V2X 환경에 적합한 차량 식별 및 추적 기술에 관한 연구

이준택, 김찬민, 서지원
한국자동차연구원
jtlee@katech.re.kr, cmkim@katech.re.kr, jwseo@katech.re.kr

A Study on Vehicle Identification and Tracking Technique in V2X Environments

Jun-Taek Lee, Chan-Min Kim, Ji-Won Seo
Korea Automotive Technology Institute

요 약

최근 자동차는 자율주행차 혹은 스마트카로 진화하며 다양한 외부 통신 인터페이스를 포함하고 있습니다. 각 기능 통제를 위해 차량 소프트웨어의 복잡성과 자동차 기술 발전에 따라 통신 인터페이스의 증가로 인하여 자동차에 대한 사이버 공격 가능성 및 위험성이 꾸준히 증가하고 있습니다. 특히, 커넥티드카의 안전을 위한 V2X(Vehicle to Everything)통신이 보안 취약점을 가질 경우, 이는 탑승자의 생명에 직접적인 위협을 초래할 수 있습니다. 그러나, 지능형 교통 시스템에서는 익명성을 위해 일정 시간이 지나면 차량의 식별정보를 변경해 공격자를 찾는데 어려움이 있다. 따라서 본 논문에서는 지능형 교통 시스템 내에서 이상행위를 유발하는 차량을 탐지하기 위해 V2X에 활용되는 표준 메시지 정보를 통해 식별하여 추적하는 기술을 제안하고자 한다.

1. 서론

자동차 산업의 발달과 함께 교통 시스템은 자동차와 인프라, 네트워크 디바이스 등과 실시간으로 정보 교환이 가능한 지능형 자동차 인프라 환경으로 발전하고 있다. 그러나, 자동차 내부 혹은 외부의 연결성 증가로 인해 사이버 공격 경로가 증가하고 이로 인한 위협 가능성 역시 증대되고 있다[1]. 지능형 교통 시스템에 대한 사이버 공격은 교통 신호 마비 등 다양한 방식으로 진행될 수 있고, 이러한 사이버 공격들은 막대한 사회적, 경제적 손실을 유발하고 국민의 안전에도 직·간접적인 영향을 미칠 수 있다.

이처럼 교통사고를 예방하는 기능을 담당하는 지능형 교통 시스템은 국민의 생명에도 직접적인 영향을 미칠 수 있으므로, 지능형 교통 시스템에 대한 안전한 보안 체계의 필요성은 더욱 증가하고 있다. 다시 말해, 지능형 자동차 인프라 환경에서 발생할 수 있는 보안 위협을 원천적으로 차단하고 방어할 수 있는 체계의 구축이 요구된다.

그러나, 일반 컴퓨팅 시스템에서와 다르게 지능형 교통 시스템에서는 공격자를 특정하는데 다음과 같은 어려움이 존재한다. 지능형 시스템에서는 차량 운전자의 프라이버시를 보장하기 위해 익명성을 제공한다. 구체적으로 특정 시간이 지나면 차량의 식별자(예:Vehicle ID 혹은 MAC 주소) 및 통신에 활용되는 인증서가 주기적으로 변경된다. 따라서, 공격자는 이러한 익명성을 역으로 악용하여 자신의 자취를 쉽게 숨기며 공격이 가능해진다.

이를 대응하기 위해 국·내외 다양한 기존 연구들은 이상행위를 유발하는 차량을 식별하기 위해 다양한 방법을 제안해왔다. 먼저 차량 번호판 정보 혹은 카메라 정보와 같은 이미지 정보를 인공지능으로 학습하여 탐지하는 기법이 있다[2][3][4]. 해당 연구들은 센서 및 이미지 정보가 없는 환경에는 적용이 어렵다는 한계가 존재한다. 그리고 차량에 장착되는 Wifi, 블루투스 등 별도 장치의 통신을 탐지해서 차량을 식별하는 기법도 있으나, 해당 연구들은 특정한 장치가 장착되어 있어야한다는 제약조건이 있기 때문에 한계가 존재한다[5][6].

