JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 21, No. 6 : 1100~1105 Jun. 2017

셀룰러 망 통신보안을 위한 D2D 통신 송신전력 제어 기법

이기송[1] · 홍준표[2*]

Device-to-Device Communication Power Control Technique for Ensuring Communication Security of Cellular System

Kisong Lee[1] · Jun-Pyo Hong[2*]

[1]Department of Information and Telecommunication Engineering, Kunsan National University, Gunsan, 54150, Korea
[2*]Department of Information and Communications Engineering, Pukyong National University, Busan, 48513, Korea

요 약

본 논문에서는 셀룰러 통신과 D2D (device-to-device)통신이 같은 주파수를 통해 이루어지는 이기종 네트워크(heterogenous network)에서 셀룰러 망의 보안통신을 돕기 위한 D2D 통신 디바이스의 전력제어 기법을 제안하고 성능을 살펴본다. 기존의 보안통신이 고려되지 않은 이기종 네트워크에서는 D2D통신 신호가 간섭으로 작용하여 셀룰러 통신 성능에 악영향을 미쳤으나 도청자를 고려한 보안통신에서는 D2D통신 신호가 도청자의 신호수신을 방해하여 보안 전송률 성능 향상에 도움이 될 수 있다. 본 연구에서는 셀룰러 망의 보안통신 요구치를 만족시키며 D2D 통신 전송률을 극대화 시킬 수 있는 새로운 전력제어 기법을 제안하고 최적화 문제를 통해 최적 송신 전력의 closed-form 표현을 도출하였다. 또한 시뮬레이션을 통해 제안기법의 성능 특성을 확인하였다.

ABSTRACT

In this paper, we propose a power control technique for D2D communication in the heterogenous network consisting of cellular and D2D communication systems. Although the transmit signal of D2D communication degrades the performance of cellular system by interfering the signal reception at CU in the conventional heterogenous networks without eavesdroppers, it can be utilized as jamming signal for preventing other devices from recovering the transmitted information if there are eavesdroppers in the network. The proposed power control technique maximizes the achievable rate of D2D communication while ensuring the target security performance of cellular communication system. Through simulation results, we validate the analysis results and compare the performance with the conventional D2D communication scheme that utilizes its full transmit power for maximizing the achievable rate regardless of the performance of cellular system.

키워드 : 단말간 통신, 이기종 네트워크, 보안 전송률, 아웃티지 확률, 사물 인터넷

Key word : D2D communication, Heterogeneous network, Secrecy rate, Outage probability, Internet-of-Things

Received 23 April 2017, **Revised** 25 April 2017, **Accepted** 30 April 2017

* **Corresponding Author** Jun-Pyo Hong (E-mail:jp_hong@pknu.ac.kr, Tel:+82-51-629-6227)
Department of Information and Communications Engineering, Pukyong National University, Busan, 48513, Korea

Open Access https://doi.org/10.6109/jkiice.2017.21.6.1100 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

최근 스마트 기기의 등장과 통신 기술의 발달이 사물 인터넷(Internet-of-Things)의 실현을 가속화하고 있다. 사물 인터넷의 발달은 우리의 생활을 더 편리하게 할 것으로 예상되지만, 허용되지 않은 사용자에게 개인의 정보가 유출되는 정보 보안(Security) 문제에 대한 사회적 우려도 함께 커지고 있다[1,2]. 도청자가 존재하는 경우, 보안 전송률(Secrecy rate)은 송신기와 수신기 사이의 데이터 전송률과 송신기와 도청자 사이의 데이터 전송률의 차로 정의될 수 있으며[3], 이러한 보안 전송률을 향상시키기 위한 방법으로써 물리계층 보안(Physical layer security)에 관한 연구가 활발히 진행되고 있다[4-7]. 보안 전송률을 향상시키기 위한 가장 효과적인 방법 중 하나는 협력적 잡음(Cooperative jamming)을 이용하여 도청자의 통신정보 해석을 방해하는 것이다. [4]에서는 다수의 릴레이가 존재하는 분산 네트워크에서 협력적 잡음을 생성하기 위한 빔포밍 벡터(Beamforming vector)를 최적화하는 연구를 수행하였다. [5]에서는 보안 전송률 향상을 위해 수신기가 잡음을 생성하는 환경에서 보안 아웃티지 확률(Secrecy outage probability)을 최소화하기 위한 잡음 전력 조절 기법을 제안하였다. [6]에서는 송신기와 수신기 사이에 존재하는 노드를 릴레이로 활용할 것인지 잡음 생성하는 jammer로 사용할 것인지를 선택하는 기준을 제안하였다. 또한, 셀룰러 망(Cellular network)과 단말간 통신망(Device-to-device communication, D2D)이 함께 존재하는 이기종 네트워크(Heterogeneous network)에서 셀룰러 망의 보안 전송률을 향상시켜주기 위한 협력적 D2D 통신 기법에 대한 연구도 진행 되었다[7].

