International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-5, June 2020

Modeling and Simulation of Replay Attack Detection using V2X Message in Autonomous Vehicles in WSN based IoT Environment

Won Jin Chung, Tae Ho Cho

Abstract*: An autonomous vehicle is a car that drives itself to its destination without driver intervention. Autonomous driving provides driver convenience and prevents accidents caused by driver carelessness. Autonomous vehicles recognize external environments using sensors such as cameras and riders. In addition, autonomous vehicles collect information by using vehicle-to-everything communication in places they do not recognize. During vehicle-to-everything communication, vehicle-to-infrastructure communication communicates with the infrastructure installed on the road and receives information. In other words, the autonomous vehicle receives information from the infrastructure located in an unrecognized place and grasps the road conditions. However, because infrastructure is expensive to install and maintain, technology that uses wireless sensor networks instead of infrastructure has been proposed. Since the sensor node used in the wireless sensor network is placed outside and communicates wirelessly, it is easily compromised from an attacker. Attackers can use a compromised node to attempt various attacks that affect the system, such as replay attacks. These attacks can also have a fatal effect on autonomous vehicles that use information from sensor nodes. The attacker constantly transmits false information to autonomous vehicles, causing a disruption in the driver's schedule. In addition, autonomous vehicles may cause traffic accidents due to path planning using incorrect information. The proposed scheme in this paper uses an autonomous vehicle to defend against replay attacks and detects compromised nodes. The sensor node sends a message to the base station and the autonomous vehicle to notify them when an event occurs. Thereafter, the message is transmitted to the traffic management center and the base station to be mutually verified. This paper shows that by modeling and simulating EF-ITS, it is possible to defend against replay attacks with a probability of 90% and detect compromised nodes.

***Keywords*: autonomous vehicles, discrete event systems specification formalism, internet of things, wireless sensor networks**

I. INTRODUCTION

Recently, as the Internet of Things (IoT) technology and the Information and Communication Technology (ICT) technology have been developed, many devices with the latest technologies are being developed [1]. These devices are used in automation environments such as smart cities, smart agriculture, and smart factories. Among them, smart cities are a platform to solve various urban problems by combining new technologies such as ICT and big data. Smart cities aim to solve urban problems and improve the quality of life of citizens through the latest technology [2], [3]. The composition of smart cities is largely divided into infrastructure, data, and service. Infrastructure technology measures and transmits various city information to provide services to smart cities. The infrastructure technology is divided into various technologies such as communication infrastructure and spatial information infrastructure. IoT technology used in smart cities efficiently manages urban infrastructure such as roads, ports, and waterways. To construct the infrastructure, various communication technologies such as fifth generation (5G), IoT, and software defined networking / network function virtualization are used [4], [5]. Smart cities can easily share information using these communication technologies. Next, the data technology is changed or processed in an optimal form to utilize the collected information according to the service purpose. Next, data technology collects data generated in the city to solve various problems, then exchanges all information by connecting the city with different networks. Therefore, all actions that occur in the city such as energy, traffic, and weather should be processed as data. Various technologies such as artificial intelligence, blockchain, and next-generation security are required to collect information [6]. Finally, service technology provides processed information to citizens, public institutions, and service users. These services are provided by various smart devices such as autonomous vehicles, smart health, and intelligent robots. In summary, smart cities should be provided with services that will make it easier for citizens to live by organizing infrastructure and collecting data. Among the services that make up a smart city, autonomous vehicles are a key element that reduce the burden on citizens to drive [7].

Revised Manuscript Received on June 30, 2020.
* 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

Autonomous driving is rapidly developing alongside 5G, and various technologies are being researched accordingly. Recently, autonomous vehicle research has been conducted so much that the technology corresponding to level 3 will be introduced soon. Level 3 autonomous driving is a technique that maintains a lane on its own without holding the steering wheel. Security is becoming important as these cars are developed. Many security studies are being conducted to reduce traffic accidents caused by attacks.

An autonomous vehicle is a car that recognizes and judges the road conditions without driver assistance and plans its own driving route. Additionally, to find the optimal route, infrastructures that can communicate with the autonomous vehicle are needed. In other words, intelligent transportation system (ITS) technology is required for autonomous driving [8]. ITS is a technology that provides and utilizes traffic information and services by combining control and communication technologies with means of transportation and transportation facilities. ITS technology provides efficient road traffic use and driver safety and convenience, which helps reduce economic losses. ITS has services such as ATMS, ATIS, APTS, CVO, AVHS, of which the details are described in the next chapter [9]. ITS technology requires continuous monitoring through infrastructure. However, a monitorable infrastructure is expensive to install and maintain. Technologies that use wireless sensor networks (WSN) to solve cost problems have been researched [10]. A WSN can monitor a wide area using a low-cost sensor node, and collect the data monitored by the sensor node and transmit it to the base station (BS) [11], [12], [13]. The BS analyzes the collected data and delivers it to the user. However, since the sensor node is installed outside, it is easily compromised by an attacker. Attackers can cause various attacks using compromised nodes. Among various attacks using compromised nodes, a replay attack is an attack that continuously sends previously received data. If a reuse attack occurs on the sensor node used for ITS, the autonomous vehicle will only receive the previous data. Due to this, an autonomous vehicle may speed up at a time it should be decelerating, and an accident may occur. Further, the arrival time may be delayed due to continuous deceleration messages. Another possible situation is if the vehicle receives a straight message on a road that requires a turn, the vehicle will not turn and an accident will occur. To prevent such an attack, security schemes for verifying a message in a BS have been proposed. However, the verification of the message through the BS in an urgent situation may cause an accident with a late response. In this paper, we propose a method of verifying the message of a sensor node and finding a compromised node using an autonomous vehicle. When an autonomous vehicle receives a message from a sensor node, it temporarily stores the message. After that, the autonomous vehicle collects information by itself and compares it with the information of the sensor node. If the information is different, the autonomous vehicle notifies the traffic management center (TMC) of this situation [14]. When the TMC receives information from the autonomous vehicle, it analyzes the road conditions. If the wrong information is transmitted to the autonomous vehicle, the TMC sends a verification message to the BS. The BS backtracks the message to find the compromised node and takes further action. In this way, it is possible to defend against replay attacks from the WSN and detect compromised nodes.

