https://doi.org/10.7840/kics.2023.48.10.1215

클러스터 기반 기기간 직접 통신을 위한 물리계층 보안 기술의 보안 전송률 분석

방 인 규•, 김 종 현*, 김 태 훈°

Secrecy Rate Analysis of Physical-Layer Security Technique for Cluster-Based D2D Communications

Inkyu Bang•, Jong-Hyun Kim*,
Taehoon Kim°

요 약

본 논문에서는 다수의 기기가 클러스터(cluster)를 형성하여 기기간 직접통신(device-to-device: D2D)을 통해 데이터를 전송하는 상황에서 인공잡음(artificial noise)을 활용하는 물리계층 보안(physical-layer security) 기법의 보안 전송률(secrecy rate)을 분석한다. D2D 클러스터는 클러스터 헤드(cluster head)와 클러스터 멤버들로 구성되며 클러스터 헤드는 클러스터 멤버들에게 데이터를 전송하는 역할을 수행한다. 본 연구에서는 두 개의 D2D 클러스터와 하나의 악의적 도청자로 구성된 네트워크 상황에서 하나의 D2D 클러스터 내의 데이터 전송의 보안성을 높이기 위해 또 다른 D2D 클러스터를 활용하는 방안을 제안한다. 또한 제안기법의 보안 성능의 근사치를 수학적으로 분석하고 이를 모의실험을 통해 검증한다.

Key Words : physical-layer security, artificial noise, device-to-device (D2D), secrecy rate, upper-bound

ABSTRACT

In this paper, we investigate and analyze the secrecy rate of an artificial noise-based physical-layer security technique for cluster-based D2D communications. D2D clusters consist of multiple devices including a cluster head in charge of broadcasting the data to other cluster members. We consider two D2D clusters and a single eavesdropper, where one D2D cluster generates artificial noise to enhance the secrecy of another D2D cluster. We derive an approximation of the secrecy rate and verify our analysis through simulations.

Ⅰ. 서 론

D2D (device-to-device) 통신은 4G 이동통신망에서부터 활용되고 있는 기기간 직접통신 기술로 그 활용도가 점차 증가하고 있으며, 5G를 넘어 6G 이동통신망에서는 더욱 활발히 활용될 것으로 기대되고 있다[1]. 예를 들어, D2D 통신은 6G의 다양한 주요 응용 서비스(스마트팩토리, 자율주행 등)를 지원하기 위한 핵심 통신기술의 역할을 수행할 것으로 예상된다. 그러나 다양한 형태의 기기가 D2D 통신을 사용할 경우, 예측할 수 없는 보안 위협이 발생할 수 있다[2]. 따라서 D2D 통신에서 보안 이슈는 D2D 통신의 활용도 증가와 함께 더욱 중요해지고 있으며 관련 연구가 필요한 상황이다.

다수의 기기가 클러스터를 형성하여 D2D 통신을 활용할 경우 주파수 자원을 효율적으로 사용할 수 있기 때문에 스마트 팩토리, 군집 차량 통신 등과 같이 다수의 기기가 활용될 것으로 예상되는 상황에서 클러스터 기반의 D2D 통신에 대한 연구가 많이 논의 되고 있다[3,4]. 일반적으로 D2D 클러스터는 하나의 클러스터 헤드(cluster head)와 다수의 클러스터 멤버(cluster member)로 구성되며 클러스터 헤드는 D2D 통신을 통해 클러스터 멤버들에게 데이터를 전송하는 역할을 수행한다. 무선 신호를 활용하는 D2D 통신은 잠재적인

※ 이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(No.2021-0-00796, 상시적 보안품질 보장을 위한 6G 자율보안 내재화 기반기술 연구, 기여율 50%)과 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2022R1F1A1076126, 기여율 50%).

