VASP: V2X Application Spoofing Platform

Mohammad Raashid Ansari, Jonathan Petit, Jean-Philippe Monteuuis, Cong Chen
Qualcomm Technologies, Inc.
Boxborough, MA, USA
{ransari, petit, jmonteuu, congchen}@qti.qualcomm.com

***Abstract*—Vehicle-to-everything (V2X) communication is essential to redefining transportation by providing real-time, highly reliable, and actionable information flows to enable safety, mobility and environmental applications. V2X communications and its solutions enable the exchange of information (e.g., Basic Safety Messages) between vehicles, and between vehicle and network infrastructure. To ensure data quality, and hence proper action, V2X data must be authenticated and correct. In this paper, we propose an extensive attack platform, called VASP, which contains 68 BSM attacks. This platform is used to enhance V2X threat assessment, design relevant detectors, guide standardization and prioritization for deployment. The objective is to provide to the security community the tool to help build a more robust V2X system.**

Keywords*—*V2X, security, attack, framework, platform

I. Introduction

Vehicle-to-everything (V2X) communication is a key enabler for Intelligent Transportation Systems (ITS). ITS devices are equipped with a radio to allow exchange of location, kinematic, or sensor data with other road users (e.g., vehicles, pedestrians) or infrastructure (e.g., signalized intersections, traffic management center). The most common message broadcasted is called Basic Safety Message (BSM), and contains location (latitude, longitude, elevation), speed, heading, brake status and other supplemental data. Every device in the transmitter's communication range can receive BSMs, and hence can adjust its operation accordingly. An example of V2X application that consumes BSMs is Emergency Electronic Brake Light (EEBL). When the received BSM exhibits an emergency brake by its sender, the receiver can avoid a chain of rear-end collisions by warning its operator of the danger. Road safety and efficiency are greatly improved thanks to this telematics awareness. However, in order to prevent unauthorized parties to send bad data onto the V2X network, every V2X message is digitally signed [1]. Therefore, attackers are limited to radio interference attacks, or must either use their own valid credentials or steal credentials in order to send wrong V2X data. Authentication is the first line of defense.

To prevent authenticated parties to send incorrect data, the ITS devices must run a misbehavior detection system (MBDS) locally. The MBDS analyzes V2X messages' content to detect implausibility, inconsistency, or inaccuracy. For example, a vehicle receives three authenticated BSMs from the same sender, but the location reported in each consecutive BSM shows erratic position jumps. These received data cannot reliably be used for V2X safety maneuvers, and hence, flagged as suspicious. Local misbehavior detection is the second line of defense.

To effectively protect against data-centric attacks, we have to understand how the consuming applications use V2X messages. The ITS community has designed basic V2X applications, and continues to develop advanced applications to further enhance the utility of V2X data. Indeed, besides BSM, signal phase and timing (SPaT) message, MAP message, signal request message, were also designed in order to deploy smart intersections and improve road safety and efficiency. Examples of advanced applications are sensor sharing and maneuver coordination, in which vehicles can share richer data or coordinate their maneuvers respectively. With the growing number of ITS applications and services, it is paramount to expand our attacker model and attacks dataset/platform accordingly. Prior work have only proposed a handful of attacks on BSM and didn't consider the impacts on the consuming applications [2], [3], [4]. In this paper, we propose 68 attacks on BSM in order to (i) foster innovation in attacks and detectors, (ii) help the community in defining priorities for standardization and deployment of V2X misbehavior detectors. To facilitate building more attacks we contribute our open-source framework called V2X Application Spoofing Platform (VASP) [5]. VASP works as a sub-module for the V2X communication simulator, VEINS [6].

The paper is organized as follows. Section II gives an overview of the related work. Section III describes some V2X applications that consume BSMs in order to understand the effect of the attacks. Section IV specifies our attacker model. Section V lists, classifies and describes the 68 BSM attacks. Section VI gives information regarding the misbehavior detectors, but note that comparing detectors is not the objective of this paper. Section VII provides a brief analysis and benefits of our attack platform. Finally, Section VIII concludes this paper.

II. Related Work

When it comes to public attacks dataset or platform for V2X misbehavior detection research, there are VeReMi and F^{2}MD. Such platforms have been used by researchers to design, compare, and validate misbehavior detectors [7], [8].

VeReMi is a labeled simulated dataset and platform providing a wide range of traffic behavior and attacker implementations [3]. The simulations were performed in LuST scenario [9], which aimed to provide comprehensive scenarios for evaluation in VEINS simulator [6]. A second version of VeReMi has been released [4] based on F^{2}MD.

