Denial-of-Service Attacks on C-V2X Networks

Nataša Trkulja
ECE Department
Boston University
Boston, MA, USA
ntrkulja@bu.edu

David Starobinski
ECE Department
Boston University
Boston, MA, USA
staro@bu.edu

Randall A. Berry
ECE Department
Nothwestern University
Evanston, IL, USA
rberry@northwestern.edu

***Abstract*—Cellular Vehicle-to-Everything (C-V2X) has been adopted by the FCC as the technology standard for safety-related transportation and vehicular communications in the US. C-V2X allows vehicles to self-manage the network in absence of a cellular base-station. Since C-V2X networks convey safety-critical messages, it is crucial to assess their security posture. This work contributes a novel set of Denial-of-Service (DoS) attacks on C-V2X networks. The attacks are caused by adversarial resource block selection and vary in sophistication and efficiency. In particular, we consider "oblivious" adversaries that ignore recent transmission activity on resource blocks, "smart" adversaries that do monitor activity on each resource block, and "cooperative" adversaries that work together to ensure they attack different targets. We analyze and simulate these attacks to showcase their effectiveness. Assuming a fixed number of attackers, we show that at low vehicle density, smart and cooperative attacks can significantly impact network performance, while at high vehicle density, oblivious attacks are almost as effective as the more sophisticated attacks.**

I. Introduction

Cellular Vehicle-to-Everything (C-V2X) is an LTE-based technology that enables communications between automotive vehicles (V2V), vehicles and pedestrians (V2P), vehicles and infrastructure (V2I), and vehicles and the network (V2N). Specifications for C-V2X communications started from release 14 of the 3rd Generation Partnership Project (3GPP) [1], [2]. This release defined two new modes of LTE operation (Mode 3 and Mode 4) whose major difference is resource allocation: where Mode 3 relies on the cellular base-station to perform resource allocation, Mode 4 has been designed to allow vehicles to allocate resources on their own. Operating in Mode 4, vehicles utilize their own radio user equipment (UE) to communicate without having access to the cellular network.

To operate in Mode 4, vehicles select appropriate resource blocks (RBs) that will be used to transmit their Basic Safety Messages (BSMs). A resource block is a set of OFDM sub-carriers within a given time-slot. Vehicles operating in Mode 4 sense and process incoming signals to select resource blocks from the 20% of those available with the lowest Received Signal Strength Indicator (RSSI) [2]. When a vehicle selects a resource block, it periodically transmits BSMs on that resource block for a certain duration called the "semi-persistent period". Once the semi-persistent period expires, the vehicle selects a new resource block with a probability p[1]. As vehicles go through this process, they may randomly end up choosing the same resource block for a period of time which results in packet collisions. It is these types of collisions that serve as the basis for the Denial-of-Service (DoS) attacks on C-V2X networks that we are envisioning.

The purpose of this paper is to investigate if and how the resource block selection process can be abused by a malicious party. Specifically, we consider one or more adversaries, each equipped with a C-V2X device, that aim to launch a DoS attack on the network by inducing packet collisions and hence lowering the packet reception ratio (PRR). We consider adversaries with different levels of sophistication. Thus, we consider "oblivious" adversaries, which ignore recent transmission activity on resource blocks and just select a new resource block with probability $p' \neq p$, versus "smart" adversaries that monitor activity on each resource block before deciding on which one to transmit next. We also consider "cooperative" adversaries that work together to ensure they attack different targets. Our goal is to assess the potency of these attacks as a function of the vehicle density and the number of attackers.

Our main contributions are as follows:

1) We show that C-V2X networks are vulnerable to DoS attacks caused by adversarial resource block selection.
2) We introduce attack types of increasing level of sophistication, and investigate their effect through analysis and simulation based on the specifications of the C-V2X protocol.
3) We show that the most effective oblivious attack is one where the attacker selects a new resource block with probability $p' = 1$. This result is formally proven for a special case and shown to hold in general through simulation.
4) We show that collaborative attacks are more potent than smart attacks, which in turn are more potent than oblivious attacks, especially at low vehicle density. Yet, at

[1]In general p can be set anywhere in the range between 0.2 and 1. In our simulations, we use $p = 0.2$ as in [3], while in some of our theoretical results we allow p to take any value in $[0, 1]$.

Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2021
21 February 2021
ISBN 1-891562-68-1
https://dx.doi.org/10.14722/autosec.2021.23006
www.ndss-symposium.org

high vehicle density, oblivious attacks become almost as effective as the more sophisticated attacks.

To the best of our knowledge, the attacks presented in this paper have not been studied before. The goal of the paper is to provide insight into these attacks, and hence we start by evaluating them in simple network configurations. In the paper's conclusion, we discuss potential areas for future work.

This paper is organized as follows. Section II discusses existing work regarding DoS attacks on vehicular networks and C-V2X security in general. Section III introduces the different attack types. Section IV presents analysis that sheds light on the effectiveness of the attacks. Section V showcases the results we obtained by simulation to investigate the effectiveness of the different attack types under a variety of conditions. Section VI concludes the paper.

II. Related Work

Denial-of-Service attacks have long been recognized as a significant threat to vehicular networks [4]. Their ability to congest the RF spectrum and prevent vehicles from accessing necessary RF resources, their ability to impede the flow of safety-critical information between vehicles, as well as their ability to deny vehicles access to road-side units (RSUs) have rendered them one of the most dangerous attacks against vehicular networks. DoS attacks have been studied to a great extent within the context of Dedicated Short Range Communication (DSRC). For instance, [5], [6] evaluate the performance of DSRC-based vehicular networks under jamming attacks and [7]–[9] focus on developing DoS detection mechanisms and antijamming techniques.

Being more recent than DSRC, research on C-V2X has mostly focused on performance aspects, e.g., [3], [10]. There is a limited pool of work that investigates the security aspect of C-V2X networks. The work in [11] reviews potential threats to C-V2X networks, including Denial-of-Service attacks, recognizing that such attacks could compromise the reliability of C-V2X service. The work in [12] evaluates the security of the C-V2X protocol, as outlined in [2], and proposes a privacy-preserving scheme. Additional work develops a mechanism for detecting DoS attacks while operating in Mode 3 of the C-V2X protocol [13]. That work identifies a DoS attack that maliciously reserves the resources at an evolved NodeB (eNB) node with the goal of denying service to honest vehicles. To the best of our knowledge, our work is the first to explore the impact of DoS attacks in Mode 4 of C-V2X networks.

III. Attack Types

In this section, we introduce different types of DoS attacks based on adversarial resource block selection. These attacks increase the likelihood of packet collisions. Under the assumption that all resource blocks are orthogonal, packet collisions happen when two or more vehicles in the system choose the same resource block at the same time. Here, we assume that all vehicles are within a close enough range of each other so that when such a collision occurs, this results in neither of the two vehicles' messages being received by the remaining vehicles. Note that such collisions may occur even in the absence of attacks due to the random nature of resource block selection. There simply will be instances when two or more vehicles happen to randomly choose the same resource block even without any malicious vehicles in the system. This scenario, without malicious vehicles, represents the **baseline** case against which we will be comparing the different attack types.

Before describing the attack types, we need to define several important system parameters. We assume that BSMs are sent by each vehicle every T_{tr} seconds, which we refer to as the *transmission period*. Each vehicle v_i uses a resource block r_i to transmit its BSM, where i represents a specific resource block. T_s is the number of transmission periods within a semi-persistent period, that is vehicle i transmits BSMs on resource block r_i for T_s times. Upon the expiration of the semi-persistent period, an honest vehicle changes its resource block with a probability p as mentioned earlier.

Attacker goal. The attacker's goal is to minimize the packet reception ratio (PRR) in the network, which is the fraction of correctly received packets to the total number of transmitted packets.

Attacker capabilities. We assume each attacker to be a vehicle with the same C-V2X capabilities as the target vehicles (e.g., they receive and transmit valid BSMs). In particular, each attacker can only use one resource block at a time and switch its selected resource block after a semi-persistent period. We use the following characteristics to further classify the attacks:

- **Oblivious**: An attack is oblivious if attacker vehicles do not have to listen in on target vehicles' communication (i.e., which resource blocks they are transmitting on).
- **Cooperation**: An attack type is cooperative if attackers cooperate to deliver a more efficient attack.

