Journal of Korea Multimedia Society Vol. 18, No. 4, April 2015(pp. 533-540)
http://dx.doi.org/10.9717/kmms.2015.18.4.533

도청자가 존재하는 무선 협력 네트워크의 전달 단말 선택을 통한 보안 전송률 최대 전송기술 및 성능분석

주민철[†], 권대길[††], 조진웅[†††]

Maximizing Secrecy Rate and Performance Analysis of Relay Selection for Cooperative Diversity Networks in Presence of an Eavesdropper

MinChul Ju[†], Tai-Gil Kwon[††], Jin-Woong Cho[†††]

ABSTRACT

We study relay selection in decode-and-forward (DF)-based relay networks consisting of a source, a destination, an eavesdropper, and multiple relays, where each terminal has a single antenna and operates in a half-duplex mode. In these networks, it is desirable to protect the confidential message from the source to the destination against the eavesdropper with the help of a single selected relay. Specifically, we begin by investigating DF-based networks for the scenario instantaneous signal-to-noise ratios (SNRs) related to the eavesdropper are available. For the scenario, we propose relay selection to maximize the secrecy rate of DF-based networks with and without direct-paths, and we derive the exact secrecy outage probabilities in closed-form.

Key words: Decode-and-forward (DF)-based Relay Network, Eavesdropper, Relay Selection, Secrecy Outage Probability

1. 서 론

군용/민간용 통신에서의 보안에 대한 강화가 요구되면서 정보보안에 대한 관심이 급증하고 있다[1]. 이를 위해 수학적 복잡성과 비가역성을 기반으로 하는 상위계층에서의 보안 알고리즘을 이용하는 방법들에 대한 연구가 많이 진행되었는데, 최근들어 물리계층에서의 보안 역시 많이 요구되고 있어 연구가 활발히 진행되고 있다. 구체적으로는 도청자를 가정하는 도청 채널(wiretap channel)에 대한 연구로 이어졌다[2-4]. 다른 한편으로, 전달 단말을 이용한 무선 협력(cooperative diversity networks)에 대한 연구가 활발한데, 이는 전파수신영역을 확장하고 채널의 결함을 보완해주는 역할을 한다[5-6]. 무선 협력 통신에서는 두 가지 방식이 많이 사용되는데, 그 중 복조후전송(decode-and-forward)은 소스 단말로부터 수신된 신호를 전달 단말이 먼저 복조한 후 다시 재부호화해서 전송하는데, 네트워크의 프로토콜과 채널 코딩등과 같이 사용될 수 있어서 많은 연구가 진행되고 있다.

최근들어 정보보안이 무선 협력 네트워크에서 많이 연구됨에 따라 물리계층 보안이 무선 협력 네트워

※ Corresponding Author : Tai-Gil Kwon, Address: (121-835) World cup buk-ro 54-gil, Mapo-gu, Seoul, Korea, TEL : +82-2-6388-6667, FAX : +82-2-6388-6707, E-mail : tgkwon@keti.re.kr
Receipt date : Jan. 20, 2015, Revision date : Feb 14, 2015
Approval date : Feb. 27, 2015
[†] School of Electrical Engineering, Kookmin University, Seoul, Korea (E-mail : mcju@kookmin.ac.kr)
[††] Realistic Media Platform Research Center, KETI, Korea
[†††] Realistic Media Platform Research Center, KETI, Korea (E-mail : chojw@keti.re.kr)
※ This work was supported by the Power Generation & Electricity Delivery of the Korea Institute of Energy Technology Evaluation and Planning(KETEP) grant funded by the Korea government Ministry of Trade, Industry & Energy. [No. 20131010501720]

크 측면에서 연구되어 지고 있다. 특히 물리계층 보안 이슈 중에서 무선 협력 네트워크의 외부에 도청자(external eavesdropper)가 존재하는 경우에 대한 연구가 활발히 진행되고 있다. 구체적으로 살펴보면, 기존의 직접 통신(direct communications) 방식에서 많이 연구되었던 도청 채널을 전달 단말들이 존재하는 무선 협력 네트워크로 확장하는 연구가 진행되고 있는데, Barros와 Rodrigues는 처음으로 외부의 도청자가 존재하는 무선 협력 네트워크의 도청 채널을 연구하였으며 [7], Han과 Sun은 무선 협력 네트워크의 도청 채널에서의 여러 보안 사항에 주목하였다 [8]. Krikidis는 직접경로가 없는 무선 협력 네트워크의 보안 아웃티지 확률(secrecy outage probability)의 근사값을 구하였다[9]. 하지만 아직까지 보안 전송률을 최대화하는 전달 단말 선택에 대한 논의가 없어, 본 연구에서 이를 보완할 연구를 하고자 한다.

본 논문에서는 하나의 소스 단말과 다수의 전달 단말들과 하나의 목적지 단말과 하나의 도청 단말로 이루어진 무선 협력 네트워크에서 복조후전송 방식의 보안 전송률을 최대화 하는 전달 단말 선택에 대해 연구한다. 이때 각각의 단말들은 하나의 안테나를 가지고, 반이중방식(half-duplex)으로 동작한다. 구체적으로 하나의 시나리오 목적 단말과 도청 단말에 관계한 모든 채널의 신호대잡음비(signal-to-noise ratio: SNR)의 즉시(instantaneous) 값을 알고 있을 때에 대하여 각각의 보안 전송률을 최대화하는 방법을 제안하고, 고려된 시나리오에 대하여 정확한 보안 아웃티지 확률을 구한다.

본 논문의 구성은 다음과 같다. 2장에서 하나의 도청 단말이 존재하는 복조후전송 방식의 무선 협력 네트워크에 대하여 서술한 다음, 3장에서 보안 전송률을 최대화 하는 전달 단말 선택에 대해 제안하고, 제안하는 방법의 보안 아웃티지 확률을 구한다. 그리고 4장에서는 제안한 방식으로 실험한 결과를 모의실험 결과와 비교하여 성능을 평가하고 5장에서 결론을 맺는다.

