International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 01, January-2021

Modeling and Simulation of Blackhole Attack Detection using Multipath Routing in WSN-based IoV

Won Jin Chung
Department of Electrical and Computer Engineering
Sungkyunkwan University
Suwon, Republic of Korea

Tae Ho Cho*
Department of Computer Science and Engineering
Sungkyunkwan University
Suwon, Republic of Korea

Abstract— **The Internet of Vehicles (IoV) is a technology that combines the Internet of Things and an intelligent transportation system (ITS), and it is being studied to provide driver convenience and reduce traffic accidents. Autonomous vehicles use advanced driver assistance systems sensors such as cameras, riders, and radar to recognize the road environment. In addition, autonomous vehicles use a high definition map (HD-map) to search a driving route, and use vehicle to everything (V2X) communication technology to acquire external information to drive safely. However, HD-maps and V2X communication have a lot of influence on the external environment. To solve this problem, a scheme for applying a wireless sensor network (WSN) to an ITS has been proposed. WSNs can detect wild animals, so building infrastructure in wild animal haunting areas can prevent road kills caused by autonomous vehicles. However, the sensor node of a WSN is deployed outside and has the disadvantage of being vulnerable to security because it uses wireless communication. If a black hole attack is attempted on the WSN used for the IoV, the message may not be delivered and damage from a car accident may occur. To solve this problem, the IoV must be efficiently authenticated using public keys, and WSN must detect and respond to attacks to deliver accurate information. The proposed scheme prevents accidents by detecting a black hole attack through base station and initializing the damaged node by performing secondary verification through the IoV. The proposed scheme evaluates the performance by simulation using discrete event system specifications. The proposed scheme shows a detection rate of 70% when a black hole attack is attempted with 87.0414% probability through the experimental results.**

Keywords— Discrete Event System Specification; Internet of Vehicle; Network Security; Wireless Sensor Network

I. INTRODUCTION

Due to the recent development of internet of things (IoT) technology, IoT devices are rapidly increasing and are being used in various fields. IoT is a necessary element leading to the fourth industrial revolution and is being used in conjunction with technologies such as artificial intelligence and robots [1]. IoT technology is a method of providing new services by connecting people and objects, objects to objects, and providing services in various fields such as factories, farms, and logistics industries, thereby increasing the convenience of users' work. IoT is deployed not only in tasks but also in cities to provide various services to citizens [2]. IoT is applied to CCTV systems so that they can cope with threatening situations such as crime and air pollution. In addition, IoT is deployed in cities to provide convenience for citizens through various services such as providing free WIFI, sharing vehicle flow, and weather information [3]. The main technologies of IoT are sensing technology, wired/wireless communication and network infrastructure technology, and IoT service interface technology. Sensing technology is a technology used to acquire various information such as temperature, heat, and gas from the surrounding environment [3]. Physical sensors used in IoT are evolving into smart sensors to improve application characteristics, and virtual sensing functions are also included [4]. Wired and wireless communication and network infrastructure technology is a technology that can connect various services such as 3G, 4G, and Bluetooth. Lastly, IoT service interface technology plays a role in linking people, objects, and services that make up IoT with application services that perform specific functions [5]. IoT is being deployed and used in various fields such as smart factories, smart farms, smart cities and using these technologies. In addition, IoT technology is being applied in various fields such as security, utilities, industrial automation, farming, and health care [2]. Among various fields of IoT technology, internet of vehicles (IoV) technology, in which next-generation intelligent transportation system (ITS) technology is fused, is an important factor in developing smart cities [6],[7]. IoV facilitates autonomous driving by interacting with vehicles and vehicles, vehicles and infrastructure, etc. For these functions to work smoothly, various studies on autonomous driving such as road recognition technology and accident prevention technology are required. An autonomous vehicle is a vehicle that drives itself safely to its destination by recognizing the surrounding environment without driver intervention [8],[9]. Autonomous vehicles are currently working toward commercialization of vehicles capable of level 3 autonomous driving, and can be driven on specific roads without driver manipulation. Autonomous vehicles have the purpose of providing the driver's convenience and reducing traffic accidents. Most traffic accidents start with the driver's carelessness [10]. In addition, traffic accidents are also increasing as the aging problem increases [11]. Autonomous driving technology is conducting research on improving the performance of driving technology to reduce traffic accidents caused by driver carelessness and aging. For safe driving, autonomous vehicles need environmental awareness, location recognition and mapping, judgment, control, and human computer interaction. Autonomous vehicles use sensors to create a similar field of view to that of the driver. The sensors recognize and respond to the external environment required for driving. In addition, autonomous vehicles utilize GPS technology to determine their exact location [12]. The technologies of high definition maps (HD-map) and vehicle to everything (V2X) used in autonomous vehicles reduce the risk of accidents where autonomous vehicles are not aware of themselves [13],[14]. In addition, autonomous vehicles use wireless sensor networks (WSNs) to acquire external environmental information [15]. Sensor nodes used in WSNs can communicate the location of an accident in advance, and can be deployed in a wide location to detect the appearance of wild animals and transmit information to autonomous vehicles [16]. In Korea, accidents caused by wild animals increased by about 50% in 2019 as compared to 2015. Such an accident is an anxiety factor that threatens the driver's safety, as it leads not only to damage to animals but also to secondary accidents [17]. To reduce such accidents, a method of reducing the speed of a vehicle by transmitting information about the appearance of wild animals to the driver in advance using a WSN has been proposed [15]. Autonomous vehicles can use these technologies to drive safely to their destinations. However, autonomous vehicles are susceptible to malicious attacks, which can lead to accidents. Attacks by autonomous vehicles cause traffic accidents and can result in property damage as well as personal injury [18]. To drive safely, autonomous vehicles must establish an internal security system and receive normal messages from external sources. The autonomous vehicle judges a malicious message altered by an attacker as a normal message. When autonomous vehicles receive false information, it is difficult for them to make decisions about autonomous driving, and receiving a large number of false messages can lead to an accident. Therefore, to prevent accidents involving external messages, not only the efficient security of autonomous vehicles but also the security technology of the system that transmits external information is important [18]. Among the various messages transmitted from outside, messages transmitted by WSNs can also affect autonomous vehicles. If the attacker incorrectly transmits the wild animal appearance information detected by the sensor node to the autonomous vehicle, the autonomous vehicle does not receive the information in advance and suddenly stops or an accident occurs. This is a situation that can even damage a driver in an autonomous vehicle. Therefore, even if an attack occurs, to deliver a message about wild animals to an autonomous vehicle, a security technology that detects attacks in WSNs is required. In this paper, we propose a method to protect against black hole attacks occurring in WSNs to deliver accurate information to autonomous vehicles. The black hole attacks block messages by using compromised nodes on information detected by WSNs and prevent the transmission of wild animal appearance information to autonomous vehicles [19]. To prevent such attacks, this paper proposes an additional verification scheme using multipath message delivery and IoV infrastructure in WSNs.

