논문 19-44-05-05 The Journal of Korean Institute of Communications and Information Sciences '19-05 Vol.44 No.05
https://doi.org/10.7840/kics.2019.44.5.829

파워 분할 기반의 릴레이 프로코톨의 보안 성능에 시간에 따른 채널 변화가 미치는 영향

이 기 송•, 임 진 택°

Effects of Outdated Channel on Secrecy Performance of Power Splitting-Based Relaying Protocol

Kisong Lee•, Jin-Taek Lim°

요 약

본 논문에서는 시간에 따른 채널의 변화로 인한 오차가 존재하는 무선 환경에서 센서의 전원 부족 문제와 보안 문제를 동시에 해결하기 위해 파워 분할 기반의 릴레이 프로토콜을 제안한다. 릴레이는 비신뢰성을 갖는 잠재적 도청자이며, 전원이 없어 외부의 RF 신호로부터 에너지를 하베스팅한다. 또한, 릴레이가 발신원으로부터 전송되는 정보를 해석하는 것을 막기 위해 목적지는 발신원이 정보를 전송하는 동안 방해 전파를 전송한다. 시간에 따라 채널이 변하지 않는다면 목적지는 릴레이 신호로부터 방해 전파를 완벽하게 제거하여 발신원의 정보를 정확히 해석할 수 있지만, 그렇지 않은 경우는 제거되지 않은 잔여 방해 전파가 남아 목적지의 수신 성능을 열화 시킨다. 이러한 상황에서 보안 성능 지표인 아웃티지 확률을 도출하고, 이를 최적화 할 수 있는 방해 전파 비율 및 파워 분할 비율을 찾는다. 다양한 환경에서 시뮬레이션을 통해 제안 방안이 기존 방안에 비해 보안 성능을 개선함을 보인다.

Key Words : Secure communication, Energy harvesting, Power splitting, Relay, Outdated channel

ABSTRACT

In this paper, we propose a power splitting-based relaying protocol to resolve the energy shortage problem of sensors and information security at the same time in wireless environments with the error caused by the outdated channel. An untrusted relay can be a potential eavesdropper, and it should harvest energy from the external RF signals because it has no power source. In addition, a destination sends a jamming signal to prevent the relay from decoding information transmitted by a source while the source transmits the information signal. If the channel is not outdated, the destination can interpret the source's information by eliminating the jamming signal perfectly from the relaying signals. Otherwise, a residual jamming signal which cannot be canceled out degrades the receiving performance of the destination. In this situation, we derive a secrecy performance metric, e.g., outage probability, and find the values of jamming power ratio and power splitting ratio for optimizing the outage probability. Through the simulations under various environments, we show that the proposed scheme improves the secrecy performance, compared to the conventional scheme.

※ 이 성과는 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2018R1C1B6003297).
• First Author : Chungbuk National University, School of Information and Communication Engineering, kslee85@cbnu.ac.kr, 정회원
° Corresponding Author : Agency for Defense Development, jtyim@kaist.ac.kr, 정회원
논문번호 : 201902-453-A-RN, Received February 8, 2019; Revised February 24, 2019, 2014; Accepted March 8, 2019

Ⅰ. 서 론

무선 통신뿐 만 아니라 센서의 전원 부족 문제를 해결하기 위해 라디오 주파수(Radio frequency, RF)를 이용하여 정보와 전력을 동시에 전송(Simultaneous wireless information and power transfer, SWIPT)하기 위한 기술이 이에 대한 해결책으로 떠오르고 있다[1]. [2]에서는 SWIPT를 위한 파워 분할 기법을 제안하였고, [3]에서는 3개의 노드가 존재하는 무선 환경에서 SWIPT를 위한 릴레이 기법을 제안하였다. 뿐만 아니라 무선 통신 및 사물 인터넷 기술의 발달로 다양한 네트워크가 혼재함에 따라 인증 받지 못한 도청자로부터 정보 유출을 막는 보안 기술에 대한 중요성도 커졌다. 이에 따라 별도의 암호키 없이 방해 전파(Jamming signal)를 통해 도청자로의 정보 흐름을 근본적으로 차단시켜 주는 기술인 물리계층 보안(Physical layer security)이 제안되었다[4]. [5]에서는 협력적 방해 전파 전송을 통해 정보 보안을 보장하기 위한 파워 할당 방안을 제안하였다. [6,7]에서는 에너지 하베스팅이 가능한 릴레이 네트워크에서 보안 전송률을 최대화 하기 위한 최적의 파워 분할 비율을 도출하였다. [8]에서는 잠재적 도청자가 될 수 있는 비신뢰성을 갖는 릴레이(Untrusted relay)로부터 정보를 보호하기 위한 보안 전송 기법을 연구하였다. 하지만 기존의 연구들은 채널 정보를 완벽히 알고 있다는 가정 하에 진행된 것으로, 시간에 따라 채널이 변하면서 오차가 발생하는 실제 무선 환경에 직접적으로 적용하기는 어렵다[9,10].

