The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 19, No. 1, pp.21-27, Feb. 28, 2019. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2019.19.1.21
JIIBC 2019-1-4

# 다수의 중계기가 존재하는 복호 후 재전송 기반 협력 통신 시스템에서 부분적인 중계기 선택을 사용하는 물리 계층 보안의 성능 분석

# Performance Analysis of Physical Layer Security using Partial Relay Selection in Cooperative Communication based on Decode-and-Forward with Multi-Relay

박솔*, 공형윤**

**Sol Park*, Hyung-Yun Kong****

**요 약** 본 논문에서는 다수의 중계기가 존재하는 복호 후 재전송 기반의 협력 통신 시스템에서 부분적인 중계기 선택 기법을 사용 했을 때의 보안 불능 확률을 연구한다. 수신 노드와 도청 노드는 각각 송신 노드와 중계 노드 모두에서 신호를 수신한다고 가정한다. 수신된 두 신호는 MRC 기법을 사용하여 다이버시티 이득을 얻는데 이용된다. 본 논문에서는 다수의 중계기가 존재하는 시스템의 보안 불능 확률 식을 계산하고, 그 식이 타당한지 증명하기 위해서 이론값과 모의실험 결과값을 비교한다. 중계기의 수에 따라 보안 불능 확률이 어떻게 변하는지를 모의실험 결과를 통해 도출한다.

**Abstract** In this paper, we investigate the secrecy outage probability when using a partial relay selection scheme in cooperative communication systems based on decode-and-forward with multi-relay. It is assumed that both the receiving node and the eavesdropping node receive signals at both the transmitting node and the relaying node. The two received signals are used to obtain the diversity gain using the MRC scheme. In this paper, we compute the theoretical formula of secrecy outage probability and compare the theoretical value with the simulation value to prove that equation is valid. The simulation results show how the secrecy outage probability varies with the number of relays.

**Key Words :** relay selection, physical layer security, cooperative diversity, secrecy outage probability

## Ⅰ. 서 론

물리 계층 보안은 정보 이론적 관점에서 무선 시스템의 보안을 강화하는 방법이다. 일반적으로 물리 계층 보안을 실현하기 위해 중계기 시스템을 이용한다. 송신 노드와 수신 노드 사이에 존재하는 중계기 중, 보안 용량을 최대로 만드는 최적의 중계기를 선택하여 중계함으로 시스템의 보안을 향상 시킬 수 있다.

논문 [1]에서 Wyner에 의해 물리 계층 보안이 처음으로 제안됐다. 논문 [2]에서는 가우시안 채널에서 물리 계층 보안이 연구됐다. 단일 중계기가 존재하는 협력통신 시스템에서 물리 계층 보안은 논문 [3]에서 연구됐다.

*준회원, 울산대학교 전기공학부(교신저자)
**정회원, 울산대학교 전기전자정보시스템공학부
접수일자 2018년 11월 7일, 수정완료 2019년 1월 17일
게재확정일자 2019년 2월 8일

Received: 7 November, 2018 / Revised: 17 January, 2019 / Accepted: 8 February, 2019
*Corresponding Author: emdemddl@mail.ulsan.ac.kr
School of Electrical Engineering, University of Ulsan, Korea

다수의 중계기가 존재하는 시스템에서, 최적의 중계기를 선택하여 중계하는데 이용함으로 자원의 낭비를 막으면서 다수의 중계기를 통해 중계하는 것과 같은 성능을 얻을 수 있다. 중계기 선택 기법에는 기회주의적 중계기 선택 기법과 부분적인 중계기 선택 기법이 있다. 부분적인 중계기 선택 기법은 송신 노드와 중계 노드 링크 중심의 중계기 선택 기법과 중계 노드와 수신 노드 링크 중심의 중계기 선택 기법으로 분류할 수 있다. 일반적으로 기회주의적 중계기 선택 기법이 부분적인 중계기 선택 기법에 비해서 더 나은 채널 성능을 보인다. 하지만 물리계층 보안의 경우 중계 노드와 수신 노드 링크 중심의 부분적인 중계기 선택 기법이 다른 중계기 선택 기법에 비해서 더 나은 보안 성능을 보인다[4].