A. Attack Type 1: Oblivious Attack

In **attack type 1**, attacker vehicles select a resource block with a probability p' choosing from the entire pool of RBs. There are a couple of special cases of this attack type:

- $p' = 0$. This implies that the attacker vehicles never change the resource block they originally and randomly selected. As the attacker resource block selection is random, it may or may not select a resource block that is in use by a target vehicle at the start of the attack. Attacker vehicles may also choose the same resource block, even if it is an idle resource block. Therefore, the collisions are solely dependent on the pure chance that the attacker vehicle selects a resource block already in use at the start of the attack.
- $p' = 1$. This implies that the attacker vehicles change the resource block upon expiration of every semi-persistent period. They randomly select a new resource block among all possible blocks. The attacker vehicles may or may not choose a resource block that is already in use; this is again dependent on chance. We anticipate this special case to be more effective than when $p' = 0$.

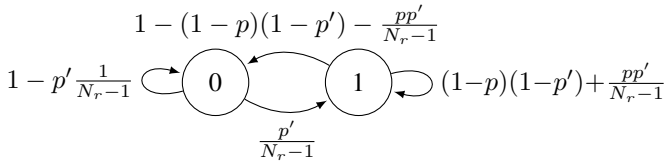

Fig. 1. Markov chain state diagram for two vehicles (one attacker, one target). State 0 represents the state in which the target vehicle and the attacker vehicle use different resource blocks. State 1 represents the state in which the target and the attacker use the same resource block, resulting in packet collision.

B. Attack Type 2: Smart Attack

In **attack type 2**, attacker vehicles look for resource blocks that are being used by only one vehicle (which we refer to as a *loner vehicle*) and select one of such resource blocks. The adversaries have to spend a period of time listening to messages sent by target vehicles to establish a list of loner vehicles' resource blocks from which they randomly choose their own. Attacker vehicles do not cooperate implying that they may choose the same loner vehicle to attack during one attack period, reducing the effectiveness of attack.

C. Attack Type 3: Cooperative Attack

In **attack type 3**, attacker vehicles look for all resource blocks that are being used by loner vehicles and each selects one of those resource blocks while ensuring no two attackers choose the same block. They have to spend a period of time listening to messages sent by target vehicles to establish a list of loner vehicles' resource blocks from which they choose their own RBs. Additionally, they have to communicate between themselves to ensure that they select different resource blocks from this list. This attack type is cooperative making it more efficient in theory, but also more challenging to implement in practice.

IV. Analysis

In this section, we analyze the potency of oblivious attacks. Lemmas 1 and 2 assume that the vehicles are synchronized implying that their semi-persistent periods are aligned.

Lemma 1. *Consider attack type 1 (oblivious attack), with one attacker and one target. Then, for any $0 < p \leq 1$, PRR is minimized with $p' = 1$.*

Proof. If there are two vehicles in the system, a single target and a single attacker, then we can model these vehicles as a Markov chain with two possible states:

- State 0: The two vehicles use different resource blocks.
- State 1: The two vehicles use the same resource block.

To minimize the PRR, the best strategy for the attacker is to maximize the fraction of time spent in state 1 because collisions take place in that state. The packet collision probability corresponds to the probability of finding the Markov chain in state 1. A Markov chain state diagram for this system is depicted in Figure 1.

Next, we explain the transition probabilities shown in Figure 1. Recall that N_r denotes the total number of resource blocks. A transition from state 0 to state 1 occurs when the attacker moves to a resource block used by the target vehicle. Note that the target vehicle will never switch to the resource block currently used by the attacker (because the channel is perceived as busy and the target won't select it as per the protocol). The transition probability from state 1 to state 0 is the complement of the transition probability from state 1 to itself. Such a self-transition occurs either if both the attacker and the target continue to use their current mutual resource block or if they both choose the same new resource block.