This paper is organized as follows. Section 2 describes WSN, Autonomous vehicle, WSN-based ITS, and discrete event systems specifications. Section 3 presents the EF-ITS 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. Wireless Sensor Networks

A WSN is composed of small sensor nodes and a BS, and a large number of sensor nodes are deployed in a large area. The sensor nodes used in WSNs can detect various types of events such as sound, pressure, and light detection depending on the type of sensor. The detected events are transmitted to the BS through wireless communication between sensor nodes. Users can utilize WSNs in various fields such as hospitals, farms, and factories using events collected from sensor nodes. However, since the sensor node is low in memory and processing power, and operates on a battery, energy is limited. In addition, since it is located outside and transmits and receives data wirelessly, it can be easily compromised by an attacker. Attackers can use a compromised node to attempt various attacks, such as wormholes, replay attacks, and select forwarding attacks [15], [16], [17]. These attacks quickly exhaust the energy of the sensor node and drop important packets. Among these attacks, the replay attack stores previously received messages on the compromised node. After that, the compromised node changes the newly received message to a stored message and sends it to another sensor node. If a replay attack is attempted on a system that needs to update data in real time, the system causes an erroneous operation. Many security schemes have been proposed to prevent such attacks. However, most security techniques have the disadvantage of consuming a lot of energy from the sensor node.

B. Autonomous Vehicles

Autonomous Vehicles are a future transportation method that drive themselves to a designated destination without any driver's intervention. Autonomous vehicles communicate with various infrastructures such as other autonomous vehicles, traffic lights, and signs. Based on this, the autonomous vehicle recognizes the road conditions and plans the shortest route to the destination. Since autonomous vehicles drive on their own, traffic accidents can be reduced if universalization proceeds. According to WHO's report, as of 2016, more than 1.35 million people were damaged by traffic accidents worldwide [18]. Traffic accidents caused by vehicles are mostly caused by careless and aging drivers. When autonomous vehicles become commercially available, these problems can be solved, and such accident damage can be reduced. The function of autonomous vehicles is defined from level 0 to level 4.

The currently developing autonomous vehicle aims to commercialize by applying level 3 technology. Level 3 is a technology that enables partial autonomous driving without driver intervention in limited conditions such as a car-only road. In addition, vehicle-to-vehicle distance control and collision avoidance techniques are being further researched [19], [20]. Autonomous vehicles recognize the external environment and select the best route to reach their destination. Various technologies are needed for this.

First, an autonomous vehicle is equipped with a camera, a radar, and a LiDAR to recognize the external environment [21]. In addition, there is an advanced driver assistance systems (ADAS) sensor that notifies of nearby approaching vehicles or traffic signal changes, which helps in driving [22]. The camera corresponds to the eyes of a car and recognizes complex environments such as signs, lanes, and traffic lights. Radar measures the frequency and time of radio waves that return from firing electromagnetic waves to calculate the distance from nearby objects and the speed of the vehicle. Since radar uses radio waves, it has the advantage of not being affected by weather. Lastly, LiDAR supports 2D and 3D scanning, and can detect in 3D omnidirectional mode. LiDAR has the disadvantage of being expensive despite its good performance. Autonomous vehicles need to communicate with the infrastructure as well as sensors that recognize the external environment. The infrastructure sends information through vehicle-to-everything (V2X) communication with an autonomous vehicle in close proximity to a place where it is difficult to recognize the external environment [23]. V2X is a technology in which autonomous vehicles exchange information with other autonomous vehicles or infrastructure through a communication network. V2X is divided into vehicle-to-vehicle (V2V), vehicle–to-nomadic device (V2N), and vehicle-to-infrastructure (V2I) depending on the purpose. Through V2X communication, it is possible to prevent accidents by transmitting/receiving information on the location and speed of other cars and traffic conditions around the vehicle. To autonomously drive, a global navigation satellite system (GNSS) that measures an accurate position is also required [24]. GNSS receives 3D location information and time information continuously, and calculates the location by observing the phase and time difference when the radio waves reach the vehicle. The exact location of autonomous vehicles measured by GNSS is applied to a high-definition map (HD-map) [25]. An HD-map is 10 times more precise than digital maps, and most of the maps are expressed in 3D. HD-maps reduce positioning errors as compared to digital maps. In addition, HD-maps have the advantage of providing predictable driving by providing static and dynamic information. In this way, autonomous vehicles use various functions to drive to their destinations. That is, autonomous vehicles not only collect the external environment through their sensors, but also collect information using communication. However, if the wrong information transmitted from the outside is continuously transmitted to the autonomous vehicle, the arrival time to the destination may be delayed or an accident may occur.

