IoV에서 축적된 교통 정보를 활용한 MARINE 기반 중간자 공격 탐지 방법

정원진[O], 조대호[*]
[O]성균관대학교 전자전기컴퓨터공학과,
[*]성균관대학교 소프트웨어학과
e-mail: wonjin12@skku.edu[O], thcho@skku.edu[*]

MARINE-based Man in the Middle Attack Detection Method Using Traffic Information Accumulated in IoV

Wonjin Chung[O], Taeho Cho[*]
[O]Department of Electrical and Computer Engineering, Sungkyunkwan University,
[*]Department of Computer Science and Engineering, Sungkyunkwan University

● 요 약 ●

차량 인터넷은 목적지까지 스스로 주행하는 자율 주행 자동차의 최적 경로 설정을 도와주는 차세대 네트워크이다. 자율 주행 자동차의 원활한 자율 주행을 위해서는 도로 위 객체 인지뿐만 아니라 실시간 교통 정보가 수신되어야 한다. 공격자는 자동차로 전달되는 메시지를 탈취하여 내용을 변경하거나 메시지를 제거하는 중간자 공격을 시도할 수 있다. 중간자 공격을 탐지하기 위해 MARINE 기법이 제안되었지만, 주행하는 자동차가 적은 환경에서 중간자 공격을 탐지하기 어렵다. 제안 방법은 이러한 문제를 해결하기 위해 교통 정보 센터에 축적된 교통 정보를 이용하여 자동차에 전달되는 메시지를 분석하고 중간자 공격을 탐지하는 방법을 제안한다.

키워드: 차량 인터넷(internet of vehicle), 네트워크 보안(network security), 시뮬레이션(simulation)

I. Introduction

최근 컴퓨터 기술과 5세대 무선 네트워크 기술 발전으로 완전 자율 주행이 실현할 수 있는 기술로 발전되었다. 차량인터넷(Internet of Vehicle; 이하 IoV)은 스마트 도로에서 주행하는 자율 주행 자동차가 노변 기지국(Road Side Unit; 이하 RSU) 또는 다른 자율 주행 자동차와 통신을 하며 목적지까지 주행을 도와주는 차세대 차량 네트워크 기술이다 [1]. 자율 주행 자동차는 카메라, 레이더, 라이다와 같은 다양한 센서를 이용하여 도로 위 객체들을 인지하고, Vehicle to Everything (V2X) 통신을 통해 실시간 교통 정보를 수신한다 [2]. 이러한 통신 과정에서 악의적인 공격자는 중간자 공격(Man in The Middle attack)을 시도하여 교통사고를 유발할 수 있다[3]. 중간자 공격을 탐지하기 위해 Man in The Middle Attack Resistance Trust Model in Connected Vehicles (MARINE)이 제안되었다 [4]. MARINE은 신뢰할 수 있는 자동차를 구별하여 중간자 공격을 탐지하는 기법이다. 하지만 주행 중인 자동차의 거리를 속이거나 연속적인 중간자 공격이 발생하면 MARINE을 통한 공격 탐지가 어렵다. 본 논문에서는 축적된 교통 정보 분석을 통한 다양한 유형의 중간자 공격 탐지 방법을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 자율 주행 자동차, MARINE 그리고 이산사건 시스템 명세를 소개한다. 3장에서는 제안 방법을 통해 중간자 공격 탐지를 보여준다. 4장에서는 결론 및 향후 연구를 제시한다.

II. Background

해당 장에서는 자율 주행 자동차와 중간자 공격 탐지기법인 MARINE 그리고 이산사건 시스템 명세(Discrete EVent System specification, 이하 DEVS)에 대해 소개한다.

1. 자율 주행 자동차

자율 주행 자동차는 운전자의 조작 없이 자동차 스스로 목적지까지 최적 경로를 계산하여 주행하는 자동차이다. 현재 자율 주행 기술 단계는 레벨 3에 속하며, 앞으로 출시될 자동차는 차량 운행 보조 장치가 아닌 스스로 주행하는 기술이 탑재된 자동차로 분류된다 [5]. 자율 주행 기술은 도로 위 객체 인지를 위한 다양한 종류의 센서들과 실시간으로 도로 상황 정보를 수신할 수 있는 통신 기술을 이용하여 주행한다. 자율 주행에 사용하는 통신 기법으로는 V2X

통신을 이용하며, 다양한 도로 상황 정보를 수신한다[6]. V2X 통신은 통신하는 대상에 따라 Vehicle to Vehicle (V2V) 통신, Vehicle to Infrastructure (V2I) 통신, Vehicle to Pedestrian (V2P) 통신 등 다양하게 분류된다 [2]. 이러한 통신을 통해 공사 현장, 사고 지역 등 주행이 어려운 교통 정보를 실시간으로 수신할 수 있으며 자동차의 센서로 인지하지 못하는 사각지대를 V2X 통신을 통해 파악할 수 있다.