본 논문에서는 셀룰러 망과 D2D 통신망이 혼재하는 이기종 네트워크에서 셀룰러 망의 정보를 엿듣고자 하는 도청자가 존재하는 환경을 고려하였다. 본 시스템에서 D2D 디바이스 간의 전송되는 신호는 도청자에게 잡음으로 작용하여, 셀룰러 망의 정보를 보호하는데 도움을 줄 수 있다. D2D 디바이스가 도청자와 관련된 무선 채널의 채널 상황 정보(CSI: Channel State Information)의 확률적 분포만을 알고 있는 상황에서, 셀룰러 망의 통신 보안 요구량을 보장해주며 D2D 통신의 전송률을 극대화할 수 있는 최적의 D2D 전력 할당 비율을 도출하였다. 또한, 시뮬레이션을 통해 제안하는 분석의 정확성을 검증하고, 기존 방안과의 비교를 통해 정보 보안 측면에서 제안 방안의 우수성을 검증하였다.

Ⅱ. 시스템 모델

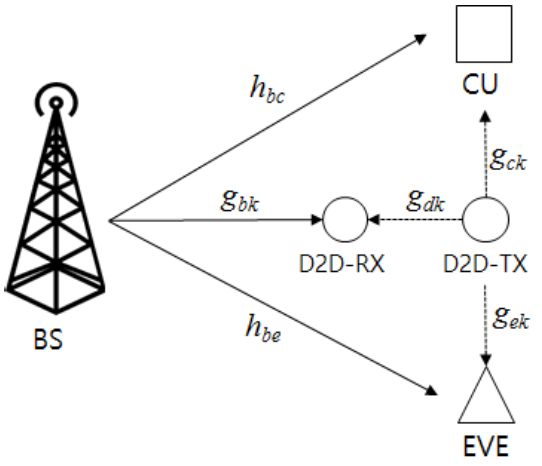

Fig. 1 System model for heterogenous networks

본 논문에서는 그림 1에서처럼 D2D 통신을 위한 D2D 송수신기 (Tx/Rx: Transmitter/Receiver), 셀룰러 망을 구성하기 위한 기지국(BS: Base Station)과 사용자(CU: Cellular User), 도청자(Eve: Eavesdropper)가 존재하는 이기종 네트워크를 고려한다. 셀룰러 망과 D2D 통신망은 같은 주파수 대역을 사용하며, Eve는 BS에서 CU로 전송되는 신호를 도청하고자 한다. 본 환경에서 D2D 디바이스 간에 전송되는 신호는 셀룰러 망에 간섭으로 작용하지만, 동시에 Eve에 잡음으로도 작용하여 Eve의 셀룰러 망 신호도청을 방해하는 역할을 한다. 이때 D2D-Tx의 송신 전력에 따라 D2D통신 신호가 셀룰러 망의 보안통신에 도움이 될 수도 있고 방해가 될 수도 있기 때문에, 셀룰러 망의 보안통신 성능을 어느 정도 보장시켜주며 D2D 통신 전송률을 극대화하는 D2D 송신전력 제어기법을 제안한다.

