논문 21-46-11-06 The Journal of Korean Institute of Communications and Information Sciences '21-11 Vol.46 No.11
https://doi.org/10.7840/kics.2021.46.11.1811

비신뢰 전이중 중계망에서 사용자 스케줄링 및 인공잡음을 위한 최적의 전력 할당

방 인 규◆, 김 태 훈*, 임 진 택°

User Scheduling and Optimal Power Allocation for Artificial Noise in Untrusted Full-Duplex Relay Networks

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

요 약

본 논문에서는 비신뢰 전이중 중계기가 존재하는 다중사용자 중계 네트워크에서 보안 전송을 위한 중계 프로토콜 및 사용자 스케줄링 기법을 제안한다. 제안 기법은 중계 프로토콜을 고려한 수학적 분석에 기반하여 매 순간 최적의 보안 전송률(secrecy rate)을 달성할 수 있도록 사용자를 선택하고 인공잡음을 생성한다. 모의실험을 통해 제안 기법의 보안 성능을 보안 전송률 관점에서 평가한다.

Key Words : physical-layer security, user scheduling, untrusted relay, artificial noise

ABSTRACT

In this paper, we propose an optimal user scheduling scheme in untrusted relaying networks. The proposed scheduling scheme selects a user considering secrecy rate analysis for a given relaying protocol and allocates optimal power for artificial noise generation. We evaluate the secrecy rate of the proposed scheme through simulations.

Ⅰ. 서 론

5G 이동통신 시대의 도래와 함께 무선통신은 일상생활의 필수 요소가 되었으나, 다양하고 많은 무선 기기의 사용은 여러 무선 보안 문제를 초래하고 있다. 물리계층 보안(physical-layer security)은 각종 물리계층 기술과 무선 채널의 특성을 활용하여 무선 신호에 대한 도청을 보호하고자 하는 연구 분야이다. 무선 기기의 급증과 무선 신호의 범람으로 무선 보안에 대한 중요성이 더욱 강조될 것으로 예상되는 차세대 통신 환경에서 물리계층 보안의 역할이 주목을 받고 있다[1].

최근 물리계층 보안 연구는 송·수신기 및 도청기가 존재하는 기본적인 무선 도청 모델뿐만 아니라, 중계기를 활용하는 중계망(relay network)에서의 도청모델 등 다양한 환경을 고려한 연구가 진행되고 있다. 중계망에서는 송신기와 수신기 사이의 직접적인 무선 신호 전송이 어려울 경우, 중계기를 통해 안정적인 무선 신호 전송이 가능하다. 그러나 송신기의 무선 신호가 중계기를 통해 전달되기 때문에 중계기가 악의적인 도청에 활용될 경우 심각한 보안 문제가 발생할 수 있다. 이러한 이유로, 중계기를 비신뢰(untrusted) 노드로 간주하는 물리계층 보안 연구가 논의가 되고 있다[2,3].

물리계층 보안에서는 인공잡음(artificial noise), 보안 빔포밍(secrecy beamforming) 등이 대표적인 보안 전송 기술로써 활용된다. 인공잡음은 도청 공격을 효과적으로 방해하기 위해 의도적으로 재밍(jamming) 신호를 만들어내는 기술로 시스템의 보안성능(secrecy performance)을 높이기 위해 활용되는 대표적인 기술이다. 인공잡음을 생성하고 활용하는 방법은 2008년부터 본격적으로 논의되었으며[4], 이후 많은 논문들이 다중 안테나 혹은 추가적인 사용자 등을 이용하여 인공잡음을 생성하고 분석하는 방법을 연구하였다[5].

