논문 20-45-07-02 The Journal of Korean Institute of Communications and Information Sciences '20-07 Vol.45 No.07
https://doi.org/10.7840/kics.2020.45.7.1145

보안 아웃티지 확률을 최소화하기 위한 무선 충전이 가능한 보안 릴레이 프로토콜

이 기 송•, 최 현 호°

Wireless-Powered Secure Relaying Protocols for Minimizing Secrecy Outage Probability

Kisong Lee•, Hyun-Ho Choi°

요 약

본 논문에서는 사물인터넷 환경에서 센서의 전원 부족과 정보 보안 문제를 동시에 해결하기 위해 보안 릴레이 프로토콜을 제안한다. 무선 충전이 가능한 릴레이는 파워 분할 혹은 시간 전환 기법을 이용하여 수신한 RF 신호로부터 에너지를 하베스팅하고, 이 전력을 이용하여 수신한 신호를 목적지에 전달한다. 또한, 도청자가 발신원으로부터 전송되는 데이터를 해석하는 것을 막기 위해 목적지는 발신원이 데이터를 전송하는 동안 방해 전파를 전송한다. 정해진 기준 값 이상의 보안 전송 요구를 보장하기 위한 보안 아웃티지 확률을 수식적으로 도출하고, 이를 최소화 할 수 있는 파워 분할 및 시간 전환 비율을 찾는다. 다양한 환경에서 시뮬레이션을 통해 제안 방안이 기존 방안에 비해 보안 아웃티지 확률을 개선함을 보인다.

Key Words : Secure communication, Energy harvesting, Power splitting, Time switching, Secrecy outage probability

ABSTRACT

In this paper, we propose power splitting-based and time-switching-based relaying protocols to solve the energy shortage of sensors and information security at the same time in internet-of-things. A wireless-powered relay uses power splitting or time switching policy to harvest energy from the received RF signals, and it utilizes this harvested energy to forward the received signal to a destination. In addition, a destination transmits jamming signal to prevent an eavesdropper from interpreting data sent by a source while the source sends the data signal. We mathematically derive secrecy outage probability to ensure a predetermined secrecy requirement, and find the optimal power splitting and time switching ratios to minimize secrecy outage probability. Through the simulations under various cases, we confirm that the proposed schemes improve secrecy outage probability, compared to the conventional schemes.

※ 이 성과는 2019년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2019R1A2C4070466).
◆ First Author : Dongguk University, Department of Information and Communication Engineering, kisonglee@dongguk.edu, 정회원
° Corresponding Author : Hankyong National University, School of ICT, Robotics & Mechanical Engineering, hhchoi@hknu.ac.kr, 종신회원
논문번호 : 202004-094-A-RN, Received April 23, 2020; Revised May 11, 2020; Accepted May 14, 2020

Ⅰ. 서 론

최근 사물인터넷 (Internet-of-Things, IoT) 분야에서 암호키 없이 무선 채널로 방해 전파를 전송하여 도청을 차단시켜 주는 기술인 물리계층 보안(Physical layer security)에 대한 관심이 커지고 있다[1,2]. 특히 목적지가 방해 전파를 전송하여 도청자가 발신원의 신호를 해석하는 것을 막는 협력적 방해 전파 기술에 대한 연구가 활발하다[3-5]. 이 기술은 추가적인 노드나 안테나의 장착 없이 네트워크를 구성하고 있는 목적지가 직접 방해 전파를 전송한다는 점에서 효율적이며 경제적이다. 뿐만 아니라 최근 무선 센서의 데이터 처리량이 늘어남에 따라 심각해지는 전원 부족 문제를 해결하기 위해 정보와 전력 동시 전송 기술(simultaneous wireless information and power transfer, SWIPT)에 대한 수요도 커지고 있다[6-9]. 대표적인 SWIPT 기술로는 파워 분할[7]과 시간 전환[8] 기법이 있으며, 무선 충전이 가능한 릴레이에 이를 적용한 새로운 릴레이 프로토콜 역시 제안되었다[9]. 최근에는 물리 계층 보안과 SWIPT를 결합하여 무선 충전이 가능한 릴레이 네트워크에서 보안 전송률을 최대화하기 위한 파워 분할 및 시간 전환 기법이 제안되었다[10,11]. 하지만 IoT 환경에서는 서비스의 품질(quality of service, QoS)을 보장해 주는 것이 중요하므로 보안 전송률을 최대화 하는 것보다 도청이 발생할 확률을 특정 값 이하로 낮춰주는 보안 아웃티지 확률 최소화가 더 중요한 성능 지표가 될 수 있다.

