Hindawi
Security and Communication Networks
Volume 2021, Article ID 2890132, 9 pages
https://doi.org/10.1155/2021/2890132

Research Article

AVoD: Advanced Verify-on-Demand for Efficient Authentication against DoS Attacks in V2X Communication

Taehyoung Ko,[1] **Cheongmin Ji**,[1] **and Manpyo Hong**[2]

[1]*Department of Computer Engineering, Ajou University, Suwon 16499, Republic of Korea*
[2]*Department of Cyber Security, Ajou University, Suwon 16499, Republic of Korea*

Correspondence should be addressed to Manpyo Hong; mphong@ajou.ac.kr

Received 21 June 2021; Revised 17 October 2021; Accepted 10 November 2021; Published 1 December 2021

Academic Editor: Azeem Irshad

Owing to the development of information and communication technology (ICT), autonomous cooperative vehicles are being developed. Autonomous cooperative driving combines vehicle-to-everything (V2X) communication technology in existing autonomous driving and provides safe driving by sharing information between communication entities. However, security factors should be considered during communication. Security Credential Management System (SCMS) has been proposed as one of these elements, but it is vulnerable to denial-of-service (DoS) attacks due to message authentication costs. In congested situations, the number of messages exchanged between vehicles becomes very large. However, the performance of the on-board unit (OBU) is not sufficient to handle huge number of messages, which can lead to a DoS attack. Therefore, a technique to prevent DoS attacks on autonomous cooperative driving vehicles using SCMS has been proposed in this paper. The proposed technique reduces authentication costs by classifying similar messages into multiple categories and authenticating only the first message represented in the group for a unit time. The effectiveness of this technique has been demonstrated by comparing the time it takes to verify huge number of message signatures in each method.

1. Introduction

With the recent development of information technology, autonomous driving technology has been actively researched in the automotive field. Research costs in the automotive field are increasing every year, and the proportion of software and computer services is also increasing. In addition, patents for self-driving cars have been increasing since 2015 [1,2], and IT companies such as Google and Apple, as well as automobile manufacturers, such as Mercedes and BMW, have been developing self-driving cars [3]. The advantage of autonomous driving is that there are fewer errors caused by humans because of minimal human intervention, compared to manual driving. In particular, according to a survey [4] conducted by the National Highway Traffic Safety Administration (NHTSA), 94% of car accidents were caused by drivers. Therefore, it is possible to perform safe driving using autonomous driving technology in which the driver is a system and not a human being, when compared to manual driving.

However, because autonomous driving alone is not sufficient to perform safe driving, autonomous cooperative driving using vehicle-to-everything (V2X) communication technology is required. Autonomous cooperative driving is not judged by only one vehicle but communicates with nearby vehicles or roadside fixed V2X communication units (road side unit (RSU)) to make judgments for safer driving. However, security factors must be considered, because V2X communication is used to communicate with other elements. In fact, white hackers infiltrated vehicles from the outside and showed examples of attacks that manipulated various functions in the vehicle [5,6]. In this regard, measures for message integrity verification, authentication, and personal protection should be implemented. As a result, security system and standards have been established.

The U.S. Department of Transportation (USDOT) is currently developing, applying, and implementing a V2X security authentication system called the Security Credential Management System (SCMS) [7] to enhance the security of autonomous cooperative driving. The SCMS is a PKI-based

message authentication system. Each participant performing V2X communication using SCMS can trust shared information through authentication. There are three design objectives for the SCMS. The first is to ensure accuracy and reliability of the information exchanged, the second is to protect the privacy of the driver, and the third is to support the identification of devices revoked through malfunctioning device identification and certificate revocation list (CRL) distribution. Therefore, the SCMS provides a security infrastructure for issuing and managing security certificates. Each entity that wants to perform V2X communication can register with the SCMS, obtain a security certificate from the certification authority, and authenticate the message to prove that it is a trusted entity. Certificates used in SCMS are largely divided into certificates for the on-board equipment (OBE) and certificates for the RSU. Certificates for OBE include OBE Enrollment Certificate, Pseudonym Certificate, and Identification Certificate. The OBE can request for another certificate using Enrollment Certificate. Pseudonym Certificate is mainly used for short-term, basic safety message (BSM) authentication, and misbehavior reporting. Multiple Pseudonym Certificates obtained from the Pseudonym Certificate Authority are changed after expiration validity period. The OBE uses Identification Certificates to identify special and public vehicles. Certificates used by the RSU include the RSU Enrollment Certificate and Application Certification. An Enrollment Certificate is used by the RSU to receive application certification. Application certification is used by the RSU to provide secure transportation services, such as signing over air messages. During V2X communication, each entity can report misbehaving *o* malfunctioning. CRLs are created through misbehavior report and added to the blacklist inside SCMS. Each entity can block messages from revoked entities using CRLs.