각각의 노드에는 단일 안테나가 장착되어 있으며, D2D-Tx-to-D2D-Rx, BS-to-CU, BS-to-Eve, BS-to-D2D-Rx, D2D-Tx-to-CU, D2D-Tx-to-Eve 간의 채널을 각각 h_{dk}, h_{bc}, h_{be}, g_{bk}, g_{ck}, g_{ek}로 정의한다. 각각의 채널은 λ의 평균을 갖는 지수 분포(Exponential distribution)

를 따른다고 가정한다. D2D-Tx는 협력 전송을 위하여 CU로부터 채널 피드백을 받아, h_{bc}와 g_{ck}에 대한 채널 정보를 얻을 수 있다. 또한, 채널 추정을 통해 g_{bk}와 h_{dk}에 대한 채널 정보 역시 얻을 수 있음을 가정한다. 그러나 Eve와 관련된 채널인 h_{be}와 g_{ek}에 대해서 D2D-Tx가 직접적으로 정확한 정보를 얻기 어려우므로, 채널 발생의 확률적 분포만 알고 있다고 가정한다. 또한, 각 노드에서의 수신 신호에는 $n \sim CN(0,\sigma^2)$의 동일한 Additive White Gaussian Noise(AWGN)이 존재한다고 가정한다.

D2D-Rx에서 수신되는 신호는 다음과 같이 표현 가능하다.

$$y_r = \sqrt{\alpha P} h_{dk} z + \sqrt{P_{BS}} g_{bk} s + n. \tag{1}$$

수식 (1)에서 P와 P_{BS} 는 각각 D2D-Tx와 BS의 전송 전력이며, z와 s는 각각 D2D-Tx와 BS가 전송하는 신호를 의미한다. 또한, α는 D2D-Tx의 전력할당 비율로써, $\alpha \in [0,1]$의 범위를 갖는다. 예를 들어 $\alpha = 1$일 때 D2D-Tx는 전체 전력을 사용하여 신호 z를 전송하고, $\alpha = 0$일 때는 전송을 멈춘다. z와 s는 $E[|z|^2] = E[|s|^2] = 1$의 정규화된 전력을 갖는다. D2D 통신망의 데이터 전송률은 수식 (2)와 같다.

$$R_{D2D} = \log_2\left(1 + \frac{\alpha P |h_{dk}|^2}{P_{BS}|g_{bk}|^2 + \sigma^2}\right). \tag{2}$$

CU에서 수신되는 신호와 셀룰러 망의 데이터 전송률은 각각 수식 (3)과 (4)와 같다.

$$y_c = \sqrt{P_{BS}} h_{bc} s + \sqrt{\alpha P} g_{ck} z + n. \tag{3}$$

$$R_C = \log_2\left(1 + \frac{P_{BS}|h_{bc}|^2}{\alpha P |g_{ck}|^2 + \sigma^2}\right). \tag{4}$$

반면, Eve에서 수신되는 신호와 데이터 전송률은 각각 다음 수식 (5)와 (6)과 같다.

$$y_e = \sqrt{P_{BS}} h_{be} s + \sqrt{\alpha P} g_{ek} z + n. \tag{5}$$

$$R_E = \log_2\left(1 + \frac{P_{BS}|h_{be}|^2}{\alpha P |g_{ek}|^2 + \sigma^2}\right). \tag{6}$$

CU에서 달성 가능한 보안 전송률은 다음과 같이 CU에서의 데이터 전송률과 Eve에서의 데이터 전송률의 차로 구할 수 있다.

$$\begin{aligned} R_S &= [R_C - R_E]^+ \\ &= \left[\log_2\left(1 + \frac{P_{BS}|h_{bc}|^2}{\alpha P |g_{ck}|^2 + \sigma^2}\right) - \log_2\left(1 + \frac{P_{BS}|h_{be}|^2}{\alpha P |g_{ek}|^2 + \sigma^2}\right)\right]^+ \\ &= [\log_2(1+\Gamma_C) - \log_2(1+\Gamma_E)]^+. \end{aligned} \tag{7}$$

수식 (7)에서 $[x]^+ = \max\{0, x\}$ 으로 정의된다. 따라서 0보다 큰 보안 전송률을 얻기 위해서는 Γ_C가 Γ_E보다 커야한다. 그렇지 않은 경우 R_S는 0이 되어 셀룰러 망의 통신 보안은 보장되지 않는다. 셀룰러 망의 통신 보안 요구량을 정의하기 위해, 보안 아웃티지 확률을 수식 (8)과 같이 나타낼 수 있다.