2. 연구 배경 및 제시된 시스템 모델

2.1 연구배경

통신 시스템의 채널 용량을 획기적으로 늘일 수 있는 다중 안테나(multiple-input-multiple- output: MIMO)를 사용하는 무선통신이 많은 관심을 끌어 연구가 진행되었다. 이러한 다중 안테나를 유동성이 높은 모바일 사용기기에 적용하기 힘든데 이는 기기의 크기가 너무 작아서 다중 안테나를 설치하기가 매우 어렵기 때문이다. 이러한 문제를 해결하기 위해 최근 무선 협력 네트워크가 많은 연구자들의 관심을 끌어 연구되고 있는데, 이는 모바일 기기들의 신호를 재전송함으로써 안테나를 가상적으로 묶어서 다중 안테나의 효과를 얻을 수 있기 때문이다. 특히 다수의 전달 단말이 존재하는 경우, 전달 단말을 효율적을 사용하는 많은 방법들이 제안되었는데, 분산화된 다중 안테나(distributed MIMO)와 분산화된 시공간 블록 코드(distributed space-time block codes: distributed STBCs), 그리고 전달 단말 선택 기법이 있다. 이 중에서 분산화된 다중 안테나와 분산화된 시공간 블록 코드는 수신단에서의 수신 신호가 시간과 주파수가 정확히 일치되어야 성능 향상을 꾀할 수 있으나, 각각의 발진 소자를 개별적으로 가지고 있는 무선 협력 네트워크에서는 이를 정확히 일치하기 매우 어렵기 때문에 연구가 많이 진행되지는 않았다. 그래서 많은 연구자들이 전달 단말 선택 방법을 통한 시스템 성능향상에 많은 연구를 진행해왔는데, 이 방법에서는 전달 단말 중에서 채널 상태가 좋은 전달 단말을 선택해 소스 단말로부터 전송된 신호를 재전송하는 방식이다. 이러한 방식을 이용할 경우 전달 단말의 개수가 늘어날수록 그 성능이 획기적으로 늘어난다는 것이 매우 잘 알려진 사실이다[10].

이러한 무선 협력 네트워크에서는 각 기기들이 기본적으로 신호를 재전송하므로 도청이나 정보변조 등의 정보보안에 매우 취약하다는 단점이 존재한다. 이러한 정보보안 강화를 위한 물리계층 보안이 최근

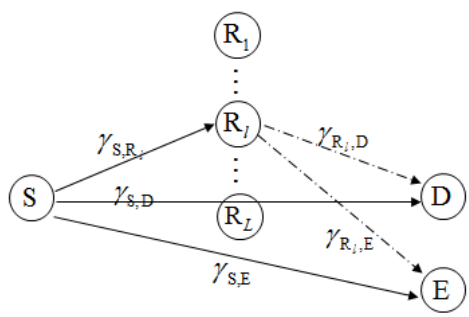


Fig. 1. System model for a relay network in the presence of an eavesdropper.

들어 무선 협력 네트워크 측면에서 연구되어 지고 있다. 구체적으로는 기존의 직접 통신방식에서 많이 연구되었던 도청 단말이 존재할 때의 도청 채널을 확장하여, 전달 단말들이 존재하는 무선 협력 네트워크에서의 도청 채널에 대한 연구가 진행되고 있다. 하지만 아직까지 다수의 단말이 존재하는 무선 협력 네트워크에서의 보안 전송률을 최대화하는 전달 단말 선택에 대한 논의가 없고 이에 대한 수학적 성능 분석이 없어, 본 연구에서 이를 보완할 연구를 하고자 한다.

2.2 시스템 기술

시스템은 하나의 소스 단말(S)과 다수의 전달 단말($\mathrm{R}_l : l=1,\cdots,L$)들, 하나의 목적지 단말(D)과 도청 단말(E)로 이루어지는데, 각각의 단말은 하나의 안테나를 가지고 반이중방식을 사용하고 에러 체크 코드는 사용하지 않는다. 소스 단말로부터 전송되는 심볼 s는 단위 전송전력을 가진다. $h_{\mathrm{S,D}}$는 소스 단말과 목적지 단말 사이의 채널 상수이고, $h_{\mathrm{S,E}}$는 소스 단말과 도청 단말 사이의 채널 상수이고, $h_{\mathrm{S,R}_l}$는 소스 단말과 전달 단말 사이의 채널 상수이며, $h_{\mathrm{R}_l\mathrm{D}}$는 l번째 전달 단말과 목적지 단말 사이의 채널 상수이고, $h_{\mathrm{R}_l\mathrm{E}}$는 l번째 전달 단말과 도청 단말 사이의 채널상수이다. 각각의 채널 상수는 독립적(independent)하고, 두 타임 슬롯동안 고정되어 있다고 가정한다. 그리고, $h_{\mathrm{S,D}} \sim CN(0,\Omega_{\mathrm{S,D}}), h_{\mathrm{S,E}} \sim CN(0,\Omega_{\mathrm{S,E}}), h_{\mathrm{S,R}_l} \sim CN(0,\Omega_{\mathrm{S,R}_l})$, $h_{\mathrm{R}_l\mathrm{D}} \sim CN(0,\Omega_{\mathrm{R}_l\mathrm{D}})$, $h_{\mathrm{R}_l\mathrm{E}} \sim CN(0,\Omega_{\mathrm{R}_l\mathrm{E}})$이며, 이때 $h \sim CN(m,\sigma^2)$는 평균값 m와 분산 σ^2을 가지는 가우시안(Gaussian) 확률변수 h를 나타낸다. 목적 단말에서는 소스 단말로부터 전송된 신호를 두 가지 다른 경로(직접경로와 전달경로)를 통해서 받게 된다.