C. WSN-based ITS

ITS is a next-generation transportation system that provides traffic information and services by combining intelligent technologies such as electronics, information, communication, and control with existing transportation systems to provide efficient and safe transportation [26]. ITS provides efficient transportation. Therefore, drivers can shorten their arrival time to their destination or avoid accidents using real-time information. ITS is divided into 5 services according to the purpose of use. Each service is briefly described in Table 1.

Table- I: Representative services used in ITS

Service	Service definition
Advanced Traffic Management System (ATMS)	Service for realizing the optimal signal system by grasping traffic information in real time
Advanced Traveler Information Systems (ATIS)	A service to provide drivers with real-time congestion and bottlenecks through road navigation information and GPS navigation in a vehicle
Advanced Public Transportation System (APTS)	A service aimed at improving the efficiency of public transportation by providing information on public transportation operation systems such as buses and city railroads
Commercial Vehicle Operation (CVO)	Services for efficient operation and management of business vehicles
Advanced Vehicle and Highway System (AVHS)	Service aimed at automatic driving systems using communication devices installed on vehicles and roads

Driver can drive efficiently through use of the ITS service. If ITS is introduced on the road, drivers can quickly travel to their destination by calculating the shortest route based on real-time traffic conditions and bypass information. In addition, if there are no pedestrians at the traffic lights, ITS can reduce traffic congestion caused by signal waiting by changing the signals to reduce the waiting time. ITS traffic monitoring technology is divided into inductive loop sensors, cameras, and vision-based sensors. Inductive loop sensors can detect vehicles occupying or passing through a space due to the inductance change that occurs when the insulated electric induction wires pass over the road. CMOS camera sensors can capture image data and analyze the images to analyze the traffic situation [27]. CMOS camera sensors can be powerful tools for not only measuring traffic conditions at intersections and highways, but also sending real-time video to operators. This sensing technology can be effectively used for traffic monitoring, but it can only be monitored at the installed location. Therefore, a large cost is incurred to grasp the transportation system as a whole, and additionally, installation costs and maintenance problems are caused. Therefore, a technique to solve the problem using WSNs has been proposed. WSNs solve the cost problem because they operate as a low-cost group of sensor nodes as well as provide distributed processing. In addition, since wireless communication is used, the cost of wiring installation is reduced. In addition,

sensor nodes are installed in areas where wild animals appear frequently. When the sensor nodes detect a wild animal, they use vehicular ad-hoc network (VANET) communication to send notification messages to the driving vehicle. Vehicles driving in these areas can receive alert messages to prevent accidents caused by wild animals. When sensor nodes used in WSN-Based ITS are deployed every 300m, messages can be delivered to autonomous vehicles [28], [29].

D. Discrete Event System Specification

Discrete event systems specifications (DEVS) is a formal theory proposed by Zeigler, and is a simulation theory that models the real world to derive virtual results [30], [31]. DEVS formalism is complete, easy to modify and extend, and provides tools for object-oriented modeling of discrete event systems according to mathematical formulas based on set theory. DEVS formalism is a system that uses set theory, and it has excellent compatibility with continuous time model expression. DEVS formalism is composed of an atomic model and a couple model. The atomic model is the smallest unit model that is no longer decomposed. The couple model is an atomic model or a combined model of coupled models.

The atomic model describes the behavior of the system as the lowest basic module in the hierarchical structure. The atomic model consists of three sets and four functions. The mathematical expression of the atomic model M is as follows [32].

$M=<X, Y, S, \delta_{ext}, \delta_{int}, \lambda, ta>$

X: Set of external input event types

Y: Output set

S: Sequential state set

δ_{ext}: $Q \times X \rightarrow S$: External transition function

Q is total state set of

$Q = \{(s,e) \mid s \in S \text{ and } 0 \leq e \leq ta(s)\}$

δ_{int}: $S \rightarrow S$: Internal transition function

λ: $S \rightarrow Y$: Output function

ta: $S \rightarrow R0, \infty +$: Time advance function

The atomic model expresses the state of the target system as a set S, and executes the internal transition function and external transition function to transition the state of the model.

The coupled model is a model created by connecting several models internally. The coupled model is able to express a larger system by having an atomic model or a sub-coupled model as a child. The mathematical specification of the coupled model is as follows [32].

$DN=<D, \{M_i\}, \{I_i\}, \{Z_{i,j}\}, select>$

D: Set of component names

M_i: Set of the basic model

I_i: Set of influences of I

$Z_{i,j}$: $Y_i \rightarrow X_i$: Output translation

$select$: Tie-breaking function

Simulation includes a simulator corresponding to the atomic model of DEVS and a coordinator corresponding to the coupled model. The simulation calls the functions of the implemented DEVS model and returns the results.