$$p_{out}(\alpha) = \Pr[\Gamma_C \le \Gamma_E]. \tag{8}$$

위의 수식을 통해서, 셀룰러 망의 보안 아웃티지 확률을 ϵ 이하로 보장해주면서 D2D 통신망의 데이터 전송률을 극대화하기 위한 전력할당 비율을 도출하는 최적화 문제를 다음과 같이 정의할 수 있다.

$$\begin{aligned} \max_{\alpha} \quad & R_{D2D} \\ s.t. \quad & C1: p_{out}(\alpha) \le \epsilon \\ & C2: 0 \le \alpha \le 1. \end{aligned} \tag{9}$$

Ⅲ. D2D 전력 조절 방안

3 장에서는 최적화 문제 (9)를 풀기 위한 최적의 전력할당 비율 α를 closed-form으로 찾고자 한다. 먼저, 제약조건 C1을 만족시키는 α의 값은 h_{bc}와 g_{ck}에 대한 CSI 정보 및 h_{be}와 g_{ek}의 확률 밀도 함수(PDF: Probability Density Function)를 이용하여 찾을 수 있다. 채널 정보를 기반으로 보안 아웃티지 확률은 다음의 수식과 같이 표현할 수 있다.

$$
\begin{aligned}
p_{out}(\alpha) &= \Pr\left[\frac{|h_{bc}|^2}{\alpha P|g_{ck}|^2+\sigma^2} \le \frac{|h_{be}|^2}{\alpha P|g_{ek}|^2+\sigma^2}\right] \\
&= \Pr\left[A \le \frac{|h_{be}|^2}{\alpha P|g_{ek}|^2+\sigma^2}\right] \\
&= \Pr\left[A\left(\alpha P|g_{ek}|^2+\sigma^2\right) \le |h_{be}|^2\right] \\
&= \int_0^\infty \Pr\left[|h_{be}|^2 \ge A\left(\alpha P x+\sigma^2\right) \| g_{ek}|^2 = x\right] \\
&\quad \bullet\, f_{|g_{ek}|^2}(x)dx \\
&= \int_0^\infty e^{-\frac{A(\alpha P x+\sigma^2)}{\lambda_{be}}} \bullet \frac{1}{\lambda_{ek}} e^{-\frac{x}{\lambda_{ek}}} dx \\
&= \frac{1}{\lambda_{ek}} e^{-\frac{A\sigma^2}{\lambda_{be}}} \int_0^\infty e^{-\left(\frac{A\alpha P}{\lambda_{be}}+\frac{1}{\lambda_{ek}}\right)x} \bullet dx \\
&= \frac{\lambda_{be} e^{-\frac{A\sigma^2}{\lambda_{be}}}}{\frac{|h_{bc}|^2}{|g_{ck}|^2}\lambda_{ek}+\lambda_{be}} \\
&\quad \frac{\frac{\sigma^2}{\alpha P}}{} \\
&\overset{(a)}{\approx} \frac{\lambda_{be}}{\frac{|h_{bc}|^2}{|g_{ck}|^2}\lambda_{ek}+\lambda_{be}} exp\left[-\frac{|h_{bc}|^2\sigma^2}{\left(\alpha P|g_{ck}|^2+\sigma^2\right)\lambda_{be}}\right].
\end{aligned}
\tag{10}
$$

수식 (10)에서 $A=\frac{|h_{bc}|^2}{\alpha P|g_{ck}|^2+\sigma^2}$ 이며, $f_{|g_{ek}|^2}(x)$는 채널 $|g_{ek}|^2$에 대한 PDF이다. 또한, 근사 관계 (a)는 σ^2이 충분히 작다는 high signal-to-noise ratio (SNR)의 가정에서 도출된 것이다.

