Journal of The Institute of Electronics and Information Engineers Vol.53, NO.4, April 2016 http://dx.doi.org/10.5573/ieie.2016.53.4.079
ISSN 2287-5026(Print) / ISSN 2288-159X(Online)

논문 2016-53-4-9

하드웨어왜곡과 불완전한 채널상태정보가 물리계층보안에 미치는 영향

(The Impact of Hardware Impairments and Imperfect Channel State Information on Physical Layer Security)

심 규 성*, 도 트리 뉴**, 안 병 구***

(Kyusung Shim*, Nhu Tri Do**, and Beongku An©)

요 약

물리계층보안은 신호의 물리적 특성을 이용하여 정보를 보호하는 보안 기법이다. 현재 이에 대한 연구가 활발히 진행 중이지만 해결해야할 다음과 같은 문제점들이 존재한다. 도청자는 자신의 존재를 숨기기 위해서 자신의 채널상태정보를 다른 합법적인 노드와 공유하지는 않는다. 그리고 노드가 신호를 전송할 때 하드웨어 왜곡이 발생하지만 많은 연구들은 노드 모델들이 이상적인 것으로 가정을 하고, 하드웨어 왜곡문제를 고려하지 않고 있다. 이와 같은 문제점들을 해결하기 위한 본 논문의 주요한 특징 및 기여도는 다음과 같다. 첫째, 도청자의 채널상태정보를 얻기 위해서 조력자노드를 합법적인 노드주변에 설치하고, 조력자노드의 채널상태정보를 이용하여 노드모델에서 하드웨어 왜곡을 고려한다. 둘째, 제안된 시스템 모델의 인터셉트 확률에 대한 Closed-Form Expression을 제시한다. 제안된 시스템의 성능평가를 위해서 다양한 시뮬레이션를 통하여 제안된 시스템 모델의 물리계층보안에 미치는 영향을 알아본 결과, 불완전한 채널상태정보는 인터셉트 확률에는 영향을 미치지 못한 반면에, 불완전한 노드모델의 경우, 인터셉트 확률, 에르고딕 시크리스 용량과 보안채널용량에 영향을 준다는 것을 보여준다.

Abstract

Physical layer security is cryptography technique to protect information by using physical nature of signals. Currently, many works on physical layer security have been actively researching while those researching models still have some problems to be solved. Eavesdropper does not share its channel state information with legitimate users to hide its presence. And when node transmits signal, hardware impairments are occurred, whereas many current researches assume that node model is ideal node and does not consider hardware impairments. The main features and contributions of this paper to solve these problems are as follows. First, our proposed system model deploys torch node around legitimate user to obtain channel state information of eavesdropper and considers hardware impairments by using channel state information of torch node. Second, we derive closed-form expression of intercept probability for the proposed system model. The results of the performance evaluation through various simulations to find out the effects on proposed system model in physical layer security show that imperfect channel state information does not effect on intercept probability while imperfect node model effects on intercept probability, Ergodic secrecy capacity and secrecy capacity.

Keywords : Physical layer security, Hardware impairment, Imperfect channel state information, Torch node, Intercept probability

* 학생회원, 홍익대학교 스마트도시과학경영대학원 정보시스템전공
(Information System, Graduate School of Smart City Science Management, Hongik University)
** 학생회원, 홍익대학교 일반대학원 전자전산공학과
(Dept. of Electronic and Computer Engineering in Graduate School, Hongik University)
*** 평생회원, 홍익대학교 컴퓨터정보통신공학과
(Dept. of Computer & information Communication Engineering, Hongik University)
© Corresponding Author(E-mail: beongku@hongik.ac.kr)

※ This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ICT/SW Creative Research program (IITP-2015-R2212150026) supervised by the IITP(Institute for Information & communication Technology Promotion).
Received ; February 16, 2016 Revised ; March 9, 2016 Accepted ; March 29, 2016

Ⅰ. 서 론

무선통신은 전기나 자기적인 신호가 공기를 통하여 전달된다. 이러한 무선통신의 개방성으로 인하여 악의적인 사용자가 마음만 먹으면 언제나 통신을 엿듣고 정보를 가로 챌 수 있다. 또한 스마트폰의 보급으로 인하여 무선통신의 사용빈도가 늘어나고 무선통신을 이용하여 중요한 정보를 주고받는 경우가 점점 증가하고 있다. 따라서 무선통신의 보안에 대한 요구가 증가하고 있다. 지금까지의 보안은 주로 암호학이었다. 암호학은 수학적 복잡성에 기반을 둔 보안방법으로 정보를 보내기 전에 데이터를 수학적으로 복잡한 알고리즘을 이용하여 변형 시켜서 전송한다. 그러면 합법적인 사용자는 이미 암호화 한 알고리즘을 푸는 방법을 알고 있어서 쉽게 풀 수 있다. 하지만 불법적인 사용자가 중간에 정보를 가로챘다면, 어떤 방법으로 암호화 되었는지 모르기 때문에 푸는데 상당한 시간이 소요되고, 그로 인해 암호를 풀었을 때는 이미 또 다른 암호로 바뀌어서 해독한 암호는 더 이상 필요가 없게 된다. 이것이 암호학을 이용한 정보보안방법이다. 암호학은 수학적 복잡성에 기반을 두기 때문에 컴퓨터의 계산 속도가 빨라짐에 따라서 점점 보안의 견고성을 약해지고 있다.

