International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Modeling and Simulation of DoS Attack Response in WSN based IoT

Won Jin Chung, Tae Ho Cho

Abstract: ***Autonomous vehicles are cars that drive autonomously and safely to their destination. Autonomous vehicles offer driver convenience but can also be used as an attack tool to cause accidents. The attacker can infiltrate the controller area network exchanging information of the electronic control unit of the autonomous vehicles and take control of the vehicle's movement. As a result, the attacked autonomous vehicles may drive abnormally and cause an accident. In addition, an attacker can try various attacks such as a denial of service attack that sends many unnecessary packets to autonomous vehicles and paralyzes the network, and a replay attack that continuously sends old information that does not match the current road conditions. These attacks can cause vehicles accidents without infiltrative the controller area network controllers of autonomous vehicles. This paper proposes a countermeasure to denial of service attacks on autonomous vehicles, which uses the autonomous vehicles speed information sensed by sensor nodes of wireless sensor networks. In the event of an accident, for example, the autonomous vehicles detect a denial of service attack by comparing the information calculated at the base station with the Autonomous vehicles' own information. The autonomous vehicles maintain speed based on the information received from the base station. Then the base station communicates with the infrastructure based on the road condition information received from the wireless sensor networks sensor nodes. This allows the infrastructure to control the roads and prevent further accidents. This paper shows that the WSN-based IoT can be modeled and simulated based on discrete event systems to cope with denial of service attacks on autonomous vehicles, enabling them to operate normally and safely.***

Keywords: internet of things, autonomous vehicles, Wireless sensor networks, discrete event systems specification formalism, network security

I. INTRODUCTION

Internet of Things (IoT) technology is attracting attention as a means to provide various services by integration with information communications technologies (ICTs) and fifth-generation (5G) technologies [1][2]. IoT is a core service in this hyper-connected age, involving radio-frequency identification (RFID) tags, sensors, actuators, and smartphones to interconnect people and things [1]. According to Gartner [3], the IoT market predicts that 20 billion objects will be connected to the Internet by 2020, up from 3.8 billion objects in 2014. Many IoT devices can quickly share and collect information through 5G communication to provide customized services for IoT device users.

The IoT consists of devices, networks, platforms, services, and security [4][5]. The components of IoT are designed and implemented in various forms according to standards organizations and development companies. First, a device is an object that collects information from various other objects through a sensor or controls another device through an actuator. Second, the network exchanges the collection and control of information as necessary elements for device-to-device interaction or connecting a device to a platform. Third, the platform provides features for integrated management of heterogeneous devices and applications and is also responsible for connecting IoT devices to the network. Fourth, services allow users to access information on a device or platform through an application. Finally, because security uses the cloud computing capabilities of IoT devices to collect information, the inherent security of the base system is often excluded. Therefore, to enhance security, IoT devices must strengthen security by considering mutual authentication and data encryption between devices.

IoT technology has the following features for providing services to users. The first feature is two-way networks, whereby IoT technology enables people or things to exchange data in both directions [6]. One-way networks are passive services in which devices access the Internet and collect information, whereas two-way networks are active services in which devices share information with each other. IoT devices use two-way networks to enable information collection and control without human intervention. Therefore, IoT devices can acquire a large amount of information through autonomous communication and can provide various services using the acquired information. The second feature is cloud computing connectivity [7]. Most IoT devices are connected to the Internet and use cloud computing to store, process, and analyze large amounts of data without the need for high-specification information devices. In addition, IoT devices can share all the information in the external environment with other IoT devices through cloud computing.

Manuscript published on November 30, 2019.
* Correspondence Author
Won Jin Chung*, Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, Republic of Korea. Email: wonjin12@skku.edu
Tae Ho Cho*, Department of Computer Science and Engineering, Sungkyunkwan University, Suwon, Republic of Korea. Email: thcho@skku.edu

The third feature enables the sale of services through IoT devices. Enterprises can earn revenue by selling services over the network while users are using products that support IoT technology. The final feature leads to convergence and integration. IoT technology can connect with cloud, big data, and mobile technologies to create new business models and technologies. IoT technology also contributes to the creation of new industries by merging with businesses and industries that have not been previously linked due to the scalability of network connections. IoT technology is used in various fields such as smart cities, smart factories, smart farms, and smart healthcare based on the aforementioned configurations and features. Among the IoT devices that comprise smart cities, Autonomous vehicles (AVs) are being developed into a feasible technology given the current construction of 5G communication infrastructure along with expanding IoT technology [2][8].

An AV is a car that recognizes the driving environment without the driver's direct control, determines the relevant risks, and plans the driving route. Vehicles equipped with high-performance, high-reliability automatic driving functions are organically combined with infrastructure and communication technology that enables them to safely navigate various surrounding environments by utilizing complex information obtained from sensors. Advanced driver assistance system (ADAS) technology recognizes the environment and determines the risk factors [9]. Autonomous vehicles also use high-definition maps (HD maps) [10], global navigation satellite systems (GNSSs) [11], and vehicle to everything (V2X) communications for safe driving [12]. For safe autonomous driving, AVs must receive reliable information. Otherwise, they may respond to the wrong information during V2X communication and cause an accident. An attacker can cause an accident by various methods, such as a denial-of-service (DoS) attack, a distributed DoS (DDoS) attack, a spoofing attack, a black hole attack, or a replay attack on an AV [13]. The attacked AV causes an accident because the packets for vehicle information are modified (a spoofing attack) or deleted (a black hole attack), or it continuously receives previous road information (a replay attack) to maintain a speed that is not compatible with the current surrounding environment [14][15]. If an attacker attempts to attack a large number of AVs and infrastructures (a DDoS attack), the security measures of the AVs are defenseless [16]. Also, in rare emergency cases, an AV is prevented from sending an accident signal due to an attack on its V2X communication.

