물리계층 보안 성능 향상을 위한 재밍 조건

Effective Conditions of Friendly Jamming for Physical Layer Security

저자
(Authors)

김종엽, 주창희, 최지환
Jongyeop Kim, Changhee Joo, Jihwan Choi

출처
(Source)

전자공학회논문지 56(2), 2019.2, 3-9(7 pages)
Journal of the Institute of Electronics and Information Engineers 56(2), 2019.2, 3-9(7 pages)

발행처
(Publisher)

대한전자공학회
The Institute of Electronics and Information Engineers

URL

http://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE07617378

APA Style

김종엽, 주창희, 최지환 (2019). 물리계층 보안 성능 향상을 위한 재밍 조건. 전자공학회논문지, 56(2), 3-9

Journal of The Institute of Electronics and Information Engineers Vol.56, NO.2, February 2019 https://doi.org/10.5573/ieie.2019.56.2.3
ISSN 2287-5026(Print) / ISSN 2288-159X(Online)

논문 2019-56-2-1

물리계층 보안 성능 향상을 위한 재밍 조건

(Effective Conditions of Friendly Jamming for Physical Layer Security)

김 종 엽*, 주 창 희**, 최 지 환***

(Jongyeop Kim, Changhee Joo, and Jihwan Choi©)

요 약

물리계층 보안기법은 무선 채널의 통계적 특성에 의존하지 않는 인공노이즈 기법과 결합되어 MIMO 시스템, 멀티유저, 릴레이 시나리오 등 다양한 모델에서 연구되고 있다. 하지만 정교하게 수립되지 않는 무분별한 재밍 전략은 오히려 보안성능을 감소시키기 때문에 성능에 영향을 주는 요소들을 이론적으로 분석해야 한다. 따라서, 본 논문에서는 도청자가 존재하는 MIMO 채널에서 재밍파워와 노드배치의 관점에서 보안성능의 변화를 살펴보았다.

Abstract

Physical layer security techniques have been studied in various models such as the MIMO system, multiple users, and relay scenarios combined with the artificial noise scheme that does not depend on the statistical characteristics of wireless channel. However, it is necessary to theoretically analyze the factors affecting the secrecy performance because the jamming strategies that are not elaborately established are rather detrimental to the performance. In this paper, we examined the change of security performances of the MIMO system regarding jamming power and node placements in the presence of eavesdroppers.

Keywords : Physical layer security, Friendly jamming, Eavesdropping, Secrecy outage probability

Ⅰ. 서 론

5G 시대의 IoT 무선 환경은 수백, 수천 단말들이 무선 연결성을 바탕으로 서로 간의 협업을 통해 다양한 서비스와 어플리케이션들을 제공할 것이다. 하지만 대부분의 패킷 송수신은 무선 채널을 통해 전송되기 때문에 매체의 전파특성을 악용하는 노드가 쉽게 정보를 도청할 수 있는 보안 문제를 야기 시킬 수 있다.

그 동안 무선 네트워크분야는 위의 보안문제를 해결하기 위해서 암호학 기반의 보안 기술을 개발하여 널리 사용하여 왔다. 하지만 연산능력에 기반하는 전통적인 암호학 기술은 양자 컴퓨터가 개발되면 더 이상 복잡한 연산량 방식으론 보안달성이 힘들다. 따라서 이를 해결하기 위해서, 최근 정보이론적 관점의 물리계층 보안

* 학생회원, 대구경북과학기술원 정보통신융합전공
(Dept. of Information and Communication Engineering, Daegu Gyeongbuk Institute of Science and Technology)
** 정회원, 울산과학기술원 전기전자컴퓨터공학부
(School of Electrical and Computer Engineering, Ulsan National Institute of Science and Technology)
*** 정회원, 대구경북과학기술원 정보통신융합전공
(Dept. of Information and Communication Engineering, Daegu Gyeongbuk Institute of Science and Technology)
© Corresponding Author(E-mail: jhchoi@dgist.ac.kr)
※ 이 연구는 방위사업청 및 국방과학연구소의 재원에 의해 설립된 신호정보 특화연구센터 사업의 지원을 받아 수행되었음.
Received ; August 30, 2018 Revised ; December 12, 2018 Accepted ; January 30, 2019

기술이 많은 관심을 받고 있다.

정보이론적 관점의 보안연구의 시작은 1949년 Shannon이 도청자의 연산능력과 무관한 완벽 보안 시스템의 제안이 그 출발 이었다[1]. 하지만 사전에 보안 키를 공유해야 하는 한계성을 지녔기 때문에 이를 극복하는 채널기반의 솔루션을 Wyner가 1975년에 제안하였다[2]. Wyner의 연구는 도청자의 달성 가능한 채널용량이 적법한 노드의 채널용량보다 낮다면 정보이론적 관점에서 기밀통신이 가능함을 Secrecy capacity(보안용량) 의 개념으로 정의하였다. 보안용량은 도청 노드와 적법한 수신기 간의 채널용량의 차이를 의미하며, 그 동안 보안용량을 향상시키기 위해서 빔 형성기법, 협력 재밍 기법, 릴레이 전송, 의도적인 노이즈 재밍 등의 다양한 정보이론과 융합된 형태의 물리계층보안 솔루션들이 제안되어왔다[3].