첫 번째 타임 슬롯에 목적지 단말과 도청 단말이 직접 경로를 통해서 수신하는 신호 $r_{\mathrm{D},1}$과 $r_{\mathrm{E},1}$은 다음과 같이 주어진다.

$$r_{\mathrm{D},1} = \sqrt{E_{\mathrm{S}}}h_{\mathrm{S,D}}s + v_1, \quad r_{\mathrm{E},1} = \sqrt{E_{\mathrm{S}}}h_{\mathrm{S,E}}s + u_1 \tag{1}$$

이때 E_{S}은 소스 단말의 전송전력이고 v_1과 u_1는 가산성 잡음으로 평균값 0과 분산 1인 복소 가우시안 확률 변수이므로, $v_1 \sim CN(0,1)$과 $u_1 \sim CN(0,1)$이다. 전달경로의 경우, l번째 전달 단말에서 수신하는 신호 $r_{\mathrm{R},l}$은 다음과 같이 주어진다.

$$r_{\mathrm{R},l} = \sqrt{E_{\mathrm{S}}}h_{\mathrm{S,R}_l}s + w_l \tag{2}$$

이때 w_l는 가산성 잡음으로 평균값 0과 분산 1인 복소 가우시안 확률 변수이므로, $w_l \sim CN(0,1)$이다.

복조후전송 방식을 사용하므로, l번째 전달 단말에서 복조후 다시 재부호화한 심볼 $\hat{s}$을 전송한다. 그러면 두 번째 타임 슬롯에 목적지 단말과 도청 단말이 비직접 경로를 통해서 수신하는 신호 $r_{\mathrm{D},2}$와 $r_{\mathrm{E},2}$은 다음과 같이 주어진다.

$$r_{\mathrm{D},2} = \sqrt{E_{\mathrm{R}}}h_{\mathrm{R}_l\mathrm{D}}\hat{s} + v_2, \quad r_{\mathrm{E},2} = \sqrt{E_{\mathrm{R}}}h_{\mathrm{R}_l\mathrm{E}}\hat{s} + u_2 \tag{3}$$

이때 E_{R}은 전달 단말의 전송전력이고 v_2와 u_2는 가산성 잡음으로 평균값 0과 분산 1인 복소 가우시안 확률 변수이므로, $v_2 \sim CN(0,1)$과 $u_2 \sim CN(0,1)$이다.

소스 단말로부터 목적지 단말 사이의 채널의 즉시 신호대잡음비와 평균 신호대잡음비를 $\gamma_{\mathrm{S,D}}$와 $\bar{\gamma}_{\mathrm{S,D}}$로, 소스 단말로부터 도청 단말 사이의 채널의 즉시 신호대잡음비와 평균 신호대잡음비를 $\gamma_{\mathrm{S,E}}$와 $\bar{\gamma}_{\mathrm{S,E}}$로, 소스 단말로부터 l번째 전달 단말 사이의 채널의 즉시 신호대잡음비와 평균 신호대잡음비를 $\gamma_{\mathrm{S,R}_l}$와 $\bar{\gamma}_{\mathrm{S,R}_l}$로, l번째 전달 단말로부터 목적지 단말 사이의 채널의 즉시 신호대잡음비와 평균 신호대잡음비를 $\gamma_{\mathrm{R}_l\mathrm{D}}$와 $\bar{\gamma}_{\mathrm{R}_l\mathrm{D}}$로, l번째 전달 단말로부터 도청 단말 사이의 채널의 즉시 신호대잡음비와 평균 신호대잡음비를 $\gamma_{\mathrm{R}_l\mathrm{E}}$와 $\bar{\gamma}_{\mathrm{R}_l\mathrm{E}}$로 두면 각각은 다음과 같이 주어진다.

$\gamma_{\mathrm{S,D}} = E_{\mathrm{S}}|h_{\mathrm{S,D}}|^2$, $\gamma_{\mathrm{S,E}} = E_{\mathrm{S}}|h_{\mathrm{S,E}}|^2$, $\gamma_{\mathrm{S,R}_l} = E_{\mathrm{S}}|h_{\mathrm{S,R}_l}|^2$,
$\gamma_{\mathrm{R}_l\mathrm{D}} = E_{\mathrm{R}}|h_{\mathrm{R}_l\mathrm{D}}|^2$, $\gamma_{\mathrm{R}_l\mathrm{E}} = E_{\mathrm{R}}|h_{\mathrm{R}_l\mathrm{E}}|^2$ 이고, $\bar{\gamma}_{\mathrm{S,D}} = E_{\mathrm{S}}\Omega_{\mathrm{S,D}}$,
$\bar{\gamma}_{\mathrm{S,E}} = E_{\mathrm{S}}\Omega_{\mathrm{S,E}}$ $\bar{\gamma}_{\mathrm{S,R}_l} = E_{\mathrm{S}}\Omega_{\mathrm{S,R}_l}$, $\bar{\gamma}_{\mathrm{R}_l\mathrm{D}} = E_{\mathrm{R}}\Omega_{\mathrm{R}_l\mathrm{D}}$,
$\bar{\gamma}_{\mathrm{R}_l\mathrm{E}} = E_{\mathrm{R}}\Omega_{\mathrm{R}_l\mathrm{E}}$이다.

