Fatal C-V2X Denial-of-Service Attack Degrading Quality of Service in a Highway Scenario

Kyungtae Kim, Dongyoon Kwon, Woo-Cheol Jin, Sinuk Choi, Jinmo Kim, and Ji-Woong Choi

***Abstract*—A denial-of-service (DoS) attack, which prevents other nodes from accessing resources, is one of the fatal security threats in the V2X field. This paper analyzes the DoS attack on C-V2X networks from various viewpoints. First, we derive the conditions for the vulnerable vehicle that are expected to suffer fatal damage when subjected to the DoS attack. Then, we provide a method for the attacker to identify the vulnerable vehicle satisfying the derived conditions. We also verify that the attacker can more easily identify the vulnerable vehicle on a highway where the traffic density is generally constant. We confirm that the DoS attack that attacks the vulnerable vehicle satisfying the derived conditions causes more damage than the conventional DoS attack provided in another study in terms of reliability, coverage, and timeliness (up to 2% reduction in packet delivery ratio, up to 30 m reduction in communication coverage, and 0.15-second increase in the lower 1% update delay). In addition, we compare the ratio of packet errors by MAC of C-V2X to those caused by the DoS attack and verify the lethality of an attack depending on the traffic density. This paper provides insight into DoS attacks on C-V2X network, and future studies will cover the topic of attack detection and defense.**

***Index Terms*—Cellular vehicle-to-everything, cooperative awareness, denial-of-service, safety-related messages, vehicle-to-everything security.**

I. INTRODUCTION

AN autonomous vehicle, replacing human drivers with automation systems, has been in the spotlight recently. Generally, the autonomous vehicle operates in three process: 1) Recognition, 2) decision, and 3) control. In the recognition process, the autonomous vehicle utilizes various sensors (e.g., LiDAR, radar, and camera), which act as the driver's eyes, to identify other vehicles and objects [1]. However, autonomous vehicles with sensors have great difficulties recognizing objects in non-line-of-sight (NLOS) environments or adverse weather conditions [2]. For this reason, unfortunately, many collision accidents caused by the failure to recognize objects during autonomous driving have been reported [3]. For more reliable autonomous driving, overcoming the sensor drawbacks and perfectly recognizing objects surrounding the vehicle is essential.

How can the recognition be improved while driving autonomously? Vehicle-to-everything (V2X) communication, enabling data exchange between a vehicle and other objects, can be a solution [4]. V2X standard defines a basic-safety message (BSM), the most general V2X message transmitted every 100 ms. BSM contains various information about the transmitting vehicle, such as the vehicle's latitude, longitude, height, driving direction, and so on [5]. The receiving vehicles can update information about other vehicles in real-time, and the recognition process can be improved by complementing other sensors.

Meanwhile, technologies that can be applied to V2X are divided into two types: Dedicated short range communication (DSRC) based on Wi-Fi and cellular-V2X (C-V2X) based on cellular technology [6]. The two technologies have competed over the V2X standard, but C-V2X, led by Qualcomm, is recently attracting more attention [7]. As of 2023, C-V2X is divided into LTE-V2X (release 14/15) and NR-V2X (release 16/17). C-V2X consists of network communication through the base station (uplink and downlink) and direct communication connecting each vehicle without the base station (sidelink). For the C-V2X sidelink, 3GPP defines two operation modes. The two modes send messages through the sidelink PC5 interface, but there is a difference in the resource allocation technique. In mode3 (LTE-V2X) or mode1 (NR-V2X), the resource is allocated by the base station, while in mode4 (LTE-V2X) or mode2 (NR-V2X), the vehicle autonomously determines the resource [8]. According to the studies of LTE-V2X, mode3 provides better quality-of-service (QoS) than mode4 owing to the base station's broad coverage [9]. However, there is less room for research about mode3 since the base station management generally depends on the operator. Therefore, recent studies about C-V2X mainly deal with mode4. In this paper, LTE-V2X sidelink mode4 is abbreviated as C-V2X.

As mentioned, since the V2X is a key technology related to safety, concerns about security threats are also increasing at the same time as it is in the limelight. If a critical problem occurs in V2X security, it is evident that it will cause fatal confusion in the traffic. For example, one malicious vehicle pretends to be multiple vehicles by transmitting numerous messages. In this case, the receiving vehicle may mistakenly believe that there are more vehicles on the road than driving vehicles,

Manuscript received December 29, 2022; revised June 3, 2023; approved for publication by Molisch, Andy Division 2 Editor, November 30, 2023.

This work was supported in part by the National Research Foundation of Korea (NRF) grant funded by the Ministry of Science and Information and Communications Technology (MSIT) of the Korean government (No. NRF-2021R1A2C2008415), and in part by the Institute of Information and Communications Technology Planning and Evaluation (IITP) funded by the msIT of the Korean Government (No. 2022-0-01053).

K. Kim is with LG Innotek, Seoul, Republic of Korea, email: kyungtae.kim@lginnotek.com.

D. Kwon is with Toris, Daegu, Republic of Korea, email: dykwon@toriskorea.com.

W.-C. Jin, S. Choi, J. Kim, and J.-W. Choi are with Electrical Engineering and Computer Science, DGIST, Daegu, Republic of Korea, email: {wlsdncjf93, lmy0829, jmkim, jwchoi}@dgist.ac.kr.

J.-W. Choi is a corresponding author.

Digital Object Identifier: 10.23919/JCN.2023.000066

1229-2370/23/$10.00 © 2023 KICS

which may cause malfunctions such as sudden stops. Another example is that a malicious vehicle intentionally prevents a target vehicle from transmitting messages. In this case, the attacked vehicle is completely deleted from the other vehicle's recognition via V2X; therefore, this attack may confuse the road.

For this reason, several studies have addressed security threats on V2X networks, such as DoS, malware, illusion, jamming, and so on [10]. Among these threats, the DoS attack has the following fatalities: 1) $Malicious$: It is performed with a malicious objective; 2) $Disruptive$: It disrupts the network capabilities; 3) $Remote$: It is performed using the remote network [11]. Because of these fatalities, the risk of the DoS attack on V2X networks has been constantly raised [12]. However, the majority of early DoS attack studies analyzed DSRC, which is a relatively old technology. [13] evaluates the DSRC performance in the presence of the DoS attack. [14] analyzes the jamming attack, including DoS, in terms of DSRC's reliability for safety applications. [15] proposes real-time detection for the DoS attack in DSRC networks.

On the other hand, several DoS studies on cellular technology are only limited to uplink and downlink, which is a commercial network [16]. Studies related to the DoS attack on sidelink are relatively scarce. This is because the C-V2X is a relatively new technology defined in 2017. In sidelink, the DoS attack is expected to be more lethal since the eNodeB for resource control is not deployed; therefore, research on sidelink DoS attack is required. For the first time, the author of [17] introduces the DoS attack on the C-V2X network and quantifies its damage. [17] provides superior insight into the DoS attack; however, there are some interesting unsolved questions. How is the damage of the DoS attack determined? How will the packet errors affect drivers (or autonomous vehicles) while driving? What is the relationship between packet errors caused by the characteristics of C-V2X and packet errors caused by the DoS attack? To solve the above questions, this paper aims to analyze the DoS attack on the C-V2X network from a more diverse perspective based on [17]. The specific contributions are as follows:

- We derive the conditions of the vulnerable vehicle to the DoS attack.
- We propose the DoS attack satisfying one of the derived conditions in a highway environment.
- We analyze the ratio of packet errors caused by the C-V2X characteristic to those caused by the DoS attack.
- We evaluate the damage due to the DoS attack on the C-V2X network from various viewpoints: Reliability, coverage, and timeliness, which are related to the recognition process of autonomous driving.

We organize this paper as follows. Section II provides the background for understanding this paper. Section III derives conditions for the most vulnerable vehicle to the DoS attack. Additionally, we propose the DoS attack satisfying the derived conditions. Section IV evaluates its damage regarding reliability, coverage, and timeliness through the system-based network simulation. Section V concludes the paper.

