논문 22-47-05-08 The Journal of Korean Institute of Communications and Information Sciences '22-05 Vol.47 No.05
https://doi.org/10.7840/kics.2022.47.5.756

차량 군집주행 네트워크를 위한 물리계층 보안: 최적의 전력 할당을 통한 인공 잡음 생성

방 인 규◆, 김 종 현*, 김 태 훈°

Physical-Layer Security for Vehicular Platooning Networks: Artificial Noise Generation with Optimal Power Allocation

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

요 약

본 논문에서는 하나의 기지국, 다수의 차량으로 이루어진 두 개의 군집(platoon), 및 도청 차량이 존재하는 차량 군집주행 네트워크(vehicular platooning network)에서 기지국의 하향링크(downlink) 데이터 전송에 대한 보안 전송률을 분석하고 인공잡음(artificial noise) 기반의 물리계층 보안(physical-layer security) 기법을 제안한다. 제안기법은 하나의 군집 내의 모든 차량이 기지국으로부터 동일한 하향링크 데이터를 전송 받을 때, 다른 군집 내의 모든 차량이 인공잡음을 생성하도록 함으로써 보안 전송률을 높일 수 있다. 또한, 제안 기법은 인공잡음을 생성하는 전력을 최적화하여 보안 전송률 관점에서 추가적인 성능이득을 얻을 수 있다. 최종적으로 모의실험을 통해 제안기법의 성능을 다른 기법들과 비교 분석한다.

Key Words : physical-layer security, artificial noise, vehicular platooning network, secrecy rate, power control

ABSTRACT

In this paper, we propose an artificial noise-based physical-layer security technique to enhance the secrecy of downlink transmission in a vehicular platooning network that consists of one base station, two platoons, and one eavesdropping vehicle. We introduce a notion of artificial noise (AN) generation by the platoon and investigate an optimal power control for generating AN that can effectively maximize the secrecy rate. Through simulations, we evaluate the secrecy rate of our proposed schemes.

Ⅰ. 서 론

최근 이동통신 기술의 발전과 함께 차세대 이동통신망(6G)에서는 자율주행 기술이 대표 응용 애플리케이션으로 주목을 받고 있다[1]. 자율주행 관련 다양한 시나리오 중 군집주행(platooning)은 교통량, 도로 안전성 등 다양한 이점으로 인해 가까운 시기에 실생활에 적용될 것으로 예상되고 있다. 이를 위해 다양한 기술이 복합적으로 발전되어야 하며, 그 중 무선 통신 기술의 신뢰성과 보안성이 최우선적으로 확보되어야 한다.

다수의 차량이 군집을 형성하여 주행하고 있는 차량 군집주행 네트워크에서 차량 군집 주변의 익명의 차량은 잠재적 공격자(예: 도청자)로 간주될 수 있으며, 차량 군집은 여러 보안 위협에 노출될 수 있다. 그 중, 무선 신호의 전파 특성으로 인해 발생하는 무선 도청(eavesdropping) 위협에 대한 분석 및 연구는 무선통신의 물리계층 보안(physical-layer security) 분야의 주요 관심사이다. 최근 물리계층 보안 분야에서는 차량 네트워크를 포함하여 다양한 네트워크 환경에서 다중 안테나 기술 및 인공잡음(artificial noise, AN) 기술 등을 활용하여 보안 전송률(secrecy rate)을 높이고자하는 많은 연구가 진행되고 있다[2]. 또한, 이동통신망 사용자와 군집 차량을 동시에 고려하는 상황에서 보안 전송을 위한 최적의 자원 할당 방법 등이 연

※ 이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00796, 상시적 보안품질 보장을 위한 6G 자율보안 내재화 기반기술 연구).

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

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

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

논문번호 : 202201-004-A-LU, Received January 3, 2022; Revised February 22, 2022; Accepted February 26, 2022

구되고 있으나[3], 여전히 차량 네트워크에서 인공잡음과 함께 군집주행의 특성을 반영한 물리계층 보안 연구는 상대적으로 미흡한 실정이다.

본 연구에서는 차량 군집주행 네트워크에서 기지국의 하향링크(downlink) 데이터 전송에 대한 보안 전송률을 분석하고 인공잡음 기반의 물리계층 보안 기법을 제안한다.

