Adaptive Resource Reservation to Survive Against Adversarial Resource Selection Jamming Attacks in 5G NR-V2X Distributed Mode 2

Taki Eddine Toufik Djaidja*, Bouziane Brik*, Sidi Mohammed Senouci* and Yacine Ghamri-Doudane†
* *DRIVE Laboratory* EA1859, Univ. Bourgogne Franche Comté, F58000 Nevers, France
†*Laboratory of Informatics, Image and Interaction (L3I)*, Univ. La Rochelle, France
{taki-eddine.djaidja,bouziane.brik,sidi-mohammed.senouci}@u-bourgogne.fr
yacine.ghamri@univ-lr.fr

***Abstract*—New Radio Vehicle-to-Everything (NR-V2X) distributed communication mode utilizes a semi-persistent scheduling (SPS) scheme, in which a reserved radio resource is used for a certain duration. However, attackers can exploit the predictability of SPS's resource assignment to cause packet dropping, by selecting already reserved resources. In this paper, we first develop a feedback-based attack detection strategy then devise the optimal evasion policy based on a fuzzy inference system that dynamically adapts the resource reservation time. Simulation results show the effectiveness of our scheme in greatly reducing packet dropping-based attacks, and also in improving the packet reception ratio within the network.**

***Index Terms*—NR-V2X, sidelink mode 2, SPS, packet dropping, adversarial resource selection, fuzzy logic.**

I. Introduction

5G New Radio Vehicle to everything (NR-V2X) technology has been standardised by the 3^{rd} Generation Partnership Project (3GPP) [1]. 5G NR-V2X enables direct SideLink (SL) communications between vehicles to support advanced V2X services, such as automated and connected driving use cases [2]. The radio resource of SL communications can be assigned in either centralized (Mode 1 in NR-V2X) or distributed (Mode 2 in NR-V2X) way [5]. In the centralized mode, the base station ensures resource allocations, whereas vehicles are in charge of managing their resource allocations in the second mode. This distributed resource assignment is performed using the sensing-based Semi Persistent Scheduling (SPS) algorithm [3].

The SPS algorithm leverages neighbor vehicles pattern about resource use to allocate radio resources. Once a vehicle decides on an available resource, it reserves the same frequency resource to transmit a certain number of consecutive packets. In such a context, the resource reservation duration depends mainly on both Resource Reservation Interval (RRI) and re-selection Counter (RC) [4]. RRI is the time interval between two consecutive packets, it has a constant value that could be 20, 50 or any multiple of 100ms up to 1s. RC represents the number of transmissions a vehicle is allowed before having to select a new RU. It is a value between 5 and 15, selected randomly before each resource reservation. After each transmission, the value of RC decrements until reaching zero. In this case, either the reserved resource will be kept (with a probability p_k), or a new resource reservation procedure will be triggered. [6]. Figure 1 illustrates a vehicle's resource scheduling scheme.

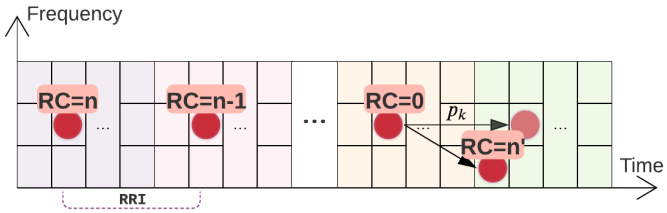


Fig. 1: Resource scheduling procedure.

Leveraging neighbors' resource reservation pattern can be very useful to minimize communication collisions, especially for the distributed allocation, this aspect can be exploited by malicious nodes (attackers) as well. A malicious vehicle may sense resource reservation information of a nearby vehicle in order to transmit on the same resource. Thus, the victim vehicle fails to send its beacon packets to its neighbors. This results in isolating the victim vehicle from its neighbors and without knowing whether it (the victim) is being attacked. Figure 2 showcases this attack scenario. Moreover, if dropped packets include emergency and alarms information, this packet dropping attack, known also as adversarial resource selection, may cause devastating effects in the vehicular network, and can lead to accidents and fatalities.