본 논문에서는 무전원의 비신뢰성을 갖는 릴레이가 존재하는 2-hop 네트워크에서 발신원(Source)과 목적지(Destination) 사이의 보안 전송을 보장하는 파워 분할 기반의 릴레이 프로토콜을 제안하고자 한다. 릴레이는 발신원과 목적지와는 다른 보안 레벨(Security level)을 갖고 있으며, 릴레이 고유의 전원을 사용하기보다는 발신원과 목적지로부터 전송된 신호에서 하베스팅한 에너지를 이용하여 신호의 전달을 돕는 합리적인 시나리오를 가정하였다. 비신뢰성을 갖는 릴레이가 발신원이 전송하는 정보를 해석하는 것을 막기 위해 발신원이 정보를 전송하는 동안 목적지도 방해 전파를 전송한다. 릴레이는 수신한 신호의 파워로부터 일정 비율을 에너지 하베스팅을 하는데 사용하고, 나머지 비율은 정보를 수신하는데 사용한다. 그 후 하베스팅 한 에너지를 이용해 수신한 신호를 증폭하여 목적지에 전송한다. 릴레이와 목적지 사이의 채널이 시간에 따라 변하지 않는다면 목적지는 릴레이 신호로부터 방해 전파를 완벽히 제거할 수 있지만, 채널이 변하여(Outdated) 오차가 존재하는 경우에는 방해 전파를 완벽히 제거할 수 없다. 그러므로 채널 오차를 고려하여 아웃티지 확률(Outage probability)을 수식적으로 정리하고, 이를 최적화 할 수 있는 방해 전파 비율 및 파워 분할 비율을 numerical하게 찾는다. 또한, 다양한 시뮬레이션 환경에서 방해 전파 전송을 위해 항상 최대 파워를 사용하는 기존 방안과의 비교를 통해 제안 방안의 우수성을 검증한다.

Ⅱ. 시스템 모델

본 논문에서는 그림 1에서처럼 발신원, 릴레이, 목적지 등 3개의 노드가 존재하는 2-hop 릴레이 네트워크를 고려한다. 여기서 릴레이는 잠재적 도청자 역할을 할 수 있는 비신뢰성이 있는 노드라 가정한다[8]. 노드 i와 j사이의 채널 h_{ij}는 independent and identically distributed (i.i.d.) 플랫 페이딩을 가정하며, $i,j \in \{s,r,d\}$이다[6-8]. 여기서 s, r, d는 각각 발신원, 릴레이, 목적지를 나타낸다. 채널의 파워 게인 $|h_{ij}|^2$은 mean이 λ_{ij}인 지수적 분포(Exponential distribution)를 따르며, 다음과 같은 확률 밀도 함수(Probability density function, pdf)를 갖는다.

$$f_{|h_{ij}|^2}(x) = \frac{1}{\lambda_{ij}} e^{-\frac{x}{\lambda_{ij}}}, \quad x \geq 0. \tag{1}$$

또한, 릴레이와 목적지가 받는 수신 신호에는 $n_r = n_d \sim CN(0,\sigma^2)$을 따르는 Additive White Gaussian Noise(AWGN)이 존재한다고 가정한다.

