JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 20, No. 3 : 558~564 Mar. 2016

인공 잡음 및 송수신기 보호 구역을 활용한 보안 성능 향상

채승호*

Secrecy Enhancement via Artificial Noise with Protected Zones of Transmitter and Receiver

Seong Ho Chae*

School of Electrical Engineering, Korea Advanced Institute of Science and Technology, Daejeon 34141, Korea

요 약

네트워크 간섭은 수신기 및 도청기의 디코딩을 방해함에 따라, 보안 및 서비스 품질에 긍정 및 부정적 영향을 동시에 미친다. 인공 잡음의 전송은 이러한 네트워크 간섭의 상충되는 영향을 간접적으로 제어 가능하게 한다. 본 논문은 송수신기 보안 보호 구역 및 인공 잡음 전송을 활용한 보안 성능 향상 기법을 제안하고, 확률 기하 이론을 통해 성능 이득을 분석한다. 먼저, 송수신기 사이 거리, 송수신기 보호 구역 크기에 따른 서로 다른 4가지 시나리오에 대해, 임의의 인공 잡음 전송에 대한 연결 실패 확률과 보안 실패 확률을 분석한다. 다음으로, 보안 전송율을 분석하고, 이의 최대화를 위한 최적 인공 잡음 전송 전력비를 찾는다. 마지막으로, 시뮬레이션을 통해, 보호 구역 크기와 같은 다양한 시스템 파라미터들의 최적 인공 잡음 전송 전력비에 대한 영향을 살펴본다.

ABSTRACT

The network interference gives positive and negative effects to security and QoS simultaneously by disturbing the decoding of receiver and eavesdropper. The transmission of artificial noise enables to indirectly control these contradicting effects. This paper proposed the secrecy enhancement technique via artificial noise with protected zones of transmitter and receiver and investigated its gain by using stochastic geometry. For given arbitrary artificial noise power ratio, we first analyzed connection outage probability and secrecy outage probability for four different scenarios (separated, overlapped, included secrecy protected zones- type A, B) according to distance and size of protected zones of the transmitter and receiver. We then derive the secrecy transmission rate and find the optimal artificial noise power ratio to maximize it. Finally, with numerical examples, we investigate the effects of the system parameters such as size of protected zones of transmitter and receiver on the optimal artificial noise power ratio.

키워드 : 물리 계층 보안, 보안 전송율, 인공 잡음, 보호 구역

Key word : Physical Layer Security, Secrecy Transmission Rate, Artificial Noise, Protected Zones

Received 28 January 2016, **Revised** 11 February 2016, **Accepted** 25 February 2016

* **Corresponding Author** Seong Ho Chae (E-mail:shchae82@kaist.ac.kr, Tel:+82-42-350-7526)
School of Electrical Engineering, Korea Advanced Institute of Science and Technology, Daejeon 34141, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2016.20.3.558 print ISSN: 2234-4772 online ISSN: 2288-4165

This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(http://creativecommons.org/li-censes/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright Ⓒ The Korea Institute of Information and Communication Engineering.

Ⅰ. 서 론

최근 스마트 폰과 같은 무선 통신 기기의 보급으로 인해 모바일 뱅킹, 전자 결제 등 다양한 서비스가 이루어짐에 따라, 고도의 보안 기술이 요구 되고 있다. 최근, 물리 계층에서의 네트워크 보안 향상 방안에 대한 관심이 증가함에 따라, 보호 구역(protected zone) 설치, 인공 잡음(artificial noise) 전송, 방향성 안테나를 통한 섹터화 전송(sectored transmission)등 다양한 보안 향상 기법들이 개발되었다[1-5]. 최근, [4, 5]에서, 송신기가 하나의 보호구역을 가질 때, 인공 잡음 활용에 따른 보안 향상 이득에 관한 연구가 진행되었으나, 아직까지 송수신기가 동시에 보호 구역을 가질 때, 최적 인공 잡음 활용 방안에 대한 연구는 이루어지지 않았다.

