Assessing Trustworthiness of V2X Messages: A Cooperative Trust Model Against CAM- and CPM-Based Ghost Vehicles in IoV

Runbo Su[a], Yujun Jin and Ye-Qiong Song[b]
LORIA, CNRS, Université de Lorraine, France

Keywords: Trust, IoV, CAM, Collective Perception Service, Misbehavior Detection, Veins Simulation, Ghost Vehicle.

Abstract: A number of V2X (Vehicle-to-Everything) messages are standardized by the European Telecommunication Standardization Institute (ETSI), such as CAM (Cooperative Awareness Message) and CPM (Collective Perception Message). Since road safety and traffic efficiency are on the basis of the assumption that correct and accurate V2V messages are shared, ensuring the trustworthiness of these V2X messages becomes an essential task in IoV (Internet of Vehicles) security. However, containing safety-related information makes V2X messages susceptible to malicious insider attacks from compromised vehicles after the PKI (Public Key Infrastructure) authentication step (Farran and Khoury, 2023), such as Ghost Vehicles (GV) (Gyawali and Qian, 2019), passively or actively reaching a 'ghost' state in terms of communication, position, etc. By integrating CPS (Collective Perception Service) in the Veins simulator, our work aims to propose a trust assessment model in IoV against several types of CAM- and CPM-based GV to increase security. The simulation results provide a preliminary analysis of the feasibility of the proposed model and show the effectiveness in terms of assessing V2X messages' trustworthiness.

1 INTRODUCTION AND MOTIVATION

IoV is a rapidly evolving paradigm combining vehicles, roadside infrastructure, and communication technologies to provide a connected intelligent transportation system. IoV facilitates numerous functionalities like cooperative collision avoidance, intelligent traffic management, and routing optimization, and thus, vehicles can benefit from these functionalities, resulting in more comfortable and secure driving. Given this, V2X messages are introduced and implemented to exchange information regarding traffic situations between vehicles and other entities in IoV. For instance, CAM makes it possible for vehicles to transmit information containing their own current states, including position, speed, direction, etc. Differently, CPM tries to disseminate information about objects detected by local perception sensors. This type of V2X message, CPM, brings novel safety applications such that vehicles can gather information passively on objects placed out of their perception range through the received CPS information, meaning that each IoV entity's perception range is somehow extended. On the other side, verifying if the information in CPM is accurate also becomes crucial due to the fact that false information can lead to poor decision-making and ruin the trust between vehicles.

In the literature, the model named ART (Attack-Resistant Trust) in (Li and Song, 2015) proposed combining evidence collected to evaluate the trustworthiness of both data and mobile nodes (vehicles). More precisely, data trust is evaluated on the basis of sensed and collected data from multiple vehicles; node trust is measured in two dimensions, namely functional and recommendation trust. Besides, the work in (Gai et al., 2017) proposed a Ratee-based Trust Management (RTM) system by introducing social attributes of vehicles to increase the accuracy regarding trustworthiness. However, they did not adopt V2X messages for communication. A model called T-VNets (Kerrache et al., 2016) proposed a novel trust architecture for vehicular networks using received V2X messages to estimate trust. Despite the introduction of CAM and the feasibility of this framework, CPS is not supported. A recent work (Tsukada et al., 2022) combining sensing data and CPM provided an interesting scheme to check V2X messages cooperatively, but trust issues in CPM are not sufficiently

[a] https://orcid.org/0000-0001-5116-8207
[b] https://orcid.org/0000-0002-3949-340X

Su, R., Jin, Y. and Song, Y.
Assessing Trustworthiness of V2X Messages: A Cooperative Trust Model Against CAM- and CPM-Based Ghost Vehicles in IoV.
DOI: 10.5220/0012605200003702
Paper published under CC license (CC BY-NC-ND 4.0)
In *Proceedings of the 10th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS 2024)*, pages 276-283
ISBN: 978-989-758-703-0; ISSN: 2184-495X

discussed in this work.

From the above review, we can notice that CPM and CAM are rarely considered in their trust framework. Besides, most current works do not discuss CAM- and CPM-based GV attacks. To overcome these limitations, we integrate CPS in the Veins simulator to enable vehicles to share CPM containing their own PO (Perceived Object) and PO in received CPM. We also propose a trust assessment model to address CAM-based GV attacks misbehaving in communication quality, namely OOA (On-Off Attack) and NCA (NewComer Attack), and four CPM-based GV, namely Constant, Constant Offset, Random, and Random Offset. Finally, we conduct the simulation with the above CAM- and CPM-based GV to validate the performance of the proposed model from the perspective of increasing security in vehicular communication.

The rest of this paper is organized as follows. Section 2 gives details of the trust evaluation in CAM and in CPM and explicates the integration of CPM in Veins. After that, the simulation results, GV attack model, and performance validation are presented in Section 3. Lastly, Section 4 draws the conclusion and outlines our future work.

2 PROPOSED FRAMEWORK

In this section, we first introduce the trust framework and then detail the computation of trust in CAM. After that, we explicate the integration of CPS into the Veins simulator and, finally the evaluation of trust in CPM.

