The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 18, No. 2, pp.49-54, Apr. 30, 2018. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2018.18.2.49
JIIBC 2018-2-6

재머와 다이버시티를 사용하는 복호 후 재전송 기반 물리 계층 보안의 성능 분석

Performance Analysis of Physical Layer Security based on Decode-and-Forward using Jammer and Diversity

박솔*, 공형윤**

Sol Park*, Hyung-Yun Kong**

요 약 본 논문에서는 복호 후 재전송 기반의 중계기 시스템에서 협력 다이버시티와 재머를 사용했을 때의 보안 불능 확률을 연구한다. 협력 다이버시티를 얻기 위해서 수신자와 도청자에서 MRC 기법을 사용한다. MRC 기법을 사용하기 위해서 송신자와 수신자, 송신자와 도청자 사이의 직접 링크를 사용한다. 보안용량을 증가시키기 위해서 의도적인 잡음 신호를 발생 시키는 재머를 사용한다. 재머는 의도적인 잡음을 발생시켜 도청자의 채널 품질을 떨어뜨리고 물리 계층 보안이 실현될 수 있도록 돕는다. 보안 성능을 평가하기 위해서 보안 불능 확률이 사용된다. 시스템은 레일리 페이딩 채널 하에 있다고 가정한다.

Abstract In this paper, we study the secrecy outage probability when using cooperative diversity and jammer in a relay system based on decode-and-forward. MRC method is used in receiver and eavesdroppers to obtain cooperative diversity. To use the MRC technique, direct links between the sender and receiver, and between the sender and the eavesdropper are used, respectively. Jammers are used to generate intentional noise siganls to increase security capacity. Jammers generate intentional noise, degrading the channel quality of the eavesdropper and helping physical layer security be realized. The secrecy outage probability is used to evaluate security performance. Assume that the system is under the Rayleigh fading channel.

Key Words : decode-and-forward relay, physical layer security, cooperative diversity, outage probability, jammer

Ⅰ. 서 론

협력통신은 페이딩 채널에서 다이버시티 이득을 증가시키고 채널 용량을 향상시키는 효율적인 해결책이다[1]. 하지만 무선 통신이 가지는 무지향성의 한계 때문에 보안에 취약하다는 단점을 가지고 있다. 무선 신호는 특정 방향으로만 전송되는 것이 아니라 모든 방향으로 나아가기 때문에 허가 받지 않은 사용자가 송신자의 메시지를 감청할 수 있다. 무선 네트워크에서 보안은 매우 중요한 이슈이다. 기존의 무선 네트워크 보안은 상위 계층의 암호화 기법을 사용했다. 그러나 상위 계층에서의 보안이 잠재적인 도청자들의 공격으로부터 취약해짐에 따라 물리 계층에서도 보안을 구현하는데 관심이 증가하고 있다[2]-[6].

*준회원, 울산대학교 전기공학부
**정회원, 울산대학교 전기전자정보시스템공학부(교신저자)
접수일자: 2018년 1월 24일, 수정완료: 2018년 2월 24일
게재확정일자: 2018년 4월 6일

Received: 24 January, 2018 / Revised: 24 February, 2018
Accepted: 6 April, 2018
**Corresponding Author: hkong@ulsan.ac.kr
School of Electrical Engineering, University of Ulsan, Korea

