능동안전(제어) IV

차량 고신뢰성을 위한 혼돈 암호화 메시지 인증

박서희* · 송호진* · 이수윤* · 백영미**

Chaotic Encryption Based Message Authentication for High Reliability of Automobiles

Seo-Hee Park*, Ho-Jin Song*, Su-Yun Lee*, Youngmi Baek**

Key Words : In-vehicle network(차량 내부 네트워크), Symmetric key(대칭키), Block cipher(블록 암호), Chaotic map (혼돈 맵), Authentication(인증)

ABSTRACT

Modern vehicles have shifted from a completely isolated system to an open-connected system. Although modern vehicles have become more convenient, they lead to exposing security vulnerabilities newly and the safety of passengers and drivers threatened. To improve the security of an in-vehicle network, in this paper, we propose a cryptography-based message authentication using a one-dimensional chaotic map (MACM). The proposed MACM provides control data with data integrity for electronic control units (ECUs) for driving by performing message authentication using a symmetric key. The symmetric key that is implicitly synchronized is used to verify the message authentication code (MAC), which is a ciphertext, against the control data in the received message. To do this, we exploit a chaotic map with is capable of efficiently and securely generating a secret key to encrypt control data to be transmitted over a controller area network (CAN) bus. It is a kind of chaotic system with a high sensitivity to a given initial condition and a property of ergodicity. In addition, the initial condition for performing the chaotic map is evolved using the final result generated after conducting a specific chaotic map. It causes the randomness of the secret key to be enhanced. Therefore, the MACM with the secret key based on the chaotic map is capable of generating different ciphertext even though there exists the same control data. This is the reason that the ciphertext is used as a message authentication code. After a sender transmits the control data with the ciphertext (i.e., MAC), a receiver compares the received control data with the plain text derived from MAC by conducting the same chaotic map of the sender. If message authentication fails, the receiver determines that message as a cyber attack and sends a CAN error message to all ECUs on the bus. From performance evaluation, it is shown that is capable of operating in real-time and detecting the injected cyber-attacks 100%. It is also demonstrated that it ensures the high reliability of vehicle control by the proposed MACM.

※This work was supported by the Gyeongnam SW Convergence Cluster 2.0(Specialized Industry Reinforcement) and the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT)(No. 2021R1F1A1048179).

* 창신대학/학생
** 창신대학/교수
E-mail : qkrtjgml5089@naver.com

주행 안정성 보장을 위한 가변 주기 메시지 인증

송호진* · 박서희* · 이수윤* · 백영미**

Message Authentication According to a Variable Authentication Interval for Ensuring Driving Safety

Ho-Jin Song*, Seo-Hee Park*, Su-Yun Lee*, Youngmi Baek**

Key Words : In-Vehicle Network(차량 내부 네트워크), Message Authentication Code(메세지 인증코드), Cryptographic Hash Function(암호화해시함수)

ABSTRACT

Although a controller area network (CAN) protocol is a de-facto standard, it suffers from a lack of security functionality. To immediately detect a cyber-attack injected from the external connection point and exclude it from driving control, there is a straightforward way that all nodes connected to a CAN bus participate in message authentication. Before using control data, all receivers should conduct message authentication whenever a sender transmits its CAN message with a message authentication code (MAC). However, if there are many receiving messages under a high bus load rate, it may be not possible for a receiver to perform each authentication completely within a given time. To address this problem, in this paper, we propose a message authentication to be performed with a variable authentication interval using a cryptographic hash function. In other words, we focus on message authentication at varied authentication intervals for each message, rather than performing message authentication for each message so that we ensure real-time transmission and processing for control data on receivers. At an initial phase in the proposed method, to reduce the overhead of the authentication, the authentication interval increases exponentially when the message is repeatedly determined to be a reliable message by a receiver. If the message is determined not to be legitimate, the receiver eliminates the receiving messages and then initializes the authentication interval of that message. It indicates that the receiver changes the normal state of the message with that identification number into a suspicious state. The proposed method is very efficient to perform message authentication under a high bus load rate as well as to improve driving safety.

※This work was supported by the Gyeongnam SW Convergence Cluster 2.0(Specialized Industry Reinforcement) and the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT)(No. 2021R1F1A1048179).