2.1 Overview of the Proposed Trust Framework

In IoV, sensing, communication, and computation capacities for vehicles are required, we colored these three in blue, purple, and brown in Fig. 1, respectively. The figure's upper part displays a vehicle in cooperative IoV with equipment, and the lower part illustrates functional flows within the vehicle and how the proposed trust model interacts with V2X OBU (On-Board Unit) and OBS (On-Board Sensor). In IoV, **V2X OBU** supports the communication between IoV entities, including both receiving and transmitting V2X messages: Vehicles or other entities periodically broadcast CAM to share their states and be aware of others through processing received CAM; Unlike CAM's 'I am here' manner, CPM is 'I see someone here' message to complement CAM; **OBS** in IoV consists of exteroceptive and interoceptive sides, where the former senses the surroundings and the latter monitors the vehicle's dynamics. Lastly, the **Carputer** refers to computing hardware in the vehicle, where the trust in CAM and in CPM will be investigated. We designed an extended cooperative scheme for CAM and CPM messages: the vehicle's sensing data will be counted to evaluate all incoming messages; Trustful CPM will be utilized to assess other incoming CPM. Once misbehavior of either CAM or CPM is detected, MR will be generated and sent to Misbehavior Authority (MA) as defined in (ETSI, 2020), and thus fraudulent V2X messages will be rejected and marked. It is important to note that this work aims to propose a trust assessment model helping detect CAM- and CPM-based GV attacks and to provide a preliminary analysis in the feasibility study, and the correctness of incoming MR is not included in the current scope.

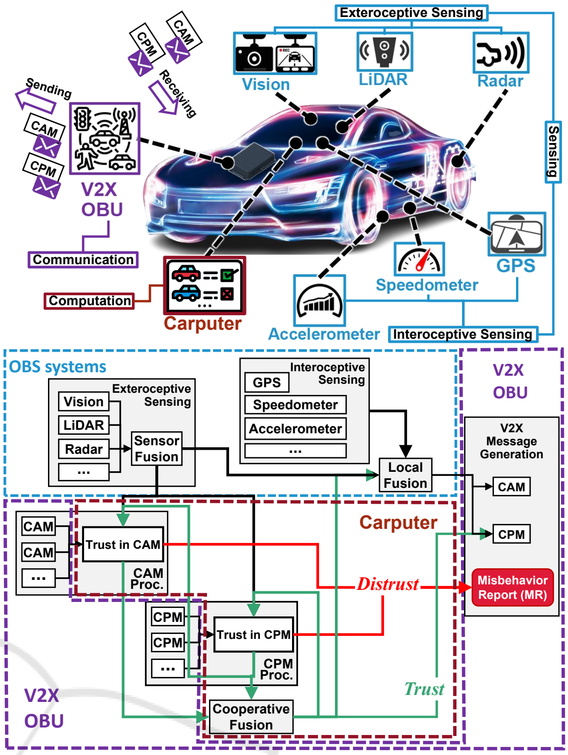


Figure 1: IoV on-board equipment and the functional flows showing how the trust model interacts with OBS and V2X OBU. Distrustful and trustful messages are highlighted in red and green, respectively.

2.2 Trust in CAM

Trust in CAM can be affected by numerous QoS (Quality of Service) factors: communication success rate, freshness of the message, etc. Since CAM is a multi-casting one-hop and one-way message standard, CAM-based communication is without request, reply, or forwarding operations (ETSI, 2019). It also means that transmission failure cannot be detected. As defined in the CAM standard, each vehicle can only passively receive CAM messages from others in a single hop. Moreover, the CAM message may be generated in an unstable manner due to the high-dynamic nature of IoV and the complex road traffic situation. Based on the above discussion, as shown in Fig. 2 we consider assessing the freshness of the message and the level of acquaintance to measure the trust in CAM.

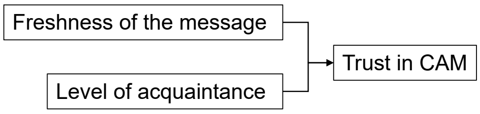


Figure 2: Composition of Trust in CAM.

Freshness of the Message p_1. With the purpose of avoiding using outdated information, from the CAM receiver's point of view, the more recent the CAM is, the more the message can be trusted. In this sense, the exponential time decay model can be employed to weigh the CAM information regarding the message's timestamp. The weight for n^{th} CAM $w[n]$ from CAM sender i is:

$$w^i[n] = \rho^{t-t_n^i} \tag{1}$$

where $\rho \in]0,1[$ refers to the decay factor, which reflects the importance of the history, i.e., $\rho = 0.5$ indicates that the trust in the CAM drops by half every second, t is the current time and t_n^i is the timestamp of n^{th} CAM from the vehicle i. Assuming that the transmission frequency is one second, the discrete weighted sum of the decay function in time is equal to the convolution with $w[n]$, and its value converges to $\frac{1}{1-\rho}$. The computation of p_1 of a CAM sender i is defined as:

$$p_1^i = (1-\rho)\sum_1^N w^i[n] \tag{2}$$

where $w^i[n]$ is given in (1).

