논문 19-44-04-09 The Journal of Korean Institute of Communications and Information Sciences '19-04 Vol.44 No.04
https://doi.org/10.7840/kics.2019.44.4.678

지연 채널 정보를 고려한 시간 전환 기반 릴레이 프로토콜의 보안 성능 분석 및 개선 방안

임 진 택•, 이 기 송*, 나 인 호°

Secrecy Performance Analysis and Enhancement Scheme for Time Switching-Based Relaying Protocol under Outdated Channel State Information

Jin-Taek Lim•, Kisong Lee*, In-Ho Ra°

요 약

본 논문에서는 무선 채널의 시변 특성을 반영한 보안 릴레이 프로토콜을 제시한다. 전달원은 전원의 수명 연장을 위해 시간 전환 기법을 이용하여 주변의 RF 신호들로부터 에너지를 하베스팅 한다. 전달원은 정보의 전달을 도와주지만, 수신원의 정보 열람은 허용되지 않은 비신뢰적인 전달원으로 가정한다. 따라서, 수신원은 송신원이 전달원으로 정보신호를 전송할 때 이를 저해하는 방해 신호를 전송한다. 수신원은 전달원으로부터 신호를 전달 받으면 자가 방해신호를 제거하여 송신원의 신호를 해석한다. 하지만 채널 시변 특성에 의하여 수신원이 방해신호를 전송할 때의 채널과 수신원이 전달원으로부터 신호를 수신할 때의 채널 정보에는 시간 지연에 의한 오차가 존재하며, 이러한 지연 채널 정보 하에서는 방해신호가 완벽히 제거될 수 없다. 잔류 방해 신호가 존재하는 상황에서 주요 보안 성능 지표인 아웃티지 확률과 에르고딕 보안 전송률을 유도하고, 이를 최적화 할 수 있는 방해 신호 비율 및 시간 전환 비율을 도출한다. 시뮬레이션을 통하여 제안하는 방법이 기존 방안에 비해 우월한 성능을 달성함을 보인다.

Key Words : Secure communication, Energy harvesting, Time switching, Relay, Outdated channel state information

ABSTRACT

In this paper, we propose a secure relaying protocol to reflect time-varying nature of wireless channel. In order to extend the lifetime of the battery in the relay, the relay harvests the energy from surrounding RF signals by using a time switching method. The relay is also assumed to be an untrusted relay, which assists in the transmission of the source's information but does not allow the reading of it. Therefore, the destination transmits the jamming signal when the source sends the information signal to the relay. The destination decodes the signal from the relay after the jamming signal cancellation. However, there is a time difference between the channel when the jamming signal is transmitted by the destination and the channel when the relay transmits the

※ 본 연구는 2016년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2016R1A2B4013002).
• First Author : Korea Advanced Institute of Science and Technology, School of Electrical Engineering, jtyim@kaist.ac.kr, 정회원
° Corresponding Author : Kunsan National University, School of Computer, Information and Communication Engineering, ihra@kunsan.ac.kr, 정회원
* Chungbuk National University, School of Information and Communication Engineering, kslee85@cbnu.ac.kr, 정회원
논문번호 : 201902-459-C-RE, Received February 13, 2019; Revised March 27, 2019; Accepted April 10, 2019

signal to the destination, then it causes the residual jamming signal at the destination after the cancellation process. In the presence of the residual jamming signal, we derive the outage probability and the ergodic secrecy rate, which are key indicators of secure communication performance, and obtain the optimal jamming power ratio and the optimal time switching ratio. Simulation shows that the proposed scheme is superior to the conventional scheme.