파워 분할 기반 릴레이 프로토콜은 그림 2와 같이 전체 블록 시간 T동안 2개의 phase로 구성되어 있다. 첫 번째 phase에서는 릴레이가 발신원의 정보를 도청하는 것을 막기 위해, 발신원이 정보(Source signal, s)를 전송하는 동안 목적지도 방해 전파(z)를 전송한다.

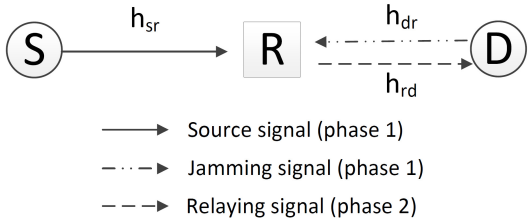

그림 1. 보안 릴레이 네트워크의 시스템 모델
Fig. 1. System model of secure relay networks

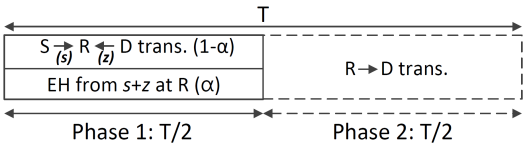

그림 2. 파워 분할 기반 릴레이 프로토콜
Fig. 2. Power splitting-based relaying protocol

릴레이는 무전원 노드이므로 수신한 신호의 파워 중 α만큼의 비율을 이용하여 에너지 하베스팅을 하고, $1-\alpha$만큼의 비율을 이용하여 신호를 수신한다[2]. 여기서 α를 파워 분할 비율이라 하며, $0 \le \alpha \le 1$의 범위를 갖는다. 두 번째 phase에서 릴레이는 하베스팅한 에너지를 이용한 Amplify-and-Forward (AF) 기법을 통해 신호를 목적지에 전송한다. 릴레이와 목적지 간의 채널이 변하지 않았다면 목적지는 릴레이 신호에 포함된 파일럿(Pilot) 신호로부터 획득한 h_{rd}에 대한 채널 상태 정보(Channel state information, CSI)에 기반하여, 방해 전파를 제거하고 발신원의 정보를 복원할 수 있다. 하지만 두 phase 간의 시간이 변함에 따라 채널이 변하여 오차가 존재한다면 목적지는 릴레이 신호로부터 방해 전파를 완벽하게 제거할 수 없다. 그러므로 채널이 변한 상황에서는 방해 전파를 최대 파워로 전송하는 것이 최적이 아닐 수 있다. 그러므로 시간에 따른 채널 오차, 방해 전파 비율, 에너지 하베스팅 비율 등의 파라미터가 아웃티지 확률과 같은 보안 성능에 미치는 영향을 알아보고자 한다.

Ⅲ. 파워 분할 기반 릴레이 프로토콜

첫 번째 phase 동안 릴레이가 수신하는 신호는 아래와 같이 표현이 가능하다.

$$y_r = \sqrt{(1-\alpha)P}h_{sr}s + \sqrt{(1-\alpha)\kappa P}h_{dr}z + n_r. \quad (2)$$

수식 (2)에서 s와 z는 크기 1의 파워를 갖는 정규화된 신호, P는 발신원과 목적지의 최대 전송 파워, κ는 방해 전파 전송 비율로 $0 \le \kappa \le 1$의 범위를 갖는다. 채널이 시간에 따라 변하므로 h_{dr}은 h_{rd}와 같지 않으며, 이때 두 채널 간의 관계는 아래와 같이 나타낼 수 있다[9,10].

$$h_{dr} = \rho h_{rd} + \sqrt{1-\rho^2}\, w. \quad (3)$$

수식 (3)에서 ρ는 채널 상관 계수(Channel correlation coefficient)로써 Jakes' autocorrelation model에 의해 다음과 같이 $\rho = J_0(2\pi f_d T_d)$ 표현 가능하다. 여기서 J_0는 the zeroth order Bessel function이며, f_d와 T_d는 각각 h_{rd}에 대한 최대 도플러 주파수와 h_{dr}은 h_{rd}사이의 시간차를 나타낸다. ρ는 f_d와 T_d로부터 쉽게 추정이 가능하다. 또한, w는 오차를 나타내는 기호로 h_{rd}와 같은 분포 $w \sim CN(0, \lambda_{rd})$를 따르는 랜덤 변수이다[9,10]. 릴레이에서의 Signal-to-Interference-plus-Noise Ratio (SINR)은 다음과 같다.