물리 계층 보안의 주목적은 주요 링크에서의 채널 용량은 높이고 동시에 도청 링크의 채널 용량은 낮추는데 있다. 논문 [2-3]에서는 송신자의 신호와 중계기의 신호를 모두 이용하여 물리 계층 보안을 실현했다. 송신자와 중계기의 신호를 모두 이용하기 위해서 MRC 또는 SC 기법을 이용하여 수신자와 도청자에서 다이버시티 이득을 얻었다. 물리 계층 보안의 주목적은 도청 링크의 채널 품질을 하락 시켜서 도청자가 송신자의 메시지를 제대로 감청할 수 없도록 만드는 것이다. 이를 위하여 최근 연구에서는 의도적 잡음을 전송하여 도청 링크에 간섭을 발생시키고 통신을 방해하는 방법을 제안하였다. 재밍 신호를 이용하는 방법은 크게 두 가지로 분류할 수 있다. 첫 번째 기법은 송신자 또는 수신자에서 재밍 신호를 발생 시켜 전송하는 방법이다[4]. 송신자에서 신호를 전송할 때, 메시지 신호와 함께 재밍 신호를 전송하여 도청자에서의 품질을 하락 시킨다. 이 때 수신자에서는 송신자의 재밍 신호를 알고 있기 때문에 채널 용량에는 변화가 없다. 수신자에서 송신자의 재밍 신호를 미리 알기 위해서 사전에 송신자와 수신자 간의 협력이 필요하지만, 수신자의 채널 용량의 변화 없이 도청자의 링크에만 영향을 주기 때문에 보안 용량을 크게 늘릴 수 있는 방법이다. 두 번째 방법은 여러 중계기 가운데 물리 계층 보안을 위해서 선택된 중계기를 제외한 나머지 중계기 중에서 재머를 선택하는 것이다. 선택된 재머는 송신자 또는 중계기가 신호를 전송하는 동안에 의도적인 잡음을 전송하여 물리 계층 보안을 실현한다[5]. 이 때 발생한 잡음은 도청자뿐만 아니라 수신자에서도 동일하게 간섭으로 작용하게 된다. 재머를 사용하는 경우 재머에 의한 간섭이 수신자 보다 도청자에서 더 영향이 클 경우에만 보안 용량의 증대를 가져올 수 있다. 보안 용량을 극대화 하기 위한 최적의 재머를 선택하는 방법은 논문 [5]에 의해 제안되었다.

본 논문에서는 재머와 협력 다이버시티를 사용하는 중계기 시스템에서 물리 계층 보안을 연구한다. 중계기는 송신자의 신호를 수신자로 전달하기 위해서 복호 후 재전송 기법을 사용한다. 재머는 도청 링크의 품질을 떨어뜨리기 위해서 의도적인 잡음을 발생 시킨다. [5]에서는 중계기가 항상 송신자의 신호를 완벽하게 복호하는 경우를 가정했다. 본 논문에서 중계기는 페이딩의 영향으로 인해 송신자의 메시지를 완벽하게 복호할 수 없다고 가정한다. 송신자와 수신자, 송신자와 도청자 사이의 직접 링크를 고려한다. 수신자와 도청자는 송신자와 중계기로부터 신호를 각각 전송 받아서 다이버시티 결합을 통한 이득을 얻을 수 있다. 수신자와 도청자는 재머에 의한 의도적인 잡음의 정보를 알 수 없기 때문에 간섭을 제거할 수 없다. 본 논문은 다음과 같이 구성된다. 2장에서 시스템 모델을 설명하고 3장에서 보안 불능 확률이 계산된다. 시뮬레이션 결과는 4장에서 보여 지며, 5장에서 결론짓는다.