Ⅰ. 서 론

무선 통신환경에서 추가적인 인프라의 구축 없이 신호의 전달 거리를 늘리기 위한 협력 통신에 대한 연구가 활발히 진행되고 있다[1]. 협력 통신에서 전달원은 AF(Amplify-and-Forward) 나 DF(Decode-and-Forward) 방식을 통해 송신원의 신호를 수신원으로 전달한다. AF 방식의 경우 전달원이 자신의 전력을 이용하여 신호를 증폭한 후 이를 전송하는데, 이때 유발되는 전력 소모는 전달원의 전력 수명을 단축시킬 수 있다. 이를 위한 해결책으로, RF 신호를 이용하여 전력과 정보를 모두 전송하기 위한 SWIPT (Simultaneous Wireless Information and Power Transfer) 기술이 제안되었다[2]. SWIPT의 대표적인 방법으로 시간을 분할하여 전력과 정보를 수신하는 시간 전환 방식이 있다[3]. 또한, 전달원이 주변의 RF 신호로부터 전력을 충전하고, 이를 이용하여 신호를 증폭하고 전송하는 릴레이 프로토콜 역시 제안되었다[4].

전달원이 송신원과 수신원의 정보 전달에 협력하더라도, 여러 응용 환경에서 전달원은 잠재적 도청자(Eavesdropper)가 될 수 있다. 이러한 도청원의 정보 열람을 방해하기 위하여 물리계층에서의 보안방식이 제안되었다[5]. 물리계층의 보안 통신은 별도의 약속된 암호키 없이 방해 신호만을 이용하여 도청자의 신호 해석을 막는 기술이다. 협력 통신의 경우, 송신원이 전달원으로 정보전송을 수행할 때 수신원이 전달원으로 방해신호를 전송함으로써 물리계층 보안을 달성할 수 있다. 기존 연구에서는 에너지 하베스팅이 가능한 보안통신에서 최적의 에너지 하베스팅 방법에 대한 연구를 수행하였다[6-8]. 하지만 채널 환경이 역동적으로 변할 때는 수신원이 방해 신호를 전송할 때의 채널과 수신원이 전달원으로부터 신호를 받아 방해 신호를 제거할 때의 채널이 서로 다를 수가 있다[9,10]. 이러한 채널 정보 오차로 인해 제거 되지 않고 남은 잔류 방해 신호 성분은 치명적인 보안 성능 저하를 유발한다.

본 논문에서는 에너지 하베스팅 기능을 갖춘 비신뢰적 전달원(Untrusted relay)이 존재하는 네트워크에서 시간 지연에 의한 채널 정보 오차를 반영하여 송신원(Source)과 수신원(Destination) 사이의 보안 성능을 분석한다. 보안 성능 지표로는 아웃티지 확률(Outage probability)과 에르고딕 보안 전송률(Ergodic secrecy rate)을 이용한다. 또한, 수식화한 성능 지표를 통해 최적 방해 신호 크기 비율 및 시간 전환 비율을 수치적으로 찾는다. 다양한 시뮬레이션 환경에서 기존 방안과의 성능 비교를 통해 제안 방안의 우수성을 검증한다.

Ⅱ. 시스템 모델

그림 1은 무선 충전 장치를 갖춘 전달원을 이용한 보안 통신 모델을 나타낸다. 네트워크는 송신원(S), 전달원(R), 수신원(D)의 총 3개의 노드들로 구성된다. 여기서 전달원은 동시에 잠재적 도청원이다[6]. 각 노드는 단일 안테나를 갖추고 있으며, 반이중 방식의 통신을 수행함을 가정한다.

시간 전환 기반의 릴레이 프로토콜의 작동 원리는 그림 2와 같다. 프로토콜에 할당된 총 시간 T중에서, βT에 해당하는 부위상(Subphase) 1의 시간 동안, 전달원은 송신원에서 전송된 정보 신호와 수신원에서 전송된 방해 신호를 이용하여 에너지 하베스팅을 수행한다. 여기서 β는 시간 전환 비율을 나타내며,