Let π_0 and π_i respectively represent the stationary probabilities to find the Markov chain in state 0 and in state 1. These probabilities can be computed using the balance equation:

$$\pi_0 \frac{p'}{N_r - 1} = \pi_1 \left(1 - (1-p)(1-p') - \frac{pp'}{N_r - 1}\right). \quad (1)$$

Combining Eq. (1) with the normalization equation $\pi_0 + \pi_1 = 1$, we obtain

$$\pi_1 = \frac{p'}{(N_r - 1)[p + p'(1-p) + \frac{p'}{N_r - 1}(1-p)]}. \quad (2)$$

We next take the derivative of π_1 with respect to p'. If it is positive for all $p' \in [0, 1]$, it means that π_1 is maximized when $p' = 1$.

Taking the derivative of the expression given in Eq. (2) we obtain

$$\frac{d\pi_1}{dp'} = \frac{p}{(N_r - 1)(p + p'(1-p) + \frac{p'}{N_r - 1}(1-p))^2} > 0, \quad (3)$$

for all $0 \leq p' \leq 1$ and $0 < p \leq 1$.

Therefore, we conclude that π_1 increases with p' and achieves its maximum when $p' = 1$. Conversely, the PRR decreases with p' and is minimized when $p' = 1$. □

From the proof, we note that the derivative of the packet collision probability π_1 decreases with p' (while staying positive), i.e., increasing p' leads to a diminishing return. That is, increasing p' has a much greater effect in reducing the PRR while p' is low compared to when p' is already on the higher end of its range from 0 to 1. Our simulations in Section V show that the same effect holds true in the general case of many attackers and many targets.

From the proof, we further note that the derivative of the packet collision probability converges to 0 as p tends to 0, that is the effect of p' becomes negligible as p tends to 0. The next lemma shows that this result holds in the general case.

Lemma 2. *Consider attack type 1 (oblivious attack), with an arbitrary number of attackers N_a and an arbitrary number of target vehicles N_v. If $p = 0$, then PRR is unaffected by p' for any $0 < p' \leq 1$.*

Proof. If $p = 0$, then each target vehicle always stays on the same resource block (RB). Because the attackers choose their RBs randomly, in steady-state, each attacker is equally likely to be transmitting on any RB, independently of p' (assuming $p' > 0$, so that the initial state of each attacker does not have

an effect in steady-state). Therefore, if there are N_r RBs, the probability that a given attacker transmits on RB r_i is $1/N_r$, for any $i \in \{1, 2, \ldots, N_r\}$. Assume RB r_i is used by a target vehicle, then the steady-state probability that RB r_i is jammed by one or more attackers is $1-(1-1/N_r)^{N_a}$, which is independent of p' and i. □

V. Simulation Results

In this section, we present Monte-Carlo simulation results to measure the potency of each attack type. Specifically, we aim to answer the following questions:

1) What impact does the number of attackers have on the potency of each type?
2) What impact does the value of p' have on the potency of attack type 1?
3) Which attack types are the most and the least potent, and under what conditions?

We measure the potency of the different attack types using the packet reception ratio (PRR) metric, which is the ratio of the number of packets that were successfully received to the total number of packets sent (BSMs in our case). We explore how PRR changes as a function of the total number of vehicles in the network, where *the total number of vehicles* is defined as the sum of the target vehicles and the attacker vehicles.

Simulation Setup

To simulate the attack types, we adapt a Monte-Carlo simulation model in Matlab of C-V2X networks that was introduced in [3]. The simulations are run under the following assumptions and conditions unless otherwise noted in the figures' captions:

- The vehicular network is fully-connected, implying that all vehicles are within the range of one another.
- There is no signal fading and packet losses are only due to collisions.
- Simulation time is 300 s.
- Number of simulation trials is 10.
- Transmission period, T_{tr}, is 100 ms.
- The length of the semi-persistent period is $T_s T_{tr} = 1$ s.
- There are 200 resource blocks ($N_r = 200$).
- The probability that a target vehicle changes its resource block is $p = 0.2$.

Note that the initial offsets of the semi-persistent periods for different vehicles are chosen at random, and hence the semi-persistent periods are not synchronized. Simulation parameters are representative of real-world C-V2X configurations [14], though actual deployments may implement a random semi-persistent period with a mean time of 1 s.