본 논문에서는 중계 노드와 수신 노드 링크 중심의 부분적인 중계기 선택 기법과 협력 다이버시티를 사용했을 때, 복호 후 재전송 기반의 협력통신 시스템에서 물리 계층 보안의 보안 불능 확률에 대해서 분석하고 모의실험을 통해 검증한다.

2장에서는 시스템의 모델을 설명하고 3장에서 제안하는 시스템의 보안 불능 확률을 계산한다. 4장에서 제안하는 시스템의 모의실험 결과를 분석하고 검증한다. 5장에서 본 논문을 결론짓는다.

## II. 시스템 모델

하나의 송신자, 수신자, 도청자, 그리고 다수의 중계기가 존재하는 복호 후 재전송 기반의 협력 통신 시스템을 가정한다. 송신자와 중계기 링크의 신호 대 잡음비(Signal to Noise Ratio, 이하 SNR)가 사전에 정의한 임계값 $\gamma_{th}$ 보다 큰 경우에만 중계기에서 송신자의 신호를 완벽하게 복호했다고 가정한다. 협력통신 시스템에서 수신자는 중계기를 통해 중계되는 신호뿐만 아니라 송신자와 수신자 사이의 직접 링크를 통해 송신자의 신호를 수신 받게 된다. 중계기의 중계 신호와 송신자의 원 신호가 수신자에서 MRC(Maximal Ratio Combining) 기법을 사용하여 결합된다고 가정한다. 중계기 선택 기법은 중계기와 수신자 링크 중심의 부분적인 중계기 선택 기법이 사용된다. 각 노드 사이의 채널 환경은 레일리 페이딩 채널을 따르며, 반이중 모드를 가정한다. 전체 시스템은 두 개의 타임 슬롯으로 구성된다고 가정한다. 첫 번째 타임 슬롯에서 송신자는 수신자, 도청자, 그리고 다수의 중계기로 신호를 브로드캐스팅 한다. 두 번째 타임 슬롯에서 중계기는 전송 받은 송신자의 신호를 복호한 후 다시 부호화하여 수신자와 도청자로 브로드캐스팅 한다. 즉, 수신자와 도청자는 각각 송신자의 신호와 중계기의 신호를 전송 받게 된다.

중계기, 수신자, 그리고 도청자에서 전송 받은 신호는 각각 다음과 같이 나타낼 수 있다.

$$y_{SR_i} = \sqrt{P_S} h_{SR_i} x_S + n_{SR_i} \quad (1)$$

$$y_{R_iD} = \sqrt{P_R} h_{R_iD} x_{R_i} + n_{R_iD} \quad (2)$$

$$y_{R_iE} = \sqrt{P_R} h_{R_iE} x_{R_i} + n_{R_iE} \quad (3)$$

여기서 $P_S$와 $P_R$는 송신자와 중계기의 전송 전력이며 본 논문에서는 두 전송 전력이 동일하다고 가정한다. $h_{SR_i}$, $h_{R_iD}$, 그리고 $h_{R_iE}$는 각각 송신자와 중계기, 중계기와 수신자 그리고 중계기와 도청자 사이의 채널로 정의한다. 이 때 각 채널의 분산은 $\sigma_{ab}^2 = d_{ab}^{-\beta}$이다. 여기서 a와 b는 각각 송신자-중계기, 중계기-수신자, 그리고 중계기-도청자가 된다. $\beta$는 경로 손실 계수이며 본 논문에서 $\beta = 3$으로 가정한다.

a와 b 노드 사이의 SNR은 다음과 같이 나타낸다.

$$\gamma_{ab} = \frac{P_a |h_{ab}|^2}{N_o} \quad (4)$$

여기서 $N_o$는 AWGN(Additive White Gaussian Noise)의 분산이다.

레일리 페이딩 채널일 때, a와 b 노드 사이의 채널에 대한 PDF와 CDF는 각각 다음과 같다[5].

$$f_{\gamma_{ab}}(z) = \alpha_{ab} e^{-z\alpha_{ab}} \quad (5)$$

$$F_{\gamma_{ab}}(z) = 1 - e^{-z\alpha_{ab}} \quad (6)$$

여기서 $\alpha_{ab} = 1/\gamma_{ab}$이다.