물리계층보안 기법의 주요한 컨셉은 적법한 노드와 악의적 노드가 겪는 페이딩이나 채널 노이즈의 차이를 다이버시티나 코딩기법 등을 통해 더 크게 증가시키는 것이다. 즉, 이러한 채널이득차이로 적법한 노드들은 기밀통신 달성이 가능하다. 하지만 기존의 기법들은 정확한 채널정보를 요구하기 때문에 실질적으론 성취되기가 매우 어렵다. 따라서, 이를 해결하기 위해서 Goel과 Negi[4]는 무선 채널의 통계적 특성에 비 의존적인 인공노이즈(Artificial Noise, AN) 기법을 제안하여 수신단의 성능저하 없이 보안용량 향상이 가능함을 보였다. 그 후, 인공노이즈 기법들은 Multiple Input Multiple Output (MIMO), 멀티유저, 협력 재밍, Full-duplex[5], 릴레이 시나리오, 하드웨어 왜곡영향[6~7] 등 다양한 모델들과 결합되어 연구되어 왔다. 하지만 무분별한 재밍 전략은 보안성능 향상을 얻을 수 없으며, 오히려 보안성능을 하락시키기 때문에 정교한 재밍 전략이 요구된다. 예를 들어, 파워 예산이 한정된 시스템에서 재밍 사용은 통신 전송을 위한 파워량과 상충관계를 가지기 때문에 적절한 파워할당 전략이 요구된다. 특히, 다양한 거리감쇠비가 고려 될 수 있는 현실적인 모델에서는 노드배치와 파워할당에 따라서 재밍으로 인한 보안성능이 달라지기 때문에 이에 대한 고려가 필요하다.

본 논문에서는, 강력한 도청능력을 가정한 재밍 켄슬레이션기반의 스마트 도청자 문제[5]와는 달리 수동적인 도청자가 존재하는 일반적인 보안위협 환경에서의 물리계층 보안전략을 제안하고자 한다. 이는, 기존의 많은 보안연구들이 실제 도청상황을 가장 잘 반영하는 수동적인 도청자 케이스를 고려하고 있지만, 여전히 파워분배 문제의 해결책과 노드배치의 관점에 따른 정량적인 성능분석이 충분히 이루어지지 않았기 때문이다. 우리는 먼저, 송신단에서 재밍과 데이터 전송간의 파워할당이 보안성능에 어떠한 영향을 주는지를 조사하고, 노드들의 배치에 따라서 Friendly jamming이 보안성 향상에 얼마나 기여하는지를 확인하였다. 특히, Friendly jamming이 보안에 도움을 주는 노드배치 전략을 재밍 효과지역이라고 정의하고, 본 연구에서 이러한 효과지역과 비효과지역 내에서 재밍파워에 따른 보안 성능을 비교 및 분석하였다.

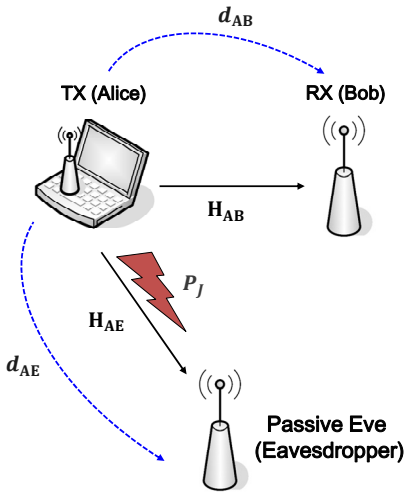


그림 1. 채널 내 도청자가 존재하는 시스템 모델
Fig. 1. A system model in the presence of an eavesdropper on the channel.

Ⅱ. 시스템 모델

우리는 MIMO채널환경에서 송신기(Alice)와 수신기(Bob) 그리고 도청자(Eve)가 존재하는 도청 시나리오를 가정한다. 그림 1과 같이 도청자는 적법한 송신기의 기밀데이터를 채널에서 자신을 은닉하여 도청을 수행하는 수동적인 모델로 가정한다. 모든 채널은 Rayleigh fading 영향을 받으며, 동일한 블록 길이 내에서 Slow fading을 겪는다고 가정한다. 송신기와 수신기 그리고 도청자가 사용하는 안테나는 각각 $N_A \geq 2$, $N_B \geq 2$, $N_E \geq 2$ 이며, 송신기-수신기의 채널행렬 그리고 송신기-도청자의 채널은 $\boldsymbol{H}_{AB} \subset C^{N_A \times N_B}$와 $\boldsymbol{H}_{AE} \subset C^{N_A \times N_E}$로 정의된다. 또한, 도청자의 성능이 더 좋은 Worst-case 시나리오 가정을 위해서 수신기는 Selection Combining(SC) 다이버시티 기법[8]으로 최대 채널이득을 가지는 i번째 채널을 선택하여 수신하며, 아래와 같이 표현된다.

$$i = \arg\max_{k\in 1,.....,N_B} |h_{AB,k}|, \quad (1)$$

$h_{AB,k} \in C^{N_A \times 1}$은 $\boldsymbol{H}_{AB}$의 k번째 열을 의미한다. 도청자는 수신기보다 효율성이 높은 Maximal Ratio Combining(MRC) 기법[9]을 사용한다고 가정한다.