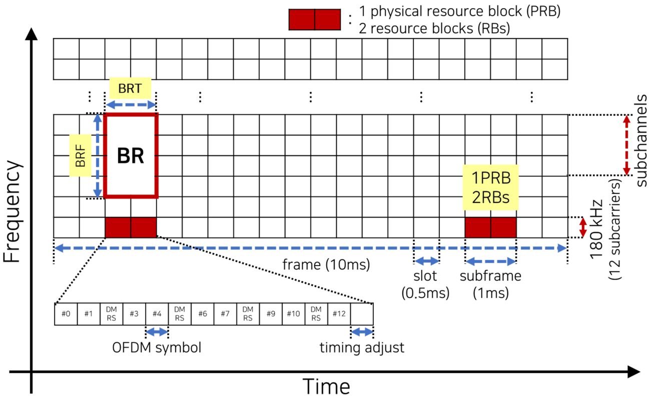

Fig. 1. C-V2X time-frequency resource grid.

II. Background

A. Overview of the C-V2X Sidelink

1) C-V2X waveform: C-V2X inherits the uplink of the legacy LTE; thus, it utilizes single-carrier frequency division multiple access (SC-FDMA) in the PHY and MAC layers. Therefore, C-V2X utilizes the time and frequency domains for multiplexing, as shown in Fig. 1. The time domain is divided into a frame of 10 ms, a subframe of 1 ms, and a slot of 0.5 ms. The time domain reference for resource allocation is a 1 ms subframe that contains 14 OFDM symbols. One subframe comprises 4 demodulation reference symbols (DMRS) and 9 data symbols for a payload transmission. The last symbol, which will not be transmitted, acts as a time guard allowing the transmitter to return to the receiver state before the next frame [18].

On the other hand, in the frequency domain, C-V2X supports a 10 MHz or 20 MHz bandwidth at the 5.9 GHz frequency band, an intelligent transportation system (ITS) frequency officially designated in most countries [19]. The C-V2X channel bandwidth is divided into units of 180 kHz, which is a set of 12 orthogonal subcarriers with a 15 kHz bandwidth. A 0.5 ms slot with a bandwidth of 180 kHz is called a resource block (RB), and an RB pair is called a physical resource block (PRB). The RB pair or the PRB is the minimum unit for a resource allocation in C-V2X. A set of consecutive RB pairs at one subframe in the frequency domain is called a subchannel. The 3GPP specification of 36.213 determines the number of RBs that can constitute one subchannel as follows: 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 25, 30, 48, and 50 RBs [20]. The C-V2X node can utilize one or multiple subchannels to transmit packets. The number of required subchannels and RBs is determined by the modulation and coding scheme (MCS) and packet payload.

By referring to [21], this paper analyzes the time-frequency resource grid of Fig. 1 into beacon units, where a beacon denotes a periodic BSM transmitted at a frequency of 10 Hz. When it is assumed that all vehicles transmit the BSM beacon of the same payload at the same frequency, it is

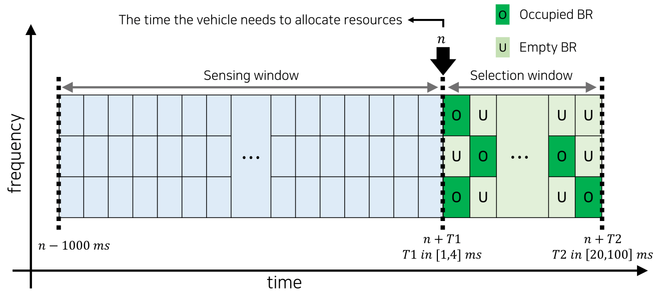

Fig. 2. SB-SPS by C-V2X mode4.

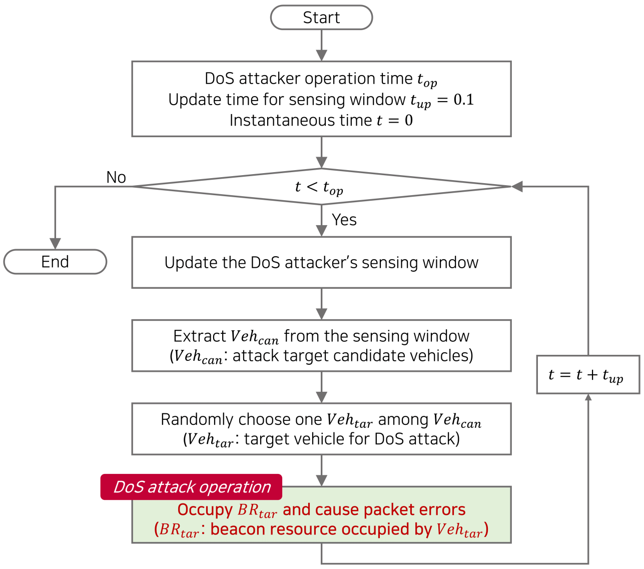
Start
DoS attacker operation time t_{op}
Update time for sensing window $t_{up}=0.1$
Instantaneous time $t=0$
$t<t_{op}$
No
Yes
End
Update the DoS attacker's sensing window
Extract Veh_{can} from the sensing window
(Veh_{can}: attack target candidate vehicles)
Randomly choose one Veh_{tar} among Veh_{can}
(Veh_{tar}: target vehicle for DoS attack)
DoS attack operation
Occupy BR_{tar} and cause packet errors
(BR_{tar}: beacon resource occupied by Veh_{tar})
$t=t+t_{up}$

Fig. 3. DoS attack on C-V2X network ('$Smart\ attack$' introduced in [17]).

possible to derive the number of resources the vehicles can occupy in one period. As shown in Fig. 1, the subchannel required to transmit one BSM beacon is named the beacon resource (BR), and the BR-time (BRT) and BR-frequency (BRF) are introduced to analyze the BR in the time-frequency resource grid. The number of BRs, denoted N_{BR}, is given by N_{BR} = BRT × BRF.

2) C-V2X mode4 resource allocation: In C-V2X mode4, vehicles use a sensing-based semi-persistent scheduling (SB-SPS) scheme to autonomously occupy the BR while avoiding the BRs occupied by other vehicles. The SB-SPS operates as a listen-before-talk process, estimating the resource occupied through continuous resource sensing (listen), avoiding it, and using the resource (talk). As shown in Fig. 2, based on the time n that the vehicle requires a resource allocation, the time domain is divided into the sensing window of $[n-1000$ ms, $n]$ and the selection window of $[n+T1, n+T2]$, where $T1$ is in [1, 4] ms, and $T2$ is in [20, 100] ms. Each vehicle performs four steps for occupying the BR and transmitting the BSM beacon as follows:

- $Step1 : Channel\ sensing\ (listen)$

The vehicle continuously measures the sidelink received signal strength indication (S-RSSI) on every BR during 1000 subframes (1 second) to distinguish the BRs estimated as being used by other vehicles.

- $Step2 : Extraction\ of\ candidate\ resources$

The vehicle extracts candidate BRs to occupy after excluding the BRs used by other vehicles. The $Step2$ extraction considers two factors based on the received BSM beacons: 1) The measured S-RSSI of the BR and 2) the resource reservation information in a sidelink control information (SCI) included in BSM. If the number of candidate BRs is less than 20% of the N_{BR} (the total available BRs), increase the S-RSSI threshold by 3 dB and perform $Step2$ iteratively. This process is carried out until the candidate BR is at least 20% of the total available BRs.

- $Step3 : Resource\ selection\ and\ beacon\ transmission\ (talk)$

The vehicle extracts the BRs having the lowest average S-RSSI measured in the sensing window among the candidate BRs filtered by $Step2$. The number of BRs to be extracted, called the best BRs, is 20% of the total number of BRs. Then, the vehicle randomly chooses one BR among the best BRs. Randomly choosing a BR prevents many vehicles from selecting a BR with the lowest S-RSSI simultaneously [18]. A reselection counter, uniformly randomly determined between 5 and 15 (at beacon frequency 10 Hz), is also assigned. This counter is the number of times the allocated BR can be consecutively used, which is decremented by 1 for each beacon transmission. The vehicle uses the selected BR as much as the reselection counter value. This resource scheduling scheme is named 'semi-persistent scheduling'.