In this paper, we design an improved SPS scheme to defend against adversarial resource selection attacks and alleviate their impact. Firstly, we develop an efficient feedback mechanism that informs vehicles about collisions. Then, we leverage a fuzzy inference system to devise an optimal defense policy [7], [8]. Specifically, we dynamically adjust the resource reservation time (re-selection counter) based on the context, i.e. being attacked or not. Experimental results show the effectiveness of the proposed solution not only in reducing packet dropping-based attacks, but also in improving the packet delivery ratio in the network, and therefore ensuring the SPS performance.

The rest of the paper is organized as follows. The next sec-

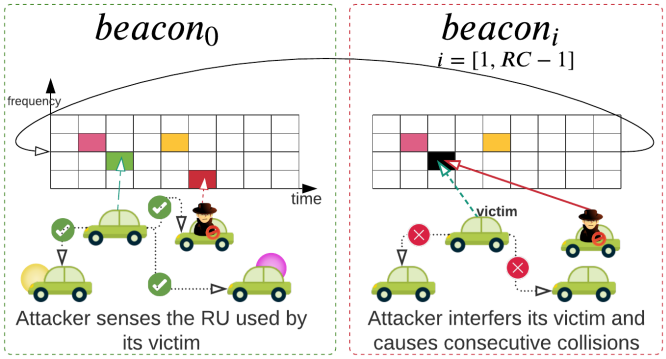


Fig. 2: Adversarial resource selection jamming attacks.

tion reviews related works. Section III discusses the methodology in three steps, first exploring the attacker's strategy and the intuitive solutions to it, then explaining the proposed detection mechanism, and finally the mitigation strategy. Section IV discusses the simulation results before concluding in Section V.

II. Related Works

Existing works can be classified into three main categories: (*i*) works exploring jamming attacks in wireless networks [9]; (*ii*) works studying channel surfing approaches against these attacks in vehicular networks [10], [11]; (*iii*) works addressing how to reduce packet collisions [12], [13].

In [9], the authors proposed two defense mechanisms to avoid interference and jamming attacks in wireless networks: channel surfing and spatial retreat. The former relies on continuously switching the channel when being attacked, while the latter is suitable for mobile nodes that can move to a safe place outside the interference zone. However, spatial evasion is not suitable for vehicular networks due to the constrained mobility of vehicles.

To mitigate jamming attacks in Vehicular Ad hoc Network (VANETs), the authors in [10], suggested to randomly alternate between the available service channels, attack detection was not considered in this channel surfing-based approach. Similarly, the authors in [11] introduced an evasive approach against packet dropping attacks. Their detection mechanism relies on feedback from the first neighbouring vehicle which will use a resource unit (RU) in the same frequency domain as the victim, indicating the occurrence of collisions in the SL Control Information (SCI). Upon the detection of an attack, the victim changes to a random different sub-frame of the same sub-channel for its RU. This reduces the attacker's ability to predict the resource used by the victim, but increases the number of legitimate collisions due to the use of an unreserved RU each time. Furthermore, the possibility of multiple attackers was not considered in this approach; another attacker can act as the feedback provider and abort the detection process.

Other works were put forward to enhance and improve the distributed mode in Cellular-V2X (C-V2X). In [12], the authors proposed an approach to reduce continuous collisions, by reserving multiple resources and allocating them alternatively. The authors in [13] presented a mechanism to reduce the number of collisions. Their approach enables terminals to transmit explicit feedback about the current channel conditions, and acknowledges radio resources that have been successfully decoded. They also designed a candidate resource selector to extend the sensing range and reduce the number of hidden terminal situations.

In this work, we specifically focus on adversarial resource selection jamming attacks in C-V2X. Differently from the works mentioned above, we tackle both the detection and mitigation of these attacks in the case of one and multiple smart jammers.