$ASR$은 수신자의 채널 용량과 도청자의 채널 용량의 차로 정의한다. MRC 기법을 사용하는 협력 통신 시스템의 i번째 중계기를 통한 $ASR$은 다음과 같이 나타낼 수

있다.

$$ASR_i = \frac{1}{2}\left[\log_2\left(\frac{1+\gamma_{R_iD}+\gamma_{SD}}{1+\gamma_{R_iE}+\gamma_{SE}}\right)\right]^+ \quad (7)$$

여기서 $[x]^+$는 $\max[x,0]$을 의미한다.

## Ⅲ. 보안 불능확률

이 장에서는 부분적인 중계기 선택 기법을 사용하는 복호 후 재전송 기반의 협력 통신 시스템의 보안 불능 확률을 분석한다.

물리 계층 보안 시스템에서 중계기와 수신자 링크 중심의 부분적인 중계기 선택 기법은 다음과 같이 최적의 중계기를 선택한다.

$$R_b = \arg\max_{i=1,\ldots,M}(ASR_i) \quad (8)$$

보안 불능 확률은 $ASR$이 목표 보안율인 $R_S$ 보다 작을 확률로 정의한다. 이 때 $R_S > 0$이다. 제안하는 시스템의 보안 불능 확률은 논문 [6]을 참고하여 다음의 식으로 계산할 수 있다.

$$P_{out} = \Pr[ASR_b < R_S | \gamma_{SR_b} > \gamma_{th}]\Pr[\gamma_{SR_b} > \gamma_{th}] + \Pr[ASR < R_S | \gamma_{SR_b} < \gamma_{th}]\Pr[\gamma_{SR_b} < \gamma_{th}] \quad (9)$$

여기서 $ASR_b$는 최적의 중계기에 의한 $ASR$로, $\gamma_{SR_b}$는 송신자와 최적의 중계기 링크의 $SNR$로 정의한다.

송신자와 수신자의 직접 링크가 존재하는 경우, 선택된 중계기가 송신자의 신호를 올바르게 복호하지 못하더라도 직접 링크를 통하여 서로 통신이 가능하다. 이 때의 $ASR$은 다음과 같다.

$$ASR = \frac{1}{2}\left[\log_2\left(\frac{1+\gamma_{SD}}{1+\gamma_{SE}}\right)\right]^+ \quad (10)$$

식 (9)에 (7)와 (10)을 대입하여 다음과 같이 전개할 수 있다.

$$P_{out} = \Pr[\max_{i=1,\ldots,M} ASR_i < R_S]\Pr[\gamma_{SR_b} > \gamma_{th}] + \Pr[\gamma_{SD} < \rho\gamma_{SE} + (\rho-1)]\Pr[\gamma_{SR_b} < \gamma_{th}] \quad (11)$$

여기서 $\rho = 2^{2R_S}$이다.

식 (11)의 $\Pr[\gamma_{SR_b} > \gamma th]$, $\Pr[\gamma_{SD} < \rho\gamma_{SE} + (\rho-1)]$ 그리고 $\Pr[\gamma_{SR_b} < \gamma th]$는 (5), (6)를 이용하여 각각 다음과 같이 계산할 수 있다.

$$\Pr[\gamma_{SR_b} > \gamma th] = e^{-\gamma_{th}\alpha_{SR_b}} \quad (12)$$

$$\Pr[\gamma_{SR_b} < \gamma th] = 1 - e^{-\gamma_{th}\alpha_{SR_b}} \quad (13)$$

$$\Pr[\gamma_{SD} < \rho\gamma_{SE} + (\rho-1)] = \int_0^\infty F_{\gamma_{SD}}(\rho - 1 + \rho x) f_{\gamma_{SE}}(x)\,dx = 1 - \frac{\alpha_{SE} e^{-(\rho-1)\alpha_{SD}}}{\rho\alpha_{SD} + \alpha_{SE}} \quad (14)$$

