랜덤 스위치 안테나 배열의 수학적으로 정확한 보안 전송률

서정곤, 유병하, 정해준
인천대학교

{wnrlqnsek, syeon2513, haejoonjung}@inu.ac.kr

Mathematically Exact Secrecy Rate of Randomly Switched Antenna Arrays

Jung-gon Seo, Byungha You, Haejoon Jung
Dept. of Information and Telecommunication Engineering, Incheon National Univ.

요 약

본 논문은 물리계층 보안 (PLS: Physical-layer security)에 기반한 Antenna Subset Modulation (ASM) 기법에 대한 정확한 수학적 분석을 제공한다. ASM 기법 중 하나인 switched array 에 대한 기존의 근사적 이론 결과는 시뮬레이션 결과와는 다른 결과를 보였다. 이에 착안하여, 본 논문에서는 array factor 와 보안 전송률 (secrecy rate)에 대해 근사치 없이 수학적으로 분석하여 이들의 closed-form 표현을 제공한다. 또한, 높은 수치의 보안 전송률을 갖는 최적의 부분집합의 크기 (subset size)가 있음을 시뮬레이션 결과를 통해 보인다.

Ⅰ. 서 론

물리계층 보안 (PLS: Physical-layer security) 기술은 무선통신 과정에서 의도하지 않은 수신자(도청자)에게 정보가 유출되는 것을 최소화시키기 위해 무선 채널의 임의성을 활용한다 [1]. [2]에서 제안된 switched arrays 를 활용한 PLS 기술은 Antenna Subset Modulation (ASM) 기법 중의 하나로서, 송신자의 안테나를 매 전송 심볼마다 랜덤하게 두 파트로 나누어 전송하여 보안을 달성하는 방식이다. 하나는 신호를 보내는 부분집합이고 다른 하나는 보내지 않는 부분집합이며, 그 개수는 일정하게 유지된다. [2]의 저자들은 이러한 안테나 선택 과정을 베르누이 (Bernoulli) 랜덤변수로 근사화 하였다. 그러나 이것은 개별 안테나 요소를 일정 확률을 가지고 선택하는 것이기 때문에 매 심볼마다 부분집합 개수가 변하게 되는 결과로 이어진다. 따라서, 유한 개의 송신 안테나가 두 부분집합으로 나뉠 때 부분집합의 크기는 고정된 채 각각을 구성하는 요소만 달라지게 되는 실제 결과와는 거리가 있다.

이를 극복하기 위해, 본 논문에서는 고정된 개수의 안테나 요소가 랜덤하게 선택되는 과정에 상응하는 정확한 수학적인 분석을 수행한다. 이 분석을 통해 얻은 보안 전송률 (secrecy rate)에 대한 이론 값과 기존의 근사적 이론 값, 그리고 시뮬레이션을 통해 얻은 실험적 결과값을 비교한다. 또한, 높은 수치의 보안 전송률을 달성하는 최적의 부분집합 크기를 보인다.

Ⅱ. 본 론

2-1. 시스템 모델

서로 d 만큼 거리를 두고 있는 N개의 요소로 구성되는 uniform linear array (ULA) 안테나가 송신자에 장착되어 있다고 가정한다. 또한, 송신자로부터 각각 ρ_R, ρ_E 만큼 떨어져 있고 방위각 (azimuth angle)은 θ_R, θ_E 인 수신자와 도청자의 개별 위치는 (ρ_R, θ_R) (ρ_E, θ_E)와 같이 나타낸다. 수신 안테나 이득(안테나 수에 비례)은 각각 g_R, g_E 이고, 이들 모두 하나의 안테나를 가진다. 전송 데이터 심볼 $s(k) \in \mathbb{C}$은 $\mathbb{E}(|s(k)|^2) = 1$이며, 여기서 k는 transmit time index (TTI)를 나타낸다. 송신자가 프리코딩 (precoding) $w(k) = [w_1(k),\ w_2(k), \cdots, w_N(k)] \in \mathbb{C}^N$를 적용한다고 할 때 수신자는

$$y(\rho, \theta, k) = \sqrt{Pg}h^*(\rho, \theta)w(k)s(k) + z(k) \quad (1)$$

와 같이 표현되는 신호를 수신한다. 여기서, $z(k) \sim CN(0, \sigma^2)$ 은 부가 잡음이며 $h^*(\rho, \theta)$ 은 (ρ, θ) 에 위치한 수신자의 $1XN$ 크기의 채널 벡터이다. 여기서 x^* 은 복소수 x 의 켤레이다. [2]에 따라 가시거리 (LOS: line-of-sight) 채널을 가정하면, n번째 송신 안테나와 수신자 사이의 채널에 해당하는 n번째 채널 벡터는 다음과 같다.

