비동기식 도청자와 적법 수신기의 채널 추정오류를 고려한 에르고딕 보안 전송률 분석

염현식, 하정석
한국과학기술원
overlimit@kaist.ac.kr, jsha@kaist.edu

Ergodic Secrecy Rate Analysis for Non-coherent Eavesdropper and Legitimate Receiver with Channel Estimation Error

Hyeonsik Yeom, Jeongseok Ha
Korea Advanced Institute of Science and Technology

요 약

최근에 채널의 상반성을 만족하는 시분할 이중통신 상황에서 도청자에게 채널 정보 누설을 방지하고자 하향링크 파일럿을 사용하지 않는 물리 계층 보안 시나리오에 관해 연구되었다. 앞서 언급한 보안 통신 시나리오는 수신기에서의 채널 추정의 오류가 보안 통신 성능에 크게 영향을 미친다. 하지만 기존의 연구들은 완벽한 채널 추정 과정을 가정하여 분석 및 검증하였다. 따라서, 본 논문에서는 채널 추정의 오류가 앞선 보안 통신 네트워크에서 어떠한 영향을 미치는지 분석을 하고 실험을 통해 검증한다.

Ⅰ. 서 론

무선 통신 기술은 개방된 자원을 매개체로 하여 전파를 통해 정보를 전송하는 기술이다. 이러한 특징으로 인해 보안에 관한 문제가 항상 제기되어왔다. 현재 보안 무선 통신을 위해 암호학 기반의 기술들이 많이 사용되고 있지만, 암호학 기반의 보안은 진보된 프로세서들 및 양자컴퓨터기술의 발전으로 인한 연산성능 향상으로 인해 위협받고 있다. 이에 따라, 컴퓨팅 성능과 상관없이 정보 이론을 이용한 완벽한 보안 무선 통신 기법인 물리 계층 보안 기술이 주목을 받고 있다.

최근에 상반성 (reciprocity)을 만족하는 채널이며 시분할 이중통신 (Time Division Duplex, TDD) 방식을 사용하는 경우, 채널 추정을 위해 오직 상향링크 파일럿 (pilot)만을 사용하여 도청자에게 채널 정보를 제공하지 않아 도청자는 비동기식 수신기 (non-coherent receiver)로 작동을 하며 송신자가 정보를 전송할 때 적법 수신기에 대한 채널을 보상하여 전송하여 적법 사용자는 채널의 영향을 받지 않게 되어 동기식 수신기 (coherent receiver)로 작동하는 시나리오에 대해 분석이 되었다 [1]. 하지만, 실제 통신 상황에서는 채널 추정의 오류가 필연적으로 존재하며, 이는 통신 성능의 감소를 일으킨다. 따라서 본 논문에서는 도청자가 비동기식 수신기로 작동할 때, 적법 수신기에 관한 채널 추정의 오류가 보안 성능에 미치는 영향을 분석한다.

본 논문에서는 2장에서 채널 추정으로 인해 발생하는 오류와, 이를 기반으로 한 보안 통신 시스템 모델에 관해 설명한다. 3장에서는 보안 데이터 전송률의 하계를 구하고 4장에서는 시뮬레이션을 통해 앞서 구한 하계의 타당성을 보이고 분석한다. 마지막 장에서는 결론을 맺는다.

Ⅱ. 제안하는 시스템 모델

한 명의 도청자가 존재하는 단일 셀 네트워크 환경을 가정하며, 하향링크 보안 무선 통신 상황을 가정한다. 송신자는 다중 안테나를 사용하며, 안테나 개수는 N_t으로 나타낸다. 그리고, 수신자와 도청자는 한 개의 안테나를 갖는다. T는 상관 시간 (coherent time)으로, 채널이 일정하게 유지되는 시간을 의미한다. 송신자와 수신자 사이의 채널은 $\mathbf{h}_b \in \mathrm{C}^{1\times N_t}$, 송신자와 도청자 사이의 채널은 $\mathbf{h}_e \in \mathrm{C}^{1\times N_t}$로 표기된다. 각각 채널은 레일레이 페이딩 (rayleigh fading)을 따른다고 가정하여 각각 공분산이 $d_b^{-\alpha}, d_e^{-\alpha}$인 원형 대칭 정규분포 (circular symmetric Gaussian distribution)를 갖는다. 이때, d_b, d_e는 각각 송신자와 수신자, 도청자 사이의 물리적인 거리를 의미하며, α는 거리 감쇄 계수를 의미한다.