2.3 보안 전송률

목적지 단말은 첫 번째 타임 슬롯동안 받은 신호인 식 (1)의 $r_{\mathrm{D},1}$과 두 번째 타임 슬롯동안 받은 신호인 식 (3)의 $r_{\mathrm{D},2}$를 종합하여 소스 단말과 목적지 단말 사이 채널의 상호 정보량(mutual information) $I_{\mathrm{S,D},l}$을 구하는데, $I_{\mathrm{S,D},l}$은 다음과 같이 주어진다.

$$I_{\mathrm{S,D},l} = \begin{cases} \frac{1}{2}\log_2(1+\gamma_{\mathrm{S,D}}), & I([\mathrm{S,R}_l]) < R \\ \frac{1}{2}\log_2(1+\gamma_{\mathrm{S,D}}+\gamma_{\mathrm{R}_l\mathrm{D}}), & I([\mathrm{S,R}_l]) \geq R \end{cases} \tag{4}$$

이때 $I([\mathrm{S},\mathrm{R}_l])$은 소스 단말로부터 l번째 전달 단말 사이 채널의 상호정보량이며, R(bps/Hz)은 최종 요구되는 전송률을 나타낸다. 식 (4)에서 로그 전 상수가 1/2인 것은 소스 단말로부터 목적지 단말로 총 두 타임 슬롯이 필요하기 때문이다. 식 (4)와 비슷하게 소스 단말과 도청 단말 사이 채널의 상호정보량 $I_{\mathrm{S,E},l}$을 구하는데, $I_{\mathrm{S,E},l}$은 다음과 같이 주어진다.

$$I_{\mathrm{S,E},l}=\begin{cases}\frac{1}{2}\log_2(1+\gamma_{\mathrm{S,E}}), & I([\mathrm{S},\mathrm{R}_l])<R\\ \frac{1}{2}\log_2(1+\gamma_{\mathrm{S,E}}+\gamma_{\mathrm{R}_l\mathrm{E}}), & I([\mathrm{S},\mathrm{R}_l])\geq R\end{cases} \tag{5}$$

이러한 네트워크에서의 l번째 전달 단말을 거쳐서 통신이 이루어질 때의 보안 전송률은 다음과 같이 주어진다.

$$S_l=[I_{\mathrm{S,D},l}-I_{\mathrm{S,E},l}]^+ \tag{6}$$

이때 $[x]^+=\max[0,x]$를 나타낸다. 식 (4)와 식 (5)를 식 (6)에 대입하면 다음과 같이 주어진다.

$$S_l=\begin{cases}\frac{1}{2}\log_2\left(\frac{1+\gamma_{\mathrm{S,D}}}{1+\gamma_{\mathrm{S,E}}}\right), & I([\mathrm{S},\mathrm{R}_l])<R\\ \frac{1}{2}\log_2\left(\frac{1+\gamma_{\mathrm{S,D}}+\gamma_{\mathrm{R}_l\mathrm{D}}}{1+\gamma_{\mathrm{S,E}}+\gamma_{\mathrm{R}_l\mathrm{E}}}\right), & I([\mathrm{S},\mathrm{R}_l])\geq R\end{cases} \tag{7}$$

3. 도청자가 존재하는 무선 협력 네트워크의 전달 단말 선택

이 장에서는 다수의 단말이 존재하는 무선 협력 네트워크에서의 보안 전송률을 최대화하는 전달 단말 선택 방법을 제시하고, 이에 대한 보안 아웃티지 확률에 대한 수학적 성능 분석을 한다.

3.1 전달 단말 선택 기법

도청 단말이 없는 무선 협력 네트워크에서의 전달 단말 선택 방법을 통한 시스템 성능향상에 많은 연구를 진행해왔는데, 이 방법에서는 전달 단말 중에서 채널 상태가 좋은 전달 단말을 선택해 소스 단말로부터 전송된 신호를 재전송하는 방식이다. 이러한 방식을 도청 단말이 있는 무선 협력 네트워크로 확장하려 식 (7)에서 구한 l번째 전달 단말을 거쳐서 통신이 이루어질 때의 보안 전송률을 다음과 같이 최대화할 수 있다.

$$l=\max_{l=1,\cdots,L}S_l \tag{8}$$

이용할 전달 단말 선택 방식은 전달 단말의 개수가 늘어날수록 그 성능이 획기적으로 늘어난다는 것이 매우 잘 알려진 사실이다. 식 (8)을 바탕으로 선택된 전달 단말은 두 타임 슬롯동안 소스 단말로부터 목적지 단말로의 정보전송을 돕는다. 그리고 위의 선택에 의해 얻을 수 있는 보안 아웃티지 확률 $P_{\mathrm{out}}(R)$은 다음과 같이 주어진다.

$$P_{\mathrm{out}}(R)=\Pr\left[\max_{l=1,\cdots,L}S_l<R\right] \tag{9}$$

제시된 보안 아웃티지 확률은, 선택된 전달 단말을 통해 소스 단말의 정보가 전송되었을 때 목적지 단말로 전달되는 정보량과 도청 단말로 새는 정보량의 차가 요구되어지는 전송률 R보다 작을 확률을 나타낸다. 윗 식에서 알 수 있듯이, 식 (8)을 바탕으로 선택된 전달 단말은 보안 전송률을 최대화 하면서 동시에 보안 아웃티지 확률을 최소화하는 역할을 한다. 식 (7)을 식 (9)에 대입하면, 보안 아웃티지 확률 $P_{\mathrm{out}}(R)$은 다음과 같이 전개된다.

$$\begin{aligned}P_{\mathrm{out}}(R)&=E_{\gamma_{\mathrm{S,D}},\gamma_{\mathrm{S,E}}}\left[\prod_{l=1}^{L}\left(\Pr\left[\frac{1}{2}\log_2\left(\frac{1+x}{1+y}\right)<R, I([\mathrm{S},\mathrm{R}_l])<R\middle|\gamma_{\mathrm{S,D}}=x,\gamma_{\mathrm{S,E}}=y\right]\right.\right.\\&\quad\left.\left.+\Pr\left[\frac{1}{2}\log_2\left(\frac{1+x+\gamma_{\mathrm{R}_l\mathrm{D}}}{1+y+\gamma_{\mathrm{R}_l\mathrm{E}}}\right)<R, I([\mathrm{S},\mathrm{R}_l])\geq R\middle|\gamma_{\mathrm{S,D}}=x,\gamma_{\mathrm{S,E}}=y\right]\right)\right]\\&=E_{\gamma_{\mathrm{S,D}},\gamma_{\mathrm{S,E}}}\left[\prod_{l=1}^{L}\Phi_l(x,y)\right]\end{aligned} \tag{10}$$