III. Methodology

In this section, we detail our optimal defense strategy to deal with adversarial resource selection jamming attacks. First, through the attackers' point of view, we examine the strategy used to obtain maximum damage. Then, as a first step of the defence, we propose a feedback-based detection strategy. Finally, we put forward an attack mitigation strategy.

A. Attacker strategy and intuitive solutions

The main objective of adversarial resource selection attacks is to cause a maximum number of consecutive collisions to a victim. This will prevent other vehicles within the communication range from decoding victim messages. Rendering the victim vehicle undetected on the road may lead to catastrophic accidents. An attacker, being an internal node, has all the necessary information for a successful attack through gathered information from SCI and beacons.

Through the received beacon packets, an attacker targets a nearby vehicle which is taking the same road. Once the target is selected, the attacker tries to keep the victim in range by matching its speed and following it. The attacker senses the used resource and reservation time from SCI then schedules its beacon messages on it. The attacker continues to sense victim's information to detect the victim's resource change (for re-selection or evasion). When that happens, the attacker switches to the new used resource. An attack can last for $RC-1$ times, meaning that the victim is only able to transmit the first beacon message correctly during the whole reservation time (Figure 2). This message is necessary for the attacker to collect the information needed to repeat the attack.

In case of multiple attackers, they ensure that the victims are distinct. So, the number of jammed nodes is equal to $min(N_{attackers}, N_{legitimates})$. Consequently, there are $N_{legitimates}$-$N_{attackers}$ legitimate nodes transmitting messages correctly (except some normal occurrences of legitimate collisions). Despite the immense danger on the targeted vehicles, attackers are considered non-aggressive jammers, because their impact on the system is considered minor, the case for this is established later through simulation shown in Figure 5.

The first basic solution is to enable targeted vehicles to select a new RU after each sent beacon, meaning that the value of RC becomes equal to 1. This will prevent the attackers

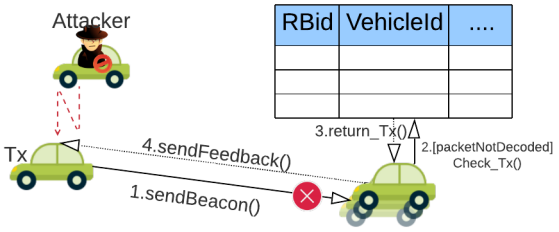


Fig. 3: Communication diagram: feedback sending.

to sense the RU used by victims, making the attack useless and futile. Unfortunately, this solution increases the number of legitimate packet collisions as there is no resource reservation step. Another solution is to make the RC adaptive. When a vehicle is attacked, it makes many consecutive RU re-selections after each beacon period. In this case, the attacker will try to compete and find the victim, but will not be able to keep up and will eventually give up. Additionally, in order to minimize legitimate collisions, the victim will gradually increase its reservation period, but if a new attack is detected, it repeats the process again.

B. Attack detection strategy

In broadcast NR-V2X transmissions, blind re-transmission is applied to ensure high reliability [2] and handle packet collisions. However, the RU used is included in the SCI. Thus, the network is still vulnerable to adversarial resource selection. Another weakness in C-V2X is the inability of the victim to detect attacks due to half duplex mode and broadcast nature, hence the design of our feedback mechanism for collision (or attack) detection. In fact, in the case of packet collisions, neighboring nodes may detect the transmitted beacon message (high received signal on RU) but fail to decode it, so the transmitter (Tx) remains unknown. Thanks to the reservation mechanism, neighboring vehicles can check the table of last received beacons. If RU was reserved before, Tx can be identified easily and with high confidence. After that, the close neighboring vehicles (which are within communication range of the victim) have to provide feedback reporting the collision's occurrence to Tx. Figure 3 explains the feedback sending process.

We suppose that the feedback is sent in unicast mode (supported by NR-V2X). However, the feedback is aborted if it is considered obsolete. We also assume that the feedback is always correctly received. If the feedback ratio of a transmitted beacon is greater than a threshold (ϕ), the vehicle will then consider the packet as dropped and triggers an immediate resource re-selection, the feedback ratio is calculated by dividing the number of received feedback on the number of neighboring vehicles (which is the number of the last received beacons). As shown in steps 3 and 5 of algorithm 1, the threshold is used for false positive alarms reduction due to infrequent legitimate collisions, and also for trust concerns due to malicious nodes injecting false feedback (this type of attackers are not considered in the paper).