채널 추정 과정은 도청자에게 채널 정보의 누설을 방지고자, 상향링크 파일럿만 전송하는 상황을 가정한다. 이후 기지국은 LMMSE 기반 채널 추정을 한다. 추정된 채널, $\tilde{\mathbf{h}}_b \sim CN(0, \sigma_{\tilde{h}_b}^2 \cdot \mathbf{I}_{N_t})$ 은 원형 대칭 정규분포를 따르며, 채널 추정오류, $\mathbf{e} = \mathbf{h}_b - \tilde{\mathbf{h}}_b \sim CN(0, \sigma_e^2 \cdot \mathbf{I}_{N_t})$ 는 추정된 채널과 독립적인 원형 대칭 정규분포를 따른다. 이때 각 공분산 값은 다음과 같이 표현된다.

$$\sigma_{\tilde{h}_b}^2 = c \cdot d_b^{-\alpha}, \sigma_e^2 = (1-c) \cdot d_b^{-\alpha},$$

이때, $0 \le c \le 1$은 채널 추정의 성능을 나타내는 파라미터이다.

기지국은 $\mathbf{s} \in \mathrm{C}^{1\times \mathrm{T}}$의 정보 신호를 $\mathbf{w} \in \mathrm{C}^{N_t \times 1}$의 빔 형성을 통해 전송한다. 전송하는 신호, $\mathbf{X} \in \mathrm{C}^{N_t \times T}$는 다음과 같다.

$$\mathbf{X} = \sqrt{P_t (N_t - 1)/(c \cdot d_b^{-\alpha})} \cdot \mathbf{w} \cdot \mathbf{s},$$

여기서, P_t는 상관 시간 단위당 기지국에서 사용되는 전력을 의미하고, 정보 신호는 원형 대칭 정규분포를 따른다 ($\mathbf{s} \sim CN(0, \mathbf{I}_T)$). 기지국은 송신자가 동기식 수신기로 작동하도록 추정된 채널을 기반으로 의사 역행렬 (pseudo-inverse matrix) 을 통해 채널을 보상해서 정보 신호를 적법 수신자에게 전송한다 $\left(\mathbf{w} = \tilde{\mathbf{h}}_b^{\mathrm{H}} \cdot \left(\tilde{\mathbf{h}}_b \cdot \tilde{\mathbf{h}}_b^{\mathrm{H}}\right)^{-1}\right)$.

수신자의 수신 신호인 $\mathbf{y}_b$는 다음과 같이 표현된다.

$$\mathbf{y}_b = \mathbf{h}_b \cdot \mathbf{X} + \mathbf{n}_b = \sqrt{\frac{P_t(N_t-1)}{c \cdot d_b^{-\alpha}}} \cdot (1+h') \cdot \mathbf{s} + \mathbf{n}_b \in C^{1\times T},$$

여기서, $\mathbf{n}_b \sim CN(0, \mathbf{I}_T)$은 수신자의 열잡음, $h' = \mathbf{e} \cdot \mathbf{w}$은 채널 추정 오류로 인해 발생하는 부분이다.

도청자의 수신 신호인 $\mathbf{y}_e$ 는 다음과 같다.

$$\mathbf{y}_e = \mathbf{h}_e \cdot \mathbf{X} + \mathbf{n}_e = \sqrt{P_t(N_t-1)} \cdot g \cdot \mathbf{s} + \mathbf{n}_e \in C^{1\times T},$$

이때, $\mathbf{n}_e \sim CN(0, \mathbf{I}_T)$은 도청자의 열잡음, $g = \mathbf{h}_e \cdot \mathbf{w} / \sqrt{c \cdot d_b^{-\alpha}}$는 도청자의 유효채널 (effective channel)이다.