암호학과 달리 물리계층보안은 신호의 물리적 특성을 이용하여 불법적인 사용자에게 정보자체를 전달하지 않아 정보를 보호하는 방법이다. 합법적인 사용자와 불법적인 사용자의 정보의 차이를 보안채널용량(secrecy capacity)이라하는데, 보안채널용량은 Shannon에 의해서 처음 개념이 정의 되었고[1], 이후 Wyner에 의해서 채널용량의 차이를 이용하면 합법적인 사용자에게는 정보를 전달하면서 불법적인사용자에게는 정보가 전달되지 않을 수 있다는 것을 증명하였다[2]. 이를 바탕으로 많은 물리계층보안을 위한 시스템모델과 방법들이 연구되고 있다.

논문[3]의 시스템 모델은 소스노드, 목적지노드, 하나의 중계노드 그리고 하나의 도청자노드로 구성되어있다. 제안된 시스템 모델에서 도청채널과 메인채널의 채널이득의 변화가 물리계층보안에 미치는 영향이 연구되었다. 논문[4]의 시스템 모델은 소스노드, 목적지노드, 다수의 중계노드 그리고 도청자노드로 구성되어있다. 소스노드에서 목적지노드까지 다수의 중계노드를 거친다. 이때, 중계노드의 수가 증가함이 물리계층보안에 미치는 영향이 연구되었다. 논문[5]의 시스템 모델은 소스노드와 목적지노드, 다수의 중계노드 그리고 도청자노드로 구성되어있다. 이때, 하나의 중계노드를 여러 가지 방법으로 선택하여 각 선택방법이 물리계층보안에 미치는 영향이 연구되었다. 논문[6]의 시스템 모델은 소스노드, 목적지노드, 다수의 중계노드 그리고 다수의 도청자노드로 구성되었다. 이때, 다수의 중계노드중 하나의 중계노드를 여러 가지 방법으로 선택하고, 다수의 도청자노드가 정보를 가로채려고 할 때, 하나의 도청자노드와는 달리 다수의 도청자노드가 물리계층보안에 미치는 영향이 연구되었다. 연구[7]에서는 소스노드, 다수의 목적지노드, 다수의 중계노드 그리고 다수의 도청자노드로 구성되어있다. 이러한 시스템에서 최적의 중계노드를 선택하고 여러 가지 채널환경에서 물리계층보안이 연구되었다. 연구[8]의 시스템모델은 소스노드, 목적지노드, 그리고 도청자노드로 구성되어있다. 소스노드와 도청자노드는 여러 개의 안테나로 구성되어있다. 다수의 안테나중 하나의 안테나를 다양한 방법으로 선택하여 안테나 선택이 물리계층보안에 미치는 영향이 연구되었다.

현재 앞에서 설명한 연구들[3~8]에서 다양한 시스템 모델이 물리계층보안에 미치는 영향들이 연구되고 있다. 하지만 위의 논문들에서는 공통적으로 도청자노드가 자신의 채널상태정보(channel state information/ CSI)를 공유한다고 가정하고 있다. 하지만 실제 도청자노드는 불법적인 사용자로써, 자신의 존재를 다른 노드에게 숨기고 정보를 가로채기 때문에 자신의 CSI를 다른 노드와 공유하지 않는다. 따라서 본 논문에서는 자신의 CSI를 공유하지 않는 도청자노드의 CSI를 유추하기 위해서 다음과 같은 방법이 사용된다. 조력자노드는 직접 소스노드와 목적지노드간의 통신에는 직접관여를 하지 않는 노드를 말한다. 조력자노드는 통신에는 관여하지 않지만 자신의 CSI를 주변노드에 전송하여 도청자노드의 채널상태를 유추하는데 필요한 정보를 제공한다. 조력자노드의 불완전한 채널상태정보(imperfect CSI)를 이용하여 도청자노드의 채널상태정보를 유추한다[9].

또한, 연구들[3~8]에서 사용된 노드 모델은 이상적인 노드이다. 이상적인 노드는 전송할 때 보내고자하는 신호를 이상적으로 처리하여 전송한다. 하지만, 실제 노드는 불완전하여 하드웨어왜곡이 발생한다. 이러한 하드웨어왜곡이 발생하는 이유는 페이즈 노이즈, I/Q 불균형, 고증폭 비선형성 등이 있다[10]. 이러한 하드웨어왜곡이 시스템이 어떠한 영향을 미치는지에 대한 연구는 현재 진행 중 이다. 그리고 하드웨어 왜곡이 물리계층보안에 미치는 영향에 대한 연구는 미비하다.