본 논문에서는 송수신기 각각 서로 다른 크기의 보호 구역을 가지고, 도청기가 보호 구역 외부에서 도청을 시도할 때, 보호 구역 크기에 따른 서로 다른 4가지 시나리오에 대해, 네트워크 보안 향상을 위한 최적 인공 잡음 전송 방법을 탐구한다. 이를 위해 먼저 확률 기하 이론을 바탕으로, 연결 실패 확률 및 보안 실패 확률 을 분석하고, 보안 전송율 최대화를 위한 최적 인공 잡음 전송 전력비를 찾는다. 마지막으로, 다양한 실험 평가를 통해 분석된 이론적 결과들을 검증하고, 보호 구역 반지름, 최대 허용 가능 연결/보안 실패 확률 등 다양한 시스템 파라미터에 따른 최적 인공 잡음 전력비의 변화와 보안 향상 이득을 살펴 본다.

본 논문의 구성은 다음과 같다. II장에서 본 논문에서 고려하는 시스템 모델과 성능 지표를 설명하고, III장에서 4가지 시나리오에 대해 연결 및 보안 실패 확률, 보안 전송율을 분석하고, 최적 인공 잡음 전력비를 찾는다. IV장에서는 모의 실험을 통해 최적 인공 잡음 전력비에 대한 시스템 파라미터들의 영향을 살펴본다. 마지막으로, V장에서 결론을 맺는다.

Ⅱ. 시스템 모델 및 성능 지표

그림 1은 송신기(Alice)가 수신기(Bob)에 보안 메시지를 전송하고, 임의로 위치한 도청기들 (Eves)이 송신기의 메시지를 도청하고 있고, 복수 개의 간섭원들 (Interferers)이 Bob과 Eves에 동시에 간섭을 미치고 있

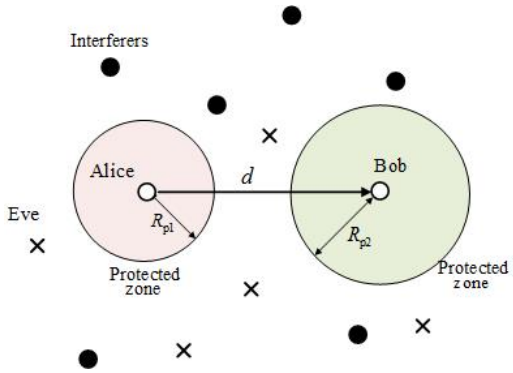


Fig. 1 System model

는 애드혹 네트워크를 나타낸다. Alice와 Bob은 2D 평면에서 각각 원점과 (d,0)에 위치함을 가정한다. Alice와 Bob은 주변에 각각 서로 다른 크기의 도청으로부터 자유로운 보호 구역 (Eve들이 존재할 수 없는 특정 영역)을 가진다. 보호 구역은 출입 통제 구역 또는 보안 펜스와 같은 물리적인 시설 또는 주변 지역 기기를 활용한 도청기 사전 검출로 형성될 수 있다. 이러한, 보호 구역은 각각 Alice와 Bob을 중심으로 반지름 $R_{p1}(>0)$와 $R_{p2}(>0)$의 원으로 모델링 가능하다.

간섭원 및 Eve들은 2D 평면의 임의의 위치에 존재하며, 이를 밀도 λ_I와 λ_E의 독립 균등 푸아송 포인트 프로세스(Poisson Point Process)로 모델링 한다. i번째 간섭원의 위치를 X_i로 표기하고, 모든 간섭원들의 위치 집합을 $\Phi_I = \{X_1, X_2, \ldots\}$로 표기한다. 각 노드들은 동일한 전송 전력 P를 가지며, 모든 전송 신호들은 지수승 α의 신호 감쇄(pathloss exponent)를 겪는다. 모든 채널 페이딩 이득은 독립적이고 동일한 (independent and identically distributed: i.i.d) 평균이 1인 지수분포(exponential)를 따름을 가정한다. 네트워크 내의 모든 노드들은 단일 안테나를 가지며, Alice는 모든 노드들에 대한 채널 정보(Channel State Information)가 없으며, Bob까지의 거리 d 에 대한 정보만 가지고 있음을 가정한다. 네트워크 간섭에 비해 열 잡음이 거의 무시될 수 있을 정도로 작은 간섭 우세 환경을 가정한다.