Symposium on Vehicles Security and Privacy (VehicleSec) 2023
27 February 2023, San Diego, CA, USA
ISBN 1-891562-88-6
https://dx.doi.org/10.14722/vehiclesec.2023.23071
www.ndss-symposium.org

BSM Field	Description
DSRCmsgID	Data elements used in each message to define the Message type
MsgCount	Counter that increases by one with each BSM sent.
TemporaryID	The identifier of the ITS device
Dsecond	Time since ignition started
Positions	Represents the geographic latitude, longitude, and altitude of the vehicle in the WGS84 coordinate system.
PositionAccuracy	Various quality parameters used to model the positioning accuracy for each given axis.
TransmissionAndSpeed	Represents the speed of the vehicle.
Heading	The current direction value is expressed in units of 0.0125 degrees.
SteeringWheelAngle	Represents the current steering angle of the steering wheel.
Accelerations	Represents the longitudinal, lateral, and vertical acceleration of the vehicle.
Yaw rate	Represents the yaw rate of the vehicle.
BrakeSystemStatus	Represents a data element that records various control states related to braking of the vehicle.
VehicleSize	Represents the length and width of the vehicle.

TABLE I: BSM information

F^{2}MD is a simulation framework for simulating malfunctioning V2X nodes that produce erroneous information (e.g., inaccurate position, velocity, and acceleration for vehicles), as well as misbehavior detection algorithms (e.g., based on local plausibility checks) [2].

VeReMi and F^{2}MD provided a good baseline to develop V2X misbehavior detectors. However, it is not possible to assess the effect of attacks on V2X applications directly. Our framework, VASP, offers two V2X applications as targets for attack developers: 1) EEBL and 2) Intersection Movement Assist (IMA). These are explained in Section III-B. In addition, VASP offers an extensive list of 68 attack implementations that are described in Section V.

III. System Model

A. Basic Safety Messages (BSM)

The BSM is a V2X message that is being broadcasted by its transmitter to surrounding ITS devices. Table I depicts the data contained in a BSM. Upon reception of a BSM, the receiving vehicle knows the location, kinematic state, and the dimension of the transmitting vehicle. The BSM will be used by V2X applications, for instance, to slow down in case of a car accident ahead.

B. V2X Applications

V2X applications consume the content of V2X messages. For clarity's sake, this paper focuses on two V2X applications named Electronic Emergency Brake Light (EEBL) and Intersection Movement Assist (IMA).

a) Electronic Emergency Brake Light (EEBL): The EEBL application gives a warning if a vehicle in front of the ego vehicle brakes suddenly with high deceleration. The SAE standard J2945/1 [10] defines that an EEBL application follows the following steps before sending out a warning:

1) Check if the "hard braking event" flag is set in the received BSM.
2) If Step 1 is true, check if the transmitting vehicle is in front of the ego vehicle.
3) If Step 2 is true, check if the transmitting vehicle is within a certain safety distance from the ego vehicle

If all the above conditions are true, an EEBL warning is raised.

b) Intersection Movement Assist (IMA): The IMA application specifically enables safe movement at an intersection of roads. The SAE standard J2945/1 [10] defines the workings of a typical IMA application as follows:

1) Detect if the ego vehicle is approaching an intersection. This could be performed using a map or SPaT and MAP messages from the V2X infrastructure (e.g., traffic light).
2) If Step 1 is true, calculate the time-to-collision (TTC) and distance-to-collision (DTC) values from any vehicles approaching the same intersection based on BSMs received from them. TTC and DTC calculations are made with the intersection as the reference.
3) Calculate if TTC and DTC of ego vehicle matches with any other vehicle's TTC and DTC, respectively. Matching TTC and DTC means comparatively similar values.

If any of the TTC and DTC values match, an IMA warning is raised.

IV. Attacker Model

An attacker targeting connected vehicles can be modelled as follow [11]:

Internal versus External: The internal attacker is an authenticated member of the network that can communicate with other members. The external attacker cannot properly sign her messages, which limits the diversity of attacks. Nevertheless, she can eavesdrop the V2X broadcast communication.

Malicious versus Rational: A malicious attacker seeks no personal benefits from the attacks, and aims to harm the members or the functionality of the network. Hence, she may employ any means disregarding corresponding costs and consequences. On the contrary, a rational attacker seeks personal profit and, hence, is more predictable in terms of attack means and attack target.

Active versus Passive: An active attacker can generate packets or signals to perform the attack, whereas a passive attacker only eavesdrops the communication channel (i.e., wireless or in-vehicle wired network).

Local versus Extended: An attacker can be limited in scope, even if she controls several entities (vehicles or base stations), which make her local. An extended attacker controls several entities that are scattered across the network, thus extending her scope.

Direct versus Indirect: A direct attacker reaches her primary target directly, whereas an indirect attacker reaches her primary target through secondary targets.

Our work will focus on an internal, malicious and rational, active, local attacker, which injects forged data.

Lastly, a concern in the security community is to differentiate attacks from genuine system faults. We assume that

Criteria	High	Medium	Low
Reproducibility	The attack is easily reproducible	The attack is reproducible with some limitations	The attack is hard to reproduce due to its complexity or operational cost.
Impact	The attack infects the system and can lead to catastrophic damage (e.g., an accident)	The attack infects the system and can lead to moderate damage (e.g., traffic jam)	The attack has no impacts on the system but can inflict minor harm
Stealthiness	Unknown attack occurs in certain applications	The attack needs several misbehavior detectors, message types, or data sources to be detected	Broadcasted information readily explain the misbehavior

TABLE II: Risk ratings and criteria [12]

faults are transient but attacks are persistent, deliberate, and obvious.