송신기는 도청공격을 예방하기 위해서 null-space기반[4]의 인공노이즈를 데이터와 함께 다중 안테나에 실어서 전송한다. 전송되는 시그널의 형태는 $\boldsymbol{x}(n) \subset C^{N_A \times 1}$로써, 아래와 같이 표현된다.

$$\boldsymbol{x}(n) = [\boldsymbol{w}_s \boldsymbol{w}_1 \cdot \cdot \cdot \boldsymbol{w}_{N_{A-1}}] \begin{bmatrix} s(n) \\ J_1(n) \\ \cdot \\ \cdot \\ J_{N_{A-1}(n)} \end{bmatrix}$$
$$= \boldsymbol{w}_s s(n) + \boldsymbol{w}(n), \quad (2)$$

$s(n)$은 시간 n에서의 $P_S = E[|s(n)|^2]$ 파워량의 기밀데이터 시그널을 의미하며, $\boldsymbol{w}_s = \frac{\boldsymbol{h}_{AB,i}}{\|\boldsymbol{h}_{AB,i}\|}$는 정규화된 빔포밍 계수이다. 또한, 인공노이즈 $\boldsymbol{w}(n)$는 아래와 같이 표현되는데

$$\boldsymbol{w}(n) = \sum_{k=1}^{N_A - 1} \boldsymbol{w}_k J_k(n), \quad (3)$$

$\boldsymbol{w}_k$는 $\boldsymbol{h}_{AB,i}^H$의 Null-space 방향의 직교빔포밍계수를 의미한다(즉, $\boldsymbol{h}_{AB,i}^H \boldsymbol{w}(n) = 0$ 성립). 또한, $(\bullet)^H$은 전치공액연산을 의미하며, 인공노이즈 $J_k(n)$는 Independent and identical Gaussian distribution을 따르는 노이즈로 $N(0, \sigma_{JA}^2/(N_A - 1))$로 정의된다. 그러므로 전송된 재밍파워는 $P_J = E[\|\boldsymbol{w}(n)\|^2]$이다. 우리는 현실적인 파워예산을 고려하기 위해서 아래와 같은 순간 파워 제약조건을 가정한다.

$$P_S + P_J \le P_{TX}, \quad (4)$$

P_{TX}는 송신기의 총 파워예산을 의미한다.

적법한 수신노드는 송신단의 Null-space 재밍기법 (3)을 통해 Friendly jamming의 간섭 없이 온전한 메시지 시그널을 수신하기 때문에 아래의 식 (5)로 표현된다.

$$y_B = \boldsymbol{h}_{AB,i}^H \boldsymbol{w}_s s(n) d_{AB}^{-\alpha/2} + n_B(n), \quad (5)$$

$n_B(n)$는 Complex additive white Gaussian noise $CN(0, \sigma_n^2)$를 따르며, $d_{AB}^{-\alpha/2}$의 α는 거리감쇠계수를 의미한다. 또한, 악의적인 도청노드가 수신하는 시그널은 아래의 식 (6)과 같다.

$$y_E = \boldsymbol{H}_{AE}^H \boldsymbol{w}_s s(n) d_{AE}^{-\alpha/2} + \boldsymbol{H}_{AE}^H \boldsymbol{w}(n) d_{AE}^{-\alpha/2} + \boldsymbol{n}_E(n), \quad (6)$$

$\boldsymbol{n}_E(n)$는 Complex additive white Gaussian noise $CN(0, \sigma_n^2)$를 따른다. 그러므로 본 모델에서, 도청자는 식 (5)와는 다르게 송수신단의 채널정보 또는 빔포밍 정보 없이 Friendly jamming 영향을 제거할 수 없다. 이는 물리계층보안을 달성하는 Friendly jamming 기법으로 우리 모델링의 핵심 아이디어를 의미한다.