Alice는 중첩 구조의 Wyner 인코딩 스킴 [5]을 사용하여 보안 메시지를 전송하는데, 전송되는 코드워드 전송율은 R_T이고, 그 중 실제 전송 보안 메시지 전송율은 $R_S(<R_T)$이다. 두 전송율 R_T와 R_S의 차이 $R_E = R_T - R_S$는 보안 통신을 위한 추가 발생 전송율이다. Alice와

Bob 사이의 채널 용량이 R_T보다 크고 Alice와 Eve의 채널 용량이 R_E보다 작을 경우, Alice는 Bob에게 레전 송율 R_S의 보안 메시지를 도청 없이 성공적으로 전송 가능하다. 따라서, 다음과 같은 두 가지 실패 사건(outage event)을 정의할 수 있다.

- E_{co}(연결 실패(connection outage)): Alice와 Bob 사이의 채널 용량이 R_T보다 작아, Bob이 전송된 코드워드 디코딩에 실패
- E_{so}(보안 실패(secrecy outage)): Eve들 중에서, Alice와 Eve 사이에 채널 용량이 R_E보다 큰 Eve가 적어도 하나 이상 존재하여 보안에 실패

한편, Alice는 Eve의 메시지 디코딩을 방해하기 위해, 자신의 전송 전력 일부를 가우시안 인공 잡음에 할당하여, 코드워드 및 인공 잡음을 동시에 전송한다. 즉, Alice는 코드워드를 ξP의 전송 전력으로, 인공 잡음을 $(1-\xi)P$의 전송 전력으로 동시에 전송한다. 여기서, $\xi \in (0,1]$는 전송 전력 비율이다. Bob에서의 수신 신호 대비 간섭 비율 (Signal to interference ratio: SIR)은 다음과 같이 표현된다.

$$\gamma_B(\xi) = \frac{\xi P G_{BA} d^{-\alpha}}{\sum_{i \in \Phi_I} P G_{Bi} |X_{Bi}|^{-\alpha} + (1-\xi) P G_{BA} d^{-\alpha}} \quad (1)$$

여기서, G_{BA}는 Alice와 Bob사이의 채널 이득, G_{Bi}는 Bob과 간섭원 i사이의 채널 이득, $|X_{Bi}|$는 Bob과 간섭원 i사이의 거리를 의미한다. 유사하게, Eve k의 수신 신호 대비 간섭 비율은 다음과 같이 표현된다.

$$\gamma_E^{(k)}(\xi) = \frac{\xi P G_{kA} |Y_{kA}|^{-\alpha}}{\sum_{i \in \Phi_I} P G_{ki} |Y_{ki}|^{-\alpha} + (1-\xi) P G_{kA} |Y_{kA}|^{-\alpha}} \quad (2)$$

여기서, G_{kA}는 Alice와 Eve k사이의 채널 이득, 는 Eve와 간섭원 사이의 채널 이득, G_{ki}는 Eve k와 간섭원 i 사이의 거리, $|Y_{kA}|(=|Y_k|)$는 Alice와 Eve k사이의 거리를 의미한다.

전력비 ξ의 증가는 Bob과 Eve의 수신 신호 대비 간섭 비율을 동시에 증가시키므로, 연결 실패 확률을 감소시킴에 반해 보안 실패 확률은 증가하는 트레이드 오프(trade-off)관계를 가진다. 따라서, 임의의 전송 전력비 $\xi \in (0,1]$에 대해서, 연결 실패 확률과 보안 실패 확률은 다음과 같이 쓸 수 있다.

$$\Pr[E_{co}|\xi] = E_{\Phi_I}\{\Pr[\gamma_B(\xi) \le \beta_T | \Phi_I]\} \quad (3)$$

$$\Pr[E_{so}|\xi] = E_{\Phi_I, \Phi_E}\left\{\Pr[\max_{k \in \Phi_E} \gamma_E^{(k)}(\xi) > \beta_E | \Phi_I, \Phi_E]\right\} \quad (4)$$

