차량 통신 네트워크에서 핸드오버 실패 확률 분석에 관한 연구

하승철[§], 이용재[§], 이다은[§], 방인규[§*], 김태훈[†*]

[§]국립한밭대학교 지능미디어공학과, [†]국립한밭대학교 컴퓨터공학과

{scha, yjlee, delee}@edu.hanbat.ac.kr, {ikbang, thkim}@hanbat.ac.kr

A Study on the Analysis of Handover Failure Probability in V2X Networks

Seungcheol Ha[§], Yongjae Lee, Daeun Lee, Taehoon Kim[†*], Inkyu Bang[§*]

[§]Department of Intelligence Media Engineering, Hanbat National University

[†]Department of Computer Engineering, Hanbat National University

요 약

본 연구는 V2X (Vehicle-to-Everything) 통신 네트워크에서 합법적인 노변 기지국(legitimate roadside unit)과 차량 간의 핸드오버(handover) 과정에서 악의적인 노변 기지국(malicious roadside unit)이 핸드오버를 가로채는 위협 모델을 새롭게 정의한다. 추가적으로 악의적인 기지국이 핸드오버 가로채기를 성공하는 경우를 핸드오버 실패(handover failure)로 정의하고 핸드오버 실패 확률을 분석한다.

Ⅰ. 서론

6G 이동통신에서는 초고속, 초신뢰성, 저지연의 정보를 지원하기 위해 향상된 V2X를 제공할 것으로 예상한다. 현재 상용화된 5G-V2X 보다 발전된 6G-V2X가 언급되는 이유로 도시화, 기술의 발전, 자율주행차의 증가로 광범위한 요구사항을 충족하기 위해 언급된다. 자율주행에서 V2X 기술은 자동차와 네트워크 간의 통신으로 외부 데이터를 받아 도로 상황을 파악할 수 있는 중요한 기술이다 [1]. 그러나 기술의 발전에 따라 기지국과 차량 간의 핸드오버를 악의적으로 방해하는 기술도 발전되고 있다.

V2X에서 GPS Spoofing Attack은 매우 치명적인 결과를 초래하게 된다. 공격자는 차량의 GPS 수신기에 잘못된 정보를 제공하여 차량의 위치를 변경하여 경로를 벗어나게 할 수 있다. GPS Spoofing Attack은 공격자가 위조된 GPS 신호를 차량의 수신기로 전송할 때 발생한다. 내비게이션 시스템은 강한 GPS 신호를 수신하도록 설계되어 위조된 GPS의 신호가 합법적인 노변 기지국의 GPS 신호보다 약하면 GPS Spoofing Attack이 성공하게 된다 [2]. 본 논문에서는 Spoofing Attack을 활용하여 노변 기지국과 차량 간의 핸드오버 과정을 방해하는 위협 모델을 정의하고 핸드오버 실패 확률을 수학적으로 분석한다.

Ⅱ. 시스템 모델

본 논문에서는 합법적인 노변 기지국과 차량 간의 핸드오버 순간에 악의적인 노변 기지국이 합법적인 노변 기지국을 핸드오버 신호를 Spoofing 하여 차량의 핸드오버 과정을 방해하는 위협 모델을 가정한다. 그림 1은 악의적인 사용자가 Spoofing Attack을 활용하여 차량의 핸드오버 과정을 공격하는 상황을 나타낸다. 악의적인 기지국의 공격 목표는 차량에 Spoofing Attack을 활용하여 합법적인 노변 기지국의 핸드오버 신호를 가로채는 것이다. 파란색 방사선은 합법적인 노변 기지국의 신호이고, 주황색 방사선은 악의적인 노변 기지국의 신호이다. 차량은 수신 SNR 기반으로 핸드오버 절차를 진행하기 때문에 악의적인 노변 기지국은 합법적인 노변 기지국보다 높은 SNR 신호를 송신하여 차량은 악의적인 노변 기지국으로 핸드오버를 수행하도록 강제한다.