The structure of this paper is as follows. Chapter 2 describes WSNs and IoV. Chapter 3 presents the EF-ITS model and explains the major atomic models. Chapter 4 shows the performance of the proposed model. Chapter 5 discusses conclusions and future research.

II. RELATED WORK

A. *Wireless Sensor Networks*

WSNs are a monitoring technology in which sensor nodes are deployed in a large area to monitor and deliver results to base stations (BS) [20]. Sensor nodes are efficient devices for monitoring a large area because they are inexpensive and compact compared to other monitoring devices. WSNs can monitor a variety of environments because the sensors measured by the sensor nodes can be changed according to the purpose. The BS collects the information monitored by the sensor nodes and delivers it to the user. Users can use the vast amount of data delivered to the BS as information for applications. However, since the sensor nodes are deployed outside and communicate wirelessly, they are easily compromised by an attacker [21]. Attackers can attempt a variety of attacks using compromised nodes [22]. In particular, network layer attacks attempted in WSNs can put a load on a sensor node because the data collected by the sensor node is not delivered to the BS or the network path is incorrectly connected [22]. Because WSNs are deployed for monitoring, misleading information can confuse users. WSN security is an important issue on which many studies have been conducted. In WSN security, a technique to defend against malicious attacks using multi-path, time stamp, sequence number, etc. is being studied [23],[24].

B. *Internet of Vehicles*

IoV is a technology that combines IoT and ITS, and is a technology that will become the centerpiece of the future urban industry [6],[7]. An autonomous vehicle, a key element of IoV, is a technology that goes to its destination without the driver's manipulation. Autonomous driving is divided into levels 0 through 5 by the society of automotive engineers (SAE) [25]. Level 5 is a fully autonomous technology that enables the system to operate at all times under all conditions. Currently, companies are promoting the introduction of conditional autonomous driving technology with at least three levels or higher that enables autonomous driving on the highway [26]. In addition, research is being conducted to introduce a highly autonomous technology that allows drivers to interfere only in specific sections. Autonomous vehicles must use HD-maps for autonomous driving of three or more levels and require V2X technology to receive data from external infrastructure. An HD-map is a 3D map of the road and surrounding environment information. HD-maps have an error range of 10 cm, which is more than 10 times higher than conventional maps [13]. Autonomous vehicles recognize their surroundings with advanced driver assistance systems (ADAS) sensors such as cameras, lidar, and radar [27]. However, since autonomous vehicles are highly affected by the external environment, recognition errors occur when heavy rain or heavy snow falls. For this reason, autonomous vehicles can cause accidents if they rely solely on ADAS sensors. Therefore, an HD-map helps safe driving because it stores surrounding environment information. In addition to HD-maps, V2X, which helps to recognize the external environment, collects information from external infrastructure. V2X is divided into various elements such as Vehicle to Vehicle (V2V), Vehicle to Pedestrian (V2P), and Vehicle to Infrastructure (V2I), depending on the communication element [14]. V2V helps autonomous vehicles cope with unexpected situations that may occur while driving through communication. In addition, accidents can be communicated to other autonomous vehicles to reduce secondary damage such as chain collisions. V2I can collect various information on the road by transmitting information on the vehicle being driven to the BS. In addition, autonomous vehicles receive real-time traffic situation information from base stations in real time to prevent traffic jams or accidents. Since autonomous vehicles drive while receiving various information, the information received must be accurate. However, an attacker can eavesdrop and falsify messages sent to autonomous vehicles, causing confusion in driving. When an autonomous vehicle receives an erroneous message, the mileage and the time it takes to arrive are increased, and when the damage of an attack is large, it can cause an accident [28]. To prevent such attacks, integrity verification and sender authentication must be performed through a certificate and public key when sending and receiving messages, and a secure communication channel must be used.