• First Author : (ORCID:0000-0001-7109-1999) Hanbat National University, Department of Intelligence Media Engineering, ikbang@hanbat.ac.kr, 부교수, 정회원

° Corresponding Author : (ORCID:0000-0002-9353-118X) Hanbat National University Department of Computer Engineering, thkim@hanbat.ac.kr, 부교수, 정회원

* (0000-0002-5532-2117) Electronics and Telecommunications Research Institute, jhk@etri.re.kr, 책임연구원, 정회원

논문번호 : 202307-010-A-LU, Received July 12, 2023; Revised July 18, 2023; Accepted July 18, 2023

무선 도청(eavesdropping)의 가능성이 존재한다. 물리계층 보안(physical-layer security)은 무선 신호의 보안성을 정보이론 관점에서 연구하는 분야로 최근 D2D 통신, 차량 간 통신 등 다양한 네트워크 환경에서 이론적으로 무선 신호의 보안성을 개선하는 관련 연구가 진행되고 있다[3,4].

물리계층 보안에서는 인공잡음(artificial noise: AN)의 개념을 활용하여 무선 신호의 보안성을 높일 수 있다[5]. 인공잡음 기술은 물리계층 보안 관련 여러 연구에서 논의 되었으나, D2D 클러스터 기반의 네트워크 환경에서는 상대적으로 그 논의가 활발하지 않은 상황이다. 또한, 보안 전송률에 대한 수학적 분석은 무선통신 시스템 설계 시 무선 보안 기준을 설정하는 척도로 활용될 수 있으나, D2D 클러스터 기반의 네트워크 환경에서 이러한 분석이 미흡한 실정이다. 따라서 본 연구에서는 클러스터 기반 D2D 통신에서 인공잡음이 활용될 경우의 보안 전송률을 닫힌 형태로 유도하고 그 활용 가능성을 논의한다.

Ⅱ. 시스템 모델

본 논문에서는 그림 1과 같이 두 개의 D2D 클러스터(c_{data}, c_{AN})와 하나의 도청 기기가 존재하는 네트워크에서 하나의 D2D 클러스터(c_{data})에서만 데이터 전송이 발생하는 상황을 가정한다. 즉, c_{data}의 클러스터 헤드(d_0)는 클러스터 내의 N개의 클러스터 멤버들(d_n)에게 D2D 통신을 통해 데이터를 전송하며, c_{AN}의 $N+1$개의 기기(a_k)는 c_{data}의 D2D 통신 보안성을 높이기 위해 인공잡음을 생성한다. 모든 기기는 단일 안테나를 가정한다.

h_n과 h_e은 각각 d_0와 d_n 사이 그리고 도청 기기와 d_0 사이의 채널 계수를 의미한다. $g_{n,k}$과 $g_{e,k}$은 각각 d_n과 a_k 그리고 도청 기기와 a_k 사이의 채널 계수를 의미한다. 무선 채널 환경은 모든 채널 계수 h_n, h_e, $g_{n,k}$, $g_{e,k}$가 독립 가우시안 분포를 따르는 레일리(Rayleigh) 채널 모델을 가정하며, 분석의 편의를 위해 h_n, h_e의 평균 채널 이득은 σ_h^2, $g_{n,k}$와 $g_{e,k}$의 평균 채널 이득은 각각 σ_g^2와 σ_e^2으로 가정한다. 클러스터 내의 동일 데이터 전송(broadcasting)을 가정할 경우 d_n과 도청 기기에서의 데이터 전송률은 다음과 같다.

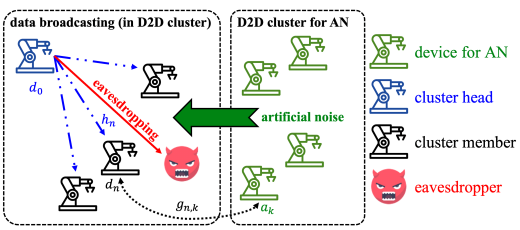

그림 1. 클러스터 기반 D2D 네트워크 모델($N=3$ 예시)
Fig. 1. A cluster-based D2D network(e.g., $N=3$)

$$R_d = \min_{n\in\{1,\cdots,N\}}\left\{\log_2\left(1+\frac{\| h_n \|^2}{\| \boldsymbol{G}_n\boldsymbol{u} \|^2\lambda_a+1/\rho_d}\right)\right\}, \quad (1\text{-}1)$$

$$R_e = \log_2\left(1+\frac{\| h_e \|^2}{\| \boldsymbol{G}_e\boldsymbol{u} \|^2\lambda_a+1/\rho_d}\right), \quad (1\text{-}2)$$