Ⅲ. 보안성능의 평가

본 연구에서 제안하는 재밍의 보안성능을 유도하기 위해서 사용하는 지표는 보안용량으로 아래의 식 (7)로 정의 된다[10].

$$C_S = \log_2(1 + \Gamma_{Bob}) - \log_2(1 + \Gamma_{Eve}) \ge R_S, \quad (7)$$

R_S는 달성가능한 Secrecy rate을 의미하며, C_S는 R_S의 상한경계이다. 식의 간략화를 위해 거리감쇠에 대한 파워표현을 식 (8)과 같이 정의한다.

$$P_{S,AB} = \frac{P_S}{d_{AB}^{\alpha/2}\sigma_n^2}, P_{S,AE} = \frac{P_S}{d_{AE}^{\alpha/2}\sigma_n^2},$$
$$P_{J,AE} = \frac{P_J}{d_{AE}^{\alpha/2}\sigma_n^2}. \quad (8)$$

식 (7)의 Γ_{Bob}와 Γ_{Eve}는 각각 수신단과 도청자 노드에서의 Signal to Interference Noise Ratio(SINR)을 의미하며 식 (5)와 (6)으로부터 식 (9)와 (10)이 유도된다.

$$\Gamma_{Bob} = \frac{P_S d_{AB}^{-\alpha/2} |h_{AB,i}|^2}{\sigma_n^2} = P_{S,AB}\zeta_{AB} \quad (9)$$

$$\Gamma_{Eve} = \frac{P_S d_{AE}^{-\alpha/2} |h_{AE}|^2}{P_J d_{AE}^{-\alpha/2} |h_{AE}|^2 + \sigma_n^2} = \frac{P_{S,AE}\zeta_{AE}}{P_{J,AE}\zeta_{AE} + 1}, \quad (10)$$

ζ_{AB}와 ζ_{AE} 는 각 노드들 간의 채널이득 $|h_{ij}|^2$을 의미한다.

본 연구에서, 보안성능평가는 확률적인 관점 지표인 Secrecy Outage Probability(SOP)를 사용한다. SOP의 의미는 달성가능한 보안통신율(R_S)이 목표로 하는 보안통신율(η)보다 낮은 경우를 유도하는 정전확률모델로 식 (11)로 정의한다[11].

$$\begin{aligned} P_{out}(\eta) &= P(R_S < \eta) \\ &= P[C_S < \eta | \Gamma_{Bob} > \Gamma_{Eve}]\, P[\Gamma_{Bob} > \Gamma_{Eve}] \\ &\quad + P[C_S < \eta | \Gamma_{Bob} \le \Gamma_{Eve}] P[\Gamma_{Bob} \le \Gamma_{Eve}]. \end{aligned} \tag{11}$$

식 (11)에서 $P\left[C_S < \eta | \Gamma_{Bob} \le \Gamma_{Eve}\right] = 1$ 이기 때문에, 아래와 같이 식 (12)로 다시 쓸 수 있다.

$$\begin{aligned} P_{out}(\eta) = & \underbrace{P[C_S < \eta | \Gamma_{Bob} > \Gamma_{Eve}]\, P[\Gamma_{Bob} > \Gamma_{Eve}]}_{A_1} \\ & + \underbrace{P[\Gamma_{Bob} \le \Gamma_{Eve}]}_{A_2}, \end{aligned} \tag{12}$$

A_1은 아래 (13)과 같이 유도되는데,

$$\begin{aligned} A_1 &= \int_0^{\infty} \int_{\gamma_E}^{2^{R_S(1+\gamma_E)-1}} f_E(\gamma_E) f_B(\gamma_B) d\gamma_B d\gamma_E \\ &= \underbrace{\int_0^{\infty} \int_0^{2^{R_S(1+\gamma_E)-1}} f_E(\gamma_E) f_B(\gamma_B) d\gamma_B d\gamma_E}_{B_1} \\ &\quad - \underbrace{\int_0^{\infty} \int_0^{\gamma_E} f_E(\gamma_E) f_B(\gamma_B) d\gamma_B d\gamma_E}_{B_2}, \end{aligned} \tag{13}$$

이때, $A_2 = B_2$ 임을 쉽게 알 수 있기 때문에 간략화된 최종 SOP 식은 (14)로 표현가능하다.

$$P_{out}(\eta) = \int_0^{\infty} F_B(2^{\eta}(1+\gamma_E)-1) f_E(\gamma_E) d\gamma_E, \tag{14}$$

$F_B(\bullet)$는 Γ_{Bob}의 Cumulative Distribution Function (CDF)이며 $f_E(\bullet)$는 Γ_{Eve}의 Probability Density function(PDF)를 의미한다. Γ_{Bob}의 CDF는 아래의 과정으로 간단히 유도할 수 있다[8].

$$\begin{aligned} F_B(\gamma_B) &= P\left[\frac{P_S d_{AB}^{-\alpha/2} |h_{AB,i}|^2}{\sigma_n^2} < \gamma_B\right] \\ &= \prod_{k=1}^{N_B} F_{\zeta_{AB,k}}(\zeta_{AB,k} < \frac{\gamma_B}{P_{S,AB}}) \\ &= \left[1 - \exp\left(\frac{-\gamma_B}{P_{S,AB}\overline{\zeta_{AB}}}\right)\right]^{N_B}, \end{aligned} \tag{15}$$