식 (10)에서 알 수 있듯이 보안 아웃티지 확률 $P_{\mathrm{out}}(R)$은 소스 단말로부터 l번째 전달 단말 사이 채널의 상호정보량 $I([\mathrm{S},\mathrm{R}_l])$이 요구되어지는 전송률 R보다 작을 경우에는 직접경로의 전송률이 연관되어 있으며, 상호정보량 $I([\mathrm{S},\mathrm{R}_l])$이 요구되어지는 전송률 R보다 클 경우에는 직접경로의 전송률과 l번째 전달 단말 경로의 전송률이 연관되어 있다. 이때 식 (10)의 $\Phi_l(x,y)$은 다음과 같이 전개된다.

$$\begin{aligned}\Phi_l(x,y)&=\Pr\left[\frac{1+x}{1+y}<T,\gamma_{\mathrm{S},\mathrm{R}_l}<T\right]+\Pr\left[\frac{1+x+\gamma_{\mathrm{R}_l\mathrm{D}}}{1+y+\gamma_{\mathrm{R}_l\mathrm{E}}}<T,\gamma_{\mathrm{S},\mathrm{R}_l}\geq T\right]\\&=\Pr\left[\frac{1+x}{1+y}<T\right]\Pr\left[\gamma_{\mathrm{S},\mathrm{R}_l}<T\right]+\Pr\left[\frac{1+x+\gamma_{\mathrm{R}_l\mathrm{D}}}{1+y+\gamma_{\mathrm{R}_l\mathrm{E}}}<T\right]\Pr\left[\gamma_{\mathrm{S},\mathrm{R}_l}\geq T\right]\end{aligned} \tag{11}$$

$\xi(x,y)=T(y+1)-(x+1)$라 두면, 다음을 얻을 수 있다.

$$\Phi_l(x,y)=\begin{cases}\Pr\left[\gamma_{\mathrm{S},\mathrm{R}_l}<T\right]+\Pr\left[\gamma_{\mathrm{S},\mathrm{R}_l}\geq T\right]\Pr\left[\gamma_{\mathrm{R}_l\mathrm{D}}<T\gamma_{\mathrm{R}_l\mathrm{E}}+\xi(x,y)\right], & \xi(x,y)>0\\ \Pr\left[\gamma_{\mathrm{S},\mathrm{R}_l}\geq T\right]\Pr\left[\gamma_{\mathrm{R}_l\mathrm{D}}<T\gamma_{\mathrm{R}_l\mathrm{E}}+\xi(x,y)\right], & \xi(x,y)\leq 0\end{cases} \tag{12}$$

위에서 제시된 $\xi(x,y)$에 따라서 전개되는 수식이 달라짐을 주지해야한다. 이때 $\gamma_{\mathrm{S,R}_l}$, $\gamma_{\mathrm{R}_k\mathrm{D}}$, $\gamma_{\mathrm{R}_k\mathrm{E}}$는 평균값 $\bar{\gamma}_{\mathrm{S,R}_l}$, $\bar{\gamma}_{\mathrm{R}_k\mathrm{D}}$, $\bar{\gamma}_{\mathrm{R}_k\mathrm{E}}$을 갖는 지수 함수의 확률 변수들이므로 각각의 확률밀도함수(probability density function: PDF)은 다음과 같이 주어진다. $f_{\gamma_{\mathrm{S,R}_l}}(x)=\frac{1}{\bar{\gamma}_{\mathrm{S,R}_l}}\exp\left(-\frac{x}{\bar{\gamma}_{\mathrm{S,R}_l}}\right)$과 $f_{\gamma_{\mathrm{R}_k\mathrm{D}}}(x)=\frac{1}{\bar{\gamma}_{\mathrm{R}_k\mathrm{D}}}\exp\left(-\frac{x}{\bar{\gamma}_{\mathrm{R}_k\mathrm{D}}}\right)$과 $f_{\gamma_{\mathrm{R}_k\mathrm{E}}}(x)=\frac{1}{\bar{\gamma}_{\mathrm{R}_k\mathrm{E}}}\exp\left(-\frac{x}{\bar{\gamma}_{\mathrm{R}_k\mathrm{E}}}\right)$이고, 이때 $f_X(\cdot)$는 확률 변수 X의 확률밀도함수이다. 그러므로 식 (12)의 $\Phi_l(x,y)$는 다음과 같이 주어진다.

이때 $A_1(l)=\bar{\gamma}_{\mathrm{R}_k\mathrm{D}}\exp(-T/\bar{\gamma}_{\mathrm{S,R}_l})/(\bar{\gamma}_{\mathrm{R}_k\mathrm{D}}+\bar{\gamma}_{\mathrm{R}_k\mathrm{E}}T)$, $A_2(l)=\bar{\gamma}_{\mathrm{R}_k\mathrm{E}}T\exp(-T/\bar{\gamma}_{\mathrm{S,R}_l})/(\bar{\gamma}_{\mathrm{R}_k\mathrm{D}}+\bar{\gamma}_{\mathrm{R}_k\mathrm{E}}T)$이다. 식 (13)에서 알 수 있듯이 $\xi(x,y)$에 따라서 $\Phi_l(x,y)$가 서로 다른 지수함수(exponential function)의 형태로 주어진다.