본 논문에서는 발신원(source)과 목적지(destination) 사이에 무선 충전이 가능한 릴레이(relay)와 도청자(eavesdropper)가 존재하는 2-hop 네트워크에서 보안 아웃티지 확률(secrecy outage probability)를 최소화하는 보안 릴레이 프로토콜을 제안하고자 한다. 제안하는 프로토콜에서는 도청자가 발신원이 전송하는 신호를 해석하는 것을 막기 위해 발신원이 신호를 전송하는 동안 목적지도 방해 전파를 전송한다. 또한, 릴레이는 수신한 신호로부터 일정 비율의 전력을 이용하여 에너지를 하베스팅하고, 나머지 비율의 전력은 신호를 수신하는데 사용한다. 릴레이는 하베스팅 한 에너지를 이용해 수신한 신호를 증폭하여 목적지에 전송하며, 목적지는 릴레이 신호로부터 자신이 보낸 방해 전파를 완벽히 제거하여 발신원의 신호를 복원한다. 하지만 도청자는 목적지가 보낸 방해 전파로 인해 발신원의 신호를 완벽하게 해석할 수 없다. 이러한 환경에서 정해진 기준 값 이상의 보안 전송 요구를 만족시키기 위한 보안 아웃티지 확률을 수식적으로 정리하고, 이를 최소화 할 수 있는 최적의 파워 분할 비율과 시간 전환 비율을 수치적으로 찾는다. 또한, 다양한 시뮬레이션 환경에서 고정된 파워 분할 비율과 시간 전환 비율을 사용하는 기존 방안과의 비교를 통해 제안 방안의 우수성을 검증한다.

Ⅱ. 시스템 모델

본 논문에서는 그림 1에서처럼 발신원, 무선 충전이 가능한 릴레이, 목적지, 도청자 등 총 4개의 노드가 존재하는 2-hop 릴레이 네트워크를 고려한다. 노드 i와 j사이의 채널 h_{ij}는 independent and identically distributed (i.i.d.) 플랫 페이딩을 가정하며, $i,j \in \{s,r,d,e\}$이다. 여기서 s, r, d, e는 각각 발신원, 릴레이, 목적지, 도청자를 나타낸다. 채널의 파워 게인 $|h_{ij}|^2$은 mean이 λ_{ij}인 지수적 분포(Exponential distribution)를 따르며, 각 노드가 받는 수신 신호에는 $n_i \sim \mathcal{CN}(0,\sigma^2)$을 따르는 additive white Gaussian noise(AWGN)가 존재한다고 가정한다. 또한, 발신원, 릴레이, 목적지는 채널 피드백을 통해 적법한 노드간의 채널 정보(h_{sr}, h_{rd})를 알고 있다고 가정한다.

보안 릴레이 프로토콜은 전체 블록 시간 T동안 2개의 phase로 구성되어 있다. 첫 번째 phase에서는 도청자가 발신원의 신호를 도청하는 것을 막기 위해, 발신원이 릴레이에 신호(source signal, s)를 전송하는 동안 목적지도 방해 전파(jamming signal, z)를 동시에 전송한다. 릴레이는 무전원 노드이므로 수신한 신호의 전력 중 일정 비율을 이용하여 에너지 하베스팅을 하고, 남은 전력을 이용하여 신호를 수신한다. 두 번째 phase에서 릴레이는 하베스팅한 에너지를 이용하여 amplify-and- forward (AF) 방식으로 신호를 목적지에 전송한다. 목적지는 릴레이 신호로부터 자신이 전