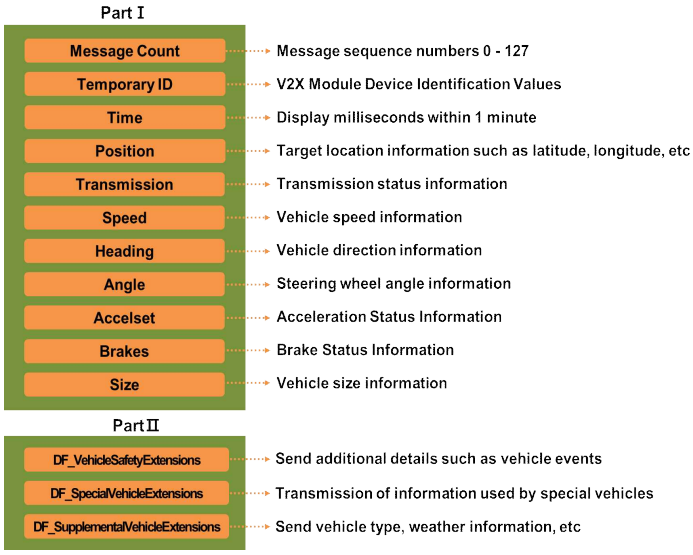
따라서, 본 논문에서는 이러한 한계를 극복하여 차량 통신에 사용되는 표준 메시지를 활용하여 차량의 이상행위를 탐지하는데 도움이 되는 기법들을 제안하고자 한다. 고려하는 공격 시나리오로는 악의적인 차량이 우선순위가 높은 표준 메시지를 송신함으

로써 주변 차량들에게 교통 혼란을 유발하는 것이다. 이러한 악의적인 차량을 탐지하기 위해 본 연구에서는 이상행위를 유발하는 1)차량 식별 기술과 2) 차량 추적 기술을 제안하고자 한다. 이러한 기술들은 향후 지능형 자동차 인프라 환경을 가상화하여, 보안 기술이 적용되었을 시 공격 시나리오가 무력화됨을 보일 예정이다.

2. 배경

C-ITS는 Cooperative-Intelligent Transport Systems의 약자로 차세대 지능형 교통 시스템을 말한다. 차량, 인프라, 행인 등 교통 환경의 구성원들 사이에서 정체 등 주변 교통 상황과 교통사고 등 위험 상황 정보를 실시간으로 공유하여 운전자에게 교통안전, 교통 효율성, 편안함 등을 제공하는 것을 목표로 하는 시스템이다. C-ITS의 전 단계인 ITS는 차량과 인프라 등에 정보통신기술을 접목한 시스템으로 하이패스, 버스도착안내 등이 ITS에 해당한다. C-.ITS와 ITS의 차이는 통신 방식에서 있는데, ITS는 관제센터에서 정보를 수집 및 가공하여 전달하는 단방향 구조지만 C-ITS는 V2X 통신을 통해 차량과 차량, 차량과 인프라 등 다양한 관계에서 정보를 양방향으로 전달한다.

V2X는 차량과 차량, 차량과 도로 인프라, 차량과 보행자 간에 정보를 교환하는 기술을 의미한다. V2X에서는 주로 SAE(Society of Automotive Engineering)에서 정의한 SAE J2735 표준[7]을 활용하여 정보를 교환하며 주로 사용하는 메시지 중 가장 대표적으로는 BSM 메시지가 있다.



(그림 1) SAE J2735에서 정의하는 BSM 메시지

BSM는 Basic Safety Message의 약자로, 기초 안전 메시지를 말한다. 그림 1과 같이 SAE J2735 표준에서 정의되었으며 내용에 따라 Part1과 Part2로 구분할 수 있고 차량의 식별자, 위도, 경도, 속도, 방향, 제동 상태 등의 정보를 포함하는 메시지이다.

3. 차량 식별 기술

차량 식별 기술은 V2X 네트워크에서 별도의 침입탐지 시스템이 이상행위 차량을 탐지하고 탐지한 차량의 식별자를 전달받는다는 가정하에 설계되었다. 차량 식별 기술은 기본적으로 BSM 메시지에 포함된 차량의 식별자를 통해 차량을 식별한다. 이상행위 차량의 식별자를 전달받으면 그 식별자를 Target 식별자로 설정한다. 그리고 주변 차량들이 브로드캐스트하는 모든 BSM 메시지들을 수집하여 각 차량별로 식별자를 기준으로 분류하여 저장한다.

메시지 분류 과정 중 차량의 식별자가 Target 식별자와 동일한 BSM메시지를 발견한 경우 해당 차량을 이상행위 차량으로 판단하고 해당 메시지의 위·경도와 방향, 속도 등을 추출하여 현재 차량 위치와 예상 차량 위치를 지도에 표기하여 별도로 식별한다. 예상 차량 위치는 현재 차량위치를 기반으로 방향과 속도정보를 활용하여 계산한다. 계산된 예상 차량 위치는 이상행위 차량을 더 정확하게 식별하는데 사용되고 뒤에 언급될 차량 추적기술에서도 활용된다.