V. Attacks

Attacks are defined as attack messages transmitted with the sole purpose of disrupting the normal flow of either the road traffic, the target vehicle, or the V2X network. This section describes attack types, policies, and scenarios. We also provide a risk level rating of Low (L), Medium (M) or High (H) for each attack based on our own threat analysis. We use three factors to derive the risk level – reproducibility, impact, and stealthiness. Table II defines the criteria for each of the risk levels [12]. We have developed a framework called V2X Application Spoofing Platform (VASP) [5] to encourage implementing and comparing attacks. VASP works as a submodule of the open-source V2X communication simulator VEINS [6]. Please refer to the README file of VASP to learn how to install and run VASP [5]. It includes implementations of all the attacks (Sections V-A, V-B, V-C, V-D, V-E, V-F). All attacks were crafted manually, however, the attacks were injected using automated attack policies discussed in (Section V-G).

A. Attacks based on types of values transmitted

Various types of attacks can be developed based on the type of values transmitted. We define the attack types as follows.

Ghost node-based: The attacker transmits messages to create a fake node on the V2X network. The fake node is used to launch attacks and trigger unwanted behaviors. Note that the attacker's own messages are transmitted without attacks, i.e., are genuine messages. This attack is highly reproducible as the attacker can create new messages with any information she wants. In terms of impact, this attack has the ability to instill high damage by carefully crafting a series of BSMs to perform an attack. Since this attack uses a different BSM to attack, the attacker could use a different certificate to sign messages, hence exhibiting a high stealthiness. Moreover, each ghost vehicles could mimic plausible mobility patterns. This attack type has a high risk level overall.

Self-Telemetry changing: The attacker changes her own kinematic information in the transmitted messages. By reporting false kinematic information, the attack aims at negatively affecting applications or prediction algorithms. Since the attacker has control over the message content, this attack is also highly reproducible. Impact-wise, the attack has a moderate risk level because only some perturbations are added to the original kinematic fields. In terms of stealth, this attack uses the same certificate for attack and benign messages, which would increase its detectability in case of sporadic attack strategy (see Section V-G). Overall, this type of attack has a moderate risk level.

Constant/Constant Offset: The attacker either keeps the data of the targeted kinematic field constant or constantly offsets it by a certain value. For example, in a Constant Position attack, the attacker will transmit the same position even though she is moving in reality. Similarly, in a Constant Position Offset attack, the attacker will add a constant offset to the real position values. We consider this attack type highly reproducible as the attacker has control over the message content. The attack has a low impact risk level only constant values are transmitted, which is not an effective technique alone. Also, once a static attack is detected, it can be easily reported and ignored. Regarding stealthiness, we rate this attack a low risk level because easily detectable as abnormal to the natural flow of traffic. Overall, this attack type has a low to medium risk level.

Random/Random Offset: The attacker either keeps transmitting random data for the targeted kinematic field or randomly offsets the real value. For example, in a Random Position attack, the attacker will transmit random positions regardless of her actual movement. Similarly, in a Random Position Offset attack, the attacker will add a random offset to the real position values. This attack is highly reproducible as the attacker has control over the message content. Randomly changing values only acts like noise. Noise that could be easily filtered out. Hence, the impact is low. This attack type is not stealthy at all as it uses the attacker's same certificates for attack and benign messages. On top of which, these attacks act like noise in the V2X system with no correlation between messages. Overall, these attacks have a low risk level.

High: The attacker transmits excessively high/large values for the targeted kinematic field. For example, the attacker transmits higher values for speed than the highest top-speed of an on-road vehicle (e.g., 455.3 km/h [13]). As the attacker has control over message contents, this attack is highly reproducible for the attacker. Impact-wise, this attack is rated at a moderate risk level. If this attack is performed on dimensions i.e., high dimensional vehicle, the attack would not have a great impact as vehicles would just move away from such a vehicle and approach cautiously. However, if the speed or acceleration is sent as high values, receiving vehicles might perceive this as a possible collision event. These attacks are not stealthy as such values will be easily detected as implausible and the attacker would need to be sophisticated to maintain correlations between different fields, e.g, position, speed, acceleration. Overall, this attack type mostly has a low risk level. Its risk level increases to high or medium when combined with acceleration or speed, respectively.

Low: Similar to "High" attack type, the attacker transmits excessively low/small values for the targeted kinematic field. The risk level for this type of attack follows exactly the same pattern as for "High" attack type.

B. Attacks based on kinematic value used

Various types of attacks can be developed based on which kinematic field is used to perform that attack. They are defined as follows.

