협력 네트워크를 위한 자가 전파방해 기반 기회적 중계 기법

*김진수 **이재홍
서울대학교
*jskim97@snu.ac.kr

Self-jamming based opportunistic relaying for a cooperative network

*Jinsu Kim **Jae Hong Lee
Seoul National University

요 약

본 논문은 협력 네트워크(cooperative network)에서 무선 채널의 보안성(security) 강화를 위한 자가 전파방해(self-jamming) 기반 기회적 중계(opportunistic relaying) 기법을 제안한다. 단일 송신 단말(source)과 단일 수신 단말(destination)이 다중 중계 단말(relay)의 협력을 통해 송수신하는 이중 홉(dual-hop) 네트워크에서 도청 단말(eavesdropper)에 의한 정보 절취를 최소화하기 위해 자가 전파방해 기법과 기회적 중계 기법을 결합한다. 이를 통해 무선 채널의 방송(broadcasting) 특성에 기인한 도청 용이성을 저하시키고, 다중 중계 단말의 송신 전력을 최소화하여 협력 네트워크의 수명(lifetime)을 연장한다. 컴퓨터 모의실험 결과를 통해 제안된 기법이 다중 중계기가 있는 이중 홉 협력 네트워크에서 보안 전송률(secrecy rate)의 불능확률(outage probability) 성능을 제고함을 보인다.

1. 서론

무선 채널(wireless channel)의 신뢰도(reliability)는 채널의 공간 다이버시티 차수(spatial diversity order)가 증가할수록 향상된다 [1]. 협력 네트워크에서의 단일 송신 단말과 단일 수신 단말간 무선 채널은 중계 단말 수에 비례하는 공간 다이버시티 차수를 갖는다 [2].

중계 단말 다중 전송(multiple transmission: MR) 기법은 송 수신 단말간 채널의 공간 다이버시티 차수를 증가시키지만, 동시에 중계 단말과 도청 단말간 채널의 공간 다이버시티 차수도 증가 시켜 불법 도청 단말에 대한 보안성을 저하한다. 중계 단말 기회적 전송(opportunistic transmission: OR) 기법은 중계 단말과 도청 단말간 채널의 공간 다이버시티 차수를 단일로 고정 시킨다.

도청 채널(wiretap channel)에서의 대부분 기회적 전송 기법은 도청 단말이 오직 중계 단말과 수신 단말간 무선 채널에서만 정보 절취를 한다고 가정한다 [3]. 본 논문에서는 도청 단말이 중계 단말과 수신 단말간 무선 채널뿐만 아니라 송신 단말과 중계 단말간 무선 채널에서도 정보 절취를 하는 환경에서 효율적 자가 전파방해 기법을 제안한다.

이 논문은 2012 년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임. (No. 2012-0005692).

2. 시스템 모델

단일 송신 단말(source: S), 단일 수신 단말(destination, D), 단일 도청 단말(eavesdropper: E), K 개의 중계 단말이 있는 협력 네트워크를 고려한다. 각 단말은 단일 안테나를 사용하며, 동시에 송신과 수신을 할 수 없다고 가정한다. 중계 단말은 복호화재전송(decode-and-forward)을 협력 방식으로 사용한다.

중계 단말들은 송신 단말과 수신 단말간 경로의 중간에 위치하며 송신 단말은 중계 단말 집합 $\mathrm{K} = \{1, 2, ..., K\}$ 의 도움을 통해서만 수신 단말과 정보를 주고 받을 수 있다고 가정한다. 도청 단말은 중계 단말에 근접해 있으며 송신 단말과 수신 단말의 위치를 모른다고 가정한다.

단말 A 와 단말 B 간의 무선 채널 계수(wireless channel coefficient) h_{AB} 을 평균이 0 이고 분산이 Ω_{AB} 인 원형 대칭 복소 가우시안 확률 변수(zero-mean circularly symmetric complex Gaussian random variable)로 가정하면, 채널 이득 계수(channel gain coefficient) $\left|h_{\mathrm{AB}}\right|^2$ 은 장애율(hazard rate) $1/\Omega_{\mathrm{AB}}$ 인 지수 분포(exponential distribution)을 갖는다.

3. 자가 전파교란 기반 기회적 중계 기법

송신 단말과 수신 단말은 두 단계(phase)를 통해 통신한다.

첫 번째 단계에서는, 송신 단말이 중계 단말들에게 메시지 신호(message signal)을 전송하는 동안 수신 단말이 전파교란 신호(jamming signal)를 방송한다. 송신 단말과 수신 단말은 각각 ζP 와 $(1-\zeta)P$ 의 전력을 사용한다고 가정한다. $\zeta \in (0, 1]$은 메시지 신호에 할당되는 전력의 비를 나타낸다. k번째 중계 단말과 도청 단말에서의 순시 신호대간섭및잡음비(signal to interference plus noise ratio: SINR)는 다음과 같다.

$$\gamma_{Sk} = \frac{\zeta P|h_{Sk}|^2}{N_0 + (1-\zeta)P|h_{Dk}|^2} \quad (1)$$

$$\gamma_{SE} = \frac{\zeta P|h_{SE}|^2}{N_0 + (1-\zeta)P|h_{DE}|^2} \quad (2)$$

각 단말에서의 수신 시 잡음은 평균이 0 이고 분산이 N_0 인 가산 백색 가우시안 잡음(additive white Gaussian noise)을 가정한다.