※ 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).
※ 이 논문의 일부는 한국통신학회 2021년도 하계종합학술발표회(21'.06.16~21'.06.18)에서 발표되었습니다.
◆ First Author : (ORCID:0000-0001-7109-1999)Hanbat National University Department of Information and Communication 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 : 202108-218-A-LU, Received August 30, 2021; Revised September 10, 2021; Accepted September 13, 2021

본 논문에서는 비신뢰 중계기(untrusted relay)가 존재하는 중계 네트워크에서 지금까지 논의가 거의 되지 않고 있는 다중사용자(multiuser)와 주파수 효율을 높이기 위한 전이중(full-duplex) 통신 방식의 특성을 추가적으로 고려했을 때의 중계 프로토콜 및 사용자 스케줄링(scheduling) 기법을 분석한다. 또한, 보안 전송률(secrecy rate) 분석 결과를 바탕으로 스케줄링 기준 설정 방법 및 수신기에서 최적의 인공잡음(artificial noise) 생성을 위한 전력 할당 방법을 구체적으로 논의한다. 모의실험을 통해 제안 기법의 보안 성능을 보안 전송률 관점에서 평가한다.

Ⅱ. 시스템 모델

본 논문에서는 그림 1과 같이 비신뢰 전이중 중계기(untrusted relay)와 전이중 수신기(destination)가 존재하는 다중 사용자(전체 N명) 중계 네트워크 모델을 가정한다. 매 시간 슬롯(time slot)마다 스케줄링 된 한 명의 사용자(source)는 데이터를 전송한다. 송신기(사용자)와 수신기 사이의 직접(direct) 무선 링크는 존재하지 않으며, 사용자는 중계기를 통해서 데이터를 전송할 수 있다. 중계기를 활용한 데이터 전송은 다음과 같이 총 두 단계(두 시간 슬롯)로 구성된다.

1단계(source → relay): 스케줄링에 의해 선택된 사용자(n번째 사용자 가정)는 중계기로 데이터 전송을 하며, 동시에 수신기는 비신뢰 중계기의 도청 가능성을 줄이기 위해 임의잡음(random noise) 형태의 인공잡음을 생성하고 전파한다.

2단계(relay → destination): 중계기는 전달 받은 데이터를 증폭하여(amplifying) 수신기에 전달한다. 1단계에서 보안 전송을 위해 수신기가 생성했던 인공잡음은 2단계에서 수신기가 완벽히 상쇄(cancellation)할 수 있다고 가정한다.

여기서, 전이중 중계기와 전이중 수신기를 가정했기 때문에 특정 사용자의 2단계 데이터 전송이 진행되는 동안 새롭게 스케줄링된 다른 사용자의 1단계 데이터 전송이 동시에 진행될 수 있다. h_n은 n번째 송신기와 중계기 사이의 채널 계수를 나타내며, g 중계기와 수신기 사이의 채널 계수를 나타낸다. 각 채널 계수는 독립 가우시안 분포를 따르는 레일리 블록 페이딩 채널 모델을 가정한다. 즉 $h_n \sim CN(0,\sigma_h^2)$, $g \sim CN(0,\sigma_g^2)$이 된다. σ_h^2, σ_g^2는 각 무선링크의 평균 채널 이득이 값을 나타내고 각 사용자와 중계기는 동일한 평균 채널 이득 값을 가진다. 각 채널계수(h_n, g)는 두 시간 슬롯 동안은 변하지 않으며 매 데이터 전송마다 독립적으로 변한다. 중계기와 수신기는 전이중 통신을 하기 때문에 잔여 자기 간섭(residual self-interference or RSI)이(즉, i_{RSI}) 존재한다. 두 기기에서 동일한 평균 RSI 값을 가정하고 $i_{RSI} \sim CN(0,\sigma_{RSI}^2)$으로 모델링한다.

n번째 사용자가 스케줄링 된다고 가정할 경우, 중계 프로토콜의 1단계와 2단계에서 중계기와 수신기의 수신 신호 대 간섭 및 잡음비(SINR)는 각각 다음과 같이 계산할 수 있다[2].

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

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

여기서, $\theta \in [0,1]$은 수신기가 생성하는 인공잡음의 전력 비율을 나타내고, σ_n^2은 가산 백색 가우시안 잡음(AWGN)의 평균 전력 값을 나타낸다. P는 각 노드의 전송 전력을 의미하고 아래첨자 S, R, D는 source, relay, destination을 대표한다. G는 중계기의 증폭 전송에 따른 중계 이득을 나타내며 다음과 같이 계산된다.

$$G^2 = \frac{P_R}{|h_n|^2 P_S + \theta|g|^2 P_D + \sigma_{RSI}^2 + \sigma_n^2}. \quad (2)$$

논문에서 제안하는 중계 프로토콜을 사용하고 n번째 사용자가 스케줄링 되었다고 가정했을 때, 보안 전송률(secrecy rate)은 수식 (1-1)과 (1-2)를 이용하여 다음과 같이 계산할 수 있다.