2. MARINE

자율 주행 자동차는 다양한 통신을 통해 정보를 수신하며 최적 경로를 계산하여 주행함으로써 운전자는 시간 및 자원을 효율적으로 사용할 수 있다. 따라서 주행 중 실시간으로 수신하게 되는 정보는 주행에 필요한 교통 정보가 전달되어야 한다. 하지만 악의적인 공격자는 교통에 혼란을 주기 위해 자동차에 전달되는 메시지를 제거하거나 전달된 메시지의 내용을 변경하는 중간자 공격을 시도한다 [7]. 자율 주행 자동차가 변조된 메시지를 수신한다면 잘못된 주행으로 인해 시간적, 자원적 손해가 발생하며, 중간자 공격이 계속 발생하면 사고로 인한 인명피해가 발생할 수 있다. 중간자 공격으로 인한 피해를 줄이기 위해 MARINE이 제안되었다 [3]. MARINE은 IoV에 적용할 수 있는 중간자 공격 탐지 기법으로 엔티티 중심 신뢰 모델과 데이터 중심 신뢰 모델이 결합한 신뢰 모델이다 [8]. 이는 중간자 공격 탐지를 위해 수신된 메시지의 신뢰 평가를 기반으로 노드의 신뢰가 계산되는 모델이다. MARINE을 이용한 중간자 공격 탐지 절차는 다음과 같다. 먼저 공격자를 탐지하기 위해 발신자의 자동차를 평가하여 신뢰성을 식별한다. 신뢰할 수 있는 자동차일 경우 정보 품질, 자동차의 메시지 전달 능력, 이웃 자동차의 평가를 바탕으로 수신된 데이터를 검증한다. 메시지 검증이 완료되면 전달받은 자동차에서 메시지가 처리된다.

3. 이산사건 시스템 명세

DEVS는 사건의 발생에 따라 모델의 상태가 변하면서 발생하는 이벤트를 중심적으로 기술되는 계층적 형식론이다 [9]. DEVS는 크게 원자 모델과 결합 모델로 구성된다. 먼저 원자 모델은 실세계의 객체 행위를 표현하며, 이는 발생하는 입력 이벤트와 시간 진행에 따른 상태 전이를 중점으로 기술된다. 다음으로 결합 모델은 원자 모델 또는 다른 결합 모델을 연결하여 커다란 시스템을 형성할 수 있는 기능을 제공한다.

III. The Proposed Scheme

MARINE은 자동차 또는 메시지의 신뢰도를 이용하여 중간자 공격을 탐지하는 보안 기술이다. 하지만 자동차의 주행 빈도가 낮은 장소에서 신뢰받은 자동차로부터 송신된 메시지가 중간자 공격으로 인하여 메시지의 내용이 변조된다면 메시지를 수신할 자동차는 변경된 메시지 내용으로 잘못된 주행을 하게 된다. 또한, 다수의 변조된 메시지가 전달되면 피해 자동차는 변조된 메시지의 내용을 정상 메시지 내용으로 인식하게 된다. 위와 같은 중간자 공격 유형을 탐지하기 위해 교통 정보 센터에 축적된 상황 정보와 상태 전이 횟수를 이용한 탐지 방법을 제안한다.

1. IoV 모델

제안 방법은 보안 평가를 위해 자율 주행 자동차, RSU와 같은 IoV에 필요한 DEVS 이론 기반 객체를 디자인한다. 아래 Fig. 1은 자율 주행 자동차 모델과 RSU 모델의 메시지를 송수신을 위한 ROAD 모델의 다이어그램이다. RSU는 다양한 도로 인프라를 통해 정보를 수신하며 필요한 정보를 자율 주행 자동차에 전달한다. 또한, 자율 주행 자동차로부터 받은 정보를 교통 정보 센터로 전달하며, 정보를 수신한 교통 정보 센터가 전체적인 도로 관리를 할 수 있도록 한다.