본 논문의 연구내용에 대한 주요한 특징 및 기여도를 설명하면 다음과 같다.

- 기존 연구와 달리, 보다 실제와 유사한 시스템 모델에서의 물리계층보안을 연구하였다. 즉, 도청자노드가 자신의 CSI를 공유하지 않아 조력자노드의 불완전한 CSI를 이용하여 도청자노드의 SCI를 유추하고, 노드는 불완전하여 전송 시 왜곡이 발생한다.
- 제시된 시스템 모델에서 메인채널보다 도청채널이 많은 정보를 가로채는 확률(intercept probability)를 구하고 수학적으로 증명하여, Closed-Form Expression을 제시한다.
- 다양한 시뮬레이션 결과를 제시하여 제안된 시스템 모델의 물리계층보안에 미치는 영향을 다양한 측면에서 비교 분석한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 본 논문에서 제안하는 노드모델과 시스템모델에 대하여 자세히 설명한다. Ⅲ장에서는 제안된 시스템모델의 수학적 모델을 제시하고 Intercept Probability의 Closed-Form Expression을 증명한다. Ⅳ장에서는 다양한 시뮬레이션 결과를 제시하고 시스템 모델이 물리계층보안에 미치는 영향에 대해서 확인하고, 마지막 Ⅴ장에서는 결론을 내고 본 논문을 마무리한다.

Ⅱ. 시스템 모델

본 장에서는 본 논문에서 제안하는 노드 모델과 시스템 모델에 대해서 설명한다.

1. 노드 모델

일반적인 노드 모델의 경우 그림 1의 좌측(그림 1(a))과 같다. 일반적인 노드는 완전하기 때문에 전송 시에 왜곡이 발생하지 않는다.

하지만 실제 노드의 경우 연구[10]에서와 같이 노드에서 신호를 처리할 때 왜곡이 발생한다(그림 1(b)). 이러한 왜곡을 error vector magnitudes(E VMs)라고 한다. 3GPP LTE의 경우, EVMs는$\kappa_t \in [0.08, 0.175]$조건을 만족해야 한다[11].

2. 시스템 모델

본 논문에서 제시한 시스템 모델은 그림 2와 같다.

시스템 모델은 소스노드(S), 목적지노드(D), 조력자노드(T), 그리고 도청자노드(E)로 구성되어있다. 시스템에서 S와 D는 서로 직접 신호를 전달한다. E는 도청자이

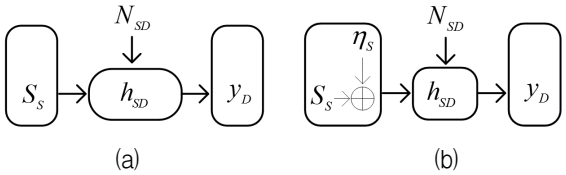


그림 1. 일반적인 노드모델(a)과 불완전한 노드모델(b)의 비교
Fig. 1. Comparison of ideal node model(a) and non-ideal node model(b).

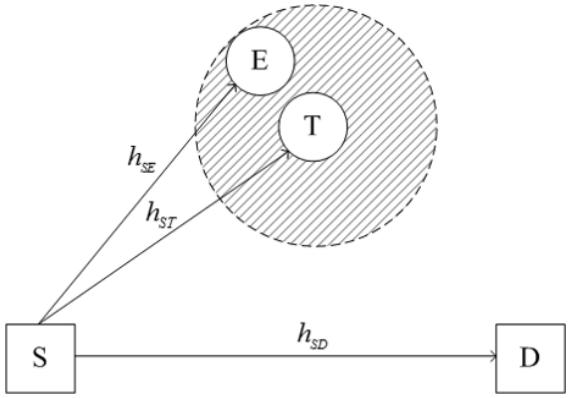


그림 2. 시스템 모델
Fig. 2. System model.

기 때문에 자신의 CSI를 주변 노드에게 전달하지 않는다. T는 S와 D간의 통신에는 관여하지 않고 자신의 CSI를 S와 D에게 전달하여 S와 D로 하여금 E의 CSI를 자신의 CSI를 통하여 유추할 수 있도록 도와준다. 그리고 본 논문에서는 S와 D사이 채널을 메인채널, S와 T사이의 채널을 조력채널, 그리고 S와 E사이 채널을 도청채널이라 한다. 각 노드들은 동일한 종류의 노드로서 전송파워, 왜곡의 정도가 동일하다. 채널환경은 line-of-sight(LOS) 가 존재하지 않는 Rayleigh-fading환경이다.