$$\begin{aligned}\Gamma_r &= \frac{(1-\alpha)P|h_{sr}|^2}{(1-\alpha)\kappa P|h_{dr}|^2 + \sigma^2} \\ &= \frac{(1-\alpha)|h_{sr}|^2\gamma}{(1-\alpha)\kappa(\rho^2|h_{rd}|^2 + (1-\rho^2)|w|^2)\gamma + 1}.\end{aligned} \quad (4)$$

수식 (4)에서 $\gamma = \frac{P}{\sigma^2}$는 전송 Signal-to-Noise Ratio (Transmit SNR)이다. 또한, 릴레이가 하베스팅한 에너지는 다음과 같다.

$$\begin{aligned}E_h &= \frac{T\eta\alpha(P|h_{sr}|^2 + \kappa P|h_{dr}|^2)}{2} \\ &= \frac{T\eta\alpha(P|h_{sr}|^2 + \kappa P\rho^2|h_{rd}|^2 + \kappa P(1-\rho^2)|w|^2)}{2} \\ &= \frac{T\eta\alpha P_e}{2}.\end{aligned} \quad (5)$$

수식 (5)에서 η는 에너지 변환 효율이며, P_e는 단위 시간 당 하베스팅한 파워이다.

두 번째 phase에서 릴레이는 받은 신호를 A_r 만큼 증폭하여 목적지에 전송한다. 릴레이가 전송하는 신호는 아래와 같이 표현된다.

$$\begin{aligned}x_r &= A_r \cdot y_r \\ &= \sqrt{\frac{P_r}{(1-\alpha)(P|h_{sr}|^2 + \kappa P|h_{dr}|^2) + \sigma^2}} \cdot y_r \\ &= \sqrt{\frac{P_r}{(1-\alpha)P_e + \sigma^2}} \cdot y_r.\end{aligned} \quad (6)$$

수식 (6)에서 $P_r = \frac{E_h}{T/2} = \eta\alpha P_e$은 릴레이의 전송 파워이다. 또한, 목적지가 수신하는 신호는 아래의 수식으로 표현 가능하다.

$$\begin{aligned}y_d &= h_{rd}x_r + n_d \\ &= A_r\sqrt{(1-\alpha)P}h_{sr}h_{rd}s + A_r\sqrt{(1-\alpha)\kappa P}h_{dr}h_{rd}z \\ &\quad + A_r h_{rd}n_r + n_d.\end{aligned} \quad (7)$$

목적지는 h_{rd}의 CSI 정보를 기반으로 수신한 신호로부터 방해전파를 다음과 같이 제거하고, $\hat{y}_d$의 신호를 획득한다.

$$\begin{aligned}\hat{y}_d &= y_d - A_r\rho h_{rd}^2\sqrt{(1-\alpha)\kappa P}z \\ &= A_r\sqrt{(1-\alpha)P}h_{sr}h_{rd}s + A_r h_{rd}n_r + n_d \\ &\quad + A_r\sqrt{(1-\alpha)\kappa P}\sqrt{1-\rho^2}\,h_{rd}wz.\end{aligned} \tag{8}$$

수식 (8)에서 $A_r\sqrt{(1-\alpha)\kappa P}\sqrt{1-\rho^2}\,h_{rd}wz$는 시간에 따른 채널 변화로 발생한 오차로 인해 완벽히 제거되지 못하고 남은 방해 전파이다. 목적지에서의 SINR은 다음과 같이 표현된다.

$$\begin{aligned}\Gamma_d &= \frac{|A_r|^2(1-\alpha)P|h_{sr}|^2|h_{rd}|^2}{|A_r|^2(1-\alpha)(1-\rho^2)\kappa P|h_{rd}|^2|w|^2+\sigma^2(1+|A_r|^2|h_{rd}|^2)} \\ &\approx \frac{|h_{sr}|^2|h_{rd}|^2}{\kappa(1-\rho^2)|h_{rd}|^2|w|^2+\dfrac{|h_{rd}|^2}{(1-\alpha)\gamma}+\dfrac{1}{\eta\alpha\gamma}}.\end{aligned} \tag{9}$$

