논문 21-46-12-11 The Journal of Korean Institute of Communications and Information Sciences '21-12 Vol.46 No.12
https://doi.org/10.7840/kics.2021.46.12.2180

차량 대 차량 네트워크에서 비신뢰 중계 노드에 대한 보안 중계 프로토콜의 성능 분석

방 인 규◆, 김 종 현*, 이 상 민**, 김 태 훈°

Performance Analysis of Secure Relaying Protocol Against an Untrusted Relay Node in V2V Networks

Inkyu Bang◆, Jong-Hyun Kim*, Sang-Min Lee**, Taehoon Kim°

요 약

본 논문에서는 차량 대 차량 네트워크에서 두 차량 사이의 데이터 전송을 위해 다른 임의의 차량이 중계 노드로 활용되는 상황을 가정하고, 이 때, 데이터 전송의 기밀성을 보장하는 보안 중계 프로토콜을 제안하고 성능을 분석한다. 제안 중계 프로토콜은 중계에 참여하는 임의의 차량을 온전히 신뢰할 수 없는 비신뢰(untrusted) 중계 노드로 가정하고, 보안 전송을 위해 인공잡음 및 간섭 제거(interference cancellation) 기술을 활용한다. 또한, 차량 네트워크의 무선 채널의 특성을 잘 나타내는 double Rayleigh 페이딩 모델을 가정하여 중계 프로토콜의 보안 성능을 분석한다. 최종적으로, 모의실험을 통해 다양한 환경에서 보안 중계 프로토콜의 성능을 보안 전송률 관점에서 평가한다.

Key Words : physical-layer security, V2V networks, untrusted relay, double Rayleigh fading, artificial noise

ABSTRACT

In this paper, we consider a relay-assisted vehicle-to-vehicle (V2V) networks, where an arbitrary relaying vehicle is assumed to be an untrusted relay node. To improve the secrecy performance of the relaying protocol, we propose a secure relaying protocol based on both artificial noise and interference cancellation techniques. We investigate our relaying protocol under double Rayleigh fading model and evaluate its secrecy performance through simulations in terms of secrecy rate.

Ⅰ. 서 론

5G 이동통신 기술은 증강현실·가상현실, 원격제어, 차량통신 등 높은 수준의 대역폭 및 지연시간을 요구하는 응용서비스를 본격적으로 지원할 수 있을 것으로 기대된다. 물리계층 보안(physical-layer security)은 각종 물리계층 기술과 무선 채널의 특성을 활용하여 무선 보안(wireless security)을 연구하는 분야이다. 차량통신 등과 같은 다양한 형태의 무선통신 기술이 일상생활에 더욱 밀접하게 보급될 것으로 예상되는 차세대(예: 6G) 통신 환경에서 물리계층 보안의 역할은 더욱 중요해질 것으로 예상된다[1].

최근 물리계층 보안 연구는 차량통신 네트워크, 중계 네트워크 등의 다양한 네트워크 환경에서 무선 도청을 가정하고 해당 시스템 모델의 보안 성능을 분석하는 연구가 주로 진행되고 있다[2-4]. 차량통신 네트워크에서 차량 대 차량 통신 상황을 가정할 경우, 송신·수신 차량 사이의 직접적인 무선 신호 전송이 어려운 상황(예: 고속도로)이 발생할 수 있다. 이 때, 송신·수신 차량 사이의 임의의 차량을 중계기로 활용할 경우 무선 신호를 성공적으로 중계할 수 있지만, 완전히 신뢰하기 어려운 (비신뢰) 중계 차량이 도청에 악용될 경우 심각한 보안 문제가 발생할 수 있다. 최근

※ 이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(No.2021-0-00796, 상시적 보안품질 보장을 위한 6G 자율보안 내재화 기반기술 연구, 기여율 50%)과 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2020R1F1A1069934, 기여율 50%).