Position: The attacker either creates a ghost vehicle with fake positions or modifies her own position to launch position-based attacks. Risk levels of these attacks mainly depend on their combination with the Constant, Constant Offset, Random, Random Offset, High and Low attack types. Following attacks are in addition to Constant, Constant Offset, Random, Random Offset, High, and Low type attacks:

- *Targeted constant position:* Attacker chooses a target node (in this case a moving vehicle) and transmits a position that is in front of it. The attacker continues to transmit the same position until the target is out of the communication range. This attack is moderately reproducible as the attacker needs to have the resources to target vehicles quickly enough to cause a reaction from them. Also, this attack needs position data from a victim before attacking. Impact-wise, this attack has a moderate risk level as the attacks might not work on curved roads if the attacker does not take road curvature into account. Also, in a dense traffic scenario, it may not be feasible to transmit a fake vehicle location as it may overlap another vehicle's location. Many such edge cases can be thought about for this kind of attack. This attack is low in stealth because as soon as the attacker transmits the attack messages, the victim can recognize and report that no vehicle was present where the BSM claimed one to be. Overall rating: moderate. Reason: This attack could cause a vehicle to suddenly brake and cause a rear-end collision by a following vehicle.
- *Sudden appearance:* Attacker transmits a ghost vehicle message with position that is right in front of the target node (in this case, a moving vehicle). Reproducibility-wise, this attack is at a moderate risk level. The reason being similar to the Targeted constant position attack. Impact-wise, this attack has the potential to be highly damaging if timed correctly. This attack is low in stealth because right after the attack is performed, it will become apparent that no vehicle is present where the BSM claims one to be. Overall: high. Reason: Knee-jerk reaction from an autonomous vehicle could cause problems in parking lots as well as on the road.
- *Sudden disappearance:* Attacker stops transmission to go into radio silence to throw off any tracking mechanisms used by other nodes. Reproducibility: This attack is high in reproducibility as the attacker has complete control to stop transmissions anytime. Impact: Receiving vehicles would only stop tracking this attacker, they will not be harmed if they cannot track it. Stealth: This attack is highly stealthy but due to the nature of this attack. Overall rating: low. Reason: No issues as a vehicle would just stop transmitting V2X messages. It will still be visible by the sensors of other cars.

Speed: The attacker spoofs her own speed before transmitting BSMs. All attacks on speed pertain to Constant, Constant Offset, Random, Random Offset, High, and Low type attacks. Attacks related to speed usually have a moderate risk level except to LowSpeed attack because this attack could cause Time-To-Collision (TTC) and Distance-To-Collision (DTC) values to be larger than reality meaning other vehicles would think they have more time to clear their occupied space.

Acceleration: The attacker spoofs her own acceleration before transmitting BSMs. All attacks on acceleration pertain to Constant, Constant Offset, Random, Random Offset, High, and Low type attacks. Attacks using acceleration are of moderate to high risk. They become high risk when combined with "Low" type attacks because they can cause TTC and DTC values to be larger than reality and give the perception that receiving vehicles have more time to clear their occupied spaces.

Heading: The attacker spoofs her own heading before transmitting BSMs. Following attacks are in addition to Constant, Constant Offset, Random, Random Offset, High, and Low type attacks. This type of attack has an overall low risk level.

- *Opposite heading:* Attacker transmits opposite direction to her true heading, i.e., 180 degrees addition to true heading. Attack is highly reproducible as the attacker has complete control over message content. Attack has high impact rating as vehicles may react to this attack and cause a cascading effect on the traffic. This attack is moderately stealthy because the detectors might detect the attacker's car moving the opposite direction at a higher than expected speed if a vehicle is in reverse gear. This attack has a high risk level overall because it could fool a vehicle into thinking the attacker vehicle is coming towards it and force it to take evasive maneuvers causing more disruptions in dense traffic conditions.
- *Perpendicular heading:* Attacker transmits perpendicular direction to its true heading, i.e., 90 degrees addition/subtraction to/from true heading. Attack is highly reproducible as the attacker has complete control over message content. Attack has high impact rating as vehicles may react to this attack and cause a cascading effect on the traffic. This attack is moderately stealthy because the detectors might believe a car is laterally moving to change lanes. This attack also has an overall high risk level because vehicles driving beside the attacker might think there is an incoming collision with the attacker.
- *Rotating heading:* Attacker transmits a message with a certain offset to the previously transmitted heading. For example, if at time t=0, heading h=0, x=10. Then at time t=1, heading=10; at t=2, heading=20. Hence, the vehicle would seem to be rotating around its axis. The attack is highly reproducible as the attacker has complete control over the message's content. The attack has a low impact rating as vehicles may slow down before approaching such a car. Even if other cars are closer to the attacker, they could confirm such behavior by onboard sensors. This attack is low in stealth as the spoofing will be detected easily

by onboard perception systems. This attack could be perceived as a vehicle that encountered slippery surface, hence, this attack has a low risk level overall.

Yaw Rate: The attacker spoofs her own yaw-rate before transmitting BSMs. All attacks on yaw-rate pertain to Constant, Constant Offset, Random, Random Offset, High, and Low type attacks. These attacks have a low risk level overall even though they are highly reproducible due to attacker's ability to change the message content. However, impact-wise, these attacks are dependent on the heading being wrong as well. Otherwise it is too easy to calculate the correct yaw rate with values of heading over two consecutive BSMs.