여기에서 수식 (6)의 A_r에 해당하는 값을 수식 (9)에 대입한 후, $1/\gamma^2$에 관련된 수식을 지워주면 근사화된 수식을 얻을 수 있다. SNR이 큰 환경에서는 $1/\gamma^2$에 관련된 값이 다른 값보다 현저히 작아 이러한 근사화가 가능하다. 수식 (4)와 (9)로부터 보안 전송률은 다음과 같이 정의할 수 있다[4].

$$R_S = \left[\frac{T}{2}\log_2\left(\frac{1+\Gamma_d}{1+\Gamma_r}\right)\right]^+. \tag{10}$$

정리된 수식을 기반으로 우선 정보 보안이 만족되지 않을 확률인 아웃티지 확률을 도출해 보고자 한다. 정보 보안이 만족되지 않는 경우는 다음과 같이 2가지 경우가 있다. 릴레이가 에너지 하베스팅 회로를 구동시킬만한 충분한 파워를 수신하지 못하는 경우의 확률을 파워 아웃티지 확률(Power outage probability)라 하고, 다음과 같이 표현한다.

$$\begin{aligned}P_{pout} &= \Pr[P_e < P_{th}] \\ &= \int_0^\infty\int_0^\infty\int_0^\infty I_{P_e<P_{th}}(x_1,x_2,x_3) \\ &\quad \times f_{|h_{sr}|^2}(x_1)f_{|h_{rd}|^2}(x_2)f_{|w|^2}(x_3)dx_1dx_2dx_3.\end{aligned} \tag{11}$$

수식 (11)에서 $I_A(x)$는 x에서 A의 사건이 발생한 경우는 값이 1로 결정되며, 그렇지 않은 경우는 값이 0으로 결정되는 함수이다. 또한, P_{th}는 에너지 하베스팅 회로를 구동시키기 위해 필요한 최소한의 파워이다. 또한, 네트워크의 보안 전송률이 정해진 기준 값 R_{th}보다 낮은 경우도 보안 전송 요구를 만족시키지 못한다. 이때의 확률을 보안 아웃티지 확률(Secrecy outage probability)라 하고 다음과 같이 표현 가능하다.

$$\begin{aligned}P_{sout} &= \Pr\left[\frac{1+\Gamma_d}{1+\Gamma_r}<\delta\right] \\ &= \int_0^\infty\int_0^\infty\int_0^\infty I_{\frac{1+\Gamma_d}{1+\Gamma_r}<\delta}(x_1,x_2,x_3) \\ &\quad \times f_{|h_{sr}|^2}(x_1)f_{|h_{rd}|^2}(x_2)f_{|w|^2}(x_3)dx_1dx_2dx_3.\end{aligned} \tag{12}$$

수식 (12)에서 $\delta = 2^{2R_s/T}$이다. 수식 (11)과 (12)를 통해 최종적인 아웃티지 확률은 다음과 같이 표현 가능하다[8].

$$P_{out} = P_{pout} + (1-P_{pout})P_{sout}. \tag{13}$$

아웃티지 확률을 최소화하는 α와 κ는 아래와 같이 numerical하게 찾을 수 있다.

$$(\alpha_{out}^*, \kappa_{out}^*) = \arg\min_{\alpha,\kappa} P_{out}. \tag{14}$$

Ⅳ. 시뮬레이션 결과

시뮬레이션에서 사용한 파라미터는 $\gamma = 70dB$, $\eta = 0.7$, $P_{th} = -30dBm$, $R_{th} = 1bps/Hz$ 이다[1]. 또한, 발신원과 릴레이 사이의 거리와 릴레이와 목적지 사이의 거리는 5 m로 하였으며, path-loss exponent는 2.7로 설정하였다. 채널 페이딩은 mean이 1인 지수 확률 변수로 생성하였다.