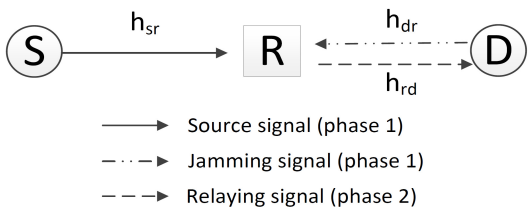

그림 1. AF 릴레이 네트워크의 시스템 모델
Fig. 1. System model of AF relay networks

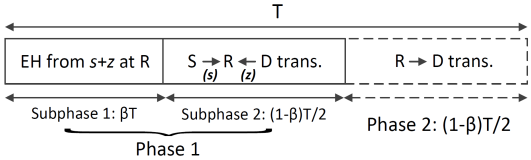

그림 2. 시간 전환 기반 릴레이 프로토콜
Fig. 2. Time switching-based relay protocol

$0 < \beta < 1$의 범위를 갖는다. $(1-\beta)T/2$ 시간의 부위상 2에서 전달원은 송신원의 신호를 수신한다. 마지막으로 $(1-\beta)T/2$ 시간의 위상(Phase) 2에서, 전달원은 부위상 1에서 하베스팅 한 에너지를 이용하여 증폭한 신호를 수신원으로 전달한다.

노드 i와 노드 j 간의 채널 h_{ij}는 평균이 0이고 분산이 λ_{ij}인 복소 가우시안 분포를 따른다고 가정한다 ($h_{ij} \sim CN(0, \lambda_{ij})$)[6-8]. 따라서, 채널의 진폭($|h_{ij}|^2$)은 평균이 λ_{ij}인 지수 분포 모델을 따르고, 이에 대응하는 확률분포함수(Probability Density Function)는 아래와 같이 표현된다.

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

노드 간 채널이 완벽한 호혜성(Reciprocity)를 가진다면, 동일한 시간 순간에서 $|h_{ij}|^2$ 와 $|h_{ji}|^2$ 는 같은 값을 갖는다. 하지만 제안하는 프로토콜에서 채널 h_{dr}은 위상 1에서 사용되는 반면 h_{rd}는 위상 2에서 사용된다. 위상 1과 위상 2에 T_d만큼의 시간 차이가 있을 때, 두 채널은 완벽히 같지 않고 T_d에 상응하는 오차를 가지게 된다. 이러한 채널의 시변화 특성을 반영한 h_{rd}와 h_{dr}의 관계는 아래의 식으로 모델링이 가능하다[9,10].

$$h_{dr} = \rho h_{rd} + \sqrt{1-\rho^2}\, w. \tag{2}$$

여기서 w은 h_{rd}와 동일한 분포를 따르지만 서로 독립인 확률 변수이다 ($w \sim CN(0, \lambda_{rd})$). ρ는 h_{rd}와 h_{dr}의 상관 관계를 나타낼 수 있는 채널 상관 상수(Channel Correlation Coefficient)로 $\rho = J_0(2\pi f_d T_d)$의 제이크 상관성 모델(Jakes' autocorrelation model)을 통하여 모델링 되었다[9,10]. J_0는 0차 베셀 함수(the zeroth order Bessel function), f_d는 도플러 주파수, T_d는 채널의 시간 차이를 나타낸다. 일반적으로, 노드 사이의 상대 속도를 알면 f_d를 계산하여 ρ를 유추할 수 있다.

Ⅲ. 시간 전환 기반 릴레이 프로토콜

위상 1에서 전달원이 수신하는 신호 y_r은 다음과 같다.

$$y_r = \sqrt{P} h_{sr} s + \sqrt{\kappa P} h_{dr} z + n_r. \tag{3}$$

식 (3)에서 P는 송신원과 수신원의 전송 전력이며, 정보신호 s와 방해신호 z는 $E[|s|^2] = E[|z|^2] = 1$의 정규화 된 전력을 갖는다. n_r은 Additive White Gaussian Noise(AWGN)로 $CN(0, \sigma^2)$의 분포를 따른다. κ는 방해신호 전력 비율로 $0 \leq \kappa \leq 1$의 범위를 갖는다. 이때, 전달원에서 하베스팅 된 에너지는 다음과 같다.