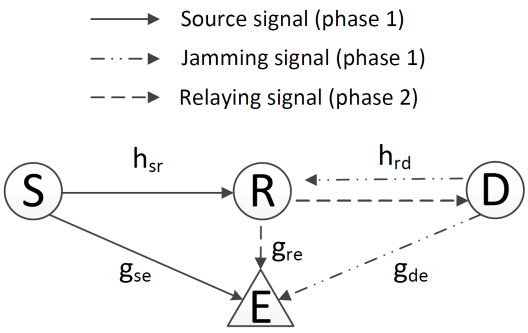

그림 1. 보안 릴레이 네트워크의 시스템 모델
Fig. 1. System model of secure relay networks

송한 방해 전파 z를 제거함으로써 발신원의 신호를 해석할 수 있지만, 도청자는 방해 전파로 인해 발신원의 신호를 해석하는데 어려움을 겪는다.

Ⅲ. 파워 분할 기반 보안 릴레이 프로토콜

파워 분할 기반 보안 릴레이 프로토콜(power splitting-based secure relaying protocol, PSR)의 경우 그림 2에서처럼 첫 번째 phase에서 릴레이가 수신한 전력을 나눠 ρ의 비율은 에너지 하베스팅에 사용하고, $1-\rho$의 비율은 신호를 수신하는데 사용한다. 첫 번째 phase 동안 릴레이가 수신하는 신호는 아래와 같이 표현이 가능하다.

$$y_r = \sqrt{(1-\rho)P_S}h_{sr}s + \sqrt{(1-\rho)P_D}h_{rd}z + n_r. \quad (1)$$

식 (1)에서 s와 z는 크기 1의 파워를 갖는 정규화된 신호이며, P_S와 P_D는 각각 발신원과 목적지의 전송 파워이다. 또한, 릴레이가 하베스팅한 에너지는 다음과 같다.

$$E_h = \frac{T\eta\rho(P_S|h_{sr}|^2 + P_D|h_{rd}|^2)}{2} = \frac{T\eta\rho P_h}{2}. \quad (2)$$

식 (2)에서 η는 에너지 변환 효율이다.

반면, 첫 번째 phase 동안 도청자가 수신하는 신호는 아래와 같다.

$$y_e^{[1]} = \sqrt{P_S}g_{se}s + \sqrt{P_D}g_{de}z + n_e. \quad (3)$$

이때 도청자의 signal-to-interference-plus- noise ratio (SINR)는 식 (4)와 같다.

$$\Gamma_e^{[1]} = \frac{P_S|g_{se}|^2}{P_D|g_{de}|^2 + \sigma^2}. \quad (4)$$

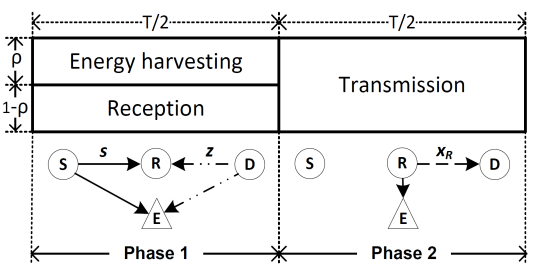

그림 2. 파워 분할 기반 보안 릴레이 프로토콜
Fig. 2. Power splitting-based secure relaying protocol

두 번째 phase에서 릴레이가 하베스팅한 에너지를 이용하여 전송하는 신호는 다음과 같다.

$$x_r = A_r \cdot y_r = \sqrt{\frac{P_R}{(1-\rho)P_h + \sigma^2}} \cdot y_r. \quad (5)$$

여기서 릴레이의 전송 파워는 $P_R = \frac{E_h}{T/2} = \eta\rho P_h$로 표현된다. 또한, 목적지가 수신하는 신호는 아래와 같다.