II. 시스템 모델

하나의 송신자, 수신자, 도청자, 중계기 그리고 재머가 존재하는 협력 통신 시스템을 가정한다. 중계기는 송신자의 신호를 항상 완벽하게 복호할 수 없다. 송신자와 중계기 사이의 SNR이 사전에 정해둔 임계값 γ_{th} 보다 큰 경우에만 중계기에서 송신자의 메시지를 완벽하게 복호한다고 가정한다. 송신자와 수신자, 송신자와 도청자 사이의 직접 링크가 존재한다고 가정한다. 수신자와 도청자는 송신자와 중계기로부터 전송 받은 신호를 MRC (Maximal Ratio Combining)을 통하여 협력 다이버시티 이득을 얻는다. 각 노드 사이의 채널 환경은 레일리 페이딩 채널을 따른다. 반이중 모드를 가정한다. 중계기는 전송과 수신을 동시에 할 수 없으며 이는 송수신을 위한 두 개의 직교 채널이 필요하다는 것을 의미한다. 시스템은 두 개의 타임 슬롯으로 나뉜다. 첫 번째 타임 슬롯에서 송신자와 재머는 수신자와 도청자에게 신호를 전송한다. 재머의 신호는 수신자와 도청자에서 간섭으로 작용한다. 두 번째 타임 슬롯에서 중계기는 송신자로부터 전송 받은 신호를 복호한 후 수신자와 도청자에게 재전송한다. 두 번째 타임 슬롯에서도 첫 번째 타임슬롯과 동일하게 도청자의 채널 품질을 떨어뜨리기 위한 의도적 잡음이 재머로부터 전송된다. 무선 통신의 성질 때문에 재머의 신호는 도청자뿐만 아니라 수신자에서도 동일하게 전송되면 간섭으로 작용한다. 주요 링크와 도청자 링크의 CSI 정보는 송신자에서 알지 못한다. a와 b 단자 사이의 SNR은 다음과 같이 표현된다.

$$\gamma_{ab} = \frac{P_a |h_{ab}|^2}{N_o} \tag{1}$$

P_a는 a 단자의 전송 전력이며 N_0는 AWGN의 분산이다. h_{ab}는 a와 b 단자 사이의 채널로써 분산 $\sigma_{ab}^2 = d_{ab}^{-\beta}$ 을 가진다. d_{ab}는 a와 b 사이의 유클리디안 거리이고 β는 경로 손실 계수이다. 레일리 페이딩 채널이므로 평균 SNR 이 $1/\alpha_{ab}$ 일 때, PDF와 CDF는 각각 다음과 같다[7].

$$f_X(z) = \alpha_{ab} e^{-z\alpha_{ab}} \quad (2)$$

$$F_X(z) = 1 - e^{-z\alpha_{ab}} \quad (3)$$

보안 불능 확률은 보안용량이 목표 보안율 R_S 보다 작을 확률로 한다. 이 때 $R_S > 0$ 이다.

Ⅲ. 보안 불능확률

이 장에서는 복호 후 재전송 기반의 중계기와 재머를 가지는 시스템에서 협력 다이버시티를 사용할 때의 보안 불능 확률을 분석한다. 이를 위해서 기본적인 물리 계층 보안의 협력 다이버시티 또는 재머가 사용된 시스템을 설명한다.

1. 물리 계층 보안

하나의 송신자, 수신자, 도청자 그리고 중계기를 포함하는 시스템을 가정한다. 협력 다이버시티를 사용하지 않기 때문에 수신자와 도청자에서 송신자와의 직접 링크는 고려하지 않는다. 재머가 사용되지 않으며 간섭은 없다고 가정한다. 물리 계층 보안에서 보안용량은 주 채널의 용량과 도청자 채널의 용량의 차로 정의된다[3].

$$ASR = \frac{1}{2}\left[\log_2\left(\frac{1+\gamma_D}{1+\gamma_E}\right)\right]^+ \quad (4)$$

송신자와의 직접 링크와 간섭이 없기 때문엔 수신자와 도청자의 SNR은 각각 다음과 같다.

$$\gamma_D = \gamma_{RD} \quad (5)$$

$$\gamma_E = \gamma_{RE} \quad (6)$$

식 (4) ASR의 CDF는 다음과 같다.

$$\begin{aligned} F_{ASR}(R_S) &= \Pr[ASR < R_S | \gamma_R > \gamma_{th}] \\ &= \Pr[\max(\frac{1}{2}log_2(\frac{1+\gamma_D}{1+\gamma_E}),0) < R_S | \gamma_R > \gamma_{th}] \\ &= \Pr[\gamma_D < \rho\gamma_E + (\rho-1) | \gamma_R > \gamma_{th}] \\ &= \int_0^\infty F_{\gamma_D}(\rho-1+\rho x | \gamma_R > \gamma_{th}) f_{\gamma_E}(x) dx \end{aligned} \quad (7)$$