차량의 식별자가 Target 식별자와 같지 않다면 해당 차량을 일반 차량으로 판단한다. 차량식별기술은 주변 차량에 대해서는 식별 및 추적하지 않지만 이상행위 차량과의 비교를 위해 저장한다.

마지막으로 Target 식별자가 일정시간 이상 식별되지 않으면 시스템은 이상행위 차량의 식별자, 즉 Target 식별자가 변경되었다고 가정하고 차량추적 기술을 이용하여 이상행위 차량을 추적한다.

4. 차량 추적 기술

차량 추적 기술은 차량 식별 기술 수행과정에서 일정시간 이상 Target 식별자가 식별되지 않을 경우 수행된다. 차량 추적 기술은 차량 식별 기술과 마찬가지로 BSM 메시지를 기반으로 이상행위 차량을 추적하기 때문에 가장 먼저 주변 차량들의 BSM 메시지를 수집한다. 수집된 BSM 메시지들은 2가지 검증 과정을 수행하게 되며 2가지 검증 과정을 모두 충족할 경우 해당 BSM 메시지를 이상행위 차량으

로부터 수신된 BSM 메시지로 판단하여 해당 메시지의 식별자를 Target 식별자로 재설정한다.

첫 번째 검증 과정은 해당 BSM 메시지의 식별자가 최근에 수신되었는지 확인하는 것이다. 차량 식별 기술 수행과정에서 모든 메시지는 차량 식별자를 기준으로 분류되어 저장되었는데, 저장된 차량의 식별자들을 불러와 현재 메시지들의 차량 식별자들과 비교한다. 만약 메시지의 식별자가 기존에 저장되어 있지 않은 식별자일 경우 첫 번째 과정을 충족한 것으로 한다.

두 번째 검증 과정은 차량 식별 기술에서 계산한 예상 차량 위치와 현재 메시지의 실제 차량 위치를 비교하는 것이다. 계산한 거리가 오차 허용범위 이내라면 두 번째 과정을 충족한 것으로 한다.

해당 메시지가 모든 검증 과정을 충족하였을 경우 Target 식별자를 재설정한 뒤 이상행위 차량의 식별 및 추적을 지속한다.

5. 결론

최근 자동차 기술 발전으로 자율주행차와 스마트카가 더욱 확산되며, 차량의 외부 통신 인퍼페이스가 다양하게 포함되고 있습니다. 그러나 이러한 기술 발전으로 인해 자동차의 소프트웨어 복잡성과 함께 자동차 사이버 공격의 가능성과 위험성을 증가하고 있습니다. 따라서 본 논문에서는 V2X 통신의 표준 메시지 정보를 활용하여 차량을 식별하고 추적함으로써 안전한 교통 시스템을 구축할 수 있는 기법들에 대한 소개를 하였습니다. 본 논문을 통해 자동차 산업과 사업 전반에 긍정적인 영향을 미칠 것이라 기대합니다.

ACKNOWLEDGMENT

본 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No. 2022-0-00979-002, 자율주행차량 데이터 및 V2X 통신 네트워크보안성 평가 기술 및 시험기준 개발)

참고문헌

[1] TREND MICRO, “The Evolution of Connected Cars as Defined by Threat Modeling UN R 155-Listed Attack Vectors”, Sep 02. 2021, The Evolution of Connected Carsas Defined by Threat Modeling UN R 155-Listed Attack Vectors, 2021.

[2] Jiang, J., Yang, Y., Li, Y., Wang, R., & Zeng, S. (2022). Lane-level vehicle counting based on V2X and centimeter-level positioning at urban intersections. International Journal of Intelligent Transportation Systems Research, 1-18.

[3] Minsung Kang, & Young-Chul Lim (개최날짜). Multi-class Multi-Object Tracking using Re-Identification. the Korean Society of Automotive Engineers 2020 Annual Autumn Conference & Exhibition, 2020

[4] Jiang, J., Yang, Y., Li, Y. et al. Lane-Level Vehicle Counting Based on V2X and Centimeter-level Positioning at Urban Intersections. Int. J. ITS Res. 20, 2022

[5] M. B. Brahim and H. Menouar, "V2X-based traffic flow calculation with support of unique identifier randomization," 2016 2nd IEEE International Conference on Computer and Communications (ICCC), Chengdu, China, 2016

[6] M Ullmann, T Strubbe, C Wieschebrink. Misuse Capabilities of the V2V Communication to Harm the Privacy of Vehicles and Drivers. International Journal on Advances in Networks and Services, 2017

[7] SAE International, SAE J2735 V2X Communications Message Set Dictionary: https://www.sae.org/standards/content/j2735_202007/, 2020