$$\begin{aligned} y_d &= h_{rd}x_r + n_d \\ &= \frac{\sqrt{(1-\rho)P_SP_R}h_{sr}h_{rd}s + \sqrt{P_R}h_{rd}n_r}{\sqrt{(1-\rho)P_h + \sigma^2}} \\ &\quad + \underbrace{\frac{\sqrt{(1-\rho)P_DP_R}h_{rd}^2 z}{\sqrt{(1-\rho)P_h + \sigma^2}}}_{self-cancellation} + n_d. \end{aligned} \quad (6)$$

식 (6)에서 목적지는 방해 전파 $\frac{\sqrt{(1-\rho)P_DP_R}h_{rd}^2 z}{\sqrt{(1-\rho)P_h + \sigma^2}}$를 self-cancellation을 통해 제거함으로써, 발신원의 신호를 안정적으로 수신할 수 있다. 식 (6)으로부터 목적지의 SINR은 다음과 같이 도출할 수 있다.

$$\Gamma_d = \frac{\eta\rho(1-\rho)P_hP_S|h_{sr}|^2|h_{rd}|^2}{\eta\rho P_h|h_{rd}|^2\sigma^2 + \sigma^2\{(1-\rho)P_h + \sigma^2\}}. \quad (7)$$

식 (7)을 이용하여 목적지에서의 데이터 전송률은 $R_D = \frac{T}{2}\log_2(1+\Gamma_d)$로 표현이 된다.

반면, 두 번째 phase동안 도청자가 수신한 신호는 다음과 같다.

$$\begin{aligned} y_e^{[2]} &= g_{re}x_r + n_e \\ &= \frac{\sqrt{(1-\rho)P_SP_R}h_{sr}g_{re}s + \sqrt{(1-\rho)P_DP_R}h_{rd}g_{re}z}{\sqrt{(1-\rho)P_h + \sigma^2}} \\ &\quad + \frac{\sqrt{P_R}g_{re}n_r}{\sqrt{(1-\rho)P_h + \sigma^2}} + n_e. \end{aligned} \quad (8)$$

이때 도청자의 SINR은 다음과 같이 표현된다.

$$\Gamma_e^{[2]} = \frac{\eta\rho(1-\rho)P_hP_S|h_{sr}|^2|g_{re}|^2}{\eta\rho P_h|g_{re}|^2\{(1-\rho)P_D|h_{rd}|^2 + \sigma^2\} + \sigma^2\{(1-\rho)P_h + \sigma^2\}}. \quad (9)$$

식 (4)와 (9)를 이용하여 도청자의 전체 데이터 전송률은 $R_E = \frac{T}{2}\log_2\left(1+I_e^{[1]}+I_e^{[2]}\right)$로 표현할 수 있다.

보안 전송률은 R_D와 R_E의 차로 정의되므로 다음과 같이 표현된다[1].

$$R_S = [R_D - R_E]^+ = \left[\frac{T}{2}\log_2\left(\frac{1+\Gamma_d}{1+I_e^{[1]}+I_e^{[2]}}\right)\right]^+. \quad (10)$$

식 (10)에서 $[x]^+ = \max(x,0)$이다.

네트워크의 보안 전송률이 정해진 기준 값 r_q보다 낮은 경우 보안 전송 요구를 만족시키지 못한다. 이때의 확률을 보안 아웃티지 확률이라 하고, 다음과 같이 표현한다.

$$P_{out} = \Pr[R_S < r_q] = \Pr\left[\frac{1+\Gamma_d}{1+I_e^{[1]}+I_e^{[2]}} < 2^{\frac{2r_q}{T}}\right]. \quad (11)$$

보안 아웃티지 확률을 최소화하는 최적의 파워 분할 비율은 아래의 수식으로부터 수치적으로 찾을 수 있다.

$$\rho^* = \arg\min_{0\le\rho\le 1} P_{out}. \quad (12)$$

Ⅳ. 시간 전환 기반 보안 릴레이 프로토콜

시간 전환 기반 보안 릴레이 프로토콜(time switching-based secure relaying protocol, TSR)의 경우 그림 3에서처럼 첫 번째 phase의 αT의 시간 동안 릴레이가 수신한 전력을 이용하여 에너지 하베스팅을 수행하며, $\frac{(1-\alpha)T}{2}$의 시간동안 발신원의 신호를 수신한다. 이때 릴레이가 하베스팅한 에너지와 수신한 신호는 각각 다음과 같다.