$$\begin{aligned} E_h &= T\beta\eta(P|h_{sr}|^2 + \kappa P|h_{dr}|^2) \\ &= T\beta\eta(P|h_{sr}|^2 + \kappa P\rho^2|h_{rd}|^2 + \kappa P(1-\rho^2)|w|^2) \\ &= T\beta P_e. \end{aligned} \tag{4}$$

식 (4)에서 η는 에너지 변환 효율이고, P_e는 단위 시간 당 하베스팅 된 전력으로 해석할 수 있다. 식 (3)을 이용하여, 전달원에서의 Signal-to-Interference-and-Noise Ratio (SINR)를 유도하면 다음과 같다.

$$\begin{aligned} \Gamma_r &= \frac{P|h_{sr}|^2}{\kappa P|h_{dr}|^2 + \sigma^2} \\ &= \frac{|h_{sr}|^2\gamma}{\kappa(\rho^2|h_{rd}|^2 + (1-\rho^2)|w|^2)\gamma + 1}. \end{aligned} \tag{5}$$

식 (5)에서 $\gamma = \frac{P}{\sigma^2}$는 송신 Signal-to-Noise Ratio (Transmit SNR)이다.

위상 2에서 전달원은 받은 신호를 A_r만큼 증폭하여 수신원에 전송한다. 전달원이 전송하는 신호는 아래와 같이 표현된다.

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

식 (6)에서 $P_r = \frac{2\beta}{1-\beta} P_e$는 하베스팅된 에너지를 이용한 전달원에서의 전송 전력이다. 또한, 수신원이 수신하는 릴레이 신호는 아래의 수식으로 표현된다.

$$\begin{aligned} y_d &= h_{rd} x_r + n_d \\ &= A_r \sqrt{P} h_{sr} h_{rd} s + A_r \sqrt{\kappa P} h_{dr} h_{rd} z + A_r h_{rd} n_r + n_d. \end{aligned} \tag{7}$$

식 (7)에서 n_d 역시 AWGN으로 n_r과 같은 $CN(0,\sigma^2)$ 분포를 따른다. 수신원은 전달원으로부터 피드백 받은 채널 h_{rd}에 대한 CSI(Channel State Information) 정보를 기반으로 수신한 신호로부터 방해 신호를 제거한다. 방해 신호가 제거된 후 수신원이 받은 최종 신호 $\hat{y}_d$는 아래와 같다.

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

식 (8)에서 $A_r\sqrt{\kappa P}\sqrt{1-\rho^2}h_{rd}wz$는 채널의 시변화 특성에서 기인하는 오차로 인해 완벽히 제거되지 못하고 남은 잔류 방해신호이다. 식 (8)을 이용하여, 수신원에서의 SINR은 다음과 같이 표현된다.

$$\Gamma_d = \frac{|A_r|^2 P|h_{sr}|^2|h_{rd}|^2}{|A_r|^2(1-\rho^2)\kappa P|h_{rd}|^2|w|^2 + \sigma^2(1+|A_r|^2|h_{rd}|^2)} \tag{9}$$

$$\approx \frac{|h_{sr}|^2|h_{rd}|^2}{\kappa(1-\rho^2)|h_{rd}|^2|w|^2 + \frac{|h_{rd}|^2}{\gamma} + \frac{1-\beta}{2\eta\beta\gamma}}. \tag{10}$$

일반적으로, $\frac{1}{\gamma^2}$을 가진 항은 크기가 매우 작아 무시가 가능하기 때문에 근사식 (10)을 사용하여도 무방하다.

식 (5)와 (10)로부터, 보안 전송률은 다음과 같이 정의된다[5].

$$R_S = \left[\frac{(1-\beta)T}{2}\log_2\left(\frac{1+\Gamma_d}{1+\Gamma_r}\right)\right]^+. \tag{11}$$

정의된 보안 전송률로부터 보안 통신의 주요 지표인 에르고딕 보안 전송률과 아웃티지 확률을 구할 수 있다. 먼저, 에르고딕 보안 전송률은 보안 전송률의 장기적 관점에서의 성능 지표로 식 (11)에 정의된 모든 확률 변수에 대해 평균을 취함으로써 아래와 같이 구할 수 있다.