*Corresponding Authors: Taehoon Kim and Inkyu Bang

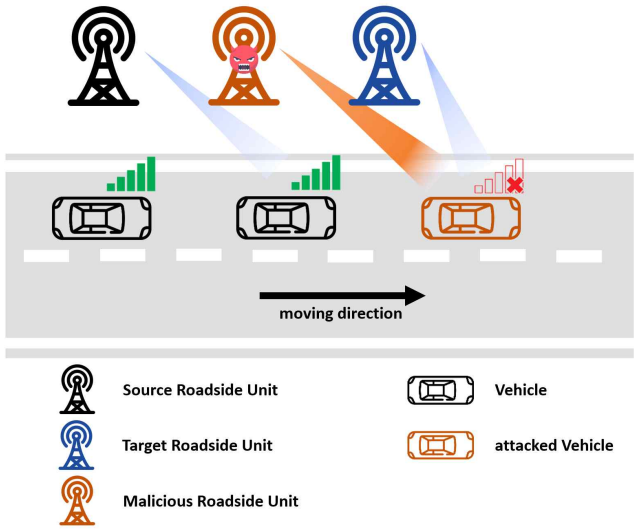

그림 1. 시스템 모델 및 위협 모델

합법적인 노변 기지국과 악의적인 노변 기지국은 각각 α_1, α_2개의 안테나를 장착하고 있다고 가정하며, 무선 신호 수신을 위해 MRC (Maximum Ratio Combining) 수신를 사용한다고 가정한다. 합법적인 노변 기지국과 차량과의 무선 채널 계수는 평균이 0인 가우스 분포를 따르는 h으로, 악의적인 노변 기지국과 차량과의 무선 채널 계수는 평균이 0인 가우스 분포를 따르는 g으로 가정한다. 각각 무선 채널에 대해 분산은 각각 $\frac{1}{\beta_1}, \frac{1}{\beta_2}$으로 가정한다. 이 경우 차량과 각 기지국 간의 수신 신호는 감마 분포(Gamma distribution)로 모델링이 된다. 악의적인 노변 기지국의 공격으로 인한 핸드오버 실패 확률은 다음과 같이 정의된다

.

$$\Pr[\|h\|^2 SNR \leq \|g\|^2 SNR] \qquad (1)$$

Ⅲ. 핸드오버 실패 확률

수식 (1)로 확률 변수는 $\Pr[X \leq Y]$으로 나타낼 수 있다. 여기서 X는 합법적인 노변 기지국과 차량이 핸드오버 될 확률 변수이고, Y는 악의적인 노변 기지국과 차량이 핸드오버 될 확률 변수이다.

이때 합법적인 노변 기지국에 Margin SNR(δ)을 추가시킨 확률 변수는 $\Pr[X+\delta \leq Y]$으로 표현되고, 다음과 같이 표현될 수 있다.

$$\Pr[Z \leq -\delta] \tag{2}$$

수식 (2)는 각각 확률 변수들은 감마 분포를 따르므로 다음과 같이 계산할 수 있다.

$$F(t) = d\int_{\max\{0,-t\}}^{\infty} x^{\alpha_2-1}e^{-\beta_2 x}\gamma(\alpha_1,\beta_1(x+t))dx \tag{3}$$
$$d = \frac{\beta_2^{\alpha_2}}{\Gamma(\alpha_1)\Gamma(\alpha_2)}, (t \in R)$$

수식 (3)에서 α_1, α_2 와 $\frac{1}{\beta_1}, \frac{1}{\beta_2}$는 각각 합법적 위성과 악의적 위성의 안테나 수와 무선 채널의 분산을 의미한다. 여기서 $\gamma(\alpha_1, \beta_1(x+t))$는 하한 불완전 감마 함수를 의미한다. 하한 불완전 감마 함수의 정의에 따라 수식 (3)을 상한 불완전 감마 함수가 포함된 형태로 다음과 같이 유도할 수 있다 [3].

$$F(t) = d\int_{\max\{0,-t\}}^{\infty} x^{\alpha_2-1}e^{-\beta_2 x}[\Gamma(\alpha_1)-\Gamma(\alpha_1,\beta_1(x+t))]dx, (t \in R) \tag{4}$$

