물리 계층 보안과 간섭 제약 환경에서 증폭 후 전송 기법의 성능 분석

Performance Analysis of the Amplify-and-Forward Scheme under Interference Constraint and Physical Layer Security

팜옥손, 공형윤*

Pham Ngoc Son, Hyung-Yun Kong*

요 약 언더레이 프로토콜은 2차 시스템이나 인지된 사용자가 1차 사용자의 품질 저하 없이 동일한 주파수를 사용하는 인지 기술이다. 또한, 무선 환경의 중계 특성으로 인해, 몇몇 노드는 도청 노드라고 불리며, 다른 통신 링크를 위한 정보를 수신한다. 이러한 이유로, 물리 계층의 보안은 도청의 발생을 막기 위해 보안 성취율을 고려하여 응용된다. 본 논문에서는, 물리 계층 보안과 간섭 제약 환경에서 증폭 후 전송 기법의 성능을 협력 통신 노드를 이용하여 분석한다. 이 모델에서, 중계기는 송신단에서 수신단으로의 신호 전송을 돕기 위해 증폭 후 전송 기법을 사용한다. 우수한 중계기는 기회주의적 중계기 선택 기법으로 선정되며, 단 대 단 보안 성취율을 기초로 한다. 시스템 성능은 보안 성취율의 정전 확률로 평가된다. 정전 확률의 상향, 하향 한계는 국제 통계 채널 상태 정보(CSI)에 기초하며, 또한, 닫힌계로 유도된다. 시뮬레이션 결과는 인지 네트워크는 1차 사용자로부터 충분히 멀 때, 중계기에서 도청 노드까지의 거리가 중계기에서 수신단까지의 거리보다 큰 경우 시스템 성능이 향상된 것을 보여준다.

Abstract The underlay protocol is a cognitive radio method in which secondary or cognitive users use the same frequency without affecting the quality of service (QoS) for the primary users. In addition, because of the broadcast characteristics of the wireless environment, some nodes, which are called eavesdropper nodes, want to illegally receive information that is intended for other communication links. Hence, Physical Layer Security is applied considering the achievable secrecy rate (ASR) to prevent this from happening. In this paper, a performance analysis of the amplify-and-forward scheme under an interference constraint and Physical Layer Security is investigated in the cooperative communication mode. In this model, the relays use an amplify-and-forward method to help transmit signals from a source to a destination. The best relay is chosen using an opportunistic relay selection method, which is based on the end-to-end ASR. The system performance is evaluated in terms of the outage probability of the ASR. The lower and upper bounds of this probability, based on the global statistical channel state information (CSI), are derived in closed form. Our simulation results show that the system performance improves when the distances from the relays to the eavesdropper are larger than the distances from the relays to the destination, and the cognitive network is far enough from the primary user.

*정회원, 울산대학교 전기전자정보시스템공학부
접수일자 : 2013년 11월 14일, 수정완료 : 2014년 1월 15일
게재확정일자 : 2014년 2월 7일

Ⅰ. Introduction

Cognitive radio is a protocol for effectively using spectrum in which a secondary or cognitive network cooperates with a primary network[1-2]. In cognitive radio, the underlay protocol is a sharing method in which the secondary users use the same frequency as the primary users when transmitting their signals without affecting the quality of service (QoS) of the primary network. Hence, the secondary users must control their power so that the interference power of the primary user is less than a threshold value, which is called the interference constraint[1-2]. In addition, because of the problems of wireless communication, including fading and obstacles, cooperative communication is an effective solution for enhancing system performance[3]. In this model, the decode-and-forward, amplify-and-forward, and coded cooperation methods are used by relay nodes to help the source forward signals to the destinations. Methods to select the best relay have been proposed in many papers, such as partial relay selection[4-5] and opportunistic relay selection[5] through two hops during two timeslots. The partial relay selection method chooses the best relay based on the best quality at either the source-relay or the relay-destination, while the opportunistic relay selection method considers the highest end-to-end signal quality.

In a wireless communication environment, because of the broadcast characteristics of the signals, some nodes, called eavesdroppers nodes, try to obtain these signals illegally. Hence, Physical Layer Security is proposed to prevent illegal actions without using keys between the source and destination[6-7] by using an achievable secrecy rate (ASR), which is a secret signal rate from the source to its desired destination. The methods to maximize this rate have been applied[6] to enhance communication system performance. In system analysis problems with Physical Layer Security, all of the instantaneous channel state information (CSI) is known at every node (called global CSI), but in practice, the statistical CSI of the source-primary user and relays-primary user links are available based on the long-term statistics of these nodes[7].

In this paper, we propose and analyze the system performance of the amplify-and-forward scheme under an interference constraint and Physical Layer Security, in which the best relay is chosen by the opportunistic relay selection method. The system performance is evaluated based on the outage probability of ASR. Our simulation results show that the system performance improves when the locations of the eavesdropper node are farther from the relays than the destination, and the cognitive network is farther from the primary network. In addition, the exact expressions for the lower and upper bounds of the outage probability are provided, and we show that the cooperative communication model improves and outperforms direct transmission when number of relays is increased.