A. Attack Type 1: Oblivious Attack

In this attack type, attacker vehicles choose random resource blocks with the probability p'. We focus on two special cases: $p' = 0$ and $p' = 1$. For the PRR performance plots, we vary the total number of vehicles N_v and the number of attackers N_a. The results are shown in Figure 2 and Figure 3 for $p' = 0$ and $p' = 1$, respectively. The black curve is the PRR of the baseline representing the case when there are no attackers. As can be seen, the PRR drops with the increase of the total number of vehicles in both special cases. The special case of $p' = 0$ appears to have very little to no effect irrespective of the number of attackers. The special case of $p' = 1$ drops the PRR for a single attacker and five attackers by approximately 0.5% and 2% on average, respectively. This matches the analysis provided by Lemma 1 that showed that PRR is minimized when $p' = 1$ in attack type 1, but to further confirm that, we next investigate the effect of varying p' in attack type 1.

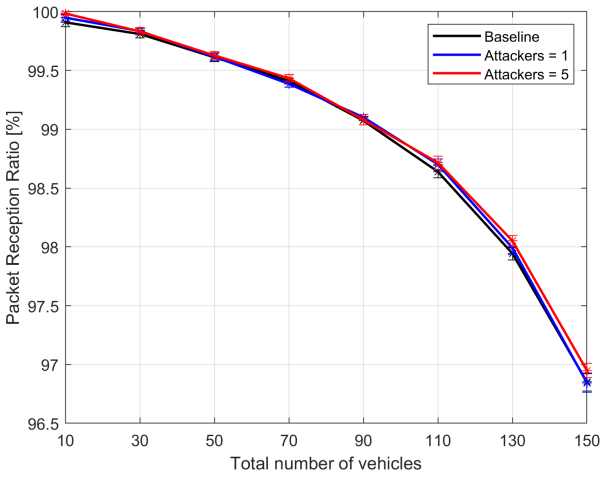

Fig. 2. PRR versus the total number of vehicles in **attack type 1,** $p' = 0$ with 95% confidence intervals. Simulation time is 3000 s.

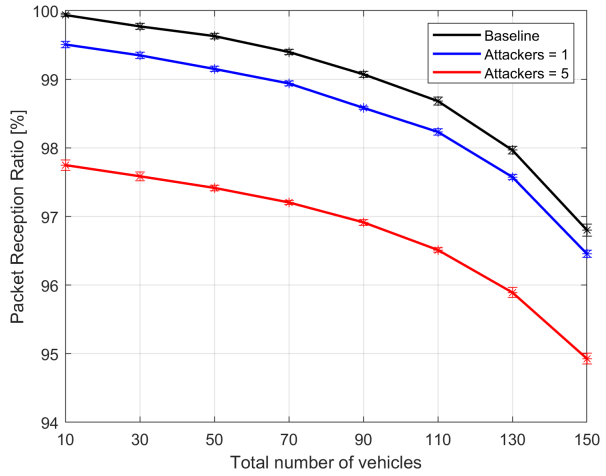

Fig. 3. PRR versus the total number of vehicles in **attack type 1,** $p' = 1$ with 95% confidence intervals. Simulation time is 3000 s.

Varying p' in Attack Type 1: To answer our second research question regarding the impact of the value of p' on the potency of attack type 1, we evaluate the PRR against the total number of vehicles. We compare the performance of the attack type at $p' = 0$, $p' = 0.5$, and $p' = 1$ while the number of attackers