In this paper, we propose a scheme to reduce vehicle accidents using wireless sensor networks (WSNs) when DoS attacks on AVs paralyze V2X communication. The proposed scheme senses the speed information by using sensor nodes embedded in the road, which transmit that information to a base station (BS). The BS calculates the average speed of an AV in each road section by using the collected information and transmits the speed information back to the AV. When the V2X communication of an AV is erratic due to a DoS attack, the AV will maintain its speed by comparing and analyzing the most recent information received from V2X communication with the information received from the BS. In addition, the sensor nodes can detect a malfunction of the vehicle and transmit relevant information to the BS to prevent secondary accidents.

This paper is organized as follows. Section 2 describes AVs, WSNs, and discrete event systems specifications (DEVSs). Section 3 presents the WSN-based IoT model. Section 4 demonstrates the performance of the proposed scheme through simulation. Finally, Section 5 presents our conclusions and discusses future research.

II. BACKGROUND

A. Autonomous vehicles

i. Overview

Autonomous vehicles plan their own driving route by recognizing and judging vehicle and road conditions through V2X communication without the driver's intervention. As such, they can be used as a future means of transportation to reduce traffic accidents. According to a World Health Organization (WHO) report, global traffic accidents killed 1.35 million people in 2016 [17]. Traffic accidents are usually caused by driver carelessness, such as signal violations, drowsy driving, and age-related mistakes. Therefore, it is expected that the rapid commercialization of AVs will significantly reduce traffic accidents.

ii. Autonomous driving technical levels

The technical levels of AVs are defined as Level 0 through Level 4 by the National Highway Traffic Safety Administration (NHTSA), according to the autonomous driving function and whether it is used internationally [18]. From Level 0 to Level 2, the driver is responsible for driving and the vehicle provides only assistive functions. Level 0 has no automation and the driver initiates all of the vehicle's movements. Level 1 supports the automation of rudimentary driving tasks such as adaptive cruise control and auto emergency braking. In Level 2, two or more rudimentary tasks are automated and the driver monitors and directly controls the driving. Vehicles at Level 3 and Level 4 are self-driven, with or without minimal assistance of the driver. Level 3 is capable of autonomous driving, without operator intervention, in limited conditions such as on motorways. At Level 4, the driver only inputs the destination and the vehicle manages and controls the driving from the starting point to that destination without the driver. The current autonomous driving technology is at Level 2, but the goal is to commercialize AVs corresponding to Level 3 by 2020. To achieve this goal, AVs have been developed and studied for lane distance control and collision avoidance procedures based on lane-keeping control technology.

iii. Autonomous driving technology

Autonomous vehicles generally operate by recognizing and determining the external environment for driving, establishing a driving strategy, and controlling the vehicle. In order for AVs to recognize the external environment, an ADAS sensor is needed, usually including a mounted camera, radar, and a light detection and ranging (LiDAR) sensor to inform the driver of nearby vehicles or changes in traffic signals.

The camera sensors recognize objects in front of the vehicle and complex environments such as lanes, traffic lights, and signs. Recent improvements in camera sensors make them capable of recognizing an object in 3D and support a stereo method for acquiring shape information and distance information. Studies to further improve image signal processing are ongoing. Radar is a sensor that detects the distance and speed of surrounding objects by emitting electromagnetic waves and measuring the time and frequency of the radio waves coming back. Unlike cameras, radar has the advantage of recognizing nearby vehicles or obstacles regardless of the weather. Finally, LiDAR uses a high-power pulse laser to obtain distance information. LiDAR supports 2D and 3D scans; in 3D scans the laser can be rotated to detect the 360-degree range in detail. However, LiDAR has the disadvantages of high price and difficulty with noise interference and processing large data sets. Autonomous vehicles require at least eight cameras, at least 10 radars, and at least one LiDAR for Level 4 autonomous driving. They also need technology to judge based on information that recognizes the external environment. For example, AVs need the technology to plan the best route from the starting point to the destination, to avoid obstacles when driving, and to judge lane-keeping, turning, acceleration, and deceleration in various situations. Finally, AVs need technology to control the judged results. The vehicle control system inherent in anti-lock brake systems (ABS) has been extended to electronic stability control (ESC), electronic stability programs (ESPs), and motor-driven power steering (MDPS) [19]. These control devices have compact structures, which improves vehicle weight, maintainability, and fuel economy. However, the overall control system has a steering problem because the hydraulic and power systems are different. In addition, a sudden start and an electronic system error can cause an uncontrollable vehicle accident, a problem which must be solved.