◆ First Author : (ORCID:0000-0001-7109-1999) Hanbat National University Department of Information and Communication 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

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

** (ORCID:0000-0002-1298-7556) Electronics and Telecommunications Research Institute, sangm@etri.re.kr, 책임연구원

논문번호 : 202011-287-A-LU, Received October 15, 2021; Revised November 5, 2021; Accepted November 9, 2021

일부 물리계층 보안 연구는 비신뢰 중계 환경을 가정하고 있으나, 인공잡음 사용 및 채널 모델 가정이 차량통신 환경에 적합하지 않는 한계점이 있다[4]. 더욱이, 차량 간 비신뢰 중계 환경에서의 물리계층 보안 연구는 구체적으로 논의된 적이 없기 때문에 이 문제에 집중하고자 한다.

본 논문에서는 직접(direct) 무선 경로가 존재하지 않는 차량 대 차량 통신 환경에서 임의의 차량이 중계 노드로 활용되었을 때, 데이터 전송의 기밀성을 보장하는 보안 중계 프로토콜의 성능을 분석한다. 임의의 차량을 비신뢰 중계 노드로 가정하고, 보안 중계 프로토콜을 위한 인공잡음(artificial noise) 및 간섭 제거 기술의 활용 방안을 논의한다. 또한, 모의실험을 통해 보안 중계 프로토콜의 성능을 송신 차량(송신기)-중계 차량(중계기), 중계 차량(중계기)-수신 차량(수신기) 각 링크의 신호 대 잡음비(signal to noise ratio; SNR) 변화에 따른 보안 전송률 관점에서 평가했다.

Ⅱ. 시스템 모델

본 논문에서는 그림 1과 같이 직접 무선 경로가 존재하지 않는 차량 대 차량 통신 환경에서 임의의 차량이 중계 노드로 활용될 수 있는 차량 대 차량 중계 네트워크 모델을 가정한다. 논문에서는 임의의 차량을 비신뢰 중계 노드로 가정하고, 송신기(source), 비신뢰 중계기(relay), 수신기(destination) 역할을 하는 3대의 차량을 고려한다. 각 노드는 단일안테나를 장착했다고 가정한다. 송신기와 수신기 역할을 하는 차량 사이에는 1대 이상의 차량(즉, 비신뢰 중계기)이 존재하기 때문에 송신기와 수신기 사이에는 직접 무선 경로가 존재하지 않는다고 가정한다. 송신기와 중계기 그리고

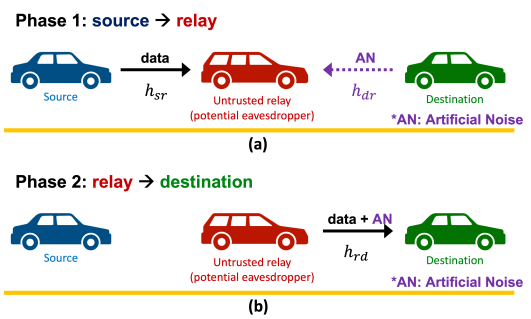

그림 1. V2V 네트워크에서 비신뢰 중계기에 대한 보안 중계 프로토콜: (a) 1단계(Phase 1), (b) 2단계(Phase 2)
Fig. 1. A secure relaying protocol against an untrusted relay node in V2V networks: (a) Phase 1, (b) Phase 2

중계기와 수신기 사이에는 직접 무선 경로가 존재한다고 가정한다. 비신뢰 중계기에 대한 정보 노출을 최소화하기 위한 보안 중계 프로토콜은 그림 1(a)와 그림1(b)와 같이 두 단계로 구성된다.

1단계(source → relay): 송신기는 중계기로 데이터를 전송한다. 동시에 수신기는 비신뢰 중계기의 도청 가능성을 줄이기 위해 임의잡음(random noise) 형태의 인공잡음(artificial noise)을 생성하고 전파한다. h_{sr}은 송신기와 중계기 사이의 채널 계수를 의미하고 h_{dr}은 수신기와 중계기 사이의 채널 계수를 의미한다.