Society of Automotive Engineers (SAE) has created a standard that defines the Dedicated Short Range Communications (DSRC) message set and On-Board System Requirements for V2V Safety Communications. The message used by each entity to exchange information with each other uses the message defined in document SAE J2735 [8]. SAE J2735 is Dedicated Short Range Communications (DSRC) message set. SAE J2735 includes a set of DSRC messages, a data frame, and data elements that make up each message. Some of these message sets include the basic safety message (BSM), common safety request (CSR), and emergency vehicle alert (EVA). BSM is a message that contains basic information about a vehicle, including its current location, speed, gear information, and braking information. BSM broadcasts 10 messages per second to surrounding vehicles. CSR can be unicast as a message asking for additional information between vehicles exchanging BSMs. Additional information requested by CSR includes light, wiper, brakeStatus, brakePressure, and weather data measured by sensors. The EVA message broadcasts a warning message that an emergency vehicle is operating nearby and that the vehicle's drivers need attention. In addition to the above-mentioned messages, other messages defined in J2735 are used to communicate with vehicles to exchange road and driving information for safe driving.

SAE J2945/1 [9] is a standard document that contains the system requirements of the on-board unit (OBU) for secure V2V communication proposed by SAE. The standards specify the standard profiles, functional requirements, and performance requirements. The standard profiles contain 802.11 related requirements for basic communication and IEEE 1609.2 [10] related to security. In particular, it is required to use Secure Hash Algorithm (SHA) 256 as the hashing algorithm and Elliptic Curve Digital Signature Algorithm (ECDSA) 256 with NIST p256 as the signature. Symmetric encryption requires support for AES-128. In addition, there are requirements for recording the position of the vehicle and the route it travels.

Despite these security systems, V2X communication has a big security threat. That is a denial-of-service (DoS) attack. DoS attacks on SCMSs can cause delays in traffic flow as well as car crashes. Therefore, the goal of this paper is to propose advanced verify-on-demand (AVoD), a technique to prevent DoS attacks on autonomous cooperative vehicles using SCMS, and to validate its effectiveness in preventing DoS attacks.

The remainder of this paper is organized as follows. Section 2 discusses related works on DoS attack in V2X environment and its countermeasure. Section 3 describes the security analysis in autonomous cooperative driving. Section 4 explores the AVoD proposed in this study. Section 5 examines the actual implementation of AVoD, and Section 6 presents the conclusions.

2. Related Works

In the V2X environment, a safe driving environment is provided by exchanging information between each entity. Due to these characteristics, an attack that reduces availability can have a fatal impact on the whole network. This section discusses research on attacks that compromise availability and studies on countermeasures for such attacks.

Trkulja et al. [11] introduced a set of denial-of-service attacks on C-V2X networks operating in Mode 4. The attack presented in this research is caused by adversarial resource block selection. This attack is a very sophisticated and efficient attack. In this study, each attack is analyzed by setting three types of enemies. With a fixed number of attackers, this study shows that smart and cooperative attacks can have a significant impact on network performance when the vehicle density is low, whereas when the vehicle density is high, the unconscious attack is more effective than sophisticated attack.

Another type of attack that reduces availability is a jamming attack. Safety applications in vehicle networks include real-time information contained in periodically exchanged messages called beacons. A jamming attack that interferes with beacon transmission is studied in the work of Benslimane et al. [12]. This study investigates the effect of jamming attack on beacon broadcast and proposes a real-time MAC (Media Access Control) based detection method for jamming attack. This method works well when the number of vehicles constituting the platoon is fixed, while it

does not work well when the number of vehicles belonging to the platoon changes frequently.

Studies have been conducted on the use of lightweight protocols in the authentication process to prevent attacks that compromise availability [13–15].

In 2020, Vasudev et al. [13] proposed lightweight mutual authentication scheme for V2V Communication in Internet of Vehicles. In their work, a scheme with a lower computation cost was proposed compared to the efficient mutual authentication schemes that were previously proposed [16–18]. In addition, those authors used SHA-3 with 256 bit, which is relatively robust in collision attacks compared to the study using SHA-1 [19]. This scheme performs 17 hash functions including the registration phase to perform mutual authentication. This method consumes lower computation cost compared to the existing methods, but still has vulnerabilities to collision attacks. In particular, the security strength is lower than that of ECDSA, which provides strong authentication. In addition, it cannot be applied to environments using SCMS. S.A.A. Hakeem et al. [14] proposed lightweight message authentication and privacy preservation protocol for V2X communications. This scheme uses hash chain of secret keys for a Message Authentication Code (MAC). It reduces computation overhead and communication overhead compared to using standard security protocols. The advantages of this technology are attractive, but useless in an environment where standards are enforced. In 2018, S. Taha et al. [15] proposed lightweight group authentication scheme for achieving low latency with high mobility in vehicular networks. For this reason, the authors clustered vehicles and assigned each vehicle a role within the cluster. Their scheme aims to create a shared group key within the cluster as well as mutual authentication between vehicles in the cluster. However, their scheme is a group authentication method and cannot be applied to the V2X network using SCMS targeted in this paper.

Another countermeasure is to improve the authentication speed using hardware. Using General-Purpose computing on Graphics Processing Units (GPGPU) to accelerate the hardware, ECDSA authentication speed improvement was achieved [20]. However, in OBU or RSU that performs ECDSA, the performance of the GPU is low, so it is difficult to exert a great effect. Another scheme [21] is to use parallel programming. This method is available because most embedded CPUs have multicores. Those authors performed ECDSA signature verification in parallel using 16 threads. As a result, the processing speed was four times faster than that of a single thread.