Algorithm 1 FeedBackListener

Input: fb: FeedBackMessage
number_feedback: Array[][]
$number\_close\_neighbors$: Integer
Output: number_feedback
1: **if** Check_RU(fb.RU$_{id}$) **then**
2: number_feedback[fb.RU$_{id}$,fb.t] ++
3: $\alpha \leftarrow \frac{number\_feedback[fb.RU_{id}, fb.t]}{number\_close\_neighbors}$
4: **if** $\alpha > \phi$ **then**
5: RC $\leftarrow$ 0
6: **end if**
7: **end if**

C. Attack mitigation strategy

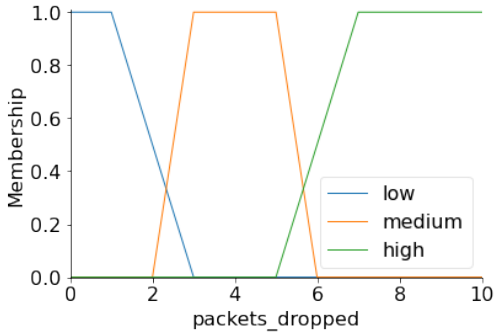
Once an attack is detected, the victim vehicle must update its RC value to reselect a new radio resource. To do so, we designed a fuzzy inference system (FIS) that decides the reservation period of each next selected RU. This novel scheme of resource reservation is described in algorithm 2 where, in step 4, the RC value is updated according to our designed FIS.

Algorithm 2 Ressource Reservation

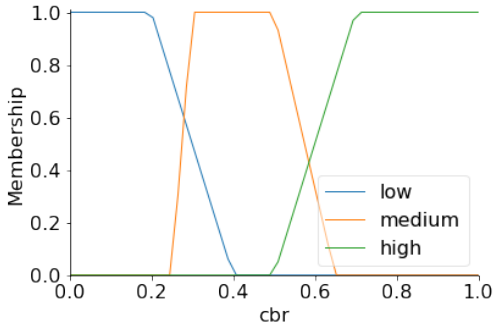
Require: $RC == 0$
{SPS Scheme}
1: channelSensing()
2: RU $\leftarrow$ ressourceSelection()
3: cbr $\leftarrow$ calculateCBR()
{Updating RC}
4: RC $\leftarrow$ fis(number_feedbacks[:,t-Λ:t],cbr)

Fuzzy inference systems are powerful decision-making algorithm [14]. A FIS comprises four main modules: a fuzzifier, a set of rules forming a knowledge base, a fuzzy inference engine, and a de-fuzzifier. For the fuzzifier, we consider two inputs that we deemed relevant for the corresponding output (RC value). The fuzzy sets are shown in Figure 4.

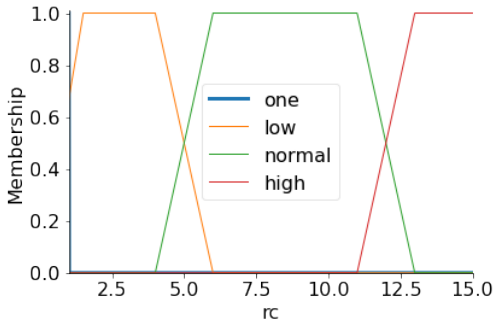
- **Number of Dropped Packets**: the number of dropped packets in the observation interval ([t-Λ, t]), helps classifying the collisions as legitimate or malicious, through three linguistic values: low, medium and high.
- **Channel Busy Ratio** (CBR): represents the time ratio the channel is sensed as busy on the total observation time, as defined in SPS scheme. The highest the CBR, the more vehicles will struggle in finding a RU, and hence the channel congestion. CBR depends mainly on vehicle density.
- **RC value**: represents the output of our FIS. We distinguish four linguistic values: One (fuzzy singleton), Low, Normal and High. One is used when trying immediately to escape from the attacker, Low represents the gradual increase towards the Normal state as defined in the standards [5], High RC values are greater than 10.