$$\begin{aligned}R &= (1-P_{pout})E_{|h_{sr}|^2,|h_{rd}|^2,|w|^2}[R_S] \\ &= (1-P_{pout})\int_0^\infty\int_0^\infty\int_0^\infty \frac{(1-\beta)T}{2}\left[\log_2\left(\frac{1+\Gamma_d}{1+\Gamma_r}\right)\right]^+ \\ &\quad \times f_{|h_{sr}|^2}(x_1)f_{|h_{rd}|^2}(x_2)f_{|w|^2}(x_3)dx_1dx_2dx_3.\end{aligned} \tag{12}$$

여기서 P_{out}은 에너지 하베스팅 회로를 구동시킬만한 충분한 전력을 수신하지 못해 전력 아웃티지(Power outage)가 발생할 확률로 아래와 같이 정의된다

$$\begin{aligned}P_{pout} &= \Pr[P_e < P_{th}] \\ &= \int_0^\infty\int_0^\infty\int_0^\infty I_{P_e<P_{th}}(x_1,x_2,x_3) \\ &\quad \times f_{|h_{sr}|^2}(x_1)f_{|h_{rd}|^2}(x_2)f_{|w|^2}(x_3)dx_1dx_2dx_3.\end{aligned} \tag{13}$$

여기서 P_{th}는 에너지 하베스팅 회로 구동을 위한 최소한의 전력이다. 유도된 식 (12)로부터 에르고딕 보안 전송률을 최대화하는 β와 κ를 아래의 식을 통해 수치적으로 찾을 수 있다.

$$(\beta_R^*,\kappa_R^*) = \arg\max_{\beta,\kappa} R \tag{14}$$

다음으로 두 번째 성능 지표인 아웃티지 확률을 구한다. 아웃티지 확률을 구하기 위해서는 보안 아웃티지 확률(Secrecy outage probability)을 먼저 구해야한다. 보안 아웃티지 확률이란 보안 전송률이 정해진 최소 요구값 R_{th}보다 낮은 경우 발생한다. 이를 식으로 표현하면 아래와 같다.

$$\begin{aligned}P_{sout} &= \Pr[\frac{1+\Gamma_d}{1+\Gamma_r} < \delta] \\ &= \int_0^\infty\int_0^\infty\int_0^\infty I_{\frac{1+\Gamma_d}{1+\Gamma_r}<\delta}(x_1,x_2,x_3) \\ &\quad \times f_{|h_{sr}|^2}(x_1)f_{|h_{rd}|^2}(x_2)f_{|w|^2}(x_3)dx_1dx_2dx_3.\end{aligned} \tag{15}$$

수식 (15)에서 $\delta = 2^{2R_{th}/T}$이다. 수식 (13)과 (15)를 통해 최종적인 아웃티지 확률을 아래와 같이 구할 수 있다[11].

$$P_{out} = P_{pout} + (1-P_{pout})P_{sout}. \tag{16}$$

또한, 아웃티지 확률을 최소화하는 β와 κ를 아래와 같이 수치적으로 찾을 수 있다.

$$(\beta_{out}^*,\kappa_{out}^*) = \arg\min_{\beta,\kappa} P_{out}. \tag{17}$$

Ⅳ. 시뮬레이션 결과

시뮬레이션 환경은 다음과 같다. 송신 SNR γ=70 dB, 전력 변환 효율 η=0.7, 보안 전송률 최소 요구값

R_{th}=1 bps/Hz, 에너지 하베스팅 회로 구동을 위한 최소 전력 P_{th}=30 dBm로 설정하였다[4,6]. 또한, 송신원과 전달원 사이의 거리(d_{sr}) 및 전달원과 수신원 사이의 거리(d_{rd})는 5 m로 하였으며, 경로 손실 상수(α)는 2.7로 가정하였다. 또한, 채널 페이딩은 mean이 1인 지수 확률 변수로 생성하였다.

