2021년도 한국통신학회 추계종합학술발표회

잠재적 도청자가 존재하는 상향링크 셀룰라 네트워크를 위한 사용자 스케쥴링 기법

손 웅(충남대학교), 유희정(고려대학교), 정방철(충남대학교)

woongson@cnu.ac.kr, heejungyu@korea.ac.kr, bcjung@cnu.ac.kr

User Scheduling for Multi-User Uplink Cellular Networks with Potential Eavesdroppers

Woong Son (Chungnam National Univ.), Heejung Yu (Korea Univ.) and Bang Chul Jung (Chungnam National Univ.)

요 약

본 논문에서는 다수의 공인단말들이 존재하는 상향링크 셀룰라 네트워크에 자신의 스케쥴에 따라 무작위로 도청을 시도하는 잠재도청자들이 다수 존재할 때, 잠재도청자들을 고려한 보안 아웃티지 확률 (secrecy outage probability, SOP)을 낮출 수 있는 사용자 스케쥴링 기법을 제안한다. 특히, 공인 기지국으로부터 스케쥴링을 받을 수도 있는 잠재도청자들이 공인단말의 전송을 엿듣기 때문에 제안하는 사용자 스케쥴링 기법에서는 공인단말들이 잠재도청자까지의 채널 정보를 획득하여 이용할 수 있다. 제안하는 사용자 스케쥴링 기법과 기존 채널이득기반의 기회적 스케쥴링 기법을 적용하였을 때의 보안 아웃티지 확률을 비교분석하였으며, 제안하는 사용자 스케쥴링 기법의 우수함을 검증하였다.

Ⅰ. 서 론

최근에는 사물인터넷, 클라우드 등의 무선 이동통신 기술이 발달함에 따라 네트워크 애플리케이션 서비스 기술들이 다양해지고 있으며, 단말간 무선 전송되는 개인정보에 대한 보안성이 매우 중요해졌다. 학계에서는 물리계층에서 도청자를 고려하여 정보이론 기반으로 보안 용량과 보안 아웃티지 확률 (secrecy outage probability) 등의 개념을 정의하고, 다양한 물리계층 보안 (physical-layer security) 성능 향상을 위한 기술들이 활발하게 발표되고 있다. 본 논문에서는 간헐적으로 도청하는 잠재도청자 [1]를 고려한 상향링크 셀룰라 네트워크에서의 보안 아웃티지 확률을 현저히 낮출 수 있는 사용자 스케쥴링 방법을 제안하였고, 수학적 분석 및 모의실험을 통해 이를 검증하였다.

Ⅱ. 시스템 모델

본 논문에서 고려하는 시스템 모델에서는 단일 기지국과 N_{MS}개의 공인단말들 및 N_E개의 도청자들이 존재하며, 모두 단일 안테나를 탑재하고 있다. 모든 무선채널들은 전송 중에는 변하지 않는 준정적 상태로 가정한다. i번째 공인단말로부터 기지국까지의 무선채널은 $h_{B,i} \sim CN(0,\sigma_B^2)$, j번째 도청자까지의 무선채널은 $h_{j,i} \sim CN(0,\sigma_E^2)$이고, 모든 채널들은 독립적이고 균등한 분포를 따른다고 가정한다. 이때, i번째 공인단말이 기지국으로 메시지를 전송할 때, 시스템에서 달성가능한 보안 전송률과 보안 아웃티지 확률의 정의는 각각 다음과 같다.

$$R_{\mathrm{sec},i} = \left[\log_2\left(\frac{1+|h_{B,i}|^2\rho}{1+\max_{j\in\mathcal{M}_E}|h_{j,i}|^2\rho}\right),0\right]^+, \quad P_{out,i} = \Pr(R_{\mathrm{sec},i} < R_o).$$

여기서 $\rho = P/N_0$는 수신 신호 대비 잡음 비 (signal to noise ratio, SNR)이며, P는 송신전력이고 N_0는 잡음 분산이다. 집합 $\mathcal{M}_E$는 N_E개의 도청단말 중에서 도청확률 P_E로 도청을 시도할 때, 이번 전송에서 엿듣기를 시도하는 도청자의 집합, R_o는 목표 보안 전송률로 달성가능한 보안 전송률이 이 수준을 넘지 못할 경우에 보안 아웃티지가 발생한다.

Ⅲ. 잠재 도청자들을 고려한 사용자 스케쥴링 기법

N_{MS}개의 공인단말들은 자신의 데이터를 기지국을 송신하기 위해 기지국으로부터 선택받게 된다. 본 논문에서 고려한 사용자 스케쥴링 기법 2개를 아래에 정리하였다.