This paper is organized as follows: Section 2 describes the system; Section 3 calculates and analyzes the cognitive system performance using the outage probability of ASR; Section 4 presents the simulation results; and Section 5 summarizes our conclusions.
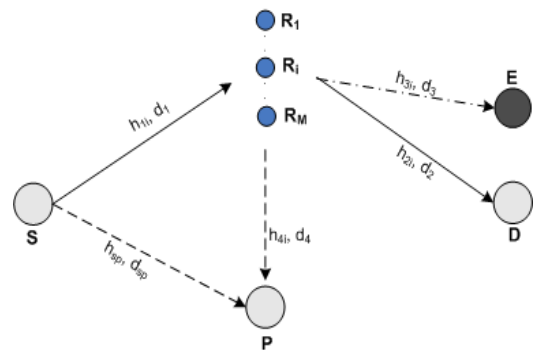

그림 1. 시스템 모델
Fig. 1. System model

Ⅱ. System Model

Fig. 1 presents the system model of the amplify-and-forward scheme under an interference

constraint and Physical Layer Security. In Fig. 1, the secondary network includes a source S, a destination D, an eavesdropper node E, and relays Ri, $i \in \{1, 2, ..., M\}$, where S wants to transmit signals to the destination D with the help of M relays under an interference constraint at the primary network (node P) and Physical Layer Security against the eavesdropper node E. In this communication model, the source S and relays Ri will decrease their power so that the interference at the primary user P is below a threshold value, and the eavesdropper node E wants the signals of the S–D communication link without the agreement of S and D. We assume the following:

- Each node has a single antenna.
- Eavesdropper node E keeps a close watch on and is near the destination D.
- All channels are flat and block Rayleigh fading channels in which the channel coefficients are constant in a packet interval and change from packet to packet.
- The global channel state information (CSI) is available regarding any two nodes.
- The additive white Gaussian noise (AWGN) at all relays and receiver nodes has the same zero mean and variance N_0.

In Fig. 1, $\left(h_{sp}, d_{sp}\right)$, $\left(h_{1i}, d_{1i}\right)$, $\left(h_{2i}, d_{2i}\right)$, $\left(h_{3i}, d_{3i}\right)$, and $\left(h_{4i}, d_{4i}\right)$ denote the Rayleigh fading channel coefficients and the link distances of S–P, S–Ri, Ri–D, Ri–E, and Ri–P, where $i \in \{1, 2, ..., M\}$.

Set $\omega_{sp} = \left|h_{sp}\right|^2$, $\omega_{1i} = \left|h_{1i}\right|^2$, $\omega_{2i} = \left|h_{2i}\right|^2$, $\omega_{3i} = \left|h_{3i}\right|^2$ and $\omega_{4i} = \left|h_{4i}\right|^2$, which are exponential random variables with parameters $\lambda_{sp} = d_{sp}^{\beta}$, $\lambda_{1i} = d_1^{\beta} = \lambda_1$, $\lambda_{2i} = d_2^{\beta} = \lambda_2$, $\lambda_{3i} = d_3^{\beta} = \lambda_3$, and $\lambda_{4i} = d_4^{\beta} = \lambda_4$, respectively, where β is a path-loss exponent.

In this paper, we propose an amplify-and-forward scheme under an Interference Constraint and Physical Layer Security (called the AFICPLS protocol), where the best relay is chosen using an opportunistic relay selection (ORS) method. We assume that there is not a direct link from S to D or from S to E. The operation principle of this protocol is based on a time-division channel model, and is split into two time slots. In the first time slot, the source S broadcasts the signal ps to all secondary relays Ri. The signal received at the ith relay Ri, $i \in \{1, 2, ..., M\}$, is given as

$$y_i = \sqrt{P_S} h_{1i} p_s + n_i \tag{1}$$

where PS is the transmit power of the source S, and ni is the additive white Gaussian noise (AWGN) at relay Ri.

During the second time slot, the selected relay Ri amplifies the received signal with a power gain Ai and then forwards the signal to the destination D and the eavesdropper node E. The signals received at the destination D and the eavesdropper node E are given, respectively, as

$$y_D = \sqrt{P_{R_i}} h_{2i} A_i y_i + n_D = \sqrt{P_{R_i}} h_{2i} A_i \sqrt{P_S} h_{1i} p_s + \sqrt{P_{R_i}} h_{2i} A_i n_i + n_D \tag{2}$$

$$y_E = \sqrt{P_{R_i}} h_{3i} A_i y_i + n_E = \sqrt{P_{R_i}} h_{3i} A_i \sqrt{P_S} h_{1i} p_s + \sqrt{P_{R_i}} h_{3i} A_i n_i + n_E \tag{3}$$

where PRi is the transmit power of the ith relay Ri; nD and nE are the additive white Gaussian noise (AWGN) at the destination D and the eavesdropper node E, respectively, and $A_i = 1 / \sqrt{P_S \left|h_{1i}\right|^2}$ is the gain relay[5].