일반적인 무선통신 시스템에서 메인채널을 통해 D로 전달되는 신호는 다음과 같다.

$$y_{SD} = \sqrt{P} h_{SD} x_S + n_D \tag{1}$$

여기서 $\sqrt{P}$는 노드의 전송파워, h_{SD}는 메인채널의 채널효율, 그리고 n_D는 메인채널 상에 존재하는 노이즈이다.

하지만 본 논문에서 사용되는 노드 모델은 그림 1(b). 와 같이 불완전하여 하드웨어 왜곡이 발생한다. 하드웨어 왜곡이 존재하는 노드 모델에서 메인채널에서 D로 전달되는 신호는 다음과 같다.

$$y_{SD} = \sqrt{P} h_{SD}(x_S + \eta_S) + n_D \quad (2)$$

여기서 η_S는 하드웨어에서 발생하는 왜곡의 정도를 나타내며, $\eta_S \sim CN(0, \kappa^2 P)$ 와 같은 분포를 갖는다.

도청자노드(E)는 자신의 CSI를 전송하지 않는다. 따라서 본 논문에서는 조력자노드(T)가 전송한 T채널효율(h_{ST})을 이용하여 E의 채널효율(h_{SE}) 유추할 수 있다. E의 채널효율(h_{SE})을 구하면 다음과 같다.

$$h_{SE} = \rho h_{ST} + \epsilon \sqrt{(1-\rho^2)} \quad (3)$$

여기서 ρ는 h_{ST}와 h_{SE}의 채널효율의 정확성을 나타낸다. ρ가 1에 가까울수록 h_{ST}와 h_{SE}는 같음을 나타낸다. 따라서 ρ의 범위는 $0 \le \rho \le 1$이다.

식(3)을 이용하여 E에서 수신된 신호를 구하면 다음과 같다.

$$\begin{aligned} y_{SE} &= \sqrt{P} h_{SE}(x_S + \eta_S) + n_E \quad (4) \\ &= \sqrt{P}(\rho h_{ST} + \epsilon \sqrt{(1-\rho^2)})(x_S + \eta_S) + n_E \end{aligned}$$

식(2)와 식(4)를 이용하여 메인채널과 도청채널의 신호대잡음비(signal-to-Noise Ratio/SNR)을 구하면 다음과 같다.

$$\gamma_{SD} = \frac{P g_{SD}}{\kappa P g_{SD} + N_0} \quad (5)$$

$$\gamma_{SE} = \frac{P g_{SE}}{\kappa P g_{SE} + N_0} \quad (6)$$

여기서 g_{SD}와 g_{SE}는 메인채널과 도청채널의 채널이득으로 각각 $g_{SD} = |h_{SD}|^2$, $g_{SE} = |h_{SE}|^2$ 로 정의된다.

식(5)와 식(6)을 바탕으로 메인채널과 도청채널의 채널용량을 구하면 다음과 같다.

$$C_{SD} = \log_2(1 + \gamma_{SD}) \quad (7)$$

$$C_{SE} = \log_2(1 + \gamma_{SE}) \quad (8)$$

보안채널용량이란, 메인채널이 도청채널의 차이로서 어떤 채널에 더 많은 정보가 전달되는지를 나타낸다. $C_{sys} > 0$인 경우, 메인채널에 정보가 더 많이 전달되고 있고, $C_{sys} < 0$인 경우, 도청채널에 정보가 더 많이 전달되고 있고, $C_{sys} = 0$인 경우, 두 채널에 동일한 양의 정보가 전달됨을 나타낸다. 보안채널용량은 다음과 같다.

$$C_{sys} = C_{SD} - C_{SE} \quad (9)$$

Ⅲ. 이론적인 분석: 인터셉트 확률 분석

본장에서는 시스템 모델에서 도청자노드(E)가 얻은 정보의 양이 목적지노드(D)가 얻은 정보의 양보다 큰 경우로 정의된 인터셉트 확률(Intercept Probability/IP: P_{IP})의 수학적 모델을 제시하고, P_{IP}의 Closed-form Expression을 구한다.

수학적 모델 증명에 앞서 각 채널의 확률분포를 살펴본다. 각 채널은 서로 독립이고 동일한 확률분포를 갖는 Rayleigh fading으로 각 채널은 다음과 같은 누적확률분포와 확률밀도함수를 따른다[12].

$$F_i(x) = 1 - \exp\left(-\frac{x}{\lambda_i}\right) \quad (10)$$

$$f_i(x) = \frac{1}{\lambda_i} \exp\left(-\frac{x}{\lambda_i}\right) \quad (11)$$

식(10)과 식(11)에서 i는 $i \in \{g_{SD}, g_{SE}\}$이고, λ_i는 각 채널의 평균채널이득이다.