$$\Pr[\max_{i=1,2} ASR_i < R_S] = 1 - [\Phi_S e^{(1-\rho)\alpha_{SD}}(\frac{\alpha_{R_1D}(1-\Phi_{R_1})}{\alpha_{R_1D}-\alpha_{SD}} + \frac{\alpha_{R_2D}(1-\Phi_{R_2})}{\alpha_{R_2D}-\alpha_{SD}} + \frac{\Phi_{R_1}\Phi_{R_2}(\alpha_{R_1E}+\alpha_{R_2E})}{\rho\alpha_{SD}+\alpha_{R_1E}+\alpha_{R_2E}} - \frac{(\alpha_{R_1D}+\alpha_{R_2D})(1-\Phi_{R_1})(1-\Phi_{R_2})}{\alpha_{R_1D}+\alpha_{R_2D}-\alpha_{SD}}) + (1-\Phi_{R_1})e^{(1-\rho)\alpha_{R_1D}}(1 - \frac{\rho\alpha_{R_1D}(1-\Phi_S)}{\rho\alpha_{R_1D}+\alpha_{SE}} - \frac{\alpha_{R_1D}\Phi_S}{\alpha_{R_1D}-\alpha_{SD}}) + (1-\Phi_{R_2})e^{(1-\rho)\alpha_{R_2D}}(1 - \frac{\rho\alpha_{R_2D}(1-\Phi_S)}{\rho\alpha_{R_2D}+\alpha_{SE}} - \frac{\alpha_{R_2D}\Phi_S}{\alpha_{R_2D}-\alpha_{SD}}) - (1-\Phi_{R_1})(1-\Phi_{R_2})e^{(1-\rho)(\alpha_{R_1D}+\alpha_{R_2D})} \times (1 - \frac{\alpha_{R_1D}+\alpha_{R_2D}\Phi_S}{\alpha_{R_1D}+\alpha_{R_2D}-\alpha_{SD}} - \frac{\rho(\alpha_{R_1D}+\alpha_{R_2D})(1-\Phi_S)}{\rho(\alpha_{R_1D}+\alpha_{R_2D})+\alpha_{SE}})] \quad (15)$$

식 (11)의 $\Pr[\max_{i=1,\ldots,M} ASR_i < R_S]$는 Appendix를 참고하여 $M=2$인 경우 식 (15)과 같이 계산될 수 있다.

식 (15)에서 $\Phi_S = \alpha_{SE}/(\rho\alpha_{SD}+\alpha_{SE})$, $\Phi_{R_1} = \rho\alpha_{R_1D}/(\rho\alpha_{R_1D}+\alpha_{R_1E})$, $\Phi_{R_2} = \rho\alpha_{R_2D}/(\rho\alpha_{R_2D}+\alpha_{R_2E})$로 정의 한다.

식 (12), (13), (14) 그리고 (15)를 식 (11)에 대입하면 제안하는 시스템의 보안 불능 확률을 얻을 수 있다.

## Ⅳ. 모의실험 및 결과

이 장에서는 3장의 성능 분석식과 제안하는 시스템의 모의실험 결과를 비교하여 식이 타당한지를 검증한다. 또한, 중계기 수에 따라 제안하는 시스템의 보안 불능 확률이 어떻게 변하는지를 조사한다.

그림 1에서 전송 전력 $P_S = P_R = 1$, 거리 손실 계수 $\beta = 3$, 목표 보안율 $R_S = 1$ 으로 가정한다. 각 노드들의 위치는 다음과 같다. 송신 노드 (0, 0), 수신 노드 (0, 1) 도청 노드 (1, 0), 중계기 1 (0.3, 0.6), 중계기 2 (0.4, 0.4), 중계기 3 (0.2, 0.5), 중계기 4 (0.6, 0.4).

그림 1을 통해 3장의 분석식과 모의실험 결과가 일치함을 볼 수 있다. 이를 통해 제안하는 시스템의 보안 불능 확률 분석식이 타당함을 알 수 있다. 또한 그림 1을 통해 M이 증가할수록 보안 불능 확률은 낮아짐을 확인할 수 있다. 이는 중계기의 수가 증가하면 시스템의 보안 성능은 더욱 향상된다는 것을 의미한다.

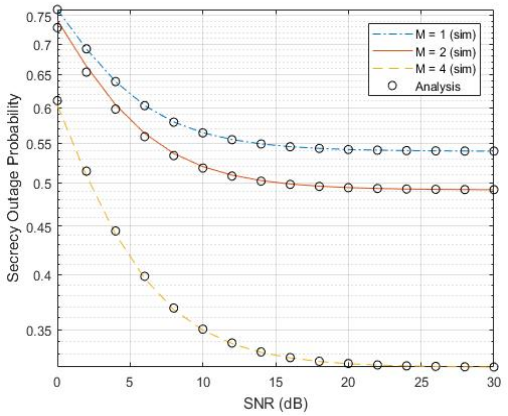


**그림 1. 중계기 수에 따른 보안 불능확률**
**Fig. 1. SOP according to the number of relays**

## Ⅴ. 결 론

본 논문은 다수의 중계기 존재하는 복호 후 재전송 기반의 협력 통신 시스템에서 부분적인 중계기 선택 기법을 사용할 때의 물리 계층 보안을 연구했다. 제안하는 시스템의 보안 불능 확률을 계산하고 모의실험 결과를 통해 분석식의 타당성을 검증했다. 또한 모의실험 결과를 통해 제안하는 시스템의 성능을 분석했다.