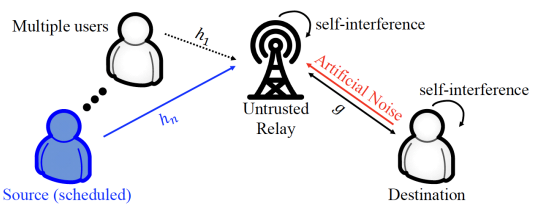

그림 1. 비신뢰 전이중 중계기와 전이중 수신기가 존재하는 다중 사용자 중계 네트워크 모델
Fig. 1. A relay network consists of an untrusted full-duplex relay, full-duplex receiver, and multiple (half-duplex) users

$$R_n^{\text{sec}}(\theta)=\left[\frac{\log_2(1+\Gamma_{D,n}(\theta))}{\log_2(1+\Gamma_{R,n}(\theta))}\right]^+, \quad (3)$$

여기서 $[x]^+=\max\{x,0\}$을 나타내며 수식 (1-1)과 (1-2)에 표현되어 있는 중계기와 수신기의 SINR은 θ의 함수가 되기 때문에 n번째 사용자의 보안 전송률 역시 θ의 함수가 된다. 본 논문의 시스템 모델은 모든 노드의 단일 안테나를 가정하였으나 다중 안테나로 확장이 가능하다. 단, 이 경우, 보안 전송률 분석 등이 새롭게 진행되어야 한다.

Ⅲ. 인공잡음 전력 최적화 및 사용자 스케줄링

본 장에서는 논문에서 제안하는 중계 프로토콜을 사용했을 때 보안 전송률(serecy rate)을 최대화 시키기 위한 인공잡음 생성 전력의 최적화와 사용자 스케줄링 기법에 대해서 논의한다.

3.1 수신기의 인공잡음 생성 전력 최적화

제안 중계 프로토콜을 사용할 경우 스케줄링 된 사용자의 보안 전송률은 전이중 수신기에서 생성하는 인공잡음 전력의 함수로 표현된다. 따라서 미분을 이용하여 수식 (3)의 보안 전송률이 최대화되는 최적의 θ^* 값을 계산할 수 있다. 단, 수식의 간결함을 위해 P_S, P_R, P_D의 값이 P로 모두 동일하다고 가정한다. 또한, $\Gamma_{SR}=\frac{|h_n|^2P}{\sigma_n^2}$, $\Gamma_{RD}=\frac{|g|^2P}{\sigma_n^2}$, $\Gamma_i=\frac{\sigma_{RSI}^2}{\sigma_n^2}$ 및 $\alpha=\Gamma_{SR}+\Gamma_i+1$, $\beta=\Gamma_{RD}-\Gamma_i-1$의 표기를 사용한다. 이 때, 최적의 θ^* 값은 다음과 같이 계산할 수 있다.

$$\theta^*=\min\left\{\frac{\alpha(\Gamma_i+1)}{\beta\Gamma_{RD}}+\frac{\sqrt{\alpha(\Gamma_{SR}+\Gamma_{RD})}}{\beta},1\right\}, \quad (4)$$

여기서 $\Gamma_{RD}>\Gamma_i+1$의 조건을 만족하는 경우에만 수식 (4)을 이용해서 최적의 θ^* 값을 계산할 수 있다. 반대로, $\Gamma_{RD}\le\Gamma_i+1$인 경우에는 θ 값에 상관없이 수식 (3)의 보안 전송률이 0이 된다. 결과적으로 수신기는 특정 사용자가 스케줄링 되었을 때, 보안 전송률을 극대화하는 인공잡음의 전력 비율 θ^*의 값을 수식 (4)을 이용하여 계산할 수 있다.