Ⅱ. 시스템 모델

본 논문에서는 그림 1과 같이 하나의 기지국, 두 개의 차량 군집 및 하나의 도청 차량이 존재하는 차량 군집주행 네트워크를 가정한다. 각 차량 군집은 N대의 차량으로 구성되며 $\{v_1,\dots,v_N\}$과 $\{a_1,\dots,a_N\}$으로 표시한다. $\{v_1,\dots,v_N\}$ 군집은 군집 내의 모든 차량($v_n \forall n \in \{1,\dots,N\}$)이 기지국으로부터 동일한 하향링크 데이터를 전송 받는 군집이며, PRD (platoon receiving data)로 명명한다. $\{a_1,\dots,a_N\}$ 군집은 군집 내의 모든 차량($a_m \forall m \in \{1,\dots,N\}$)이 PRD의 보안 전송률을 높이기 위해 인공잡음을 생성하는 군집이며, PAN(platoon generating artificial noise)으로 명명한다.

h_n과 h_e은 각각 기지국과 PRD의 v_n 사이 그리고 기지국과 도청 차량 사이의 채널 계수를 나타낸다. 비슷하게, $g_{n,m}$과 $g_{e,m}$은 각각 PRD의 v_n과 PAN의 a_m 그리고 PAN의 a_m과 도청 차량 사이의 채널 계수를 나타낸다. 모든 채널 계수 h_n, h_e, $g_{n,m}$, $g_{e,m}$은 기존 연구에서 널리 활용되는 레일리(Rayleigh) 채널 모델

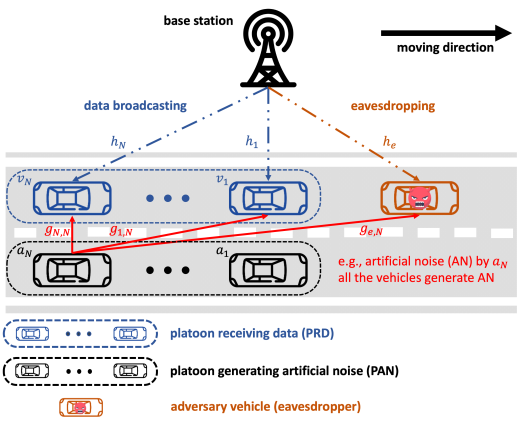

그림 1. 하나의 기지국과 두 차량 군집 및 하나의 도청 차량으로 구성된 차량 군집 네트워크 모델
Fig. 1. A vehicular platooning network consists of one base station, two vehicular platoons, and one eavesdropping vehicle

을 가정한다[3]. σ_n^2, σ_e^2, $\sigma_{n,m}^2$, $\sigma_{e,m}^2$은 각 채널 계수의 평균 채널 이득 값을 나타낸다. 단, 평균 채널 이득 값은 기지국과 차량 혹은 차량과 차량 사이의 거리에 영향을 받는다. 차량 통신을 위해 사용되는 주파수 대역에서 신호의 파장(wavelength) 길이는 차량과 기지국 혹은 차량 간 거리에 비해 충분이 짧기 때문에, 각 채널 계수 h_n, h_e, $g_{n,m}$, $g_{e,m}$은 서로 독립이라고 가정한다.[4]

보안 전송률(secrecy rate)은 합법적인 링크와 도청 링크의 데이터 전송률 차이로 정의된다[5]. 이때, 기지국으로부터 PRD의 차량과 도청 차량이 각각 받을 수 있는 최소의 하향링크 데이터 전송률은 다음과 같다.

$$R_v = \min_{n\in\{1,\cdots,N\}} \left\{ \log_2\left(1+\frac{\| h_n \|^2}{\| \boldsymbol{g}_n \boldsymbol{w} \|^2 \theta\lambda_a + 1/\rho_v}\right)\right\}, \tag{1-1}$$

$$R_e = \log_2\left(1+\frac{\| h_e \|^2}{\| \boldsymbol{g}_e \boldsymbol{w} \|^2 \theta\lambda_a + 1/\rho_v}\right), \tag{1-2}$$

여기서 수식 (1-1)은 N대의 차량에 동일한 정보가 전송되는 상황을 가정하기 때문에 최솟값 연산자를 포함한다. $\boldsymbol{w} = [w_1,\dots,w_N]^T$는 PAN의 각 차량($a_m$)이 생성하는 인공잡음 계수($w_m$)가 각 성분인 $N\times 1$ 벡터, $\theta\in[0,1]$은 PAN의 각 차량의 사용 가능한 최대 전력 대비 인공잡음 생성을 위한 전력 비율, λ_a는 기지국과 PAN 차량의 최대 전송 전력 비율, 그리고 ρ_v는 기지국의 하향링크 신호의 신호 대 잡음비(signal to noise ration, SNR)이다. 또한, $\boldsymbol{g}_n$과 $\boldsymbol{g}_e$은 각각 $g_{n,m}$, $g_{e,m}$, $\forall m$이 성분인 $1\times N$ 채널 벡터이다. 따라서 수식 (1-1)과 (1-2)의 차이로 정의되는 PRD의 보안 전송률은 다음과 같다.

