The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 18, No. 3, pp.71-75, Jun. 30, 2018. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2018.18.3.71
JIIBC 2018-3-10

재머를 사용하는 복호 후 재전송 기반 물리 계층 보안의 성능 분석

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

박솔*, 공형윤**

Sol Park*, Hyung-Yun Kong**

요 약 본 논문에서는 복호 후 재전송 기반의 중계기 시스템에서 재머를 사용했을 때의 보안 불능 확률을 연구한다. 물리 계층에서 보안 용량을 증가시키기 위해서 선택되지 않은 중계기들 중에서 재머를 선택하여 의도적인 잡음을 발생시키도록 할 수 있다. 재머에 의한 잡음은 수신자와 도청자에서 동일하게 간섭으로 작용하지만 송신자-도청자 링크 간의 채널 품질을 송시자-수신자 링크의 채널보다 더 악화 시키는 최적의 재머를 선택하여 물리 계층 보안을 강화할 수 있다. 본 논문에서는 재머의 유무에 따른 보안 불능 확률의 이론적인 식을 계산하고, 그 식이 타당한지 증명하기 위하여 이론값과 모의실험을 통한 실험값을 비교해 본다.

Abstract In this paper, we study the secrecy outage probability when using jammer in a relay system based on decode-and-forward. The jammer may be selected among the relays not selected to increase the security capacity in the physical layer so as to generate intentional noise. Jammer noise can equally interfere with the receiver and eavesdropper but can enhance the physical layer security by selecting an optimal jammer that makes the channel quality between the sender-eavesdropper links worse than the channel of the sender-receiver link. In this paper, we compute the theoretical formula of the secrecy outage probability with and without jammers, and compare the theoretical value with the simulation value to prove that the equation is valid.

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

Ⅰ. 서 론

무선 통신 네트워크의 사용이 빈번해지면서 이러한 네트워크에서 개인 정보 보호와 보안에 대한 관심이 더욱 많아지게 되었다. 기존의 네트워크에서 보안은 물리 계층이 아닌 상위 계층에서 주로 다루어졌다. 기존의 네트워크에서 보안은 메시지를 암호화 및 해독하기 위한 공통의 비밀 키가 필요하다. 이는 공통의 비밀 키의 관리와 분배가 어려워지면서 무선 시스템이 보안에 취약하도록 만들었다. 이에 따라 물리 계층에서도 보안을 구현하기 위한 연구가 계속 진행되고 있다[1-2].

물리 계층 보안은 별도의 암호화 프로토콜 없이 정보 이론적 관점에서 무선 시스템의 보안을 강화할 수 있다는 강점이 있다. 물리 계층 보안은 송신자-수신자 링크의

*준회원, 울산대학교 전기공학부
**정회원, 울산대학교 전기전자정보시스템공학부(교신저자)
접수일자: 2018년 3월 28일, 수정완료: 2018년 5월 18일
게재확정일자: 2018년 6월 8일

Received: 28 March, 2018 / Revised: 18 May, 2018
Accepted: 8 June, 2018
**Corresponding Author: hkong@ulsan.ac.kr
School of Electrical Engineering, University of Ulsan, Korea

채널 용량은 높이고 송신자-도청자 링크의 채널 용량은 낮춰 무선 시스템의 보안을 높이는 방법이다. 일반적으로 무선 통신에서 간섭은 부정적인 요인으로 작용한다. 하지만 이러한 간섭을 적절히 이용하여 물리 계층에서 보안 용량을 높이는 방법이 연구 되고 있다[3-6].

간섭을 이용하여 보안 용량을 높이는 방법은 크게 두 가지로 분류할 수 있다. 특정 노드에서 인공적인 잡음을 발생시켜 도청자 링크의 채널 품질을 악화시키는 것은 동일하나 수신자가 인공적인 잡음의 영향을 받느냐 받지 않느냐에 따라서 분류할 수 있다. 논문 [3-5]는 수신자가 인공적인 잡음에 대한 정보를 미리 알고 있다고 가정한다. 반면에 [6]은 수신자가 인공적인 잡음에 대한 정보를 모른다고 가정하며, 간섭으로 작용한다.

본 논문에서는 재머를 사용하는 복호 후 재전송 기반의 중계기 시스템에서 물리 계층 보안을 연구한다. 재머의 유무에 따른 보안 불능 확률의 이론적인 식을 계산하고, 그 식이 타당한지 증명하기 위하여 이론값과 모의실험을 통한 실험값을 비교해 본다.