여기서, $\beta_T = 2^{R_T} - 1$와 $\beta_E = 2^{R_E} - 1$는 각각 연결 실패 및 보안 실패 에 대한 임계 수신 신호 대비 간섭 비율이다. 연결 실패 및 보안 실패 사건이 동시에 발생하지 않을 때, 전송율 R_S의 보안 메시지를 Bob에게 성공적으로 전송 가능하다. 따라서, 본 논문에서 보안 메시지 전송 성공에 관한 성능 지표로서, 보안 전송율(secrecy transmission rate) 을 다음과 같이 정의한다 [4].

$$R = R_S(1 - \Pr[E_{co}|\xi])(1 - \Pr[E_{so}|\xi]) \quad (5)$$

Ⅲ. 성능 분석

3.1. 보안 실패 확률 분석

Alice의 보호 구역 반지름이 R_{p1}이고, Bob의 보호 구역 반지름이 R_{p2}일 때, 보안 실패 확률을 분석한다. 식 (4)의 보안 실패 확률은 다음과 같이 쓸 수 있다.

$$\Pr[E_{so}|\xi] = 1 - E_{\Phi_I, \Phi_E}\left\{\Pi_{k \in \Phi_E} \Pr[\gamma_E^{(k)}(\xi) \le \beta_E | \Phi_I, \Phi_E]\right\}. \quad (6)$$

임의의 Eve k에 대한 보안 실패 확률은 다음과 같다.

$$\Pr[\gamma_E^{(k)}(\xi) \le \beta_E | \Phi_I, \Phi_E] = 1 - \exp\left(-\frac{|Y_k|^{\alpha} \beta_E I_{\Phi_I}^{(k)}}{P[(1+\beta_E)\xi - \beta_E]}\right) \cdot 1\left(\xi > \frac{\beta_E}{1+\beta_E}\right) \quad (7)$$

여기서, $I_{\Phi_I}^{(k)} = \sum_{i \in \Phi_I} P G_{ki} |Y_{ki}|^{-\alpha}$로 Eve k에 간섭 전력, $1(A)$는 A의 조건이 만족하면 1값을 반환하고 만족하지 않으면 0을 반환하는 표시(indicator)함수이다. Eve들의 간섭 전력들 $\{I_{\Phi_I}^{(k)} | k \in \Phi_E\}$ 사이에는 주어진 간섭원들의 위치로 인해 서로 상관관계를 가지고, 이는 분석을 매우 어렵게 한다. 하지만, 최근, 간섭 전력들의 상관관계를 무시하는 것이 상관관계가 있을 때의 실제 성능에 매우 미미한 영향을 미치는 것이 밝혀졌다[4,5]. 이러한 사실로부터, 간섭원들의 위치가 각 Eve에 대해서, 서로 독립적임을 가정하면, 다음과 같은 수식을 얻을

수 있다.

$$\begin{aligned} & E_{\Phi_I,\Phi_E}\left\{\Pi_{k\in\Phi_E}\Pr[\gamma_E^{(k)}(\xi)\le\beta_E|\Phi_I,\Phi_E]\right\} \\ & \simeq E_{\Phi_E}\left\{\Pi_{k\in\Phi_E}E_{\Phi_I}\left\{\Pr[\gamma_E^{(k)}(\xi)\le\beta_E|\Phi_I,\Phi_E]\right\}\right\} \end{aligned} \tag{8}$$

$$\begin{aligned} & \overset{(a)}{=} E_{\Phi_E}\left\{\Pi_{k\in\Phi_E}\left[1-K_{\beta_E}(\xi,|Y_k|)\right]\right\} \\ & = \exp\left(-\lambda_E\int_S K_{\beta_E}(\xi,|Y_k|)1\left(\xi>\frac{\beta_E}{1+\beta_E}\right)\right) \end{aligned} \tag{9}$$

식 (9)의 등호 (a)는 다음 관계식에 의해 성립한다.