그림 3은 방해 전파 파워 비율(κ)에 대한 아웃티지 확률(P_{out})을 보여준다. 채널이 시간에 따라 변하지 않아 h_{rd}와 h_{dr}이 같은 경우($\rho = 1$)는 목적지가 최대 파워로 방해 전파를 전송하는 것이 최적이다 ($\kappa_{out}^* = 1$). 하지만 h_{rd}와 h_{dr}이 같지 않은 경우($\rho = 0.9$)는 제거되지 않는 방해 전파가 목적지의 수신 성능을 떨어트려 방해 전파 파워를 줄이는 것이 P_{out} 측면에서 최적이다 ($\kappa_{out}^* = 0.14$). $\rho = 1$일 때와 $\rho = 0.9$일 때 사용된 최적의 파워 분할 비율은 각각 $\alpha_{out}^* = 0.965$과 $\alpha_{out}^* = 0.97$이다.

그림 4는 파워 분할 비율(α)에 대한 아웃티지 확률

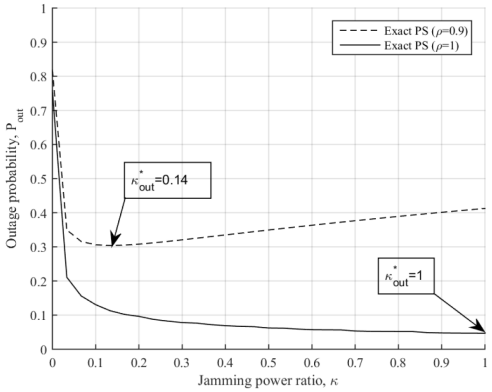

그림 3. 아웃티지 확률 vs. 방해 전파 파워 비율
Fig. 3. Outage probability vs. jamming power ratio

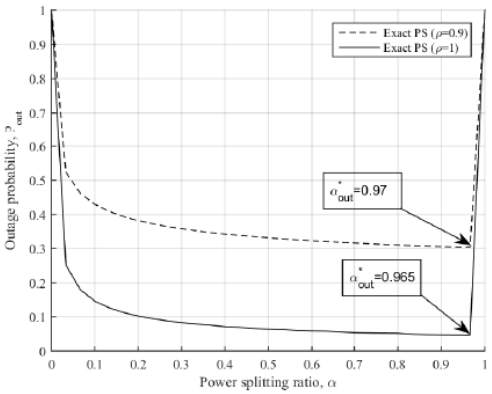

그림 4. 아웃티지 확률 vs. 파워 분할 비율
Fig. 4. Outage probability vs. power splitting ratio

(P_{out})을 보여준다. $\rho=1$일 때와 $\rho=0.9$일 때의 최적의 파워 분할 비율은 각각 $\alpha_{out}^{*}=0.965$와 $\alpha_{out}^{*}=0.97$이다. 이를 통해 α는 κ에 비해 상대적으로 시간 변화에 따른 채널 오차에 큰 영향을 받지 않는 것을 확인할 수 있다. 또한, 릴레이가 수신한 파워의 대부분을 이용하여 에너지 하베스팅을 수행하는 것이 P_{out}을 최소화하기 위해 최적임을 알 수 있다. $\rho=1$일 때와 $\rho=0.9$일 때 사용된 최적의 방해 전파 파워 비율은 각각 $\kappa_{out}^{*}=1$과 $\kappa_{out}^{*}=0.14$이다.

그림 5는 채널 상관 계수(ρ)에 대한 아웃티지 확률 (P_{out})을 보여준다. 여기서 Exact PS는 주어진 ρ마다 그림 3과 4에서 얻은 최적의 κ와 α를 사용하는 제안 방안이며, Ref. PS는 항상 최대 파워로 ($\kappa=1$) 방해 전파를 사용하는 기존 방안이다 [8]. h_{rd}와 h_{dr}의 채널 값이 심하게 달라질수록 제거되지 않는 방해 전파의 크기가 커지므로 두 방안 모두 P_{out}이 상당히 커진다. 하지만 제안 방안은 기존 방안에 비해 전 구간에서 압도적으로 낮은 P_{out}을 달성할 수 있음을 보여준다. 다만 $\rho=1$일 때는 최대 파워로 방해 전파를 전송하는 것이 최적이므로 제안 방안과 기존 방안의 성능이 동일하다.