III. MODEL DESING

A. Overview

When an autonomous vehicle moves to a destination using WSN information, an accident may occur due to a replay attack occurring in a compromised node. To solve these problems, autonomous vehicle information and WSN information are analyzed to detect compromised nodes, and EF-ITS models are designed and verified through simulation.

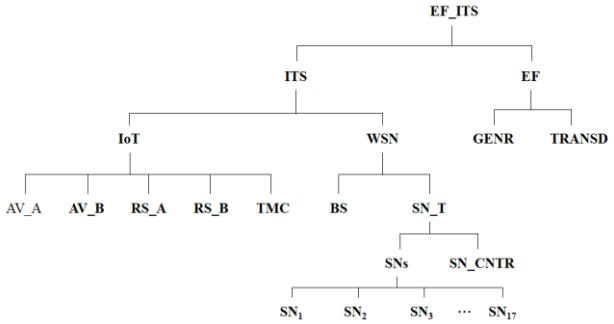

Fig. 1. Structure of the EF_ITS Model

Fig. 1 shows the overall structure of the EF-ITS model. This model consists of atomic models that represent behaviors occurring in the real world, such as autonomous vehicles and sensor nodes, and coupled models that connect them. The experiment includes an EF model consisting of a GENR model and a TRANSD model. In the GENR of the EF model, events are randomly generated, and the TRANSD model measures the processing results.

B. Model Definition

The EF-ITS model is composed of an Internet of Things model (IoT model) and a Wireless sensor networks model (WSN model). The IoT model consists of an autonomous vehicle model (AV model) that detects compromised nodes while driving to a specified destination, a road sign model (RS model) that represents a speed limit section, and a Traffic Management Center model (TMC model) that collects and manages all information related to autonomous driving. The WSN model consists of a sensor node model (SN model) that detects events and a base station model (BS model) that analyzes events received from the sensor node model.

First, the AV model and the TMC model included in the IoT model will be described. The AV model basically performs the same operation, but is divided into the AV_A model and the AV_B model to distinguish the location of the vehicle. The front vehicle AV_A model has six phases: *passive, stop, drive, report, transmit, and forwarding*. The rear vehicle AV_B has seven phases: *passive, stop, drive, transmit, compute, wait, and verification*.

Fig. 2 and Fig. 3 show the state transition diagrams of the AV models. Since the two models have different states according to roles, if the positions of the two car models change, the state of the models also changes. First, the autonomous vehicle accelerates to drive while stopped. Therefore, the AV model also starts in the stop state, the speed is calculated through the internal transfer function, and then moves to the drive state.

The AV model transitions to different states depending on the port received from other models when it is in stop and drive states. The AV model sends a message so that the SN model corresponding to the vehicle location can recognize the vehicle, and receives input from the SN model depending on the situation. The AV model transmits its position and speed to other AV models and TMC models.

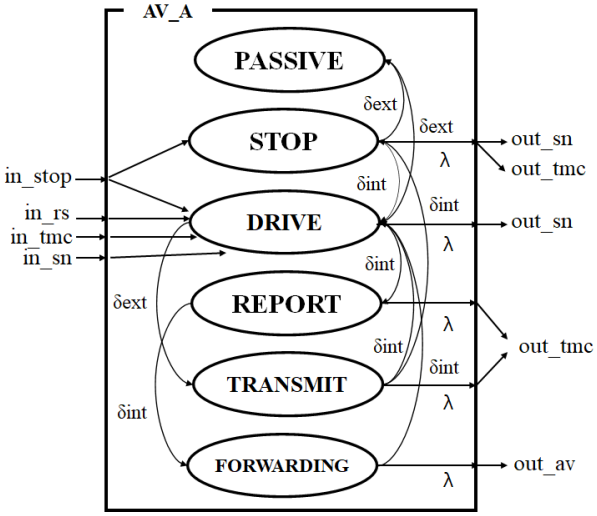

Fig. 2. State Transition Diagram of the AV_A Model

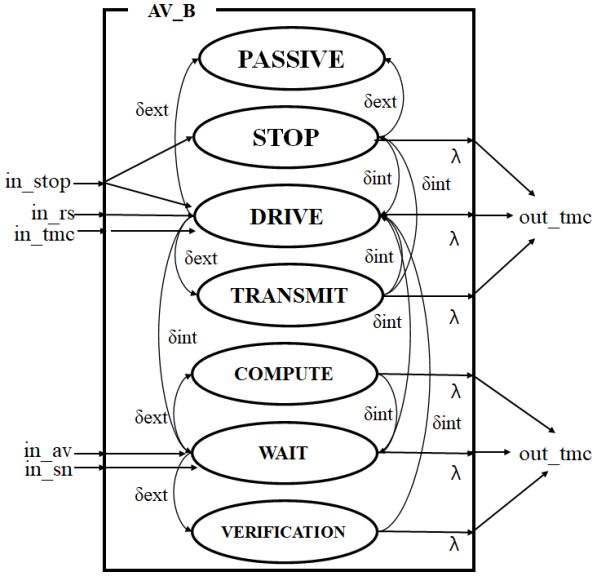

Fig. 3. State Transition Diagram of the AV_B Model

When the position of the AV model approaches the speed limit area, a deceleration message is received from the RS model. In addition, the AV model transitions to the verification state when the contents of the message received from the SN model and other AV models are different. The AV model then sends a notification message to the TMC model and maintains speed.