2단계(relay → destination): 중계기는 전달 받은 데이터를 증폭하여(amplifying) 수신기에 전달한다. 중계기는 1단계에서 데이터와 인공잡음을 모두 수신했기 때문에 2단계에서는 데이터와 인공잡음이 증폭되어 전송된다. h_{rd}은 중계기와 수신기 사이의 채널 계수를 의미한다. 수신기는 파일럿 신호를 통해 h_{rd}을 추정할 수 있고 1단계에서 생성한 인공잡음 신호도 알고 있기 때문에 간섭 상쇄(interference cancellation) 기술을 이용하여 인공잡음의 효과를 제거할 수 있다. 단, 완벽하게 제거되지 않은 간섭은 잡음으로 모델링된다. 비신뢰 중계기 역시 간섭 상쇄 기술을 활용할 수 있지만 1단계에서 수신기가 전송한 인공잡음은 수신기만 알 수 있는 정보이다[5]. 따라서 비신뢰 중계기는 1단계에서 수신한 인공잡음을 제대로 제거할 수 없다.

채널 계수 h_X $(X \in \{sr, dr, rd\})$은 차량 대 차량 통신 환경에서 많이 쓰이는 채널 페이딩 모델을 가정하며 다음과 같이 표현된다[6].

$$h_X = \frac{g_X}{\sqrt{1+d^{\alpha}}}, \tag{1}$$

여기서 d는 차량 간 거리, α는 경로감쇄 지수(path-loss exponent)를 의미하며, g_X는 double Rayleigh 분포를 따르는 확률 변수이다. 또한 $|g_X|^2$의 확률 밀도 함수(probability density function; PDF)는 제 2종 변형 Bessel 함수이며 $f_{|g_X|^2}(x) = 2K_0(2\sqrt{x})$와 같이 표현된다.

Ⅲ. 보안 전송률 분석

중계 프로토콜의 1단계와 2단계에서 중계기와 수신기의 수신 신호 대 간섭 및 잡음비(signal to

interference plus noise ratio; SINR)는 각각 다음과 같이 계산할 수 있다[2].

$$\Gamma_R = \frac{|h_{sr}|^2 P_S}{\theta |h_{dr}|^2 P_D + \sigma_n^2}, \quad (2\text{-}1)$$

$$\Gamma_D = \frac{|h_{sr}|^2 P_S |h_{rd}|^2 P_R}{|h_{rd}|^2 P_R \sigma_n^2 + (\sigma_n^2 + \sigma_\epsilon^2)\left(|h_{sr}|^2 P_S + \theta |h_{dr}|^2 P_D + \sigma_n^2\right)}, \quad (2\text{-}2)$$

여기서, $\theta \in [0,1]$는 수신기가 생성하는 인공잡음의 전력 비율을 나타내고, σ_n^2은 가산 백색 가우시안 잡음(additive white Gaussian noise; AWGN)의 평균 전력 값을 나타낸다. σ_ϵ^2은 간섭 상쇄 과정 중에 발생하는 잔여 잡음을 나타낸다. P는 각 노드의 전송 전력을 의미하고 아래 첨자 S, R, D는 source, relay, destination을 대표한다.

보안 전송률은 수식 (2-1)과 (2-2)를 이용하여 최종적으로 다음과 같이 계산할 수 있다.

$$R_{\text{sec}}(\theta) = \left[\frac{\log_2(1+\Gamma_D(\theta))}{\log_2(1+\Gamma_R(\theta))} \right]^+, \quad (3)$$

여기서 $[x]^+ = \max\{x,0\}$을 나타내며 수식 (2)에 표현되어 있는 중계기와 수신기의 SINR은 θ의 함수로 표현되기 때문에 수식 (3)의 보안 전송률 역시 θ의 함수가 된다.

Ⅳ. 성능 평가

중계 프로토콜의 보안 성능 평가를 위해 차량들이 일렬로 주행하는 상황(예: 고속도로)을 가정하였다. 또한, 송신기와 비신뢰 중계기 그리고 중계기와 수신기 사이의 거리는 $d = 5m$로 동일하게 가정하고 $\alpha = 2.0$을 가정하였다.