Level of Acquaintance p_2. Malicious attackers may try to refresh their trust in IoV by re-communicating with a new fabricated identity, which is one of the intelligent attacks identified in (Su et al., 2022). To deal with this, newcomers should not be trusted as much as known ones, meaning that the known vehicle's trust can be gained more easily than newcomers. Given this, the number of communications is utilized for differing 'known' and 'less-known' vehicles, and p_2 is defined as:

$$p_2^i = \rho^{\frac{\lambda}{n}}, \quad \lambda \in R_+, \tag{3}$$

where n is the same as in (2) and (1) as the index of CAM sent by the vehicle i, and λ is a scale factor, e.g., under the parameter setting ρ=0.5, λ=5, the 5^{th} (n=5) CAM outputs $p2$=0.5, meaning that the level of acquaintance is average.

Total Trust in CAM Counting p_1 **and** p_2. To take both p_1 and p_2 into computation, we consider them equally important for the trust in CAM:

$$T_c^i = (p_1^i * p_2^i)^{\frac{1}{2}} \tag{4}$$

To summarize, $p1$ value calculates the freshness of the message, and $p2$ value determines the level of acquaintance. In such a manner, the OOA attacker misbehaves within a fixed period by pausing sending CAM, or the NCA attacker re-communicates by faking its identity will be punished.

2.3 Implemented CPM Structure

Before we explain the trust in CPM, the integration of CPS into the Veins simulator will be presented here, as CPS is incompletely supported in Veins. PO can be broadcast by vehicles via CPS, which enhances local perception, and road safety can be thus improved (ETSI, 2023). In our work, CPM was taken into consideration for IoV communication. To achieve this, we first integrated CPM into Veins in the form of a message in OMNeT++. Previous V2X studies on standards of ETSI are based on CAM and the corresponding C language standard library. We refactored CPM in C++ on the basis of the Veins-Inet subproject use case, bypassing encapsulation to enable more dynamic calling and debugging, as well as a more consistent message structure defined by the OMNeT++ framework. CPM will be sent in segments to simulate vehicles' sending capabilities and increase data processing flexibility.

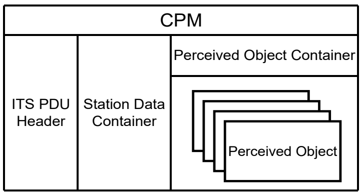


Figure 3: Structure of implemented CPM in Veins

As shown in Fig. 3, the implemented CPM structure is composed of: (i) an ITS PDU Header including the information of the protocol version, the message type, etc.; (ii) The Station Data Container provides information containing the station type and the position of the CPM generator; And (iii) a Perceived Object Container, which will be added in case that any road object has been perceived.

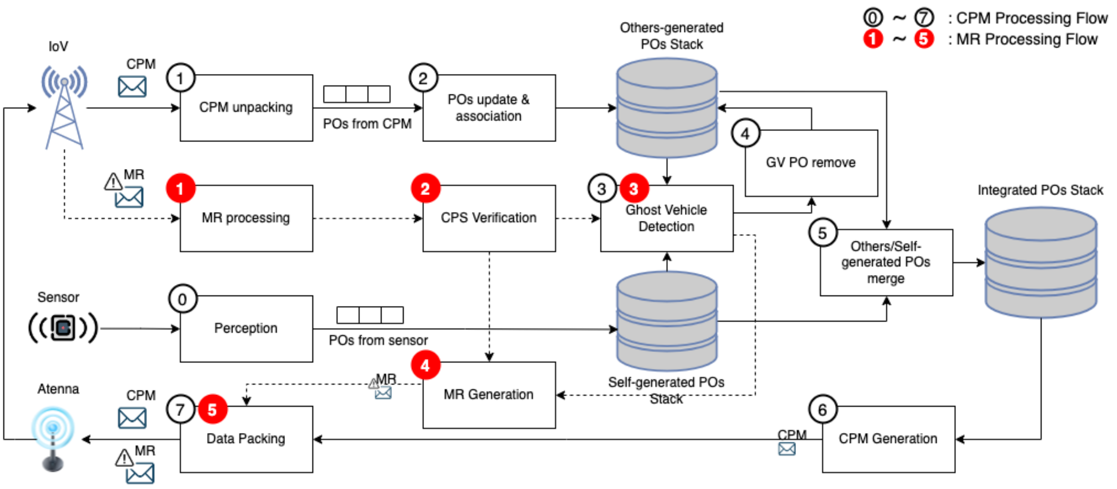


Figure 4: Pipeline of CPS application integrated in Veins Simulator

2.4 Trust in CPM

Figure 4 shows the pipeline of CPS application integrated into the Veins simulator that is categorized into two principle processing flows, namely CPM and MR, numbered by two-color labels, respectively. For any vehicle, sensors' data is regarded as the most credible source because of the first-hand information. We approximate the sensors' detection range as a circular area with a pre-configured radius to simulate the vehicle's perception capability.