Autonomous driving requires autonomous driving infrastructure as well as system element technology. First, a precise global navigation satellite system (GNSS) is needed to detect the location of an AV [20]. GNSS emits radio waves and calculates the vehicle location by observing the time and phase difference when the radio wave reaches the vehicle; it receives continuous 3D position and visual information, enabling the vehicle to navigate. However, in tight clearance situations a satellite-based augmentation system (SBAS) is needed [21]. For example, a large semi-trailer might have only 25 cm of clearance on the left and right to pass through a normal lane, which can be a road threat if its precise location is not known. SBAS technology delivers location information via geostationary satellites, so when used with GNSS it can pinpoint an AV. Also necessary is an HD map in which all the fixed objects on the road are represented digitally [22]. HD maps are very reliable because their information on surrounding terrain has a low margin of error. HD maps are 10 times more accurate than digital maps and display the terrain properties in 3D. HD maps have the following characteristics:

- Positioning error is drastically reduced
- Provide data that can adapt to the environment
- Existing Information is highly reliable
- Reduced system size and drive down prices
- Reduced fuel use
- Enable predictive driving with static and dynamic information

HD maps are labor- and time-intensive to create and update. To solve this problem, we are conducting research to build HD maps in near real time using artificial intelligence. Finally, cooperative-intelligent transport systems (C-ITSs) are required for autonomous driving. C-ITS helps to receive information and drive smoothly through V2X communication where the vehicle itself is difficult to recognize.

iv. Attack

Autonomous vehicles are driven in cooperation with other AVs through vehicular ad-hoc networks (VANETs), the flagship technology of V2X. VANET technology has evolved dramatically over time, but still has many security issues that need to be addressed. For example, cooperative adaptive cruise control (CACC) is an ACC enhancement that supports the co-driving of AVs by integrating wireless vehicle-to-vehicle (V2V) communications to enable monitoring of nearby vehicles. Security attacks on a CACC vehicle stream can potentially affect the string stability of the system and can compromise the safety and privacy of the CACC vehicle stream passengers. Security attacks on CACC vehicle streams are classified as the application layer, network layer, system level, and privacy leakage attacks. At the application layer, a variety of attacks damage vehicles, including message forgery attacks that manipulate and rebroadcast messages, and spoofing attacks that impersonate other vehicles to inject false information [23]. Network layer attacks can affect the functionality of multiple user applications. DoS attacks at the network layer use vehicle botnets, and such attacks can cause physical congestion. DoS attacks attempt to inundate AVs with resources, preventing them from performing other essential driving tasks. There is also a method of generating a high frequency in the channel through a jamming device to prevent communication with other vehicles. The system-level attack method is to drop packets so that the vehicle cannot receive them. Autonomous vehicles are equipped with a hardware security module (HSM) that stores digital keys and performs all cryptographic operations such as message signing, verification, encryption, and hashing. However, encryption operations in HSM are resource-intensive, which limits the number of tasks that can be processed at one time. Therefore, when a DoS attack occurs on an AV, network is paralyzed by sending an enormous amount of packets that cannot be handled by the HSM [24].

B. Wireless Sensor Networks

i. Overview

WSNs consist of small sensor nodes that use low power, and a BS that manages the sensor nodes. The sensor nodes monitor physical and environmental conditions such as temperature, sound, and pressure, and communicate wirelessly with each other when events occur [25][26]. Therefore, when multiple sensor nodes are deployed, large area monitoring is possible. The BS collects and analyzes the monitoring information and provides the processed information to the user through a wired/wireless communication network. This information is useful in a variety of areas, such as natural disasters (tsunamis, earthquakes, forest fires),

cultural property management, and building and factory automation. However, because sensor nodes are battery operated, power supply can be a problem; if multiple nodes do not receive power, some areas might not be monitored. To address this, research is ongoing to develop continuous power supply systems, such as solar cells. Sensor nodes are vulnerable to outsider attacks because they are located outside and use wireless communication. They are easily compromised by malicious attackers because of their limited computer power and memory performance; attack methods include sniffing, tampering with messages, and denial of service from the compromised nodes. Therefore, much security research has been conducted to prevent such attacks, and various security schemes have been proposed. In particular, a localized encryption and authentication protocol (LEAP), which protects packets using private keys, pairwise keys, cluster keys, and group keys, has been studied as a network layer security technique [27]. Another security scheme, an energy-efficient distributed deterministic key management scheme (EDDK), has been proposed that solves the key management problems of LEAP and uses the public key method for joining additional nodes [28].

ii. VANET-WSN

Autonomous vehicles must be able to communicate V2X for autonomous driving. VANET, the representative technology of V2X, is a part of the Mobile Ad-hoc Network (MANET) that affects vehicle safety and traffic management. VANET is based on the IEEE 802.11 a/g technology known as the Wi-fi Standard and is currently defined by the IEEE 802.11p standard, which supports transmissions up to 54 Mbps in vehicles traveling up to 200 km/h [29]. VANET supports V2X depending on the service configuration and delivery type. For example, V2V supports vehicle-to-vehicle communication, V2I supports vehicle-to-infra communication, and V2N supports vehicle-to-nomadic devices communication. However, because it is expensive to support VANET, a hybrid network, VANET-WSN communication, has been proposed [30]. The sensor nodes used in WSNs are inexpensive and are installed on roads at regular intervals to monitor road conditions. Autonomous vehicles collect messages from the sensor nodes using the IEEE 802.15.4 standard called Data Collection (DC). The sensor nodes detect changes in the state of a road, such as an accident or an obstacle, and transmits a message to the vehicle. The driver of the vehicle will hopefully have time to recognize the data and take action. The tree-like structure of routing protocol for low-power and lossy networks (RPLs) is effective for collecting data. However, since an RPL is not designed to support VANET-WSN, a GI-RPL using geographical information has been developed, whereby the information collected by the sensor nodes can be easily delivered to vehicles.