수식 (10)에 의해 제약조건 C1은 다음 수식 (11)로 표현될 수 있다.

$$
\frac{1}{\alpha P|g_{ck}|^2+\sigma^2} \ge -\frac{\lambda_{be}}{|h_{bc}|^2\sigma^2}\log\left(\epsilon\left(\frac{|h_{bc}|^2}{|g_{ck}|^2}\frac{\lambda_{ek}}{\lambda_{be}}+1\right)\right). \tag{11}
$$

만약 $\epsilon > 1/\left(1+\frac{|h_{bc}|^2}{|g_{ck}|^2}\frac{\lambda_{ek}}{\lambda_{be}}\right)$를 만족한다면, 수식 (11)의 오른쪽 수식은 항상 0보다 작게 된다. 그에 따라 수식 (11)은 아래의 수식 (12)로 변환되고, 수식 (12)는 모든 α에 대해서 성립하게 된다.

$$
\alpha \ge -\frac{\sigma^2}{P|g_{ck}|^2}\left\{\frac{|h_{bc}|^2}{\lambda_{be}\log\left(\epsilon\left(\frac{|h_{bc}|^2}{|g_{ck}|^2}\frac{\lambda_{ek}}{\lambda_{be}}+1\right)\right)}+1\right\}. \tag{12}
$$

반면, $\epsilon \le 1/\left(1+\frac{|h_{bc}|^2}{|g_{ck}|^2}\frac{\lambda_{ek}}{\lambda_{be}}\right)$를 만족하면, 제약조건 C1을 만족하는 α의 범위는 수식 (13)과 같이 찾을 수 있다.

$$
\alpha \le \alpha_{out} = \left[-\frac{\sigma^2}{P|g_{ck}|^2}\left\{\frac{|h_{bc}|^2}{\lambda_{be}\log\left(\epsilon\left(\frac{|h_{bc}|^2}{|g_{ck}|^2}\frac{\lambda_{ek}}{\lambda_{be}}+1\right)\right)}+1\right\}\right]_0^1. \tag{13}
$$

수식 (13)에서 $[y]_0^1 = \min(\max(0,y),1)$이다. 즉, α의 값을 α_{out}보다 작은 값으로 설정하면 셀룰러 망의 보안 아웃티지 확률이 ϵ이하로 보장이 된다.

반면, D2D 통신망이 R_{D2D}를 최대화하기 위해서는 $\alpha=1$로 설정하여 전체 전력을 이용하여 신호를 전송하여야 한다. 그러므로 최적화 문제 (9)를 풀기 위한 최적의 α는 최종적으로 다음과 같이 구해질 수 있다.

$$
\alpha^* = \min(\alpha_{out}, 1). \tag{14}
$$

수식 (14)에서 $\alpha_{out} > 1$인 경우에는 D2D-Tx가 전체 전력을 사용하더라도 셀룰러 망의 통신 보안 요구량을 침해하지 않으므로, D2D 통신망의 데이터 전송률을 극대화하기 위해 $\alpha^*=1$로 설정하게 된다. 그 반대로 $\alpha_{out} \le 1$인 경우는 D2D-Tx가 전체 전력을 사용하면 셀룰러 망의 통신 보안 요구량을 침해하게 되므로 $\alpha^* = \alpha_{out}$으로 설정하게 된다.

Ⅳ. 시뮬레이션 결과

이번 장에서는 시뮬레이션 결과를 통해 앞장의 최적 전력할당에 대한 분석결과 정확성을 확인하고 제안 기법과 기존 D2D통신의 차이점을 살펴보도록 한다. 모든 시뮬레이션은 matlab을 통해 이루어졌으며 공통되는 시뮬레이션 환경은 다음과 같다. BS 송신전력 PBS = 30dBm, 잡음 전력 σ 2=-50dBm, 아웃티지 확률 제약 ε = 0.1, 경로감쇄지수 β=3, 기기들 사이 거리 dbc = 74m, dbk = 90m, dbe = 90m, dek = 2m, dck = 8.3m, dek = 4.9m을 고려한다. 각 채널 이득은 평균 λxy = dxy-β을 갖는 지수분포를 따른다. 즉, CU근처에서 도청을 시도하는 Eve와 이를 방해하는 D2D 통신 상황을 나타낸다.