The last countermeasure is to change the authentication policy. SAE proposed verify-on-demand (VoD) [22] to increase the processing speed of the encryption module, address the security vulnerability presented above, and ultimately prevent DoS attacks. VoD changes the authentication policy instead of using the authentication protocol specified in IEEE1609.2 by using this; the number of messages to be authenticated is reduced. VoD will be covered in more detail in Section 3.

3. Security Analysis

There are two security vulnerabilities in autonomous cooperative driving using the SCMSs. The first is the processing speed of the encryption module. In the Notice of Proposed Rulemaking for Federal Motor Vehicle Safety Standards [23] issued by the National Highway Traffic Safety Administration (NHTSA), it is stated that DSRC equipment must perform validation of at least 5500 BSMs per second. Message processing proceeds in the order of interpreting the content of the message after its authentication. Therefore, in crowded situations, the OBU must be able to perform more than 5500 BSM signature verifications per second. However, ECDSA cannot process 5500 BSMs per second because it requires more time to authenticate than the existing RSA [24–27]. According to the research that measured the authentication time in the actual OBU [14], processing speed of OBU is only 35 verifications per second in the case of the software module. In the case of the hardware module, processing speed of OBU is only 163 verifications per second. Eventually, owing to limitations in the performance of hardware and cryptographic modules, many BSM authentications arising from congestion situations are not performed well. The second vulnerability is DoS attack. This vulnerability arises from the aforementioned vulnerability, which prevents the normal behavior of OBUs by sending more BSM messages than they can handle. These vulnerabilities can lead to traffic accidents or congestion during autonomous cooperative driving using SCMSs. Furthermore, if authentication is omitted to prevent DoS attacks, the risk of forgery or tampering attacks is encountered. In this section, situations in which conflicts occur in autonomous cooperative driving environments and security threats that can arise in each situation are discussed.

3.1. Attacker Model. In this study, the attacker launches a DoS attack on a vehicle that performs autonomous cooperative driving. The goal of a DoS attack is to disrupt the road and ultimately paralyze it. Vehicles targeted for attack are vehicles located within 1 km radius of the attacker, which is the propagation range of basic DSRC/WAVE messages. The attacker must be able to generate a large number of BSMs. The attacker can send BSMs more than 10 times per second using the modified program. The attacker has multiple certificates normally issued from the SCMS. It is assumed that the attacker remotely penetrates vehicle of the normal user through backdoor for obtain a certificate. Using these certificates, the attacker sends BSMs as impersonating normal user. The victim reports to Registration Authority (RA; RA manages CRLs) to add a certificate that signed the attack BSMs to CRLs. Since then, when BSMs signed with a certificate listed in CRLs are received, those are dropped. For this reason, attackers use a different certificate for each attack to effectively perform attacks. It is also assumed that more than one attacker OBU is used to transmit 5500 BSMs per second.

3.2. Attack Situation. In SAE J2945/1 [9], seven threatening crash-imminent scenarios were selected considering the frequency, cost, and functional years lost. It is designed to prevent collisions by operating safety applications for each scenario. Crash-imminent scenarios are shown in Table 1. All of them, except blind spot warning (BSW) and lane change warning (LCW), operate using sensors and BSM. Therefore, in order to avoid collisions, it is important to receive the BSM without interruption. The attacker uses this point to perform an attack. As shown in Figure 1, the attacker sends a large number of BSMs to the target vehicle. Vehicles within the attacker's DSRC/WAVE transmission range become the target vehicle. When the attack starts, the target cars cannot receive BSMs normally. Because BSMs cannot be received normally, among the scenarios shown in Table 1, other scenarios except 'Vehicle(s) Changing Lanes-Same Direction' have a high probability of collision. For example, when a lead vehicle is stopped, it is necessary to detect the sudden halt of the vehicle in front, using FCW. However, it does not receive the BSM due to a DoS attack, which causes a crash owing to the delay in understanding the situation that occurred earlier.

3.3. Countermeasures. As discussed in Section 2, two countermeasures are considered to prevent this security threat. The first is using hardware. A simple method is to use a high-performance processor in OBU for authentication. Other methods are methods of using a hardware module. Authentication speed can be improved using GPGPU [20] or Hardware Security Module. However, this method is not covered in this paper because this method requires additional hardware.

The second countermeasure is the software method. Software methods include changing authentication policies and using a lightweight authentication algorithm. A lightweight authentication algorithm can be used to perform authentication quickly and securely. However, since this paper targets the V2X network using SCMS and IEEE 1609.2, this method is not discussed. Finally, the method presented in this paper changes the authentication policy. This paper uses the ECDSA required by the standard and proposes a more efficient authentication policy.

The method of performing message authentication in SCMS is the verification and then process (VATP). As shown in Figure 2, the OBU first authenticates the messages received from the antenna, checks the threat level, and then notifies the driver if they are determined to be a threat. This method performs authentication on every message; thus, the slower the encryption module processes, the slower the driver is informed of the threat. In addition, a DoS attack that consumes all the computing power of OBUs for authentication, thereby preventing it from performing other functions, can occur.