$$\begin{aligned} & E_{\Phi_I}\left\{\Pr\left[G_{kA}\le\frac{|Y_k|^\alpha\beta_E I_{\Phi_I}^{(k)}}{P[(1+\beta_E)\xi-\beta_E]}\right]\right\} \\ & \overset{(b)}{=} 1-\exp\left(-\lambda_I|Y_k|^2\left(\frac{\beta_E}{(1+\beta_E)\xi-\beta_E}\right)^{2/\alpha}C_0^\alpha\right) \end{aligned} \tag{10}$$

여기서, $C_0^\alpha=2\pi^2/\alpha\csc(2\pi/\alpha)$ 이고,

$K_{\beta_E}(\xi,|Y_k|)=\exp(-\lambda_I|Y_k|^2(\frac{\beta_E}{[(1+\beta_E)\xi-\beta_E]})^{2/\alpha}C_0^\alpha)$.

식 (10)의 등호 (b)는 $I_{\Phi_I}^{(k)}$의 적률 생성 함수 (moment generating function: MGF)로부터 성립한다[6].

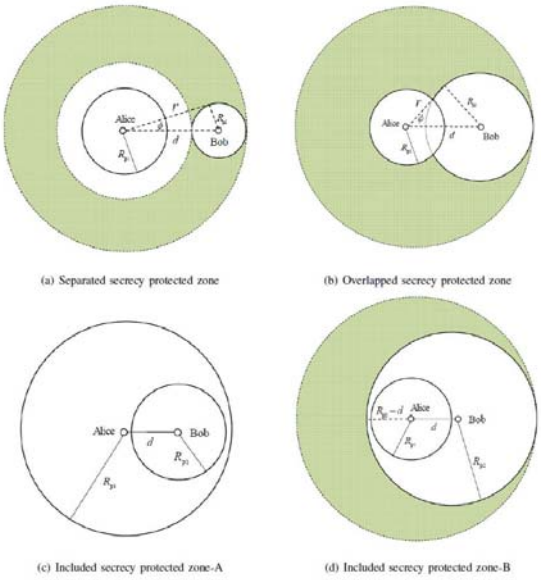


Fig. 2 Four different cases: (a) Separated secrecy protected zone, (b) Overlapped secrecy protected zone, (c) Included secrecy protected zone – Type A, (d) Included secrecy protected zone – Type B

식 (9)의 적분 영역 구간 S는 Alice의 보호 구역 반지름 R_{p1}, Bob의 보호 구역 반지름 R_{p2}, Alice와 Bob 사이의 거리 d에 의해, 그림 2와 같이 (a) 분리 보안 보호 구역 (SP), (b) 중복 보안 보호 구역 (OP), (c) 포함 보안 보호 구역 – Type A (IP-A), (d) 포함 보안 보호 구역 – Type B (IP-B)로 4가지 시나리오로 구분된다.

각 시나리오 s∈{SP, OP, IP-A, IP-B}에 해당하는 보안 실패 확률은 다음과 같다.

• Case 1 (SP): 분리 보안 보호 구역 (Alice와 Bob의 보호구역이 서로 중첩되지 않는 경우, 즉, $R_{p2}\le d-R_{p1}$)

$$\begin{aligned} & \Pr[E_{so}|\xi,s=SP]\approx \\ & \exp(-2\pi\lambda_E\int_{R_{p1}}^{\infty}K_{\beta_E}(\xi,r)1\left(\xi>\frac{\beta_E}{1+\beta_E}\right)rdr \\ & +2\lambda_E\int_{R_{p1}}^{\infty}\phi(r)K_{\beta_E}(\xi,r)1\left(\xi>\frac{\beta_E}{1+\beta_E}\right)rdr) \end{aligned} \tag{11}$$

여기서, $\phi(r)=\arccos\left(\frac{r^2+d^2-R_{p2}^2}{2rd}\right)$

$$K_{\beta_E}(\xi,r)=\exp(-\lambda_I r^2(\frac{\beta_E}{[(1+\beta_E)\xi-\beta_E]})^{2/\alpha}C_0^\alpha),$$