그림 2는 제안 중계 프로토콜을 사용했을 때, 송신기-중계기, 중계기-수신기 각 링크의 신호 대 잡음비(signal to noise ratio; SNR) 변화에 따른 보안 전송률을 나타낸다. 보안 전송률이 높을수록 노란색으로 표시되며, 낮을수록 파란색으로 표시된다. 수신기에서 인공잡음 생성을 위한 전력 비율은 $\theta = 1$으로 설정하고 인공잡음을 제거하기 위한 간섭 상쇄의 잔여 잡음은 백색잡음과 같은 수준을 가정했다.(즉, $\sigma_\epsilon^2/\sigma_n^2 = 0\,dB$) 송신기-중계기의 SNR, 중계기-수신기의 SNR이 높아질수록 높은 보안 전송률을 달성할 수

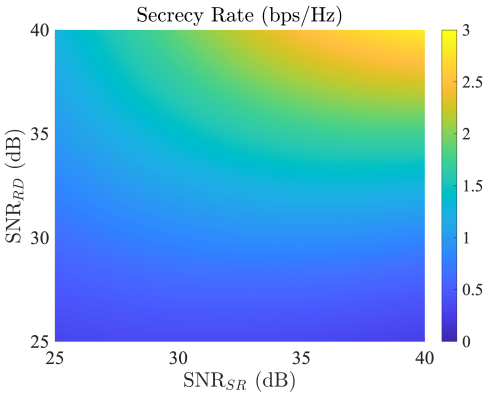

그림 2. 송신기-중계기, 중계기-수신기의 SNR 변화에 따른 제안 중계 프로토콜의 보안 전송률($\theta = 1, \sigma_\epsilon^2/\sigma_n^2 = 0\,dB$)
Fig. 2. Secrecy rate of proposed relay protocol when SNR varies and $\theta = 1, \sigma_\epsilon^2/\sigma_n^2 = 0\,dB$

있는 것을 확인할 수 있으며, 중계 프로토콜의 보안 전송률은 중계기-수신기의 SNR 변화에 좀 더 민감하게 반응하는 것을 확인할 수 있다.

그림 3은 중계 프로토콜의 1단계에서 수신기의 인공잡음 생성 전력의 비율에 따른 보안 전송률을 나타낸다. 송신기-중계기 및 중계기-수신기의 SNR은 각각 $25\,dB$와 $35\,dB$으로 설정하였다. 성능 비교를 위해 인공잡음의 생성 비율을 최적화하지 않고 항상 최대의 전력을 할당하는 경우($\theta = 1$)를 참고 성능(reference)으로 활용하였다. 또한, 수신기의 간섭 상쇄에 따른 잔여 잡음(σ_ϵ^2)을 다양하게 설정하였고, 두 개의 그래프에서 제안기법(proposed)의 경우 모두 최적의 θ^* 값이 존재하는 것을 확인할 수 있다. 최적의 θ^* 값은 수

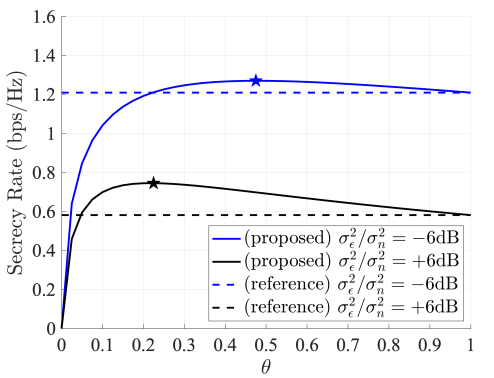

그림 3. 인공잡음 생성 전력 비율 변화에 따른 제안 중계 프로토콜의 보안 전송률($P_S/\sigma_n = 25\,dB$, $P_R/\sigma_n = 35\,dB$)
Fig. 3. Secrecy rate of proposed relay protocol when θ varies and $P_S/\sigma_n = 25\,dB$, $P_R/\sigma_n = 35\,dB$