The basic flow of the VoD is shown in Figure 3. Unlike VATP, which performs message authentication first, VoD first checks the threat level of the message after receiving the message. Subsequently, only messages judged to be threats are authenticated. This message is called "threat message (threat BSM)." In conclusion, if it is not a threat message, it is ignored. It means that authentication is not performed. This approach prevents DoS attacks by reducing messages to be processed, compared to conventional methods, because only threat messages are authenticated.

Table 1: Crash-imminent scenarios and its safety applications [9].

Crash scenario	Safety applications
Lead vehicle stopped	FCW
Lead vehicle decelerating	EEBL FCW
Control loss without prior vehicle action	CLW
Vehicle turning at nonsignalized junctions	IMA LTA
Straight crossing paths at nonsignalized junctions	IMA
Vehicle) changing lanes—same direction	BSW/LCW
Left turn across path—opposite direction	LTA

4. AVoD (Advanced Verify-on-Demand)

4.1. AVoD Overview. The VoD discussed above is a technique that prevents DoS attacks by reducing the number of messages to be processed. However, this technique is still vulnerable to DoS attacks. VoD only authenticates messages deemed to be threats, and if the number of such messages exceeds the processor's throughput, the DoS attack will still be valid. Therefore, in this section, advanced verify-on-demand (AVoD) is proposed. The basic flow of the AVoD is shown in Figure 4. AVoD is a method that performs authentication smoothly, even when many BSMs that are considered to be threats are received. AVoD prevents DoS attacks by classifying messages deemed as threats and authenticating only the first message represented in the group for a unit time.

4.2. AVoD Components. The AVoD module consists of a threat table and a threat classifier. The threat classifier categorizes messages based on the criteria for current driving conditions. Classified messages are stored in threat table and sent to signature verification module. If there is a message already classified as the same type, the next message is ignored without signature verification. Threat table is a table that stores messages classified by the threat classifier. Table 2 shows an example of threat table in which packets are recorded. It records safety applications, vehicle locations, vehicle directions, and number of packets.

4.3. AVoD Algorithm. A Threat classifier classifies each received BSM according to relative location with other vehicles and stores it in threat table. In this way, when more than 5500 threat BSMs occur per second, these BSMs can be classified into several types. After that, only the first message of each type performs signature verification and subsequent messages are ignored. The reason is that the threat to the ignored message is already generating an alert.

There are three criteria for classifying BSMs in a threat classifier. The first is the safety application to be used. The message is classified by determining the safety application

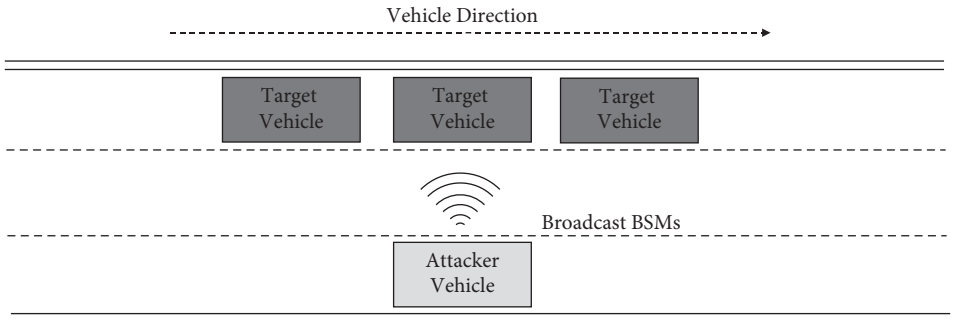

Figure 1: Attack situation.

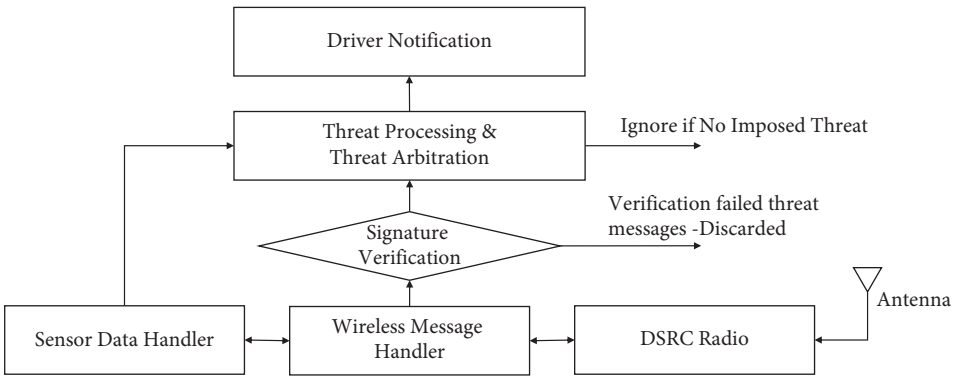

Figure 2: Verify-and-then-process flow [22].