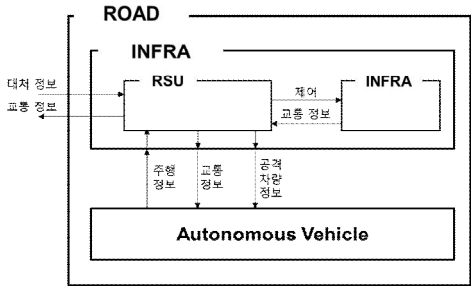

Fig. 1. ROAD 모델 다이어그램

RSU는 자율 주행 자동차의 신뢰도를 계산하기 위한 정보를 수신하기도 하며 이러한 정보를 교통 정보 센터로 정보를 보내 계산하여 전달받는다. 이후 전달받은 정보를 통해 RSU의 네트워크에 접근한 자동차를 관리한다.

2. 세부 동작

MARINE은 대부분의 중간자 공격을 탐지하지만, 시골과 같이 주행하는 자동차가 적은 지역에서 중간자 공격을 탐지하기 어렵다. 제안 방법은 이러한 유형의 공격을 탐지하기 위해 교통 정보 센터에 축적된 상황 정보를 분석하여 중간자 공격을 탐지한다. Fig. 2는 MARINE에서 탐지가 어려운 중간자 공격 유형을 보여준다.

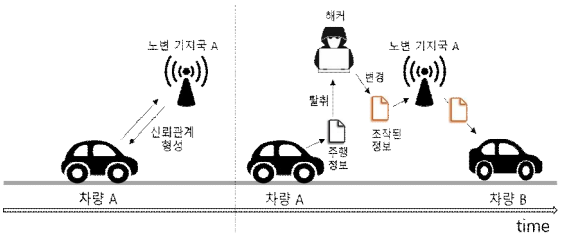

Fig. 2. 다양한 유형의 MiTM 공격

신뢰받은 자동차가 다시 메시지를 전달할 때 중간자 공격이 발생하면 신뢰 모델에 중점을 둔 MARINE을 통한 탐지가 어렵다. 또한, MARINE은 자동차 주행 빈도가 낮은 지역에서 공격 차량 리스트를 이용하여 차량 신뢰 여부를 판단하기 때문에 많은 양의 신뢰성 있는 정보가 축적되어야 정확한 탐지가 가능하다. 하지만 자동차 주행

빈도가 낮은 지역일수록 교통 정보 센터에 정보가 축적되기까지 오랜 시간이 걸린다. 제안 방법은 자동차의 주행 정보를 이용하여 중간자 공격을 탐지한다. 자율 주행 자동차의 주행 과정에서 RSU에 접근하면 해당 자동차의 모든 주행 관련 정보가 RSU를 통해 교통 정보 센터로 전달된다. 전달된 정보는 시간 경과에 따른 이벤트 발생 중점으로 저장된다. 교통 정보 센터는 축적된 정보를 분석하여 공격자의 메시지 변조나 삭제를 탐지할 수 있다. 하지만 이러한 방법은 정확하게 탐지할 수 있으나 탐지 시간이 오래 걸리는 단점이 있다. 이러한 문제를 해결하기 위해 상황 정보 횟수를 추가하여 중간자 공격을 차단한다. Fig. 3은 상황 정보 횟수를 이용한 공격 차단 과정을 보여준다.

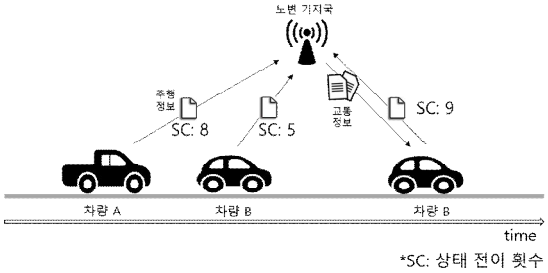

Fig. 3. 상태 전이 횟수를 이용한 공격 차단

DEVS 형식론 기반 원자 모델은 이벤트가 발생할 때마다 상태 전이가 발생한다. 따라서 자율 주행 자동차의 주행을 위한 행위들은 일정 패턴을 형성하며, 자동차의 종류에 따라 모두 다른 형태의 패턴을 형성하게 된다. 제안 방법은 주행하는데 필요한 상태 전이 횟수를 암호화 키로 이용하여 메시지를 암호화하고 RSU에 전달하면 중간자 공격을 차단할 수 있다. 공격자는 공격 대상 자동차에서 전달되는 메시지를 탈취하여도 상황에 따라 암호화키가 다르므로 메시지 복호화가 어렵다. 이는 자동차의 주행에 대한 이벤트뿐만 아니라 RSU에 전달되는 입력 이벤트에 따라 상태가 다르게 전이되기 때문이다. 제안 방법은 상황 정보 횟수를 이용하여 중간자 공격을 차단하고, 탐지하지 못한 공격은 교통 정보 센터에서 축적된 주행 정보를 분석하여 탐지할 수 있다.