$\rho = 2^{2R_S}$ 이며, $\gamma_R < \gamma_{th}$인 경우 $F_{ASR}(R_S) = 1$이다. γ_R에 대한 CDF는 레일리 페이딩 채널을 가정했기 때문에 식 (3)을 사용하여 다음과 같이 표현할 수 있다.

$$F_{\gamma_R}(\gamma_{th}) = \Pr[\gamma_R < \gamma_{th}] = 1 - e^{-\gamma_{th}\alpha_R} \quad (8)$$

α_R는 송신자와 중계기 사이의 평균 SNR의 역수이다. γ_D에 대한 CDF도 동일한 방법으로 구할 수 있다.

$$F_{\gamma_D} = (z) = \Pr[\gamma_D < z] = 1 - e^{-z\alpha_D} \quad (9)$$

α_D는 중계기와 도청자 사이의 평균 SNR의 역수이다. γ_E에 대한 PDF는 식 (2)를 이용하여 계산할 수 있다.

$$f_{\gamma_E}(z) = \alpha_E e^{-z\alpha_E} \quad (10)$$

보안 불능확률은 중계기에서 송신자의 신호를 완벽하게 복호했을 때와 그렇지 않을 때로 구분하여 계산한다.

$$\begin{aligned} P_{out} &= \Pr[ASR < R_S | \gamma_R > \gamma_{th}] \Pr[\gamma_R > \gamma_{th}] \\ &+ \Pr[ASR < R_S | \gamma_R < \gamma_{th}] \Pr[\gamma_R < \gamma_{th}] \end{aligned} \quad (11)$$

식 (7)-(11)을 이용하여 다음의 식을 얻을 수 있다.

$$\begin{aligned} P_{out} &= (\int_0^\infty F_{\gamma_D}(\rho-1+\rho x | \gamma_R > \gamma_{th}) f_{\gamma_E}(x) dx) \\ &\quad \times e^{-\gamma_{th}\alpha_R} + 1 \times (1 - e^{-\gamma_{th}\alpha_R}) \\ &= (1 - \frac{\alpha_E e^{-(\rho-1)\alpha_D}}{\rho\alpha_D + \alpha_E}) \times e^{-\gamma_{th}\alpha_R} + (1 - e^{-\gamma_{th}\alpha_R}) \\ &= 1 - \frac{\alpha_E e^{-(\rho-1)\alpha_D} e^{-\gamma_{th}\alpha_R}}{\rho\alpha_D + \alpha_E} \end{aligned} \quad (12)$$

2. MRC를 사용하는 물리 계층 보안

협력 다이버시티를 이용하는 경우 송신자와의 직접 링크를 고려한다. MRC 기법을 이용하는 경우 최종단에서 SNR은 각 링크의 SNR의 합과 같다. 수신자와 도청자의 SNR은 다음과 같이 계산된다.

$$\gamma_D = \gamma_{SD} + \gamma_{RD} \tag{13}$$

$$\gamma_E = \gamma_{SE} + \gamma_{RE} \tag{14}$$

이 경우 γ_D에 대한 CDF는 [8]을 참고하여 다음과 같이 계산할 수 있다.

$$F_{\gamma_D}(z) = \int_0^\infty f_{\gamma_{SD}}(x) F_{\gamma_{RD}}(z-x)dx$$
$$= 1 - \frac{\alpha_{SD} e^{-z\alpha_{RD}}}{\alpha_{SD} - \alpha_{RD}} - \frac{\alpha_{RD} e^{-z\alpha_{SD}}}{\alpha_{RD} - \alpha_{SD}} \tag{15}$$

γ_E에 대한 PDF 또한 [8]을 참고하여 다음과 같이 계산할 수 있다.

