잠재 도청단말이 존재하는 무선 통신망 하향링크 성능 분석

손 웅(충남대학교), 정방철(충남대학교)

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

Performance Analysis of Downlink Cellular Networks with Potential Eavesdroppers

Woong Son (Chungnam National Univ.) and Bang Chul Jung (Chungnam National Univ.)

요 약

본 논문은 하향링크 셀룰라 네트워크에서 공인단말과 잠재 도청단말이 존재하는 환경에서 기지국으로부터 전송되는 데이터의 물리계층 보안 성능을 분석하였다. 잠재 도청단말은 기지국으로부터 방송되는 메시지에 대한 수신이 비허가된 단말로서 공인단말 중 스케줄링되지 않은 단말 또는 다른 셀에 속한 단말, 셀 밖의 단말 등이 될 수 있다. 잠재 도청단말들은 제안하는 3가지 도청 방법 (full, random, opportunistic eavesdropping)을 사용하여 공인단말로 전송되는 메시지를 도청할 수 있으며 이에 따른 하향링크 셀룰라 네트워크의 보안 outage 확률을 분석하였다.

Ⅰ. 서 론

최근 5G 이동통신, IoT 네트워크, 클라우드, 인공지능 등의 기술이 발전하면서 도처에 존재하는 무선통신 단말들이 무선통신을 기반으로 클라우드에 연결되어 네트워크 응용 서비스를 제공받게 되었다. 클라우드 서버로부터 전송되는 개인정보 메시지 전송을 위해 보안성능이 매우 중요해졌다. 이러한 보안문제를 해결하기 위해서 학계에서는 정보이론적으로 보안용량 또는 보안 아웃티지 확률 (secrecy outage probability, SOP)의 개념을 정립하였고 이 성능을 향상시키기 위해 공인네트워크 주변에 존재할 수 있는 잠재 도청단말을 고려한 물리계층 보안통신 기술에 대한 연구들이 활발히 진행되고 있다 [1]. 본 논문에서는 전력 등의 현실적인 문제로 인해 항상 도청할 수 없는 잠재 도청 단말의 동작을 고려하여 3가지 도청 방법을 고려하였고 공인단말과 잠재 도청단말이 존재하는 하향링크 셀룰라 네트워크에서 도청단말들의 3가지 도청 방법에 따른 SOP 성능을 컴퓨터 모의실험을 통해 분석하였다.

Ⅱ. 시스템 모델

본 논문에서는 기지국과 공인단말 1개, 잠재 도청단말 1개가 존재하는 하향링크 셀룰라 네트워크를 고려한다. 모든 통신 기기들은 단일안테나를 장착하였고, 메시지를 방송하는 동안 준정적 상태로 채널이 변하지 않는다. 기지국으로부터 공인단말까지의 공인채널은 $h_{MS} \sim CN(0,\lambda_{MS})$, 잠재 도청단말까지의 도청채널은 $h_E \sim CN(0,\lambda_E)$으로 서로 독립적이고 비균등한 분포를 따른다고 가정한다. 기지국으로부터 방송되는 메시지를 s라고 정의하고, 방송 메시지의 전력제한 $\mathbb{E}[|s|^2]=P$가 존재한다고 가정한다. 일반성을 잃지 않고, 공인단말과 도청단말에서의 수신신호 모델은 다음과 같다.

$$y_{MS} = h_{MS}s + z_{MS}, \quad (1)$$

$$y_E = h_E s + z_E, \quad (2)$$

이때, z_{MS}과 z_E는 각각 공인단말 및 도청단말에서의 열잡음이며, 평균이 0, 분산이 N_0인 복소가우시안 분포를 따른다고 가정한다.

수신신호 모델로부터 공인단말과 도청단말에서의 SNR을 계산하면 다음과 같다.

$$\gamma_{MS} = P|h_{MS}|^2/N_0, \quad (3)$$

$$\gamma_E = P|h_E|^2/N_0. \quad (4)$$

식 (3)와 (4)을 이용하여 최종적으로 달성할 수 있는 보안전송률을 다음과 같이 나타낼 수 있다.

$$R_{SEC} = \left[\log_2\left(\frac{1+\gamma_{MS}}{1+\gamma_E}\right), 0\right]^+. \quad (5)$$

달성할 수 있는 보안전송률 R_{SEC}가 미리 정의된 아웃티지 보안전송률 R_o 이하가 되는 경우, outage event가 발생하게 된다.