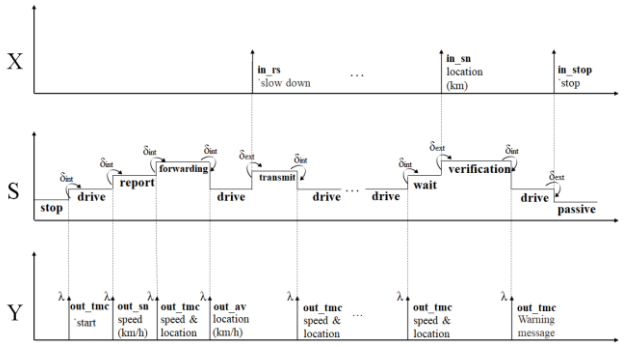

Fig. 4. Timing Diagram of the AV Models

Fig. 4 shows the timing diagram of the AV models. The input is divided into four types, and the state transition varies depending on the input port type. The AV model starts in the stop state and transitions to the drive state. The speed of the AV model changes when it is in the drive state. Then, the AV model transmits the changed information to the SN model and the other AV models. Upon receiving the V2X message from the IoT model, the state of the AV model transitions to the transmit state. AV model output is the current speed and position information of the vehicle and is transmitted to the TMC model. The AV model transitions to the verification state to verify the message received from the SN model. The received message determines whether there is an abnormality through verification, and sends the result to the TMC model. After the simulation is over, the AV model receives a stop message and transitions to the passive state.

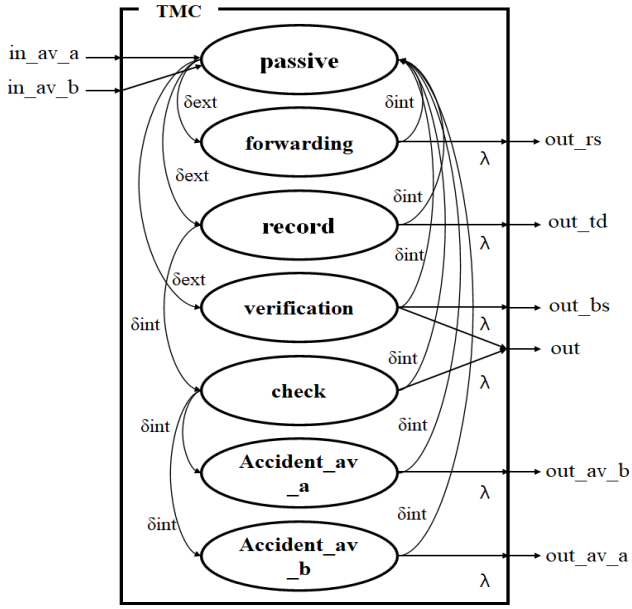

Fig. 5. State Transition Diagram of the TMC Model

Fig. 5 shows the state transition diagram of the TMC model that manages autonomous vehicles and detects replay attacks. The TMC model has seven states: *passive*, *forwarding*, *record*, *verification*, *check*, *accident_av_a*, *and accident_av_b*. When the information of the autonomous vehicle is input, the TMC model transitions to the forwarding state to determine whether the driving position is a restricted speed area and transmits the position to the RS model. The message delivered to the RS model determines whether the location of the autonomous vehicle is applicable.

If the location of the autonomous vehicle is applicable, the RS model sends a deceleration message to the AV model. In addition, the TMC model transitions to the record state to store the driving record of the vehicle. When a warning message is received from the AV model, the TMC model transitions to the verification state and checks the stored driving record to validate the delivered message. If the revalidation results determine that it is a replay attack, the TMC sends a warning message to the BS model.

In addition, if the autonomous vehicle is in an accident or an emergency stop situation, the TMC model transitions to the accident state and transmits a V2X message so that the AV model can transition to the stop state. Fig. 6 shows the timing diagram of the TMC model.

The TMC model transitions to different states depending on the input and message content. The first input shows the process of receiving location information from the AV_A model and transmitting it to the RS model.

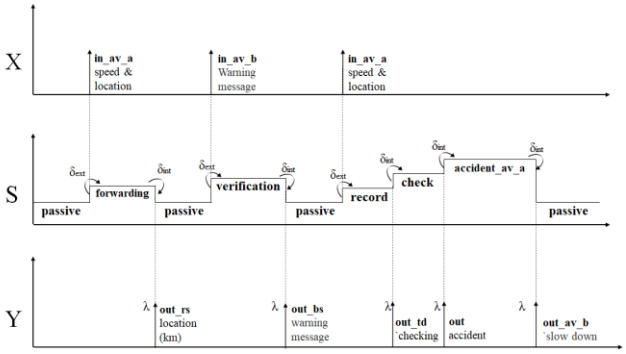

Fig. 6. Timing Diagram of the TMC Model

The second shows the process of validating the replay attack. First, when a warning message is input from the AV_B model, the TMC model transitions from the passive state to the verification state. Thereafter, the TMC model transmits the revalidation results to the BS model. The last process is when an accident occurs in the vehicle. The TMC model transitions to the check state to determine whether there is an accident. If an accident occurs, the TMC model transitions to the accident state of the vehicle and sends an accident message to other vehicles.