$$E_h = T\eta\alpha(P_S|h_{sr}|^2 + P_D|h_{rd}|^2) = T\eta\alpha P_h. \quad (13)$$

$$y_r = \sqrt{P_S}h_{sr}s + \sqrt{P_D}h_{rd}z + n_r. \quad (14)$$

반면, 첫 번째 phase 동안 도청자가 수신하는 신호와 SINR은 각각 아래와 같다.

$$y_e^{[1]} = \sqrt{P_S}g_{se}s + \sqrt{P_D}g_{de}z + n_e. \quad (15)$$

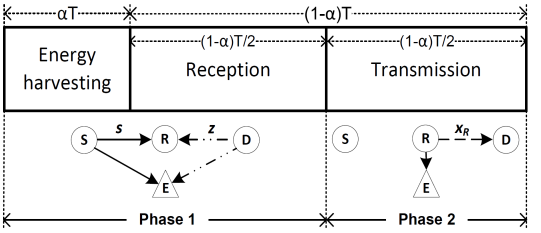

그림 3. 시간 전환 기반 보안 릴레이 프로토콜
Fig. 3. Time switching-based secure relaying protocol

$$I_e^{[1]} = \frac{P_S|g_{se}|^2}{P_D|g_{de}|^2+\sigma^2}. \quad (16)$$

또한, $\frac{(1-\alpha)T}{2}$의 시간을 갖는 두 번째 phase에서 릴레이가 하베스팅한 에너지를 이용하여 전송하는 신호는 다음과 같다.

$$x_r = \sqrt{\frac{P_R}{P_h+\sigma^2}} \cdot y_r. \quad (17)$$

여기서 릴레이의 전송 파워는 $P_R = \frac{E_h}{(1-\alpha)T/2} = \frac{2\eta\alpha P_h}{1-\alpha}$로 표현된다. 또한, 목적지가 수신하는 신호는 아래와 같다.

$$y_d = \frac{\sqrt{P_S P_R}h_{sr}h_{rd}s + \sqrt{P_R}h_{rd}n_r}{\sqrt{P_h+\sigma^2}} + \underbrace{\frac{\sqrt{P_D P_R}h_{rd}^2 z}{\sqrt{P_h+\sigma^2}}}_{self-cancellation} + n_d. \quad (18)$$

식 (18)에서 목적지는 방해 전파 $\frac{\sqrt{P_D P_R}h_{rd}^2 z}{\sqrt{P_h+\sigma^2}}$를 제거할 수 있으며, 이때 목적지의 SINR은 다음과 같이 도출할 수 있다.

$$\Gamma_d = \frac{2\eta\alpha P_h P_S|h_{sr}|^2|h_{rd}|^2}{\left\{2\eta\alpha P_h|h_{rd}|^2 + (1-\alpha)\left(P_h+\sigma^2\right)\right\}\sigma^2}. \quad (19)$$

식 (19)을 이용하여 목적지에서의 데이터 전송률은 $R_D = \frac{(1-\alpha)T}{2}\log_2(1+\Gamma_d)$로 표현이 된다.

반면, 두 번째 phase동안 도청자가 수신한 신호와 SINR은 다음과 같다.

$$y_e^{[2]} = \frac{\sqrt{P_S P_R}\, h_{sr} g_{re} s + \sqrt{P_D P_R}\, h_{rd} g_{re} z + \sqrt{P_R}\, g_{re} n_r}{\sqrt{P_h + \sigma^2}} + n_e. \tag{20}$$

$$\Gamma_e^{[2]} = \frac{2\eta\alpha P_h P_S |h_{sr}|^2 |g_{re}|^2}{2\eta\alpha P_h |g_{re}|^2 \left(P_D |h_{rd}|^2 + \sigma^2\right) + \sigma^2 (1-\alpha)\left(P_h + \sigma^2\right)}. \tag{21}$$

식 (16)와 (21)를 이용하여 도청자의 전체 데이터 전송률은 $R_E = \frac{(1-\alpha)T}{2} \log_2\left(1 + \Gamma_e^{[1]} + \Gamma_e^{[2]}\right)$로 표현할 수 있다.