(a) Number of dropped packets



(b) Channel Busy Ratio



(c) Reselection Counter

Fig. 4: Fuzzy sets.

Once an attack is detected, our strategy is to allow vehicles to escape by consecutively changing resources. However, the aim is also to avoid constant resource reselection when legitimate collisions are produced. This generally occurs in congested traffic, where either CBR is high or the change of RU is frequent.

As for the inference system, we established a set of fuzzy rules for decision making validated by tests. Table I illustrates the set of fuzzy rules we devised. These rules are designed to ensure that our inference system finds the right trade-off between the necessity of consecutively changing RU to escape attacks, and staying on the same RU when legitimate collisions occur.

If the number of packets dropped by the vehicle is considered high, it definitely indicates an attack in progress, regardless of the CBR value. In this case the only solution is to set RC to one in order to escape the attacker. If the number of packets dropped by the vehicle is considered medium, it is difficult to deduce whether they are being dropped due to an attack or due to legitimate collisions. In this case, it is necessary to check the CBR value to devise the optimal strategy:

- High CBR: Changing RC will likely cause collisions with other neighbouring vehicles since the probability of finding an available RU is low.
- Medium CBR: The available RUs will allow the vehicle to escape the attack or avoid the legitimate collisions by gradually diminishing RC to increase the rate of re selection.
- Low CBR: The system will not suffer any side effects, therefore it is better to put RC to one in order to clear out of any kind of collisions (malicious or legitimate).

As for the case of a low number of packets dropped, RC is kept to normal except when CBR is low. In that event, a high value is assigned to RC thereby slowing down on the re-selection procedure.

Inputs		**Output**
Dropped Packets	**CBR**	**RC**
HIGH	-	ONE
MEDIUM	HIGH	NORMAL
MEDIUM	LOW	ONE
MEDIUM	MEDIUM	LOW
LOW	HIGH	NORMAL
LOW	MEDIUM	NORMAL
LOW	LOW	HIGH

TABLE I: Fuzzy rules examples.

For de-fuzification, we used the centroid method which is calculated as follow:

$$x^* = \frac{\int \mu(x) x dx}{\int \mu(x) dx}$$

where:

- x^* the output value;
- $\mu(x)$ is the RC membership value for the point x.

IV. Simulation and Results

To validate the proposed scheme and analyze its performances, we used LTE-V2V simulator [15]. It implements the sensing based SPS scheme used in LTE-V2X mode 4, which is similar to NR-V2X mode 2. We performed the simulation over 20 seconds on a 2 km road of 3 lanes per direction. The vehicles follow Poisson distribution in their positioning with a density $\rho \in \{50, 75, 100, 125, 150\}$ vehicles per km. The vehicles send beacon packets at 10Hz frequency with a transmission power of 23 dBm. Two main 2 sub-channels per sub-frame are used by vehicles to send their packets and hence 200 RU.

We compared our scheme performance to the SPS scheme according to the Packet Reception Ratio (PRR). PRR represents the ratio between the number of vehicles that correctly received beacon packets and the total number of vehicles

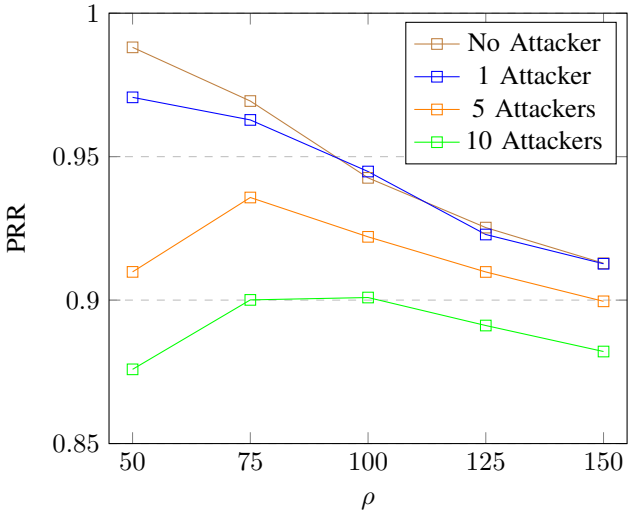


Fig. 5: Impact of adversarial resource selection attacks on PRR.