## APPENDIX

$\Pr[\max_{i=1,\ldots,M} ASR_i < R_S]$을 계산한다.

$$\Pr[\max_{i=1,\ldots,M} ASR_i < R_S] \tag{A.1}$$

다수의 중계기가 존재하는 시스템에 대한 (A.1)의 분석 식은 $M=2$인 경우의 식을 먼저 구한 후, 그 식을 확장하면 쉽게 구할 수 있다.

$M=2$인 경우, (A.1)는 다음과 같이 다시 쓸 수 있다.

$$\Pr[ASR_1 < R_S, ASR_2 < R_S] \tag{A.2}$$

여기서 $ASR_1$와 $ASR_2$는 각각 중계기 1과 중계기 2가 선택됐을 때의 보안 용량으로 정의한다.

(A.2)에 식 (7)을 대입하면 다음과 같다.

$$\Pr[1+\gamma_{SD}-\rho(1+\gamma_{SE}) < \min(\rho\gamma_{R_1E}-\gamma_{R_1D}, \rho\gamma_{R_2E}-\gamma_{R_2D})] \tag{A.3}$$

(A.3)은 다음 3개의 확률로 나누어 계산할 수 있다.

$$\Pr[1+\gamma_{SD}-\rho(1+\gamma_{SE}) < t] \tag{A.4}$$
$$\Pr[\rho\gamma_{R_1E}-\gamma_{R_1D} < t] \tag{A.5}$$
$$\Pr[\rho\gamma_{R_2E}-\gamma_{R_2D} < t] \tag{A.6}$$

(A.4)는 $\rho+t-1 \geq 0$와 $\rho+t-1 < 0$로 구분지어 계산해야 한다.

$\rho+t-1 \geq 0$인 경우, (A.4)는 식 (5), (6) 그리고 (15)

의 $\Phi_S$을 이용하여 다음과 같이 계산할 수 있다.

$$\int_0^{\infty} F_{\gamma_{SD}}(\rho+t-1+\rho x) f_{\gamma_{SE}}(x)dx$$
$$= 1-\frac{\alpha_{SE} e^{-(\rho+t-1)\alpha_{SD}}}{\rho\alpha_{SD}+\alpha_{SE}} = 1-\Phi_S e^{(1-\rho)\alpha_{SD}} e^{-\alpha_{SD} t} \quad (A.7)$$

$\rho+t-1<0$인 경우, (A.4)는 식 (5), (6)를 이용하여 다음과 같이 계산할 수 있다.

$$\int_{\frac{1-\rho+t}{\rho}}^{\infty} F_{\gamma_{SD}}(\rho+t-1+\rho x) f_{\gamma_{SE}}(x)dx$$
$$= (1-\frac{\alpha_{SE}}{\rho\alpha_{SD}+\alpha_{SE}}) e^{-(\frac{1-\rho-t}{\rho}\alpha_{SE})}$$
$$= (1-\Phi_S) e^{(\frac{\rho-1}{\rho})\alpha_{SE}} e^{\frac{t}{\rho}\alpha_{SE}} \quad (A.8)$$

(A.5)와 (A.6)는 $t/\rho \geq 0$와 $t/\rho < 0$로 구분지어 계산해야 한다.