C. *ITS-based WSN*

Autonomous vehicles recognize and drive road and driving environment information using technologies such as HD-maps and V2X as well as ADAS sensors. V2I transmits and receives information to autonomous vehicles using infrastructure installed on the road. In this case, a large cost and time are consumed to configure the infrastructure, and a lot of maintenance resources are consumed. In addition, in the case of an emergency vehicle such as an ambulance or an emergency situation requiring an emergency stop, the V2X may be unable to cope with the situation because it receives situation information from the infrastructure or vehicle too late. To solve this problem, a technology for collecting surrounding environment information using a WSN was proposed [15]. Since the sensor node is small and low-cost, the infrastructure configuration is flexible. WSNs monitor traffic conditions and, in the event of an accident or traffic jam, communicate to autonomous vehicles so that they can change routes. Sensor nodes are placed every 300m on the road, and because they transmit information to autonomous vehicles, they can transmit without packet loss [15]. In addition, it is possible to continuously monitor wild animals by placing sensor nodes in a large area. Before wild animals appear on the road, situational information is communicated to an autonomous vehicle so that road kills can be prevented. However, since sensor nodes are easily damaged, security is important because if an attack is attempted on the WSN, it may cause not only data forgery but also automobile accidents [22].

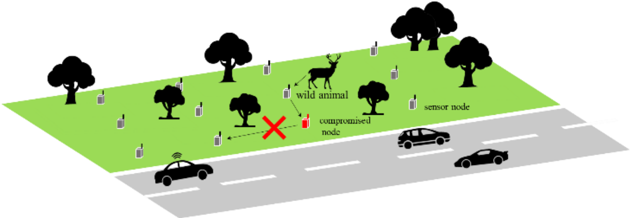

Fig. 1. A black hole attack on a WSN

Fig.1. shows a situation in which an accident may occur due to manipulation of sensor node data information. The attacker uses the compromised node to drop a message containing information about the appearance of wild animals. Since autonomous vehicles do not receive information, if wild animals appear on the road, a road kill may occur due to a late reaction of the ADAS sensor and secondary damage may occur.

D. *Discrete Event System Specification*

The Discrete event system specification (DEVS) was proposed to Zeigler as a hierarchical formalism for modelling [29][30]. The model modeled by DEVS formalism is easy to reuse, and a hierarchical model can be defined. Currently, DEVS is extended and used in various types of simulation theory such as real-time and parallel processing. DEVS formalism consists of an atomic model that expresses the behavior of the real world and a coupled model that combines it and expresses it as a large system.

1) ***Atomic Model***

The atomic model is the most basic module in a hierarchical structure and is modeled based on the behavior of the system. The atomic model consists of a total of seven functions, and the mathematical expression of the atomic model M is as follows [30].

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

X: Set of external input event types

S: Set of sequential state set

Y: Set of external output event types

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

Atomic models have ports for input (X) and output (Y) to communicate with other models. In addition, the internal transition function (δ_{int}) and the external transition function (δ_{ext}) are executed for event processing to transition the state of the model.

2) ***Coupled Model***

The coupled model is a model created by connecting several models internally. A coupled model can represent a larger system by having an atomic model or another coupled model as a child. A coupled model consists of a total of seven functions, and the experiential expression for the combined model DN is as follows [30].

DN = <X, Y, M, EIC, EOC, IC, SELECT>

X: Input event set

Y: Output event set

M: DEVS components set

EIC: External input coupling relation

EOC: External output coupling relation

IC: Internal coupling relation

SELECT: Time-breaking function

The coupled Model has the purpose of expressing a large system by combining atomic models or coupled models, and the priority of message delivery using the select function is set and executed according to the time flow.