- $Step4 : Resource\ reselection$

When the reselection counter reaches zero, the vehicle decides whether to reuse the BR with probability p or select a new BR with probability $1-p$. The probability p can be set from 0 to 0.8, and the 3GPP specification does not define a specific value. When the vehicle reuses the BR, a new reselection counter is assigned, and $Step3$ is performed. If not, the vehicle performs $Step1$ again.

B. Denial-of-Service Attack on C-V2X Network

The DoS attack on C-V2X network introduced in [17] is briefly provided in this subsection. As described in Section II-B, the vehicle using C-V2X mode4 reduces the likelihood of packet collisions by avoiding the resources used by other vehicles through the SB-SPS process. Contrary to the above, the DoS attack increases the likelihood of packet collisions by intentionally occupying the resources being used by other vehicles. Fig. 3 shows the process of the DoS attack on C-V2X network in [17] ([17] expresses this attack process as a '$Smart\ attack$'). The DoS attacker is assumed to have the same communication capability as other C-V2X vehicles. This assumption makes it impossible for other ordinary vehicles to identify the DoS attacker. When the DoS attacker initiates an attack, the attacker identifies the resources being occupied through the sensing window. This is the same as $Step1$ of the SB-SPS introduced above. Vehicles using occupied resources become target candidates for the attack, denoted by Veh_{can}. Then, the DoS attacker randomly chooses one vehicle among Veh_{can} as a target vehicle Veh_{tar} and transmits a dummy message, which intentionally causes a packet collision. This packet collision reduces the signal-to-noise interference (SINR) of the vehicles that receive the packet sent from Veh_{tar}, resulting in packet errors. At the end of each attack, the DoS attacker decides whether to continue attacking the same vehicle or to change. Through this process, this DoS attack aims to reduce the packet delivery ratio (PDR), which is specified as the ratio of correctly received packets to the total number of transmitted packets, by causing many errors due to deliberate packet collisions.

Here, Fig. 4 shows an example to compare the typical SB-SPS scheme and the DoS attack on C-V2X network. Note the red vehicle, Veh_6, parked on the shoulder of the road. This vehicle is in a state where it has to determine which BR to use for transmitting packets. In the typical SB-SPS of C-V2X mode4, the vehicle excludes the BRs found to be occupied by other vehicles and chooses the one to occupy among the remaining BRs. This procedure reduces the packet collisions between vehicles as much as possible. In this example, Veh_6 occupies BR_2 and is not occupied by other vehicles, so there is no packet collision.

On the other hand, in the case of the DoS attack, Veh_6 operates differently when Veh_6 is set as a DoS attacker. The Veh_6 extracts the candidate vehicles Veh_{can} for the attack by detecting the occupied BRs (BR_1, BR_5, BR_7, BR_{10}, and BR_{17}) through its sensing window. In 'Smart attack' by [17], Veh_6 randomly chooses patrol car Veh_3, as the target vehicle Veh_{tar} among Veh_{can}. Therefore, the DoS attacker occupies BR_1 to transmit a dummy packet with non-useful information. This scheme lowers the SINR of the vehicles that receive the packets transmitted from Veh_3, causing numerous packet errors. Consequently, other vehicles cannot receive the critical messages sent from the patrol car due to the DoS attack.

The fatal problem with the DoS attack on C-V2X network is that the attacked vehicle does not identify that it is being attacked. This is because, unlike the legacy uplink and downlink LTE, the C-V2X mode4 does not have a feedback process for verifying whether the message is successfully transmitted and received. The other reason is that C-V2X only utilizes half-duplex communication; therefore, it cannot receive messages while transmitting. According to the literature, packet collisions in C-V2X occur when the density of the vehicles increases, even without malicious DoS attackers [22]. Therefore, it is challenging to determine whether a packet collision is a malicious DoS attack.

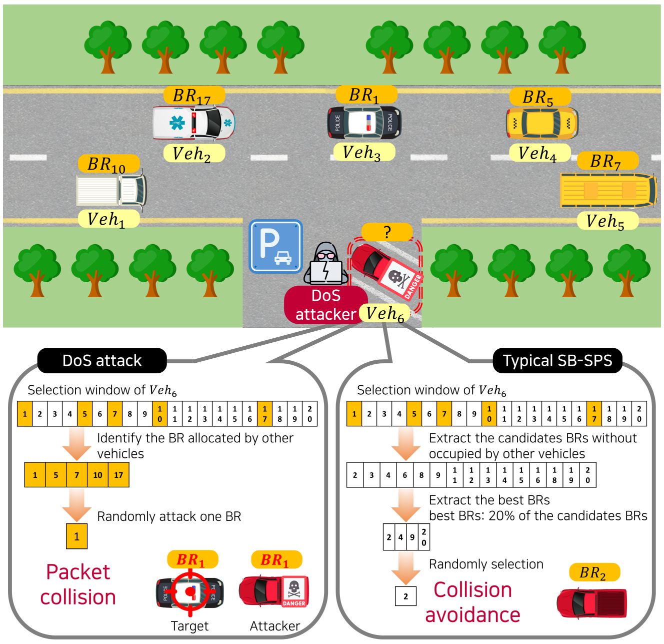

Fig. 4. Comparison between typical SB-SPS and DoS attack (Vector icons are designed by flaticon, URL: https://www.flaticon.com).

III. Fatal C-V2X DoS Attack in Highway Scenarios

A. Conditions of the Vulnerable Vehicle to the DoS Attack

To fatally attack the C-V2X network by causing numerous packet errors, the DoS attacker has to identify a vehicle vulnerable to an attack and select it as a target vehicle. As shown in Fig. 5, the two conditions for selecting the target vehicle are as follows:

- $Vehicle\ having\ many\ neighbors$ (Fig. 5(a))

The definition of a *neighbor* indicates a set of vehicles that can receive messages within a specific range from the vehicle that sends a beacon message. This specific range is called an awareness range, denoted by the r_{aw}, and the recipient within a r_{aw} is called a neighbor [21]. In other words, the neighbors in the awareness range of transmitting vehicles can receive the packet. r_{aw} is a design choice determined by a specific V2X application. For example, in the case of a periodic beacon message transmission, it is typically set r_{aw} as 2–300 m [23]. Therefore, a vehicle with many neighbors may incur considerable damage when subjected to the DoS attack. In conclusion, for the fatal DoS attack, the DoS attacker must identify how many neighbors N_{neigh} each candidate vehicle has, and then the target vehicle is chosen as a vehicle with many neighbors, as shown in Fig. 5(a).

- $Vehicle\ located\ close\ to\ the\ DoS\ attacker$ (Fig. 5(b))

Due to the characteristics of radio waves, the interference strength caused by the DoS attacker depends on the distance between the attacker and the target vehicle and the transmit power/antenna gain of the DoS attacker. Since the transmit power and antenna gain are fixed, the distance between the attacker and the target vehicle, denoted by d_{attack}, is the most crucial factor in determining the interference strength. As the distance d_{attack} increases, the interference experienced by the neighbors of the target vehicle relatively decreases. For this reason, packet errors may not occur even when subjected to the DoS attack due to the lower interference. On the other hand, as the distance d_{attack} gets closer, neighbors of the target vehicle

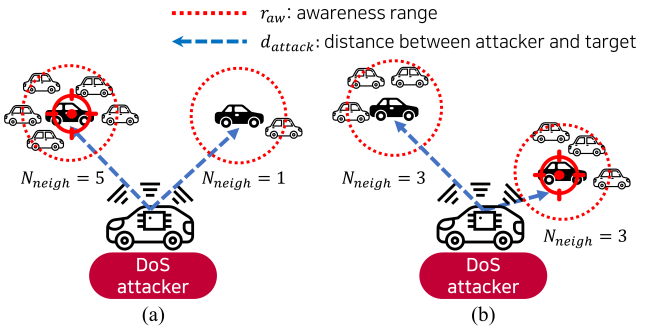

Fig. 5. Conditions for causing many packet errors: (a) Vehicle having many neighbors; (b) vehicle located close to the DoS attacker.