IV. Conclusions

IoV는 자율 주행 자동차가 안전하게 목적지까지의 주행을 도와주는 차세대 네트워크 기술이다. 자율 주행 자동차는 정밀한 센서를 이용하여 도로 위의 객체들을 인지하고 실시간 교통 정보를 수집하여 도로 상황에 맞는 최적의 경로를 계산하여 주행한다. 자율 주행 자동차에 전달되는 교통 정보는 신호 정보, 사고 정보, 통제 구역 정보 등 다양한 내용이 포함되어 있으며 경로 설정에 영향을 주기 때문에 정확한 정보가 전달되어야 한다. 악의적인 공격자는 자율 주행 자동차에 전송되는 정보를 중간에 탈취해 내용을 변조하거나 삭제하는 중간자 공격을 시도한다. 중간자 공격은 도착 시각을 지연시키고 사고를 유발한다. MARINE은 IoV에 사용할 수 있는 중간자 공격 탐지 기법이다. 하지만 MARINE은 많은 양의 도로 정보를 이용하여 중간자 공격을 탐지하기 때문에 자동차 이동량이 적은 지역에서 발생하는 중간자 공격을 탐지하기 어렵다. 제안 방법은 이러한 환경에서 중간자 공격을 탐지하기 위해 교통 정보 센터에 축적된 교통 정보를 이용한다. 또한, 제안 방법의 탐지 시간 문제를 해결하기 위해 상황 정보 횟수를 이용한다. 제안 방법은 다양한 유형의 중간자 공격을 탐지함으로써 네트워크 보안 향상에 기여한다. 추후 연구는 결합 모델에서의 시공간 규칙을 이용한 중간자 공격 탐지 연구를 진행할 예정이다 [10].

ACKNOWLEDGEMENT

이 논문은 2021년도 정부(과학기술정보통신 부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.NRF-2021R1A2C2005480)

REFERENCES

[1] Yang, Fangchun, et al. "An overview of internet of vehicles," China communications, Vol. 11, No. 10, pp. 1-15, 2014.

[2] Molina-Masegosa, Rafael, and Javier Gozalvez. "LTE-V for sidelink 5G V2X vehicular communications: A new 5G technology for short-range vehicle-to-everything communications," IEEE Vehicular Technology Magazine, Vol. 12, No. 4, pp. 30-39, 2017.

[3] Ahmad, Farhan, et al. "Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies," Sensors, Vol.18, No. 11, pp. 4040, 2018.

[4] Ahmad, Farhan, et al. "MARINE: Man-in-the-middle attack resistant trust model in connected vehicles." IEEE Internet of Things Journal, Vol. 7, No. 4, pp. 3310-3322, 2020.

[5] SAE International, "Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles (J3016B)," Tech. Rep., 2018. [Online]. Available: https://www.sae.org/standards/content/j3016{_}201806/

[6] Hobert, Laurens, et al. "Enhancements of V2X communication in support of cooperative autonomous driving," IEEE communications magazine, Vol. 53, No.12, pp. 64-70, 2015.

[7] Alazzawi, Murtadha A., et al. "Efficient conditional anonymity with message integrity and authentication in a vehicular ad-hoc network," IEEE Access, Vol. 7, pp. 71424-71435, 2019.

[8] Chen, Ji-Ming, Ting-Ting Li, and John Panneerselvam. "TMEC: a trust management based on evidence combination on attack-resistant and collaborative internet of vehicles," IEEE Access, Vol. 7, pp. 148913-148922, 2018.

[9] Zeigler, Bernard P. "DEVS representation of dynamical systems: Event-based intelligent control." Proceedings of the IEEE, Vol. 77, No. 1, pp. 72-80, 1989.

[10] Cho, Tae Ho. "Simulation Methodology-Based Context-Aware Architecture Design for Behavior Monitoring of Systems." Symmetry, Vol.12, No.9, pp. 1568, 2020.