P_{IP}(도청에 성공한 확률(Intercept Probability))는 도청채널용량이 메인채널용량보다 큰 확률로 다음과 같다.

$$\begin{aligned} P_{IP} &= \Pr(C_{sys} < 0) \quad (12) \\ &= \Pr(C_{SD} < C_{SE}) \\ &= \Pr\left(\frac{a_1 g_{SD}}{a_2 g_{SD} + a_3} < \frac{a_1 g_{SE}}{a_2 g_{SE} + a_3}\right) \\ &= \Pr(\Omega < z) \end{aligned}$$

식(12)에서 $a_1 = P$, $a_2 = \kappa^2 P$, $a_3 = N_0$, $g_{SD} = x$, $g_{SE} = y$ 그리고 $\Omega = a_1 x / a_2 x + a_3$, $z = a_1 y / a_2 y + a_3$ 이다. 랜덤변수 X, Y에 대한 확률분포는 식(10), 식(11)과 같다. 이를 이용하여 $F_\Omega(z)$를 구하면 다음과 같다.

$$\begin{aligned} F_\Omega(z) &= \Pr(\Omega < z) \quad (13) \\ &= \Pr\left(\frac{a_1 x}{a_2 x + a_3} < z\right) \\ &= \Pr\left(x < \frac{a_3 z}{a_1 - a_2 z}\right) \end{aligned}$$

$$= \begin{cases} F_X\left(\dfrac{a_3 z}{a_1 - a_2 z}\right) & , 0 \le z < \dfrac{a_1}{a_2} \\ 1 & , z \ge \dfrac{a_1}{a_2} \end{cases}$$

a_1, a_2, a_3 는 양수 이다. 그리고 z는 양의 랜덤변수 이다. $a_1 - a_2 z \le 0$인 경우만 $F_\Omega(z)$이 성립하게 된다.

식(13)을 이용하여 식(12)을 전개하면 식(14)과 같다.

$$\begin{aligned} P_{IP} &= \int_{a_1/a_2}^{\infty} f_Y(y)dy + \int_0^{a_1/a_2} F_X\left(\frac{a_3 z}{a_1 - a_2 z}\right) f_Y(y)dy \quad (14) \\ &= \int_{a_1/a_2}^{\infty} \frac{1}{\lambda_Y}\exp\left(-\frac{y}{\lambda_Y}\right)dy \\ &+ \int_0^{a_1/a_2} \frac{1}{\lambda_Y}\exp\left(-\frac{y}{\lambda_Y}\right)dy \\ &- \int_0^{a_1/a_2} \frac{1}{\lambda_Y}\exp\left(-\frac{y}{\lambda_Y}\right) \\ &\times \exp\left(-\frac{1}{\lambda_X}\left(\frac{a_3(\frac{a_1 y}{a_2 y + a_3})}{a_1 - a_2(\frac{a_1 y}{a_2 y + a_3})}\right)\right)dy \end{aligned}$$

적분은 다음과 같은 성질을 갖는다.

$$\int_a^b f(x)dx + \int_b^c f(x)dx = \int_a^c f(x)dx \quad (15)$$

따라서, 위 성질을 이용하여 식(14)을 정리하면 다음과 같다.

$$\begin{aligned} P_{IP} = & \int_0^{\infty} \frac{1}{\lambda_Y}\exp\left(-\frac{y}{\lambda_Y}\right)dy \quad (16) \\ & - \int_0^{a_1/a_2} \frac{1}{\lambda_Y}\exp\left(-\frac{y}{\lambda_Y}\right)\exp\left(-\frac{y}{\lambda_X}\right)dy \end{aligned}$$

식(16)를 [13, Eq.(3.310)], $\int_0^{\infty} p e^{-px}dx = 1$,을 이용하여 계산하면 다음과 같다.

$$P_{IP} = 1 - \frac{\lambda_X}{\lambda_X + \lambda_Y}\left(1 - \exp\left(\frac{\lambda_X + \lambda_Y}{\kappa^2 \lambda_X \lambda_Y}\right)\right) \quad (17)$$

식(17)이 제안된 시스템 모델에서 도청채널의 채널용량이 메인채널의 채널용량보다 큰 경우 P_{IP}의 Closed-Form Expression이다.

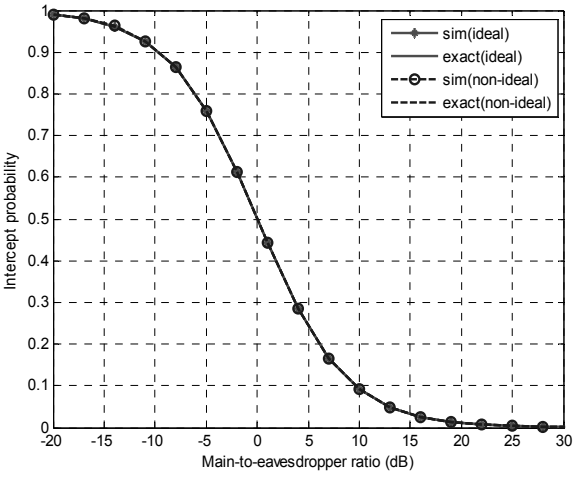


그림 3. 다른 노드모델에서 MER 증가에 따른 인터셉터 확률 P_{IP}의 변화

Fig. 3. Intercept probability P_{IP} versus the MER at different node model.