그림 3은 방해 신호 전력 비율(κ)에 대한 에르고딕 보안 전송률(R)을 나타낸다. $\rho=1$일 경우, 송신원이 최대 전력으로 방해 신호를 전송하는 것이 R을 최대화하는데 최적임을 확인할 수 있다 (즉, $\kappa_R^*=1$). 하지만 $\rho=0.9$일 때는 제거되지 않는 잔류 방해신호로 인해 방해신호 전력 비율을 0.24로 줄이는 것이 최적임을 알 수 있다. 낮아진 최적 방해 신호 전력 비율로부터, 채널 정보 오차가 존재하는 경우 방해신호를 통해 얻는 보안 이득보다 잔류 방해신호로 인한 신호 해석의 불이익이 더 크다는 것을 알 수 있다.

그림 4는 시간 전환 비율(β)에 따른 R의 변화를 보여준다. ρ가 작아져 잔류 방해신호 성분이 커질수록 β를 작게 하여 에너지 하베스팅 양을 줄이는 것이 R을 최대화하는데 유리함을 확인할 수 있다. 잔류 방해신호의 존재 하에서는, 하베스팅 되는 에너지의 손실보다 신호 전달에 이용되는 시간의 추가 확보가 보안 성능 개선에 더 이익이 되기 때문이다.

그림 5는 ρ에 대한 R의 변화를 보여준다. 제안 방안(Exact TS)은 ρ의 변화에 따라 최적의 κ와 β를 적응적으로 사용하는 방안이고, 기존 방안(Ref. TS)은 ρ 값의 변화에 상관없이 $\rho=1$일 때의 최적의 κ와 β를 고정하여 사용하는 방안이다[6]. ρ가 작아질수록 잔류 방해 신호가 커지기 때문에 두 방안 모두 R은 작아진다. 하지만, 제안 방안은 ρ에 따라 적응적으로 κ와 β를 조절하므로 기존 방안 대비 전 구간에서 높은 R을 달성한다.

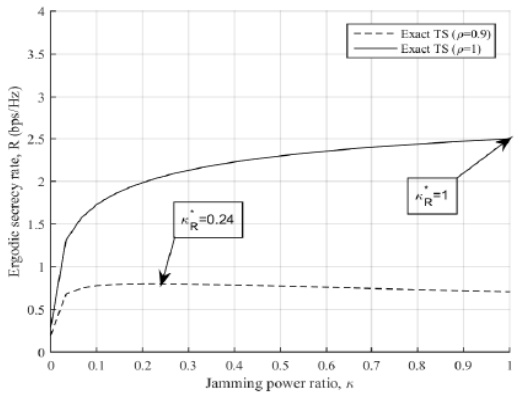

그림 3. 에르고딕 보안 전송률 vs. 방해 신호 전력 비율
Fig. 3. Ergodic secrecy rate vs. jamming signal power ratio

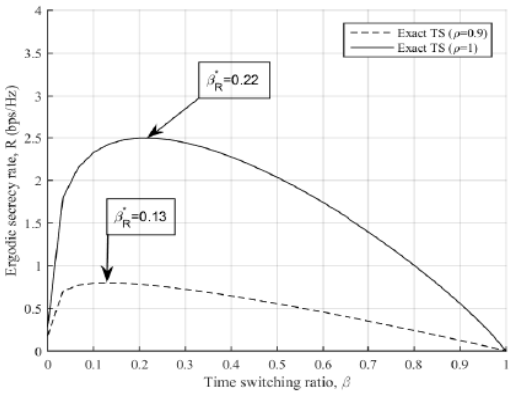

그림 4. 에르고딕 보안 전송률 vs. 시간 전환 비율
Fig. 4. Ergodic secrecy rate vs. time switching ratio