III. MODEL DESING

A. *Overview*

Autonomous vehicles can drive safely on roads with infrastructure based on ITS-based WSNs. However, if an attacker attempts a black hole attack, information is not transmitted, so autonomous vehicles can cause accidents. To solve this problem, this paper proposes a method to detect damaged nodes and prevent accidents using WSNs and IoV. The proposed scheme composes EF_ITS and is verified through DEVS simulation.

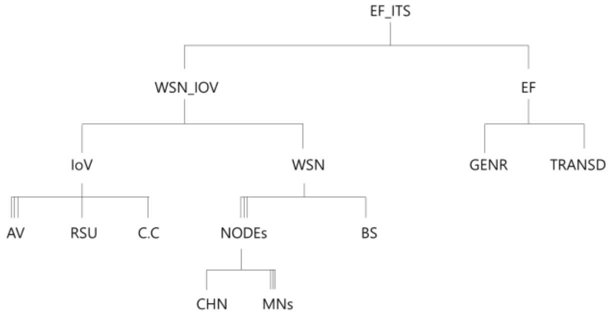

Fig. 2. Structure of the WSN-based IoV

Fig. 2. shows the structure of EF_ITS using an atomic model and a coupled model. EF_ITS includes the WSN_IoV model and the EF model. The WSN_IoV model includes an IoV model capable of V2X communication with an autonomous vehicle, and a WSN model that collects monitoring information and delivers it to a base station. The EF model includes a GENR model that randomly generates events and a TRANSD model that verifies the simulation results.

B. *Model Definition*

In this paper, to verify the performance of the proposed scheme, the elements that function in the real world are constructed as models and simulated. The IoV model consists of an AV model that functions as an autonomous vehicle, a CC model that functions as a control center that collects all information, and an RSU model that delivers information to the autonomous vehicle.

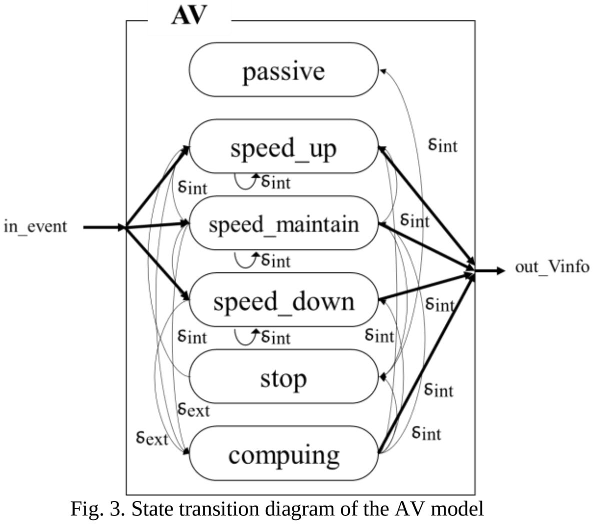

Fig. 3. State transition diagram of the AV model

Fig. 3. shows the state transition diagram of the AV model modeled after autonomous vehicle function. In AV models, most states are related to vehicle speed to express the autonomous vehicle's autonomous driving function. The AV model has the states of passive, speed_up, speed_down, speed_maintain, stop, and computing. Since autonomous vehicles drive by themselves without driver's manipulation, the state transitions through most of the AV model's internal transition functions to control speed. However, the AV model receives situation data through the in_event port when an emergency situation such as the appearance of wild animals or an accident occurs. The AV model transitions to the computing state, judges the current speed and external conditions, and transitions once more to adjust the speed to suit the situation. Later, the AV model delivers the current situation to the CC model through the out_Vinfo port.

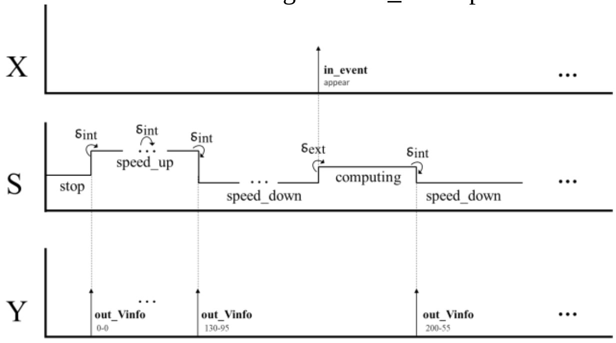

Fig. 4. Timing diagram of the AV model

Fig. 4. shows the timing diagram of the AV model. All inputs (X) of the AV model are transmitted through the in_event port. The state (S) of the AV is related to driving, and the speed is controlled through a state transition. The AV model analyzes the current situation by transitioning to the computing state when a message is delivered through the input port. The output (Y) of the AV model is transmitted to the CC model through the out_Vinfo port, and the contents of the transmitted message are speed and driving information calculated by the AV model. After transmitting the message, the AV model transitions to a speed-related state to adjust the vehicle's speed. The AV model encrypts and decrypts messages sent and received from attackers using public and private keys to maintain the integrity of messages. The AV model repeats the state transition and drives to the destination. The situation information of many autonomous vehicles is delivered to the control center through the road side unit (RSU).