As can be observed in Fig. 4, the source of POs can be either self-perceived or from incoming CPM, the latter is called others-generated in our work. After incoming CPM from other vehicles is unpacked (①), POs should be updated and associated with the receiver vehicle (②). For example, the receiver vehicle may receive a CPM in which one of the POs is itself, and thus, there is no reason that this vehicle adds itself to the outgoing CPM. Both self-perceived and others-generated POs must be verified by the GV detection process (③ & ❸). Similarly, the GV detection can be realized by either the incoming MR (❶ & ❷) or the receiver vehicle itself. When an MR informing an identified GV is broadcast, the receiver vehicle can directly forward this MR (❹) and remove the GV in POs (④). Or, if the vehicle detects the GV through its own perception capability, it will report this GV (❹). After that, the remaining self-perceived and others-generated POs will be merged into the integrated POs Stack (⑤) and then be utilized to generate outgoing CPM (⑥). Finally, the outgoing CPM or MR will sent via the vehicle's antenna (⑦ & ❺). As in ③ & ❸, the GV detection is mandatory for self-perceived and other-generated POs, and this is also the reason that we separated them to represent different PO sources in Fig. 4.

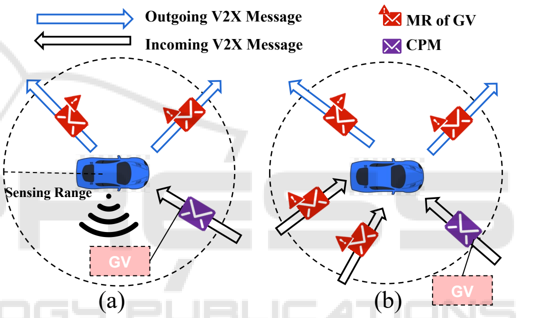


Figure 5: Two GV detection cases: in (a) or out (b) of the evaluator vehicle's perception range.

Upon receiving an incoming CPM with a new PO, if this PO is in the self-perception range and can be detected, and the associated PO is searched in the other-generated POs stack, it will be regarded as a normal PO. In case the PO cannot be detected by the CPM receiver vehicle in its perception range, it will remove this PO as in ④ and include this PO as a GV in outgoing MR as demonstrated in Fig. 5(a). Or, when the PO is out of the CPM receiver vehicle's perception range, as shown in Fig. 5(b), the PO will be considered GV if the vehicle receives two or more MR indicating this PO is GV as explicated in (Ambrosin et al., 2019). In other words, in this case, the GV detection can only work with the aid of incoming MR from other vehicles.

3 SIMULATION RESULTS

The simulation setup and implemented scenario will be presented first, and then the GV attack model. After that, we analyze the performance of the proposed model.

3.1 Simulation Environment and Traffic Scenario Considered

Veins is an open-source framework that is used for simulating communications and the interactions between vehicles in IoV (Veins,). It is based on two well-established simulators: OMNeT++, an event-based data communication simulator, and SUMO, a road traffic simulator. Veins extends these two simulators mentioned above to provide a comprehensive simulation environment for both vehicular mobility and wireless communication. As CAM communication is already supported in Veins, we integrate CPS into Veins to enable CPM communication as described in sections 2.3 and 2.4.

We summarize the simulation parameters in Table 1:

Table 1: Simulation parameter values.

Parameter	Value	
Mobility	SUMO Vandoeuvre-lès-Nancy	
Update Interval	0.1s	
Radio Type	Ieee80211DimensionalRadio	
Radio Band	5.9GHz	
Radio Bandwidth	10MHz	
Transmit Power	80mW	
Vehicle Type	CityCar	EmergencyVehicle
Vehicle Speed	10 km/h	55 km/h
Perception Range	150 m	
CAM Broadcast Frequency	1Hz	
CPM Broadcast Frequency		
ρ	0.5	
λ		

The scenario considered is based on two main assumptions: Each vehicle can track the PO in the received CPM, and the MR can not be faked. Fig. 6 shows the scene around the largest intersection called Vélodrome in the center of the city Vandoeuvre-les-Nancy in France, as the urban traffic environment considered. A three-vehicle scenario is adopted in the simulation, where node 2 (v2) is overtaking node 0 (v0), and node 1 (v1) is at a short distance in front of them. More precisely, v2 is an Emergency Vehicle with a higher speed, and other vehicles are of type City Car with a relatively lower speed. Circles in Fig. 6 (2D Visualizer) represent vehicles' perception ranges fixed at 150m.

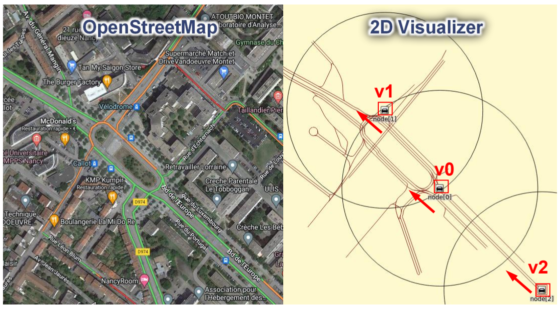


Figure 6: Considered Traffic Scenario.