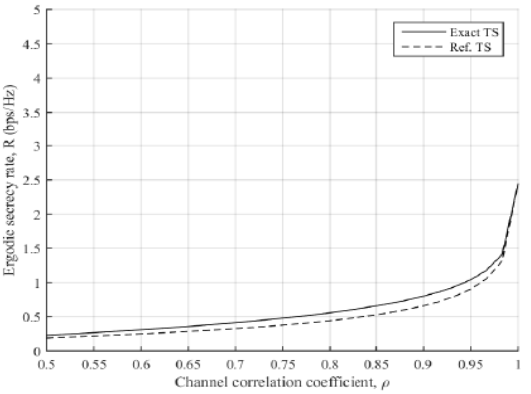

그림 5. 에르고딕 보안 전송률 vs. 채널 상관 계수
Fig. 5. Ergodic secrecy rate vs. channel correlation coefficient

그림 6은 κ에 따른 아웃티지 확률(P_{out})의 변화를 보여준다. 에르고딕 보안 전송률의 결과와 비슷하게 $\rho=1$인 환경에서는 항상 최대의 전력으로 방해신호를 전송하는 것이 P_{out} 에 대해 최적이다. 하지만, ρ가 작아짐에 따라 κ를 줄이는 것이 P_{out} 측면에서 최적임을 알 수 있다. ($\rho=0.9$일 때, $\kappa_{out}^*=0.18$).

그림 7은 β에 대한 P_{out}의 변화를 나타낸다. 에르고딕 보안 전송률과 마찬가지로 κ_{out}^*는 ρ가 1에서 0.9로 변화함에 따라 0.6에서 0.185로 줄어들었다. 채널 정보 오차가 존재하는 경우 P_{out} 관점에서 하베스팅 되는 에너지를 통한 신호 증폭 이득보다 신호 전달 시간의 추가 확보가 전체 보안 성능에 도움이 됨을 알 수 있다.

그림 8은 ρ에 대한 P_{out}의 변화를 보여준다. ρ가

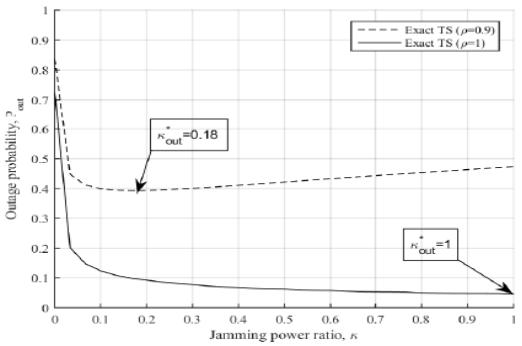

그림 6. 아웃티지 확률 vs. 방해 신호 전력 비율
Fig. 6. Outage probability vs. jamming signal power ratio

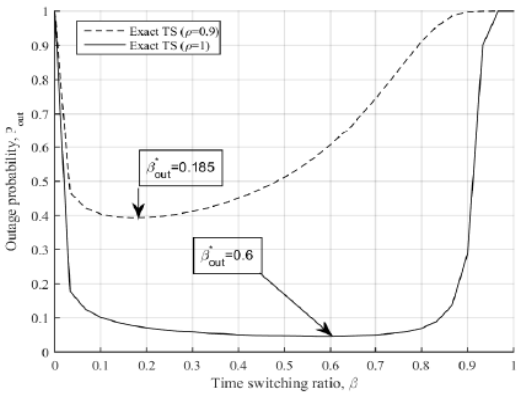

그림 7. 아웃티지 확률 vs. 시간 전환 비율
Fig. 7. Outage probability vs. time switching ratio

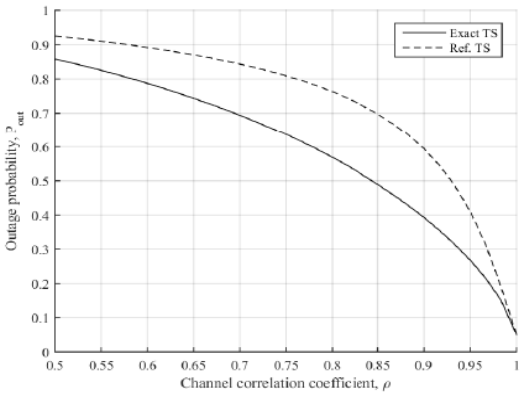

그림 8. 아웃티지 확률 vs. 채널 상관 계수
Fig. 8. Outage probability vs. channel correlation coefficient

작아짐에 따라 두 방안 모두 P_{out}이 크게 증가한다. 하지만 제안 방안은 기존 방안에 비해 전 구간에서 P_{out}이 낮음을 확인할 수 있다. 이는 적응적으로 κ와 β를 조절하는 것은 항상 P_{out}를 개선하는데 큰 도움을 줄 수 있다는 것을 의미한다.