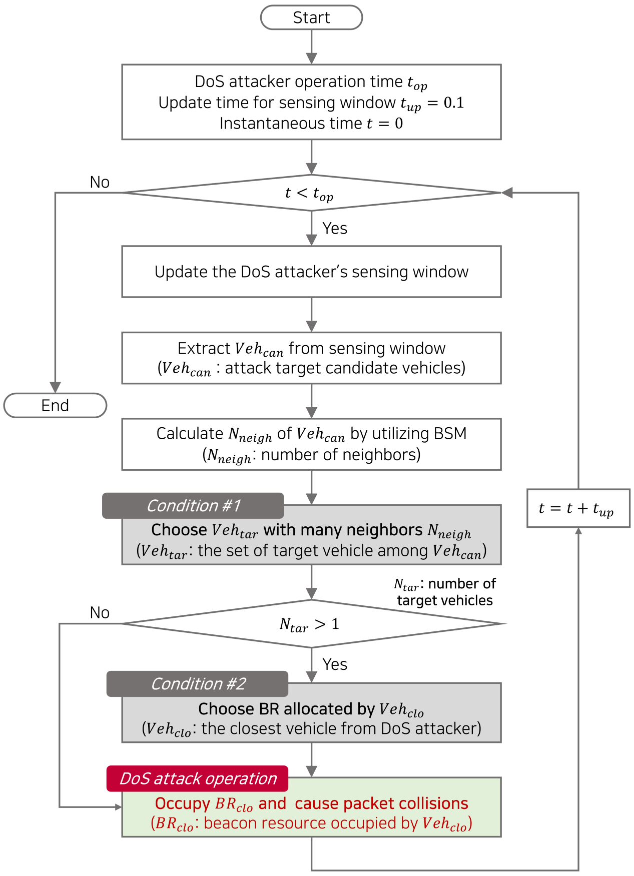
Start
DoS attacker operation time t_{op}
Update time for sensing window $t_{up} = 0.1$
Instantaneous time $t = 0$
No
$t < t_{op}$
Yes
Update the DoS attacker's sensing window
Extract Veh_{can} from sensing window
(Veh_{can} : attack target candidate vehicles)
End
Calculate N_{neigh} of Veh_{can} by utilizing BSM
(N_{neigh}: number of neighbors)
Condition #1
Choose Veh_{tar} with many neighbors N_{neigh}
(Veh_{tar}: the set of target vehicle among Veh_{can})
$t = t + t_{up}$
N_{tar}: number of target vehicles
No
$N_{tar} > 1$
Yes
Condition #2
Choose BR allocated by Veh_{clo}
(Veh_{clo}: the closest vehicle from DoS attacker)
DoS attack operation
Occupy BR_{clo} and cause packet collisions
(BR_{clo}: beacon resource occupied by Veh_{clo})

Fig. 6. Fatal DoS attack on C-V2X network.

experience considerable interference, causing numerous packet errors. Therefore, when the numerous target candidates for the DoS attack have the same number of neighbors N_{neigh} as shown in Fig. 5(b), choosing the vehicle close to the DoS attacker as the target vehicle can inflict significant damage on the C-V2X system by causing numerous packet errors.

In summary, a vehicle that has many neighbors and is close to the DoS attacker suffers the most damage when it is attacked. In this paper, we call the DoS attack satisfying the above two conditions is called as a fatal DoS attack. Fig. 6 shows a diagram of the fatal DoS attack scheme.

B. Proposal of the DoS Attack that Disrupts the Nearest Vehicle from the Attacker

However, satisfying the above two conditions for the DoS attacker is challenging. The main reason is that identifying the number of neighbors of each vehicle, which is the first condition, may involve error. For the DoS attacker, a beacon message, which includes the transmitting vehicle's velocity, direction, latitude, and longitude, can be utilized to identify the number of neighbors of each vehicle [5]. The DoS attacker would have to derive the number of neighbors of each vehicle based on the location information contained in the beacon message received. However, in this way, the number of neighbors identified by the attacker based on the beacon message may differ from the actual number of neighbors for each vehicle. This is because the DoS attacker cannot determine the vehicle's location if the neighboring vehicle of a specific vehicle is not included in the DoS attacker's awareness range. In addition, since the number of neighbors is a value that dynamically changes depending on the velocity and direction of the vehicle, a difference in value may occur between the time the DoS attacker calculates the information and the attacks. For example, suppose one target vehicle has ten neighboring vehicles traveling in the opposite direction compared to the target vehicle. In that case, the probability that ten vehicles are not neighbors of the target vehicle increases when the DoS attacker begins the attack. Another difficulty is that this scheme requires high computational power for the DoS attacker, which may violate the previous assumption that all the vehicles have the same C-V2X capability.

Meanwhile, in many V2X studies, a highway driving simulation is performed, assuming that the vehicle distribution follows a uniform or a Poisson point process (PPP) [24]. This assumption is reasonable, as it can adequately model a highway where all vehicles drive with a similar velocity. Suppose the DoS attack process introduced above is applied to the highway driving simulation modeled as uniform or PPP. In that case, the DoS attacker does not need to determine the number of neighbors, N_{neigh}, of the target candidate vehicles Veh_{can}, which is the first condition of Fig. 5(a). This is because all the vehicles driving on the highway have a similar number of neighbors due to the uniform or PPP modeling. Therefore, only the second condition of Fig. 5(b) needs to be satisfied to inflict the fatal DoS attack, and there is no need to consider the first condition of Fig. 5(a). In other words, the fatal DoS attack causing significant damage in a highway scenario attacks the closest vehicle Veh_{clo} from the DoS attacker among the candidate vehicles Veh_{can}. Fig. 7 shows the DoS attack process using the proposed scheme in a highway scenario, which is simplified compared to Fig. 6.

IV. Performance Evaluations

A. Simulation Settings

From now on, we evaluate the proposed C-V2X DoS attack through LTEV2Vsim, a system-level simulator using MATLAB [21], [23]. We compare the three schemes of the DoS attack and one scheme of the typical SB-SPS without

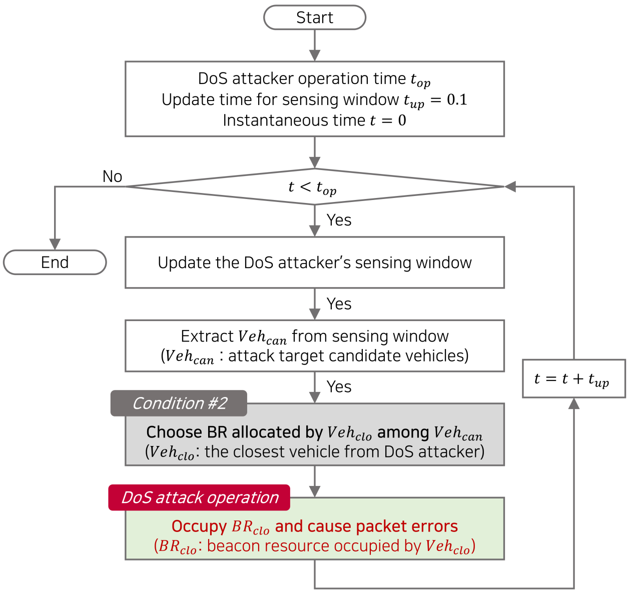
Start
DoS attacker operation time t_{op}
Update time for sensing window t_{up} = 0.1
Instantaneous time t = 0
No
$t < t_{op}$
Yes
End
Update the DoS attacker's sensing window
Yes
Extract Veh_{can} from sensing window
(Veh_{can} : attack target candidate vehicles)
Yes
$t = t + t_{up}$
Condition #2
Choose BR allocated by Veh_{clo} among Veh_{can}
(Veh_{clo}: the closest vehicle from DoS attacker)
DoS attack operation
Occupy BR_{clo} and cause packet errors
(BR_{clo}: beacon resource occupied by Veh_{clo})

Fig. 7. Proposed C-V2X DoS attack process.

the DoS attack in the highway scenario, as follows:

- **SB-SPS**: Typical SB-SPS without a DoS attack;
- **Smart**: Smart DoS attack in [17] (Fig. 3);
- **Fatal**: Fatal DoS attack satisfying the conditions of Fig. 5 (Fig. 6);
- **Proposal**: Proposed DoS attack occupying the BR used by the closest vehicle from the attacker (Fig. 7).