• Case 2 (OP): 중복 보안 보호 구역 (Alice와 Bob의 보호구역이 일부 중첩 되는 경우, 즉,

$R_{p1}<d,\ d-R_{p1}<R_{p2}<d$, 또는
$R_{p2}<d,\ d<R_{p1}<d+R_{p2}$, 또는
$R_{p1}<d,\ d<R_{p2}<d+R_{p1}$, 또는
$R_{p1}>d,\ R_{p2}>d$)

$$\begin{aligned} & \Pr[E_{so}|\xi,s=OP]\approx \\ & \exp(-2\pi\lambda_E\int_{R_{p1}}^{\infty}K_{\beta_E}(\xi,r)1\left(\xi>\frac{\beta_E}{1+\beta_E}\right)rdr \\ & +2\lambda_E\int_{R_{p1}}^{d+R_{p2}}\phi(r)K_{\beta_E}(\xi,r)1\left(\xi>\frac{\beta_E}{1+\beta_E}\right)rdr) \end{aligned} \tag{12}$$

• Case 3 (IP-A): 포함 보안 보호 구역-Type A (Alice의 보호구역이 Bob의 보호구역을 포함하는 경우, 즉, $R_{p2}<R_{p1}-d$)

$$\begin{aligned} & \Pr[E_{so}|\xi,s=IP-A]\approx \\ & \exp(-2\pi\lambda_E\int_{R_{p1}}^{\infty}K_{\beta_E}(\xi,r)1\left(\xi>\frac{\beta_E}{1+\beta_E}\right)rdr) \end{aligned} \tag{13}$$

• Case 4 (IP-B): 포함 보안 보호 구역-Type B
(Bob의 보호구역이 Alice의 보호구역을 포함하는 경우, 즉, $R_{p2} > d + R_{p1}$)

$$\Pr[E_{so}|\xi, s = IP-B] \approx \exp(-2\pi\lambda_E \int_{R_{p2}-d}^{\infty} K_{\beta_E}(\xi, r) 1\left(\xi > \frac{\beta_E}{1+\beta_E}\right) rdr + 2\lambda_E \int_{R_{p2}-d}^{R_{p2}+d} \phi(r) K_{\beta_E}(\xi, r) 1\left(\xi > \frac{\beta_E}{1+\beta_E}\right) rdr) \quad (14)$$

3.2. 연결 실패 확률 분석

Alice와 Bob 사이의 거리가 d일 때, 연결 실패 확률은 다음과 같다.

$$\Pr[E_{co}|\xi] = E_{\Phi_I}\{\Pr[\gamma_B(\xi) \le \beta_T|\Phi_I]\} = E_{\Phi_I}\left\{\Pr\left[\frac{\xi P G_{BA} d^{-\alpha}}{\sum_{i \in \Phi_I} P G_{Bi} |X_{Bi}|^{-\alpha} + (1-\xi) P G_{BA} d^{-\alpha}} \le \beta_T|\Phi_I\right]\right\} \quad (15)$$

3.1장의 증명 과정과 유사한 과정을 통하면, 다음과 같은 연결 실패 확률을 얻을 수 있다.

$$\Pr[E_{co}|\xi] = 1 - \exp(-K_{\beta_T}(\xi) d^2) 1\left(\xi > \frac{\beta_T}{1+\beta_T}\right) \quad (16)$$

여기서, $K_{\beta_T}(\xi) = \lambda_I \left(\frac{\beta_T}{[(1+\beta_T)\xi - \beta_T]}\right)^{2/\alpha} C_0^{\alpha}$.

3.3. 보안 전송율과 최적 인공 잡음 전송

3.1과 3.2장에서 분석한 각 시나리오에 대한 보안 실패 확률 (11)-(14)과 연결 실패 확률 (16)로부터, 보안 전송율 (5)는 다음과 같다.

$$R = R_S[\exp(-K_{\beta_T}(\xi) d^2)] \times [1 - \Pr[E_{so}|\xi, s]] \quad (17)$$

여기서, 각 s∈{SP, OP, IP-A, IP-B}에 대해, $\Pr[E_{so}|\xi, s] = \{$식(11), 식(12), 식(13), 식(14)$\}$이다.