$$f_{\gamma_E}(z) = \int_0^z f_{\gamma_{SE}}(x) f_{\gamma_{RE}}(z-x)dx$$
$$= \frac{\alpha_{SE}\alpha_{RE} e^{-z\alpha_{RE}}}{\alpha_{SE} - \alpha_{RE}} + \frac{\alpha_{RE}\alpha_{SE} e^{-z\alpha_{SE}}}{\alpha_{RE} - \alpha_{SE}} \tag{16}$$

식 (15)-(16)을 식 (11)에 대입하면 다음을 얻을 수 있다.

$$P_{out} = \left(\int_0^\infty F_{\gamma_D}(\rho - 1 + \rho x | \gamma_R > \gamma_{th}) f_{\gamma_E}(x)dx\right) \times e^{-\gamma_{th}\alpha_R}$$
$$+ \left(\int_0^\infty F_{\gamma_D}(\rho - 1 + \rho x | \gamma_R < \gamma_{th}) f_{\gamma_E}(x)dx\right) \times (1 - e^{-\gamma_{th}\alpha_R})$$
$$= \frac{\alpha_{SE}\alpha_{RE}}{\alpha_{SE} - \alpha_{RE}} \left(\frac{1}{\alpha_{RE}} - \frac{1}{\alpha_{SE}} - \frac{\alpha_{SD} e^{-(\rho-1)\alpha_{RD}}}{(\alpha_{SD} - \alpha_{RD})(\rho\alpha_{RD} + \alpha_{RE})}\right.$$
$$+ \frac{\alpha_{SD} e^{-(\rho-1)\alpha_{RD}}}{(\alpha_{SD} - \alpha_{RD})(\rho\alpha_{RD} + \alpha_{SE})} + \frac{\alpha_{RD} e^{-(\rho-1)\alpha_{SD}}}{(\alpha_{SD} - \alpha_{RD})(\rho\alpha_{SD} + \alpha_{RE})}$$
$$\left. - \frac{\alpha_{RD} e^{-(\rho-1)\alpha_{SD}}}{(\alpha_{SD} - \alpha_{RD})(\rho\alpha_{SD} + \alpha_{SE})}\right) \times (1 - e^{-\gamma_{th}\alpha_R})$$
$$+ \left(1 - \frac{\alpha_{SE} e^{-(\rho-1)\alpha_{SD}}}{\rho\alpha_{SD} + \alpha_{SE}}\right) \times (1 - e^{-\gamma_{th}\alpha_R}) \tag{17}$$

3. 재머를 사용하는 물리 계층 보안

재머의 신호는 중계기, 수신자 그리고 도청자에서 간섭으로 간주된다. 중계기, 수신자, 그리고 도청자에서 SNR은 다음과 같이 계산된다.

$$\gamma_R = \frac{\gamma_{SR}}{1 + \gamma_{J_1 R}} \approx \frac{\gamma_{SR}}{\gamma_{J_1 R}} \tag{18}$$

$$\gamma_D = \frac{\gamma_{RD}}{1 + \gamma_{J_2 D}} \approx \frac{\gamma_{RD}}{\gamma_{J_2 D}} \tag{19}$$

$$\gamma_E = \frac{\gamma_{RE}}{1 + \gamma_{J_2 E}} \approx \frac{\gamma_{RE}}{\gamma_{J_2 E}} \tag{20}$$

$\gamma_{J_1 R}$와 $\gamma_{J_2 D}$,$\gamma_{J_2 E}$는 각각 첫 번째 타임 슬롯의 재머 신호와 두 번째 타임 슬롯의 재머 신호에 대한 SNR을 의미한다.