3.2 Attack Model

-CAM-Based GV Attack Model. As stated in section 2, two CAM-based attack types are considered in our work:

- OOA. The attacker vehicle switches its behavior between good and bad over time to mislead the trust evaluation. In our work, we consider the OOA attacker vehicle will misbehave by intentionally doubling its original communication frequency of CAM (Su et al., 2022).
- NCA. The attacker vehicle fabricates a new identity to convey CAM with the purpose of refreshing its trust.

In the simulation, v2 is the CAM receiver, and thus, the trust evaluator and v0 will misbehave by launching the above attacks.

-CPM-Based GV Attack Model. We still fix v0 as the attacker broadcasting fake CPM of GV, and two other nodes are victims. The GV attack can be regarded as a specific form of Sybil attack, where fake-identity vehicles are created. CPM-based GV differs from CAM-based GV in a way that the attacker generates CPM containing other GV (i.e., not the attacker itself via CAM). It should be noted that CPM-based GV has no physical counterpart. As illustrated in Table 2, we involve four different types of GV in our simulation (Van Der Heijden et al., 2018).

- **Constant.** The GV's position is fixed on the map.
- **Constant Offset.** The GV will appear at a Constant Offset from the attacker, like a follower.
- **Random.** The GV's position will be randomly generated on the map.

Table 2: CPM-based GV Attack Parameters.

GV Type	Parameters/Description
Constant	$x = 461.937, y = 414.526$
Constant Offset	Δx = -100, Δy = -50
Random	Uniformly random in playground
Random Offset	d uniformly random from [0,150] θ uniformly random from [0,2π] Δx=d*cosθ, Δy=d*sinθ

- **Random Offset.** The GV will randomly appear at any location within the range of the attacker's perception range.

3.3 Performance Analysis of Trust in CAM

-Trust Under OOA Attack. We can observe that the cooperative known vehicle reaches a much higher trust level than the OOA attacker one. The misbehaving of the uncooperative vehicle, i.e., the OOA attacker, is reflected in a lower trust level as it intentionally doubles the CAM transmission frequency.

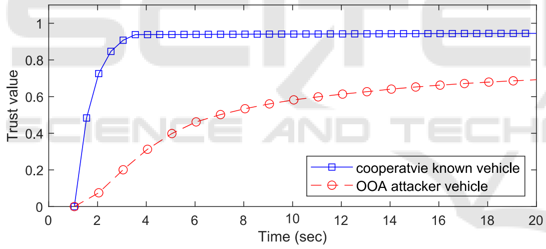


Figure 7: Trust value changes in the presence of OOA.

-Trust Under NCA attack. Differently, NCA attacker is considered at a relatively high trust level in the end, while its trust values increase more slowly than the known vehicle. This is because the newcomer vehicle lacks acquaintance of CAM messages, and thus, CAM from it will be considered less trustful.

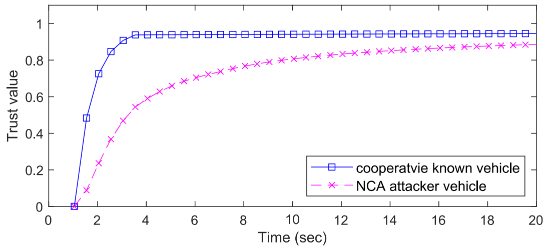


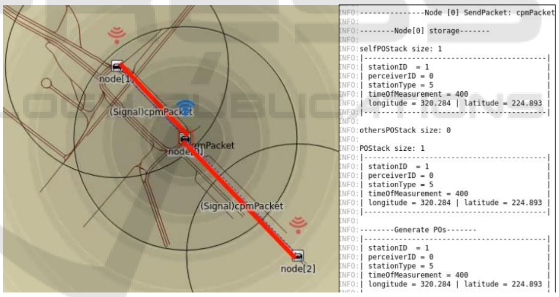
Figure 8: Trust value changes in the presence of NCA.

-Discussion. As discussed in Section 2, we evaluate the performance of trust values under OOA and NCA to measure the trust of the received CAM and the sender vehicle. The only optimal way to gain trust is to cooperate in transmitting CAM and remain known in IoV without faking the identity. For the MR generation, two thresholds are needed: 1) the number of received CAM messages and 2) the lowest acceptable trust value. In other words, the MR (Misbehavior Report) will be generated if the evaluator vehicle has received sufficient CAM messages and the trust value remains still less than the threshold. We note that the threshold can be dynamic depending on real-time traffic conditions instead of a predefined value (Hasrouny et al., 2019).

3.4 CPM Transmission and the Evaluation of Trust in CPM

For all simulation demonstrations, please refer to our recorded videos[1].

-CPM Transmission. As we can observe in Fig. 9, node0 is sending CPM, and node1 and node2 are receiving CPM. As node1 is perceived by node0, it has been included in node0's self-generated stack.