R_D와 R_E를 이용하여 보안 전송률은 다음과 같이 정의할 수 있다.

$$R_S = \left[\frac{(1-\alpha)T}{2} \log_2\left(\frac{1+\Gamma_d}{1+\Gamma_e^{[1]}+\Gamma_e^{[2]}}\right)\right]^+. \tag{22}$$

보안 전송 요구를 만족시키지 못할 때의 확률인 보안 아웃티지 확률 역시 다음과 같이 표현 가능하다.

$$P_{out} = \Pr\left[\frac{1+\Gamma_d}{1+\Gamma_e^{[1]}+\Gamma_e^{[2]}} < 2^{\frac{2r_q}{T(1-\alpha)}}\right]. \tag{23}$$

보안 아웃티지 확률을 최소화하는 최적의 시간 전환 비율은 아래의 수식으로부터 수치적으로 찾을 수 있다.

$$\alpha^* = \arg\min_{0 \le \alpha \le 1} P_{out}. \tag{24}$$

V. 시뮬레이션 결과

시뮬레이션에서 사용한 파라미터는 $T=1$, $\eta=0.5$, $\sigma^2 = -70dBm$이다[6,8]. 또한, 발신원과 목적지의 거리는 10m로 설정하였으며, 두 노드는 같은 전송 전력 $P_S = P_D = P$를 사용한다. 도청자는 두 노드 사이에서 임의 발생 시켰으며, 릴레이는 중앙에 배치하였다. 채널 발생을 위하여 path-loss exponent는 2.7로 설정하였으며, 다중경로 페이딩은 mean이 1인 지수 확률 변수로 생성하였다.

그림 4는 $r_q = 2bps/Hz$일 때 전송 전력(P)에 대한 보안 아웃티지 확률(P_{out})을 보여준다. 비교 방안으로는 0.5로 고정된 파워 분할 비율($\rho=0.5$)과 시간 전환 비율($\alpha=0.5$)을 사용하는 방안을 선정하였다. 전송 전력이 커짐에 따라 안정적인 신호의 전달이 가능해져

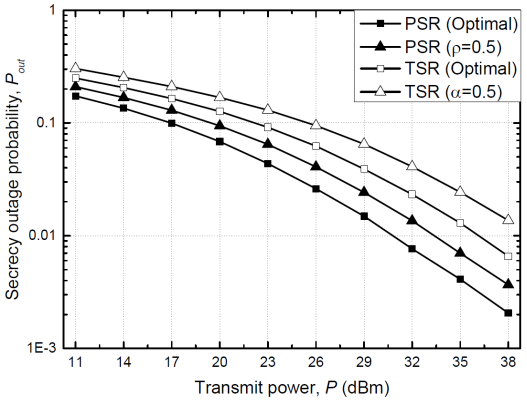

그림 4. 보안 아웃티지 확률 vs. 전송 전력
Fig. 4. Secrecy outage probability vs. transmit power

모든 방안의 보안 아웃티지 확률이 감소함을 확인할 수 있다. 또한, 최적의 ρ와 α를 사용하는 제안 방안은 고정된 ρ와 α를 사용하는 기존 방안에 비해 전 구간에서 우수한 성능을 보인다. 식 (22)에서 볼 수 있듯이 TSR의 경우 에너지 하베스팅 비율이 늘어남에 따라 보안 전송률이 선형적으로 감소한다. 반면, 식 (10)에서처럼 PSR의 경우 에너지 하베스팅 비율이 늘어남에 따라 보안 전송률이 로그 함수 안에서 감소한다. 즉, 에너지 하베스팅으로 인해 보안 전송률 측면에서 발생하는 손실이 TSR이 더 크기 때문에 PSR이 TSR보다 우수한 성능을 보인다.

