 SNR 조합에서는 각 기법의 최적의 ϕ^* 값이 달라지는 것을 관찰할 수 있다.

relay node in V2V networks," *J. KICS*, vol. 46, no. 12, Dec. 2021. (https://doi.org/10.7840/kics.2021.46.12.2180)

[3] J.-T. Lim, et al., "Impact of outdated CSI on the secure communication in untrusted in-band full-duplex relay networks," *IEEE Access*, vol. 10, pp. 19825-19835, Feb. 2022. (https://doi.org/10.1109/ACCESS.2022.3151792)

[4] I. Krikidis, et al., "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wirel. Commun.*, vol. 8, no. 10, pp. 5003-5011, Oct. 2009. (https://doi.org/10.1109/TWC.2009.090323)

[5] L. Yang, et al., "Optimal relay selection for secure cooperative communications with an adaptive eavesdropper," *IEEE Trans. Wirel. Commun.*, vol. 16, no. 1, pp. 26-42, Jan. 2016. (https://doi.org/10.1109/TWC.2016.2617328)