The following describes the SN model, SN_CNTR model, and BS model included in the WSN model.

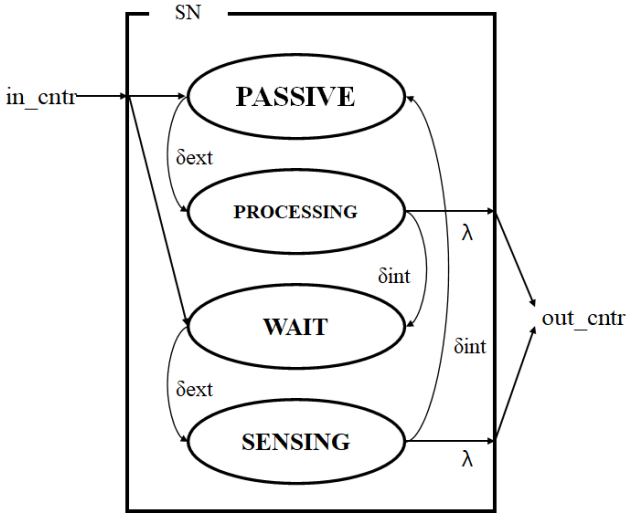

Fig. 7. State Transition Diagram of the SN Model

Fig. 7 shows the state transition diagram of the SN model that detects events and delivers them to the BS model. The SN model has four phases: *passive, processing, wait, and sensing*. The attacker attempts a replay attack using compromised nodes. Therefore, message modulation is done in the sensor node model. When a message is transmitted from the SN_CNTR model, the SN model transitions according to the content of the message, and sends the message back to the SN_CNTR model. The SN_CNTR model is a model that transmits a message by selecting a sensor node with a different ID for each location. The SN_CNTR model receives the input message and delivers it to the SN model having the corresponding ID according to the message content. Thereafter, the message output from the SN model is transmitted to the BS model and the AV model.

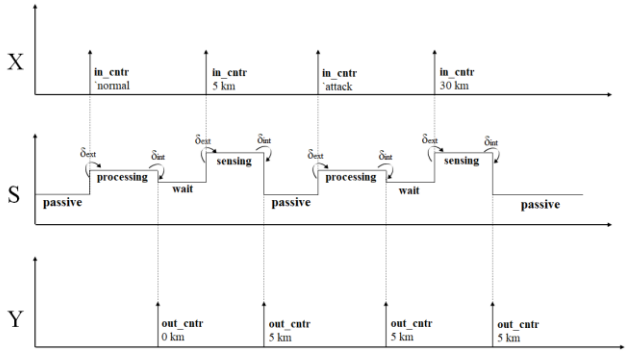

Fig. 8. Timing Diagram of the SN Model

Fig. 8 shows the timing diagram of the sensor node model. The first shows the process of delivering a normal message. The second shows the process of attacking via message tampering. First, a message generated in the GENR model is input to the SN model through the SN_CNTR model. The SN model, which received the attack message, waits to receive the message from the AV model to modulate the message. When the SN model receives speed information from the AV model, it transmits a modulated message using the previous message.

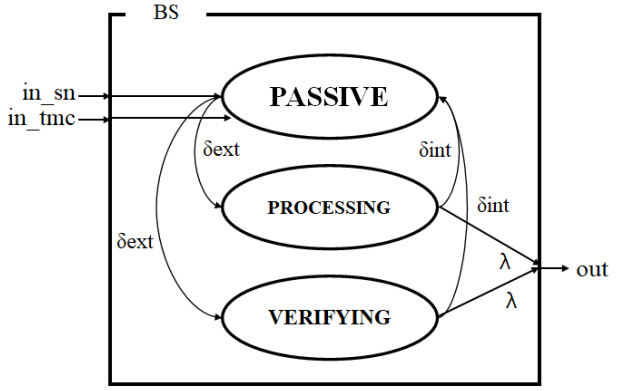

Fig. 9. State Transition Diagram of the BS Model

Fig. 9 shows the state transition diagram of the BS model. The BS model has three phases: *passive, processing, and verifying*. Upon receiving the message from the SN model, the BS model transitions from passive to processing and records the received content with the ID. Upon receiving the warning message, the BS model transitions to the verifying state. Subsequently, the BS model compares the received contents with the contents recorded by itself.

The BS model determines the replay attack through self-validation and detects the node that attempted the attack. The BS model then records the ID of the corresponding sensor node and takes further action.

IV. SIMULATION RESULTS

The proposed scheme is evaluated using DEVS based simulation. The driving distance used in the simulation is 5 km, and 17 sensor nodes are placed on the road. The restricted speed area is set to 1500m to 2000m and 4000m to 4500m, and the speed limit is set to 60kph according to the Road Traffic Act in Korea. The event value generated in the simulation is randomly generated and the attack is simulated with a probability of 40%, 60%, and 80%, respectively.