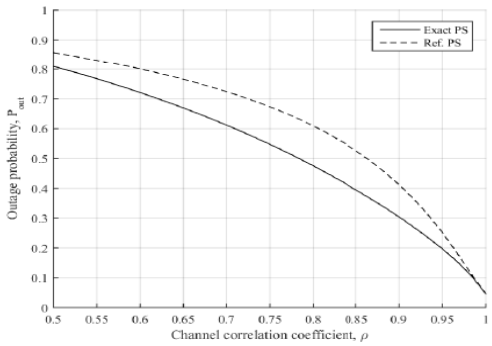

그림 5. 아웃티지 확률 vs. 채널 상관 계수
Fig. 5. Outage probability vs. channel correlation coefficient

V. 결 론

본 논문에서는 에너지 하베스팅이 가능한 릴레이로부터 발신원의 정보를 보호하기 위해 목적지가 방해 전파를 전송하는 파워 분할 기반의 릴레이 프로토콜을 제안하고, 보안 성능을 분석하였다. 시간이 변함에 따라 채널 오차가 존재하는 환경에서는 목적지가 릴레이 신호로부터 자신이 보낸 방해 전파를 완벽히 제거할 수 없다. 이러한 환경에서 네트워크의 보안 성능 지표인 아웃티지 확률을 도출하고, 이를 최적화 할 수 있는 방해 전파 비율과 에너지 하베스팅 비율을 찾았다. 시뮬레이션 결과를 통하여 시간이 변함에 따라 발생하는 채널 오차가 커질수록 방해 전파 비율을 줄이고 에너지 하베스팅 비율을 늘리는 것이 보안 성능 측면에서 최적임을 확인하였다.

References

[1] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, “Wireless networks with RF energy harvesting: A contemporary survey,” *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 757-789, 2nd Quart. 2015.

[2] L. Liu, R. Zhang, and K. Chua, “Wireless information and power transfer: A dynamic power splitting approach,” *IEEE Trans.*

Commun., vol. 61, no. 9, pp. 3990-4001, Sep. 2013.

[3] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622-3636, Jul. 2013.

[4] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[5] K.-H. Park, T. Wang, and M.-S. Alouini, "On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1741-1750, Sep. 2013.

[6] K. Lee and H.-H Choi, "Power splitting-based relaying for improving physical layer security," *J. KICS*, vol. 42, no. 7, pp. 1352-1355, Jul. 2017.

[7] K. Lee and H.-H. Choi, "Power splitting-based analog network coding for improving physical layer security in energy harvesting networks," *J. KIICE*, vol. 21, no. 10, pp. 1849-1854, Oct. 2017.

[8] S. S. Kalamkar and A. Banerjee, "Secure communication via a wireless energy harvesting untrusted relay," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2199-2213, Mar. 2017.

[9] J. Hu, W. Yang, N. Yang, X. Zhou, and Y. Cai, "On-off-based secure transmission design with outdated channel state information," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6075-6088, Sep. 2015.

[10] K. S. Hwang, M. Ju, and M.-S. Alouini, "Outage performance of opportunistic two-way amplify-and-forward relaying with outdated channel state information," *IEEE Trans. Commun.*, vol. 61, no. 9, pp. 3635-3643, Sep. 2013.

이 기 송 (Kisong Lee)

2013년 8월 : KAIST 전기 및 전자공학과 박사

2013년 9월~2015년 2월 : ETRI 융합기술연구소 연구원

2015년 3월~2017년 8월 : 군산대학교 정보통신공학과 조교수

2017년 9월~현재 : 충북대학교 정보통신공학부 조교수

<관심분야> 이동통신, 무선전력전송, 차세대 융합통신

[ORCID:0000-0001-8206-4558]

임 진 택 (Jin-Taek Lim)

2012년 8월 : 연세대학교 전기전자공학부 학사

2014년 8월 : KAIST 전기 및 전자공학과 석사

2019년 2월 : KAIST 전기 및 전자공학과 박사

2019년 3월~현재 : 국방과학연구소 선임연구원

<관심분야> 이동통신, 사물인터넷, 보안통신

[ORCID:0000-0002-9649-0459]