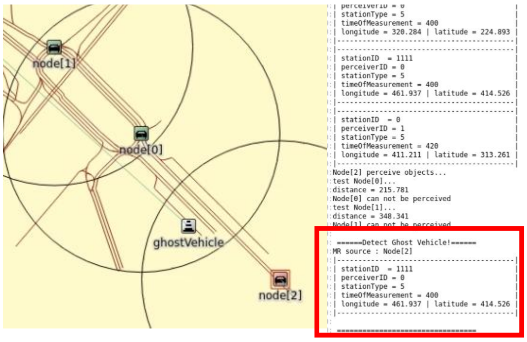
```
INFO:---------------Node [0] SendPacket: cpmPacket
INFO:
INFO:--------Node[0] storage-------
INFO:
INFO:selfPOStack size: 1
INFO:|-----------------------------------------|
INFO:| stationID  = 1                          |
INFO:| perceiverID = 0                         |
INFO:| stationType = 5                         |
INFO:| timeOfMeasurement = 400                 |
INFO:| longitude = 320.284 | latitude = 224.893 |
INFO:|-----------------------------------------|
INFO:
INFO:othersPOStack size: 0
INFO:
INFO:POStack size: 1
INFO:|-----------------------------------------|
INFO:| stationID  = 1                          |
INFO:| perceiverID = 0                         |
INFO:| stationType = 5                         |
INFO:| timeOfMeasurement = 400                 |
INFO:| longitude = 320.284 | latitude = 224.893 |
INFO:|-----------------------------------------|
INFO:
INFO:--------Generate POs-------
INFO:|-----------------------------------------|
INFO:| stationID  = 1                          |
INFO:| perceiverID = 0                         |
INFO:| stationType = 5                         |
INFO:| timeOfMeasurement = 400                 |
INFO:| longitude = 320.284 | latitude = 224.893 |
```

Figure 9: CPM Transmission Visualization.

-Constant GV Detection. Fig. 10 shows the GV is generated in node0's CPM with a pre-configured and fixed position (constant GV). Node2 will generate MR since node1111 (GV) is in node2's perception range but is not detected by node2.

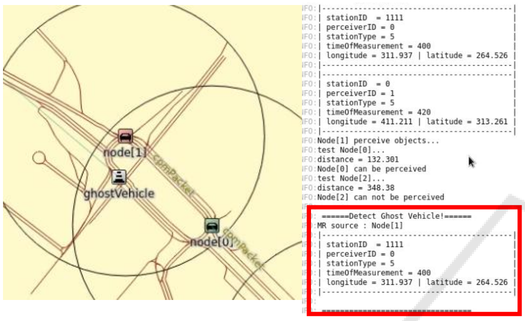
-Constant Offset GV Detection. As depicted in Fig. 11, Constant Offset GV generated by node0 remains undetected for node1 even in node1's perception range, and thus node1 reports node1111 as GV in MR. In fact, the Constant Offset vehicle would move with the attacker node0, the capture of Veins simulator cannot provide such dynamics. For a comprehensive simulation visualization of Constant Offset GV

[1] https://www.youtube.com/playlist?list=PLzIU1iYy4sJjPSz7HjvMLYme7z4D1E4KW



```
| perceiverID = 0                                 |
| stationType = 5                                 |
| timeOfMeasurement = 400                         |
| longitude = 320.284 | latitude = 224.893        |
|-------------------------------------------------|
|-------------------------------------------------|
| stationID  = 1111                               |
| perceiverID = 0                                 |
| stationType = 5                                 |
| timeOfMeasurement = 400                         |
| longitude = 461.937 | latitude = 414.526        |
|-------------------------------------------------|
|-------------------------------------------------|
| stationID  = 0                                  |
| perceiverID = 1                                 |
| stationType = 5                                 |
| timeOfMeasurement = 420                         |
| longitude = 411.211 | latitude = 313.261        |
|-------------------------------------------------|
Node[2] perceive objects...
test Node[0]...
distance = 215.781
Node[0] can not be perceived
test Node[1]...
distance = 348.341
Node[1] can not be perceived

 ======Detect Ghost Vehicle!======
MR source : Node[2]
|-------------------------------------------------|
| stationID  = 1111                               |
| perceiverID = 0                                 |
| stationType = 5                                 |
| timeOfMeasurement = 400                         |
| longitude = 461.937 | latitude = 414.526        |
|-------------------------------------------------|

 =================================
```

Figure 10: Constant GV and MR Generation.

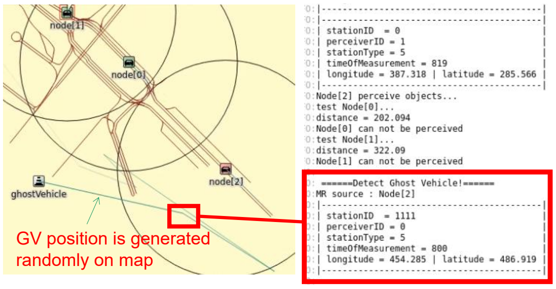


```
|-------------------------------------------------|
| stationID  = 1111                               |
| perceiverID = 0                                 |
| stationType = 5                                 |
| timeOfMeasurement = 400                         |
| longitude = 311.937 | latitude = 264.526        |
|-------------------------------------------------|
|-------------------------------------------------|
| stationID  = 0                                  |
| perceiverID = 1                                 |
| stationType = 5                                 |
| timeOfMeasurement = 420                         |
| longitude = 411.211 | latitude = 313.261        |
|-------------------------------------------------|
Node[1] perceive objects...
test Node[0]...
distance = 132.301
Node[0] can be perceived
test Node[2]...
distance = 348.38
Node[2] can not be perceived

 ======Detect Ghost Vehicle!======
MR source : Node[1]
|-------------------------------------------------|
| stationID  = 1111                               |
| perceiverID = 0                                 |
| stationType = 5                                 |
| timeOfMeasurement = 400                         |
| longitude = 311.937 | latitude = 264.526        |
|-------------------------------------------------|

 =================================
```