3.2 사용자 스케줄링

수식 (3)와 (4)을 이용하여 수신기의 인공잡음이 최적화되었을 때의 보안 전송율을 각 사용자(송신기)에 대해 다음과 같이 계산할 수 있다.

$$R_n^{\text{sec}}(\theta^*)=\left[\frac{\log_2(1+\Gamma_{D,n}(\theta^*))}{\log_2(1+\Gamma_{R,n}(\theta^*))}\right]^+, \quad (5)$$

여기서 $\Gamma_{D,n}(\theta^*)$와 $\Gamma_{R,n}(\theta^*)$는 수식 (1-1)과 (1-2)에 수식 (4)을 이용해 계산한 최적의 θ^* 값을 대입한 결과로 다음과 같이 계산할 수 있다.

$$\Gamma_{D,n}(\theta^*)=\frac{\beta\Gamma_{SR}}{(\Gamma_i+1)(\delta+\sqrt{\alpha\delta})}, \quad (6\text{-}1)$$

$$\Gamma_{R,n}(\theta^*)=\frac{\beta\Gamma_{SR}}{(\Gamma_i+1)\delta+(\Gamma_{RD}+\sqrt{\alpha\delta})}, \quad (6\text{-}2)$$

여기서 $\delta=\Gamma_{SR}+\Gamma_{RD}$이다. 수식 (5), (6-1), (6-2)를 이용할 경우, 보안 전송률을 극대화 시킬 수 있는 사용자 스케줄링 기준을 다음과 같이 정할 수 있다.

$$n^*=\arg\max_{n\in\{1,\ldots,N\}}\left\{R_n^{\text{sec}}(\theta^*)\right\}. \quad (7)$$

또한, 본 연구에서 가정하는 시스템 모델에서의 스케줄링에 따른 다중 사용자 다양화 이득(multiuser diversity gain)은 사용자(송신기)와 비신뢰 중계기 사이의 채널에 주로 영향을 받는다. 따라서 사용자와 비신뢰 중계기 사이의 채널계수만을 고려하여 수식 (7)의 스케줄링 기준보다는 조금 간단하면서 여전히 최적의 인공잡음 생성으로 보안 전송률의 개선을 기대할 수 있는 사용자 스케줄링 기준을 다음과 같이 정할 수 있다.

$$n^*=\arg\max_{n\in\{1,\ldots,N\}}\left\{|h_n|^2\right\}. \quad (8)$$

수식 (7)과 (8)에 기반한 사용자 스케줄링 및 최적의 인공잡음 생성을 활용하더라도 채널 상태에 따라 일부 전송이 실패하는 경우가 발생할 수 있다. 이는 QoS (Quality of Service)를 보장하는 연구에서 주로 논의되는 사항이며 본 논문의 주요 논의 대상이 아니다.

Ⅳ. 성능 평가

제안 기법(인공잡음 생성 및 사용자 스케줄링)의 보안 성능 평가를 위해 다음과 같은 환경에서 모의실

험을 진행하였다. 각 사용자와 비신뢰 중계기 그리고 중계기와 수신기 사이의 무선 링크는 각각 평균 15dB, 25dB의 SNR을 가정하였다. 전이중 전송 방식에 따른 중계기와 수신기에서의 잔여 자기 간섭(RSI)은 일반적으로 많이 사용이 되는 $i_{RSI}=wP^{\nu}$ 형태의 모델링을 사용하였다[2]. 해당 잔여 자기 간섭 모델은 w, $\nu\in[0,1]$ 값에 따라 잔여 자기 간섭(RSI)의 영향을 조절할 수 있으며, 본 모의실험에서는 $w=0.01$, $\nu=0$을 가정하였다.