III. Performance Analysis

Because the interference power at the primary user P is less than the threshold value Ip, the maximum power values of nodes S and Ri are, respectively:

$$P_S = \frac{I_P}{\left|h_{sp}\right|^2} = \frac{I_P}{\omega_{sp}} \tag{4}$$

$$P_{R_i} = \frac{I_P}{\left|h_{4i}\right|^2} = \frac{I_P}{\omega_{4i}} \tag{5}$$

The instantaneous end-to-end signal to noise ratios (SNRs) from the source S to the destination D and from the source S to the eavesdropper node E with the help of relay Ri are given, respectively, as

$$\gamma_{D_i} = \frac{P_S |h_{1i}|^2 A_i^2 P_{Ri} |h_{2i}|^2}{A_i^2 P_{Ri} |h_{2i}|^2 N_0 + N_0} = \frac{Q\omega_{1i}\omega_{2i}}{\omega_{sp}\omega_{2i} + \omega_{4i}\omega_{1i}} \quad (6)$$

$$\gamma_{E_i} = \frac{P_S |h_{1i}|^2 A_i^2 P_{Ri} |h_{3i}|^2}{A_i^2 P_{Ri} |h_{3i}|^2 N_0 + N_0} = \frac{Q\omega_{1i}\omega_{3i}}{\omega_{sp}\omega_{3i} + \omega_{4i}\omega_{1i}} \quad (7)$$

where $Q = I_P / N_0$.

Hence, the achievable data rates of the end-to-end links S-D and S-E through relay Ri are given as

$$R_a = \frac{1}{2}\log_2(1+\gamma_a), a \in \{D_i, E_i\} \quad (8)$$

where the factor (1/2) means that the signals are transmitted in two time slots.

The end-to-end ASR from the source S to the destination D with the help of relay Ri is given as

$$R_{SDE_i}^S = \max(R_{D_i} - R_{E_i}, 0) \quad (9)$$

Following the operation principle of the AFICPLS protocol, the best relay in the amplify-and-forward scheme is chosen based on the maximal end-to-end ASR

$$R^* = \arg\max_{i=1,2...M} R_{SDE_i}^S \quad (10)$$

where a superscript * denotes the best selected relay.

The outage probability of the AFICPLS protocol is defined as the probability that the maximal end-to-end ASR is less than the target data rate, and is given as

$$P_{AFICPLS}^{out} = \Pr\left[\max_{i=1,2...M} R_{SDE_i}^S < R_S\right]$$
$$= \Pr\left[R_{SDE_1}^S < R_S, R_{SDE_2}^S < R_S...., R_{SDE_M}^S < R_S\right] \quad (11)$$

where RS is the target data rate of the secondary network.

From (11), we note that the end-to-end ASRs $R_{SDE_i}^S$ are notin dependent of the others because of the common channel from the source S to the primary node P, (hsp in Fig. 1). In addition, the global instantaneous

channel state information (CSI) is available. In practice, the location and channel characteristic of the fixed link S-P is available so that the statistical CSI (average channel characteristic) of this link is given [7]. We denote that $m_{sp} = E[\omega_{sp}] = \lambda_{sp}^{-1}$ is the average channel S-P, and (11) is rewritten as

$$P_{AFICPLS}^{out} = \prod_{i=1}^{M} \Pr[R_{SDE_i}^S < R_S] = \prod_{i=1}^{M} \Pr[R_{D_i} < R_{E_i} + R_S]$$
$$= \prod_{i=1}^{M} \Pr\left[\frac{\omega_{1i}\omega_{2i}}{m_{sp}\omega_{2i} + \omega_{4i}\omega_{1i}} < \theta + \frac{\alpha\omega_{1i}\omega_{3i}}{m_{sp}\omega_{3i} + \omega_{4i}\omega_{1i}}\right] \quad (12)$$

where $\alpha = 2^{2R_S} > 1$, $\theta = (\alpha-1)/Q$. (17)

Solving (12) is very complex. Thus, in this protocol we consider M relays, which are located closely together and know the channel characteristics of the Ri-Plinks. We also denote that $m_{rp} = E[\omega_{4i}] = \lambda_{rp}^{-1}$, $i \in \{1,2,...,M\}$ is the average channel Ri-P, and (12) is rewritten as

$$P_{AFICPLS}^{out} = \prod_{i=1}^{M} \underbrace{\Pr\left[\frac{\omega_{1i}\omega_{2i}}{m_{sp}\omega_{2i} + m_{rp}\omega_{1i}} < \theta + \frac{\alpha\omega_{1i}\omega_{3i}}{m_{sp}\omega_{3i} + m_{rp}\omega_{1i}}\right]}_{P_i} \quad (13)$$