이때 i는 (1)의 SC기법에 의해 선택된 안테나의 채널을 의미한다. Γ_{Eve}의 PDF는 먼저 CDF를 구하고 이를 미분하여 구한다. CDF와 PDF는 아래와 같이 각각 유도된다[7].

$$\begin{aligned} F_E(\gamma_E) &= P\left[\frac{P_{S,AE}\zeta_{AE}}{P_{J,AE}\zeta_{AE}+1} < \gamma_E\right] \\ &= P\left[\zeta_{AE} < \frac{\gamma_E}{P_{S,AE} + \gamma_E P_{J,AE}}\right] \\ &= 1 - \exp\left(\frac{-\gamma_E}{\overline{\zeta_{AE}}(P_{S,AE} + \gamma_E P_{J,AE})}\right) \\ &\quad \times \sum_{k=0}^{N_E-1} \frac{\left(\frac{\gamma_E}{\overline{\zeta_{AE}}(P_{S,AE} + \gamma_E P_{J,AE})}\right)^k}{k!}, \end{aligned} \tag{16}$$

$$\begin{aligned} f_E(\gamma_E) &= \frac{d}{d\gamma_E} F_E(\gamma_E) \\ &= \frac{1}{\overline{\zeta_{AE}}} exp\left(\frac{-\gamma_E}{\overline{\zeta_{AE}}(P_{S,AE} + \gamma_E P_{J,AE})}\right) \\ &\quad \times \left[\sum_{k=0}^{N_E-1} \frac{\left(\frac{\gamma_E}{\overline{\zeta_{AE}}(P_{S,AE} + \gamma_E P_{J,AE})}\right)^k}{k!} \right. \\ &\quad \left. - \sum_{k=0}^{N_E-1} \frac{\left(\frac{\gamma_E}{\overline{\zeta_{AE}}(P_{S,AE} + \gamma_E P_{J,AE})}\right)^{k-1}}{\overline{\zeta_{AE}}(k-1)!}\right] \end{aligned} \tag{17}$$

따라서, 최종적으로 (15)와 (17)를 식 (14)에 대입하여 SOP 식 (18)을 얻을 수 있다.

$$\begin{aligned} P_{out}(\eta) = & \int_0^{\infty} \left[1 - \exp\left(\frac{-2^{\eta}(1+\gamma_E)+1}{P_{S,AB}\overline{\zeta_{AB}}}\right)\right]^{N_B} \\ & \times \frac{1}{\overline{\zeta_{AE}}} exp\left(\frac{-\gamma_E}{\overline{\zeta_{AE}}(P_{S,AE} + \gamma_E P_{J,AE})}\right) \\ & \times \left[\sum_{k=0}^{N_E-1} \frac{\left(\frac{\gamma_E}{\overline{\zeta_{AE}}(P_{S,AE} + \gamma_E P_{J,AE})}\right)^k}{k!} \right. \\ & \left. - \sum_{k=0}^{N_E-1} \frac{\left(\frac{\gamma_E}{\overline{\zeta_{AE}}(P_{S,AE} + \gamma_E P_{J,AE})}\right)^{k-1}}{\overline{\zeta_{AE}}(k-1)!}\right] \end{aligned} \tag{18}$$

Ⅳ. 보안성능 향상을 위한 고려요소

제안하는 모델의 보안성능 향상을 위해서는 재밍파워의 증가와 보안성 향상에 도움이 되는 적절한 노드들의 배치전략이 매우 중요하다. 하지만, 정교하게 제어되

지 않은 무분별한 재밍전략은 오히려 보안성능을 하락시키며, 재밍의 영향력이 낮은 지역에서의 재밍파워 할당은 적법한 통신링크의 성능을 감소시킨다. 따라서 본 절에서는 앞서 얻은 해석적인 식의 결과들을 바탕으로, 보안성능 향상에 도움을 주는 재밍파워와 재밍 효과지역에서의 적절한 재밍전략과 그 영향력 분석에 대하여 알아본다.

1. 재밍파워

일반적으로 식 (7)에서 양의 보안성능을 얻기 위해서는 Γ_{Bob} 는 증가, Γ_{Eve}는 감소시킴으로 그 격차안에서 R_S가 충분히 증가하여야 한다. 이를 성취하기 위해서 기존의 연구들은 강한파워의 인공노이즈를 사용하였다. 하지만 본 연구에서 고려하는 현실적인 파워예산 제한 모델은 재밍파워 P_J와 신호파워 P_S 간의 보안성능 상충관계를 가지기 때문에, 무분별한 재밍으로의 파워예산 투자는 항상 R_S 의 증가를 가져오지는 않는다. 따라서, 송신단과 수신단간의 채널이득을 고려한 적절한 재밍대 시그널 비율 $P_{th} = P_J/(P_S + P_J)$ 안에서 파워할당이 수행되어야 한다. 이러한 재밍 전략은 아래와 같이 표현된다.

$$P_{th} = \arg\min P_{out}(\eta). \tag{19}$$

만약, P_{th} 보다 낮은 재밍파워를 할당하면 시스템 보안성능이 감소하며, 반대로 P_{th} 보다 높은 시그널 파워를 할당해도 보안성능은 최적의 값을 얻을 수 없다. 따라서, 제한된 파워예산 안에서 적절한 파워 할당비를 찾는 것이 최적의 재밍전략이라고 할 수 있다.