γ_R와 γ_D의 CDF는 [10]을 참고하여 다음과 같이 계산할 수 있다.

$$F_{\gamma_R}(z) = \int_0^\infty F_{\gamma_{SR}}(yz) f_{\gamma_{J_1 R}}(y)dy = 1 - \frac{\alpha_{J_1 R}}{\alpha_{J_1 R} + z\alpha_{SR}} \tag{21}$$

$$F_{\gamma_D}(z) = \int_0^\infty F_{\gamma_{RD}}(yz) f_{\gamma_{J_2 D}}(y)dy = 1 - \frac{\alpha_{J_2 D}}{\alpha_{J_2 D} + z\alpha_{RD}} \tag{22}$$

γ_E에 대한 PDF는 다음과 같다.

$$f_{\gamma_E}(z) = \int_0^\infty y f_{\gamma_{RE}}(yz) f_{\gamma_{J_2 E}}(y)dy = \frac{\alpha_{RE}\alpha_{J_2 E}}{(\alpha_{J_2 E} + z\alpha_{RE})^2} \tag{23}$$

식 (21)-(23)을 식 (11)에 대입하면 재머를 사용하는 물리 계층 보안의 보안 불능확률을 구할 수 있다.

4. 재머와 MRC를 사용하는 물리 계층 보안

협력 다이버시티와 재머를 사용하는 물리 계층 보안에서 중계기의 SNR은 재머만 사용하는 경우와 같다. 수신자와 도청자의 SNR은 다음과 같이 쓸 수 있다.

$$\gamma_D = \frac{\gamma_{SD}}{1 + \gamma_{J_1 D}} + \frac{\gamma_{RD}}{1 + \gamma_{J_2 D}} \approx \frac{\gamma_{SD}}{\gamma_{J_1 D}} + \frac{\gamma_{RD}}{\gamma_{J_2 D}} \tag{24}$$

$$\gamma_E = \frac{\gamma_{SE}}{1 + \gamma_{J_1 E}} + \frac{\gamma_{RE}}{1 + \gamma_{J_2 E}} \approx \frac{\gamma_{SE}}{\gamma_{J_1 E}} + \frac{\gamma_{RE}}{\gamma_{J_2 E}} \tag{25}$$

수신자와 도청자의 SNR에 대한 CDF와 PDF는 식 (15)-(16)와 식 (22)-(23)을 구하는 계산 방법을 이용하면 얻을 수 있다. 이렇게 얻은 식을 식 (11)에 대입하여 재머와 MRC를 사용하는 물리 계층 보안 시스템의 보안 불능 확률을 계산할 수 있다.

Ⅳ. 실험 및 결과

이 장에서는 제안한 시스템 모델의 모의 실험 결과를 제시한다. 잡음 전력은 모든 단자에서 동일하게 적용된다고 가정한다. 제안한 시스템 모델에서 보안율 R_S를 다르게 했을 때의 보안 불능 확률을 비교해 본다.

그림 1, 2, 3는 도청자와 재머의 위치를 이동시켰을 때 협력 다이버시티와 재머의 사용 유무에 따라서 보안 불능 확률이 어떻게 변화하는지 보여주고 있다. 그림 1, 2, 3에서 송신자와 중계기 그리고 수신자의 위치는 동일하다. 송신자의 위치를 (0, 0)로 하고 중계기의 위치는 (0.5, 0), 수신자의 위치는 (1, 0)로 한다. 중계기에서 송신자의 신호를 완벽하게 복호할 수 있는 SNR 임계값은 3dB이다. 모의 실험에서 채널환경은 레일리 페이딩 채널이다. 거리에 따른 경로 손실(β)은 3으로 가정했다. 그림 1은 송신자와 도청자의 거리가 송신자와 수신자의 거리보다 가까울 경우이다. 이 경우 도청자에서 MRC에 의한 채널 용량의 증대가 수신자에서의 증대보다 크기 때문에 보안 용량은 오히려 줄어들게 된다. 재머의 위치가 수신자보다 도청자에 가깝기 때문에 재머의 사용은 보안 용량을 높이는데 도움이 되는 것을 확인할 수 있다. 그림 2은 송신자에서 도청자까지의 거리가 송신자에서 수신자까지의 거리와 같을 경우이다. 보안율이 높을 경우 협력 다이버시티와 재머를 모두 사용할 때보다 재머만 사용했을 때의 보안 불능확률이 낮아지는 것을 확인할 수 있다. 하지만 보안율이 낮은 경우에는 협력 다이버시티와 재머를 모두 사용했을 때 불능 확률이 낮아지는 것을 확인할 수 있다. 협력 다이버시티만 사용했을 때는 SNR에서 좋은 성능을 보이지만 SNR이 커질수록 보안 성능이 떨어지는 것을 확인할 수 있다. 그림 3는 송신자와 도청자 사이의 거리가 송신자와 수신자 사이의 거리보다 멀 때를 가정했다. 이 경우 협력 다이버시티를 사용하는 시스템의 보안 성능이 이전의 경우보다 높아지는 것을 확인할 수 있다. 이를 통하여 협력 다이버시티를 사용하는 시스템에