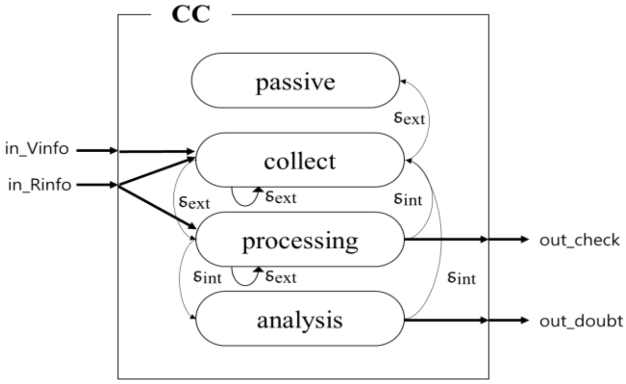

Fig. 5. State transition diagram of the CC model

Fig. 5. shows the state transition diagram of the CC model that models the function of the control center to collect and analyze various situational information. The CC model has passive, collect, processing, and analysis states. The CC model records the driving status of the vehicle and receives a message through the RSU model in case of an emergency. Since the CC model collects all the data of the IoV model, it is possible to take measures to prevent traffic accidents by judging emergency situations and attack situations through analysis and delivering messages to the AV model.

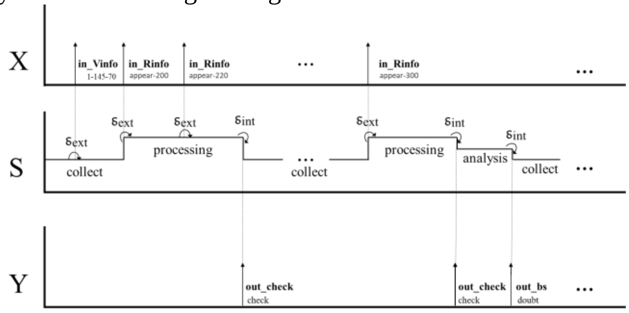

Fig. 6. Timing diagram of the CC model

Fig. 6. shows the timing diagram of the CC model. The actual control center records the driving of all autonomous vehicles. Accordingly, the CC model is recorded using driving information of all AV models transmitted through the in_Vinfo port. In addition, when a message is transmitted from the RSU model through the in_Rinfo port, the CC model transitions to a processing state and an analysis state, and is verified through data analysis of the transmitted message. The CC model detects the attack by sending a warning message to the BS model through the out_doubt port when it is determined that an attack has been attempted during message verification.

The WSN model consists of an MN model that collects events through real-time monitoring, a CHN model that collects sensor node information and delivers it to the BS, and a BS model that collects and analyzes information from the cluster head node.

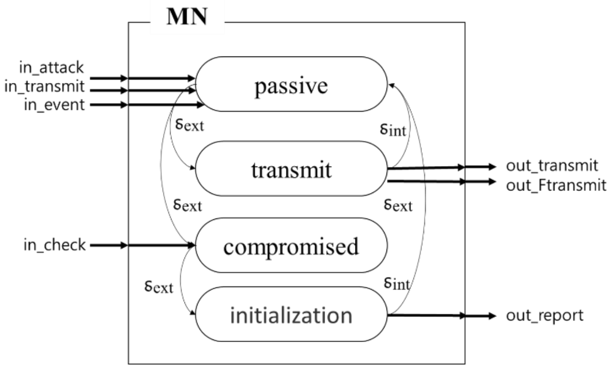

Fig. 7. State transition diagram of the MN model

Fig. 7. shows the state transition diagram of the MN model which models the functions of the sensor node. The MN model has states of passive, transmit, compromised, and initialization. The main function of the MN model is to transmit data to the BS model by transitioning to the transmit state when an event is detected. However, the MN model performs a black hole attack function that, when compromised by an attacker, transitions to a compromised state and drops all transmitted messages. The MN model that has transitioned to the damaged state repeats the message drop process until an initialization message is received from the BS model.

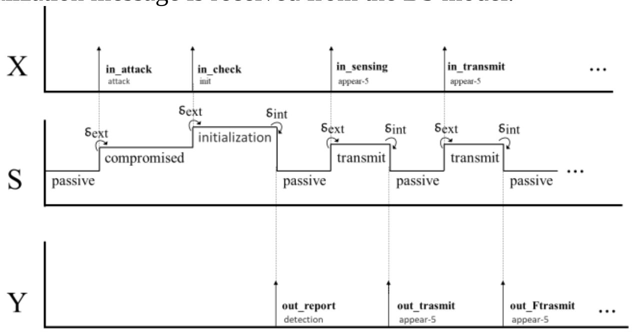

Fig. 8. Timing diagram of the MN model

Fig.8. shows the timing diagram of the MN model. The first input of the diagram shows the situation in which an attack is attempted and compromised in the MN model. In this case, in the MN model, all messages transmitted from other ports are dropped until a message is received through the in_check port. The third and fourth inputs of the diagram show the process that the MN model senses events and delivers them to the CHN model. The output ports of the MB model for the third and fourth inputs are set differently because they are transmitted to the MN model and the CHN model depending on the situation.

