자율협력주행 기반 V2X 메시지 위협 검증 방법

김아람, 김인수, 박재홍
와이즈오토모티브
kar@wise-automotive, kis@wise-automotive.com, blue@wise-automotive.com

Threat Verification Method for V2X Messages Based on Cooperative Autonomous Driving

Kim Aram, Kim Insu, Park Jaehong
WISEautomotive

요 약

본 논문은 자율주행 차량이 자율협력주행 환경에서 수신한 V2X 메시지의 위협 여부를 도로 상의 객체들의 교차 검증을 통해 판단하는 방법을 설명한다. 자율주행 차량에서 자체 보안 엔진으로 1차 검증하고, 불확실할 경우 주변 차량·RSU·인프라에 협력 검증을 요청한다. 이 과정에서 각 검증 주체의 신뢰도를 반영해 판정을 가중치화하며, 신뢰 점수 기반으로 위협 메시지를 판정하여 차량 보안을 강화한다.

Ⅰ. 서 론

V2X(Vehicle-To-Everything) 기술은 자율주행 차량과 인프라 등 다양한 객체들과의 메시지 교류를 통해 자율협력주행을 실현한다. V2X 메시지로 다양한 정보와 서비스를 제공하기 때문에 사이버보안 위협에 대응할 수 있어야 한다. 일반적으로 메시지에 대한 PKI(Public Key IInfrastructure) 등의 보안 인증을 거치지만, 악의적인 공격으로 인해 발생할 수 있는 사고의 위험성이 크고 다양한 방법으로 위협을 가할 수 있기 때문에 메시지의 안전성을 인증하는 방법도 다양해져야 한다. 본 논문에서는 자율협력주행을 통한 V2X 메시지 위협성 검증 방법을 제안한다. 메시지의 안전성 인증을 차량과 인프라 간으로 한정하지 않고, 주변 차량을 포함한 도로 상의 객체들이 검증 과정에 참여하여 위협 메시지에 대한 교차 검증을 통해 안전성 강화를 목표로 한다.

Ⅱ. 본론

자율협력주행을 통한 V2X 메시지 안전성 검증 과정은 다음과 같다. 우선 Ego차량의 자율주행 시스템이 V2X 메시지를 수신한다. 자율주행 시스템의 자체 보안 엔진은 수신 메시지의 위협성 여부를 1차 판정한다. 위협이 되거나 위협 여부를 판단하기 어려운 경우 주변 객체들에 V2X 메시지 셋을 활용하여 해당 메시지들의 검증을 요청한다.[1] 다수의 신뢰도 높은 차량 및 인프라에서 동일 메시지를 정상으로 판정하면 오탐으로 정정하고, 위협으로 판정하면 메시지 필터링이나 제한 모드 진입 등의 방법으로 위협 유형에 따라 대응한다. 이후 위협 메시지에 대한 정보를 인프라에 보고한다.

주변 객체에 위협 메시지를 검증 요청은 위협 메시지 검증은 주변 차량-RSU(Road Side Unit)-클라우드(상위 인프라) 단계 순으로 집계한다. 위협 검증은 검증 주체들의 신뢰도를 고려한다. 검증 주체들의 보안 엔진이 얼마나 신뢰성이 있는지 검증 정확도, 통신 품질, 과거 오답률 등의 정보를 보유한다. 이 신뢰정보를 통해 같은 메시지를 평가할 때 신뢰도가 높은 주체들의 판정에 높은 가중치를 부여하여 판정한다. 인프라는 위협 평가 결과, 유사한 케이스의 과거 이력, 신뢰성 등을 제공한다.

또한 메시지 신뢰도는 신뢰성을 판단할 때 단순히 정상인지 위협인지 여부로 구분하지 않고 신뢰 점수를 활용한다. 검증 결과를 취합했을 때 평균값, 분산값 등을 활용하여 신뢰도를 재계산하고 신뢰도 수준에 따라서 위협에 대한 대응 방법을 결정한다.

Ⅲ. 결론

본 논문에서는 자율협력주행을 통한 V2X 위협 메시지의 검증 방법을 설명했다. 메시지 위협 검증에 도로 상의 모든 객체가 참여하면서도 신뢰성에 따라 검증에 가중치가 반영되기 때문에 기존 보안 인증 과정에 추가하면 안전성이 강화될 것으로 기대한다.

ACKNOWLEDGMENT

이 연구는 2025년도 산업통상자원부 및 한국산업기술기획평가원(KEIT) 연구비 지원에 의한 연구임 (2410000538, 전장부품의 보안성 검증을 위한 평가(V&V) 시스템 기술개발)

참 고 문 헌

[1] SAE-J2735, *V2X Communications Message Set Dictionary*, 2020