2. 재밍효과지역

재밍의 영향력은 송신노드와 수신노드간의 거리(D_{AB})와 송신노드와 예상되는 도청노드간의 거리(D_{AE})에 의존하게 된다. 따라서 재밍 영향력의 확인을 위해서 D_{AB}와 D_{AE}의 거리 비를 아래와 같이 정의한다.

$$\rho = \frac{D_{AE}}{D_{AB}}. \tag{20}$$

만약, 고정된 파워할당 전략에서 적절한 ρ값을 찾는다면 적법한 송신단과 수신단의 최적의 노드 배치가 가능할 것이다.

비록, 실제 무선환경에서 수동적인 도청자의 위치를 정확히 알 수는 없지만 사전에 보안이 취약한 구간[12]을 확률적으로 유도할 수 있다면, 보안재밍(Friendly jamming)을 사용하여 보안성 향상이 가능하다. 또한, ρ 값은 거리감쇠계수 α와도 밀접한 관련이 있는데, 본 연구는 현실적인 Shadowed urban cellular radio 환경[13]인 $\alpha = 4$를 먼저 가정한 후, ρ값을 변화시킴에 따라 재밍효과 지역과 비효과지역 구분 시뮬레이션에서 어떤 성능 변화가 일어나는지를 분석하였다.

Ⅴ. 시뮬레이션 결과 및 분석

모든 시뮬레이션에서 $P_{TX} = 100$ mW로 고정하였으며, 재밍효과지역 시뮬레이션에선 P_S와 P_J는 50 mW로 가정하였다. 재밍파워와 거리에 따른 공정한 비교를 위해서 모든 채널이득은 정규화하여 '1'로 고정하였으며, η = 0.1로 보안성능변화를 가장 잘 보여주는 값으로 가정하였다. 또한, 안테나는 $N_B = 2$ 와 $N_E = 3$으로 가정하여 도청자의 기본적인 성능이 더 좋은 Worst-case 시나리오를 고려하였다.

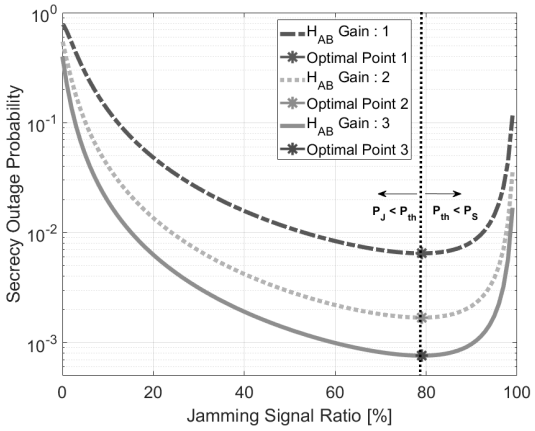


그림 2. 재밍파워와 시그널파워 할당에 따른 성능변화
Fig. 2. Secrecy Performance under Different Jamming Signal Ratios.

그림 2는 재밍파워와 시그널파워량의 변화비(JSR)에 따른 SOP 변화량을 보여준다. 고려한 송신단과 수신단간의 채널이득은 1~3 dB를 변화시켰으며 이때 식 (19)의 최적 SOP값은 *로 표시하였다. 결과는 예상대로 H_{AB} 채널이득이 높을수록 SOP값은 낮았으며 P_J를 증가시키고 동시에 P_S를 감소시켜 P_{th}로 다가갈수록 최적 값을 얻었다. 하지만 P_{th}기준보다 P_J에 파워예산을 더 투자할 때 보안성능이 점점 더 나빠지는 결과를 보였다. 이는 식 (7)에서 적절한 재밍파워 투자값

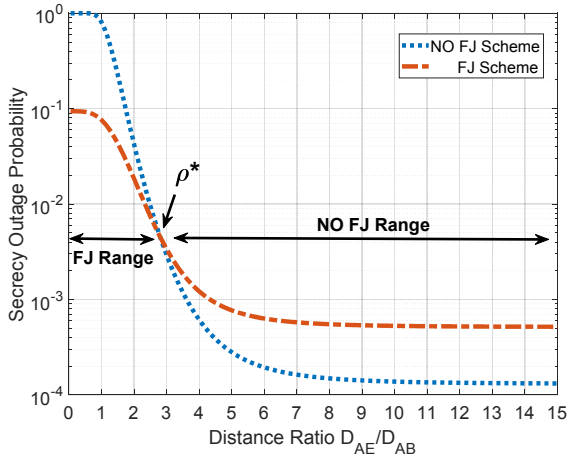


그림 3. 재밍효과지역과 비효과지역의 구분
Fig. 3. Effective and Ineffective Jamming Regions.