2장에서 시스템 모델을 설명하고 3장에서 재머의 유무에 따른 보안 불능 확률을 계산한다. 4장에서 이론값과 모의실험 결과값을 비교하며 5장에서 결론 짓는다.

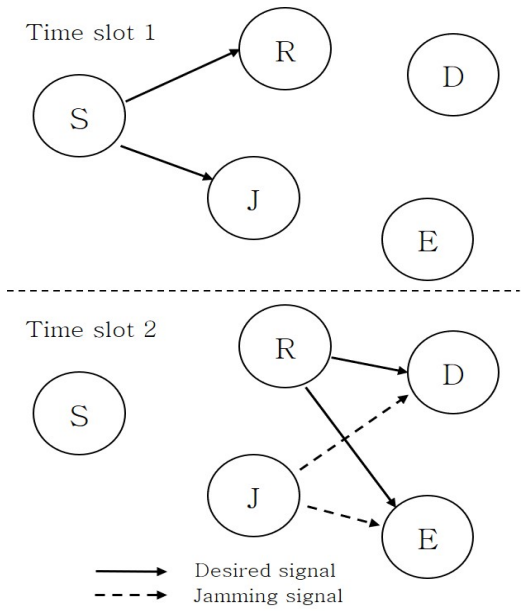


그림 1. 시스템 모델
Fig. 1. System model

II. 시스템 모델

하나의 송신자, 수신자, 도청자, 그리고 DF 기반 중계기와 재머가 존재하는 협력 통신 시스템을 가정한다. 시스템 모델은 그림 1과 같다. 중계기는 항상 송신자의 신호를 완벽하게 복호할 수 없다. 송신자-중계기 링크의 SNR(Signal-to-Ratio)이 사전에 정의해둔 임계값 γ_{th} 보다 크거나 같은 경우에만 중계기에서 송신자의 메시지를 복호할 수 있다고 가정한다. 모든 노드 사이의 링크는 레일리 페이딩 채널 하에 있으며 반이중 모드를 기본으로 한다. 수신자와 도청자는 송신자와 멀리 떨어져 있어 중계기의 도움 없이는 송신자의 메시지를 전달 받을 수 없다고 가정한다. 시스템은 두 개의 시간 슬롯으로 나뉜다. 첫 번째 시간 슬롯에서 송신자는 중계기로 메시지를 전송한다. 무선 통신에서 전파는 모든 방향으로 전달되기 때문에 클러스터 내의 모든 중계기는 송신자의 메시지를 들을 수 있다. 다수의 중계기 중 보안 용량을 최대로 하는 최적의 중계기와 최적의 재머가 논문 [6]에 의하여 이미 선택되었다고 가정한다. 두 번째 시간 슬롯에서 선택된 최적의 중계기는 송신자의 신호를 복호한 후 재전송한다. 이 때 재전송된 중계기의 신호는 무선 통신의 성질에 의해 수신자와 도청자 모두에서 감지된다. 동시에 두 번째 시간 슬롯 동안에 최적의 재머는 인공적인 잡음을 발생시키며 이 잡음은 수신자와 도청자에서 동일하게 간섭으로 작용한다. 이는 수신자와 도청자에서 재머에 의한 잡음 신호의 정보를 알 수 없다고 가정했기 때문이다.

임의의 노드 a와 b 사이의 SNR은 다음과 같다.

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

P_a는 a 노드의 전송 전력이며 N_o는 AWGN (Additive White Gaussian Noise)의 분산이다. 송신자와 중계기의 전송전력은 동일하며 P_S로 표현한다. 반면에 재머의 전송전력은 P_J로 나타내며 재머의 간섭으로부터 중계기-수신자 링크를 보호하고 보안용량을 극대화하기 위해서 재머의 전송전력은 중계기의 전송전력보다 낮다고 가정하며 $P_J = P_S / L$로 정의한다[6]. 여기서 L은 1보다 매우 큰 수로 한다. h_{ab}는 a와 b 노드 사이의 레일리 분포로서 분산 $\sigma_{ab}^2 = d_{ab}^{-\beta}$ 을 가진다. d_{ab}는 a와 b 사이의

유클리디안 거리이고 β는 경로 손실 계수이다. 평균 SNR을 $1/\alpha_{ab}$ 로 할 때, γ_{ab}는 α_{ab}를 지수분포로 하는 확률 변수이며, 그 PDF와 CDF는 각각 다음과 같다.

$$f_{\gamma_{ab}}(z)=\alpha_{ab}e^{-z\alpha_{ab}} \tag{2}$$

$$F_{\gamma_{ab}}(z)=1-e^{-z\alpha_{ab}} \tag{3}$$

보안 용량은 주요 링크의 채널 용량과 도청 링크의 채널 용량의 차로 계산되며 다음과 같다[1].