The probability Pi in (13) is also a complex function to derive an exact expression, but the lower and upper bounds can be solved in their closed forms, which can be used to evaluate the system performance. We have the results from [7] as

$$\frac{\min(m_{sp}\omega_{ai}, m_{rp}\omega_{1i})}{2m_{sp}m_{rp}} \leq \frac{\omega_{1i}\omega_{ai}}{m_{sp}\omega_{ai} + m_{rp}\omega_{1i}} \leq \frac{\min(m_{sp}\omega_{ai}, m_{rp}\omega_{1i})}{m_{sp}m_{rp}} \quad (14)$$

$$a \in \{2,3\}$$

Hence, from (14), where, the bounds of the probability Pi are given as

$$P_i \geq \Pr\left[\frac{\min(m_{sp}\omega_{2i}, m_{rp}\omega_{1i})}{m_{sp}m_{rp}} < \theta + \frac{\alpha\omega_{1i}\omega_{3i}}{m_{sp}\omega_{3i} + m_{rp}\omega_{1i}}\right]$$
$$\leq \underbrace{\Pr\left[\frac{\min(m_{sp}\omega_{2i}, m_{rp}\omega_{1i})}{m_{sp}m_{rp}} < \theta + \frac{\alpha\min(m_{sp}\omega_{3i}, m_{rp}\omega_{1i})}{2m_{sp}m_{rp}}\right]}_{P_i^{lower}}$$

$$\quad (15)$$

$$P_i \leq \Pr\left[\frac{\min(m_{sp}\omega_{2i}, m_{rp}\omega_{1i})}{2m_{sp}m_{rp}} < \theta + \frac{\alpha\omega_{1i}\omega_{3i}}{m_{sp}\omega_{3i} + m_{rp}\omega_{1i}} \right]$$

$$\leq \underbrace{\Pr\left[\frac{\min(m_{sp}\omega_{2i}, m_{rp}\omega_{1i})}{2m_{sp}m_{rp}} < \theta + \frac{\alpha\min(m_{sp}\omega_{3i}, m_{rp}\omega_{1i})}{m_{sp}m_{rp}} \right]}_{P_i^{upper}}$$

(16)

where the lower bound P_i^{lower} and upper bound P_i^{upper} are derived in Appendices A and B, respectively, as

When $\alpha \geq 2$:

$$P_i^{lower} = 1 - \frac{\lambda_3 e^{-\theta(m_{sp}\lambda_1 + m_{rp}\lambda_2)}}{\lambda_3 + \alpha\lambda_2/2 + \alpha m_{sp}\lambda_1/(2m_{rp})} \qquad (17)$$

When $\alpha < 2$:

$$P_i^{lower} = 1 - \frac{\left(m_{sp}\lambda_1 + m_{rp}\lambda_3\right)e^{-\theta m_{rp}\lambda_2 - \phi_1\left(\lambda_1 + \frac{\alpha m_{rp}}{2m_{sp}}\lambda_2 + \frac{m_{rp}}{m_{sp}}\lambda_3\right)}}{m_{sp}\lambda_1 + \alpha m_{rp}\lambda_2/2 + m_{rp}\lambda_3}$$

$$- \frac{\lambda_3 e^{-\theta m_{sp}\lambda_1 - \phi_2\left(\lambda_3 + \frac{\alpha m_{sp}}{2m_{rp}}\lambda_1\right)}}{\lambda_3 + \alpha m_{sp}\lambda_1/(2m_{rp})} + \frac{\lambda_3 e^{-\phi_2\left(\lambda_3 + \frac{m_{sp}}{m_{rp}}\lambda_1\right)}}{\lambda_3 + m_{sp}\lambda_1/m_{rp}}$$

$$- \frac{\lambda_3 e^{-\theta(m_{sp}\lambda_1 + m_{rp}\lambda_2)}\left(1 - e^{-\phi_2\left(\lambda_3 + \frac{\alpha}{2}\lambda_2 + \frac{\alpha m_{sp}}{2m_{rp}}\lambda_1\right)}\right)}{\lambda_3 + \alpha\lambda_2/2 + \alpha m_{sp}\lambda_1/(2m_{rp})}$$

(18)

$$P_i^{upper} = 1 - \frac{\lambda_3 e^{-2\theta\left(m_{sp}\lambda_1 + m_{rp}\lambda_2\right)}}{\lambda_3 + 2\alpha\lambda_2 + 2\alpha m_{sp}\lambda_1/m_{rp}} \qquad (19)$$

where $\phi_1 = m_{sp}\theta/(1 - \alpha/2)$, $\phi_2 = m_{rp}\theta/(1 - \alpha/2)$.

From (15), (16), and (12), the lower and upper bounds of $P_{AFICPLS}^{out}$ are given as

$$P_{AFICPLS}^{out-lower} = \left(P_i^{lower}\right)^M \qquad (20)$$

$$P_{AFICPLS}^{out-upper} = \left(P_i^{upper}\right)^M \qquad (21)$$

Next, in the case in which there are no relays located between S and D, we will consider the direct transmission (DT) protocol. In the DT protocol, there are four nodes: the source S, the destination D, the primary user P, and the eavesdropper E, where S wants to send the signal ps to D directly with the presence of the primary user P and the eavesdropper E in only one time slot. We denote that (h_{sd}, d_{sd}) and (h_{se}, d_{se}) are the Rayleigh fading channel coefficients and the link distances of S-D and S-E, respectively. Therefore, $\omega_{sd} = |h_{sd}|^2$ and $\omega_{se} = |h_{se}|^2$ are exponential random variables with the parameters $\lambda_{sd} = d_{sd}^\beta$ and $\lambda_{se} = d_{se}^\beta$, respectively.