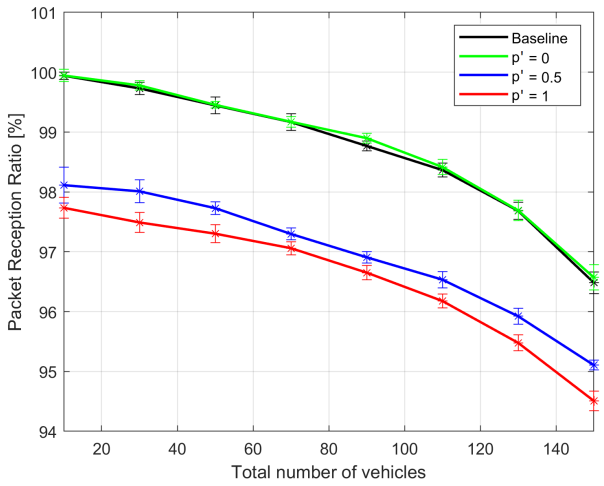

Fig. 4. PRR versus the total number of vehicles in **attack type 1** with 95% confidence intervals. We vary the value of p' to explore its effect on the potency of attack type 1. When p' is equal to 0, the attack has almost no effect. The PRR drops as the p' is increased.

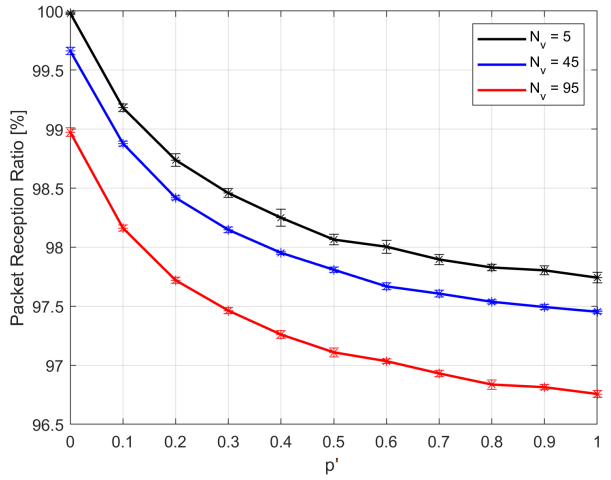

Fig. 5. PRR versus p' in **attack type 1** with 95% confidence intervals and different values of the target vehicles, N_v. The number of attackers, N_a, is fixed at 5. As p' increases, the PRR drops, with $p' = 1$ having the lowest PRR for any number of target vehicles. Simulation time is 30000 s.

N_a is fixed at 5. As shown by the resulting Figure 4, the PRR drops with the increase of p' and $p' = 1$ has the lowest PRR, in line with Lemma 1. This is perhaps the most obvious in Figure 5 where we fixed the number of attackers, N_a, to five and observed the behavior of PRR as p' is varied. The three resulting curves represent different number of target vehicles N_v. As observed from our analysis in Section IV, the effect of increasing p' becomes less pronounced as p' gets larger.

B. Attack Type 2: Smart Attack

In this attack type, attacker vehicles look for resource blocks that are used by loner vehicles and randomly select one of those resource blocks. Attackers do not cooperate implying

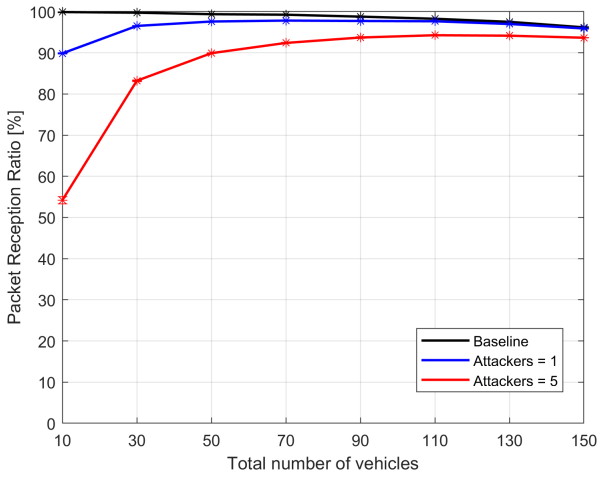

Fig. 6. PRR versus the total number of vehicles in **attack type 2** with 95% confidence intervals.

that they may target the same loner vehicle during one attack period. The results of this attack type are shown in Figure 6. The black curve is the baseline representing PRR when there are no attackers. When the total number of vehicles is 10, this attack type significantly lowers the PRR, down to 90% for a single attacker and to 55% for 5 attackers. Figure 6 shows an interesting phenomenon: as the total number of vehicles varies, with a fixed number of attackers, the PRR increases up to a certain point and then starts decreasing. Indeed, a fixed number of attackers N_a can collide with at most N_a RBs at a time. Initially, when the number of target vehicles is low, many of them are successfully jammed. However, when the number of target vehicles grows and they use different RBs, then only a subset can be affected. At high vehicle density, the PRR starts decreasing due to channel congestion.