* 창신대학/학생
** 창신대학/교수
E-mail : rhdqn202@gmail.com

가상환경에서 접근성이 용이한 자율주행 실증 맵 성능 연구

백민혁* · 박진우* · 심중석* · 박성정** · 최경호***,† · 임용섭****,†

Study on Self-driving Demonstration Map Performance with Easy Accessibility in Virtual Environment

MinHyeok Baek*, Jinu Pahk*, JungSeok Shim*, SeongJeong Park**, GyeungHo Choi***,†, YongSeob Lim****,†

Key Words : Automated vehicle(자율주행차), Self-driving verification(자율주행 실증), HD map(고정밀 지도), Open-streetmap(오픈 스트리트 맵), Virtual simulation(가상 시뮬레이션)

ABSTRACT

In recent years, automated vehicles have become a very popular topic in multidisciplinary research field. They promise not only more comfortable and new opportunities for passengers but above all more safety on the road. In terms of safety, some forms of HD map have been in development for many years. HD maps are roadmaps with inch-perfect accuracy and a high environmental fidelity which they contain information about the exact positions of pedestrian crossings, traffic lights/signs, barriers and more. Also, HD maps in order to demonstrate autonomous driving, verification of driving on the actual road are essentially needed in the virtual environment due to test cost, duration and safety issues. Therefore it has been making a real road as an HD map in the simulation and conducting a virtual driving. However, existing HD map, using high-precision data, it is expensive and time-consuming to build a new map as much as real driving. Hence, it is difficult to verify in various environments and roads. This is an obstacle for the demonstration of autonomous driving only in extremely limited roads and environments.

In this paper, we propose a new HD map implementation method that is simple and more accessible used for autonomous driving demonstration. Our HD map is created using Carla simulator, which is combined with OpenStreetMap map data. In this method, the simulator and map data are all open-source. Therefore, we can possible to easily create HD maps containing high accuracy road information for the everywhere in the world with little dependence. With high easily accessible HD map, the results showed that the accuracy of the longitudinal length in the straight road was 98.28% and in the curved road 98.42% in the curved road, respectively. Also, the accuracy for the lateral direction for the road width represented 100% compared to the manual method reflected with the exact road data.

* 대구경북과학기술원/융복합대학
** 대구경북과학기술원/학제학과 석사과정
*** 대구경북과학기술원/학제학과 교수
**** 대구경북과학기술원/로봇 및 기계전자공학과 교수
† 교신저자 : ghchoi@dgist.ac.kr
† 교신저자 : yslim73@dgist.ac.kr
E-mail : minheak06@dgist.ac.kr

가상주행시나리오에 의한 자율주행차 주행성능 검증 방법

유창열* · 김동환** · 윤종민*** · 곽지섭****

Validation Method Using Virtual Scenarios for Autonomous Driving Functions of Autonomous Vehicle

Changyeol Yoo*, Donghwan Kim**, Jongmin Yoon***, Jisub Kwak****

Key Words : Autonomous driving(자율주행), CarMaker(카메이커), Vehicle-In-the-Loop simulation(VIL시뮬레이션), Virtual driving scenario(가상주행시나리오)

ABSTRACT

To evaluate the driving safety of autonomous vehicles with level 4, the robustness of AV Stack needs to be guaranteed by applying various scenarios which represent situations on the road to the autonomous vehicles. However, it is difficult to secure robust control performance of autonomous vehicles in very dangerous emergency situations. Therefore, the validation method using Vehicle-in-the-Loop simulation is introduced, which various traffic situations around the automated vehicle can be generated and sensor data from the virtual environment can be transferred to the vehicle that updates its own position information on the road or the proving ground during driving in the real-time by using a virtual simulation environment.

Acknowledgement

본 연구는 국토교통부 자율주행기술개발혁신사업의 지원으로 수행되었음(과제번호 22AMDP-C162351-02)

* IPG Automotive Korea/주임연구원
** IPG Automotive Korea/주임연구원
*** IPG Automotive Korea/이사
**** 서울대학교 기계공학부/석박통합과정
E-mail : changyeol.yoo@ipg-automotive.com

자율주행차량의 가상 환경 내 V2X 메시지 시뮬레이션

이빈희* · 이장우** · 허관회*** · 윤종민****

Simulation of V2X Messages in the Virtual Environment of Autonomous Vehicle

Beenhui Lee*, Jangu Lee**, Kwanhoe Huh***, Jongmin Yoon****

Key Words : Autonomous driving(자율주행), CarMaker(카메이커), V2X communication(V2X 통신), Virtual driving environment(가상주행환경)