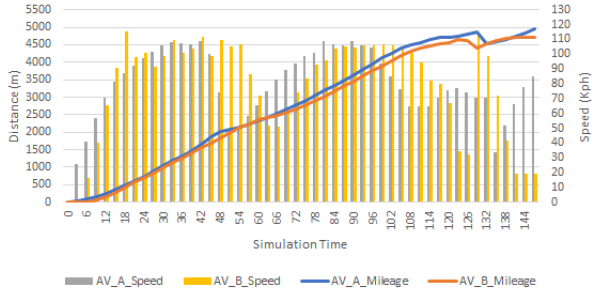

Fig. 10. AV_A and AV_B Model Average Speed and Mileage

Fig. 10 is a graph comparing the speed and travel distance of an autonomous vehicle. The autonomous vehicle shows safe driving to the destination using WSN and VANET communication even when a replay attack occurs.

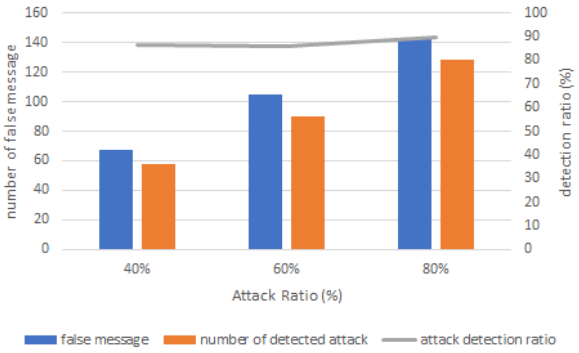

Fig. 11. Number of Attack Detections Based on the Attack Ratio

Fig. 11 shows the false message detection ratio according to the attack ratio of the replay attack. The detection rate is best when the attack ratio is 80%, and the replay attack is detected with a probability of about 89.5104%. The reason for the average detection rate of about 87% was because some events are misidentified as an attack when the speed of the autonomous vehicle was maintained. Autonomous vehicles had an average of four sudden stops when the attack rate was 80%. These results show that even if a replay attack occurs, it is possible to drive without serious damage.

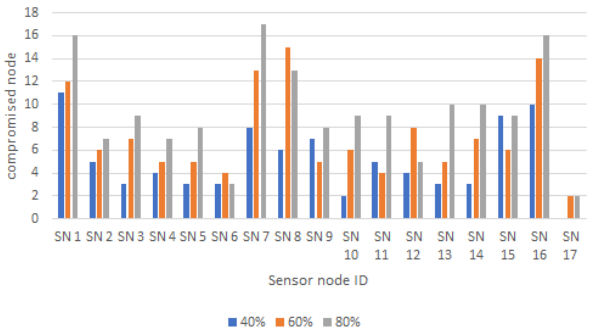

Fig. 12. Number of Compromised Nodes Based on the Attack Ratio

Fig. 12 shows the number of compromised node detections according to the attack ratio. In the simulation, a lot of attacks occur in a section where low speed driving is required. The graph confirms the number of high detections in the sensor nodes with IDs of sn1, sn7, sn8, and sn16 installed in the low-speed driving section.

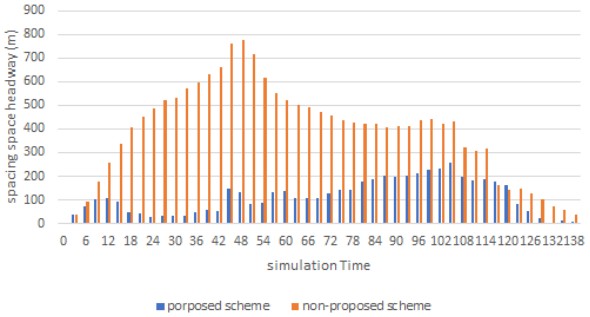

Fig. 13. Spacing headway comparison

Fig. 13 shows the vehicle spacing when the proposed scheme is applied. If the proposed scheme is not applied, the autonomous vehicle cannot maintain normal speed because it continuously receives the previous data. The graph confirms that vehicles that do not apply the proposed technique show increased spacing. When the proposed scheme is applied, autonomous vehicles can safely drive while maintaining a vehicle distance of up to 200m.

V. CONCLUSION

Autonomous vehicles recognize the surrounding environment without direct involvement of the driver, exchange information through communication with other autonomous vehicles or infrastructure, and drive themselves to their destinations. To cope with situations in which an autonomous vehicle does not recognize itself, a technique using a WSN to monitor a large area has been proposed. WSNs are installed to detect wild animals appearing on the road, and can send notification messages to vehicles through VANET communication. However, since the sensor node is installed outside, it is easily compromised. Therefore, an attacker can replay an attack through a compromised node. When a replay attack occurs through a sensor node, the vehicle continuously receives the previous message. For this reason, the drive time may be delayed or erroneous signals may be received that cause accidents. Such car accidents can lead to personal injury.

Therefore, this paper proposes a scheme to defend against replay attacks from sensor nodes and detect compromised nodes. The proposed method detects replay attacks using the following procedure. First, an autonomous vehicle that receives a message from a compromised node compares the V2X message received from another autonomous vehicle or infrastructure to determine whether the message is abnormal. Autonomous vehicles request verification by sending a V2X message to the TMC if the message is likely to be tampered with. Next, since the TMC collects information on all autonomous vehicles, it compares and analyzes the notification message received from the autonomous vehicle. After the verification, if the message is determined to be an attack, additional verification is requested from the BS for accurate determination. Finally, the BS verifies the contents using the information collected from the sensor nodes. If there is abnormally repeated content as a result of message verification, the source node is regarded as a compromised node and is coped with.