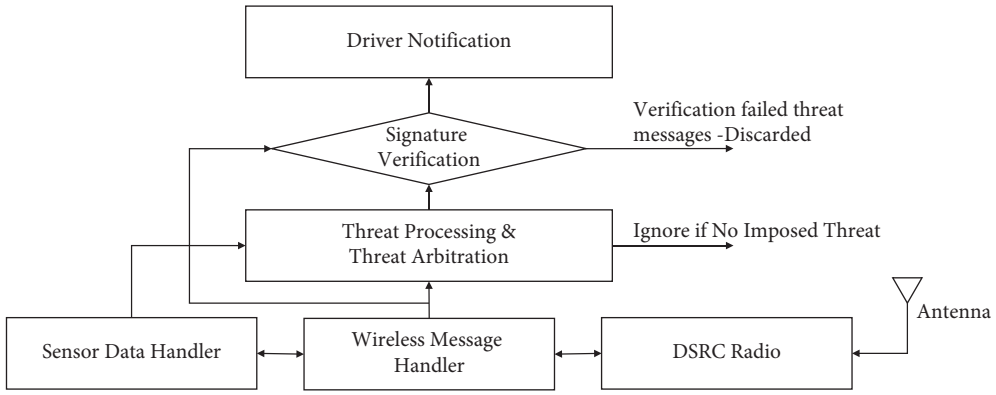

Figure 3: Verify-on-demand flow [22].

that is used to alert the driver. The next step is the location of the Remote Vehicle (RV). RV is the sender of BSMs. It is not a real sender (attacker). It is the sender written in BSMs generated by attacker. Eight spaces are defined based on the Host Vehicle (HV) to represent the location of the RV. HV is receiver of BSMs. As shown in Figure 5, it is possible to classify the location of the RV from which the message is sent, by separating it into eight zones, based on the direction in which the HV proceeds. The third factor is the direction of travel of the vehicle. The traveling direction of the vehicle can be divided into four types: the same direction as the HV, the opposite direction, the left direction at a right angle, and the right direction at a right angle. By combining these three criteria, the BSM transmitted for a unit of time is classified in real time. When AVoD module classifies BSMs, it checks to see if there are BSMs of the same type in threat table. If the same type of BSM exists in threat table, column of "number of packets" is increased by one and that BSM is ignored. On the contrary, if the same type of BSM does not exist in threat table, that BSM is delivered to the signature verification module.

4.4. Attacks on AVoD. This section describes how AVoD works using several situations. There is more than one vehicle that can be classified into the same category. In that case, the situation is divided into two. First situation is when the same type of BSM is received. Corresponding

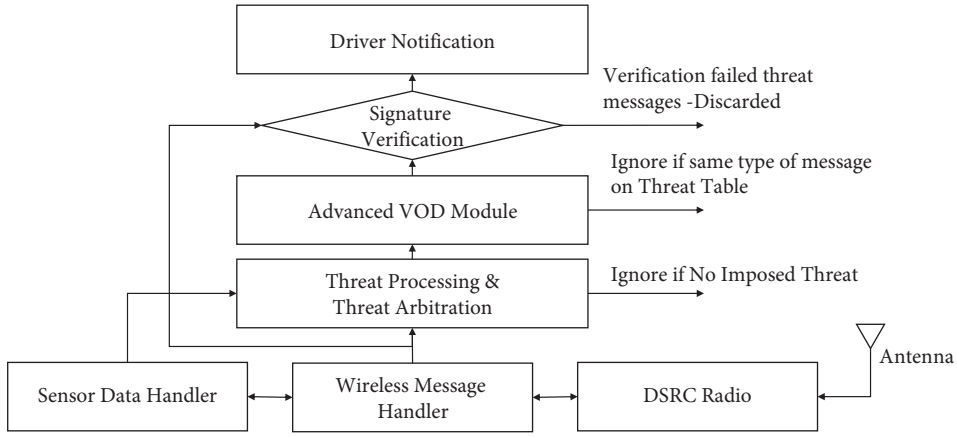

Figure 4: Advanced verify-on-demand flow.

Table 2: Threat table.

No	Safety application	Vehicle location	Vehicle direction	Number of packets
1	FCW	Center forward	Same	2
2	LTA	Left forward	Opposite	1
3	FCW	Left forward	Opposite	4
...	...	...	...	...

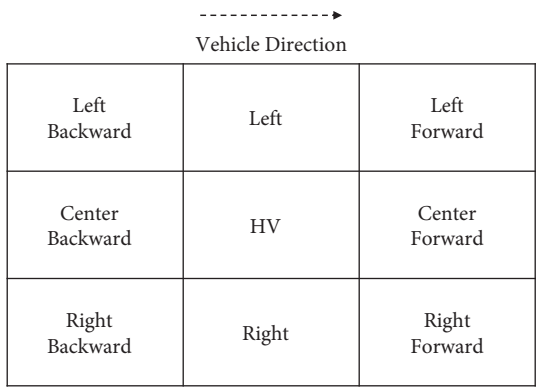

Figure 5: Vehicle location.

alert is already occurring, so signature verification is not performed. And this BSM is ignored. Second is when the different type of BSM is received. AVoD module adds it to threat table and passes it to the signature verification module.