There are two types of parameters: Traffic flow and communication. The traffic flow parameters are as follows. We define a three-lane two-way 500 m highway. The vehicle density ρ, defined as the number of vehicles per kilometer, is set from 0.06 to 0.21 in steps of 0.03. This is equivalent to the number of vehicles N_{veh}, which is set at intervals of 15 from 30 to 105. Each vehicle traverses the highway at 100±30 km/h. The simulation time t_{op} is 600 seconds. The communication parameters are as follows. We set C-V2X to utilize the 10 MHz bandwidth at the ITS band of 5.9 GHz. The PHY layer parameters are set following the 3GPP TR 36.885 of [25]. WINNER+ (B1) of [26], widely used in V2X studies, is used as the path loss model. The transmitting (TX) and receiving (RX) antenna gains are 3 dB, and the TX power is 23 dB. The antenna height is 1.5 m, and the shadowing decorrelation distance is 25 m. The shadowing standard deviations are 3 dB in LoS and 4 dB in NLoS. The beacon is generated every 0.1 seconds at the application layer, and the payload is 300 bytes. The MCS is set to 7, and the awareness range, r_{aw}, is set to 250 m. The parameters are summarized in Table I.

As explained, the number of RBs for the beacon transmission depends on the preset MCS and the payload size. According to the 3GPP TR 36.213 of [20], the number of bits transmitted under the settings of a 300-byte payload and MCS 7 is 2,472 bits, and the number of required RBs is 40 (the number of PRBs is 20). Thus, the BRF, the number of beacon resources per subframe, is 2. Since the beacon period is 100 ms, the BRT is 100. Consequently, the number of BRs (N_{BR}) in one transmission period is 200. The N_{BR} of 200 indicates that 200 vehicles can transmit beacons in one period without the packet collisions in ideal.

TABLE I
SIMULATION PARAMETERS.

Parameter	Value
Road length	Highway - 500 m
The number of road lanes	Two-way 3 lanes
The number of vehicles N_V	30−−105
Vehicle speed	100 ± 30 km/h
Simulation time t_{op}	600 seconds
Beacon period and payload	100 ms and 300 bytes
Carrier frequency	5.9 GHz
Channel bandwidth	10 MHz
TX power and TX/RX antenna gain	23 dBm and 3 dB
Pathloss model	WINNER+ (B1)
Antenna height	1.5 m
Shadowing decorrelation distance	25 m
Shadowing standard deviation	3 dB (LoS) and 4 dB (NLoS)
Communication type	C-V2X sidelink mode4
Modulation and coding scheme	7
Awareness range r_{aw}	250 m

B. Key Performance Indicators

Whether the packet is successfully received is the most crucial factor in evaluating the QoS of the V2X system. It is determined by comparing the SINR measured at the RX vehicle with the minimum threshold γ_{min} of the packet. γ_{min} is dependent on the beacon size and the MCS, and the calculated γ_{min} with parameters in Table I is 7.3 dB [25]. According to [21], the SINR γ_{ij} at the RX vehicle j (Veh_j) from the TX vehicle i (Veh_i) is given by

$$\gamma_{ij} = \frac{P_R^{ij}}{P_N + P_I}. \tag{1}$$

P_R^{ij} is the received power at Veh_j transmitted from Veh_i and P_N is the noise power. P_I is an interference power caused by the other TX vehicles that transmit in the same frame with Veh_i. Two types of interference are caused by other TX vehicles transmitting packets at the same subframe, indirect and direct interference. Indirect interference is caused by an in-band emission (IBE), which indicates the power leakage of the other vehicles utilizing the different resources within the same subframe [27]. Meanwhile, direct interference is caused by the other vehicles occupying the same resource. The equation expressing both interferences is given by

$$P_I = \sum_{\substack{k \in \nu_{Su} \\ k \neq i,j}} K_{IBE}\left(\psi_k, \psi_j\right) P_R^{kj}. \tag{2}$$

ν_{Su} is a set of vehicles transmitting in the subframe S_u occupied by Veh_i. With the parameters of Table I, ν_{Su} has a maximum of two elements because the BRF is 2. K_{IBE} is the IBE coefficient given by [25]. ψ_k is the frequency portion used by Veh_k for transmission.

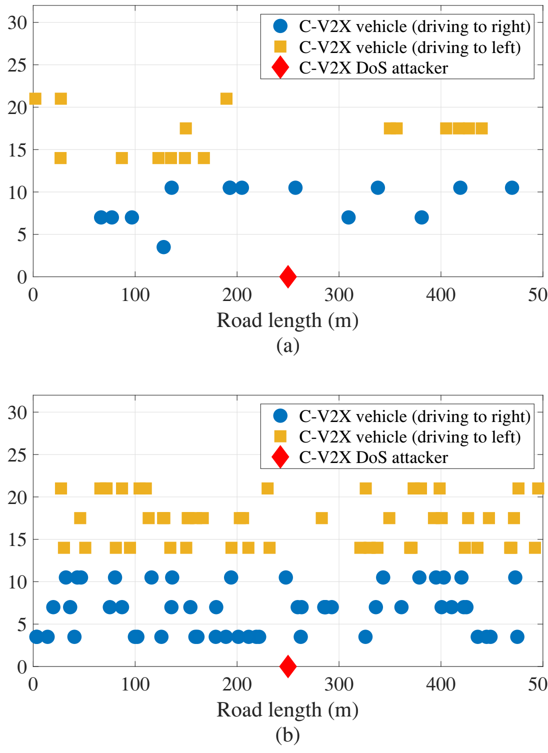

Fig. 8. Highway scenario model for C-V2X DoS attack evaluation: (a) $\rho = 0.06$ ($N_{veh} = 30$); (b) $\rho = 0.21$ ($N_{veh} = 105$).

According to [27], the SINR attenuation caused by direct interference is much more significant than indirect interference; therefore, the DoS attack is carried out through direct interference. In other words, the DoS attacker lowers the SINR below a threshold by increasing the direct interference experienced by the neighbors of the target vehicle, thereby attempting to prevent the neighbors from receiving the beacon transmitted from the target vehicle.

In our study, for a simple simulation, the bit error rate (BER)-SINR curve in the PHY layer provided in [28] is not considered, and the packet reception is determined only by comparing γ_{min} and the received SINR. We evaluate the fatality of each DoS attack on the C-V2X network in terms of reliability, coverage, and timeliness as follows:

- ***Reliability***: The average PDR is the ratio of correctly received beacons to the total transmitted beacons.
- ***Coverage***: The coverage, d_{cov}, is a communication range that satisfies PDR≥0.9, a requirement of the most common V2X application 'cooperative awareness' [29].
- ***Timeliness***: The 99th percentile of the update delay (UD) is the worst 1% of the UD values, where UD is the time difference between the beacons successfully received from the specific vehicle.

C. Simulation Results

Fig. 8 shows a highway scenario model for a C-V2X DoS attack evaluation: (a) $\rho = 0.06$ ($N_{veh} = 30$) and (b) $\rho = 0.21$ ($N_{veh} = 105$). The vehicles are arranged following the PPP. Reflecting Fig. 4, one DoS attacker, marked with a red diamond, is parked at the road-side and attacks the other vehicles. All the vehicles have the same C-V2X capabilities and parameters as listed in Table. I.

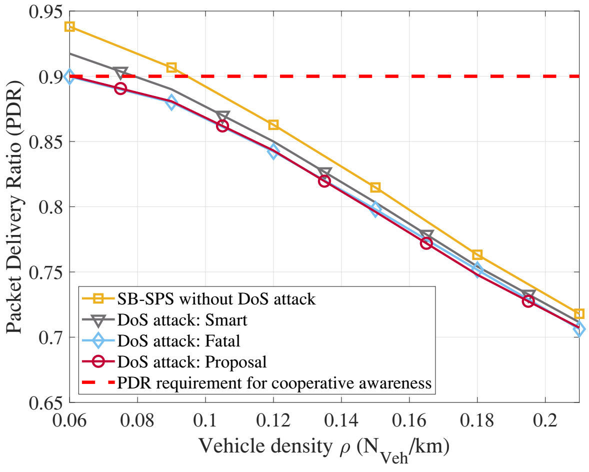

Fig. 9. Number of packet errors per each DoS attack when vehicle density ρ=0.2.