이때 $\prod_{l=1}^{L}(1-d(l))=1+\sum_{l=1}^{L}(-1)^l\sum_{\substack{m_{1=1},\cdots,m_l=1\\ m_1<\cdots<m_l}}^{L}\prod_{j=1}^{l}d(m_j)$

를 이용하면, 식 (13)에서의 항목 $\prod_{l=1}^{L}\left(1-A_1(l)\exp(-\xi(x,y)/\bar{\gamma}_{\mathrm{R}_k\mathrm{D}})\right)=1+\widehat{\sum}(-1)^l\prod_{j=1}^{l}A_1(m_j)\exp(-\xi(x,y)\sum_{j=1}^{l}1/\bar{\gamma}_{\mathrm{R}_{m_j},\mathrm{D}})$이며 $\widehat{\sum}=\sum_{l=1}^{L}\sum_{\substack{m_{1=1},\cdots,m_l=1\\ m_1<\cdots<m_l}}^{L}$ 임을 알 수 있다. 이를 종합하면, 식 (13)의 보안 아웃티지 확률 $P_{\mathrm{out}}(R)$은 다음과 같이 구할 수 있다.

식 (15)에서 구한 보안 아웃티지 확률은 적분이 필요 없는 닫힌 형태(closed form)로 주어졌기 때문에 매트랩이나 C언어를 이용하면 식에 맞게 파라미터들만 대입하면 요구되는 확률을 정확히 빨리 얻을 수 있다. 그리고 이렇게 구해진 확률로부터 소스 단말의 송신 전력이나 전달 단말의 송신 전력이나 위치 등의 변수를 결정하는데 사용될 수 있다.

$$\Phi_l(x,y)=\begin{cases}\int_0^T f_{\gamma_{\mathrm{S,R}_l}}(s)ds+\int_T^\infty f_{\gamma_{\mathrm{S,R}_l}}(s)ds\times\int_{z=0}^{\infty}\int_{t=0}^{Tz+\xi(x,y)} f_{\gamma_{\mathrm{R}_k\mathrm{D}}}(t)f_{\gamma_{\mathrm{R}_k\mathrm{E}}}(z)dtdz, & \xi(x,y)>0\\ \int_T^\infty f_{\gamma_{\mathrm{S,R}_l}}(s)ds\times\int_{z=-\xi(x,y)/T}^{\infty}\int_{t=0}^{Tz+\xi(x,y)} f_{\gamma_{\mathrm{R}_k\mathrm{D}}}(t)f_{\gamma_{\mathrm{R}_k\mathrm{E}}}(z)dtdz, & \xi(x,y)\le 0\end{cases} \tag{13}$$
$$=\begin{cases}1-A_1(l)\exp\left(\frac{\xi(x,y)}{\bar{\gamma}_{\mathrm{R}_k\mathrm{E}}}\right), & \xi(x,y)>0\\ A_2(l)\exp\left(\frac{\xi(x,y)}{\bar{\gamma}_{\mathrm{R}_k\mathrm{E}}T}\right), & \xi(x,y)\le 0\end{cases}$$

$$P_{\mathrm{out}}(R)=E_{\xi(x,y)\ge 0}\left[\prod_{l=1}^{L}\left(1-A_1(l)\exp\left(-\frac{\xi(x,y)}{\bar{\gamma}_{\mathrm{R}_k\mathrm{D}}}\right)\right)\right]+E_{\xi(x,y)<0}\left[\prod_{l=1}^{L}A_2(l)\exp\left(\frac{\xi(x,y)}{\bar{\gamma}_{\mathrm{R}_k\mathrm{E}}T}\right)\right] \tag{14}$$
$$=\int_{y=0}^{\infty}\int_{x=0}^{T(y+1)-1}\left(\prod_{l=1}^{L}\left(1-A_1(l)\exp\left(-\frac{\xi(x,y)}{\bar{\gamma}_{\mathrm{R}_l\mathrm{D}}}\right)\right)\right)f_{\gamma_{\mathrm{S,D}}}(x)f_{\gamma_{\mathrm{S,E}}}(y)dxdy$$
$$+\left(\prod_{l=1}^{L}A_2(l)\right)\int_{y=0}^{\infty}\int_{x=T(y+1)-1}^{\infty}\exp\left(\xi(x,y)\sum_{l=1}^{L}\frac{1}{\bar{\gamma}_{\mathrm{R}_k\mathrm{E}}}T\right)f_{\gamma_{\mathrm{S,D}}}(x)f_{\gamma_{\mathrm{S,E}}}(y)dxdy$$

$$P_{\mathrm{out}}(R)=1-\frac{\bar{\gamma}_{\mathrm{S,D}}\exp((1-T)/\bar{\gamma}_{\mathrm{S,D}})}{\bar{\gamma}_{\mathrm{S,D}}+\bar{\gamma}_{\mathrm{S,E}}T}\left(1-\frac{\prod_{l=1}^{L}A_2(l)}{1+\bar{\gamma}_{\mathrm{S,D}}\sum_{l=1}^{L}1/(\bar{\gamma}_{\mathrm{R}_k\mathrm{E}}T)}\right) \tag{15}$$
$$+\widehat{\sum}\frac{(-1)^l\prod_{j=1}^{l}A_1(m_j)}{1-\bar{\gamma}_{\mathrm{S,D}}\sum_{j=1}^{l}1/\bar{\gamma}_{\mathrm{R}_{m_j},\mathrm{D}}}\left(\frac{\exp((1-T)\sum_{j=1}^{l}1/\bar{\gamma}_{\mathrm{R}_{m_j},\mathrm{D}})}{1+\bar{\gamma}_{\mathrm{S,E}}T\sum_{j=1}^{l}1/\bar{\gamma}_{\mathrm{R}_{m_j},\mathrm{D}}}-\frac{\bar{\gamma}_{\mathrm{S,D}}\exp((1-T)/\bar{\gamma}_{\mathrm{S,D}})}{\bar{\gamma}_{\mathrm{S,D}}+\bar{\gamma}_{\mathrm{S,E}}T}\right)$$

$$P_{\mathrm{out}}(R)=\prod_{l=1}^{L}\left(\Pr\left[I([\mathrm{S},\mathrm{R}_l])<R\right]+\Pr\left[\frac{1}{2}\log_2\left(\frac{1+\gamma_{\mathrm{R}_l\mathrm{D}}}{1+\gamma_{\mathrm{R}_k\mathrm{E}}}\right)<R, I([\mathrm{S},\mathrm{R}_l])\ge R\right]\right) \tag{16}$$