$$h_n^*(\rho, \theta) = \frac{1}{\rho} e^{-j(\frac{N+1}{2} - n)\frac{2\pi d}{\lambda} cos\theta}$$

2-2. ASM 기법

[1]의 틀을 차용하여 진폭 weight 벡터를 $w(k) = \frac{1}{\sqrt{M}}[b(k) \odot \mathrm{h}(1, \theta_R)]$ 와 같이 정의한다. 여기서, 연산자 $\odot$ 는 아다마르 곱 (Hadamard product)이고, $b(k) = [b_1(k), b_2(k), \cdots, b_N(k)] \in \mathcal{B}$ 의 요소는 0 또는 1 을 취하며(즉, $b_n(k) \in \{0,1\}$), 여기서 $\mathcal{B}$ 는 가능한 모든 안테나의 조합을 의미한다. 달리 말하면, N개의 안테나 중 M개는 weight 값 1을 취하고, 나머지 $(N-M)$개는 0값을 취하도록 설정되는 것이다. n번째 안테나 요소의 프리코딩 weight $w_n(k)$는 다음과 같다.

$$w_n(k) = \begin{cases} \frac{1}{\sqrt{M}} e^{j(\frac{N+1}{2} - n)\frac{2\pi d}{\lambda} cos\theta_R}, & n \in L_M(k) \\ 0, & n \in L_M^C(k) \end{cases} \quad (2)$$

여기서 $L_M(k)$ 은 M 개, $L_M^C(k)$ 은 $(N-M)$ 개의 안테나 요소가 들어있는 랜덤부분집합이다. [2]에서는 (2)가, 전자의 값을 가질 확률은 $\frac{M}{N}$ 이고 후자는 $1 - \frac{M}{N}$ 인 independent and identically distributed (i.i.d.) 베르누이 랜덤변수로 근사화 되었다. 이러한 근사 모델 하에서는 $L_M(k)$와 $L_M^C(k)$의 cardinality 가 랜덤인 반면, 실제로는 $M, (N-M)$개로 고정되어 있다. 정확한 값을 구하기 위해 N 개의 원소를 가지는 유한한 전체 집합에서 크기 M 의 부분집합을 비복원추출함으로써 분석을 진행한다. (2)를 (1)에 대입하여 정리하면 다음과 같다.

$$\begin{aligned} y(\rho, \theta, k) &= \sqrt{Pg}h^*(\rho, \theta)w(k)s(k) + z(k) \\ &= \frac{\sqrt{Pg}}{\rho}\frac{s(k)}{\sqrt{M}} \sum_{n=1}^{N} b_n(k) e^{j(\frac{N+1}{2} - n)\psi(\theta)} + z(k) \\ &= \sqrt{Pg}\, s(k)\, \mathcal{F}(\rho, \theta, k) + z(k) \end{aligned} \quad (3)$$

여기서, $\mathcal{F}(\rho,\theta,k)=\frac{1}{\rho\sqrt{M}}\sum_{n=1}^{N}b_n(k)e^{j(\frac{N+1}{2}-n)\psi(\theta)}$ 는 array factor 이다 ($\psi(\theta)=\frac{2\pi d}{\lambda}(\cos\theta_R-cos\theta)$). 정보가 안정적이고 안전하게 전송될 수 있는 최대 data rate 인 보안 전송률은 다음과 같이 정의된다.

$$\eta=[C_E-C_R]^+=[\log_2(1+\gamma_E)-\log_2(1+\gamma_R)]^+ \quad (4)$$

여기서, $[x]^+=\max(0,x)$ 를 나타낸다. 보안 전송률은 무선통신 보안을 측정하기 위한 주된 지표이고, 이것은 수신자의 용량 (capacity) $C_R=\log_2(1+\gamma_R)$ 와 도청자의 용량 $C_E=\log_2(1+\gamma_E)$ 의 차에 의해 계산된다. $\gamma_R=\frac{Pg_R|\mathbb{E}[\mathcal{F}(\rho_R,\theta_R,k)]|^2}{Pg_R\mathbb{V}ar[\mathcal{F}(\rho_R,\theta_R,k)]+\sigma^2}$ 은 수신자의 신호 대 잡음비 (SNR: signal-to-noise ratio)이고, $\gamma_E=c$ 는 도청자의 SNR 이다.