Ⅳ. 성능평가

본 장에서는 논문에서 제안한 시스템 모델의 성능평가를 위하여 시뮬레이션 결과와 Ⅲ장에서 얻은 수학적 모델의 Closed-Form Expression을 비교하여 성능 평가한다. 또한, 시뮬레이션의 신뢰도를 높이기 위해서 Monte-Carlo 방법을 통하여 시뮬레이션의 신뢰성을 확보하였다. 그리고 다양한 측면에서 시뮬레이션을 하여 물리계층보안에 미치는 영향을 확인한다.

그림 3은 노드가 이상적인 노드와 불완전한 노드인 경우, 메인채널과 도청채널의 전송파워 비율(Main-to-eavesdropper ratio/MER)이 증가함에 따른 P_{IP}의 변화를 보여준다. MER이 증가함에 따라 P_{IP}은 줄어드는 것을 알 수 있다. 식(17)에 의하면 κ는 P_{IP}에 영향을 미친다. 하지만 실제 $\exp(-\lambda_X + \lambda_Y/\kappa^2\lambda_X\lambda_Y)$의 계산 값이 너무 작아서 그림 3에서는 변화가 나타나지 않는다. 하지만, Closed-Form Expression에 의해서 P_{IP}에 κ가 영향을 미침을 확인 하였다.

그림 4는 도청자노드(E)의 CSI의 정확성 ρ가 다를 때, MER이 증가함에 따른 P_{IP}변화에 미치는 영향을 보여준다. MER이 증가함에 따라 IP는 점점 감소한다. 하지만 ρ가 변함이 P_{IP}는 변하지 않는다. 그림 4를 통하여 E의 CSI의 정확성 ρ가 P_{IP}에 영향을 미치지 않는다는 것을 알 수 있다.

그림 5는 이상적인 노드와 불완전한 노드인 경우,

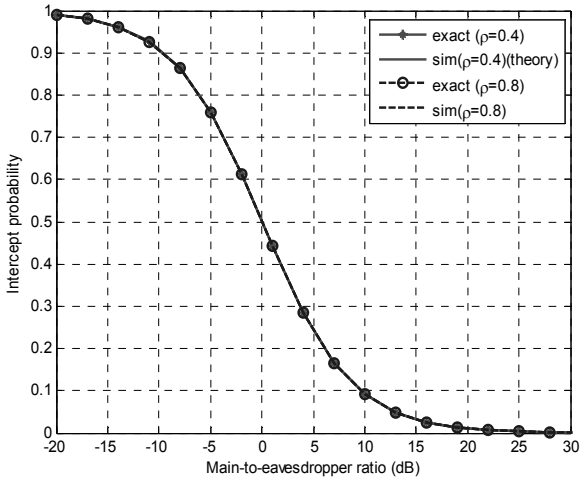


그림 4. 다른 ρ에서 MER 증가에 따른 인터셉터 확률 P_{IP}의 변화

Fig. 4. Intercept probability P_{IP} versus the MER at different values of ρ.

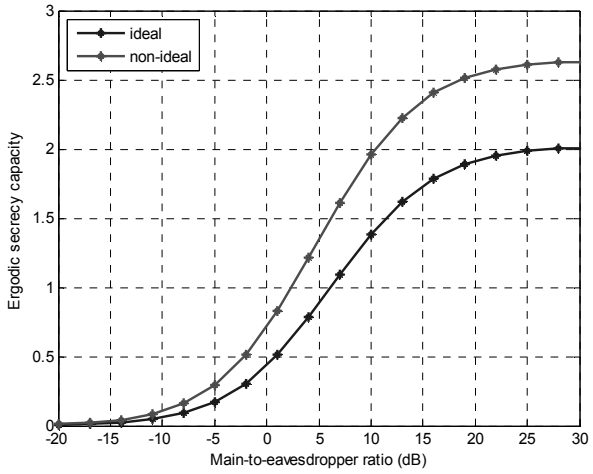


그림 5. 다른 노드모델에서 MER 증가에 따른 에르고딕 시크리스 용량의 변화

Fig. 5. Ergodic secrecy capacity versus the MER at different node model.

MER 변화에 따른 에르고딕 시크리스 용량(Ergodic secrecy capacity)의 변화를 나타낸다. MER이 증가함에 따라 에르고딕 시크리스 용량이 증가한다. 하지만 불완전한 경우의 에르고딕 시크리스 용량이 이상적인 경우의 에르고딕 시크리스 용량보다 낮다. 따라서 하드웨어 왜곡이 에르고딕 시크리스 용량을 감소시키는 요인이라는 것을 알 수 있다.