The instantaneous signal to noise ratios (SNR) of links S-D and S-E are given as

$$\gamma_{sk} = \frac{P_s|h_{sk}|^2}{N_0} = \frac{I_P}{\omega_{sp}}\frac{\omega_{sk}}{N_0} = Q\frac{\omega_{sk}}{\omega_{sp}}, k \in \{d, e\} \qquad (22)$$

The achievable data rates of links S-D and S-E are given as

$$R_{sk} = \log_2(1 + \gamma_{sk}), k \in \{d, e\} \qquad (23)$$

The ASR is given [6] as

$$R_{DT}^S = \max(R_{sd} - R_{se}, 0) \qquad (24)$$

The outage probability of DT protocol is defined as the probability that ASR is less than the target data rate.

$$P_{DT}^{out} = \Pr\left[R_{DT}^S < R_S \right] = \Pr\left[R_{sd} < R_{se} + R_S \right]$$

$$= \Pr\left[\omega_{sd} < \theta_{DT}\omega_{sp} + a_{DT}\omega_{se} \right]$$

$$= \int_0^\infty \lambda_{sp}e^{-\lambda_{sp}x} \int_0^\infty \lambda_{se}e^{-\lambda_{se}y}\left[1 - e^{-\lambda_{sd}(\theta_{DT}x + a_{DT}y)} \right]dydx$$

$$= 1 - \frac{\lambda_{sp}\lambda_{se}}{\left(\lambda_{sp} + \theta_{DT}\lambda_{sd}\right)\left(\lambda_{se} + a_{DT}\lambda_{sd}\right)}$$

(25)

where $a_{DT} = 2^{R_S} > 1$, $\theta_{DT} = (a_{DT} - 1)/Q$.

IV. Simulation Results

This section discusses some simulation results from the previous sections. The theoretical results are drawn from the expressions derived in this paper, and the simulation results are based on Monte-Carlo experiments. In a two-dimensional plane, the secondary network includes nodes S, D, and E and relays Ri,

$i \in \{1, 2, ..., M\}$, with the coordinates (0, 0), (1,0), (xE, yE), and (0. 5, 0). These nodes transmit and receive signals under effecting of the primary user P (xP, yP). Hence, the distances of links S–Ri, Ri–D, and S–D are $d_{1i} = d_1 = 0.5$, $d_{2i} = d_2 = 0.5$, and $d_{sd} = 1$ during the simulation intervals. We assume that the path–loss exponent is constant ($\beta = 3$) and that the source–primary and relay–primary statistical channel characteristics are known beforehand.
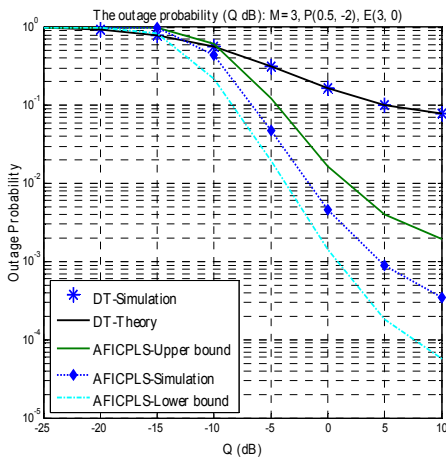

그림 2. Q에 따른 정전 확률
Fig. 2. Outage probability against Q(dB)

Fig. 2 presents the outage probability of the destination D of the AFICPLS and DT protocols against Q (dB) with the number of relays M=3, and the target data rate of the secondary network Rs=1 bit/s/Hz, the coordinates P(0.5, –3) and E(3, 0), (thus, dsp=2,dse=3,d3=2.5,d4=2). In Fig. 2, the outage probability of the AFICPLS protocol is less than that of the DT protocol at high Q regions (larger than –12 dB). This is because in the high Q regions, the interference at the primary node decreases, the transmit power of the source S and relays Ri will increase. Moreover, the signal received at the destination D will increase more than that of the eavesdropper E, so that ASR at the destination D will increase. This explains why the

performance of the AFICPLS protocol is better than the DT protocol when the interference constraints increase and $d_3 > d_2$. In addition, the expressions of the lower and upper bounds cover up the exact expression of the outage probability of the AFICPLS protocol (AFICPLS simulation).
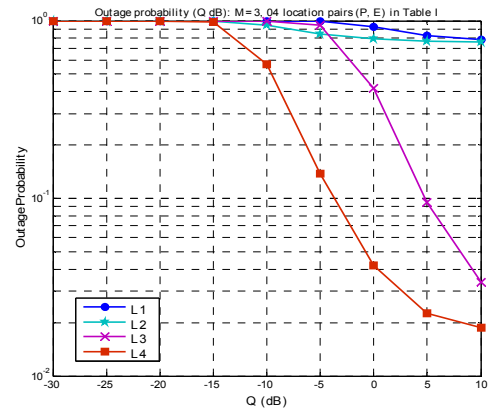