두 번째 단계에서는, 메시지 신호 복호화에 성공한 중계 단말 중 하나가 선택되어 해당 메시지 신호를 ζP 의 전력으로 수신 단말에 전송한다. 이때 송신 단말은 $(1-\zeta)P$ 의 전력으로 전파교란 신호를 방송한다. 수신 단말과 도청 단말에서의 순시 신호대간섭및잡음비는 다음과 같다.

$$\gamma_{kD} = \frac{\zeta P|h_{kD}|^2}{N_0} \quad (3)$$

$$\gamma_{kE} = \frac{\zeta P|h_{kE}|^2}{N_0 + (1-\zeta)P|h_{SE}|^2} \quad (4)$$

도청 단말에서 최대비 결합 (Maximal ratio combining: MRC) 기법을 사용한다고 가정하면, 송신 단말과 수신 단말 사이의 순시 보안 전송률(instantaneous secrecy rate)은 수식 (5)번과 같다.

$$\mathrm{I}_S = \left[\frac{1}{2}\log_2(1+\gamma_{kD}) - \frac{1}{2}\log_2(1+\gamma_{SE}+\gamma_{kE})\right]^+, \quad (5)$$

$[x]^+ = \max\{0, x\}$

최적 중계 단말은 수식 (5)의 순시 보안 전송률을 최대화 하는 단말이므로 수식 (6)번과 같이 선택된다.

$$b^* = \arg\max_{k\in \mathrm{D}} \left\{\frac{1}{2}\log_2\left(\frac{1+\gamma_{kD}}{1+\gamma_{SE}+\gamma_{kE}}\right)\right\}$$

$$= \arg\max_{k\in \mathrm{D}} \left\{\frac{\gamma_{kD}}{\gamma_{kE}}\right\} \quad (6)$$

두 번째 등식은 순시 신호대간섭및잡음비 γ_{SE} 가 k 에 독립적이기 때문에 성립하며, 집합 D 는 복호화 집합으로서 첫 번째 단계에서 송신 단말의 메시지 신호를 성공적으로 수신한 중계 단말들의 집합이다. 즉, $\mathrm{D} = \left\{k \in \mathrm{K} : \log_2(1+\gamma_{Sk}) \geq 2R_e\right\}$, R_e는 송신 단말과 수신 단말간 주파수 효율이다.

보안 전송률의 불능확률은 수식 (5)의 순시 보안 전송률이 목표(target) 보안 전송률 R_S 보다 작을 확률로 정의된다. 즉, 불능확률은 수식 (7)과 같이 정의 된다.

$$\mathrm{P}_{out}^S = \Pr\{\mathrm{I}_S < R_S\} \quad (7)$$

4. 컴퓨터 모의 실험 결과

중계 단말의 수는 3, 주파수 효율과 목표 보안 전송률은 1 bit/sec/Hz, 모든 장애율은 1 로 가정하였다. 즉, $K = 3$, $R_e = R_s = 1$, $\Omega_{Sk} = \Omega_{Dk} = \Omega_{kE} = 1$, $k \in \mathrm{K}$.

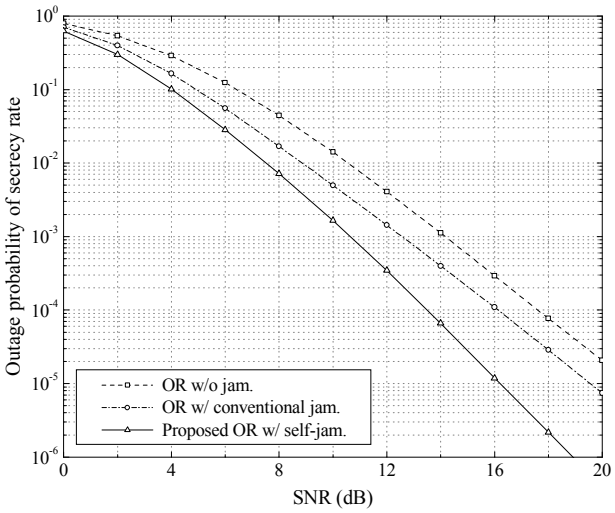

그림 1. 불능 확률 비교

5. 결론

본 논문에서는 기회적 협력 네트워크에서 무선 채널의 보안성 향상을 위한 자가 전파방해 기법을 제안하였다. 컴퓨터 모의 실험 결과를 통해 제안된 기법이 기존 보안 기법 보다 향상된 불능 확률 성능을 보임을 확인하였다.

참고문헌

[1] D. Chizhik, G. J. Foschini, M. J. Gans, and R. A. Valenzuela, "Keyholes, correlations, and capacities of multi-element transmit and receive antennas," *IEEE Trans. Wireless. Commun.*, vol. 1, no. 2, pp. 361-368, Apr. 2002.

[2] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocol and outage behavior," *IEEE Trans. Inform. Theory*, vol. 50, no. 12, pp. 3062-3080, Dec. 2004.

[3] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.