C. Discrete Event Systems Specification Formalism

i. Overview

The DEVS formalism is a mathematical framework for discrete event modeling that can be efficiently maintained because of its completeness and amenability to modification and extension. DEVS formalism is a system that uses set theory and is highly compatible with continuous-time model representation [31][32]. The DEVS formalism consists of a couple model, which is a combination of Atomic Model, which is no longer decomposed, and Atomic Model or Coupled Model.

ii. Atomic Model

The atomic model describes the behavior of a system as the lowest basic module in a hierarchical structure. Comprised of three sets and four functions, the mathematical representation of the atomic model M is:

$M = \langle X, S, Y, \delta_{int}, \delta_{ext}, \lambda, ta \rangle$
X: Set of external input event types
S: Sequential state set
Y: Set of external vent types generated as output
δ_{int}: $Q \times X \rightarrow S$: Internal transition function
$Q = \{(s,e) \mid s \in S, 0 \leq e \leq ta(s)\}$: total state of M
δ_{ext}: $Q \rightarrow Q$: External transition function
λ: $Q \rightarrow Y$: Output function
ta: $S \rightarrow$ R0, ∞ +: Time advance function

iii. Coupled Model

A coupled model is created by connecting several models internally. A coupled model is able to represent larger systems by having an atomic model or a subordinate coupled model as its children. The mathematical specification of the coupled model is as follows:

$DN = \langle D, \{M_i\}, \{I_i\}, \{Z_{i,j}\}, select \rangle$
D: Set of component names
$\{M_i\}$: Set of the basic model
I_i: Set of influences of I
$Z_{i,j}$: Output translation
$select$: Tie-breaking function

III. MODEL DESIGN

A. Overview

The proposed scheme designs and simulates a WSN-based IoT model to prevent DoS attacks on AVs. The proposed scheme analyzes and simulates how to effectively detect and avoid DoS attacks by using the V2X communication of AVs and WSN-VANET as a hybrid.

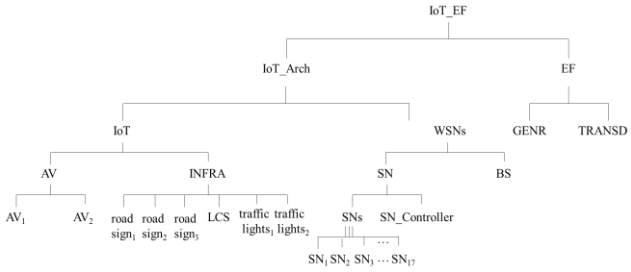

Fig. 1. Structure of the WSN-based IoT

Fig. 1 shows the overall structure of the WSN-based IoT model. This model consists of atomic models representing the real world and coupled models that connect them. All models' inputs and outputs are routed through the port. The GENR model of the EF model randomly generates general and attack events, and the TRANSD model measures the processing results.

B. Model Definition

The WSN-based IoT model is largely composed of the IoT and WSNs. First, the IoT model consists of an AV model and an INFRA model. The INFRA model consists of road sign model, a lane change system model, and a traffic lights model in detail. The WSN consists of a sensor node model and a BS model.

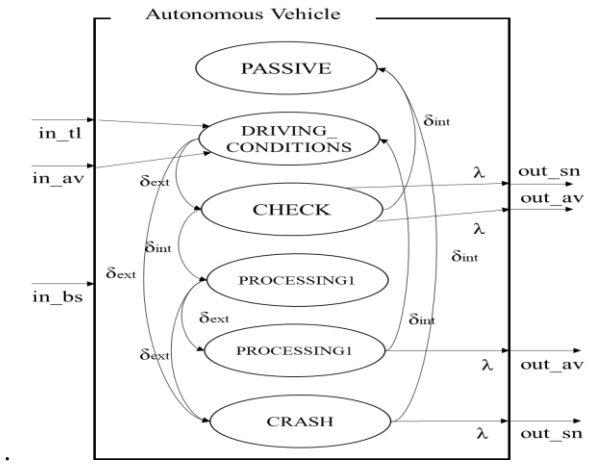

Fig. 2. State transition diagram of the AV model

Fig. 2 shows the state transition diagram of the AV model, a component of IoT. The AV model has six phases: passive, driving_condition, check, processing1, processing2, and crash. The AV model starts in the driving_condition state. When the speed information is received through other AVs or INFRA, the AV is transitions to the check state. After that, the process enters the processing1 state and waits to receive the speed information input from the BS. In the next step, when the AV transitions to the processing2 state, AV transfers the speed information compared to other AVs and transitions to either the driving_condition. If an AV receives accident information, it transitions to crash status and notifies the BS of the accident information. The AV then transitions to the passive state to prepare for the accident.

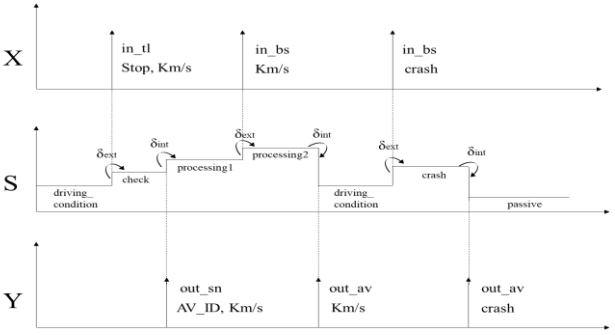

Fig. 3. Timing diagram of the AV model

Fig. 3 shows the timing diagram of the AV model. Input (X) is divided into three types and the state transition varies according to the type of input. When the AV model receives input from the infrastructure and other AVs, the state (S) transitions to the check state and the output (Y) transmits the current speed of the vehicle to the WSN model through the BS port. Then, when the average speed value is input from the BS model, the AV calculates it and transmits the speed to the other AVs through the AV's port. If the accident information is entered through the BS port in the AV model, the accident information is transmitted to other AVs to recognize the accident situation. Finally, when the stop message is received, the AV transitions to the passive state and outputs the stop message to the other models.