2-3. Array Factor 통계치 및 보안 전송률 분석

유한한 전체집합에서 샘플을 비복원추출하는 일반적인 수학적 기법이 제시된 [3]의 틀을 따라, $\beta_\theta=\sum_{n\in L_M(k)}e^{j(\frac{N+1}{2}-n)\psi(\theta)}$, $u_n=e^{j(\frac{N+1}{2}-n)\psi(\theta)}$, $(n=1,2,\cdots,N)$라 하자. 비복원추출된 M 개의 샘플이 $v_1,\ldots,v_M$ 라 할 때, β_θ 는 이들의 총합 $\sum_{n=1}^{M}v_n$에 대응되므로,

$$\mathcal{F}(\rho,\theta,k)=\frac{1}{\rho\sqrt{M}}\Big[\sum_{n\in L_M(k)}e^{j(\frac{N+1}{2}-n)\psi(\theta)}\Big]=\frac{1}{\rho\sqrt{M}}\beta_\theta \quad (5)$$

와 같이 array factor 가 정리되며 그 평균은 다음과 같다.

$$\mathbb{E}[\mathcal{F}(\rho,\theta,k)]=\frac{1}{\rho\sqrt{M}}\mathbb{E}[\beta_\theta] \quad (6)$$

[3]의 공식에 의거하여 β_θ의 평균은

$$\mathbb{E}[\beta_\theta]=\mu_{\beta_\theta}=\sum_{n=1}^{N}P(u_n)u_n=\frac{M}{N}\sum_{n=1}^{N}u_n \quad (7)$$

으로 나타낼 수 있고(여기서 $\sum_{n=1}^{N}u_n=\frac{\sin(N\psi(\theta)/2)}{\sin(\psi(\theta)/2)}$이다.), (7)을 (6)에 대입하여 정리하면 다음과 같다.

$$\mathbb{E}[\mathcal{F}(\rho,\theta,k)]=\frac{1}{\rho\sqrt{M}}\frac{M}{N}\frac{sin(N\psi(\theta)/2)}{sin(\psi(\theta)/2)} \quad (8)$$

다른 한 편, (5)의 분산은 아래와 같다.

$$\mathbb{V}ar[\mathcal{F}(\rho,\theta,k)]=\frac{1}{\rho^2M}\mathbb{V}ar[\beta_\theta] \quad (9)$$

$\mathbb{V}ar[\beta_\theta]=\mathbb{E}[|\beta_\theta|^2]-|\mu_{\beta_\theta}|^2$에서, $\mathbb{E}[|\beta_\theta|^2]$는

$$\begin{aligned}\mathbb{E}[|\beta_\theta|^2]&=\mathbb{E}[\textstyle\sum_{n=1}^{M}|v_n|^2]+\mathbb{E}[\sum_{n=1}^{M}\sum_{m\neq n}v_nv_m^*]\\&=M\Big(1-\frac{M-1}{N-1}\Big)+\frac{M}{N}\frac{M-1}{N-1}\frac{sin(N\psi(\theta)/2)}{sin(\psi(\theta)/2)}\end{aligned} \quad (10)$$

이다 [3]. 따라서 (7), (10)을 이용해 구한 $\mathbb{V}ar[\beta_\theta]$ 는 다음과 같다.

$$\mathbb{V}ar[\beta_\theta]=\frac{M(N-M)}{N^2(N-1)}\Big(N^2-\frac{\sin^2(N\psi(\theta)/2)}{\sin^2(\psi(\theta)/2)}\Big) \quad (11)$$

(9)와 (11)에 의해, 분산을 다음과 같이 얻는다.

$$\mathbb{V}ar[\mathcal{F}(\rho,\theta,k)]=\frac{1}{\rho^2M}\frac{M(N-M)}{N^2(N-1)}\Big(N^2-\frac{\sin^2(N\psi(\theta)/2)}{\sin^2(\psi(\theta)/2)}\Big) \quad (12)$$

앞서 구한 array factor 의 평균 (8)과 분산 (12)을 이용해 각 수신자들의 SNR 을 구하면, (ρ_R,θ_R)에 위치한 수신자의 SNR 은

$$\gamma_R=\frac{Pg_RM^2}{\rho_R^2\sigma^2M} \quad (13)$$

이고, (ρ_E,θ_E)에 위치한 도청자의 SNR 은

$$\gamma_E=\frac{\frac{Pg_E}{\rho_E^2}\frac{M^2}{N^2}\frac{\sin^2(N\psi(\theta)/2)}{\sin^2(\psi(\theta)/2)}}{\frac{Pg_EM}{\rho_E^2M}\frac{M(N-M)}{N^2(N-1)}\Big(N^2-\frac{\sin^2(N\psi(\theta)/2)}{\sin^2(\psi(\theta)/2)}\Big)+\sigma^2} \quad (14)$$