$t/\rho \geq 0$인 경우, (A.5)는 식 (5), (6) 그리고 (15)의 $\Phi_{R_1}$을 이용하여 다음과 같이 계산할 수 있다.

$$\int_0^{\infty} F_{\gamma_{R_1E}}(\frac{t+x}{\rho}) f_{\gamma_{R_1D}}(x)dx$$
$$= 1-\frac{\rho\alpha_{R_1D} e^{-\frac{t}{\rho}\alpha_{R_1E}}}{\rho\alpha_{R_1D}+\alpha_{R_1E}} = 1-\Phi_{R_1} e^{-\frac{t}{p}\alpha_{R_1E}} \quad (A.9)$$

$t/\rho < 0$인 경우, (A.5)는 다음과 같다.

$$\int_{-t}^{\infty} F_{\gamma_{R_1E}}(\frac{t+x}{\rho}) f_{\gamma_{R_1D}}(x)dx$$
$$= (1-\frac{\rho\alpha_{R_1D}}{\rho\alpha_{R_1D}+\alpha_{R_1E}}) e^{\alpha_{R_1D} t} = (1-\Phi_{R_1}) e^{\alpha_{R_1D} t} \quad (A.10)$$

(A.5)와 같은 방법으로 (A.6)를 계산할 수 있다.

$$\Pr[\min(\rho\gamma_{R_1E}-\gamma_{R_1D}, \rho\gamma_{R_2E}-\gamma_{R_2D}) < t] \quad (A.11)$$

(A.11)은 (A.5)과 (A.6)의 계산식을 대입하여 다음과 같이 계산할 수 있다.

$$= 1-\Phi_{R_1}\Phi_{R_2} e^{-\frac{t}{\rho}(\alpha_{R_1E}+\alpha_{R_2E})} \quad (A.12)$$
$$= (1-\Phi_{R_1}) e^{\alpha_{R_1D} t} + (1-\Phi_{R_2}) e^{\alpha_{R_2D} t}$$
$$-(1-\Phi_{R_1})(1-\Phi_{R_2}) e^{(\alpha_{R_1D}+\alpha_{R_2D}) t} \quad (A.13)$$

(A.12)와 (A.13)는 각각 $t/\rho \geq 0$과 $t/\rho < 0$인 경우의 (A.11)에 대한 계산식이다.

구하고자 하는 식 (A.1)은 $t<1-\rho$, $1-\rho \leq t<0$, 그리고 $0 \leq t$의 세 부분으로 나누어 계산한다.

(A.1)을 계산하기 위해서는 (A.12), (A.13)의 미분식인 (A.11)의 PDF 식과 (A.7), (A.8)이 필요하다.

(A.11)의 PDF는 (A.12)과 (A.13)를 미분하여 각각 다음과 같이 얻을 수 있다.

$$= \frac{1}{\rho}\Phi_{R_1}\Phi_{R_2}(\alpha_{R_1E}+\alpha_{R_2E}) e^{-\frac{t}{\rho}(\alpha_{R_1E}+\alpha_{R_2E})} \quad (A.14)$$

$$= \alpha_{R_1D}(1-\Phi_{R_1}) e^{\alpha_{R_1D} t} + \alpha_{R_2D}(1-\Phi_{R_2}) e^{\alpha_{R_2D} t}$$
$$-(\alpha_{R_1D}+\alpha_{R_2D})(1-\Phi_{R_1})(1-\Phi_{R_2}) e^{(\alpha_{R_1D}+\alpha_{R_2D})t} \quad (A.15)$$

(A.14)는 $t/\rho \geq 0$일 때의 (A.11)의 PDF이고 (A.15)는 $t/\rho < 0$일 때의 PDF이다.

$t<1-\rho$인 경우, (A.1)는 (A.8)과 (A.15)를 이용하여 다음과 같이 계산할 수 있다.

$$\int_{-\infty}^{1-\rho} (1-\Phi_S) e^{(\frac{\rho-1}{\rho})\alpha_{SE}} e^{\frac{t}{\rho}\alpha_{SE}}$$
$$\times [\alpha_{R_1D}(1-\Phi_{R_1}) e^{\alpha_{R_1D} t} + \alpha_{R_2D}(1-\Phi_{R_2}) e^{\alpha_{R_2D} t}$$
$$-(\alpha_{R_1D}+\alpha_{R_2D})(1-\Phi_{R_1})(1-\Phi_{R_2}) e^{(\alpha_{R_1D}+\alpha_{R_2D})t}] dt$$
$$= \frac{\rho\alpha_{R_1D}(1-\Phi_S)(1-\Phi_{R_1})}{\rho\alpha_{R_1D}+\alpha_{SE}} e^{\alpha_{R_1D}(1-\rho)}$$

$$+\frac{\rho\alpha_{R_1D}(1-\Phi_S)(1-\Phi_{R_1})}{\rho\alpha_{R_1D}+\alpha_{SE}}e^{\alpha_{R_1D}(1-\rho)}$$
$$-\frac{\rho(\alpha_{R_1D}+\alpha_{R_2D})(1-\Phi_S)(1-\Phi_{R_1})(1-\Phi_{R_2})}{\rho(\alpha_{R_1D}+\alpha_{R_2D})+\alpha_{SE}}$$
$$\times e^{(\alpha_{R_1D}+\alpha_{R_2D})(1-\rho)} \quad (A.16)$$