It is assumed that the attacker transmits fake messages using fake certificates after getting verified by the RV. The AVoD module analyzes the BSMs regardless of the certificate. Even if it is a fake certificate, check whether the BSM is on the threat table. Theoretically, the thread table can store 160 rows (5 safety applications, 8 vehicle locations, and 4 vehicle directions). Eventually, OBU only needs to perform 160 signature verifications during the unit time, even if it receives BSMs more than 5500 per second. For this reason, AVoD only focuses on BSMs.

5. Experiment

The AVoD proposed in this paper is a proposed technique to prevent DoS attacks. In this section, an experiment is conducted to measure AVoD performance.

5.1. Experiment Overview. The experiment is conducted by measuring the time taken to process 10,000 BSMs per second on a personal computer (PC). 10 test message sets are used, in which the proportion of threat BSM among 10,000 messages increased by 10% from 10% to 100%. These message sets are named test case (TC) 1 to 10. Using the message sets from TC1 to TC10, the processing time in VATP, VoD, and AVoD is measured, and the average value is obtained by repeating this ten times in total. This is used to examine the results of a DoS attack with many threat BSMs. This is also a weakness of the existing VoD, and the effectiveness of the AVoD in the attack is examined.

PC specifications of experimental environment are shown in Table 3.

The BOGOMIPS measurement method used in this experiment is a certain program that consists of sleep function, time calculation function, and loop. It is similar implementation of BogoMips program in Linux kernel. It is used to compare the performance difference with the PC, by measuring BOGOMIPS through the execution of the same code in the OBU.

5.2. Result of the Experiment. Figure 6 shows the experimental results. Experimental results from TC1 through TC10 show that VATP takes approximately 660 ms, all of

Table 3: PC specification of experimental environment.

Specification	
OS	Linux Kernel version 4.15.0, Ubuntu 18.04.5 LTS
CPU	Intel i7-8550U @ 1.80 GHz
RAM	32 GB
BOGOMIPS	1465.83

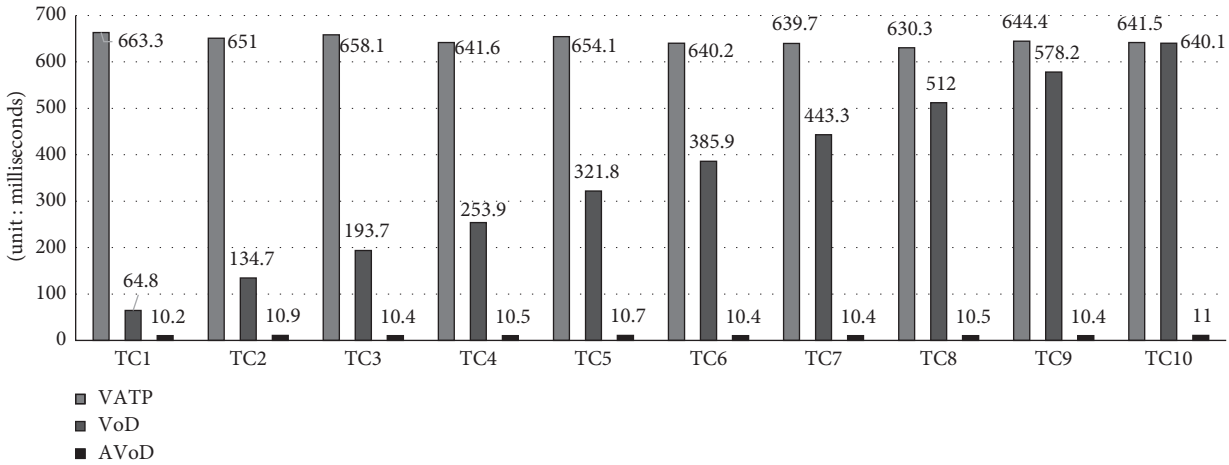

Figure 6: Result of experiment on PC.

Table 4: OBU specification of experimental environment.

Specification	
OS	Linux Kernel version 3.10.17, Ubuntu 14.04 LTS
CPU	NXP i.MX 6DualLite,800 MHz
RAM	1 GB SDRAM
BOGOMIPS	196.66 (7.45 times slow than PC)

which are similar. In the case of VoD, the execution time linearly increases as the ratio of messages containing risk increases. Finally, in the case of AVoD, it is observed that minimal execution time of 10 to 11 milliseconds is required because all attack messages are classified into several types. Compared to VoD, AVoD is processed approximately 6.35 times faster for TC1. In the case of TC10, the processing speed is up to 58 times faster. Based on this, it is established that the performance of AVoD is excellent, when the ratio of messages containing collisions, also mentioned as a weakness of the existing VoD, increased. In addition, the throughput rates in real OBUs are approximated for comparison, using BOGOMIPS figures measured in OBUs.

OBU specifications of experimental environment are shown in Table 4.

OBU's BOGOMIPS is 7.45 times slower than that of PCs, so the outcomes reflecting the corresponding values in the experimental results are shown in Figure 7. The TC2 results show that VoD takes more than one second to perform authentication. As there are 2000 threat BSMs in TC2, it is determined that the OBU can process approximately 2000 threat BSMs per second. Therefore, a DoS attack occurs even when using VoD in case the OBU receives more than 2000 threat BSMs. In the case of AVoD, TC10 takes approximately 82 milliseconds, which can be used to prevent DoS attacks by performing authentication in a short period of time, even if OBU receives more than 10,000 threat BSMs per second.