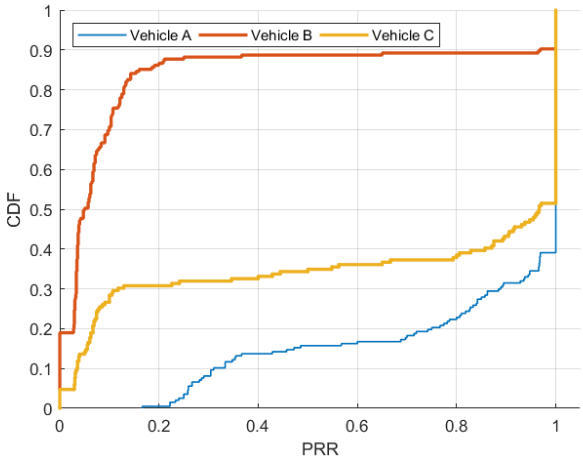


Fig. 6: Cumulative distribution function of PRR.

within the communication range of the transmitter vehicle. We set the number of attackers to $N_{attackers} \in \{0, 1, 5, 10\}$. A packet is presumed dropped if $\phi \geq 0.3$, and the observation period λ is 20 sub-frames.

Figure 5 shows the impact of the adversarial resource selection jamming attacks on the average PRR value when varying both vehicle density (ρ) as well as the number of attackers. We note that for a 0 attacker case, the dropping PRR is mainly due to legitimate collisions. Despite this, we observe that there is no great difference in PRR values between the no attacker and one attacker cases. This difference is only apparent for low-density scenarios (from 50 to 75 vehicles). We also remark that the PRR value decreases as the density increases, for all considered cases. Upon reaching high-density scenarios, the difference in PRR becomes truly small (approximately 2% between 0 and 5 attackers, 4% between 0 and 10 attackers in each scenario). The average PRR value stays above 87% for all considered cases regardless of vehicle density. These findings clearly demonstrate the low effectiveness of these attacks on the entire system, which is the reason why they are called non-aggressive.

In order to show the effectiveness of the proposed approach, we considered a scenario where vehicles density is ρ= 150 vehicle/km; we observed the PRR of three vehicles: (*i*) vehicle A: safe (unattacked), (*ii*) vehicle B: attacked and does not implements our approach, and (*iii*) vehicle C: being attacked and implements our approach. Figure 6 shows the cumulative distribution function (CDF) of PRR for each beacon sent by the different vehicles. We observe that only 10% of packets sent by the vehicle B have a PRR equal to one, an extremely low value compared to vehicles A and C which have values of 60% and 55% respectively. Vehicle B is clearly the most impacted by the attacks, as 85% of packets have a PRR less than 20%, the vehicle is almost isolated. In contrast, the PRR of vehicle C is close to that of a safe vehicle A, as 65% of packets have a PRR higher than 80% (77% for safe vehicles) .