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

여기서 γ_D와 γ_E는 각각 수신자와 도청자의 SNR이다.

보안 불능 확률은 P_{out}로 나타내며 보안용량이 목표로 하는 보안률 R_S 보다 작을 확률로 한다. 이 때 R_S는 0보다 큰 수로 한다.

Ⅲ. 보안 불능확률

이 장에서는 최적의 재머와 복호 후 재전송 기반의 최적의 중계기를 사용하는 시스템의 보안 불능 확률을 계산한다.

보안 불능 확률은 논문 [7]을 참고하여 다음의 식으로 계산할 수 있다.

$$\begin{aligned}P_{out}&=\Pr[ASR<R_S|\gamma_R>\gamma_{th}]\Pr[\gamma_R>\gamma_{th}]\\&+\Pr[ASR<R_S|\gamma_R<\gamma_{th}]\Pr[\gamma_R<\gamma_{th}]\end{aligned} \tag{5}$$

재머를 사용하지 않고 최적의 중계기가 이미 선택됐다고 가정할 때, 보안 불능 확률은 다음과 같다.

$$\begin{aligned}P_{out}&=(\int_0^\infty F_{\gamma_D}(\rho-1+\rho x|\gamma_R>\gamma_{th})f_{\gamma_E}(x)dx)\\&\times e^{-\gamma_{th}\alpha_{SR}}+1\times(1-e^{-\gamma_{th}\alpha_{SR}})\\&=(1-\frac{\alpha_{RE}e^{-(\rho-1)\alpha_{RD}}}{\rho\alpha_{RD}+\alpha_{RE}})\times e^{-\gamma_{th}\alpha_{SR}}+(1-e^{-\gamma_{th}\alpha_{SR}})\\&=1-\frac{\alpha_{RE}e^{-(\rho-1)\alpha_{RD}}e^{-\gamma_{th}\alpha_{RS}}}{\rho\alpha_{RD}+\alpha_{RE}}\end{aligned} \tag{6}$$

여기서 $\rho=2^{2R_S}$ 이며 $\gamma_R<\gamma_{th}$인 경우 중계기가 송신자의 신호를 제대로 복호할 수 없으므로 보안 불능 확률은 1이 된다. α_{SR}, α_{RD}, α_{RE}는 각각 송신자-중계기, 중계기-수신자, 그리고 중계기-도청자 링크의 평균 SNR의 역수이다.

최적의 재머와 최적의 중계기를 사용하는 시스템의 보안 불능 확률 또한 식 (5)을 통하여 계산할 수 있다.

재머를 사용하는 시스템에서 송신자-중계기, 중계기-수신자, 중계기-도청자 링크의 SNR은 다음과 같다.

$$\gamma_R=\gamma_{SR} \tag{7}$$

$$\gamma_D=\frac{\gamma_{RD}}{1+\gamma_{JD}}\approx\frac{\gamma_{RD}}{\gamma_{JD}} \tag{8}$$

$$\gamma_E=\frac{\gamma_{RE}}{1+\gamma_{JE}}\approx\frac{\gamma_{RE}}{\gamma_{JE}} \tag{9}$$

중계기-수신자, 중계기-도청자 링크에서 재머의 신호는 간섭으로 작용한다. 이 때 재머에 의한 간섭은 1보다 매우 크므로 식 (8), (9)로 근사 시킬 수 있다.

첫 번째 시간 슬롯에서 송신자-중계기 링크는 재머의 영향을 받지 않기 때문에 재머를 사용하지 않는 시스템의 불능 확률과 동일하다. 이를 계산하면 다음과 같다.

$$F_{\gamma_R}(\gamma_{th})=\Pr[\gamma_{SR}<\gamma_{th}]=1-e^{-\gamma_{th}\alpha_{SR}} \tag{10}$$

$\gamma_R<\gamma_{th}$인 경우 재머를 사용하지 않는 시스템과 동일하게 보안 불능 확률은 1이 된다.