*1) **Reliability:*** Fig. 9 shows a PDR depending on the vehicle density ρ. The red dotted line shows a PDR requirement (0.9) for cooperative awareness, a primary V2X application. The line with a square marker indicates the result of the typical SB-SPS without the DoS attack, which is the baseline for comparison. Even if there is no DoS attack, the probability of a packet collision occupying the same resource increases as ρ increases; thereby, the PDR decreases. Other lines show the results of each DoS attack scheme as follows: The smart DoS attack (Fig. 3); the fatal DoS attack (Fig. 6); and the proposed DoS attack occupying the BR used by the closest vehicle (Fig. 7). Each result is denoted by the triangle, diamond, and circle markers, respectively. Among the DoS attacks, both the fatal and the proposed DoS attack further reduce the PDR compared to the smart DoS attack, causing the reliability of the C-V2X network to worsen. Specifically, when the vehicle density is 0.06, the smart DoS attack reduces the PDR by 2% compared to the PDR without the DoS attack, but both the fatal and the proposed attacks reduce it up to 4%.

In addition, Fig. 9 shows the capacity of the C-V2X network, which refers to the number of vehicles meeting the cooperative awareness requirement. Without the DoS attack, the typical SB-SPS can accommodate up to 48 vehicles. On the other hand, when the DoS attack is applied, the number of vehicles accommodated is decreased to 40 in the smart DoS attack and 30 in the other two DoS attacks. The results of both the fatal and proposed DoS attacks are almost identical. This indicates that simply attacking the closest vehicle from the attacker satisfies the requirements of the fatal DoS attack, as shown in Fig. 5. Consequently, it is confirmed that the proposed DoS attack causes significant damage to the C-V2X system in terms of reliability.

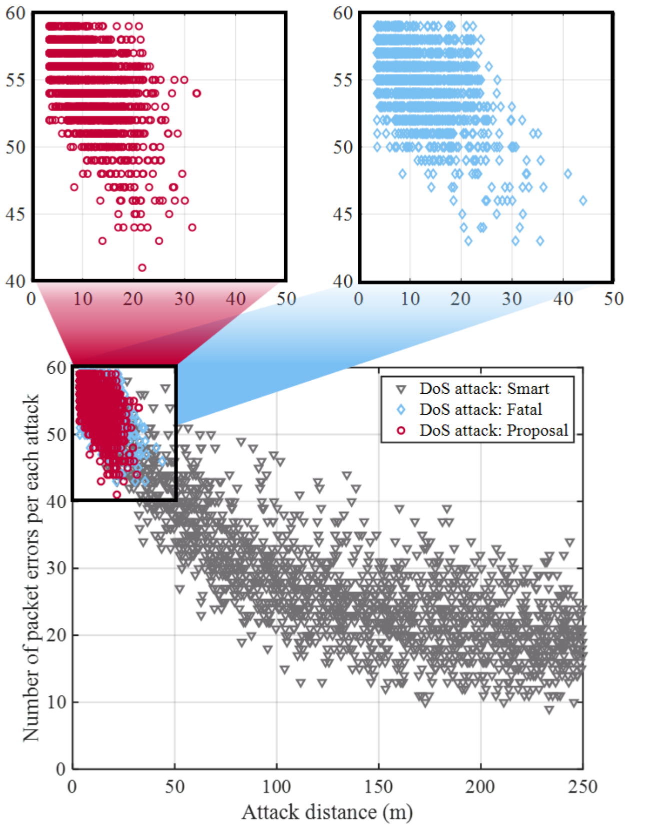

Fig. 10. Number of packet errors N_{err} at vehicle density ρ=0.12 per each DoS attack depending on attack distance d_{attack}.

Fig. 10 shows the number of packet errors N_{err} per DoS attack depending on the attack distance d_{attack}, from the DoS attacker and the target vehicle, when the vehicle density ρ is 0.12. This result shows that d_{attack} significantly impacts the reliability of the C-V2X network. As shown, N_{err} caused by the smart DoS attack is evenly distributed regardless of d_{attack}. However, the overall tendency shows that N_{err} is inversely proportional to d_{attack}. The results of other two DoS attacks are magnified at the top of Fig. 10. The fatal DoS attack causes more than 45 errors in most attacks, and the attack distance is less than 30 m. Meanwhile, the proposed DoS attack results are similar to those of the fatal DoS attack. Most attack distances are within 30 m and cause more than 45 packet errors. Based on the comparison, it can be seen that the proposed DoS attack has almost similar attack capability to the fatal DoS attack in a highway environment where vehicles travel relatively uniformly.

Fig. 11 shows the DoS attack results depending on the vehicle density ρ: (a) The average attack distance d_{attack} and (b) The average number of packet errors N_{err} per attack. As shown in Fig. 11(a), the average d_{attack} of the smart DoS attack is maintained near 125 m regardless of the vehicle density ρ. This value is half of the DoS attacker's awareness range of 250 m, and it can be seen from Fig. 10 that the d_{attack} is evenly distributed. On the other hand, the other two attacks have a similar average of d_{attack}, decreasing from 15 m to 8 m as ρ increases. The decreased d_{attack} is because the probability that the target will be close to the DoS attacker increases as the vehicle density increases.

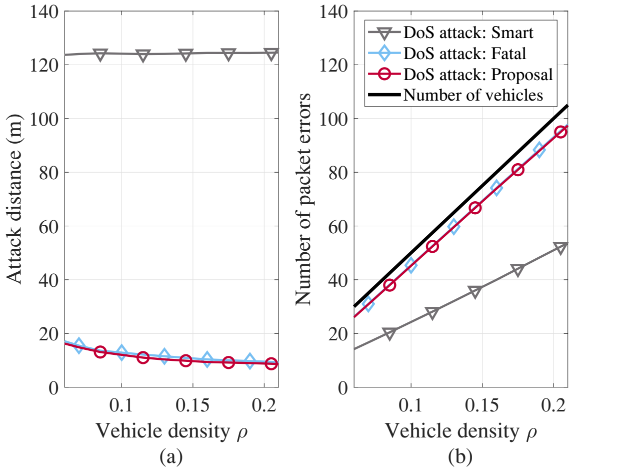

Fig. 11. The results depending on vehicle density ρ: (a) The average attack distance d_{attack}; (b) the average number of packet errors N_{err} per DoS attack.

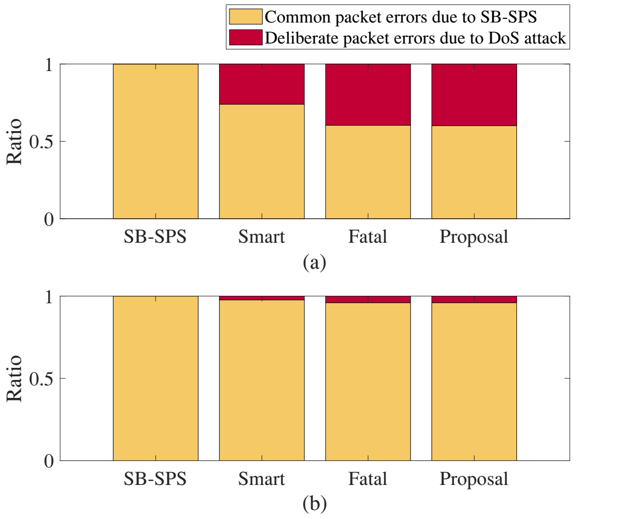

Fig. 12. A ratio between common errors due to SB-SPS and deliberate errors due to DoS attack: (a) ρ=0.06 and (b) ρ=0.21.

Fig. 11(b) represents the average number of packet errors N_{err} per attack depending on the vehicle density ρ. The black line with no marker indicates the number of vehicles N_{veh} driving on the highway. The smart DoS attack causes packet errors in vehicles that, on average, account for half of the total number of vehicles N_{veh}. In other words, since the vehicle density ρ is uniform across the highway, the attack distance d_{attack}, which is half of the awareness range r_{aw}, causes packet errors in half of the total vehicles. Meanwhile, the other two DoS attacks cause packet errors in approximately 90% of the vehicles on average. This result indicates that these attacks are much more fatal than the smart DoS attack in regard to communications reliability.