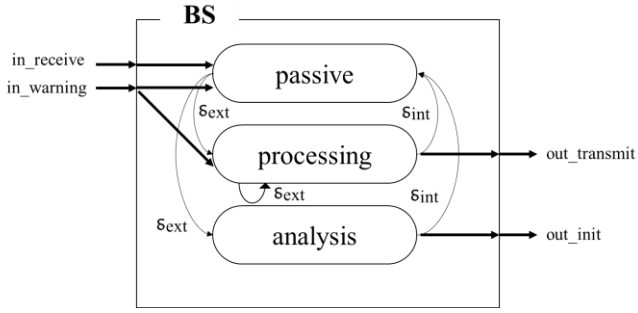

Fig. 9. State transition diagram of the BS model

Fig. 9. shows the state transition diagram of the BS model which models the function of collecting sensor node events. The BS model has passive, processing, and analysis states. Since the BS model receives all the information collected by the sensor nodes, this principle can be used for attack detection. When an event occurs, the sensor node transmits a message using multiple paths. The BS must receive two or more messages of the same content from the CHN node. When an attacker attempts a black hole attack using a compromised node, a message is dropped. Therefore, the BS cannot receive a message if the path contains a compromised node. Using this principle, black hole attacks can be detected. However, since false detection may occur due to packet loss, additional verification is required for reliable detection.

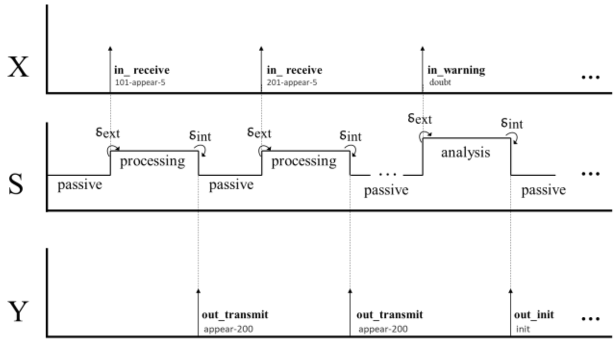

Fig. 10. Timing diagram of the BS model

Fig. 10. shows the timing diagram of the BS model. In the BS model, input occurs more than once due to message transmission from sensor nodes using multipath transmission. The transmitted message differs only in the CHN model ID, and the other information is the same. The BS model transmits event information to the RSU model through the out_transmit port which is used as driving information for the autonomous vehicle. In the proposed scheme, the appearance of wild animals is used as event and driving information to verify the performance. The last input is a message sent to the BS model after finally detecting a black hole attack in the IoV model. After that, the BS model transmits a message to the CHN model to initialize the damaged MN model.

IV. SIMULATION RESULTS

The proposed scheme uses DEVS simulation to evaluate the performance of the black hole attack detection function in WSNs. The performance evaluation of the proposed technique is simulated by modeling an IoV model, a WSN model, and an EF model that reflect the function of the real world. The total distance that AV models can drive is 6Km, and CHN nodes are placed every 300m. Each cluster head node clusters five sensor nodes into member nodes to detect wild animals. The proposed scheme evaluates the performance using three AV models. The starting point of each AV model is the same, and the starting time is different. The AV model decreases vehicle speed when the speed exceeds 110Km/s, and when wild animals occur, the speed is reduced as much as possible to prevent accidents. The GENR model randomly generates wild animal appearance events and the MN model randomly generates compromised events. A black hole attack occurs in a compromised node and receives an event from another member node, but drops it without sending it to another member node.

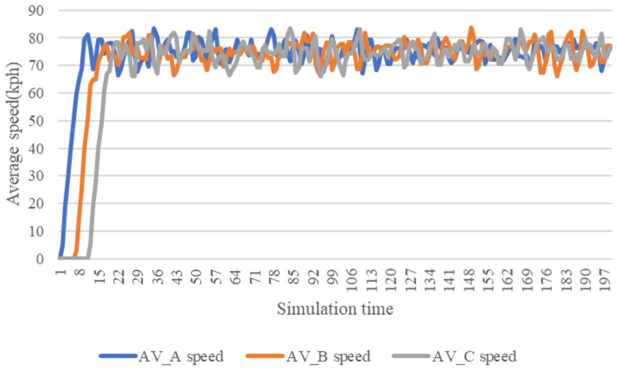

Fig. 11. Average speed of AV models

Fig. 11. shows autonomous vehicles safely driving to their destination under an attack attempt. The graph shows the state of driving while maintaining speed without an accident even if an attack occurs.