C. Attack Type 3: Cooperative Attack

In this attack type, just like in attack type 2, attacker vehicles look for resource blocks that are being used by loner vehicles. In this type, however, attacker vehicles cooperate and ensure that they all choose a different target. The results of this attack type are shown in Figure 7. The blue curve is the baseline representing PRR when there are no attackers. As can be seen from the figure, this attack is highly efficient (PRR = 10%) when there are 5 attackers and the total number of vehicles is 10. This is because there are 5 targets and 5 attackers that collaborate, which results in collisions on all 5 targets. The PRR at that point is not 0 because the attacks occur every semi-persistent period and the target vehicles are not synchronized with respect to it. Hence, there will be target vehicles that will change their resource blocks during an attack period and before the attackers have a chance to react.

D. Comparison between Attack Types

To answer our third research question, we plot the PRR versus the total number of vehicles for $N_a = 5$ for all the

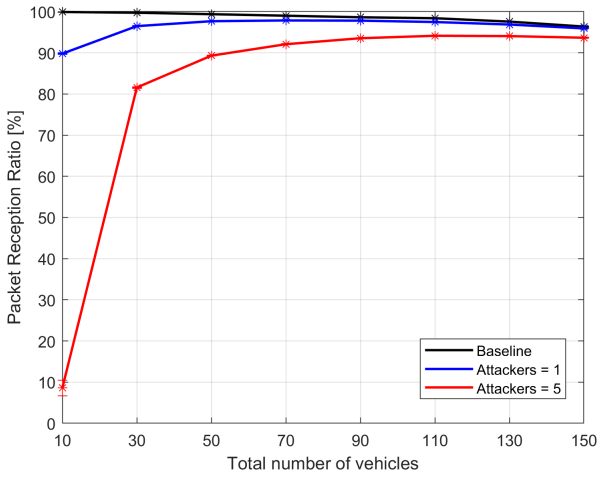

Fig. 7. PRR versus the total number of vehicles in **attack type 3** with 95% confidence intervals.

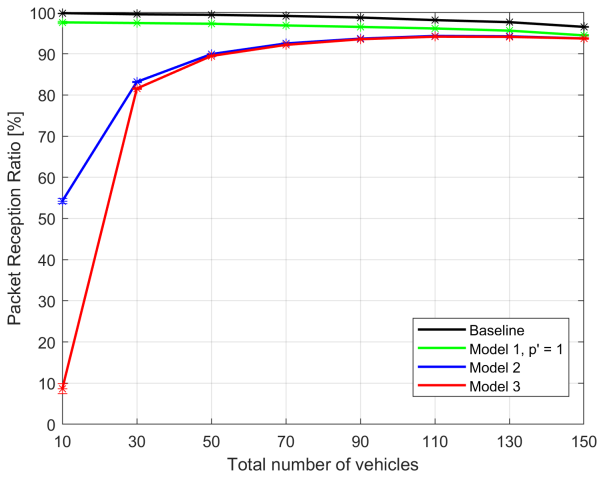

Fig. 8. Comparison of the attack types. PRR versus the total number of vehicles with 95% confidence intervals, $N_a = 5$.

attack types on the same graph (see Figure 8). As can be seen from the figure, attack type 3 is the most effective at minimizing the PRR when the vehicle density is low. Its effect is reduced as the total number of vehicles increases. This is because there will be a relatively smaller fraction of packet collisions caused by the attackers. Attack type 1 is the least effective in minimizing the PRR of the three, but the other two attack types perform only slightly better at high vehicle density.