그림 6은 도청자노드(E)의 CSI의 정확성 ρ가 다를 때, MER이 에르고딕 시크리스 용량(Ergodic secrecy capacity)에 미치는 영향을 보여준다. MER이 증가함에 따라 에르고딕 시크리스 용량은 증가한다. 반면, ρ가

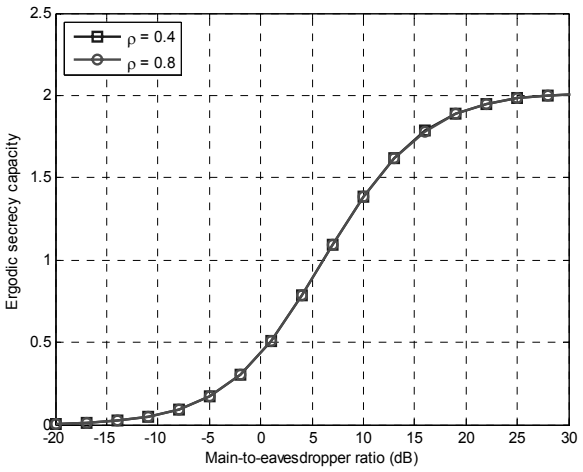


그림 6. 다른 ρ에서 MER이 증가함에 따른 Ergodic secrecy capacity의 변화

Fig. 6. Ergodic secrecy capacity versus the MER at different values of ρ.

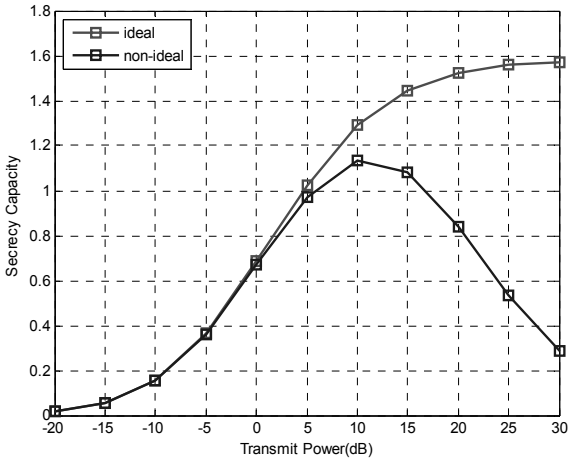


그림 7. 다른 노드모델에서 전송파워 증가함에 따라 보안채널용량 변화

Fig. 7. Secrecy capacity versus the transmit power at different node model.

변함에 따라 에르고딕 시크리스 용량은 변하지 않는다. 그림 6을 통하여 E의 CSI의 정확성 ρ가 에르고딕 시크리스 용량에 영향을 미치지 않는다는 것을 알 수 있다.

그림 7은 이상적인 노드와 불완전한 노드인 경우, 전송파워 P가 증가함에 따라 보안채널용량의 변화를 보여준다. 이상적인 노드의 경우, 보안채널용량이 계속 증가한다. 하지만 불완전한 노드의 경우, 보안채널용량이 10dB까지는 증가하지만 이후에는 감소한다. 이것은 불완전한 노드의 경우, SNR이 계속 증가하지 않고 κ의 영향을 받아서 어느 시점에서는 다시 감소하여 그림 7과 같이 된다는 것을 알 수 있다.

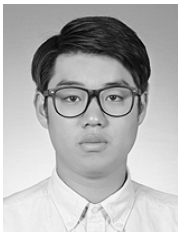
V. 결 론

본 논문에서는 기존의 연구들과 달리 실제와 유사한 환경에서의 물리계층보안에 대하여 연구하였다. 즉, 노드모델은 불완전하여 전송할 때 신호의 왜곡이 발생한다. 그리고 도청자노드는 자신의 채널상태정보를 주변노드와 공유하지 않는다. 따라서 조력노드가 제공하는 채널상태정보를 이용하여 도청자노드의 채널상태정보를 불완전하게 유추한다. 이러한 요소들이 물리계층보안에 어떠한 영향을 미치는지를 여러 가지 시뮬레이션을 통하여 확인하였다. 특히, 인터셉트 확률에 대한 Closed-Form Expression을 구하였다. 불완전한 채널상태정보는 인터셉트확률에 영향을 주지 않지만, 불완전한 노드모델은 인터셉트 확률에 영향을 주는 것을 Closed-Form Expression을 통하여 확인하였다. 불완전한 노드모델은 인터셉트 확률 이외에도 에르고딕 시크리스 용량에도 영향을 주어서 완전한 노드모델과의 에르고딕 시크리스 용량을 비교하면 불완전한 노드모델이 낮은 에르고딕 시크리스 용량을 보이는 것을 확인하였다. 그리고 보안채널용량도 완전한 노드 모델은 계속 증가하는 반면, 불완전한 노드 모델은 증가하다가 다시 감소한다. 이처럼 불완전한 노드 모델은 시스템에 많은 영향을 미친다. 따라서 불완전한 노드 모델에 대한 다양한 측면의 연구가 필요하다. 본 논문에서는 소스노드와 목적지노드 그리고 도청자노드가 존재하는 단순한 시스템 모델에서 시뮬레이션과 수학적 모델을 비교하였다. 현재 본 연구진들은 다중릴레이, 다중도청자가 존재하는 시스템처럼 더 복잡하고 현실적인 시스템 모델에서 불완전한 노드 모델이 미치는 영향에 대한 연구를 진행하고 있다.