그림 2는 제안 기법이 적용되었을 때, 사용자 수에 따른 보안 전송률의 결과이다. 다수의 사용자(송신기)가 존재하는 환경을 가정(10명에서 100명까지)하여 보안 성능에 있어 다중 사용자 다양성(multiuser diversity or MUD)의 효과를 관찰하였다. 또한 전이중 수신기가 생성하는 인공잡음 전력을 두 가지 경우(최적의 θ^{*} 값 사용 또는 고정 된 $\theta=0.2$ 값 아용)로 나누고 이에 따른 보안 성능을 비교 하였다. 제안 스케줄링 기법 이외에 추가적인 비교를 위하여 임의(random) 스케줄링 방식의 결과를 함께 나타냈다. 고정적인 인공잡음 생성 전력을 사용하는 경우($\theta=0.2$)와 비교했을 때, 수식 (4) 기반의 최적의 인공잡음 생성 전력을 사용할 경우(θ^{*}) 보안 전송률이 상당히 개선되는 것을 확인할 수 있다. 또한 임의 스케줄링 방식을 사용하는 경우와 비교 했을 때, 수식 (7) 또는 (8)을 이용한 사용자 스케줄링 방식은 다중 사용자 다양성(MUD)을 효과적으로 활용하기 때문에 임의 스케줄링 방식 대비 상당히 높은 보안 전송률을 달성할 수 있다.

그림 3은 그림 2와 동일한 모의실험 환경에서 보안 전송률이 아닌 일반 전송률(data rate)을 도시한 결과

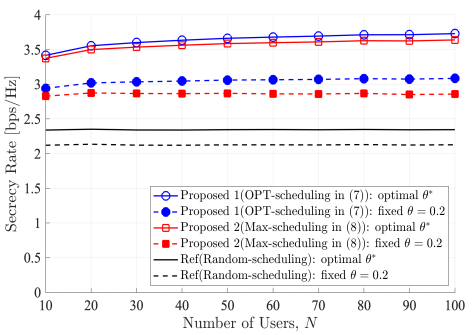

그림 2. 제안 기법(인공잡음 생성 및 사용자 스케줄링)의 적용에 따른 사용자 수 대비 보안 전송률의 결과
Fig. 2. Secrecy rate with an optimal artificial noise power allocation and user scheduling

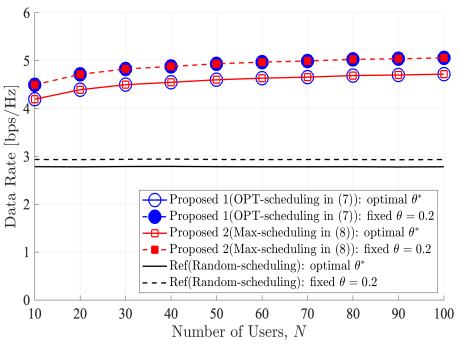

그림 3. 제안 기법(인공잡음 생성 및 사용자 스케줄링)의 적용에 따른 사용자 수 대비 일반 데이터 전송률의 결과
Fig. 3. Data rate with an optimal artificial noise power allocation and user scheduling

이다. 수식 (7)에 기반한 (보안 전송률 관점의) 최적의 스케줄링 기법과 수식(8)에 기반한 스케줄링 기법이 동일한 일반 전송률을 달성하는 것을 확인할 수 있다. 또한 보안 전송률이 아닌 일반 전송률을 관측하기 때문에 (보안 전송률 관점의) 최적의 인공잡음 생성(수식 (4))이 일반 전송률 관점에서는 최적이 아닌 것을 확인할 수 있다. 즉, 비신뢰 중계기가 도청에 악용되지 않는 확신이 있을 경우 인공잡음을 사용할 필요가 없다.

V. 결 론

본 논문에서는 비신뢰 전이중 중계기가 존재하는 다중사용자 중계망에서 보안 전송을 위한 인공잡음 전력 최적화 및 사용자 스케줄링 방법을 제안하였다. 제안 기법을 적용했을 때, 보안 전송률이 개선되는 것을 확인할 수 있었다. 따라서, 비신뢰 중계기의 도청 가능성에 대비한 제안 기법의 실제 활용 가능성이 기대된다.

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.

[2] S. Atapattu, et al., "Source-based jamming for physical-layer security on untrusted full-duplex relay," *IEEE Commun. Lett.*, vol. 23, no. 5 pp. 842-846, May 2019.

[3] J. Lim, et al., "Secure communication with

outdated channel state information via untrusted relay capable of energy harvesting," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 11323-11337, Oct. 2020.

[4] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, Jun. 2008.

[5] I. Bang and T. Kim, "Secrecy performance analysis of joint user and friendly jammers scheduling scheme against potential eavesdropping," *J. KICS*, vol. 45, no. 12, pp. 2029-2036, Dec. 2020.