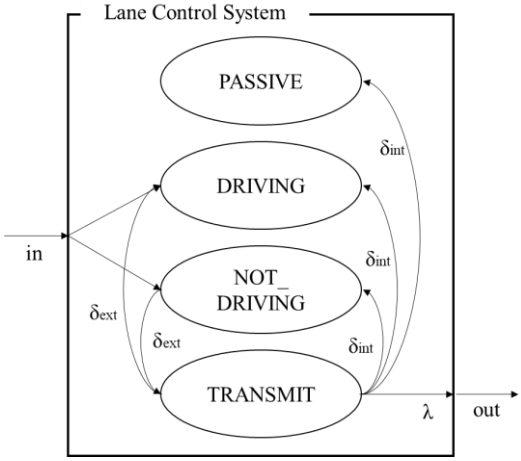

Fig. 4. State transition diagram of the land control system model

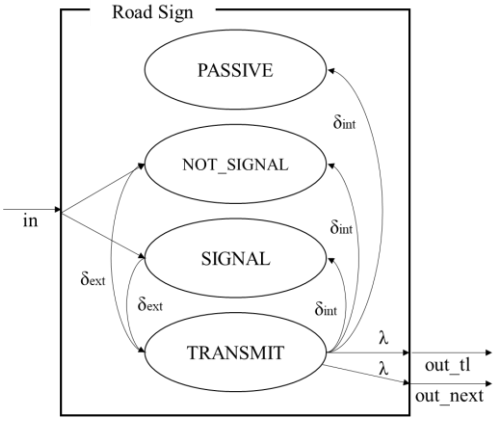

Fig. 5. State transition diagram of the road sign model

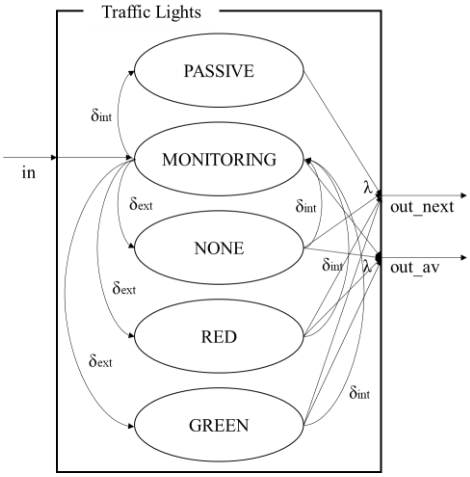

Fig. 6. State transition diagram of the traffic lights model

Fig. 4-6 shows the transition diagram of the lane control system model, the road sign model, and the traffic light model, the infrastructure of the components of IoT.

The lane control system model has four phases: passive, driving, not_driving, and transmit, and state transitions occur depending on whether or not the road is driven. The road sign model has four phases: passive, signal, not_signal and transmit, and a state transition occurs according to the specified driving speed of the road. Finally, the traffic light model has five phases: passive, monitoring, none, red, and green, and a state transition occurs according to the monitoring information of the traffic light from the AV perspective. When infrastructure models receive road information, the models make state transitions for each road situation, print the road information as messages, and send output messages to other infrastructure models or AVs.

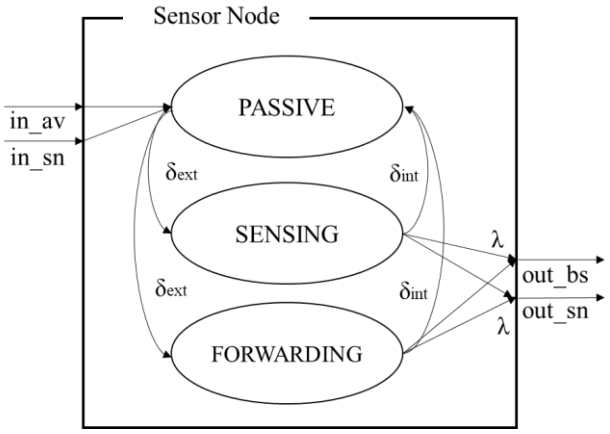

Fig. 7. State transition diagram of the sensor node model

Fig. 7 shows the state transition diagram of the sensor node model, which is component of the WSN. The sensor node model has three phases: passive, sensing, and forwarding. When the sensor node model receives an event, the sensor node model transitions to a sensing state and delivers an event message to another sensor node. The sensor node model that received the event does not transition to the sensing state, but is transitioned to the forwarding state immediately, and transmits the received message information to another node model.