그림 5는 $P = 23dBm$일 때 요구 보안 전송률(r_q)에 대한 보안 아웃티지 확률(P_{out})을 보여준다. 요구 보안 전송률이 커질수록 이를 만족시키지 못하는 경우가 자주 발생하게 되어 모든 방안의 보안 아웃티지 확률은 증가하게 된다. 또한, 그림 4에서와 같이 최적의 ρ

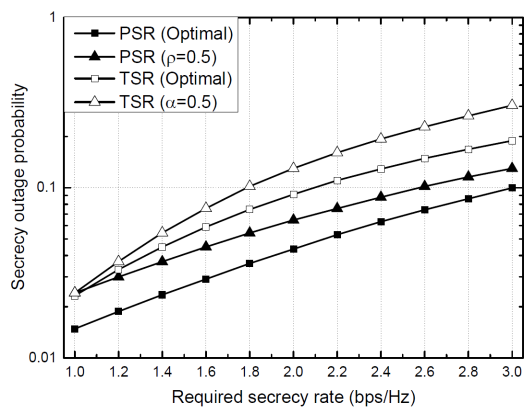

그림 5. 보안 아웃티지 확률 vs. 요구 보안 전송률
Fig. 5. Secrecy outage probability vs. required secrecy rate

와 α를 적응적으로 찾는 제안 방안은 고정된 ρ와 α를 사용하는 방안에 비해 성능을 개선시키며, PSR이 TSR보다 우수한 성능을 보이는 것을 확인할 수 있다.

Ⅵ. 결 론

본 논문에서는 도청자가 발신원의 정보를 도청하는 것을 막아 정해진 보안 요구량을 만족시켜주기 위한 파워 분할 및 시간 전환 기반의 무선 충전이 가능한 보안 릴레이 프로토콜을 제안하였다. 수학적 모델링을 통해 네트워크의 보안 성능 지표인 보안 아웃티지 확률을 도출하고, 이를 최소화 할 수 있는 최적의 파워 분할 및 시간 전환 비율을 수치적으로 찾았다. 시뮬레이션 결과를 통하여 적응적으로 에너지 하베스팅 비율을 최적의 값으로 조절해 주는 것은 보안 아웃티지 확률을 개선할 수 있음을 보였으며, TSR에 비해 PSR이 더 우수한 성능을 보임을 확인하였다. 향후 목적지에서 방해 전파를 완벽히 제거하지 못하는 실제적인 환경에서의 연구를 수행할 계획이다.

References

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

[2] L. Hu, H. Wen, B. Wu, F. Pan, R. Liao, H. Song, J. Tang, and X. Wang, "Cooperative jamming for physical layer security enhancement in internet of things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 219-228, Feb. 2018.

[3] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871-4884, Oct. 2011.

[4] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting," *IEEE Trans. Wireless Commun.*, vol. 10, no. 6, pp. 1725-1729, Jun. 2011.

[5] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical layer security," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 4, pp. 682-694, Apr. 2013.

[6] 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.

[7] 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.

[8] L. Liu, R. Zhang, and K.-C. Chua, "Wireless-powered relays in cooperative communications: Time switching relaying protocols and throughput analysis," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1607-1622, May 2015.

[9] 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.

[10] 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.

[11] 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.

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~2020년 2월 : 충북대학교 정보통신공학부 부교수
2020년 3월~현재 : 동국대학교 정보통신공학과 부교수
<관심분야> 이동통신, 무선전력전송, 차세대 융합통신
[ORCID:0000-0001-8206-4558]

최 현 호 (Hyun-Ho Choi)

2001년 2월 : KAIST 전기 및 전자공학과 졸업
2003년 2월 : KAIST 전기 및 전자공학과 석사
2007년 2월 : KAIST 전기 및 전자공학과 박사
2007년 3월~2011년 2월 : 삼성종합기술원 전문연구원
2011년 3월~현재 : 국립한경대학교 ICT로봇기계공학부 ICT로봇공학전공 교수
<관심분야> 이동통신시스템, 분산 네트워크, 저전력 통신, 무선전력전송, 생체모방 알고리즘
[ORCID:0000-0002-6785-2596]