VI. Conclusion

We introduced three types of denial-of-service attacks on C-V2X networks operating in Mode 4: oblivious, smart, and cooperative attacks. We performed extensive Monte-Carlo simulation, complemented with theoretical analysis, to investigate the potency of the various attack types. We gained the following insights from our investigation: (1) the oblivious attack is most effective when $p' = 1$; (2) for a fixed number of attackers, the smart and cooperative attacks are most effective at low vehicle density and have a significant impact; (3) when the number of target vehicles grows, oblivious attacks become almost as effective as the smart and cooperative attacks.

Our work opens several directions for further research, including modeling vehicular mobility and limited communication range, evaluating other attack objectives that are different from minimizing PRR, and incorporating channel impairments. On the theoretical side, formally proving that $p' = 1$ is optimal for an oblivious attacker in the general case is an interesting open question.

Acknowledgment

This research was supported in part by NSF under grants CNS-1908087, CNS-1908807, and CCF-2006628.

References

[1] A. Mansouri, V. Martinez, and J. Harri, "A First Investigation of Congestion Control for LTE-V2X Mode 4," in *2019 15th Annual Conference on Wireless On-demand Network Systems and Services, WONS 2019 - Proceedings*, 2019, pp. 56–63.

[2] TSGR, "TS 136 213 - V14.2.0 - LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures (3GPP TS 36.213 version 14.2.0 Release 14)," Tech. Rep., 2017. [Online]. Available: https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

[3] X. Wang, R. A. Berry, I. Vukovic, and J. Rao, "A Fixed-Point Model for Semi-Persistent Scheduling of Vehicular Safety Messages," *IEEE Vehicular Technology Conference*, vol. 2018-August, pp. 1–5, 2018.

[4] H. Hasbullah, I. A. Soomro, and J. L. Ab Manan, "Denial of service (DOS) attack and its possible solutions in VANET," *World Academy of Science, Engineering and Technology*, vol. 65, no. 5, pp. 411–415, 2010.

[5] Ó. Puñal, C. Pereira, A. Aguiar, and J. Gross, "Experimental characterization and modeling of RF jamming attacks on VANETs," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 2, pp. 524–540, feb 2015.

[6] Y. O. Basciftci, F. Chen, J. Weston, R. Burton, and C. E. Koksal, "How vulnerable is vehicular communication to physical layer jamming attacks?" in *2015 IEEE 82nd Vehicular Technology Conference, VTC Fall 2015 - Proceedings*. Institute of Electrical and Electronics Engineers Inc., jan 2016.

[7] 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, jul 2017.

[8] P. Gu, C. Hua, R. Khatoun, Y. Wu, and A. Serhrouchni, "Cooperative Antijamming Relaying for Control Channel Jamming in Vehicular Networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7033–7046, aug 2018.

[9] N. Lyamin, D. Kleyko, Q. Delooz, and A. Vinel, "Real-Time Jamming DoS Detection in Safety-Critical V2V C-ITS Using Data Mining," *IEEE Communications Letters*, vol. 23, no. 3, pp. 442–445, mar 2019.

[10] A. Nabil, K. Kaur, C. DIetrich, and V. Marojevic, "Performance Analysis of Sensing-Based Semi-Persistent Scheduling in C-V2X Networks," in *IEEE Vehicular Technology Conference*, vol. 2018-August. Institute of Electrical and Electronics Engineers Inc., jul 2018.

[11] V. Marojevic, "C-V2X Security Requirements and Procedures: Survey and Research Directions," jul 2018. [Online]. Available: http://arxiv.org/abs/1807.09338

[12] K. J. Ahmed and M. J. Lee, "Secure LTE-Based V2X Service," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3724–3732, oct 2018.

[13] Y. Li, R. Hou, K. S. Lui, and H. Li, "An MEC-Based DoS Attack Detection Mechanism for C-V2X Networks," in *2018 IEEE Global Communications Conference, GLOBECOM 2018 - Proceedings*. Institute of Electrical and Electronics Engineers Inc., 2018.

[14] T. Shimizu, B. Cheng, H. Lu, and J. Kenney, "Comparative analysis of dsrc and lte-v2x pc5 mode 4 with sae congestion control," in *2020 IEEE Vehicular Networking Conference (VNC)*.