$\gamma_R>\gamma_{th}$인 경우의 보안 불능 확률을 계산하기 위해서는 식 (8), (9)의 CDF를 구해야 한다. 식 (8), (9)의 CDF는 [8]을 참고하여 다음과 같이 계산할 수 있다.

$$F_{\gamma_D}(z)=\int_0^\infty F_{\gamma_{RD}}(yz)f_{\gamma_{JD}}(y)dy=1-\frac{\alpha_{JD}}{\alpha_{JD}+z\alpha_{RD}} \tag{11}$$

$$f_{\gamma_E}(z)=\int_0^\infty yf_{\gamma_{RE}}(yz)f_{\gamma_{JE}}(y)dy=\frac{\alpha_{RE}\alpha_{JE}}{(\alpha_{JE}+z\alpha_{RE})^2} \tag{12}$$

여기서 α_{JE}, α_{JD}는 재머-도청자, 재머-수신자 링크의 평균 SNR의 역수이다.

식 (11), (12)을 이용하여 $\gamma_R > \gamma_{th}$인 경우의 보안 불능 확률을 계산하면 다음과 같다.

$$\begin{aligned}&\Pr[ASR < R_S | \gamma_R > \gamma_{th}] \\ &= \int_0^{\infty} F_{\gamma_D}(\rho - 1 + \rho x | \gamma_R > \gamma_{th}) f_{\gamma_E}(x) dx \\ &= \int_0^{\infty} (1 - \frac{1}{1 + \beta_D(\rho - 1 + \rho x)}) \cdot \frac{\beta_E}{(1 + \beta_E x)^2} dx\end{aligned} \tag{13}$$

(13)에서 $\beta_D = \alpha_{RD}/\alpha_{JD}$, $\beta_E = \alpha_{RE}/\alpha_{JE}$이다.

(13)을 적분하기 위해서 부분분수를 이용한다. 부분분수를 이용하여 전개한 식은 다음과 같다.

$$\begin{aligned}&\Pr[ASR < R_S | \gamma_R > \gamma_{th}] \\ &= 1 - \int_0^{\infty} (\frac{C_1 K}{1 + Kx} dx - \frac{C_1 \beta_E}{1 + \beta_E x} + \frac{C_2 \beta_E}{(1 + \beta_E x)^2}) dx \\ &= 1 - C_1 \ln(K/\beta_E) - C_2\end{aligned} \tag{14}$$

여기서 $C_1 = \beta_D \beta_E \rho / (\beta_D \rho - \beta_D \beta_E \rho + \beta_D \beta_E - \beta_E)^2$, $C_2 = \beta_E / (\beta_E + \beta_D \beta_E \rho - \beta_D \beta_E - \beta_D \rho)$ 이고 $K = \beta_D \rho / (1 + \beta_D \rho - \beta_D)$이다.

식 (5), (10), (14)를 이용하여 재머를 사용하는 시스템의 보안 불능 확률 최종 식을 계산하면 다음과 같다.

$$P_{out} = 1 - C_1 e^{-\gamma_{th}\alpha_{SR}} \ln \frac{K}{\beta_E} - C_2 e^{-\gamma_{th}\alpha_{SR}} \tag{15}$$

Ⅳ. 모의실험 결과

이 장에서는 제안한 시스템 모델의 모의실험 결과를 제시한다. 재머를 사용하지 않는 무선 시스템과 재머를 사용하는 시스템의 보안 불능 확률의 모의실험 결과와 이론을 통하여 계산한 값을 비교해 본다. 재머의 유무에 따른 시스템의 채널 성능을 비교하기 위해서 모의실험을 통하여 불능 확률에 대한 그래프를 얻어 본다.

그림 2는 시스템에 따른 보안 불능 확률의 그래프이다. 그림 2를 보면 모의실험 결과와 본 논문에서 계산한 이론값이 정확히 일치하는 것을 확인할 수 있다. 이를 통해 본 논문에서 제시한 재머를 사용하는 시스템의 보안 불능 확률의 이론식이 타당함을 알 수 있다. 더불어 재머를 사용하는 시스템이 그렇지 않은 시스템에 비해 보안성이 더 뛰어남을 확인할 수 있다. 반면에 그림 3을 통하여 재머를 사용했을 때 시스템의 성능은 그렇지 않을 때보다 낮아지는 것을 확인할 수 있다. 이는 재밍 신호가 간섭으로 작용하여 시스템의 성능을 낮추기 때문이다. 모의실험에서 사용한 파라미터는 표 1에 정리했다.