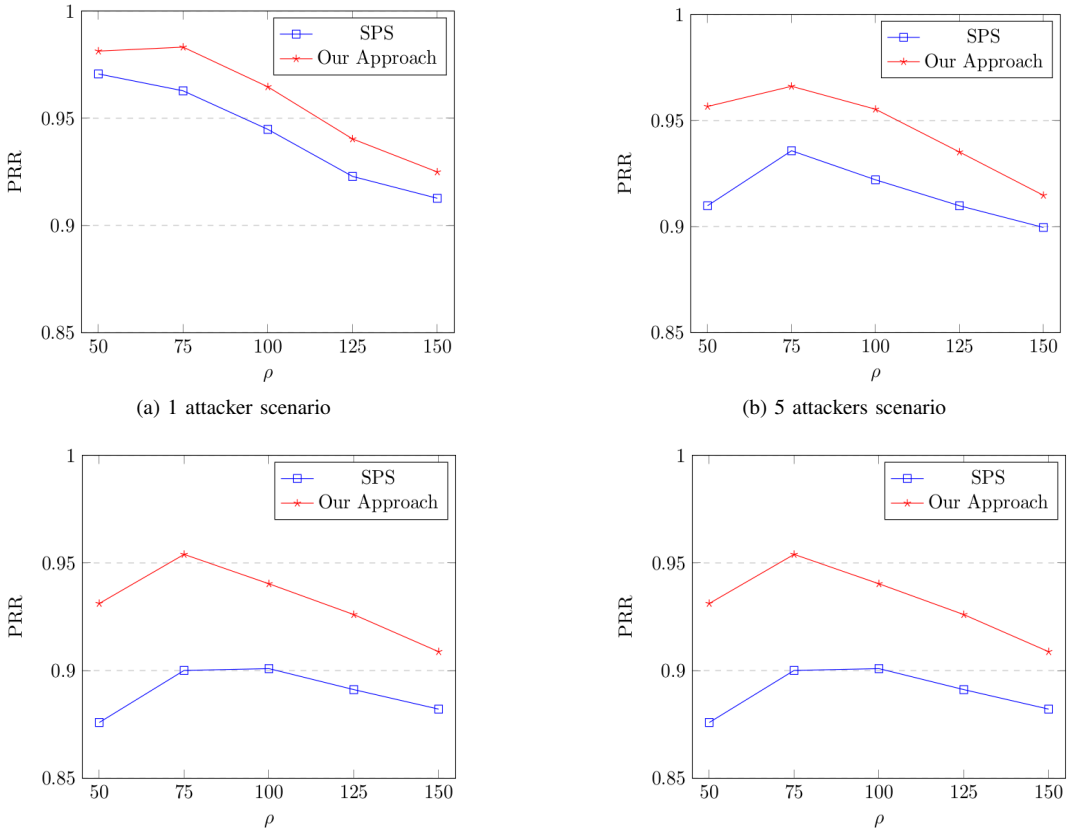
Despite varying the number of attackers, the proposed approach leads to a higher PRR compared to that of the SPS scheme, demonstrating its effectiveness in defending against adversarial resource selection attacks, as shown in (Figure 7). Even in the case of no attackers (Figure 7d), PRR is improved due to the reduction of consecutive legitimate collisions, thanks to the feedback mechanism that triggers the re-selection in vehicles, as well as the new adaptability of the RC that takes into consideration congestion situations.

V. Conclusion

In this paper, we proposed an improved version of SPS algorithm to deal with adversarial resource selection jamming attacks in C-V2X. We first designed a feedback mechanism that alerts vehicles when they fail to transmit their packets. We then leveraged a fuzzy logic to devise an optimal defense strategy against packet-dropping attacks, the strategy consists of dynamically adjusting the re-selection counter value as a key parameter in the semi persistent schemes. Simulation results show that our scheme can significantly reduce the effectiveness of such attacks, even if the attackers are numerous. Our approach also outperforms SPS scheme in terms of PRR by minimizing the number of legitimate collisions. For future works, we aim to investigate other decision making techniques like machine learning and reinforcement learning in dealing with this type of attacks. Simulation results of each method will be compared to those of other methods.

Acknowledgment

This work is achieved as part of the European project ITEA PARFAIT (https://itea3-parfait.com), which is partially funded by FEDER (European Regional Development Fund), BPIFRANCE, and the BFC region (Bourgogne-Franche-Comté).



(a) 1 attacker scenario

(b) 5 attackers scenario

(c) 10 attackers scenario

(d) no attacker scenario

Fig. 7: SPS vs. our defending approach.

REFERENCES

[1] "Release description; Release 16," 3rd Generation PartnershipProject (3GPP), Technical report (TR) 21.916, 2020.