Ⅲ. 잠재 도청단말에서의 도청 방법

한편, 도청단말은 아래 3가지 도청 방법을 채택하며, 도청하지 않는 경우에는 $\gamma_E=0$이므로, 보안전송률이 하향링크 전송률과 동일해진다.

무작위로 도청하는방법 (random eavesdropping, RE) : 도청단말의 동작 듀티사이클에 의해 도청 확률 $P_E \in (0,1)$으로 도청하는 기법이다.

항상 도청하는방법 (full eavesdropping, FE) : 기지국의 메시지 방송마다 항상 도청하는 기법으로 무작위 도청에서 도청 확률 $P_E=1$인 special case와 동일하다.

기회적으로 도청하는 방법 (opportunistic eavesdropping, OE) : 도청단말로부터 기지국까지의 도청링크의 이득이 미리 정의된 채널 임계치 ζ_E 이상일 경우에만 도청하는 기법이다. 채널 임계값이 ζ_E일 경우, 기회적으로 도청하는 방법의 도청 확률은 $P_E = e^{-\lambda_E \zeta_E}$이 되며, 이때 $P_E \in (0,1)$이다.

Ⅳ. 시뮬레이션 결과

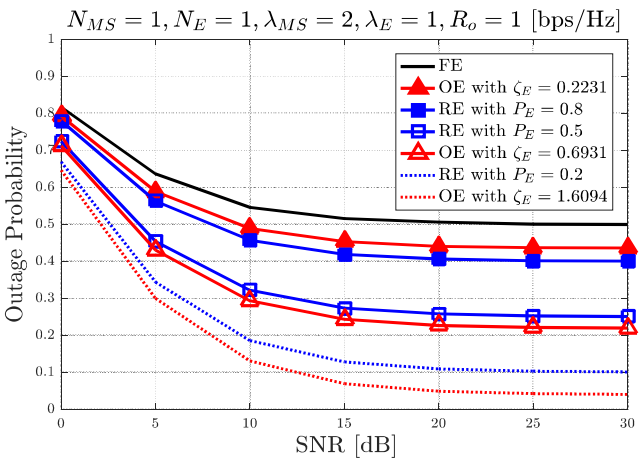

그림 1 도청 방법에 따른 SOP 성능 비교

위 그래프는 공인단말이 1개, 잠재 도청단말이 1개 존재하는 하향링크 셀룰라 네트워크에서의 $\lambda_{MS}=2$, $\lambda_E=1$이며, 미리 정의된 아웃티지 보안전송률은 $R_o=1$[bps/Hz]인 상황에서의 SNR 증가에 따른 각 도청 방법들의 SOP 성능을 보여준다. OE의 채널 임계값은 각각 $\zeta_{MS}=1.6094$와 0.6931, 0.2231이며, 이때 도청 확률을 계산하면 각각 $P_E=0.2$와 0.5, 0.8이 된다. 높은 채널 임계값을 갖는 OE와 동일한 도청 확률을 갖는 RE를 비교하면, OE가 RE보다 SOP 성능이 낮다. 그러나 낮은 채널 임계값을 갖는 경우 OE가 RE보다 SOP 성능이 우수한 것을 확인할 수 있다. 향후, 본 논문을 기반으로 다수의 공인단말과 도청단말을 고려한 SOP 성능 향상 기법에 대한 확장 연구를 진행할 것이다.

ACKNOWLEDGMENT

본 연구는 방위사업청과 국방과학연구소가 지원하는 미래전투체계 네트워크 기술 특화연구센터 사업의 일환으로 수행되었습니다 (UD160070BD).

참 고 문 헌

[1] H. Jin, W.-Y. Shin, and B. C. Jung, "On the multi-user diversity with secrecy in uplink wiretap networks," *IEEE Commun. Lett.*, vol. 17, no. 9 pp. 1778-1781, Sept. 2013.