Heading and Yaw Rate: The attacker spoofs her own heading and yaw-rate before transmitting BSMs. The attacker makes sure the heading and yaw-rate match each other so as to make it harder to detect anomaly based on either one of them. All attacks on heading and yaw-rate together pertain to Constant, Constant Offset, Random, Random Offset, High, and Low type attacks. All these attacks have a low risk level overall. Even though they are highly reproducible as attacker has complete control over the message content, heading and yaw-rate alone will only seem like a faulty sensor more than a malicious one. These attacks are apparent but the possibility of it being a faulty sensor make them moderately stealthy.

Dimension: In these attacks, the attacker spoofs her own dimension before transmitting BSMs. All attacks on dimension pertain to Constant, Constant Offset, Random, Random Offset, High, and Low type attacks. All dimension based attacks have a low risk level overall. These attacks are highly reproducible due to attacker's ability to change message content but impact-wise these attacks only make other vehicles aware of a larger (in terms of ”High” attacks) or smaller (in terms of ”Low” attacks) vehicle. Other vehicles can easily avoid an extraordinarily large vehicle.

C. Attacks on V2X applications

These attacks target specific V2X safety applications. The applications were implemented based on their description in the SAE J2945/1 standard [10].

EEBL: Attacks listed below target the EEBL application described in Section III.

- *Fake EEBL w/o stopping:* Attacker spoofs all the steps to raise an EEBL warning by transmitting BSMs for a ghost vehicle. However, the ghost vehicle does not stop after a fake EEBL event. As this attack directly impacts the EEBL application, we consider it as high risk.
- *Stop position after Fake EEBL:* In this attack, the ghost vehicle stops after a fake EEBL event. Since this attack improves on the previous one, we consider it as high risk as well.

IMA: Attacks listed below target the IMA application described in Section III.

- *Constant junction position:* Attacker keeps transmitting her position as being at the intersection. Sending a constant position on the intersection would mostly cause a traffic jam but not a fatal accident as approaching vehicles would become aware of the attacker's fake vehicle through V2X messages, hence this attack has a low risk level.
- *High Acceleration:* Attacker transmits higher acceleration values to throw off TTC and DTC calculations. This attack intends to make other vehicles think that the attacker is approaching the intersection earlier than in reality. This attack could cause TTC and DTC values to be smaller than reality meaning other vehicles would become cautious while approaching the intersection. This attack would clear the intersection but not cause accidents, hence this attack has a moderate risk level.
- *Low Acceleration:* Attacker transmits lower acceleration values to throw off TTC and DTC calculations. This attack intends to make other vehicles think that the attacker is approaching the intersection later than in reality. This attack could cause TTC and DTC values to be larger than reality meaning other vehicles would think they have more time to clear the intersection. This could cause fatal accidents at the intersection, hence this attack has a high risk level.
- *High Speed:* Attacker transmits higher speed values to throw off TTC and DTC calculations. This attack aims at making other vehicles think that the attacker is approaching the intersection earlier than in reality. This attack could cause TTC and DTC values to be smaller than reality meaning other vehicles would become cautious while approaching the intersection. This attack would clear the intersection but not cause accidents potentially, hence this attack has a moderate risk level.
- *Low Speed:* Attacker transmits lower speed values to throw off TTC and DTC calculations. This attack aims at making other vehicles think that the attacker is approaching the intersection later than in reality. This attack could cause TTC and DTC values to be larger than reality meaning other vehicles would think they have more time to clear the intersection. This could cause fatal accidents at the intersection, hence this attack has a high risk level.
- *Position offset:* Attacker transmits her position with a constant offset. Any type of attack on an intersection could be fatal as intersections are generally considered the most dangerous spots. Hence, we rate this attack with an overall high risk level.

D. Attacks based on mobility

In this attack type, the attacker creates plausible mobility pattern before performing the attack. This takes advantage of the path history that could be used by receiving vehicles to build trust in the sender.

Braking from communication range: The attacker selects a target node. Based on the position and the location, the attacker estimates the target node's communication range. The attacker then creates a ghost vehicle at the edge of the estimated communication range of the target. The attacker then reduces the distance between the ghost vehicle and the target node over subsequent BSMs by changing the ghost vehicle's position information. Once the ghost vehicle is within a striking distance, i.e., the distance where the target will not have much time to run advanced safety detection algorithms, the ghost vehicle brakes in front of the target. In this attack the attacker tries to gain "trust" of neighboring entities to launch an attack. The attacker could choose to perform any other type of an attack, not just braking. Hence, we rate this attack with a high risk level.

E. Attacks based on channel

This attack type targets the radio frequency or network protocols instead of a certain target node.

Denial of service: Attacker transmits dubious BSMs at a far higher rate than prescribed in standards. This attack intends to jam the channel so that other nodes cannot use the network to communicate. F^{2}MD defines additional variants of this attack. By performing this attack, the attacker could jam the local communication network only and hence we rated this attack with a moderate risk level.

F. Attacks selected randomly

These attacks are mounted by randomly selecting one of the above mentioned attacks in various ways.