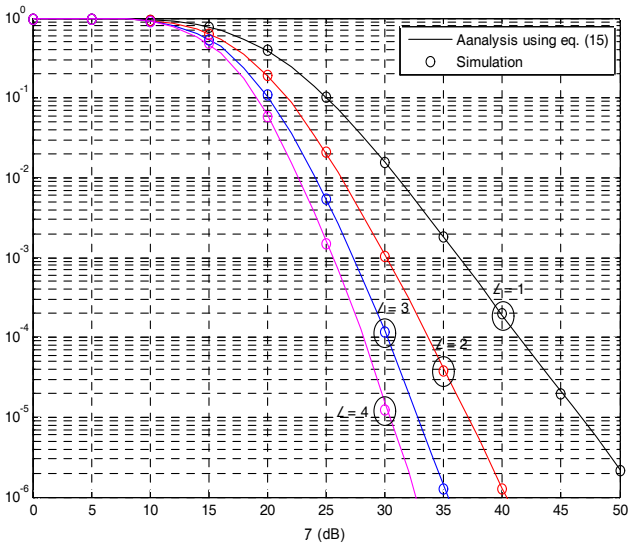


Fig. 2. Secrecy outage probability against $\bar{\gamma}$ of relay selection in DF-based networks with direct-paths. $L=1,2,3,4$, $R=1.5$ bps/Hz, $2\bar{\gamma}_{\mathrm{S,D}}=\bar{\gamma}_{\mathrm{S,R}_l}=\bar{\gamma}_{\mathrm{R}_b\mathrm{D}}=\bar{\gamma}$, $\bar{\gamma}_{\mathrm{S,E}}=5$ dB, $\bar{\gamma}_{\mathrm{R}_b\mathrm{E}}=10$ dB for $l=1,\cdots,L$.

지금까지는 소스 단말로부터 목적지 단말과 도청 단말로의 직접 경로가 있을 경우에 대하여 살펴보았는데, 직접 경로가 매우 멀거나 단말간에 물체가 있어서 신호가 전달되지 않을 경우는 식 (10)에서 $\gamma_{\mathrm{S,D}}=\gamma_{\mathrm{S,D}}=0$으로 두면 식 (16)과 같이 간략히 나타내어진다. 이를 식 (11)에서 식 (13)의 과정을 거치면 식 (14)의 보안 아웃티지 확률 $P_{\mathrm{out}}(R)$은 다음과 같이 간략히 나타내어진다.

$$P_{\mathrm{out}}(R)=\prod_{l=1}^{L}\left(1-\frac{\bar{\gamma}_{\mathrm{R}_b\mathrm{D}}}{\bar{\gamma}_{\mathrm{R}_b\mathrm{D}}+\bar{\gamma}_{\mathrm{R}_b\mathrm{E}}T}\exp\left(\frac{1-T}{\bar{\gamma}_{\mathrm{R}_b\mathrm{D}}}-\frac{T}{\bar{\gamma}_{\mathrm{S,R}_l}}\right)\right) \quad (17)$$

식 (17)은 소스 단말로부터 목적지 단말과 도청 단말로의 직접 경로가 없을 경우이므로 식 (15)에 비해서 훨신 간략화된 형태로 주어졌다.

4. 실험 결과 및 고찰

본 섹션에서는 도청자가 존재하는 무선 협력 네트워크의 전달 단말 선택을 통한 보안 전송률 최대 전송기술의 최종 보안 아웃티지 확률의 정확성을 알아보기 위해 모의실험 결과와 비교한다. 총 두 개의 그림을 제시하며, 첫 번째 그림은 직접경로가 있는 무선 협력 네트워크의 전달 단말 선택을 통한 성능이 향상되는 것을 보이며, 두 번째 그림을 통해서는 직접경로가 없는 무선 협력 네트워크의 전달 단말 선택을 통한 성능이 향상되는 것을 보인다.

Fig. 2는 평균 신호대잡음비 $\bar{\gamma}$에 대해서 도청자가 존재하는 직접경로가 있는 무선 협력 네트워크의 전달 단말 선택의 보안 아웃티지 확률을 보여주는데, 전달 단말의 개수는 $L=1,2,3,4$로 두고, 요구되는 보안 전송률은 $R=1.5$ bps/Hz로, 각 채널의 신호대잡음비는 $2\bar{\gamma}_{\mathrm{S,D}}=\bar{\gamma}_{\mathrm{S,R}_l}=\bar{\gamma}_{\mathrm{R}_b\mathrm{D}}=\bar{\gamma}$ 로, $\bar{\gamma}_{\mathrm{S,E}}=5$ dB로, $\bar{\gamma}_{\mathrm{R}_b\mathrm{E}}=10$ dB로 정하였으며, 이때 $l=1,\cdots,L$ 이다. Fig. 3은 평균 신호대잡음비 $\bar{\gamma}$에 대해서 도청자가 존재하는 직접경로가 없는 무선 협력 네트워크의 전달 단말 선택의 보안 아웃티지 확률을 보여주는데, 전달 단말의 개수는 $L=1,2,3,4$로 두고, 요구되는 보안 전송률은 $R=1$ bps/Hz로, $\bar{\gamma}_{\mathrm{S,R}_l}=\bar{\gamma}_{\mathrm{R}_b\mathrm{D}}=\bar{\gamma}$ 로, $\bar{\gamma}_{\mathrm{R}_b\mathrm{E}}=10$ dB로 정하였으며, 이때 $l=1,\cdots,L$ 이다.