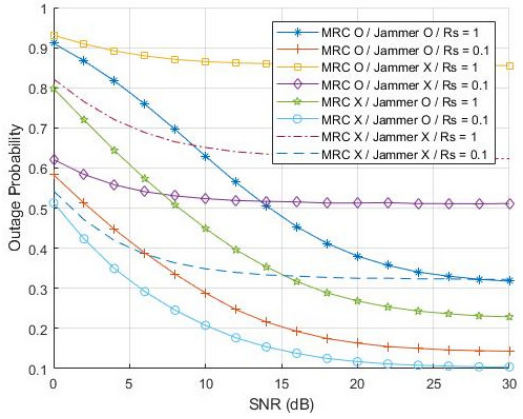

그림 1. xE=0.2, yE=0.6, xJ=0.5, yJ=0.5인 경우의 보안 불능확률
Fig. 1. Secrecy outage probability in case 1

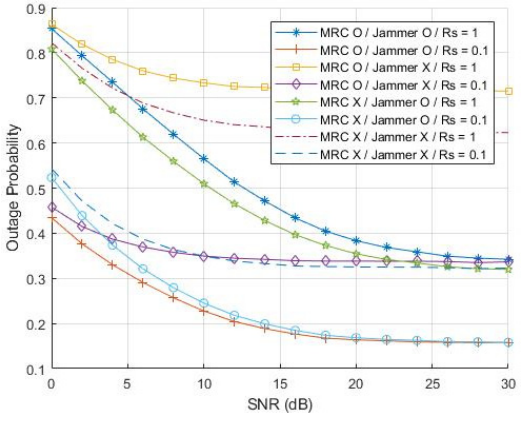

그림 2. xE=0.8, yE=0.6, xJ=0.5, yJ=0.4인 경우의 보안 불능확률
Fig. 2. Secrecy outage probability in case 2

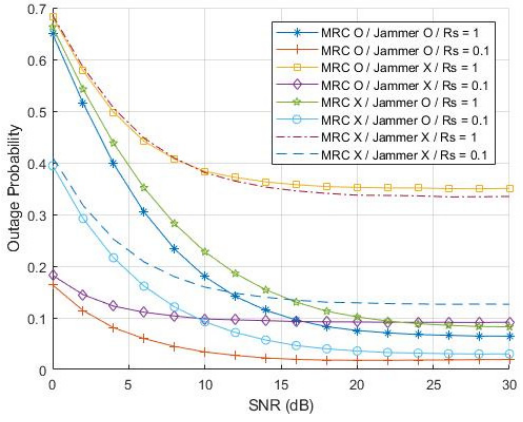

그림 3. xE=1.5, yE=0, xJ=1.8, yJ=0인 경우의 보안 불능확률
Fig. 3. Secrecy outage probability in case 3

서 보안 불능 확률은 송신자와 도청자 사이의 거리보다 송신자와 수신자 사이의 거리가 더 가까울 경우, SNR이 낮은 경우에 낮아지는 것을 확인할 수 있다. 재머를 사용하는 시스템에서는 도청자와 재머의 거리가 수신자와 재머 사이의 거리보다 가까울 때, 보안 성능이 좋아지는 것을 확인할 수 있다. 재머와 협력 다이버시티를 모두 사용하는 시스템의 보안 성능은 보안율이 낮아질수록 좋아진다는 것을 확인할 수 있었다.