Randomly select attack per node: Every time an attacker starts interacting with the V2X network, it randomly selects an attack out of the full suite of attacks described above. As this attack chooses a random attack from the above mentioned attacks, its rating highly depends on the selected attack. However, for completeness, we rated this attack at moderate risk level.

Randomly select attack per node per message: The attacker randomly selects an attack for every message transmitted. This attack would mostly cause disruption. Since this attack chooses a different attack per message, the detectors would have a hard time identifying if the attacker is using a specific attack or just fuzzing. Also, these attacks may not work where multiple BSMs are needed to launch an attack. Hence, we rated this attack as at a low risk level.

G. Attack Policies

Attack policies are defined as the process chosen by attackers to transmit attack messages. We propose two attack policies, namely, *Persistent* and *Sporadic*.

Persistent: An attacker always transmits attack messages using this policy. This attack policy makes an attacker more obvious and less targeted.

Sporadic: An attacker transmits attack messages randomly using a probability distribution to select when to attack. The attacker transmits genuine messages when it is not attacking. This policy makes attackers more stealthy.

VeReMi and F^{2}MD only employ the *Persistent* attack strategy. VASP implements both *Persistent* and *Sporadic* attack policies.

		F^{2}MD	**VeReMi**	**VASP**
# of attack		20	5	68
Attack Strategy	persistent	✓	✓	✓
	sporadic	-	-	✓
Attacked BSM fields (see Table I)	position	✓	✓	✓
	speed	✓	-	✓
	acceleration	-	-	✓
	heading	-	-	✓
	size	-	-	✓
Attacks on V2X Applications	EEBL	-	-	✓
	IMA	-	-	✓

TABLE III: Comparison of V2X attacks platform and coverage of BSM fields

H. Attack Scenarios

An attacker could use one or multiple attacks defined above to achieve her attack goal. For instance, the attacker aims to immobilize the vehicle of a nearby victim. To achieve this goal, the attacker could use several approaches as follows.

Ghost node-based attack - massive Sybil attack: As a first approach, the attacker can create several ghost vehicles to give the illusion of a traffic jam (Figure 1a). As a result, the victim's vehicle will need to brake.

Self-Telemetry changing - position overlap: As a second approach, the attacker can communicate an offset of its real position to overlap the targeted vehicle (Figure 1b). As a consequence, the automated driving system or the victim of the targeted vehicle may brake thinking there has been a collision. Note, in addition to the position offset, the attacker could have changed its type to pretend to be a pedestrian. Thus, the driving system of the targeted vehicle may believe it drove over a pedestrian.

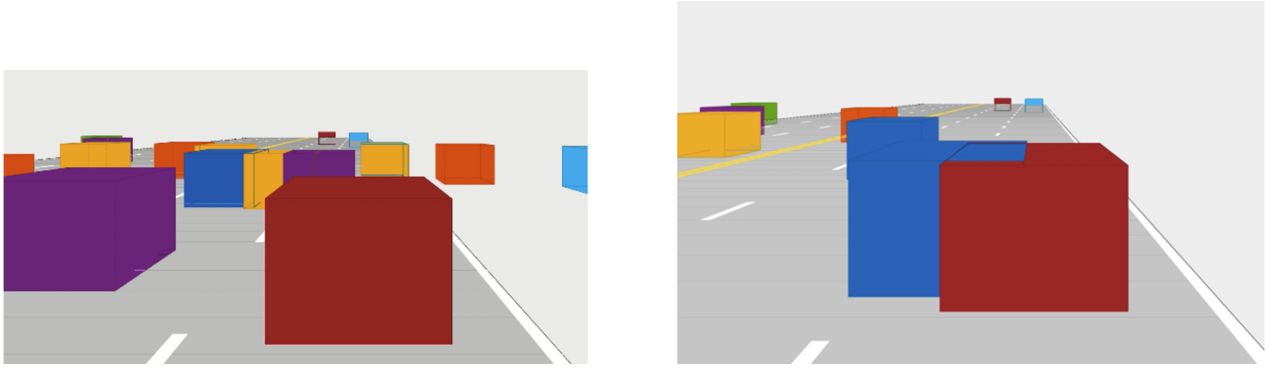
Attack on V2X application - fake EEBL: As a third approach, the attacker can transmit a V2X message including an EEBL warning (Figure 2a). Accordingly, the victim's vehicle will brake upon reception of the V2X message containing the EEBL warning (Figure 2b).

In summary, our platform, VASP, provides a wide set of attacks that allows to derive numerous attack scenarios In Section VII, we will demonstrate how VASP can be used to develop new V2X misbehavior detectors.

VI. Detectors

Detectors are algorithms that check for inconsistency or implausibility in a single V2X message or across multiple V2X messages. In this paper, we focus on inconsistency and implausibility in BSM(s). One objective is to demonstrate the benefits of having a larger attack set, not to compare detectors. Therefore, the actual detail of the detectors is considered out-of-scope.