The proposed scheme can defend against replay attacks in this way and detect compromised nodes. The proposed scheme does not cover post-attack processes such as compromised node replacement or deal with traffic accident. The proposed scheme focuses on reducing vehicle accidents by detecting compromised nodes and defending against replay attacks. As a future research, we plan to study techniques to increase the detection ratio of false messages generated from replay attacks by applying artificial intelligence.

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. Nam, Taewoo, and Theresa A. Pardo. "Conceptualizing smart city with dimensions of technology, people, and institutions." Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times. 2011
3. Benevolo, Clara, Renata Paola Dameri, and Beatrice D'Auria. "Smart mobility in smart city." Empowering Organizations. Springer, Cham, 13-28, 2016.
4. 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.
5. Ordonez-Lucena, Jose, et al. "Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges." IEEE Communications Magazine, Vol. 55, No. 5, pp. 80-87, 2017.
6. Mamoshina, Polina, et al. "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare." Oncotarget, Vol. 9, No. 5, pp.5665, 2018.
7. 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.
8. Anagnostopoulos, Christos Nikolaos E., et al. "A license plate-recognition algorithm for intelligent transportation system applications." IEEE Transactions on Intelligent transportation systems, Vol. 7, No. 3, pp. 377-392, 2006.
9. Lee, Eun-Mi, Jai-Hoon Kim, and Won-Sik Yoon. "Traffic speed prediction under weekday, time, and neighboring links' speed: Back propagation neural network approach." International Conference on Intelligent Computing. Springer, Berlin, Heidelberg, 2007.
10. Losilla, Fernando, et al. "A comprehensive approach to WSN-based ITS applications: A survey." Sensors, Vol. 11, No. 11, pp. 10220-10265, 2011.
11. Akyildiz, Ian F., et al. "Wireless sensor networks: a survey." Computer networks, Vol. 38, No. 4, pp. 393-422, 2002.
12. X. Liu, "A Survey on Clustering Routing Protocols in Wireless Sensor Networks," Sensors, vol. 12, pp. 11113-11153, Aug. 2012.
13. 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.
14. Williams, Billy M., and Angshuman Guin. "Traffic management center use of incident detection algorithms: Findings of a nationwide survey." IEEE Transactions on intelligent transportation systems, Vol. 8, No. 2, pp. 351-358, 2007.
15. Win, Khin Sandar. "Analysis of detecting wormhole attack in wireless networks." World Academy of Science, Engineering and Technology. 2008.
16. Kim, Hyun-Sung, and Sung-Woon Lee. "Enhanced novel access control protocol over wireless sensor networks." IEEE Transactions on Consumer Electronics, Vol. 55, No. 2, pp. 492-498, 2009.
17. Du, Xiaojiang, and Hsiao-Hwa Chen. "Security in wireless sensor networks." IEEE Wireless Communications, Vol. 15, No. 4, pp. 60-66, 2008.
18. World Health Organization. Global status report on road safety 2018. World Health Organization, 2018.
19. Fagnant, Daniel J., and Kara Kockelman. "Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations." Transportation Research Part A: Policy and Practice 77, pp.167-181, 2015.
20. Bansal, Prateek, and Kara M. Kockelman. "Forecasting Americans' long-term adoption of connected and autonomous vehicle technologies." Transportation Research Part A: Policy and Practice 95, pp. 49-63, 2017.
21. Ibisch, André, et al. "Towards autonomous driving in a parking garage: Vehicle localization and tracking using environment-embedded lidar sensors." 2013 IEEE Intelligent Vehicles Symposium (IV). IEEE, 2013.
22. S. Bechtolsheim, et al. "Method and system for providing an electronic horizon in an advanced driver assistance system architecture." U.S. Patent, No. 6, pp. 735,515, May 2004.
23. 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.
24. 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.
25. DL. Howard, et al. "High-definition X-ray fluorescence elemental mapping of paintings." Analytical chemistry vol. 84, no. 7, pp. 3278-3286, 2012.
26. Zhang, Junping, et al. "Data-driven intelligent transportation systems: A survey." IEEE Transactions on Intelligent Transportation Systems, Vol. 12, No. 4, pp.1624-1639, 2011.
27. Roberts, Jonathan M., Peter I. Corke, and Gregg Buskey. "Low-cost flight control system for a small autonomous helicopter." 2003 IEEE International Conference on Robotics and Automation (Cat. No. 03CH37422). Vol. 1. IEEE, 2003.
28. 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.
29. B. Tian, et al. "Application of modified RPL under VANET-WSN communication architecture." 2013 international conference on computational and information sciences. IEEE, 2013.
30. B. P. Zeigler, Object-Oriented Simulation with Hierarchical, Modular Models: Intelligent Agents and Endomorphic Systems. Cambridge, MA, USA: Academic Press, 1990.
31. 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.
32. Ohn, Syng Yup, and Sung Do Chi, eds. Model Design and Simulation Analysis: 15th International Conference, AsiaSim 2015, Jeju, Korea, November 4-7, 2015, Revised Selected Papers. Vol. 603. Springer, 2016.

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.