Figs. 2와 3에서는 다음과 같은 사항을 알 수 있다. 먼저 직접경로가 있는 경우의 수식 (15)와 직접경로가 없는 경우의 수식 (17)에서 구해진 보안 아웃티지 확률들은 전달 단말의 개수와 상관없이 모의실험 결과와 정확히 일치함을 알 수 있다. 그리고 두 개의 그림에서 알 수 있듯이, 평균 신호대잡음비 $\bar{\gamma}$가 증가할수록 채널의 상태가 좋아지므로 보안 아웃티지 확률이 낮아지는 것을 알 수 있다. 마지막으로 전달 단말의 개수가 늘어날수록 보안 아웃티지 확률이 낮아지는 것을 알 수 있는데, 이는 여러 개의 전달 단말 중에서 선택된 전달단말 채널의 상태가 좋은 것이 나타날 확률이 늘어나기 때문이다.

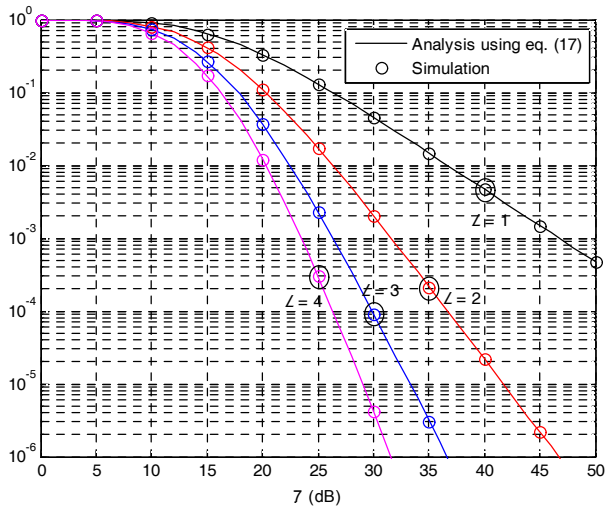


Fig. 3. Secrecy outage probability against $\bar{\gamma}$ of relay selection in DF-based networks without direct-paths. $L=1,2,3,4$, $R=1$ bps/Hz, $\bar{\gamma}_{S,R_l}=\bar{\gamma}_{R_l,D}=\bar{\gamma}$, $\bar{\gamma}_{R_l,E}=10$ dB for $l=1,\cdots,L$.

5. 결 론

본 논문에서는 도청자가 존재하는 무선 협력 네트워크의 전달 단말 선택을 통한 보안 전송률 최대 전송기술 및 성능을 분석하였다. 제안된 시스템에서의 보안 전송률을 최대로 하기 위해서 여러 전달 단말 중 하나를 선택하고, 그 선택된 전달 단말은 두 타임 슬롯동안 소스 단말로부터 목적지 단말로의 정보전송을 돕는다. 실험결과 분석된 보안 아웃티지 확률이 직접 경로의 유무와 관계없이 매우 정확하다는 것을 확인하였다. 이러한 성능 분석을 통하여 보안 무선 협력 네트워크에서의 전송 전력과 전달 단말의 개수와 위치 등을 결정할 수 있다.

REFERENCE

[1] C.E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, Vol. 28, No. 4, pp. 656-715, 1949.

[2] A.D. Wyner, "The Wire-Tap Channel," *Bell System Technical Journal*, Vol. 54, No. 8, pp. 1355-1387, 1975.

[3] I. Csiszar and J. Korner, "Broadcast Channels with Confidential Messages," *IEEE Transactions on Information Theory*, Vol. 24, No. 3, pp. 339-348, 1978.

[4] S.K. Leung-Yan-Cheong and M.E. Hellman, "The Gaussian Wire-Tap Channel," *IEEE Transactions on Information Theory*, Vol. 24, No. 4, pp. 451-456, 1978.

[5] A. Sendonaris, E. Erkip, and B. Aazhang, "User Cooperation Diversity, Parts I, II," *IEEE Transactions on Communications*, Vol. 51, No. 11, pp. 1927-1948, 2003.

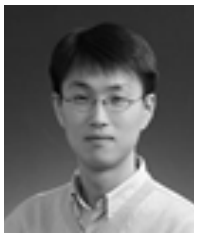
[6] J.N. Laneman, D.N.C. Tse, and G.W. Wornell, "Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior," *IEEE Transactions on Information Theory*, Vol. 50, No. 12, pp. 3062-3080, 2004.

[7] J. Barros and M.R.D. Rodrigues, "Secrecy Capacity of Wireless Channels," *Proeeding of IEEE International Information Theory Symposium*, pp. 356-360, 2006.

[8] Z. Han and Y.L. Sun, "Securing Cooperative Transmission in Wireless Communications," *Proceeding of MobiQuitous*, pp. 1-6, 2007.

[9] I. Krikidis, "Opportunistic Relay Selection for Cooperative Networks with Secrecy Constraints," *IET Communications*, Vol. 4, No. 15, pp. 1787-1791, 2010.

[10] Y.-I. Joo and K Hur, "Relay Cooperative Transmission Scheme for Distributed MAC Protocol-Based Logistic Applications," *Journal of Korea Multimedia Society*, Vol. 14, No. 3, pp. 423-432, 2011.



주 민 철

1997년 포항공과대학교 공학사
1999년 한국과학기술원 공학석사
2010년 Queen's Univ. 공학박사
1999년~2011년 전자부품연구원 선임연구원
2011년~현재 국민대학교 전자공학부 교수
관심분야 : 협동통신, 다중안테나 시스템, 물리계층 보안

권 대 길

2001년 동의대학교 공학사
2003년 고려대학교 공학석사
2002년 비클텍 연구원
2003년~현재 전자부품연구원 책임연구원
관심분야 : 무선 MAC, 네트워크 프로토콜, 임베디드 시스템

조 진 웅

1986년 광운대학교 공학사
1988년 광운대학교 공학석사
2001년 광운대학교 공학박사
1989년~1993년 동양정밀 주임연구원
1993년~현재 전자부품연구원 수석연구원
관심분야 : WPAN, 스마트그리드, 스마트팩토리