채널 추정오류로 인해 발생하는 부분, h'과 도청자의 유효채널, g은 송신 안테나의 개수가 충분하지 않은 경우에도, 가우시안 분포로 근사하는 것이 타당함이 실험적으로 보여졌으며 [1], 공분산은 다음과 같다.

$$h' \sim CN\left(0, \sigma_{h'}^2 = (1-c)/(N_t \cdot c)\right),\ g \sim CN\left(0, \sigma_g^2 = 1/(N_t d_e^{\alpha})\right).$$

Ⅲ. 에르고딕 보안 데이터 전송률의 하계

수신자는 채널 오류로 인해 비동기식 수신기 역할을 하고 도청자 또한 비동기식 수신기로 작동을 하므로 에르고딕 보안 데이터 전송률 (R_s)은 다음과 같다.

$$R_s = \left[I(\mathbf{y}_b; \mathbf{s}) - I(\mathbf{y}_e; \mathbf{s}) \right]^+.$$

현재, 비동기식 수신기의 데이터 전송률의 닫힌 식은 알려지지 않은 상태이며, 수치적으로도 적분 계산이 어렵다. 따라서, 계산이 가능한 에르고딕 보안 데이터 전송률을 구하는 것이 필요하다.

정리. 채널 추정오류가 존재하는 네트워크에서 에르고딕 보안 데이터 전송률의 하계의 식은 다음과 같다.

$$R_s \geq T \cdot \log\left[\exp\left(\ln\left(\frac{P_t(N_t-1)}{c \cdot d_b^{-\alpha}}\right) + \mathrm{E}[\ln(|1+h'|^2)]\right)+1\right]$$
$$+\log\left[P_t(N_t-1)\frac{\psi(T)}{N_t \cdot d_e^{\alpha}}+1\right] - T \cdot \log\left[P_t(N_t-1)\frac{1}{N_t \cdot d_e^{\alpha}}+1\right]$$
$$-\log\left[\frac{P_t(N_t-1)}{c \cdot d_b^{-\alpha}}\frac{1}{N_t}\frac{1-c}{c} \cdot T+1\right],$$

여기서 $\psi(\cdot)$은 다이감마 (digamma)함수를 의미한다.

증명.

$$R_s \geq T \cdot E_{h'}\left[\log\left[\exp\left(\ln\left(\frac{P_t(N_t-1)}{c \cdot d_b^{-\alpha}}\right) + \ln(|1+h'|^2)\right)+1\right]\right]$$
$$+E_s\left[\log\left[P_t(N_t-1)\frac{|\mathbf{s}|^2}{N_t \cdot d_e^{\alpha}}+1\right]\right] - T \cdot \log\left[P_t(N_t-1)\frac{1}{N_t \cdot d_e^{\alpha}}+1\right]$$
$$-E_s\left[\log\left[\frac{P_t(N_t-1)}{c \cdot d_b^{-\alpha}}\frac{1}{N_t}\frac{1-c}{c} \cdot |\mathbf{s}|^2+1\right]\right],$$
$$\geq T \cdot \log\left[\exp\left(\ln\left(\frac{P_t(N_t-1)}{c \cdot d_b^{-\alpha}}\right) + \mathrm{E}[\ln(|1+h'|^2)]\right)+1\right]$$
$$+\log\left[P_t(N_t-1)\frac{\psi(T)}{N_t \cdot d_e^{\alpha}}+1\right] - T \cdot \log\left[P_t(N_t-1)\frac{1}{N_t \cdot d_e^{\alpha}}+1\right]$$
$$-\log\left[\frac{P_t(N_t-1)}{c \cdot d_b^{-\alpha}}\frac{1}{N_t}\frac{1-c}{c} \cdot T+1\right],$$

첫 번째 부등식은 원형 대칭 정규분포가 최고의 정보 엔트로피를 갖는다는 사실과 조건부 엔트로피는 일반 엔트로피보다 작다는 사실 그리고 $\det(\mathbf{A} \cdot \mathbf{B}+\mathbf{I}) = \det(\mathbf{B} \cdot \mathbf{A}+\mathbf{I})$를 이용하였다. 마지막 부등식은 $\log(c+\exp(\cdot))$이 볼록함수임을 이용하고, Jensen의 부등식을 이용 [2] 그리고 로그 감마 분포의 평균을 이용한 것이다.