$1-\rho \le t < 0$인 경우, (A.1)는 (A.7)과 (A.15)를 이용하여 다음과 같이 계산할 수 있다.

$$\int_{1-\rho}^{0}(1-\Phi_S e^{(1-\rho)\alpha_{SD}}e^{-\alpha_{SD}t})$$
$$\times[\alpha_{R_1D}(1-\Phi_{R_1})e^{\alpha_{R_1D}t}+\alpha_{R_2D}(1-\Phi_{R_2})e^{\alpha_{R_2D}t}$$
$$-(\alpha_{R_1D}+\alpha_{R_2D})(1-\Phi_{R_1})(1-\Phi_{R_2})e^{(\alpha_{R_1D}+\alpha_{R_2D})t}]dt$$
$$=(1-\Phi_{R_1})(1-e^{\alpha_{R_1D}(1-\rho)})+(1-\Phi_{R_2})(1-e^{\alpha_{R_2D}(1-\rho)})$$
$$-(1-\Phi_{R_1})(1-\Phi_{R_2})(1-e^{(\alpha_{R_1D}+\alpha_{R_2D})(1-\rho)})$$
$$+\frac{\alpha_{R_1D}\Phi_S(1-\Phi_{R_1})}{\alpha_{R_1D}-\alpha_{SD}}(e^{\alpha_{R_1D}(1-\rho)}-e^{\alpha_{SD}(1-\rho)})$$
$$+\frac{\alpha_{R_2D}\Phi_S(1-\Phi_{R_2})}{\alpha_{R_2D}-\alpha_{SD}}(e^{\alpha_{R_2D}(1-\rho)}-e^{\alpha_{SD}(1-\rho)})$$
$$+\frac{(\alpha_{R_1D}+\alpha_{R_2D})\Phi_S(1-\Phi_{R_1})(1-\Phi_{R_2})}{\alpha_{R_1D}+\alpha_{R_2D}-\alpha_{SD}}$$
$$\times(e^{\alpha_{SD}(1-\rho)}-e^{(\alpha_{R_1D}+\alpha_{R_2D})(1-\rho)}) \quad (A.17)$$

$0 \le t$인 경우, (A.1)는 (A.7)과 (A.14)를 이용하여 다음과 같이 계산할 수 있다.

$$\int_{1-\rho}^{0}(1-\Phi_S e^{(1-\rho)\alpha_{SD}}e^{-\alpha_{SD}t})$$
$$\times\frac{1}{\rho}\Phi_{R_1}\Phi_{R_2}(\alpha_{R_1E}+\alpha_{R_2E})e^{-\frac{t}{\rho}(\alpha_{R_1E}+\alpha_{R_2E})}dt$$
$$=(1-\frac{\Phi_S(\alpha_{R_1E}+\alpha_{R_2E})e^{(1-\rho)\alpha_{SD}}}{\rho\alpha_{SD}+\alpha_{R_1E}+\alpha_{R_2E}})\Phi_{R_1}\Phi_{R_2} \quad (A.18)$$

(A.1)은 각 구간에 대해서 구한 식을 모두 더하여 얻을 수 있다. 즉, $(A.1)=(A.16)+(A.17)+(A.18)$이다. 이렇게 구한 식을 정리하면 식 (15)을 얻을 수 있다.

세 개 이상의 중계기가 존재하는 시스템에 대하여 계산하는 경우, (A.2)를 확장하여 $M=2$인 경우와 동일한 계산 방법으로 구할 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] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," IEEE Trans. Inf. Theory, vol. 24, no. 4, pp. 451 - 456, July 1978. DOI: https://doi.org/10.1109/tit.1978.1055917

[3] S. Park, H.Y. Kong, "Performance Analysis of Physical Layer Security based on Decode and Forward using Jammer and Diversity," IIBC, vol.18, no.2, pp. 49-54, April 2018.

[4] 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.

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

[6] 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.

### 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