Figure 11: Constant Offset GV and MR Generation.

and its MR generation, please refer to the video link given at the bottom.

-Random GV Detection. For random GV, its position will be generated randomly on the map through node0's outgoing CPM. As can be observed in Fig. 12, the GV's position has already changed several times. The MR generation of node2 in the figure occurred when the GV was in node2's perception range (the small red rectangle in the figure). On the other hand, none of the vehicles can ensure the GV detection when GV is out of all vehicles' perception ranges, which is exactly the case in the left part of Fig. 12.

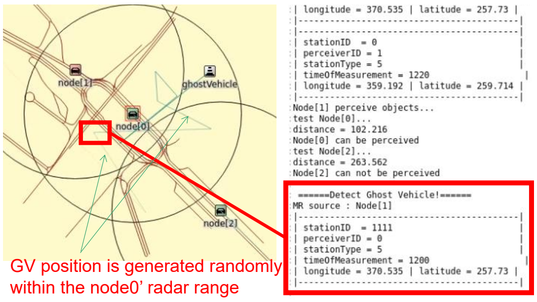


GV position is generated randomly on map

```
|-------------------------------------------------|
|-------------------------------------------------|
| stationID  = 0                                  |
| perceiverID = 1                                 |
| stationType = 5                                 |
| timeOfMeasurement = 819                         |
| longitude = 387.318 | latitude = 285.566        |
|-------------------------------------------------|
Node[2] perceive objects...
test Node[0]...
distance = 202.094
Node[0] can not be perceived
test Node[1]...
distance = 322.09
Node[1] can not be perceived
 ======Detect Ghost Vehicle!======
MR source : Node[2]
|-------------------------------------------------|
| stationID  = 1111                               |
| perceiverID = 0                                 |
| stationType = 5                                 |
| timeOfMeasurement = 800                         |
| longitude = 454.285 | latitude = 486.919        |
|-------------------------------------------------|
```

Figure 12: Random GV and MR Generation.

-Random Offset GV Detection. Similar to random GV, Random Offset GV's position changes randomly but always in the attacker's perception range, i.e., node0's range. In some cases, the GV is too far away from the attacker and it becomes evident that the PO's information is faked in CPM as the CPM generator (attacker) cannot detect this PO out of its perception range. Fig. 13 demonstrates that GV's position changes randomly within node0's perception range. When it was in node1's perception range (the small red rectangle in the figure), one MR was generated by node1 to broadcast the identified GV in its received CPM.



GV position is generated randomly within the node0' radar range

```
| longitude = 370.535 | latitude = 257.73 |
|-------------------------------------------------|
|-------------------------------------------------|
| stationID  = 0                                  |
| perceiverID = 1                                 |
| stationType = 5                                 |
| timeOfMeasurement = 1220                        |
| longitude = 359.192 | latitude = 259.714        |
|-------------------------------------------------|
Node[1] perceive objects...
test Node[0]...
distance = 102.216
Node[0] can be perceived
test Node[2]...
distance = 263.562
Node[2] can not be perceived
 ======Detect Ghost Vehicle!======
MR source : Node[1]
|-------------------------------------------------|
| stationID  = 1111                               |
| perceiverID = 0                                 |
| stationType = 5                                 |
| timeOfMeasurement = 1200                        |
| longitude = 370.535 | latitude = 257.73 |
|-------------------------------------------------|
```

Figure 13: Random Offset GV and MR Generation.

-Detection Rate of CPM-Based GV. Trust in CPM differs from Trust in CAM, the latter is on the basis of a probabilistic value in the range of [0 1] to describe the trustworthiness of the CAM source, and the former is a policy-driven trust scheme, i.e., a binary question. For this reason, the detection accuracy of CPM-based GV should be discussed regarding four GV types.

Table 3: MR generation under four CPM-based GV attacks.