여기서 수식 (1-1)의 최솟값 연산자는 c_{data}의 N개의 클러스터 멤버에게 동일한 정보가 전송되는 것을 가정하기 때문에 포함된다. $\boldsymbol{u}=[u_1,\cdots,u_{N+1}]^T$는 c_{AN}의 각 기기(a_k)가 생성하는 인공잡음 계수(u_k)가 성분인 $(N+1)\times 1$ 벡터, λ_a는 인공잡음의 생성전력과 d_0의 전송전력의 비율, 그리고 ρ_d는 d_0의 신호 대 잡음비(signal to noise ration, SNR)이다. $\boldsymbol{G}_n$과 $\boldsymbol{G}_e$은 각각 $g_{n,k}$, $g_{e,k}$, $\forall k$이 성분인 $1\times(N+1)$ 채널 벡터이다. 따라서 평균 보안 전송률은 수식 (1-1)과 (1-2)을 이용하여 다음과 같이 정의할 수 있다.

$$R_s = E[\max(R_d - R_e, 0)]. \quad (2)$$

Ⅲ. D2D 클러스터 기반 인공잡음 생성 기법

c_{AN}을 통해 생성되는 인공잡음을 적절하게 설계할 경우 c_{data}의 D2D 통신에 대한 보안 전송률을 증가시킬 수 있다. 본 연구에서 c_{AN}의 각 기기(a_k)는 채널 추정을 통해 $g_{n,k}\forall n, \forall k$의 값을 측정할 수 있고 c_{AN}의 클러스터 헤드는 a_k로부터 측정된 채널 정보를 전달받는다고 가정한다. c_{AN}의 클러스터 헤드는 $N\times(N+1)$ 채널 계수 행렬 $\boldsymbol{G}=[\boldsymbol{G}_1^T,\cdots,\boldsymbol{G}_N^T]^T$에 대한 정보를 활용할 수 있다. 따라서 c_{AN} 클러스터는 영 공간(null space)의 개념을 활용하여 c_{data} 클러스터 내의 D2D 통신에 영향을 미치지 않는 인공잡음을 생성할 수 있으며, 이를 통해 향상된 보안 전송률을 달성할 수 있다[5]. 구체적인

보안 전송률 분석은 다음 장에서 논의한다.

Ⅳ. 보안 전송률 분석

c_{AN} 클러스터가 생성하는 인공잡음은 도청 기기에게만 영향을 미친다. 따라서 수식 (1-1)과 (1-2)의 간섭 신호는 각각 $\| \boldsymbol{G}_n \boldsymbol{u} \|^2 \lambda_a = 0$, $\| \boldsymbol{G}_e \boldsymbol{u} \|^2 \lambda_a \neq 0$으로 간주할 수 있으며, 수식 (2)는 $\max(R_d - R_e, 0)$의 특성을 반영하여 다음과 같이 계산할 수 있다.

$$\begin{aligned} R_s &= E[\max(R_d - R_e, 0)] \\ &= E[R_d - R_e | R_d \geqq R_e] \\ &= \int_1^{\infty} \log_2(z) f_Z(z) dz, \end{aligned} \tag{3}$$

수식 (3)에서 Z은 수식 (1-1)과 (1-2)의 $\min\{\| h_n \|^2\}$와 $\| h_e \|^2$을 각각 X와 Y으로 표기하고 $\beta = \dfrac{1}{\| \boldsymbol{G}_e \boldsymbol{u} \|^2 \lambda_a + 1/\rho_d}$ 값이 주어졌을 때, $Z = \dfrac{1+\rho_d X}{1+\beta Y}$으로 정의되는 확률 변수이다. 수식 (3)의 닫힌 형태 표현을 유도하기 위해서는 Z의 확률 분포 분석이 필요하며 Z의 누적분포함수(CDF) $F_Z(z)$은 다음과 같이 유도할 수 있다.

$$\begin{aligned} F_Z(z) &= \iint_{\text{domain}} \log_2\left(\frac{1+\rho_d x}{1+\beta y}\right) dx dy \\ &= 1 - \frac{\rho_d \sigma_h^2}{N\beta z \sigma_e^2 + \rho_d \sigma_h^2} e^{\frac{N}{\rho_d \sigma_h^2}(1-z)}. \end{aligned} \tag{4}$$

추가적으로 수식 (4)의 미분형태인 확률밀도함수(PDF) $f_Z(z)$을 이용할 경우 수식 (3)을 계산할 수 있다.[1] 여기서 인공잡음 생성 전력이 극대화되는 상황을 가정할 경우(즉, $\lambda_a \to \infty$) 수식 (3)의 닫힌 형태는 지수적분함수 $Ei(x) = -\int_{-x}^{\infty} \dfrac{e^{-t}}{t} dt$을 포함하는 형태로 다음과 같이 표현된다.