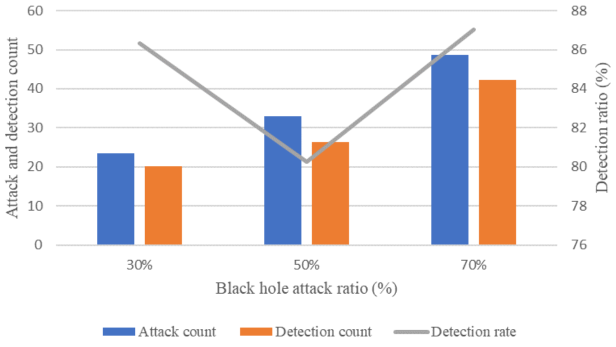

Fig. 12. Detection rate according to black hole attack rate

Fig. 12. shows the detection rate of black hole attacks according to the number of attacks. The proposed scheme shows through a graph that an attack is detected when the source node that senses the event is not a compromised node. Although the sensor node's multipath technology consumes a lot of energy, it helps to prevent accidents and detect black hole attacks by delivering accurate information to the autonomous vehicles.

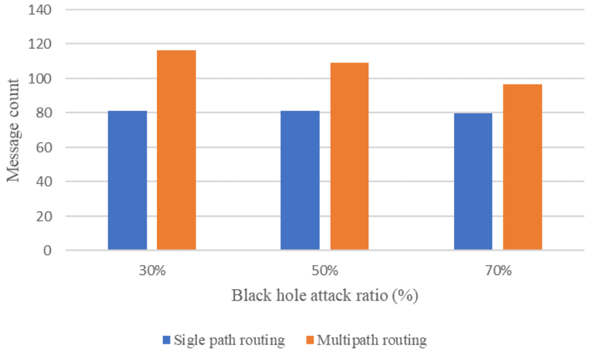

Fig. 13. Number of messages transmitted according to attack rate

Fig. 13. shows the amount of messages transmitted by the AV model according to the attack rate. The network traffic received by the AV model is more than when the proposed scheme is not used, but it has the advantage of preventing accidents from wild animals.

V. CONCLUSION

IoV is a future technology necessary to construct a smart city, and various studies are being conducted to complete the 5-step autonomous driving technology. Autonomous vehicles provide their drivers convenience because they plan and drive their own routes to their destinations without their driver's manipulation. In addition, according to the National Highway Traffic Safety Administration (NHTSA), it is stated that 94% of accidents caused by driver errors can be prevented when autonomous vehicles are commercialized [31]. Autonomous vehicles use ADAS sensors to recognize the road environment and perform safe driving using HD-maps and V2X. However, HD-maps are affected by the weather, and V2X has the disadvantage of insufficient ability to cope with urgent situations. Therefore, a technique for using a WSN in

ITS was proposed. Since the sensor nodes compose the infrastructure at a low cost, they are good for maintenance cost and are able monitor large areas. For an autonomous vehicle, using information from WSNs in areas where accidents occur or wild animals appear may be more efficient than using information from V2X. However, since sensor nodes are deployed outside and use wireless communication, they are easily compromised by attackers, and various attacks can be attempted using compromised nodes. Black hole attacks that occurs in WSNs cause confusion to users by dropping all messages delivered to the BS. In the case of ITS using a WSN, since autonomous vehicles cannot receive messages, accidents may result in places that cannot be recognized by ADAS sensors. Therefore, in this paper, we propose a second-order verification technique using multipath and IoV to detect black hole attacks. In the proposed scheme, when an event occurs, the sensor node transmits to the BS more than once by the cluster head node using multipath. After that, the second verification is performed using the autonomous vehicle and control center information. The control center delivers the attack detection result and the location of the compromised node to the BS. Finally, the BS initializes the compromised node using the information received from the cluster head node and the control center. Afterwards, IoV can continually deliver accurate information to autonomous vehicles by detecting black hole attacks and coping with compromised nodes through the proposed scheme. However, if an event occurs at the location of a compromised node, it cannot be detected through the proposed scheme because it does not generate an event detection message. In addition, since the sensor node uses multipath, there is a disadvantage in that it consumes a lot of energy. In a future research, to solve this problem, we plan to study a scheme in which the compromised node is detected using the function of IoV and the BS performs the secondary verification.

ACKNOWLEDGEMENT

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] Li, Guoping, Yun Hou, and Aizhi Wu. "Fourth Industrial Revolution: technological drivers, impacts and coping methods." Chinese Geographical Science 27.4 (2017): 626-637.

[2] Patel, Keyur K., and Sunil M. Patel. "Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges." International journal of engineering science and computing 6.5 (2016).