V. 결 론

본 논문에서는 시간 전환 기반 에너지 하베스팅 기능을 갖춘 전달원을 잠재적 도청자라고 가정할 때, 지연 채널 정보를 반영하여 수신원이 방해신호를 전송하는 시스템의 보안 성능을 분석하였다. 분석한 결과를 바탕으로 지연 채널 정보 오차는 잔류 방해신호를 늘리고, 이는 보안성능을 떨어뜨릴 수 있다는 것을 확인하였다. 또한, 네트워크 보안 성능 지표인 아웃티지 확률과 에르고딕 보안 전송률을 도출하고, 보안 성능을 개선하기 위한 최적의 방해신호 전력 비율 및 시간 전환 비율을 채널 상관 계수에 따라 적응적으로 변화시키는 릴레이 프로토콜을 제안하였다. 시뮬레이션 결과를 통하여 지연으로 인한 채널 정보 오차가 커질수록 방해신호 전력 비율과 시간 전환 비율을 줄이는 것이 보안 성능 향상 측면에서 최적임을 확인하였으며, 제안 방안이 기존 방안 대비 우월한 성능을 보임을 검증하였다.

References

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

[2] L. Liu, R. Zhang, and K. Chua, “Wireless information transfer with opportunistic energy harvesting,” *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 288-300, Jan. 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] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, “Wireless networks with RF energy harvesting: A contemporary survey,” *IEEE Commun. Surv. Tuts.*, vol. 17, no. 2, pp. 757-789, 2nd Quart. 2015.

[5] S. K. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian wiretap channel,” *IEEE Trans.*

Inf. Theory, vol. IT-24, no. 4, pp. 451-456, Jul. 1978.

[6] 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.

[7] K. Lee and H.-H Choi, "Time switching-based relaying for maximizing secrecy capacity," *J. KICS*, vol. 42, no. 10, pp. 1955-1958, Oct. 2017.

[8] K. Lee and H.-H. Choi, "Time switching-based analog network coding for maximizing the minimum required secrecy capacity in energy harvesting networks," *J. KIICE*, vol. 21, no. 11, pp. 2022-2028, Nov. 2017.

[9] D. S. Michalopoulos, H. A. Suraweera, G. K. Karagiannidis, and R. Schober, "Amplify-and-forward relay selection with outdated channel state information," in *Proc. IEEE GLOBECOM*, pp. 1-6, Miami, USA, Dec. 2010.

[10] M. Chen, T. C.-K. Liu, and X. Dong, "Opportunistic multiple relay selection with outdated channel state information," *IEEE Trans. Veh. Technol.*, vol. 61, no. 3, pp. 1333-1345, Mar. 2012.

[11] Y. Liu, L. Wang, S. A. R. Zaidi, M. Elkashlan, and T. Q. Duong, "Secure D2D communication in large-scale cognitive cellular networks: A wireless power transfer model," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 329-342, Jan. 2016.

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]

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 부교수
<관심분야> 이동통신, 무선전력전송, 차세대 융합통신
[ORCID:0000-0001-8206-4558]

나 인 호 (In-Ho Ra)

1995년 8월 : 중앙대학교 전자계산학과 박사
2007년 2월~2008년 8월 : University of South Florida, 연구교수
1995년 9월~현재: 군산대학교 컴퓨터정보통신공학부 교수
<관심분야> 무선센서 및 애드혹 네트워크, 사물인터넷, PS-LTE, 블록체인, 스마트시티, 5G 융합서비스
[ORCID:0000-0002-3936-1116]