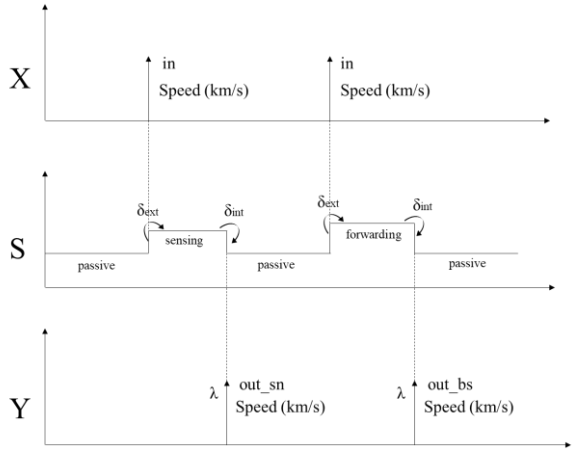

Fig. 8. Timing diagram of the sensor node model

Fig. 8 shows the timing diagram of the sensor node model. The model only inputs speed information, but the state transition depends on the port information. The first input is the information received through the AV port from the AV and transitions to the sensing state. The second input is the information received from the other sensor node model through the SN port, and transitions to the transmit state to transmit a message to the other sensor node model. The sensor node model also outputs the message to another sensor node model through the SN port, but in the case of the last sensor node, the output message is delivered to the BS model through the BS port. The SN_CNTR model selects the source sensor node model upon receiving the information generated from the AV model. When the source sensor node model is selected as the first input, the SN_CNTR model sends the output message of the source sensor node to the sensor node model of the next ID. This process is repeated to deliver a message to the sensor node model of the last ID.

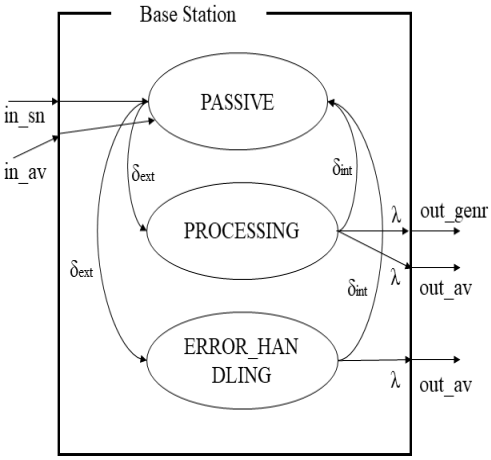

Fig. 9. State transition diagram of the BS model

Fig. 9 shows the state transition diagram of the BS model, a WSN component. The BS model consists of passive, processing and error_handling states; it is transitioned to the processing state when receiving information of the AV model through the multi-hop communication method of the sensor node model. The BS model calculates the average speed of the vehicle and passes it to the corresponding AV model. The proposed scheme can detect DoS attacks by passing the average speed to AVs and comparing the speeds. The AV compares the speed information calculated by the BS with the speed information of the vehicle and determines that it is a DoS attack when the error is large. Then the attacked AV adjusts its own speed based on the speed information received from the BS to prevent collision with other AVs. Fig. 10 shows the structure of the core functions of our proposed scheme.

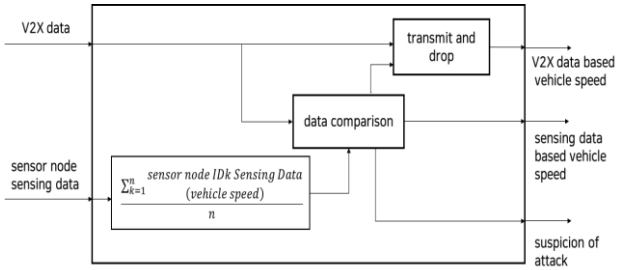

Fig. 10. Core technology of the proposed scheme

In summary, the proposed technique compares and analyzes information of AVs and BS information collected and transmitted by WSN sensor nodes, and can maintain autonomous driving even when DoS attacks are attempted on AVs.

IV. SIMULATION RESULT

The proposed scheme uses a simulation using DEVS to evaluate. The total length of the road in the simulation was 5 km and sensor nodes were placed every 300 m. The total number of sensor nodes was 17, and there were two AVs. The section where the vehicle could not be driven was at 3 km to 3.5 km, and the lane control system was located at 3 km. Road signs were placed at 1 km, 3 km, and 4 km, and the speed limit was set at 80 kph according to the Road Traffic Act in Korea. Traffic lights were placed at 2 km and 4 km, and the signals lasted 30 sec. In the simulation, events were randomly generated and were set to attack the second AV.

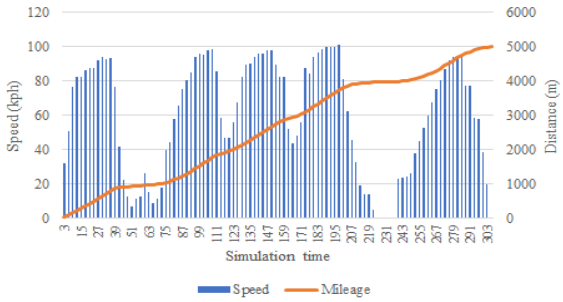

Fig. 11. AV1 model speed and mileage

Fig. 11 shows the speed and mileage of the AV1 model. The model of AV1 travels using only the information of the infrastructure, not the information of the sensor node.

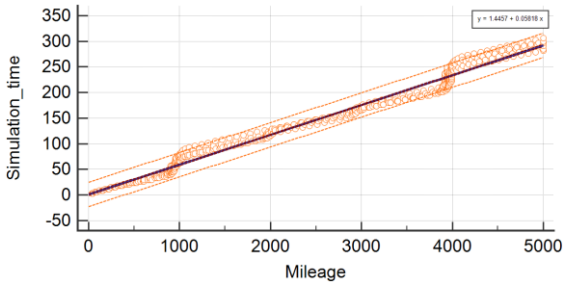

Fig. 12. 95% confidence intervals for AV1 models

Fig. 12 is a graph showing the 95% confidence interval of AV1. The graph was output using MedCalc [33].