Ⅳ. 모의실험 결과

본 장에서는 시뮬레이션을 통해 앞서 제안한 시스템 모델의 성능을 검증한다. 송신 전력 P_t는 10dB, 상관 시간 T는 1, 송신자와 수신자 사이의 거리는 3m, 도청자와의 거리는 5m 그리고 거리 감쇄 계수는 2로 설정하였다.

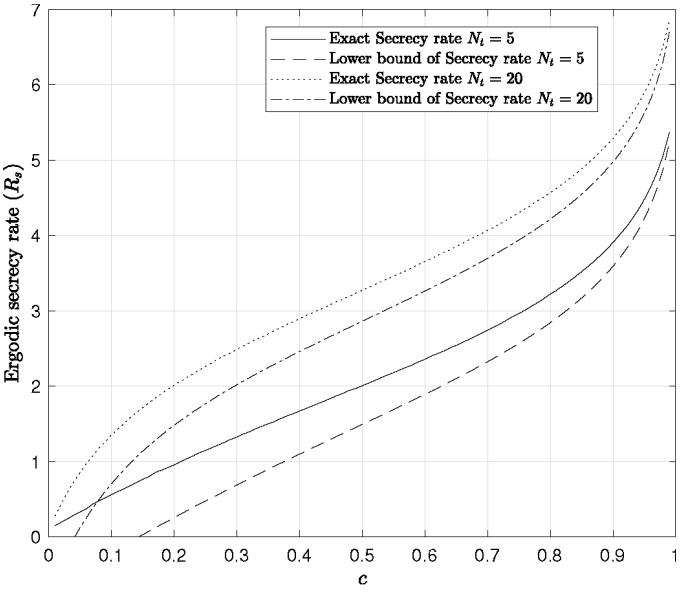

그림 1. 채널 추정성능에 따른 에르고딕 보안 데이터 전송률

그림 1에 따르면 3장에서 구한 하계값이 실제값과 근사함을 알 수 있다. 그리고 채널 추정의 성능이 좋은 부분에서는 작은 채널 추정오류가 성능에 큰 영향을 주는 것을 확인할 수 있다. 따라서 채널 추정의 성능을 보안 성능에 큰 영향을 미침을 알 수 있다.

Ⅴ. 결론 및 향후 연구

본 논문은 채널의 상반성을 만족하는 시분할 이중통신 상황에서 송신자가 적법 사용자만을 동기식 수신기로 작동하도록 만들 때, 채널 추정의 오류가 존재하는 보안 통신 환경에 관한 내용이다. 이때 채널 추정의 오류가 보안 성능에 미치는 영향을 보안 데이터 전송률의 하계를 통해 분석하였다. 연구 결과, 채널 추정성능이 좋은 부분에서는 채널 추정오류가 보안 데이터 전송률에 큰 영향을 미치는 것을 확인하였다. 이후, 보안 성능을 높이기 위해 많이 사용되는 인공 잡음 또한 추정된 채널을 바탕으로 구성되기 때문에 인공 잡음기술을 접목한 네트워크에서 채널 추정의 오류에 관한 연구를 진행할 예정이다.

ACKNOWLEDGMENT

이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. 2018-0-00831, 이종 무선 네트워크를 위한 물리 계층 보안 기술 연구).

참 고 문 헌

[1] Changick Song, "Leakage Rate Analysis for Artificial Noise Assisted Massive MIMO With Non-Coherent Passive Eavesdropper in Block-Fading," *IEEE Trans. Wireless Commun.*, vol. 18, no. 4, pp. 2111-2124, Apr. 2019

[2] Sangseok Yun, *et al.* , "On the Secrecy Rate and Optimal Power Allocation for Artificial Noise Assisted MIMOME Channels", *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3098-2113, Apr. 2018