한편, $\beta_T > \beta_E$이므로, 항상 $\frac{\beta_T}{1+\beta_T} > \frac{\beta_E}{1+\beta_E}$를 만족하므로, $\xi > \frac{\beta_T}{1+\beta_T}$에서 0이 아닌 보안 전송율을 가진다. 따라서, 보안 전송율 최대화를 위한 최적 인공 잡음 전력비는 다음과 같다.

$$\xi^* = \max_{\frac{\beta_T}{1+\beta_T} < \xi \le 1} R \quad (18)$$

s = IP-A의 경우, [4]에서 제안된 알고리즘을 통해 효율적으로 찾을 수 있으며, SP, OP, IP-B는, $(\frac{\beta_T}{1+\beta_T}, 1]$의 제한된 범위에서 1차원 조사를 통해 최적 전력비를 찾을 수 있다.

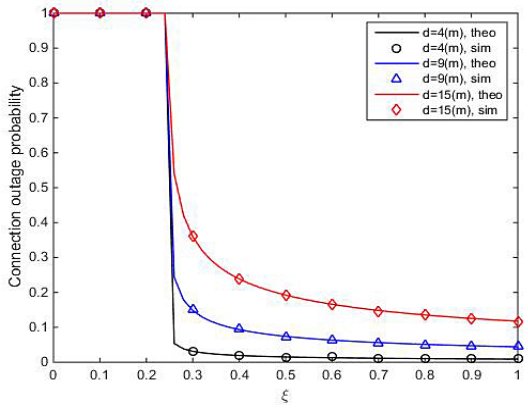
Ⅳ. 모의 실험

본 장에서는 III장에서 분석한 이론적 결과들을 검증하고, 시뮬레이션 파라미터들에 따른 최적 인공 잡음 비율의 변화를 살펴본다. 표 1은 시뮬레이션 변수의 종류와 값을 나타낸다.

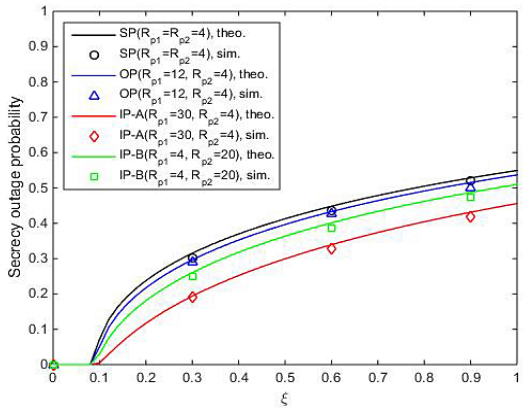
Table. 1 Simulation Parameters

Parameter	Value
Transmit Power P [dBm]	43
Distance between Alice and Bob d [m]	9
Pathloss exponent α	4
Alice protected zone radius R_{p1}[m]	4
Bob protected zone radius R_{p2} [m]	4
Interferers density λ_I[units/m^2]	0.0002
Eve density λ_E[units/m^2]	0.00008
$\beta_E(\beta_T)$[dBm]	20(25)

그림 3은 각각 Alice와 Bob 사이의 거리 d와 Alice 및 Bob의 보호 구역 반지름의 변화에 따른, ξ의 함수로서 연결 실패 및 보안 실패 확률을 보여준다. 3.1장과 3.2장에서 분석된 이론적 결과값(theo로 표기)이 실제 환경에서의 시뮬레이션 성능 결과값(sim로 표기)과 일치하는 것을 보여준다. 그림 3-(a)는 Alice와 Bob 사이의 거리가 증가함에 따라, 연결 실패 확률이 증가함을 보여준다. 그림 3-(b)는 Alice와 Bob의 보호 구역이 커짐에 따라, 보안 실패 확률이 감소하는 것을 보여준다. 그림 3에서 ξ의 증가에 따라, 연결 실패 확률은 감소하지만, 보안 실패 확률은 증가한다. 따라서, 연결 실패 확률 및 보안 실패 확률을 적절하게 조절해 주는 것이 필요하다.