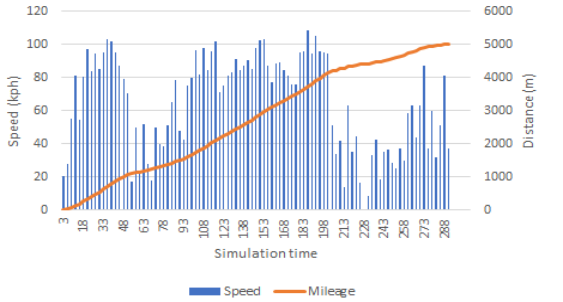

Fig. 13. AV2 model speed and mileage

Fig. 13 shows the speed and distance of the AV2 model. Because the AV2 model does not have accurate driving information due to DoS attack, the AV2 model uses the information from the infrastructure and the BS together.

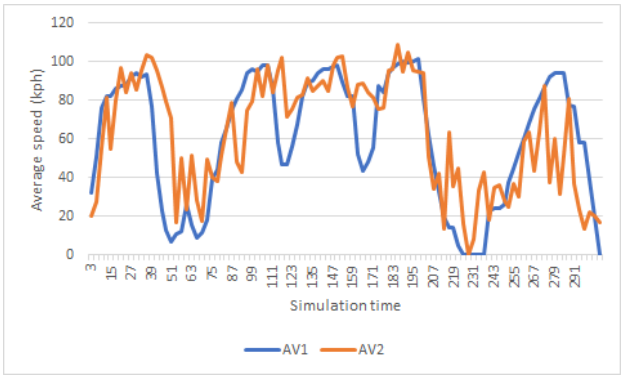

Fig. 14. AV1 and AV2 model average speed

Fig. 14 is a graph comparing the speed information of autonomous vehicles. Autonomous vehicles can drive safely without colliding with other autonomous vehicles by using information learned from V2X communication and information obtained through WSNs.

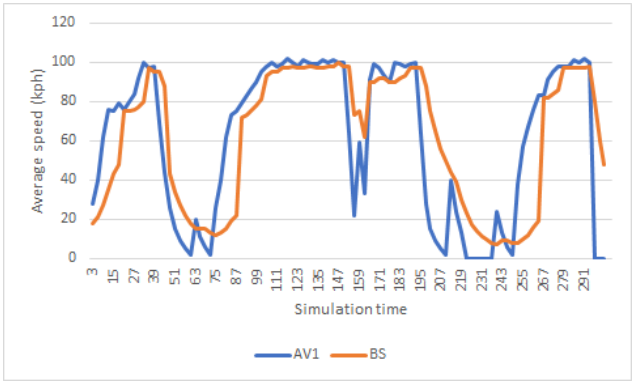

Fig. 15. AV1 model and BS model speed

Fig. 15 is a graph comparing the speed information received by V2X communication with the speed information received by the BS in the second AV. The proposed scheme demonstrates that it can prevent accidents by using information for the BS even if a DoS attack occurs in an AV.

V. CONCLUSION

An autonomous vehicle recognizes the surrounding environment through ADAS and drives without any direct involvement of a driver, through vehicle or infrastructure information and V2X communication. Autonomous driving technology can reduce accidents caused by driver mistakes and enable the driver to do other activities in the car because he or she is not driving. Although AVs provide driver convenience, when an AV is attacked it may not receive necessary driving-related signals and may cause an accident, which can cause damage and harm humans. Therefore, this paper proposes a scheme to prevent accidents when an attacker attempts a DoS attack on V2X communication, a key technology of AVs. The proposed scheme determines the speed of an AV using both the speed information obtained from the V2X communication of the AV and from the sensor nodes of WSNs.

The speed information obtained through the BS is the average speed for each section of the road. This information is less accurate than the information obtained through V2X communication in real time. However, the proposed scheme can prevent accidents from DoS attacks on autonomous vehicles by receiving speed information from BS. When V2X communication is paralyzed due to a DoS attack that causes a driver emergency, the accident situation is transmitted to the BS by way of the sensor nodes. The BS, in turn, reports road conditions to police stations and hospitals, and sends signals to infrastructure to control roads to prevent further accidents. The future research will study techniques to prevent accidents when DoS attacks simultaneously occur on AVs and sensor nodes.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. NRF-2018R1D1A1B07048961)