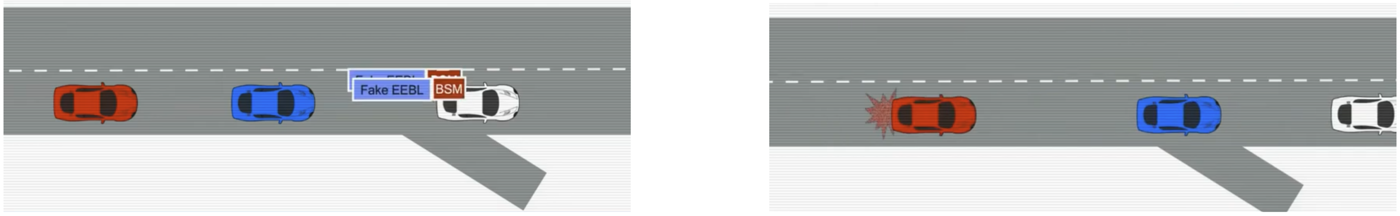
Thanks to the more extensive list of attacks provided by VASP, we selected exiting detectors and designed new ones. For example we used and extended the detectors defined by Schmidt et. al. [14] and Salazar et al. [15]. In [14], the authors defined implausible conditions for transmission and reception of BSMs, such as 1) a BSM cannot be received from further than the communication range of a vehicle; 2) BSMs cannot be transmitted at a higher frequency than 10Hz. They



(a) Ghost node-based attack: massive Sybil attack

(b) Self-Telemetry changing: position overlap

Fig. 1: Attack scenario illustrations



(a) Attacker vehicle (white/right-most) sends V2X message with fake EEBL

(b) Victim vehicle (red/left-most) brakes after receiving the fake EEBL warning

Fig. 2: Attack against V2X application: fake EEBL

		F^{2}MD			**VeReMi**			**VASP**		
	$\sum$	L	M	H	L	M	H	L	M	H
Constant	16	1	0	3	1	0	1	10	0	6
Random	18	0	1	2	0	1	1	6	4	8
High	7	7	0	0	7	0	0	0	0	7
Low	7	7	0	0	7	0	0	4	0	3
Position	7	7	0	0	7	0	0	2^*	0	5^*
Speed	6	6	0	0	6	0	0	4^*	1^*	1^*
Acceleration	6	6	0	0	6	0	0	2^*	2^*	2^*
Heading (H)	7	7	0	0	7	0	0	6^*	0	1^*
Yaw Rate (YR)	6	6	0	0	6	0	0	3^*	0	3^*
H-YR	6	6	0	0	6	0	0	4^*	0	2^*
Dimension	18	18	0	0	18	0	0	3^*	0	15^*
Bad Ratio	3	3	0	0	3	0	0	0	0	3^*
EEBL	2	2	0	0	2	0	0	0	1	1
IMA	6	6	0	0	6	0	0	1	0	5
Mobility	1	1	0	0	0	0	1	0	1	0
Channel	6	1	0	5	6	0	0	0	0	1
Random Select	2	0	0	1	2	0	0	1	0	1
$\sum(Overall)$	68	56	1	11	65	1	2	25^+	6^+	37^+

TABLE IV: Detection performance comparison (*: some figures already included in constant or random; $^+$: summation of mutually exclusive attacks)

also defined vehicle's movement implausibility and methods to validate vehicle kinematics through other sources such as maps and on-board sensors. In [15], the authors modeled the behavior of a benign vehicle based on kinematic equations and Haversine formula. From these equations, plausibility checks for individual BSM field and correlated fields were proposed.

Extending their work, we created new detectors that would validate and cross-validate different fields. We also developed detectors specifically for EEBL and IMA applications. Here, we chained detectors in a particular sequence in order to detect attacks on these applications reliably.

VII. Analysis and Discussion

Table III shows the difference between F^{2}MD, VeReMi, and VASP. As one can see, we significantly increased the attack dictionary, and cover more BSM fields. We also implemented more sophisticated attack strategies to further test misbehavior detection system.

In Section V, we discussed only some attacks that targeted specific V2X applications e.g., EEBL, IMA. However, many V2X applications have been defined in the standards [10]. These attacks could affect any of these applications. Discussing the effects of our attacks on all the applications is out of scope of this paper.

To analyze the performance of misbehavior detectors against the 68 attacks provided in VASP, we used precision, recall and F1-score as performance metrics. We ran simulations in VEINS with the attacks presented in Section V. We used the highest performing detector results to classify the attack detection performance into three level – Low (L), Medium (M), High (H). The level is assigned according to Equation 1. For example, for the RandomPosition attack, a detector that correlates position, speed and acceleration using Newtonian equations of motion could easily detect misbehavior in position data with more than 80% F1-score. On the other hand, since a high number of these random positions were beyond the communication range of the victims, the *AcceptanceRangeThreshold* detector detected this attack with more than 85% F1-score. Both detectors would be considered as *High* performers.

$$c(p, r, f1) = \begin{cases} Low, & \text{if } 0.0 \leq p, r\&f1 < 0.6 \\ Medium, & \text{if } 0.6 \leq p, r\&f1 < 0.8 \\ High, & \text{if } 0.8 \leq p, r\&f1 < 1.0 \end{cases} \quad (1)$$

where, p = Precision, r = Recall, $f1$ = F1-score, c = Performance level (Low, Medium, High).