ABSTRACT

The proportion of autonomous vehicle simulation in a virtual environment for autonomous vehicle development is increasing. In the virtual environment, various algorithms included in autonomous vehicles can be simulated. Furthermore, by configuring a V2X communication (Vehicle to Everything communication) environment in a virtual environment, it can be used to expand and test the algorithm of autonomous vehicles. In this study, a V2X communication environment is established so that autonomous vehicles can conduct simulations through V2X communication in a virtual driving environment. Through this, it can be confirmed that the scope of application of autonomous vehicle simulation in the virtual environment has been expanded, and it is confirmed that simulations of Level 4 and Level 5 autonomous vehicles as well as Level 3 autonomous vehicles can be expanded.

Acknowledgement

본 연구는 국토교통부 자율주행기술개발혁신사업의 지원으로 수행되었음(과제번호 22AMDP-C162351-02)

* IPG Automotive Korea/주임연구원
** IPG Automotive Korea/연구원
*** IPG Automotive Korea/부장
**** IPG Automotive Korea/이사
E-mail : beenhui.lee@ipg-automotive.com

상용차 전자제어 제동 장치를 위한 비상대응 시스템 설계

김유원* · 황정규**

Design of NG e-Call In-vehicle System for the Commercial Vehicle Electronic Control Braking Device

Yoowon Kim*, Jung Gyu Hwang**

Key Words : ABS(브레이크 잠김방지 시스템), VDC(자동차 자세제어), NG e-Call(교통사고 긴급통보체계), MSD(최소사고정보), ESD(확장사고정보), e-Call IVS(교통사고 긴급통보장치)

ABSTRACT

In this paper, We propose the design of emergency call in-vehicle system based on NG e-Call standard for the commercial vehicle electronic control braking system. The system proposed in this paper has the basic function of automatically a traffic accident detection by collecting and analyzing vehicle and sensor data in real time. In addition, we designed the function of trigger signal receiving of vehicle's airbag deployment via the commercial vehicle electronic control braking system, Minimum Set of Data generating, Extended Set of Data making, e-Call data transmitting, and voice call for Public Safety Answering Point.

본 연구는 산업통상자원부/한국산업기술진흥원의 지역협력혁신성장사업의 지원을 받아 수행되었음(과제번호 P0021584: 사이버보안과 기능안전이 적용된 상용차용 전자 제어 제동 및 비상대응 시스템 개발)

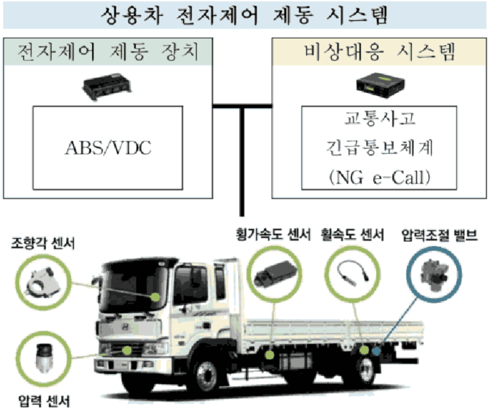

Fig 1. Commercial Vehicle Electronic Control Braking System

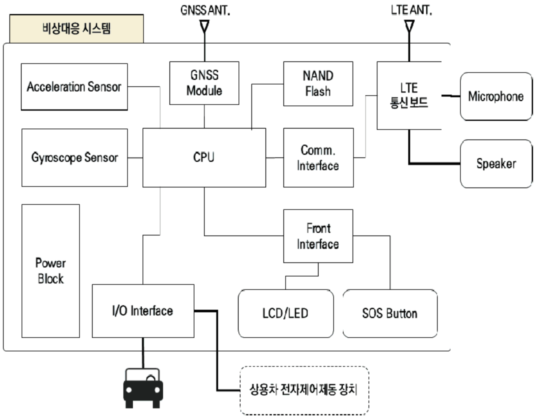

Fig 2. NG e-Call In-Vehicle System Block Diagram

* ㈜이노카/부사장
** ㈜상신브레이크/수석
E-mail : yoowon.kim@gmail.com