REFERENCES

1. L. Atzori, A. Iera, and G. Morabito. "The internet of things: A survey," Computer networks Vol. 54, No. 15, pp. 2787-2805, Oct. 2010.
2. R. Molina-Masegosa, and J. 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, Dec. 2017.
3. Gartner. "Gartner Says 6.4 Billion Connected 'Things' Will Be in Use in 2016, Up 30 Percent From 2015, Nov. 2015.
4. D. Uckelmann, M. Harrison, and F. Michahelles. "An architectural approach towards the future internet of things." Architecting the internet of things. Springer, Berlin, Heidelberg, pp. 1-24, 2011.
5. E. Fleisch. "What is the internet of things? An economic perspective." Economics, Management, and Financial Markets, vol. 5, no. 2, pp. 125-157, 2010.
6. N. Khalil, et al. "Wireless sensors networks for Internet of Things." 2014 IEEE ninth international conference on Intelligent sensors, sensor networks and information processing (ISSNIP). IEEE, 2014.
7. C. Doukas and I. Maglogiannis. "Bringing IoT and cloud computing towards pervasive healthcare." 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 922-926, IEEE, 2012.
8. M. Gerla, et al. "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds." 2014 IEEE world forum on internet of things (WF-IoT). IEEE, pp. 241-246, 2014.
9. S. Bechtolsheim, et al. "Method and system for providing an electronic horizon in an advanced driver assistance system architecture." U.S. Patent No. 6,735,515. 11 May 2004.
10. DL. Howard, et al. "High-definition X-ray fluorescence elemental mapping of paintings." Analytical chemistry vol. 84, no. 7, pp. 3278-3286, 2012.
11. JM. Dow, RE. Neilan and C. Rizos. "The international GNSS service in a changing landscape of global navigation satellite systems." Journal of geodesy vol. 83, no. 3-4, pp. 191-198, 2009.
12. S. Chen, et al. "Vehicle-to-everything (V2X) services supported by LTE-based systems and 5G." IEEE Communications Standards Magazine vol. 1, no. 2, pp.70-76, 2017.
13. D. Moore, et al. "Inferring internet denial-of-service activity." ACM Transactions on Computer Systems (TOCS) 24.2 vol. 24, no. 2, pp. 115-139, May. 2016.
14. KT. Cho and KG. Shin. "Fingerprinting electronic control units for vehicle intrusion detection." 25th USENIX Security Symposium, Aug. 2016.
15. M. Yilin and B. Sinopoli. "Secure control against replay attacks." 2009 47th annual Allerton conference on communication, control, and computing (Allerton). IEEE, Oct. 2009.
16. A. Rawat, S. Sharma, and R. Sushil. "VANET: Security attacks and its possible solutions," Journal of Information and Operations Management Vol. 3, No. 1, pp. 301-304, 2012.
17. World Health Organization. Global status report on road safety 2018. World Health Organization, 2018.
18. B. Schoettle and M. Sivak. A survey of public opinion about autonomous and self-driving vehicles in the US, the UK, and Australia. University of Michigan, Ann Arbor, Transportation Research Institute, 2014.
19. Wada, Shunichi, and Kazuhisa Nishino. "Motor-driven power steering apparatus for automobiles." U.S. Patent No. 5,404,960. 11 Apr. 1995.
20. JM. Dow, RE. Neilan and C. Rizos. "The international GNSS service in a changing landscape of global navigation satellite systems." Journal of geodesy vol. 83, no. 3-4, pp. 191-198, Feb. 2009
21. RS. Conker, et al. "Modeling the effects of ionospheric scintillation on GPS/Satellite-Based Augmentation System availability." Radio Science, vol. 38, no. 1 pp. 1-23, Jan. 2003
22. HG. Seif and X. Hu. "Autonomous driving in the iCity—HD maps as a key challenge of the automotive industry." Engineering, vol. 2,no. 2, pp. 159-162, Jun. 2016
23. AM. Malla and RK. Sahu. "Security attacks with an effective solution for dos attacks in VANET." International Journal of Computer Applications, vol. 66, no. 22, pp.45-49, Mar. 2013
24. M. Amoozadeh, et al. "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving." IEEE Communications Magazine vol. 53, no. 6, pp. 126-132, 2015
25. X. Liu, "A Survey on Clustering Routing Protocols in Wireless Sensor Networks," Sensors, vol. 12, pp. 11113-11153, Aug. 2012.
26. Weilian Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," Communications Magazine, IEEE, vol. 40, pp. 102, 2002.
27. S. Zhu, S. Setia, and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," in Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03), pp. 62–72, Washington, DC, USA, October 2003
28. 4.X. Zhang, J. He, and Q. Wei. "EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks." EURASIP Journal on Wireless Communications and Networking 2011, no. 12, 2011
29. D. Jiang and L. Delgrossi. "IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments." VTC Spring 2008-IEEE Vehicular Technology Conference. IEEE, 2008.
30. B. Tian, et al. "Application of modified RPL under VANET-WSN communication architecture." 2013 international conference on computational and information sciences. IEEE, 2013.
31. B. P. Zeigler, Object-Oriented Simulation with Hierarchical, Modular Models: Intelligent Agents and Endomorphic Systems. Cambridge, MA, USA: Academic Press, 1990.
32. B. P. Zeigler, H. Praehofer and T. G. Kim, Theory of Modeling and Simulation: Integrating Discrete Event and Continuous Complex Dynamic Systems. Cambridge, MA, USA: Academic Press, 2000.
33. MEDCALC," https://www.medcalc.org/"

AUTHORS PROFILE

Won Jin Chung Received a B.S. degree in Information Security from Baekseok University, Korea, in 2016 and is now working toward a Ph.D. degree in the Department of Electrical and Computer Engineering at Sungkyunkwan University, Korea.

Tae Ho Cho Received a Ph.D. degree in Electrical and Computer Engineering from the University of Arizona, USA, in 1993, and B.S. and M.S. degrees in Electrical and Computer Engineering from Sungkyunkwan University, Republic of Korea, and the University of Alabama, USA, respectively. He is currently a Professor in the College of Computing, Sungkyunkwan University, Korea.