We translated results from F^{2}MD [4], [2] and VeReMi [3] publications into Table IV based on Equation 1. In VeReMi [3], we analyzed the PR-curves of the detectors proposed and chose the best performing one.

To analyze F^{2}MD [2], we looked at Kamel et. al. VeReMi-extension work [4] as it uses the platform described in [2]. Kamel et al. described various types of DoS attacks whose primary purpose is to "flood the network". Hence, we concluded that all their attacks can be categorized as *Channel*-targeting attacks.

Table IV shows that F^{2}MD and VeReMi detectors have low performance for 57 and 66 out of 68 attacks respectively. VeReMi detectors have high detection rate of two low risk attacks, while F^{2}MD detectors are able to detect 11 low-to-moderate risk attacks. Our attack platform demonstrates the limitations of existing detectors. Obviously, our performances are better, catching 37 out of 68 attacks with more than 80% success rate. This highlights further the need for continuing expanding the attack platform.

Results also show that attacks against position, speed and acceleration are the riskiest. Indeed, these three fields are used in V2X applications and misbehavior detectors as primary values. The acceleration field is the root value used by the equations of motion for prediction of next state of position and speed. Hence, the V2X system highly relies on the correctness of these fields to function properly.

Additionally, VASP also demonstrates that attacks can be combined (or sequenced) to generate further disruption. For example, an attacker could combine "high speed" and "larger dimensions" attacks to simulate an approaching high speed truck, which would affect the drive policy (i.e., trajectory prediction and planning) differently than if a small vehicle with high speed was approaching.

In summary, thanks to an extensive attack dictionary like VASP, one could identify high threats and prioritize deployment of appropriate detectors.

VIII. Conclusion

In this paper we propose the largest BSM attack platform to date. We demonstrated its benefit in terms of threat identification, detector design, and deployment prioritization. We encourage the community to use and expand this V2X attack platform, VASP, by adding more sophisticated BSM attacks, other V2X message attacks, and cross-application attacks.

References

[1] IEEE, "IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages," *IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013)*, pp. 1–240, 2016.

[2] J. Kamel, M. R. Ansari, J. Petit, A. Kaiser, I. B. Jemaa, and P. Urien, "Simulation framework for misbehavior detection in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6631–6643, 2020.

[3] R. W. Heijden, T. Lukaseder, and F. Kargl, "Veremi: A dataset for comparable evaluation of misbehavior detection in vanets," in *International Conference on Security and Privacy in Communication Systems*. Springer, 2018, pp. 318–337.

[4] J. Kamel, M. Wolf, R. W. van der Heijden, A. Kaiser, P. Urien, and F. Kargl, "Veremi extension: A dataset for comparable evaluation of misbehavior detection in vanets," in *IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[5] Qualcomm Technologies Inc., "V2X Application Spoofing Platform (VASP)," https://github.com/quic/vasp, 2022, [GitHub, Online].

[6] C. Sommer, D. Eckhoff, A. Brummer, D. S. Buse, F. Hagenauer, S. Joerer, and M. Segata, "Veins: The open source vehicular network simulation framework," in *Recent advances in network simulation*. Springer, 2019, pp. 215–252.

[7] S. So, J. Petit, and D. Starobinski, "Physical layer plausibility checks for misbehavior detection in v2x networks," in *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2019, p. 84–93.

[8] S. Ercan, M. Ayaida, and N. Messai, "Misbehavior detection for position falsification attacks in vanets using machine learning," *IEEE Access*, vol. 10, pp. 1893–1904, 2022.

[9] L. Codeca, R. Frank, and T. Engel, "Luxembourg sumo traffic (lust) scenario: 24 hours of mobility for vehicular networking research," in *IEEE Vehicular Networking Conference (VNC)*, 2015, pp. 1–8.

[10] SAE, "Surface vehicle standard on-board system requirements for v2v safety communications j2945/1," *SAE*, 2020.

[11] J.-P. Monteuuis, J. Petit, J. Zhang, H. Labiod, S. Mafrica, and A. Servel, "Attacker model for connected and automated vehicles," in *ACM Computer Science in Car Symposium*, 2018.

[12] M. R. Ansari, J.-P. Monteuuis, J. Petit, and C. Chen, "V2x misbehavior and collective perception service: Considerations for standardization," in *IEEE Conference on Standards for Communications and Networking (CSCN)*, 2021, pp. 1–6.

[13] Wikipedia, "Production car speed record," https://en.wikipedia.org/wiki/Production_car_speed_record, 2020, [Online; accessed 28-April-2022].

[14] R. K. Schmidt, T. Leinmüller, E. Schoch, A. Held, and G. Schäfer, "Vehicle behavior analysis to enhance security in vanets," in *IEEE Vehicle-to-Vehicle Communications Workshop (V2VCOM)*, 2008.

[15] A. A. Andrade Salazar, P. D. McDaniel, R. Sheatsley, and J. Petit, "Physics-based misbehavior detection system for v2x communications," *SAE International Journal of Connected and Automated Vehicles*, Mar. 2022.