$$R_s = \max(R_v - R_e, 0). \tag{2}$$

수식 (2)에서 R_v와 R_e는 $\boldsymbol{w}$와 θ의 함수가 되며, $\boldsymbol{w}$와 θ의 값을 결정하는 방법은 다음 장에서 구체적으로 논의한다. 수식 (1-1)과 (1-2)의 데이터 전송률 그리고 이를 토대로 정의된 수식 (2)의 보안 전송률은 패킷 길이가 매우 긴 경우에 달성 가능하다. 차량 통신 상황에서는 짧은 길이의 패킷 전송도 빈번히 일어나기 때문에 수식 (2)의 보안 전송률을 온전히 달성할 수 없다. 그러나 유한한 패킷 길이를 고려하더라도 무

한한 패킷 길이를 전송한 경우의 보안 전송률과 그 경향성은 비슷하기 때문에 본 논문에서는 수식 (2)의 보안 전송률을 우선적으로 고려한다[6]. 또한, 다수의 차량이 존재하는 경우 PRD와 가장 가까이 위치하는 차량을 도청 차량으로 생각하여 본 연구의 제안 기법을 적용할 수 있다.

Ⅲ. 군집 기반 인공잡음 생성 기법

보안 전송률을 높이기 위한 인공잡음 생성의 기본 원리는 데이터 링크에는 인공잡음의 영향을 최소화하면서 도청 링크에는 인공잡음이 그대로 영향을 받도록 하는 것이다[7]. 제안 기법은 PAN의 모든 차량이 인공잡음을 생성하도록 하여(즉, 군집 기반 인공잡음 생성 기법) PRD의 하향링크 데이터 수신에 대한 보안 전송률(즉, 수식 (2))을 증가시키는 것을 목표로 한다. PAN의 각 차량($a_m \forall m$)은 PRD의 차량이 기지국으로 상향링크 신호를 전송할 때 채널 측정을 통해 $g_{n,m} \forall n$의 값을 측정할 수 있다. 이 정보는 PAN의 선두 차량(lead vehicle)인 a_1에 보고되며(즉, a_1은 채널 계수 행렬 $\boldsymbol{G}=[\boldsymbol{g}_1^T,\ldots,\boldsymbol{g}_N^T]^T$에 대한 정보를 알 수 있다.), a_1은 각 차량에서 생성해야할 인공잡음의 계수를 결정한다. 참고로, 다른 노드(node)의 통신을 위해 인공잡음을 생성하는 방법은 물리계층 보안에서 지속적으로 논의되고 있는 개념이다[8]. 또한 PRD의 각 차량(v_n)은 기지국과의 채널 측정을 통해 h_n의 값을 측정하고 PRD의 선두 차량 v_1에게 보고한다. v_1은 수집된 h_n 정보를 PAN의 선두 차량 a_1에 보고한다. a_1은 h_n 정보를 PAN의 인공잡음 생성 및 인공잡음 생성 전력 최적화에 활용한다.

채널 행렬 $\boldsymbol{G}$의 영 공간(null space)의 개념을 활용하여 일부 PRD 차량의 데이터 링크에 영향을 미치지 않는 인공잡음을 생성할 수 있다. 그러나 PAN은 모든 차량이 단일 안테나를 장착하고 N대의 차량으로 구성되기 때문에 총 $N-1$대의 PRD 차량만이 인공잡음의 영향을 받지 않고 1대는 필연적으로 인공잡음의 영향을 받게 된다. 따라서 PAN에서 인공잡음을 생성할 때, 다음과 같이 채널 계수의 비율을 활용하여 인공잡음의 영향이 가장 적은 PRD의 차량을 선택하여 보안 전송률을 높일 수 있다.

$$n^* = \underset{n\in\{1,\cdots,N\}}{\arg\max}\left\{\frac{\| h_n \|^2}{\| \boldsymbol{g}_n \|^2}\right\}. \quad (3)$$

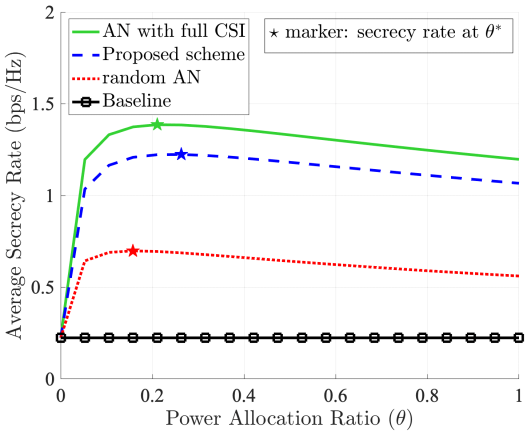

그림 2. 인공잡음 생성을 위한 전력할당 비율에 따른 평균 보안 전송률 비교($SNR=25dB$, $N=4$)
Fig. 2. Average secrecy rate for varying θ for AN generation ($SNR=25dB$, $N=4$)