Ⅳ. 모의실험 결과

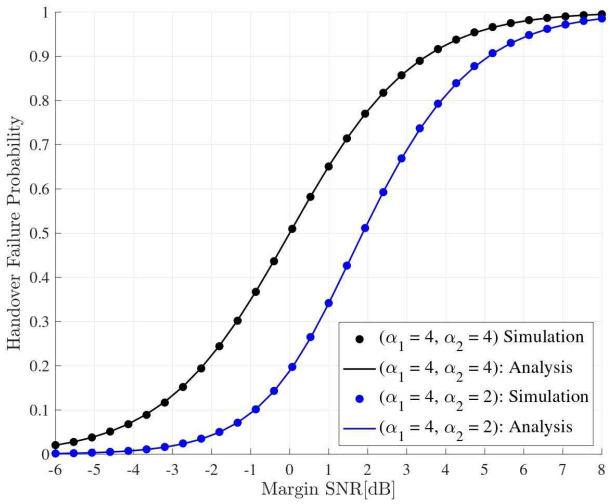

그림 2. Margin SNR 값에 따른 핸드오버 실패 확률

그림 2는 합법적인 노변 기지국에 Margin SNR을 남겼을 때의 결과이다. 검은색 그래프는 각 노변 기지국의 안테나를 4개로 설정했을 때 그래프이고, 파란색 그래프는 합법적인 노변 기지국의 안테나는 4개, 악의적인 노변 기지국의 안테나는 2개로 설정되었다. 두 개의 그래프 모두 Margin SNR이 0일 때 이후로 핸드오버 실패 확률이 급격하게 증가하는 것을 확인할 수 있다. 또한 합법적인 노변 기지국의 안테나 개수가 악의적인 노변 기지국의 안테나 수가 많을 때 핸드오버 실패 확률이 더 낮은 것을 확인할 수 있다.

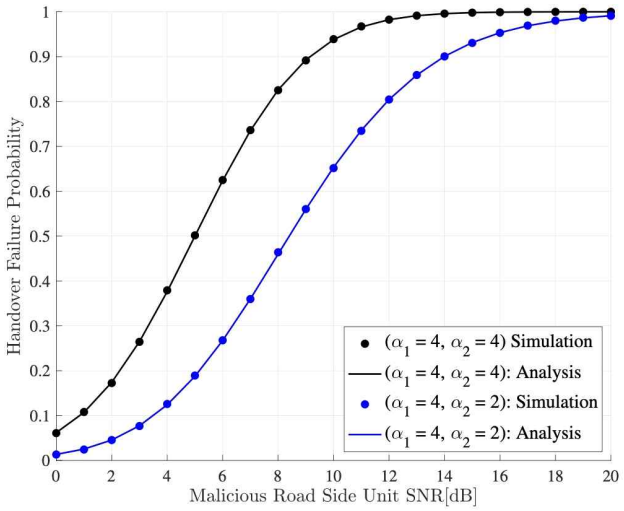

그림 3. 악의적인 노변 기지국의 SNR 변화에 따른 핸드오버 실패 확률

그림 3은 악의적인 노변 기지국의 SNR 변화에 따른 핸드오버 실패 확률 결과이다. 각 노변 기지국의 안테나 수는 그림 2의 설정과 같다. 합법적인 노변 기지국의 SNR은 5dB로 설정하고 악의적인 노변 기지국의 SNR은 0부터 20까지 증가한다. 악의적인 노변 기지국의 SNR이 증가할수록 두 그래프 모두 핸드오버 실패 확률이 증가하는 것을 확인할 수 있다. 또한 악의적 위성의 안테나 수가 많을수록 핸드오버 실패 확률이 급격히 증가하는 것을 확인할 수 있다.

Ⅴ. 결론

본 논문에서는 V2X에서 악의적인 노변 기지국이 Spoofing Attack을 활용하여 핸드오버 실패를 강제하는 위협 모델을 정의하고 핸드오버 실패 확률을 분석하였다. 모의실험의 결과로 합법적인 노변 기지국이 악의적인 노변 기지국보다 안테나 수가 많을수록 핸드오버 실패 확률이 낮아지는 것을 확인할 수 있고, 합법적인 노변 기지국이 악의적인 노변 기지국보다 SNR이 높을 때 핸드오버 실패 확률이 낮아지는 것을 확인할 수 있다. 본 연구의 결과를 확장하여 V2X 네트워크에서 핸드오버 실패 가능성을 구체적으로 분석하는 향후 연구 방향성에 대해서 생각해 볼 수 있다.

ACKNOWLEDGMENT

"본 연구는 2024년 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학사업의 연구결과로 수행되었음"(2022-0-01068)

참 고 문 헌

[1] "Noor-A-Rahim, Md, et al. "6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities." Proceedings of the IEEE 110.6 (2022): 712-734.

[2] Philipsen, Simon Grønfeldt, Birger Andersen, and Bhupjit Singh. "Threats and attacks to modern vehicles." 2021 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS). IEEE, 2021.

[3] Bernhard Klar, "A note on gamma difference distributions" 2014.