NO.	Constant	Constant Offset	Random	Random Offset
1	33	39	10	28
2	33	39	13	25
3	33	39	12	22
4	33	39	12	25
5	33	39	7	26
6	33	39	12	30
7	33	39	10	27
8	33	39	18	31
9	33	39	16	25
10	33	39	13	26

We ran 10 times 30-second simulations to test the detection rate, in which the attacker vehicle sent 1 CPM of GV per second, and thus 30 CPM of GV in total. The results are illustrated in Table 3. It should also be noted that the GV may appear at a position where none of v1 and v2 can detect it, especially the Random GV one. Given this, while both v1 and v2 can generate MR if the GV is detected, the number of MR close to 30 is more or less satisfactory. This table shows that Constant, Constant Offset, and Random Offset detection rates are somehow acceptable,

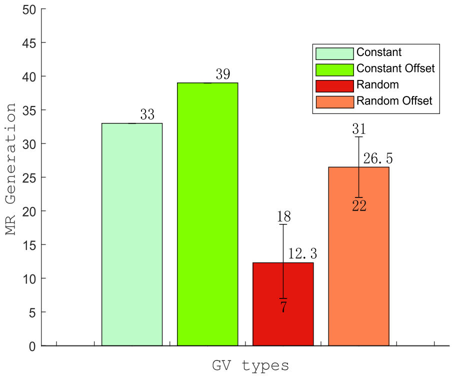


Figure 14: Comparison of detection rate of four CPM-based GV types.

except for the Random GV, which remains at a relatively low detection accuracy. Besides, as can be seen in Fig. 14, it can be noticed that there are no error bars for the former two types of CPM-based, namely Constant and Constant Offset. On the other hand, the gaps in MR generation numbers of each simulation remain considerably different for the latter two types, namely Random and Random Offset CPM-based GV types. This is because simply the 'Random' GV's position changes over time, and the probability that they stay out of detector vehicles' perception range becomes larger. Furthermore, this figure also shows the 'Offset' GV, either Constant Offset or Random Offset, remains more detectable than their original GV versions (Constant and Random). As the 'Offset' GV moves in a manner that follows one of the evaluator vehicles, it will be more likely to be in the detection range. The detection accuracy results are obtained by simulation of only two detector vehicles (honest CPS vehicles), and in this sense, we believe that as the number of CPS detectors increases, the detection success rate will grow significantly.

4 CONCLUSIVE REMARKS

As CPS is rarely considered in existing works and there was no implementation of CPM in the popular Veins simulator, in this work, we integrated CPS in Veins, enabling inter-vehicle CPM communications. Furthermore, we proposed a trust framework addressing two CAM-based GV attacks, namely OOA and NCA, and four CPM-based GV attacks, namely Constant, Constant Offset, Random, and Random Offset. A three-vehicle scenario simulation has been conducted to provide a preliminary analysis of the feasibility of the proposed model and show the effectiveness in terms of assessing V2X messages' trustworthiness.

With this proposed trust model integrating the CPS component in hand, our future work will be simulating larger-scale IoV scenarios involving more entities. On the other hand, more complicated strategic misbehavior models can also be considered in our future work to analyze the resilience of the countermeasures proposed.

REFERENCES

Ambrosin, M., Yang, L. L., Liu, X., Sastry, M. R., and Alvarez, I. J. (2019). Design of a misbehavior detection system for objects based shared perception v2x applications. In *2019 IEEE ITSC*, pages 1165–1172.

ETSI (2019). 302 637-2 v1.4.1 -intelligent transport systems; vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service. *ETSI, Apr.*

ETSI (2020). 103 415 v1. 1.1 -intelligent transport systems; security; pre-standardization study on misbehaviour detection; release 2. *ETSI, Oct.*

ETSI (2023). 103 324 v2.1.1 -intelligent transport system; vehicular communications; basic set of applications; collective perception service; release 2. *ETSI, Jun.*

Farran, H. and Khoury, D. (2023). Performance improvements of vehicular pki protocol for the security of v2x communications. In *2023 46th TSP*, pages 177–182.

Gai, F., Zhang, J., Zhu, P., and Jiang, X. (2017). Trust on the ratee: a trust management system for social internet of vehicles. *WCMC*.

Gyawali, S. and Qian, Y. (2019). Misbehavior detection using machine learning in vehicular communication networks. In *2019-2019 IEEE ICC*, pages 1–6.

Hasrouny, H., Samhat, A. E., Bassil, C., and Laouiti, A. (2019). Trust model for secure group leader-based communications in vanet. *Wireless Networks*, 25:4639–4661.

Kerrache, C. A., Lagraa, N., Calafate, C. T., Cano, J.-C., and Manzoni, P. (2016). T-vnets: A novel trust architecture for vehicular networks using the standardized messaging services of etsi its. *Computer Communications*, 93:68–83.

Li, W. and Song, H. (2015). Art: An attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE transactions on ITS*, 17(4):960–969.

Su, R., Sfar, A. R., Natalizio, E., Moyal, P., and Song, Y.-Q. (2022). Ensuring trustworthiness in ioit/aiot: A phase-based approach. *IEEE IoT Magazine*, 5(2):84–88.

Tsukada, M., Arii, S., Ochiai, H., and Esaki, H. (2022). Misbehavior detection using collective perception under privacy considerations. In *2022 19th CCNC*, pages 808–814. IEEE.

Van Der Heijden, R. W., Lukaseder, T., and Kargl, F. (2018). Veremi: A dataset for comparable evaluation of misbehavior detection in vanets. In *14th SecureComm 2018, Proceedings, Part I*, pages 318–337. Springer.

Veins. Veins. https://veins.car2x.org/. Accessed: 12.24.2023.