그림 3. Q에 따른 정전 확률과 표 1에 나타난 P, E 노드의 04 할당
Fig. 3. Outage probability against Q (dB) with 04 location pairs of nodes (P, E) as Table 1

표 1. P, E 노드의 할당
Table 1. Location pairs of nodes P and E

Notation	Coordinates P and E		Distances
L1	(0.25, –1)	(1, 0)	d_{sp}=1, d_{se}=1, d_3=0.5, d_4=1
L2	(0.25, –2)	(1, 0)	d_{sp}=2, d_{se}=1, d_3=0.5, d_4=2
L3	(0.25, –1)	(2, 0)	d_{sp}=1, d_{se}=2, d_3=1.5, d_4=1
L4	(0.25, –2)	(2, 0)	d_{sp}=2, d_{se}=2, d_3=1.5, d_4=2

Fig. 3 presents the outage probability against Q (dB) with 04 location pairs (P, E) in Table I when M=3 and Rs=1 (bit/s/Hz). In Fig. 3, the outage probability of the location pair L4 is best, while that of the location pair L1 is the worst. Hence, the system performance of the AFICPLS protocol will improve when both the primary node P and the eavesdropper node E are further from the secondary network. In addition, as seen in Fig. 3,

the AFICPLS protocol cannot be applied in communication systems when the eavesdropper node E is closer to the relays than the destination D ($d_3 \leq d_2$).
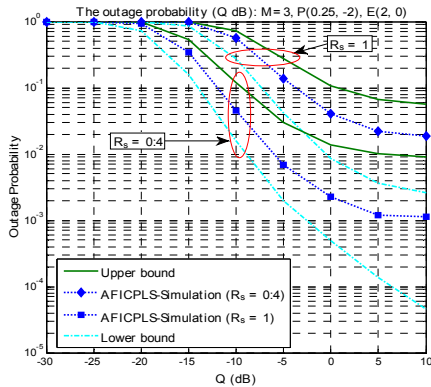

그림 4. R_s 가 0.4, 1(bit/s/Hz)로 고려되었을때의 Q에 따른 정전 확률
Fig. 4. Outage probability against Q (dB) when Rs is considered at 0.4 and 1 (bit/s/Hz)

Fig. 4 presents the outage probability against Q when M=3, P (0.25, -2), E (2, 0) (thus dsp=2,dse=2,d3=1.5,d4=2) and with different target data rates of the secondary network (Rs=0.4and Rs=1). In Fig. 4, when Rs increases, the outage probability increases, so the performance of the system decreases.

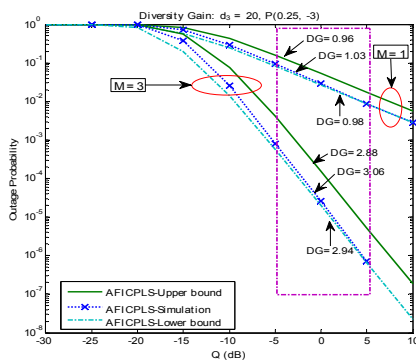그림 5. R_s = 1(bit/s/Hz), P (0.25, -3), d_{sp}=3, d_4=3,d_3=20, M =1, 3 일 때, 다이버시티 이득
Fig. 5. Diversity gain when R_s=1(bit/s/Hz), P (0.25, -3), d_{sp}=3,d_4=3,d_3=20 and M =1, 3.

Fig. 5 presents the diversity gain based on the outage probabilities against (dB) when the distances from the relays Ri to the eavesdropper E (d3) move towards infinity (d3=20). In Fig. 7, the diversity gains are calculated in the rectangular region from Q= -5 dB to 5 dB of the outage probability and achieve almost full diversity corresponding to the numbers of relays M=1 and M=3. The diversity gain values of the upper bound, simulation, and lower bound of the AFICPLS protocol are very close. Hence, the secondary network achieves full diversity when the distances from the relays to the eavesdropper E (d3) move towards infinity. In addition, when the number of relays M increase, the outage probability of the AFICPLS protocol decreases; and the exact outage probability (simulated result) closely matches with the lower bound of the AFICPLS protocol in high Q regions.

V. Conclusion

In this paper, the performance of the Amplify-and-Forward Scheme under an interference constraint and Physical Layer Security is analyzed and evaluated by the lower and upper bounds of the outage probability of ASR. The best relay is selected based on the opportunistic relay selection method in which the end-to-end ASR is maximized. Based on the simulation results, the performance of the proposed protocol outperforms the direct transmission protocol, and will improve when both the primary user and the eavesdropper node are further from the source node and the relays. The simulation results also show that lower and upper expressions cover the exact expressions of the AFICPLS protocol, and the secondary network achieves full diversity gain when the distances from the relays to the eavesdropper node move toward infinity.