이다. (13), (14)의 SNR 을 (4)에 대입하여 정확한 보안 전송률을 다음과 같이 얻는다.

$$\eta=\left[\log_2\Big(1+\frac{Pg_RM^2}{\rho_R^2\sigma^2M}\Big)-\log_2\Big(1+\frac{\frac{Pg_E}{\rho_E^2}\frac{M^2}{N^2}\frac{\sin^2(N\xi(\theta)/2)}{\sin^2(\xi(\theta)/2)}}{\frac{Pg_EM}{\rho_E^2M}\frac{M(N-M)}{N^2(N-1)}\Big(N^2-\frac{\sin^2(N\xi(\theta)/2)}{\sin^2(\xi(\theta)/2)}\Big)+\sigma^2}\Big)\right]^+ \quad (15)$$

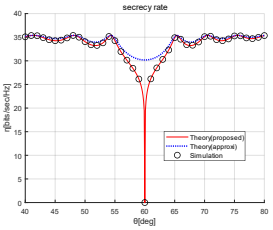

Fig. 1. $N=24$, $M=18,\theta_R=60^\circ,\rho_R=10,\rho_R=20$, $P=10^{12}$ 일 때, 보안 전송률

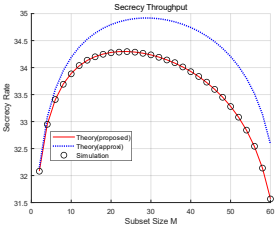

Fig. 2. $N=64,\theta_R=60^\circ,\theta_E=63^\circ,\rho_E=10,\rho_R=20$, $P=10^{12}$ 일 때, M에 따른 보안 전송률

2-4. 시뮬레이션 결과

이번 장에서는, 앞서 얻은 보안 전송률을 시뮬레이션 결과와 비교하여 분석의 타당성을 검증한다. 주파수는 5GHz, g_R=$g_E=1$, $d=\lambda/2$로 가정한다. Fig. 1 은, $\theta=\theta_R=60^\circ$ 근처에서 큰 에러를 보이는 기존 i.i.d. 모델과 달리, 본 논문의 분석에 의한 보안 전송률은 시뮬레이션 결과와의 높은 일치성을 보여준다. Fig. 2 는 부분 집합의 크기가 변함에 따라 보안 전송률이 어떻게 변하는지를 시뮬레이션을 통해 보여주며, 가장 높은 보안 전송률을 달성하는 최적의 부분집합 크기가 존재함을 알 수 있다.

Ⅲ. 결론

본 논문에서는 무선 채널을 도청자로부터 효과적으로 보호할 수 있는 PLS 기술인 ASM 기법에 대한 기존 근사 모델의 한계를 명확히 하고, array factor 통계치 및 보안 전송률에 대한 정확한 이론적 분석을 제공하였다. 이것은 유한한 전체집합에서 샘플을 비복원추출하는 모델링을 통해 이루어졌다. 제안된 수학적 모델과 기존 i.i.d. 베르누이 모델, 그리고 시뮬레이션의 보안 전송률을 비교한 결과를 제시하여, 본 논문 분석의 타당성을 평가 및 증명하였다. 나아가, 부분집합의 크기 설정에 따른 보안 전송률 변화 양상을 시뮬레이션을 통해 살펴보았고, 보안 전송률을 가장 많이 향상시키는 최적의 부분집합의 크기가 존재함을 보였다.

ACKNOWLEDGMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. NRF-2021M1A2A2061357).

참 고 문 헌

[1] B. You, I. Lee and H. Jung, "Exact Secrecy Rate Analysis of Antenna Subset Modulation Schemes," *IEEE Syst. J.*, to be published, doi: 10.1109/JSYST.2020.3017163.

[2] N. Valliappan, A. Lonzano, and R. W. Heath, "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Commun. Surv. Tut.*, vol. 19, no. 2, pp. 1027-1053, Apr.-Jun. 2017

[3] D. G. Horvitz and D. J. Thompsom, "A generalization of sampling without replacement from a finite universe," *J. Amer. Statist. Assoc.*, vol.47, no. 260, pp. 663-685, 1952.