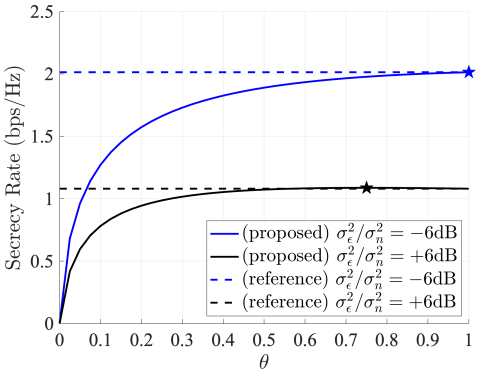

그림 4. 인공잡음 생성 전력 비율 변화에 따른 제안 중계 프로토콜의 보안 전송률($P_S/\sigma_n = 35\,dB,\ P_R/\sigma_n = 35\,dB$)
Fig. 4. Secrecy rate of proposed relay protocol when θ varies and $P_S/\sigma_n = 35\,dB,\ P_R/\sigma_n = 35\,dB$

식 (3)을 이용하여 구할 수 있다. 또한. $\sigma_\epsilon^2/\sigma_n^2$의 값이 작을수록 인공잡음을 효과적으로 제거할 수 있기 때문에 최적의 θ^*값이 커지고 보안 전송률이 증가하게 된다,

그림 4은 그림 3과 마찬가지로 중계 프로토콜의 1단계에서 수신기의 인공잡음 생성 전력의 비율에 따른 보안 전송률을 나타낸다. 송신기-중계기 및 중계기-수신기의 SNR은 각각 $35\,dB$와 $35\,dB$으로 설정하였다. 그림 3과 비교하였을 때, 송신기-중계기의 SNR이 증가하였고 그 결과, 전체적인 보안 전송률이 증가하는 것을 확인할 수 있다. 두 개의 그래프에서 모두 최적의 θ^* 값이 존재하는 것을 확인할 수 있으며, 송신기-중계시 사이의 SNR 값 증가로 비신뢰 중계기의 도청 가능성도 증가했기 때문에 최적의 θ^* 값이 높은 값을 지니는 것을 확인할 수 있다. 또한. 그림 3과 유사하게 $\sigma_\epsilon^2/\sigma_n^2$의 값이 작을수록 최적의 θ^*값이 커지고 보안 전송률이 증가하는 것을 확인할 수 있다.

V. 결 론

본 논문에서는 비신뢰 중계기가 존재하는 차량 대 차량 통신 환경에서 인공 잡음 및 간섭 제거 기법을 활용한 보안 중계 프로토콜의 성능을 분석하였다. 본 연구를 확장하여 중계 통신이 불가피한 차량 대 차량 통신에서 다양한 형태의 물리계층 보안 연구를 수행할 수 있을 것으로 기대된다.

References

[1] P. Porambage, G. Gur, D. P. M. Osorio, M. Liyange, A. Gurtov, and M. Ylianttila, “The roadmap to 6G security and privacy,” *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094-1122, May 2021.

[2] J. Lim, K. Lee, and Y. Han, “Secure communication with outdated channel state information via untrusted relay capable of energy harvesting,” *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 11323-11337, Oct. 2020.

[3] I. Bang, T. Kim, and J. Lim, “User scheduling and optimal power allocation for artificial noise in untrusted full-duplex relay networks,” *J. KICS*, vol. 46, no. 11, Nov. 2021.(To appear)

[4] S. Atapattu, N. Ross, Y. Jing, and M. Premaratne, “Source-based jamming for physical-layer security on untrusted full-duplex relay,” *IEEE Commun. Lett.*, vol. 23, no. 5 pp. 842-846, May 2019.

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

[6] Y. Ai, M. Cheffena, A. Mathur, and H. Lei, “On physical layer security of double Rayleigh fading channels for vehicular communications,” *IEEE Wireless. Commun. Lett.*, vol. 7, no. 6, pp. 1038-1041, Dec. 2018.