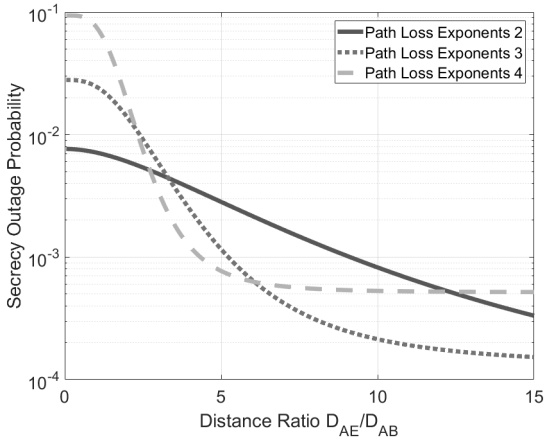


그림 4. 거리감쇠 계수와 보안성능의 관계
Fig. 4. Path Loss Exponent and Secrecy Performance.

P_{th}이상의 파워할당은 Γ_{Eve}감소보다 Γ_{Bob}의 감소를 더 만들었기 때문이다. 따라서 파워예산이 제한된 모델에서 최적의 보안성능을 얻기 위해서는 적절한 P_{th}파워비 할당이 매우 중요함을 알 수 있다.

그림 3은 식 (20)의 증가에 따른 보안성능의 변화를 분석하였다. 2가지의 케이스를 고려하였는데, 첫 번째로 FJ scheme은 Friendly jamming을 사용하였으며, 두 번째 NO FJ scheme는 보안을 위해 어떠한 재밍도 사용하지 않았다. 결과는 흥미롭게도 일정한 거리비 ρ^*이상부터는 오히려 재밍을 사용하지 않는 것이 보안성능향상에 도움을 주었다. 이러한 결과는 신호의 거리감쇠로 인해 도청자의 위험이 현저히 줄어드는 구간($\rho > 3$)부터는 오히려 P_J에 대한 파워할당보다는 P_S에 파워할당을 수행하는 것이 시스템 관점에서 전반적인 성능향상에 도움이 된다는 것을 보여주었다. 따라서, 다수 노드의 배치가 필요한 네트워크한경에서 이를 고려한 재밍기반의 보안전략을 세운다면 충분한 보안성능 향상이 가능할 것이다. 또한, 추가적으로 그림 4는 거리감쇠 계수 α를 2에서 4까지 증가시킴으로 보안성능의 변화가 어떤 차이를 가지는지 보여주었다. Urban 환경에서 Shadowing 영향이 없는 $\alpha = 3$에서의 성능변화가 $\alpha = 4$보다 더욱 컸으며, 이는 노드 배치와 거리변화에 따른 보안성능 변화가 가장 민감함을 보여주었다. 또한, 이상적인 $\alpha = 2$인 Free-space에서는 거리에 따른 보안성능 변화가 거의 선형적으로 크지 않음을 알 수 있었다. 그러므로, 우리는 고려되는 네트워크의 물리적인 환경에 따라서 보안향상을 위한 최적의 노드 배치전략이 달라져야 함을 알 수 있다.

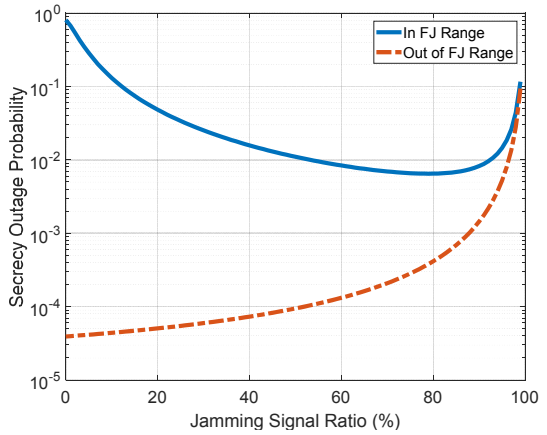


그림 5. 재밍효과/비효과 지역에서의 재밍 영향력
Fig. 5. Jamming Influence in Effective and Ineffective Jamming Regions.

마지막으로, 그림 5는 앞서 도출한 식 (20)의 결과 중 재밍효과지역 $\rho = 1$과 비효과지역 $\rho = 6$에서 재밍파워를 점차 증가시키는 경우의 보안성능 변화를 관찰하였다. 이는 앞서 얻은 결과로부터 예상 가능한 경향성으로, 재밍효과지역 내에서는 재밍파워를 증가시킬수록 보안성능은 증가하였으며(SOP 감소), 비효과지역에서는 재밍파워의 증가가 지수함수 형태로 오히려 보안성능을 감소시키는 결과를 보였다. 이러한 이유는, 파워예산이 제한된 현실적인 시스템에서는 한정적인 파워를 재밍과 메시지 모두에 할당함으로써 성능의 상충관계를 가지기 때문이다. 즉, 비효과지역에서는 재밍파워 할당이 통신파워 감소를 야기시키며 이는 보안성능의 감소결과를 초래한다. 그러므로 보안이 의심되는 지역에서 적절한 재밍파워 할당전략을 수행해야 더 나은 보안성능을 얻을 수 있을 것이다.