(a)



(b)

Fig. 3 (a) Connection outage probability for varying d (b) Secrecy outage probability for varying R_{p1} and R_{p2} with four different scenarios

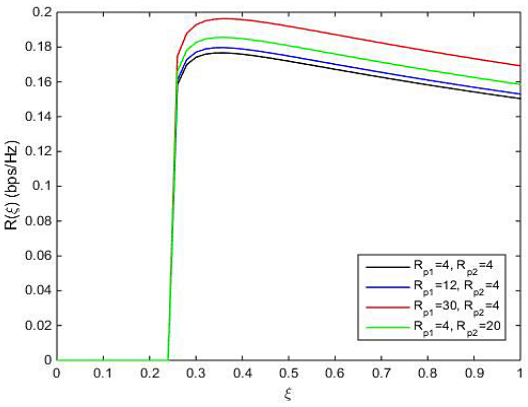


Fig. 4 Secrecy transmission rate for varying R_{p1} and R_{p2}

그림 4 는 Alice 및 Bob의 보호 구역 반지름의 변화에 따른, 전력비 ξ의 함수로서 보안 전송율의 변화를 보여준다. Alice와 Bob의 보호 구역 반지름의 크기가 커질수록, 보안 전송율이 증가하고, 최적 전력비가 점차 1로 이동한다. 이는, 도청으로부터 자유로워짐에 따라, 연결 실패 확률을 줄이는데 전송 전력을 더 많이 쓸 수 있기 때문이다. 또한, 그림 4는 인공잡음을 사용하지 않았을 때 ($\xi = 1$)보다, 최적 인공 잡음 사용시, 보안 전송율이 증가하는 것을 볼 수 있다.

Ⅴ. 결 론

본 논문에서는 확률 기하 이론적 접근을 통해, 송,수신기의 보호 구역 및 최적 인공 잡음 활용에 따른 보안 성능 향상 이득을 분석하였다. 연결 실패 확률 및 보안 실패 확률은 송, 수신기 사이의 거리와 송, 수신기의 보호 구역 크기에 따라 달라지고, 최적 인공 잡음 전송은 이러한 연결 및 보안 실패 확률의 트레이드 오프를 적절하게 조절함에 따라, 보안 전송율을 최대화 시킬 수 있다.

REFERENCES

[1] N. Romero-Zurita, D. McLernon, M. Ghogo, and A. Swami, “PHY layer security based on protected zone and artificial noise,” *IEEE Signal Processing Letters*, vol. 20, no. 5, pp. 487-490, May 2013.

[2] P. C. Pinto, J. Barros, and M. Z. Win, “Secure Communication in stochastic wireless networks-Part I: Connectivity,” *IEEE Trans. Info. Foren. and Security*, vol. 7, no. 1, pp. 125-138, Feb. 2012.

[3] M. Ghogo and A. Swami, “Physical-layer secrecy of MIMO communications in the presence of a Poisson random field of eavesdroppers,” in Proc. *IEEE Int. Conf. Commun. (ICC)*, Kyoto, Japan, pp. 1-5, Jun. 2011.

[4] S. H. Chae, W. Choi, J. H. Lee, and T. Q. S. Quek, “Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zones,” *IEEE Trans. Info. Forens. and security*, vol. 9, no. 10, pp. 1617-1628, Oct. 2014.

[5] X. Zhou, R. Ganti, J. Andrews, and A. Hjorungnes, “On the throughput cost of physical layer security in decentralized wireless networks,” *IEEE Trans. on Wireless Commun.*, vol. 10, no. 8, pp. 2764-2775, Aug. 2011.

[6] H. S. Dhillon, R. K. Ganti, F. Baccelli, and J. G. Andrews, “Modeling and analysis of K-tier downlink heterogeneous cellular networks,” *IEEE J. Sel. Areas Commun.*, vol. 30, no. 3, pp. 550-560, Apr. 2012.

채승호(Seong Ho Chae)

2010년 2월 성균관대학교 정보통신공학부 학사
2012년 2월 KAIST 전기전자공학부 석사
2016년 2월 KAIST 전기전자공학부 박사
2016년 3월 ~ 현재 KAIST 박사후연구원
※관심분야 : Stochastic geometry, Multi-RAT, Caching, 무선 통신 시스템, mmWave