Appendix

A: Solving the lower bound P_i^{lower} in (15)

The lower bound P_i^{lower} is expanded in(A.1) by detecting min formulas.

$$P_i^{lower} = \Pr\left[m_{sp}\omega_{2i} < m_{rp}\omega_{1i}, m_{sp}\omega_{3i} < m_{rp}\omega_{1i}, \frac{\omega_{2i}}{m_{rp}} < \theta + \frac{\alpha\omega_{3i}}{2m_{rp}} \right]$$

$$+\Pr\left[m_{sp}\omega_{2i} \geq m_{rp}\omega_{1i}, m_{sp}\omega_{3i} < m_{rp}\omega_{1i}, \frac{\omega_{1i}}{m_{sp}} < \theta + \frac{\alpha\omega_{3i}}{2m_{rp}} \right]$$

$$+\Pr\left[m_{sp}\omega_{2i} < m_{rp}\omega_{1i}, m_{sp}\omega_{3i} \geq m_{rp}\omega_{1i}, \frac{\omega_{2i}}{m_{rp}} < \theta + \frac{\alpha\omega_{1i}}{2m_{sp}} \right]$$

$$+\Pr\left[m_{sp}\omega_{2i} \geq m_{rp}\omega_{1i}, m_{sp}\omega_{3i} \geq m_{rp}\omega_{1i}, \frac{\omega_{1i}}{m_{sp}} < \theta + \frac{\alpha\omega_{1i}}{2m_{sp}} \right]$$

(A.1)

Next, we continue the expansions for each part of the sum in (A.1), then, after some straightforward manipulations, the lower bounds P_i^{lower} are obtained as

When $\alpha \geq 2$:

$$P_i^{lower} = 1 - \Pr\left[\omega_{1i} > m_{sp}\theta + \frac{\alpha m_{sp}}{2m_{rp}}\omega_{3i}, \omega_{2i} > m_{rp}\theta + \frac{\alpha}{2}\omega_{3i} \right]$$

$$= 1 - \int_0^\infty f_{\omega_{3i}}(x)\left\{ 1 - F_{\omega_{1i}}(m_{sp}\theta + \frac{\alpha m_{sp}x}{2m_{rp}}) \right\}\left\{ 1 - F_{\omega_{2i}}(m_{rp}\theta + \frac{\alpha x}{2}) \right\}dx$$

(A.2)

When $\alpha < 2$:

$$P_i^{lower} = \Pr\left[\omega_{1i} < m_{sp}\theta + \frac{\alpha m_{sp}}{2m_{rp}}\omega_{3i} \right]$$

$$-\Pr\left[\omega_{3i} > \frac{m_{rp}}{m_{sp}}\omega_{1i}, \omega_{1i} > \phi_1, \omega_{2i} > m_{rp}\theta + \frac{\alpha m_{rp}}{2m_{sp}}\omega_{1i} \right]$$

$$+\Pr\left[\omega_{2i} < m_{rp}\theta + \frac{\alpha}{2}\omega_{3i}, \omega_{1i} > m_{sp}\theta + \frac{\alpha m_{sp}}{2m_{rp}}\omega_{3i}, \omega_{3i} < \phi_2 \right]$$

$$+\Pr\left[\omega_{2i} < m_{rp}\theta + \frac{\alpha}{2}\omega_{3i}, \omega_{1i} > \frac{m_{sp}}{2m_{rp}}\omega_{3i}, \omega_{3i} > \phi_2 \right] =$$

$$= \int_0^\infty f_{\omega_{3i}}(x)F_{\omega_{1i}}(m_{sp}\theta + \frac{\alpha m_{sp}x}{2m_{rp}})dx$$

$$-\int_{\phi_1}^\infty f_{\omega_{1i}}(x)\left\{ 1 - F_{\omega_{2i}}(m_{rp}\theta + \frac{\alpha m_{rp}x}{2m_{sp}}) \right\}\left\{ 1 - F_{\omega_{3i}}(\frac{m_{rp}x}{m_{sp}}) \right\}dx$$

$$+\int_0^{\phi_2} f_{\omega_{3i}}(x)\left\{ 1 - F_{\omega_{1i}}(m_{sp}\theta + \frac{\alpha m_{sp}x}{2m_{rp}}) \right\}F_{\omega_{2i}}(m_{rp}\theta + \frac{\alpha x}{2})dx$$

$$+\int_{\phi_2}^\infty f_{\omega_{3i}}(x)\left\{ 1 - F_{\omega_{1i}}(\frac{m_{sp}x}{2m_{rp}}) \right\}F_{\omega_{2i}}(m_{rp}\theta + \frac{\alpha x}{2})$$

(A.3)

The result of (A.2) and (A.3) is solved as in (17) and (18), where $f_{\omega_{ai}}(x) = \lambda_a e^{-\lambda_a x}, a \in \{1,3\}$ are the probability density functions (PDFs) of ω_{1a} ;and $F_{\omega_{bi}}(x) = 1 - e^{-\lambda_b x}, \ b \in \{1,2,3\}$ are the cumulative distribution functions (CDFs) of ω_{1b} ; and $\phi_1 = m_{sp}\theta/(1-\alpha/2)$, $\phi_2 = m_{rp}\theta/(1-\alpha/2)$.