1) 수식 (3)의 일반적인 형태를 유도하는 것은 상당히 복잡하기 때문에 향후 새로운 연구주제로 다루도록 하며, 본 논문에서는 보안 전송률이 극대화되는 성능의 상한(upper bound)을 우선적으로 분석한다.

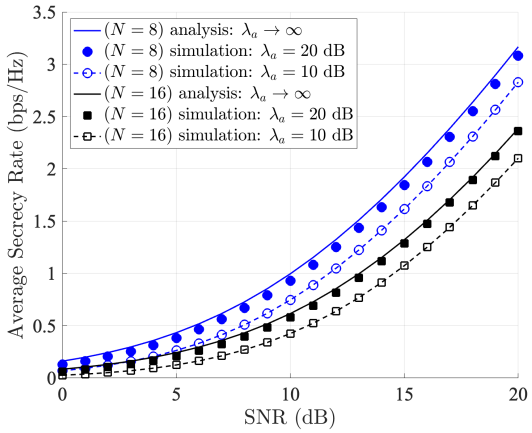

그림 2. SNR 변화에 따른 보안 전송률에 대한 수식 (5)와 모의실험 결과 비교
Fig. 2. Average secrecy rate of analysis results in (5) and simulation results for varying SNR

$$R_s = \frac{N}{\ln(2)\rho_d \sigma_h^2} Ei\left(\frac{N}{\rho_d \sigma_h^2}\right). \tag{5}$$

그림 2는 수식 (5)의 결과를 검증하기 위해 SNR 변화에 따른 분석결과와 모의실험 결과를 비교한 그래프이다. N값이 8과 16인 경우에 대해서 모의실험과 분석결과를 비교하였으며, 모의실험의 경우 λ_a 값은 10dB와 20dB의 값을 고려하였다. 수식 (5)은 λ_a 값이 큰 경우를 가정하기 때문에 모의실험에서 λ_a 값이 20dB인 경우가 10dB인 경우보다 수식 (5)의 분석결과와 더욱 일치하는 모습을 보이는 것을 확인할 수 있다.

Ⅴ. 결 론

본 논문에서는 인공잡음(artificial noise)을 활용하는 클러스터 기반(cluster-based) D2D 통신의 보안 전송률(secrecy rate)을 분석하고 성능의 상한(upper-bound)에 대한 닫힌 형태(closed-form)를 유도하였다. 본 논문의 분석결과는 D2D 기반의 무선 통신 시스템 설계에 활용될 수 있을 것으로 기대된다. 또한 본 연구의 분석을 확장하여 일반화하는 것은 향후 새로운 연구주제가 될 수 있을 것이다.

References

[1] P. Porambage, et al., “The roadmap to 6G security and privacy,” *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094-1122, May 2021.

(https://doi.org/10.1109/OJCOMS.2021.3078081)

[2] Trend Micro, "*With 5G coming, it's time to plug security gaps*," 2021. (www.trendmicro.com/en_us/research/21/g/with-5g-coming-its-time-to-plug-security-gaps.html)

[3] I. Bang, et al., "On the effect of malicious user on D2D cluster: CSI forgery and countermeasures," *IEEE ACCESS*, vol. 11, pp. 5517-5527, Jan. 2023. (https://doi.org/10.1109/ACCESS.2023.3236879)

[4] I. Bang, et al., "Physical-layer security for vehicular platooning networks: Artificial noise generation with optimal power allocation," *J. KICS*, vol. 47, no. 5, pp. 756-759, May 2022. (https://doi.org/10.7840/kics.2022.47.5.756)

[5] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless. Commun.*, vol. 7, no. 6, pp. 2180-2189, Jun. 2008. (https://doi.org/10.1109/TWC.2008.060848)