REFERENCES

[1] Shannon, C.E., “Communication theory of secrecy systems,” The Bell System Technical Journal, vol.28, no.4, pp.656-715, October 1949.
[2] Wyner, A.D., “The wire-tap channel,” The Bell System Technical Journal, vol.54, no.8, pp.1355-1387, October 1975.
[3] N. T. Do and B. An, “Secure transmission using decode-and-forward protocol for underlay cognitive radio networks,” Proc. of IEEE ICUFN2015, pp. 914 - 918, Sapporo, Japan, July 2015.
[4] K. Shim, N. T. Do, B. An, S. Nam, “Outage performance of physical layer security for multi-hop underlay cognitive radio networks with imperfect channel state information,” Proc.of ICEIC 2016, Danang, Vietnam, January 2016.
[5] Yulong Zou, Xianbin Wang, Weiming Shen, “Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks,” IEEE Journal in Selected Areas in Communications, vol.31, no.10, pp.2099-2111, October 2013.
[6] Vo Nguyen Quoc Bao, Linh-Trung N., Debbah M., “Relay Selection Schemes for Dual-Hop Networks under Security Constraints with Multiple Eavesdroppers,” IEEE Transactions in Wireless Communications, vol.12, no.12, pp.6076-6085, December 2013.
[7] Alotaibi E.R., Hamdi K.A., “Secrecy outage probability of relay networking in multiple destination and eavesdropper scenarios,” Proc. of IEEE WCNC2014., pp.2390-2395, April 2014.
[8] Alves, H., Souza, R.D., Debbah, M., Bennis, M., “Performance of Transmit Antenna Selection Physical Layer Security Schemes,” IEEE in Signal Processing Letters, vol.19, no.6, pp.372-375, June 2012.
[9] Y. Choi and D. Kim, “Performance analysis with and without torch node in secure communications,” Proc. of ATC2015, Hanoi, Vietnam, October 2015.
[10] Bjornson Emil, Matthaiou Michail, Debbah Merouane, “A New Look at Dual-Hop Relaying: Performance Limits with Hardware Impairments,” IEEE Trans. Communications, vol.61, no.11, pp.4512-4525, November 2013.
[11] Harri Holma, Antti Toskala, “LTE for UMTS: Evolution to LTE-Advanced, 2nd Edition,” Wiley, 2011.
[12] Suraweera H.A., Smith P.J., Shafi M., “Capacity Limits and Performance Analysis of Cognitive Radio With Imperfect Channel Knowledge,” IEEE Transactions in Vehicular Technology, vol.59, no.4, pp.1811-1822, May 2010.
[13] I. S. Gradshteyn, I. M. Ryzhik, A. Jeffrey, D. Zwillinger, “Table of integrals, series and products(7th ed),” Elsevier, 2007.

저 자 소 개



심 규 성(학생회원)

2012년 홍익대학교 컴퓨터정보통신공학과 (B.S)

2015년～현재 홍익대학교 스마트도시과학경영대학원 정보시스템전공 재학

<주관심분야: Wireless Networks, Mobile Ad-hoc sensor Networks, Cognitive Radio Networks, Physical Layer Security>

도 트리 뉴(학생회원)

2012년 Posts and Telecommunications Institute of Technology(PTIT), Ho Chi Minh City (B.S)

2015년 홍익대학교 대학원 전자전산공학과 (M.S)

2015년～현재 홍익대학교 대학원 전자전산공학과 (Ph.D candidate)

<주관심분야: Wireless Communications, Cognitive Radio, Physical Layer Security, Wireless Energy Harvesting>

안 병 구(평생회원)

1988년 경북대학교 전자공학과 (B.S)

1996년 (미)New York University(Polytechnic), Dept. of Computer and Electrical Eng., NY, USA (M.S)

2002년 (미)New Jersey Institute of Technology (NJIT), Dept. of Computer and Electrical Eng., NJ, USA (Ph.D)

1989년～1994년 포항산업과학기술연구원(RIST), 선임연구원

2012년 대한전자공학회 컴퓨터소사이어티 회장

2003년～현재 홍익대학교 컴퓨터정보통신공학과 교수

<주관심분야: Mobile Wireless Networks, Ad-hoc & Sensor Networks, 5G Networks, IoT, Mobile Cloud Computing, Multicast Routing, QoS Routing, VLC, Cognitive Radio Networks, Energy Harvesting, Physical Layer Security, Cross-Layer Technology, Network Coding, Cooperative Communication, Bioinformatics>