B: Solving the upper bound P_i^{upper} in(16)

The upper bound P_i^{upper} is expanded as

$$P_i^{upper} = \Pr\left[m_{sp}\omega_{2i} < m_{rp}\omega_{1i}, m_{sp}\omega_{3i} < m_{rp}\omega_{1i}, \frac{\omega_{2i}}{2m_{rp}} < \theta + \frac{\alpha\omega_{3i}}{m_{rp}} \right]$$

$$+\Pr\left[m_{sp}\omega_{2i} \geq m_{rp}\omega_{1i}, m_{sp}\omega_{3i} < m_{rp}\omega_{1i}, \frac{\omega_{1i}}{2m_{sp}} < \theta + \frac{\alpha\omega_{3i}}{m_{rp}} \right]$$

$$+\Pr\left[m_{sp}\omega_{2i} < m_{rp}\omega_{1i}, m_{sp}\omega_{3i} \geq m_{rp}\omega_{1i}, \frac{\omega_{2i}}{2m_{rp}} < \theta + \frac{\alpha\omega_{1i}}{m_{sp}} \right]$$

$$+\Pr\left[m_{sp}\omega_{2i} \geq m_{rp}\omega_{1i}, m_{sp}\omega_{3i} \geq m_{rp}\omega_{1i}, \frac{\omega_{1i}}{2m_{sp}} < \theta + \frac{\alpha\omega_{1i}}{m_{sp}} \right]$$

(B.1)

We perform some straightforward manipulations so that finally, P_i^{upper} is obtained and calculated as

$$P_i^{upper} = 1 - \Pr\left[\omega_{1i} > 2\theta m_{sp} + \frac{2\alpha m_{sp}\omega_{3i}}{m_{rp}}, \omega_{2i} > 2\theta m_{rp} + 2\alpha\omega_{3i} \right]$$

$$= 1 - \frac{\lambda_3 e^{-2\theta\left(m_{sp}\lambda_1 + m_{rp}\lambda_2\right)}}{\lambda_3 + 2\alpha\lambda_2 + 2\alpha m_{sp}\lambda_1/m_{rp}}$$

(B.2)

References

[1] Sang-Young Park; Hyung-Yun Kong, "Multihop Transmission in Cognitive Underlay Network Over Rayleigh Fading Channels", Journal of the Institute of Webcasting, Internet and Telecommunication (IWIT), vol.12, no.6, pp. 291-296, Dec. 2012.

[2] Hussain, S.I.; Abdallah, M.M.; Alouini, M.-S.; Hasna, M.; Qaraqe, K., "Performance Analysis of Selective Cooperation in Underlay Cognitive Networks over Rayleigh Channels", IEEE 12th International Workshop on Signal Processing Advances in Wireless Communications, p.116-120, 2011.

[3] Nam-Soo Kim, "Performance of DOT Relay System with MRC/GSC receiver in Rayleigh Fading Channels", Journal of the Institute of Webcasting, Internet and Telecommunication(IWIT), vol. 12, no. 5, pp. 11-16, Oct. 2012.

[4] Nam-Soo Kim, "Incremental Best Relay Selection System with Outdate CSI in Rayleigh Fading Channels", Journal of the Institute of Webcasting, Internet and Telecommunication(IWIT), vol. 12, no. 5, pp. 17-23, Oct. 2012.

[5] Minghua Xia; Aissa, S., "Cooperative AF Relaying in Spectrum-Sharing Systems: Outage Probability Analysis under Co-Channel Interferences and Relay Selection", IEEE Transactions on Wireless Communications, vol. 60, no. 11, pp. 3252-3262, 2012.

[6] Lun Dong; Zhu Han; Petropulu, A.P.; Poor, H.V., "Improving Wireless Physical Layer Security via Cooperating Relays", IEEE Transactions on Signal Processing, vol 58, no. 3, pp.1875-1888, 2010.

[7] Xiaojun Sun; Wei Xu; Ming Jiang; Chunming Zhao, "Opportunistic Selection for Decode-and-Forward Cooperative Networks with Secure Probabilistic Constraints", Wireless Personal Communications, vol. 70, no. 4, pp. 1633-1652, June 2013.

저자 소개

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 : LG 전자 회장실 전략 사업단
- 1998년~현재 : 울산대학교 전기전자정보시스템공학부 교수
<주관심분야> 모듈레이션, 채널 부호화, 검파 및 추정 기술, 협력통신, 센서네트워크

Pham Ngoc Son(학생회원)

- 2005년 2월 : Ho Chi Minh City University of Technology 학사
- 2009년 2월 : Ho Chi Minh City University of Technology 석사
- 2012년 3월 ~ 현재 : 울산대학교 전기공학부 박사 과정

<주관심분야> 협력통신, 인지기술, 물리 계층 보안, 결합 기술, 무선 센서 네트워크