5.3. Comparing with Related Works. In this section, we compare with studies to speed up ECDSA verification discussed in Section 2. A study [20] that improved the ECDSA verification speed using GPGPU was conducted using ODROID-XU4. ODROID-XU4 have Cortex-A15 Quad Core 2.0 Ghz, Cortex-A7 Quad Core 1.4 GHz, and Mali-T628 MP6 (256core). In their study, the best performance using ODROID-XU4 was 15.4 signature verifications per second. Device with better hardware performance showed lower ECDSA verification performance than the proposed scheme. Lee et al. [21] use parallel

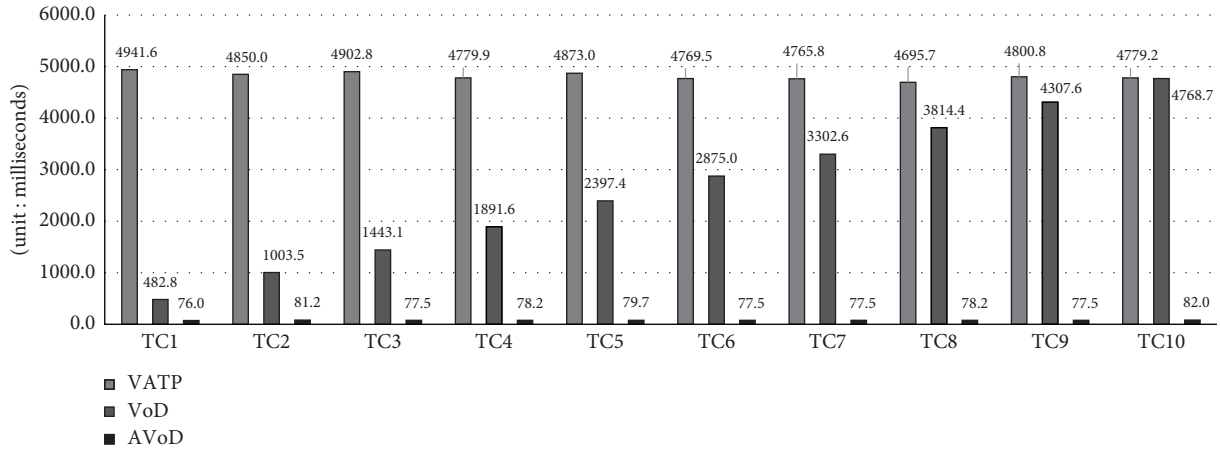

Figure 7: Result of experiment (2), approximated on OBU.

Table 5: Result of experiment, compared with S. Lee et al. [21].

Scheme	Number of threads	Verification time per one signature (unit: milliseconds)	Number of verifications per second	Time it takes to process 10,000 signatures (unit: milliseconds)
Lee et al. [21]	1	1.616	619.70	16160
	2	0.810	1233.53	8100
	4	0.417	2395.69	4170
	8	0.413	2417.32	4130
	16	0.409	2439.69	4090
Proposed scheme	1	—	—	82

programming to speed up signature verification. Those authors experimented using NXP i.MX 6 same as CPU used in this paper. Using the time to perform 10,000 ECDSA signature verifications, the verification time per unit and the number of verifications per second were calculated. Table 5 shows the experimental results. Compared indirectly to other schemes, the proposed scheme is more effective on verification BSMs.

6. Conclusion and Future Works

In this study, a technique to prevent DoS attacks in autonomous cooperative driving using SCMSs is proposed. The proposed method classifies threat messages to authenticate only the first messages received within the same group. Compared to VoD, which is a technique for preventing DoS attacks, this method has demonstrated the ability to process messages at a speed of 6.3 times to 58 times faster, depending on the situation. This proves to be a technique that effectively prevents DoS attacks that transmit a large number of messages. However, in the experiment, it is difficult to announce that an accurate result was obtained owing to the performance difference in the processing speed between the PC and the OBU when performing it on the PC rather than in the actual OBU. In future research, the challenge is to experiment with the actual OBU and determine its efficiency.

Data Availability

The cryptographic library used in the experiment for measuring the performance was OpenSSL version 3.0.0, and the curve used for ECDSA is secp256r1. As mentioned in the previous section, the experimental computer has a 1.80 GHz Quad Core CPU and a 32 GB RAM.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this study.

Acknowledgments

This research was supported by the Korea Ministry of Land, Infrastructure and Transport. It was also supported by the Korea Agency for Infrastructure Technology Advancement (Project no. 21PQOW-B152473-03).

Supplementary Materials

The supplementary material contains BOGOMIPS measurement source code. This code is used in the Result of the Experiment section. It is used to compare the performance difference with the PC, by measuring BOGOMIPS through

the execution of the same code in the OBU. (*Supplementary Materials*)

References

[1] European Automobile Manufacturers Association, "The automobile industry pocket guide 2020–2021," 2020, https://www.acea.be/uploads/publications/ACEA_Pocket_Guide_2020-2021.pdf.