V. 결 론

본 논문은 중계기 시스템에서 물리 계층 보안을 구현하기 위해서 재머와 협력 다이버시티를 사용했다. 재머와 협력 다이버시티를 사용하는 시스템의 보안 불능확률을 계산하고 모의 실험 결과를 통하여 성능을 분석했다. 기존의 연구에서 제안한 재머가 포함된 물리 계층 보안과 협력 다이버시티를 통한 물리 계층 보안 방식과 제안한 시스템의 성능을 비교 분석했다.

References

[1] A. Nosratinia, T.E. Hunter, and A. Hedayat, “Cooperative Communication in Wireless Networks,” IEEE Communications Magazine, vol.42, no. 10, pp. 74-80, Oct. 2004.

[2] S. Ghose, C. Kundu, and R. Bose, “Secrecy performnace of dualhop decode-and-forward relay system with diversity combining at the eavesdropper,” IET Commun., vol. 10, no. 8, pp. 904-914, 2016.
DOI: https://doi.org/10.1049/iet-com.2015.1060.

[3] K. Chopra, R. Bose, A. Joshi, “Secrecy Outage Performance of Cooperative Relay Network with Diversity Combining,” ICSIP’ 17, November 2016.
DOI: https://doi.org/10.1109/siprocess.2017.8124587.

[4] P.N. Son, T.V. Phu, P. Sol, L.T. Anh, H.Y. Kong, “Improving the secrecy of cooperative transmissions using unshared jamming,” NAFOSTED, Nov. 2107.
DOI: https://doi.org/10.1109/nafosted.2017.8108034.

[5] I. Krikides, J.S. Thompson, S. Mclaughlim, “Relay Selection for Secure Cooperative Networks with Jamming,” IEEE Trans. vol. 8, no. 10, pp. 1536-1276, Oct. 2009.
DOI: https://doi.org/10.1109/twc.2009.090323.

[6] H.Y. Kong, “A Solution of Binary Jamming Message to Source-Wiretapping and Disadvantage of Sharing the Jamming Signal in Physical-Layer Security,” JIIBC, vol. 14, no. 6, pp. 63-67, Dec. 2014.
DOI: https://doi.org/10.7236/jiibc.2014.14.6.63.

[7] John G. Proakis, Digital Communications, New York: McGraw-Hill, 1995.

[8] A. Papoulis, Probability, Random Varialbes, and Stochastic Processes, New York: McGraw-Hill, 2002.

저자 소개

박 솔(준회원)

- 2010년 3월 ~ 2017년 2월 : 울산대학교 전기공학부 학사
- 2017년 3월 ~ 현재 : 울산대학교 전기공학부 석사

<주관심분야> : MIMO, 협력통신, 물리 계층 보안, 에너지 하베스팅, 인지 기술

공 형 윤(정회원)

- 1989년 2월 : New York Institute of Technology(미국) 전자공학과 학사
- 1991년 2월 : Polytechnic University (미국) 전자 공학과 석사
- 1996년 2월 : Polytechnic University (미국) 전자 공학과 박사
- 1996년 ~ 1996년 : LG전자 PCS팀장
- 1996년 ~ 1998년 : LG전자 회장실 전략 사업단
- 1998년 ~ 현재 : 울산대학교 전기전자정보시스템공학부 교수

<주관심분야> : 모듈레이션, 채널 부호화, 검파 및 추정 기술, 협력통신, 센서네트워크