따라서 $n=n^*$일 경우 PAN이 생성하는 인공잡음 계수는 다음과 같이 결정된다[6].

$$\boldsymbol{w}^* \in Null(\hat{\boldsymbol{G}}), \quad (4)$$

여기서 $\hat{\boldsymbol{G}}$은 채널 행렬 $\boldsymbol{G}$에서 $n=n^*$ 번째 행을 제거한 채널 행렬을 의미한다. 이 경우, $N-1$대의 PRD 차량은 $\| \boldsymbol{g}_n \boldsymbol{w}^* \|^2 = 0$의 결과를 얻기 때문에 수식 (1-1)은 $n=n^*$일 때 데이터 전송률과 같은 값이 된다. 더욱이 PAN의 차량은 인공잡음 생성 전력 θ을 최적화하여 인공잡음의 효과를 극대화 할 수 있다. 수식 (3)과 (4)를 기반으로 수식 (1-1)을 정리할 경우, 최적의 인공잡음 생성을 위한 전력 할당 비율을 다음과 같이 결정할 수 있다.(단, PAN의 모든 차량은 동일한 θ 값을 사용한다.)

$$\theta^* = \max_{\theta\in[0,1]}\left\{\log_2\left(1+\frac{\| h_{n^*} \|^2}{\| \boldsymbol{g}_{n^*}\boldsymbol{w}^* \|^2 \theta\lambda_a + 1/\rho_v}\right)\right\}. \quad (5)$$

Ⅳ. 성능 평가

제안 기법인 군집 기반의 인공잡음 생성 기법의 성능을 평가하기 위해 공격자에게 유리한 상황, 도청 차량이 PRD와 가까운 곳에 위치하지만 PAN으로부터는 먼 곳에 위치한 환경(즉, $\sigma_n^2 < \sigma_e^2$, $\sigma_{n,m}^2 > \sigma_{e,m}^2$)을 가정하였다. 또한 차량과 기지국 및 차량과 차량 사이의 상대적 거리에 따라 σ_n^2, σ_e^2, $\sigma_{n,m}^2$, $\sigma_{e,m}^2$의 값을 서로 연관성(correlated) 있게 설정하였다. 비교 기법

으로 다음의 3가지 기법을 고려하였다. ‘AN with full CSI’: 모든 채널 정보를 활용하여 인공잡음이 상쇄되지 않는 최적의 차량을 선택하는 기법, ‘random AN’: 인공잡음이 상쇄되지 않은 차량을 임의로 선택하는 기법, ‘Baseline’: 인공잡음을 사용하지 않고 데이터 전송을 하는 기본 전송 기법이다.

그림 2는 인공잡음 생성 전력 비율 θ값의 변화에 따른 평균 보안 전송률을 나타낸다. 우선, 인공잡음을 활용할 경우, 그렇지 않은 경우에 비해 보안 전송률이 크게 증가하는 것을 확인할 수 있다. 또한 제안 기법은 도청 차량의 채널 정보를 활용하지 않지만, AN with full CSI 기법과 근소한 성능 차이만 보이는 것을 확인할 수 있으며, 수식 (5) 기반의 최적의 θ^* 값에서 가장 큰 보안 전송률을 달성할 수 있는 것을 확인할 수 있다.

V. 결 론

본 논문에서는 차량 군집주행 네트워크에서 군집 기반의 인공잡음 생성과 인공잡음 생성 전력 최적화 방법을 제안하였다. 제안 기법은 한정적인 채널 정보를 사용하지만 상당히 우수한 보안 성능을 달성할 수 있다. 본 연구를 확장할 경우 군집주행의 다양한 특성을 반영한 물리계층 보안 연구 등을 새롭게 기대해 볼 수 있다.

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.

[2] I. Bang, et al., “Performance analysis of secure relaying protocol against an untrusted relay node in V2V networks,” *J. KICS*, vol. 46, no. 12, Dec. 2021.

[3] X. Peng, et al., “Security-aware resource sharing for D2D enabled multiplatooning vehicular communications,” *IEEE VTC2019-Fall*, Sep. 2019.

[4] T. S. Rappaport, *Wireless Communications: Principles and Practice*, Prentice Hall, 1996.

[5] M. Bloch and J. Barros, “Physical-layer security: From information theory to security engineering,” *Cambridge Univ. Press*, 2011.

[6] Z. Xiang, et al., “NOMA-Assisted secure short-packet communications in IoT,” *IEEE Wireless Commun.*, vol. 27, no. 46, pp. 8-15, Aug. 2020.

[7] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, Jun. 2008.

[8] I. Bang, et al., “Artificial noise-aided user scheduling from the perspective of secrecy outage probability,” *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7816-7820, Aug. 2018.