[2] European Automobile Manufacturers Association, "The automobile industry pocket guide 2019–2020," 2019, https://www.acea.be/uploads/publications/ACEA_Pocket_Guide_2019-2020.pdf.

[3] C.-Y. Chan, "Advancements, prospects, and impacts of automated driving systems," *International Journal of Transportation Science and Technology*, vol. 6, no. 3, pp. 208–216, 2017.

[4] S. Singh, "Critical reasons for crashes investigated in the national motor Vehicle crash causation survey," *Traffic Safety Facts Crash Stats*, vol. 812 115, 2015.

[5] "Hackers remotely kill a jeep on the Highway - with me in it," 2015, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[6] C. Miller and C. Valasek, *Remote Exploitation of an Unaltered Passenger Vehicle*, Black Hat, USA, 2015.

[7] B. Brecht, D. Therriault, A. Weimerskirch et al., "A security credential management system for V2X communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 3850–3871, 2018.

[8] Society of Automotive Engineers International, *Dedicated Short Range Communications (DSRC) Message Set Dictionary: J2735*, SAE International, Warrendale, PA, US, 2018.

[9] Society of Automotive Engineers International, *On-Board System Requirements for V2V Safety Communications: J2945/1*, SAE International, Warrendale, PA, US, 2016.

[10] IEEE, *Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages*, IEEE, Piscataway, NJ, USA, 2016.

[11] N. Trkulja, D. Starobinski, and R. A. Berry, "Denial-of-Service attacks on C-V2X networks," 2020, http://arXiv:2010.13725.

[12] A. Benslimane and H. Nguyen-Minh, "Jamming attack model and detection method for beacons under multichannel operation in Vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 7, pp. 6475–6488, 2016.

[13] H. Vasudev, V. Deshpande, D. Das, and S. K. Das, "A lightweight mutual authentication protocol for V2V communication in Internet of Vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6709–6717, 2020.

[14] S. A. A. Hakeem, M. A. A. El-Gawad, and H. Kim, "Comparative experiments of V2X security protocol based on hash chain cryptography," *Sensors*, vol. 20, no. 19, 2020.

[15] S. Taha and X. S. Shen, "Lightweight group Authentication with dynamic Vehicle-clustering for 5G-based V2X communications," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, Abu Dhabi, UAE, December 2018.

[16] H. Mun, K. Han, Y. S. Lee, C. Y. Yeun, and H. H. Choi, "Enhanced secure anonymous authentication scheme for roaming service in global mobility networks," *Mathematical and Computer Modelling*, vol. 55, no. 1–2, pp. 214–222, 2012.

[17] C. C. Wu, W. B. Lee, and W. J. Tsaur, "A secure authentication scheme with anonymity for wireless communications," *IEEE Communications Letters*, vol. 12, no. 10, pp. 722-723, 2008.

[18] D. Zhao, H. Peng, L. Li, and Y. Yang, "A secure and effective anonymous authentication scheme for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 78, no. 1, pp. 247–269, 2014.

[19] M. Prerna, A. Ruhul, and G. P. Biswas, "Design of authentication protocol for wireless sensor network-based smart vehicular system," *Vehicular Communications*, vol. 9, pp. 64–71, 2017.

[20] S. Lee, H. Seo, B. Chunng, J. Choi, H. Kwon, and H. Yoon, "OpenCL based implementation of ECDSA signature Verification for V2X communication," in *Proceedings of the International Conference on Multimedia and Ubiquitous Engineering*, pp. 711–716, Salerno, Italy, November 2018.

[21] S. Lee, H. Seo, B. Chunng, and H. Kwon, "Study on parallel processing of ECDSA Verification for V2X communication," in *Proceedings of the Korea Information Processing Society Conference*, pp. 216-217, Busan, Republic of Korea, 2018.

[22] Society of Automotive Engineers International, *Verify on Demand*, 2017.

[23] National Highway Traffic Safety Administration, *Notice of Proposed Rulemaking: Federal Motor Vehicle Safety Standards*, V2V Communications, National Highway Traffic Safety Administration(NHTSA), Washington, DC, USA, 2017.

[24] T. Oder, T. Pöppelmann, and T. Güneysu, "Beyond ECDSA and RSA: lattice-based digital signatures on constrained devices," in *Proceedings of the 2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 1–6, San Francisco, CA, USA, June 2014.

[25] S. A. Manuel, F. L. Paula, and M. F. C. Tiago, "A practical evaluation on RSA and ECC-based cipher suites for IoT high-security energy-efficient fog and mist computing devices," *Sensors*, vol. 18, no. 11, 2018.

[26] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: an efficient RSU-aided message authentication scheme in Vehicular communication networks," in *Proceedings of the 2008 IEEE International Conference on Communications*, pp. 1451–1457, Beijing, China, May 2008.

[27] S. Jha, C. Yavvari, and D. Wijesekera, "Pseudonym certificate Validations under heavy Vehicular traffic loads," in *Proceedings of the IEEE Vehicular Networking Conference*, pp. 1–7, Taipei, Taiwan, December 2018.