Ⅵ. 결 론

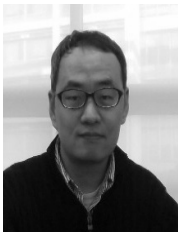
본 논문에서, 우리는 현실적인 파워 제한 송신기 모델에서 재밍파워 증가가 항상 보안성능향상에 도움을 주는 것은 아니라는 사실을 확인하였다. 또한, 재밍효과와 비효과 지역들을 정의하고 이들 지역에서 재밍과 송신신호로의 적절한 파워 투자가 높은 보안성능 달성에 핵심임을 결과를 통해 알 수 있었다. 그러므로 본 결과를 통해서, 재밍을 통한 보안 성능 향상은 각 노드들의 배치와 적절한 파워할당 전략이 수반되어야 한다는 결론을 내릴 수 있었으며, 추후 연구로 MIMO 채널에서 다수의 협력 재머들이 존재 할 때 네트워크의 보안용량을 최대화 할 수 있는 파워할당과 노드들의 배치 전략을 수립하여 보안성능을 검증할 것이다.

REFERENCES

[1] C. Shannon, “Communication theory of secrecy systems,” Bell Syst. Technical J., vol. 28, no. 4, pp. 656-715, 1949.
[2] A. D. Wyner “The wire-tap channel,” Bell Syst. Tech. J., vol.54, no. 8, pp. 1255-2387, Oct. 1975.
[3] W. Trappe, “The challenges facing physical layer security,” IEEE Commun. Mag., vol. 53, no. 6, pp. 16-20, Jun. 2015.
[4] S. Goel and R. Negi, “Guaranteeing Secrecy using Artificial Noise,” IEEE Trans. on Wireless Commun., vol. 7, no. 6, pp. 2180-2189, June 2008.
[5] J. Kim, J. Kim, J. Lee, and J. P. Choi, “Physical-Layer Security against Smart Eavesdroppers: Exploiting Full-Duplex Receivers,” IEEE Access, vol. 6, pp. 32945-32957, Jun. 2018.
[6] K. Shim, N. Tri Do and B. An, “The Impact of Hardware Impairments and Imperfect Channel State Information on Physical Layer Security,” IEIE, vol. 53, no. 4, pp. 79-86, April 2016.
[7] K. Shim, N. Tri Do, S-Y. Nam and B. An, “Physical Layer Security under Hard Impairments in Cooperative Communication Environments,” in Proc. IEIE, pp. 1641-1643, June 2016.
[8] W. C. Jakes, Microwave Mobile Communications, 1st ed. New York: Wiley, 1974.
[9] F. He, H. Man, and W. Wang, “Maximal ratio diversity combining enhanced security,” IEEE Commun. Lett., vol. 15, no. 5, pp. 509-511, May 2011.
[10] J. Kim and J. P. Choi, “Cancellation-Based Friendly Jamming for Physical Layer Security,” IEEE Globecom 2016, Dec. 2016.
[11] J. Kim and Jihwan P. Choi, “A Cancellation -Based Jamming Strategy for Physical Layer Security,” in Proc. KICS 2017, pp. 511-512, Jan. 2017.
[12] C. Karlof and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” in Proc. Ad hoc networks, 2003.
[13] Rappaport, S. T., “Wireless communications - principles and practice,” prentice-hall, 2002, chapter 4, pp. 138-139.

저 자 소 개

김 종 엽(학생회원)
2013년 계명대학교 전자공학과 학사 졸업.
2013년～현재 대구경북과학기술원 정보통신융합전공 석박통합과정 재학
<주관심분야 : 보안/재밍, 통신>



주 창 희(정회원)
1998년 서울대학교 전기전자컴퓨터공학과 학사 졸업.
2000년 서울대학교 전기전자컴퓨터공학과 석사 졸업.
2005년 서울대학교 전기전자컴퓨터공학과 박사 졸업.
2005년～2007년 Post-doc Purdue Univ.
2007년～2010년 Research Scientist, OSU.
2010년～2011년 한국기술교육대학교 정보통신학과 조교수.
2011년～현재 울산과학기술원 전기전자컴퓨터공학부 부교수.
<주관심분야 : 통신, 네트워크, 최적화>

최 지 환(정회원)
1998년 서울대학교 전기전자컴퓨터공학과 학사 졸업.
2000년 MIT EECS 석사 졸업.
2006년 MIT EECS 박사 졸업.
2006년～2012년 Principal Systems Engineer, Marvell Semiconductor, Inc.
2013년～현재 대구경북과학기술원 정보통신융합전공 부교수.
2016년～2017년 정보통신기술진흥센터 위성 분야 RP(비상근).
<주관심분야 : 위성/무선통신, 기계학습>