[2] "Architecture enhancements for 5G System (5GS) to supportVehicle-to-Everything (V2X) services," 3rd Generation PartnershipProject (3GPP), Technical Specification (TS) 23.287, 2020.

[3] "Study on NR Vehicle-to-Everything (Release 16)," 3rd Genera-tion Partnership Project (3GPP), Technical report (TR) 38.885 V16.0.0,2019.

[4] M. H. C. Garcia et al., "A Tutorial on 5G NR V2X Communications," in IEEE Communications Surveys & Tutorials, doi: 10.1109/COMST.2021.3057017.

[5] M. Harounabadi, D. M. Soleymani, S. Bhadauria, M. Leyh and E. Roth-Mandutz, "V2X in 3GPP Standardization: NR Sidelink in Release-16 and Beyond," in IEEE Communications Standards Magazine, vol. 5, no. 1, pp. 12-21, March 2021, doi: 10.1109/MCOMSTD.001.2000070.

[6] 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," in IEEE Vehicular Technology Magazine, vol. 12, no. 4, pp. 30-39, Dec. 2017, doi: 10.1109/MVT.2017.2752798.

[7] M. A. Benblidia, B. Brik, L. Merghem-Boulahia and M. Esseghir, "Ranking Fog nodes for Tasks Scheduling in Fog-Cloud Environments: A Fuzzy Logic Approach" 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), 2019, pp. 1451-1457, doi: 10.1109/IWCMC.2019.8766437.

[8] N. Tamani, B. Brik, N. Lagraa and Y. Ghamri-Doudane, "On Link Stability Metric and Fuzzy Quantification for Service Selection in Mobile Vehicular Cloud," in IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 5, pp. 2050-2062, May 2020, doi: 10.1109/TITS.2019.2911860.

[9] Wenyuan Xu, Timothy Wood, Wade Trappe, and Yanyong Zhang. 2004. Channel surfing and spatial retreats: defenses against wireless denial of service. In Proceedings of the 3rd ACM workshop on Wireless security (WiSe '04). Association for Computing Machinery, New York, NY, USA, 80–89. DOI:https://doi.org/10.1145/1023646.1023661

[10] H. NGUYEN-MINH, H. T. TRAN, A. T. GIANG and T. T. HOANG, "Channel Surfing to Mitigate against Jamming Attacks on Safety Applications in Vehicular Networks," 2020 RIVF International Conference on Computing and Communication Technologies (RIVF), 2020, pp. 1-5, doi: 10.1109/RIVF48685.2020.9140788.

[11] Y. Yoon and H. Kim, "An Evasive Scheduling Enhancement Against Packet Dropping Attacks in C-V2X Communication," in IEEE Communications Letters, vol. 25, no. 2, pp. 392-396, Feb. 2021, doi: 10.1109/LCOMM.2020.3030811.

[12] S. Jung, H. Cheon and J. Kim, "Reducing Consecutive Collisions in Sensing Based Semi Persistent Scheduling for Cellular-V2X," 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), 2019, pp. 1-5, doi: 10.1109/VTCFall.2019.8891226.

[13] P. Wendland and G. Schaefer, "Feedback-Based Hidden-Terminal Mitigation for Distributed Scheduling in Cellular V2X," 2020 IFIP Networking Conference (Networking), 2020, pp. 549-553.

[14] Harpreet Singh, Madan M. Gupta, Thomas Meitzler, Zeng-Guang Hou, Kum Kum Garg, Ashu M. G. Solo, Lotfi A. Zadeh, "Real-Life Applications of Fuzzy Logic", Advances in Fuzzy Systems, vol. 2013, Article ID 581879, 3 pages, 2013. https://doi.org/10.1155/2013/581879

[15] G. Cecchini, A. Bazzi, B. M. Masini and A. Zanella, "LTEV2Vsim: An LTE-V2V simulator for the investigation of resource allocation for cooperative awareness," 2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS), 2017, pp. 80-85, doi: 10.1109/MTITS.2017.8005625.