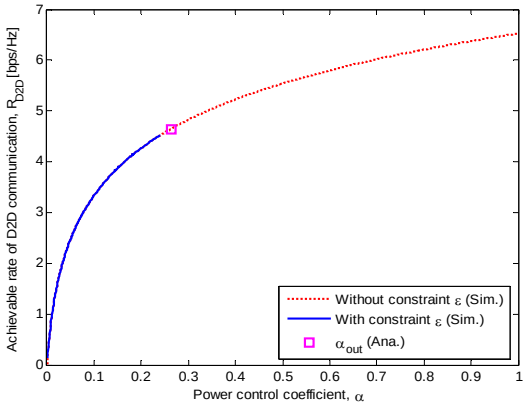

Fig. 2 Achievable rate of D2D communication versus power control coefficient

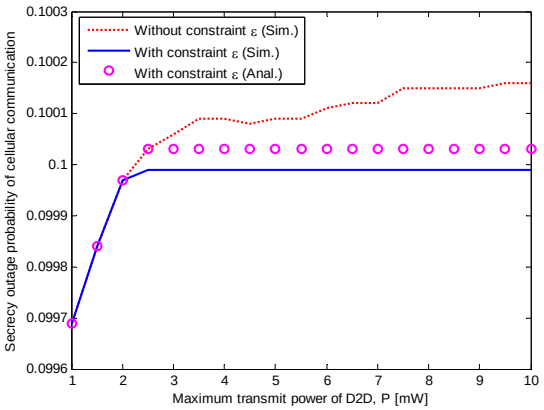

Fig. 4 Secrecy outage probability of cellular communication versus maximum transmit power of D2D communication

그림 2는 a값 변화에 따른 D2D 전송률을 보여주고 있다. D2D통신 최대 송신전력은 P=0dBm로 설정되었다. 점선은 셀룰러 망의 성능과는 상관없이 모든 a값에 대한 D2D 전송률을 보여준다. a값이 클수록 D2D 통신에 사용하는 전력이 많아지므로 전송률이 함께 증가하는 것을 볼 수 있다. 실선은 셀룰러의 보안성능을 고려했을 때 선택 가능한 a값과 그에 해당하는 전송률을 나타낸다. 본 실험 환경에서는 a=0.3이상부터는 셀룰러 시스템에 미치는 간섭의 영향으로 아웃티지 확률이 ε을 초과하게 되어 사용할 수 없다. 사각형은 전장의 분석결과 (14)를 나타낸 것이다. 실제 시뮬레이션 결과와 약간의 오차가 있는 것을 볼 수 있는데 이는 식(10)에서의 근사에 따른 것이다.

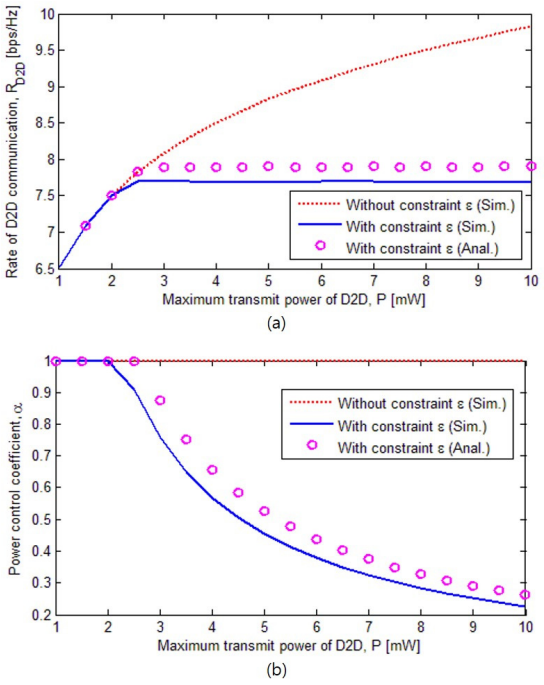

Fig. 3 D2D rate and power control coefficient versus maximum transmit power of D2D