However, as shown in Fig. 9, the difference in PDR, according to the presence or absence of the DoS attack,

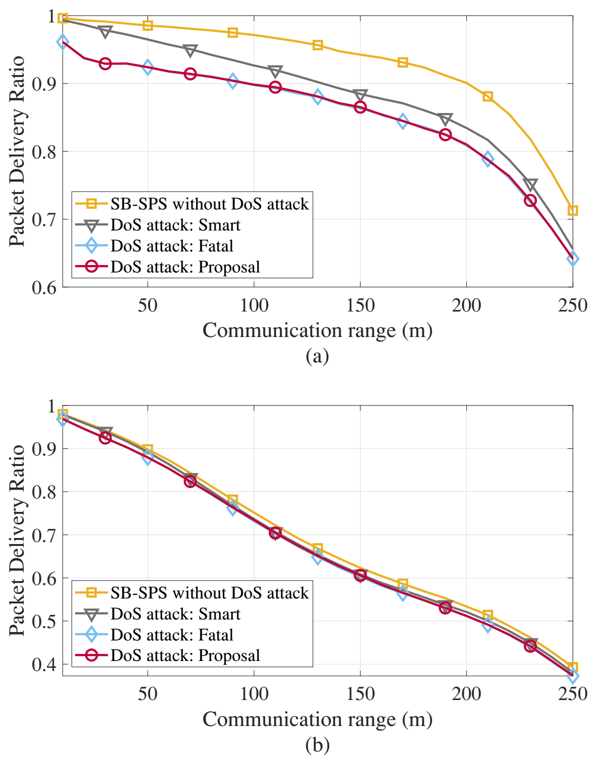

Fig. 13. Packet delivery ratio depending on communication distance: (a) ρ=0.06; (b) ρ=0.21.

gradually decreases as ρ increases. This is because the ratio of the packet errors caused by the DoS attack to the total packet errors is related to the vehicle density ρ. Fig. 12 shows the error ratio between the common errors due to SB-SPS and the deliberate errors due to the DoS attack: (a) ρ=0.06 and (b) ρ=0.21. It is confirmed that the error ratio caused by the DoS attack decreases as ρ increases. This graph indicates that the number of resource collisions that occur naturally increases as the vehicle becomes crowded so that resource collisions deliberately caused by the DoS attack are not significantly noticeable. Therefore, the damage caused by the DoS attack is more evident when the vehicle density is low.

*2) **Coverage:*** Fig. 13 shows the PDR depending on the vehicle's communication range: (a) ρ=0.06 and (b) ρ=0.21. The typical SB-SPS without the DoS attack achieves the highest PDR in both graphs. The difference in PDR, with or without DoS attack, reduces as ρ increases due to the gap in the error rate of Fig. 12. Both the fatal and proposed DoS attacks show similar results. These two attacks significantly exacerbate the PDR at the same distance compared to the smart DoS attack. Based on Fig. 13, the communication range that satisfies a specific PDR requirement can be obtained.

Fig. 14 shows a coverage, d_{cov}, that satisfies a PDR of 0.9 or higher, where d_{cov} is a communication range that can provide reliable packet transmissions for a cooperative awareness application. Specifically, when ρ is 0.06, both attacks reduce d_{cov} by 100 m (from 200 m to 100 m) compared to d_{cov} without the DoS attack, while the smart DoS attack reduces by only 70 m (from 200 m to 130 m). Similar to the previous results, the damage of d_{cov}, depending on whether the DoS attack is present, reduces as ρ increases. As ρ increases to 0.21, the difference in d_{cov} between the proposed DoS attack and the SB-SPS decreases by 8 m (from 49 m to 41 m). This is because the error rate induced by the DoS attack decreases as the vehicle density increases, as shown in Fig. 12.

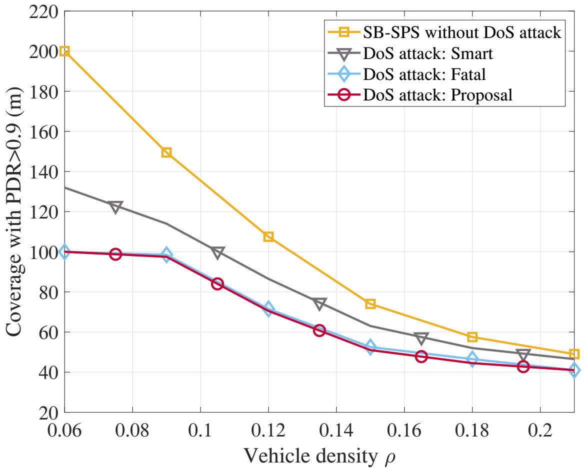

Fig. 14. Coverage that satisfies PDR 0.9 or higher.

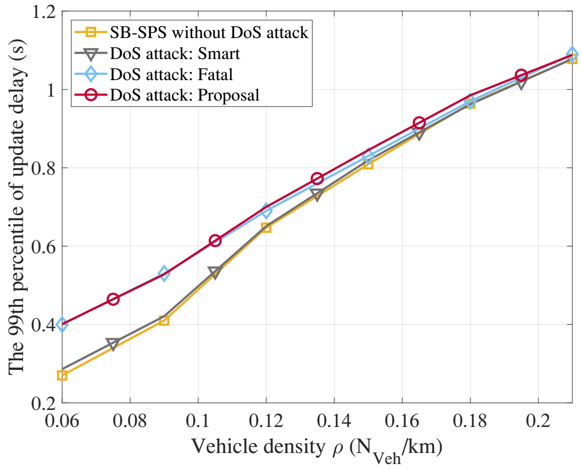

Fig. 15. The 99th percentile of update delay.

*3) **Timeliness:*** Fig. 15 shows the 99th percentile of the UD (the lower 1% of all the UDs). This value indicates the system's timeliness because it shows the worst-case delay. The shorter the UD is, the shorter the information on the nearby vehicles is updated in real-time. The result without the DoS attack linearly increases from 0.25 seconds to 1.1 seconds when ρ varies from 0.06 to 0.21. This indicates that the more crowded the vehicle is, the lower the system's timeliness. The smart DoS attack results are similar to those without the DoS attack, indicating that this attack does not significantly impact the UD. Meanwhile, the results of the fatal and proposed DoS attacks delay the lower 1% of UDs by approximately 0.4 seconds when ρ is 0.06, which is approximately 1.5 seconds longer than the previous two results. That is, the proposed DoS attack delays and hinders real-time recognition between the vehicles.

Thus far, we have verified that the DoS attack cause severe disturbances in C-V2X networks regarding reliability, coverage, and timeliness. Additionally, we verified that the proposed DoS attack occupying the BR used by the closest vehicle is the fatal DoS attack in a highway scenario. Based on the results, we are concerned that the DoS attack will become a social problem in autonomous driving, where recognition and decision process are essential through the C-V2X networks.

V. Conclusion

This paper analyzes the DoS attack on C-V2X networks from various viewpoints. First, we derive the conditions of the vulnerable vehicle that DoS attacks can most damage. Then, we derive a simple way to find this vulnerable vehicle from the DoS attacker's viewpoint. Through the system-based simulation, the damage of a DoS attack is quantitatively evaluated in terms of reliability, coverage, and timeliness, which are communication QoS indicators. Simulation results show that the DoS attack can cause damage to the recognition and decision process of autonomous vehicles. In particular, results show the damage is more severe when attacking a vulnerable vehicle satisfying the derived conditions. The damage caused by the DoS attack is relatively reduced as the traffic becomes dense. This is due to the characteristic of C-V2X, which autonomously selects resources for each vehicle via SB-SPS. We confirm this by comparing the ratio of packet errors caused by SB-SPS and the DoS attack to the total packet errors.

We hope this paper can broaden the reader's knowledge of DoS attacks on C-V2X networks. In the near future, we plan to conduct studies for attacker detection, attack avoidance/defense, etc. In addition, we will conduct a study on overcoming DoS attacks via convergence with other sensors under autonomous driving.

References

[1] W. J. Yun, M. Shin, S. Jung, S. Kwon, and J. Kim, "Parallelized and randomized adversarial imitation learning for safety-critical self-driving vehicles," *J. Commun. Netw.*, vol. 24, no. 6, pp. 710–721, 2022.