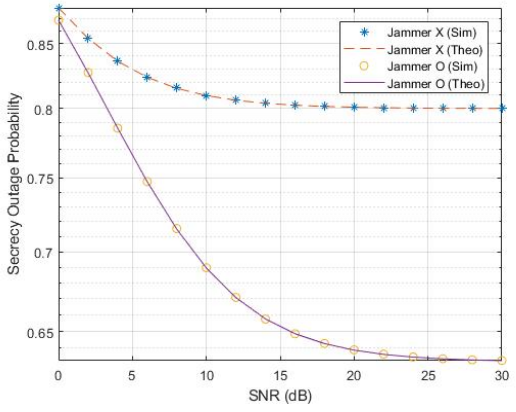


그림 2. 보안 불능 확률
Fig. 2. Secrecy outage probability

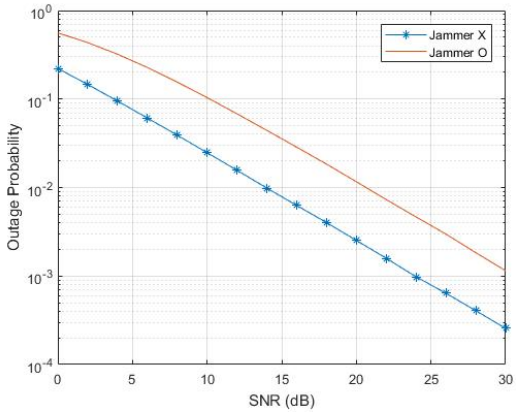


그림 3. 불능 확률
Fig. 3. outage probability

표 1. 실험 파라미터
Table 1. Simulation Parameters

거리 손실 계수	3
γ_{th}	1
R_S	1
SNR	0 ~ 30dB
송신자-중계기 거리	0.5
중계기-수신자 거리	0.5
중계기-도청자 거리	0.5
재머-수신자 거리	0.5
재머-도청자 거리	0.4123
P_S	1
L	100

V. 결 론

본 논문은 재머의 사용 유무가 물리 계층 보안에 어떤 영향을 미치는지 확인하였다. 또한 재머를 사용하는 시스템의 보안 불능 확률 식을 계산하고 모의실험 결과와 비교하여 타당함을 입증했다. 본 논문에서는 최적의 중계기와 최적의 재머가 이미 선택됐다고 가정했다. 다수의 중계기에서 최적의 중계기와 재머를 선택하는 기법을 포함하는 보안 불능 확률 식을 계산하는 것으로 본 논문을 확장시킬 수 있다.

References

[1] A. D. Wyner, "The Wire-Tap Channel," Bell Syst. Tech. J., vol.54, pp. 1355-1387, Jan. 1975. DOI: https://doi.org/10.1002/j.1538-7305.1975.tb02040.x.

[2] 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.

[3] 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.

[4] H. Long, W. Xiang, J. Wang, Y. Zhang, and W. Wang, "Cooperative Jamming and Power Allocation with Untrusty Two-Way Relay Nodes," IET Commun, vol. 8, no. 13, pp. 2290-2297, Sep. 2014. DOI: https://doi.org/10.1049/iet-com.2013.0580.

[5] L. Dong, H. Yousefi'zadeh, and H. Jafarkhani, "Cooperative Jamming and Power Allocation for Wireless Relay Networks in Presence of Eavesdropper," in IEEE Int. Conf. Commun. (ICC), June 2011. DOI: https://10.1109/icc.2011.5963094.

[6] 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://10.1109/TWC.2009.090323.

[7] K. Chopra, R. Bose, A. Joshi, "Secrecy Outage Performance of Cooperative Relay Network with Diversity Combining," ICSIP' 17, November 2016. DOI: 10.1109/SIPROCESS.2017.8124587.

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

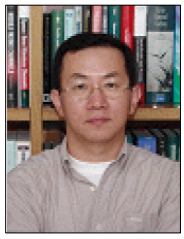
저자 소개

박 솔(준회원)

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

<주관심분야> : MIMO, 협력통신, 물리계층 보안, 에너지 하베스팅, 인지기술

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