그림 3은 D2D통신 최대 송신전력 변화에 따른 D2D 전송률(a)과 최적 a 값(b)의 변화를 보여주고 있다. 셀룰러 보안통신 성능을 고려하지 않을 경우 최대전력을 사용하는 것이 전송률을 최대화 시킬 수 있기 때문에 (b)의 붉은 선과 같이 항상 a=1이며, 전송률은 P가 증가함에 따라 함께 증가한다. 반면, 셀룰러 보안통신 성능을 고려할 경우, P 값이 작을 때는 a=1로 최대 전력을 사용하지만 P=2mW이후로는 셀룰러 보안통신 성능 보장을 만족시키기 위해 일정 수준으로 송신전력을 맞출 수 있도록 a 값이 점차 줄어든다. 이와 같은 고정된 송신전력 때문에 셀룰러 보안통신 성능을 고려할 경우는 D2D전송률이 P=2mW이후로 증가하지 않는다.

그림 4는 그림 3과 통일한 환경에서 셀룰러 통신의 보안 아웃티지 성능을 보여주고 있다. 제안된 기법은 설정된 제약 값 ε=0.1 이상으로 보안 아웃티지가 발생하지 않도록 하지만 기존 D2D 통신 기법은 P=2mW이후부터 셀룰러 보안통신 제약 값을 넘어서게 되는 것을 확인할 수 있다.

Ⅴ. 결 론

본 논문에서는 셀룰러 망과 D2D 통신망이 공존하는 이기종 네트워크 환경에서 셀룰러 망의 통신 보안 요구량을 보장하면서 D2D 통신망의 데이터 전송률을 극대화하기 위한 D2D통신 방안을 제안하였다. D2D 송수신기, 기지국, 셀룰러 사용자, 도청자가 존재하는 이기종 네트워크 환경을 수식적으로 모델링하고, 확률 분포 모델을 통해 최적의 전력할당 비율을 도출하였다. 시뮬레이션을 통해 제안하는 분석의 정확성을 검증하고, 기존 방안과의 비교를 통해 제안 방안이 셀룰러 망의 보안 및 D2D 데이터 전송률을 동시에 개선시킬 수 있음을 확인하였다.

ACKNOWLEDGMENTS

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. 2016R1C1B2012173).

This work was supported by the Pukyong National University Research Fund in 2015 (C-D-2015-1269)

REFERENCES

[1] X. Teng, J. B. Wendt, and M. Potkonjak, “Security of IoT systems: Design challenges and opportunities,” in *Proc. IEEE/ACM International Conference on Computer-Aided Design*, Nov. 2014, pp. 417-423.

[2] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, “Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios,” *IEEE Wireless Communications*, vol. 23, no. 5, pp. 60-67, Oct. 2016.

[3] S. K. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian wiretap channel,” *IEEE Transactiona on Information Theory*, vol. 24, pp. 451-456, July 1978.

[4] G. Zheng, L.-C. Choo, and K.-K. Wong, “Optimal cooperative jamming to enhance physical layer security using relays,” *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1317-1322, Mar. 2011.

[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 Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1741-1750, Sep. 2013.

[6] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, “Secure relay and jammer selection for physical layer security,” *IEEE Signal Processing Letters*, vol. 22, no. 8, pp. 1147-1151, Aug. 2015.

[7] Y. Wang, Z. Chen, Y. Yao, M. Shen, and B. Xia, “Secure communications of cellular users in Device-to-device communication underlaying cellular networks,” in 2014 Sixth *International Conference on Wireless Communications and Signal Processing. (WCSP)*, 2014.

이기송(Kisong Lee)

2009년 KAIST 전기및전자공학과 석사
2013년 KAIST 전기및전자공학과 박사
2013년~2015년 ETRI 융합기술연구소 연구원
2015년~현재 국립군산대학교 정보통신공학과 조교수
※관심분야 : Energy Harvesting Networks, Wireless Power Transfer, Self-Organizing Networks 등

홍준표(Jun-Pyo Hong)

2014년 KAIST 전기및전자공학과 박사
2014년~2015년 KAIST 전자정보연구소 연수연구원
2015년 ETRI 통신인터넷연구소 연구원
2015년~현재 국립부경대학교 정보통신공학과 조교수
※관심분야 : 정보통신 보안, 차세대 이동통신 시스템, wireless caching networks 등