[2] J. D. Choi and M. Y. Kim, "A sensor fusion system with thermal infrared camera and lidar for autonomous vehicles and deep learning based object detection," *ICT Express*, vol. 9, no. 2, pp. 222–227, 2023.

[3] R. L. McCarthy, "Autonomous vehicle accident data analysis: California ol 316 reports: 2015–2020," *ASCE-ASME J Risk and Uncert in Engrg Sys Part B Mech Engrg*, vol. 8, no. 3, 2022.

[4] M. Noor-A-Rahim *et al.*, "6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities," *Proc. IEEE*, vol. 110, no. 6, pp. 712–734, 2022.

[5] D. Kim, K. Kim, D. Kwon, and J.-W. Choi, "V2X-based vehicle speeding enforcement system," in *Proc. VTC2021-Fall*, 2021.

[6] R. Molina-Masegosa, J. Gozalvez, and M. Sepulcre, "Comparison of IEEE 802.11p and LTE-V2X: An evaluation with periodic and aperiodic messages of constant and variable size," *IEEE Access*, vol. 8, pp. 121526–121548, 2020.

[7] S. Chen, J. Hu, Y. Shi, L. Zhao, and W. Li, "A vision of C-V2X: Technologies, field testing, and challenges with chinese development," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3872–3881, 2020.

[8] K. Kim, D. Kim, S. Choi, D. Kwon, and J.-W. Choi, "Location-based maximum reuse distance resource scheduling for LTE cellular-V2X sidelink mode 3," in *Proc. IEEE ICEIC*, 2022.

[9] A. Bazzi, G. Cecchini, M. Menarini, B. M. Masini, and A. Zanella, "Survey and perspectives of vehicular Wi-Fi versus sidelink cellular-V2X in the 5G era," *Future Internet*, vol. 11, no. 6, p. 122, 2019.

[10] A. S. Mustafa, M. M. Hamdi, H. F. Mahdi, and M. S. Abood, "VANET: towards security issues review," in *Proc. IEEE ISTT*, 2020.

[11] Y. Kim, I. Kim, and C. Y. Shim, "A taxonomy for DoS attacks in VANET," in *Proc. IEEE ISCIT*, 2014.

[12] A. M. Malla and R. K. Sahu, "Security attacks with an effective solution for DoS attacks in VANET," *Int. J. Comput. Applicat.*, vol. 66, no. 22, 2013.

[13] O. Punal, C. Pereira, A. Aguiar, and J. Gross, "Experimental characterization and modeling of RF jamming attacks on vanets," *IEEE Trans. Veh. Technol.*, vol. 64, no. 2, pp. 524–540, 2014.

[14] A. Serageldin, H. Alturkostani, and A. Krings, "On the reliability of DSRC safety applications: A case of jamming," in *Proc. IEEE ICCVE*, 2013.

[15] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo, "Real-time detection of denial-of-service attacks in IEEE 802.11p vehicular networks," *IEEE Commun. lett.*, vol. 18, no. 1, pp. 110–113, 2013.

[16] M. R. Dey and M. Patra, "Hand it over carefully: Security breach during handover in 5G-V2X," in *Proc. IEEE COMSNETS*, 2023.

[17] N. Trkulja, D. Starobinski, and R. A. Berry, "Denial-of-service attacks on C-V2X networks," *arXiv preprint arXiv:2010.13725*, 2020.

[18] A. Mansouri, V. Martinez, and J. Härri, "A first investigation of congestion control for LTE-V2X mode 4," in *Proc. IEEE WONS*, 2019.

[19] K. Ansari, "Joint use of DSRC and C-V2X for V2X communications in the 5.9 GHz its band," *IET Intelligent Transport Systems*, 2021.

[20] "Technical specification group radio access network; evolved universal terrestrial radio access (e-UTRA); physical layer procedures (release 13); physical channels and modulation," *3GPP TS 36.213, V14.2.0*, 2018, Available online: https://www.3gpp.org/dynareport/36213.htm.

[21] G. Cecchini, A. Bazzi, M. Menarini, B. M. Masini, and A. Zanella, "Maximum reuse distance scheduling for Cellular-V2X sidelink mode 3," in *Proc. IEEE Globecom Wkshps*, 2018.

[22] M. Gonzalez-Martín, M. Sepulcre, R. Molina-Masegosa, and J. Gozalvez, "Analytical models of the performance of C-V2X mode 4 vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1155–1166, 2018.

[23] A. Bazzi, B. M. Masini, and A. Zanella, "How many vehicles in the LTE-V2V awareness range with half or full duplex radios?" in *Proc. ITST*, 2017.

[24] 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 Veh. Technol. Mag.*, vol. 12, no. 4, pp. 30–39, 2017.

[25] "Technical specification group radio access network; study on LTE-based V2X services," *3GPP TR 36.885 V14.0.0*, 2016, Available online: https://www.3gpp.org/dynareport/36885.htm.

[26] J. Meinila *et al.*, "D5. 3: Winner+ final channel models," *Wireless World Initiative New Radio WINNER*, pp. 119–172, 2010.

[27] D. Li and Y. Liu, "In-band emission in LTE-A D2D: Impact and addressing schemes," in *Proc. IEEE VTC-Spring*, 2015.

[28] R. Sattiraju, D. Wang, A. Weinand, and H. D. Schotten, "Link level performance comparison of C-V2X and ITS-G5 for vehicular channel models," in *Proc. IEEE VTC-Spring*, 2020.

[29] H. Bagheri *et al.*, "5G NR-V2X: Toward connected and cooperative autonomous driving," *IEEE Commun. Standards Mag.*, vol. 5, no. 1, pp. 48–54, 2021.

Kyungtae Kim received the B.S. degree in Electronic Engineering from Kyungpook National University (KNU), Daegu, South Korea, in 2013, and received the M.S. and Ph.D. degrees in Electrical Engineering from the Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu, South Korea, in 2018 and 2022, respectively. Since 2022, he is working as an Engineer in the field of automotive communication at LG Innotek, Seoul, South Korea. His research interests include cellular vehicle-to-everything communication and wireless power transfer for electric vehicle.

Dongyoon Kwon received the B.S. degree in Electronic Engineering, from Kyungsung University, Busan, South Korea, in 2021, and received the M.S. degree in Electrical Engineering and Computer Science (EECS) from the Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu, South Korea, in 2023. Since 2023, he is working as an Engineer at Toris, Daegu, South Korea. His research interests include vehicle-to-everything communication and autonomous driving.

Woo-Cheol Jin received the B.S. degree in Electronics Engineering from Kyungpook National University (KNU), Daegu, South Korea, in 2017. He is currently pursuing the Ph.D. degree with the Department of Electrical Engineering and Computer Science, Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu, South Korea. His research interests include radar and anti-UAV system.

Sinuk Choi received the B.S. degree in Electronics Engineering from Kyungpook National University (KNU), Daegu, South Korea, in 2017. He is currently pursuing the Ph.D. degree with the Department of Electrical Engineering and Computer Science, Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu, South Korea. His research interests include vehicle-to-everything communication and cellular communication system.

Jinmo Kim received the B.S. degree from the school of undergraduate studies, Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu, South Korea, in 2019, where he is currently pursuing the integrated M.S. and Ph.D. degrees with the Department of Electrical Engineering and Computer Science.

Ji-Woong Choi (Senior member, IEEE) received the B.S., M.S., and Ph.D. degrees from Seoul National University, Seoul, South Korea, in 1998, 2000, and 2004, respectively, all in Electrical Engineering. From 2004 to 2005, he was a Postdoctoral Researcher with the Inter-University Semiconductor Research Center, SNU. From 2005 to 2007, he was a Postdoctoral Visiting Scholar with the Department of Electrical Engineering, Stanford University, Stanford, CA, USA. He was also a Consultant with GCT Semiconductor, San Jose, CA, USA, for development of mobile TV receivers, from 2006 to 2007. From 2007 to 2010, he was with Marvell Semiconductor, Santa Clara, CA, USA, as a Staff Systems Engineer for next-generation wireless communication systems, including WiMAX and LTE. Since 2010, he has been with the Department of Electrical Engineering and Computer Science, Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu, South Korea, as a Professor. His research interests include wireless communication theory, signal processing, biomedical communication applications, and brain–machine interface.