기회적 피드백 (opportunistic feedback, OF) [1]에서는 특정 i번째 공인단말이 기지국까지의 채널이득이 특정 임계치보다 높을 경우에만 기지국까지의 채널이득을 피드백하고, 기지국은 다수의 공인단말들로부터 피드백 받은 채널이득들 중에서 가장 큰 채널이득을 갖는 공인단말을 선택하여 송신 기회를 제공한다.

제안하는 기회적 피드백 (two-step opportunistic feedback, TOF)은 첫 번째 단계에서 특정 i번째 공인단말이 기지국까지의 채널이득과 N_E개의 잠재도청자들의 채널이득을 고려하여 보안 아웃티지가 확정적으로 발생하지 않는 경우에는 기지국이 자신을 스케쥴링할 수 있도록 유도하기 위한 채널이득을 최대값으로 피드백한다. 그렇지 않은 경우에는 두 번째 단계에서는 기지국까지의 채널이득이 특정 임계치보다 높을 경우에만 기지국까지의 채널이득을 피드백한다. 모든 공인단말들은 위와 같은 2가지 단계를 거치며, 1개의 공인단말에서는 2번 이상의 피드백을 하지 않는다. 기지국은 다수의 공인단말들로부터 피드백 받은 채널이득들 중에서 가장 큰 채널이득을 갖는 공인단말을 선택하여 상향링크 송신 기회를 제공하며, 첫 번째 단계의 공인단말이 공인 네트워크에 적어도 1개가 존재할 경우에는 반드시 보안 아웃티지가 발생하지 않는다.

Ⅳ. 시뮬레이션 결과

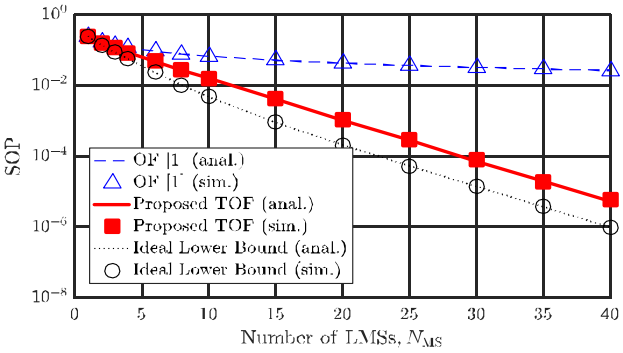

그림 1. 공인단말 수에 따른 보안 아웃티지 확률 분석

위 그림은 앞에서 소개한 시스템 모델에서 파라미터들이 $\rho = 10$[dB], $N_E = 2$, $\sigma_B^2 = \sigma_E^2 = 1$, $P_E = 0.5$, $R_o = 0.5$[bps/Hz] 그리고 N_{MS}를 최대 40까지 고려한 시스템 보안 아웃티지 확률을 수학적 분석 및 모의실험 분석을 비교한 결과이다. 기존 OF와 제안하는 TOF에서 최소로 달성할 수 있는 보안 아웃티지 확률을 비교분석하기 위해서 채널 임계치는 둘 다 0으로 설정하여, 임계치를 조정해도 위 결과보다 낮은 보안 아웃티지 확률을 절대 달성할 수 없다. 또한 이상적인 하한 (ideal lower bound)는 주어진 시스템에서 달성할 수 있는 최소 보안 아웃티지 확률을 의미한다. 공통적으로, 공인단말 수가 증가할수록 다중 사용자 다중화 (multi-user diversity)로 인하여 보안 아웃티지 확률이 감소한다. 그러나 보안 아웃티지 확률의 감소하는 수준을 비교하면, 기존 OF 대비 제안하는 TOF가 더욱 크게 감소하며, 제안하는 TOF가 이상적인 하한에 더욱 근접한 성능을 달성한다. 또한 공인링크의 무선채널이득이 가장 큰 공인단말을 스케쥴링하는 것이 항상 보안 아웃티지 성능을 최소화하는 것은 아님을 보여준다.

ACKNOWLEDGMENT

본 연구는 미래창조과학부 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. NRF-2019R1A2B5B01070697).

참 고 문 헌

[1] W. Son, H. Nam, W.-Y. Shin, and B. C. Jung, "Secrecy outage analysis of multi-user downlink wiretap networks with potential eavesdroppers," *IEEE Syst. J.*, vol. 15, no. 2, pp. 3093-3096, June 2021.