[3] Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future generation computer systems 29.7 (2013): 1645-1660.

[4] Islam, Tarikul, Subhas Chandra Mukhopadhyay, and Nagender Kumar Suryadevara. "Smart sensors and internet of things: A postgraduate paper." IEEE Sensors Journal 17.3 (2016): 577-584.

[5] Lee, In, and Kyoochun Lee. "The Internet of Things (IoT): Applications, investments, and challenges for enterprises." Business Horizons 58.4 (2015): 431-440.

[6] Gerla, Mario, 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, 2014.

[7] Yang, Fangchun, et al. "An overview of internet of vehicles." China communications 11.10 (2014): 1-15.

[8] Trepagnier, Paul Gerard, et al. "Navigation and control system for autonomous vehicles." U.S. Patent No. 8,050,863. 1 Nov. 2011.

[9] Janai, Joel, et al. "Computer vision for autonomous vehicles: Problems, datasets and state of the art." Foundations and Trends® in Computer Graphics and Vision 12.1–3 (2020): 1-308.

[10] Galley, Lars, et al. "Method and control device for recognising inattentiveness according to at least one parameter which is specific to a driver." U.S. Patent No. 8,742,936. 3 Jun. 2014.

[11] Attias, Danielle. "The autonomous car, a disruptive business model?." The automobile revolution. Springer, Cham, 2017. 99-113.

[12] Cui, Youjing, and Shuzhi Sam Ge. "Autonomous vehicle positioning with GPS in urban canyon environments." IEEE transactions on robotics and automation 19.1 (2003): 15-25.

[13] Seif, Heiko G., and Xiaolong Hu. "Autonomous driving in the iCity—HD maps as a key challenge of the automotive industry." Engineering 2.2 (2016): 159-162.

[14] Chen, Shanzhi, et al. "Vehicle-to-everything (V2X) services supported by LTE-based systems and 5G." IEEE Communications Standards Magazine 1.2 (2017): 70-76.

[15] Losilla, Fernando, et al. "A comprehensive approach to WSN-based ITS applications: A survey." Sensors 11.11 (2011): 10220-10265.

[16] Dyo, Vladimir, et al. "Wildlife and environmental monitoring using RFID and WSN technology." Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems. 2009.

[17] "Number of Roadkill Increased 50% in 4 Years: Most Likely Sacrifice, the Water Deer," The Kyunghyang Shinmun, July, 06, 2020, http://english.khan.co.kr/khan_art_view.html?artid=202007061611257&code=710100

[18] Yang, Yanjiang, et al. "V2X security: A case study of anonymous authentication." Pervasive and Mobile Computing 41 (2017): 259-269.

[19] Wazid, Mohammad, et al. "Detection and prevention mechanism for blackhole attack in wireless sensor network." 2013 International Conference on Communication and Signal Processing. IEEE, 2013.

[20] Akyildiz, Ian F., et al. "Wireless sensor networks: a survey." Computer networks 38.4 (2002): 393-422.

[21] Xing, Kai, et al. "Real-time detection of clone attacks in wireless sensor networks." 2008 The 28th International Conference on Distributed Computing Systems. IEEE, 2008.

[22] Wang, Yong, Garhan Attebury, and Byrav Ramamurthy. "A survey of security issues in wireless sensor networks." (2006).

[23] Li, Shuang, et al. "Efficient multi-path protocol for wireless sensor networks." International Journal of Wireless and Mobile Networks 2.1 (2010): 110-130.

[24] Xu, Ning, et al. "A wireless sensor network for structural monitoring." Proceedings of the 2nd international conference on Embedded networked sensor systems. 2004.

[25] "SAE Standards News: J3016 automated-driving graphic update," Levels of Driving, Jan. 07, 2019, https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic

[26] "Honda's new Legend will drive itself on busy roads", CNN, Nov. 11, 2020, https://edition.cnn.com/2020/11/11/business/honda-legend-autonomous-driving-intl-hnk/index.html

[27] Okuda, Ryosuke, Yuki Kajiwara, and Kazuaki Terashima. "A survey of technical trend of ADAS and autonomous driving." Technical Papers of 2014 International Symposium on VLSI Design, Automation and Test. IEEE, 2014.

[28] Brecht, Benedikt, and Thorsten Hehn. "A security credential management system for V2X communications." Connected Vehicles. Springer, Cham, 2019. 83-115.

[29] Concepcion, Arturo I., and Bernard P. Zeigler. "DEVS formalism: A framework for hierarchical model development." IEEE Transactions on Software Engineering 14.2 (1988): 228-241.

[30] Kwon, Y., et al. "Fuzzy-DEVS formalism: concepts, realization and applications." Proceedings AIS. 1996.

[31] Singh, Santokh. Critical reasons for crashes investigated in the national motor vehicle crash causation survey. No. DOT HS 812 115. 2015.