비신뢰 전이중 중계망에서 사용자 스케줄링 및 인공잡음에 관한 연구

방인규, 김태훈*
한밭대학교 정보통신공학과, *한밭대학교 컴퓨터공학과
ikbang@hanbat.ac.kr, *thkim@hanbat.ac.kr

A Study on User Scheduling and Artificial Noise in Untrusted Full-Duplex Relay Networks

Inkyu Bang, Taehoon Kim*
Dept. of Information and Communication Engineering, Hanbat National University
*Dept. of Computer Engineering, Hanbat National University

요 약

본 연구에서는 비신뢰 전이중 중계기와 전이중 수신기가 존재하는 무선 네트워크에서 보안 전송을 위한 중계 프로토콜 및 사용자 스케줄링 기법의 보안 전송률을 분석하고 모의실험을 통해 인공잡음의 전력 분배와 다양한 사용자 스케줄링 기법에 따른 보안 성능 차이를 확인한다.

Ⅰ. 서 론

오늘날 사물인터넷(Internet of Things)은 우리의 일상생활의 필수 요소로 자리 잡고 있다. 그러나 다양한 기기들이 무선으로 연결되기 때문에 무선 신호에 대한 잠재적 도청(eavesdropping) 가능성 역시 증가하고 있다. 무선채널을 통해 데이터를 전달하는 무선통신 시스템에서 도청 공격은 불가피한 보안 문제이며 무선통신 기술의 발달과 함께 앞으로 더욱 중요해 질 것으로 전망된다. 물리계층 보안(physical-layer security)은 무선링크의 도청 가능성을 줄이기 위한 통신 기술을 정보이론 관점에서 연구하는 분야이며, 무선 네트워크의 보안 문제 해결을 위해 지속적으로 주목 받고 있는 연구 분야 중 하나이다.

물리계층 보안에서는 송신기와 수신기 그리고 도청기 등으로 구성되는 도청 네트워크(wiretap network) 환경에서 다중 안테나(MIMO) 기술, 다중 사용자 다양성(multiuser diversity) 등 활용하여 보안성능을 개선하고 분석하는 연구가 활발히 진행되고 있다 [1]. 또한 송신기와 수신기뿐만 아니라 중계기를 활용하는 중계망(relay network)의 다양한 상황에서도 다양한 주제의 물리계층 보안 연구가 진행되고 있다. 본 연구에서는 비신뢰 전이중 중계기(untrusted full-duplex relay)와 전이중 수신기가 존재하는 무선 네트워크에서 보안 전송을 위한 중계 프로토콜 및 사용자 스케줄링 기법의 보안 성능을 분석하고 모의실험을 통해 이를 검증한다.

Ⅱ. 본론

본 연구에서 N개의 반이중(half-duplex) 송신기, 하나의 비신뢰 전이중 중계기, 하나의 전이중 수신기로 구성된 다중 사용자 중계 네트워크를 가정한다. 송신기와 수신기 사이의 직접링크는 존재하지 않으며 송신기와 중계기 그리고 중계기와 수신기 사이의 순시 채널상태정보(CSI)는 사용자 스케줄링 및 수신기의 인공잡음 생성을 위해 활용할 수 있다고 가정한다. 비신뢰 중계기의 무선 도청 가능성에 대비하기 위해 다음의 2단계로 구성된 중계 프로토콜을 사용한다. **1단계(선택된 송신기 → 중계기):** 사용자 스케줄링 기준에 근거하여 선택된 송신기는 데이터를 전송한다. 동시에 수신기는 송신 데이터의 보안성을 보장하기 위해 인공잡음을 생성하여 전송한다. 즉, 중계기는 데이터와 인공잡음을 동시에 수신한다. **2단계(중계기 → 수신기):** 중계기는 1단계에서 받은 신호를 증폭하여 수신기에게 전달한다. 중계기와 수신기에는 전이중 기능이 탑재되어 있기 때문에 송신기 별로 중계 프로토콜을 병렬적으로 운영할 수 있다. 또한 중계기와 수신기 사이의 순시 채널상태정보를 활용하여 수신기는 인공잡음 생성 전력 비율(ϕ)을 최적화할 수 있다. 사용자 스케줄링 기준으로 매순간 송신기와 중계기 사이의 채널 이득이 가장 높은 송신기를 선택하는 스케줄링 기법(max-scheduling)과 임의로 송신기를 선택하는 스케줄링 기법(random-scheduling)을 고려했다. 그림 1은 송신기 수(N) 변화에 따른 두 스케줄링 기법의 보안 전송률을 보여준다. 스케줄링 기법 및 ϕ 값에 따른 보안 전송률 차이를 확인할 수 있다.

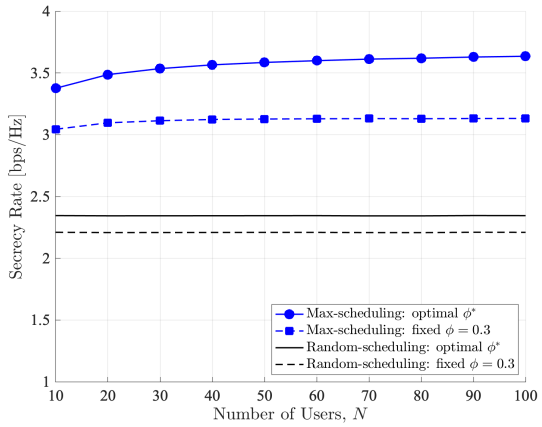

그림 1. 송신기 수(N) 변화에 따른 사용자 스케줄링 기법의 보안 전송률

Ⅲ. 결론

본 연구에서는 비신뢰 전이중 중계기가 존재하는 무선네트워크에서 사용자 스케줄링 및 인공잡음 생성 전력 비율에 따른 보안 성능을 분석하였다.

참 고 문 헌

[1] I. Bang, S. M. Kim, and D. K. Sung "Artificial noise-aided user scheduling from the perspective of secrecy outage probability," IEEE Tran. Vech. Tech., vol.67, no.8 pp. 7816-7820, Aug. 2018.