# A lightweight cooperative trust model for IoV

Runbo Su, Yujun Jin, Ye-Qiong Song

# A lightweight cooperative trust model for IoV

Runbo Su, Yujun Jin, Ye-Qiong Song
LORIA, CNRS, Université de Lorraine, France
{runbo.su, yu-jun.jin, ye-qiong.song}@loria.fr

***Abstract*—Securing V2X (Vehicle-to-Everything) communication is essential for IoV (Internet of Vehicles) as it improves road safety. As a complement to cryptographic solutions, trust models are advantageous against insider attackers in IoV. However, only a few works consider the Misbehavior Detection (MD) and Misbehavior Report (MR) of V2X messages, and the employment of On-Board Sensor (OBS) data is also missing. With this context, this poster presents a lightweight cooperative trust model taking both OBS data and V2X messages into account to eliminate malicious messages and misbehaving vehicles.**

***Index Terms*—Trust, Cooperative IoV, V2X communication, On-Board Unit (OBU), Misbehavior Detection, Security.**

## I. Introduction and Motivation

V2X communication plays an important role in IoV for cooperative sensing and maneuvering, and thus its security becomes critical. The European Telecommunication Standardization Institute (ETSI) has standardized several V2X messages, such as CAM (Cooperative Awareness Message), CPM (Collective Perception Message), and DENM (Decentralized Environmental Notification Message). To protect the highly sensitive information in these messages, cryptographic solutions are introduced. However, such solutions cannot perform as expected in the absence of dedicated infrastructures and remain challenging when detecting insider attackers, in other words, the correctness of V2X messages and the honesty of vehicles should be both assessed [1]. For this, some works apply trust models to secure IoV: To estimate the trustworthiness between vehicles, the work in [2] proposed combining evidence collected, and the work in [3] introduced social attributes of vehicles. However, they both did not adopt V2X messages for communication. A model using received V2X messages to estimate trust in IoV was presented in [4]. Despite the feasibility of this framework, MD involving collective perception service and OBS data is not supported. A recent work [5] combining sensing data and CPM for MD of CAM provided an interesting scheme to check V2X messages cooperatively, but trust issues in IoV are not discussed in this work. From the above review, we can notice that the V2X messages generation scheme and cooperative MD employing OBS data are rarely addressed, and some works focus on either message or vehicle aspects lacking MR measures. To overcome these limitations, this poster presents a lightweight cooperative trust model using OBS data and received V2X messages to assess both the communication and the behavior of vehicles. To validate the proposed model, a three-vehicle scenario simulation has been conducted by integrating the trust management in Veins [6].

## II. Proposed 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 and OBS. In IoV, **V2X OBU** supports the communication between IoV entities: Vehicles or other entities periodically

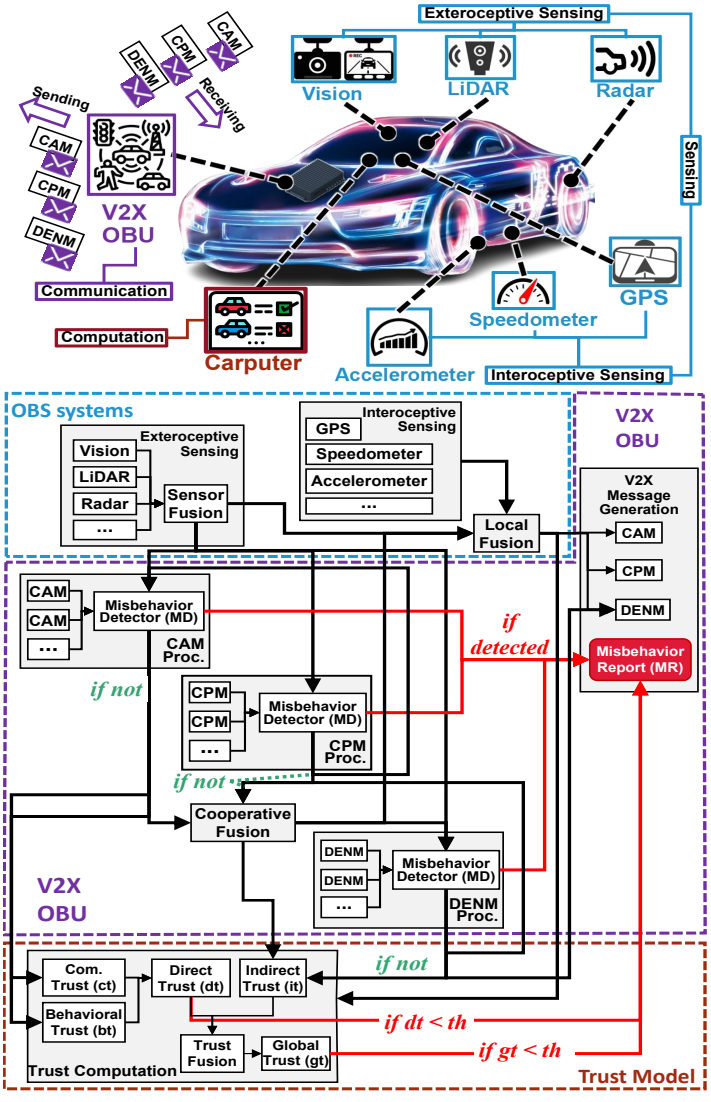


Fig. 1: IoV on-board equipment and the functional flows showing how the trust model interacts with OBS and V2X OBU.

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; DENM's dissemination will be activated if any safety-related events are detected. **OBS** in IoV consists of exteroceptive and interoceptive sides, where the former senses the surroundings and the latter monitors the vehicle's dynamics. And lastly, the **Carputer** refers to computing hardware in the vehicle. Until the end of this section, we describe the V2X messages verified by MD without MR as '**inspected honest**'.

**MD, processing, and generation of V2X messages:** We designed an extended cooperative MD scheme for all the three V2X messages: the vehicle's sensing data will be counted for the MD of all incoming messages; Inspected honest CPM will be utilized for the MD of CAM; Data fused by inspected honest CAM, CPM, and DENM will be employed for the MD of DENM. Once misbehavior is detected in any messages, a MR will be generated and sent to Misbehavior Authority (MA) as defined in [7], and thus fraudulent V2X messages will be rejected and marked. MR sources are highlighted by red arrows in Fig. 1. Besides, inspected honest incoming V2X messages will be fused with the vehicle's sensing data to generate outgoing V2X messages for other vehicles.

**Trust computation:** As shown in the brown block of Fig. 1, inspected honest CAM and sensing data will be used to compute communication trust ($ct$) and behavioral trust ($bt$), and based on these two values, the direct trust ($dt$) can be calculated. $ct$ examines the stability of V2X communication, such as the communication frequency. $bt$ estimates the physical threat level by measuring vehicles' dynamics. For indirect trust ($it$), fused inspected honest CAM, CPM, and DENM will be considered in computation, such as the relevance of the event detected in DENM. And lastly, a global trust ($gt$) value will give an overall opinion concerning the trustworthiness on the basis of both $dt$ and $it$. When $dt$ or $gt$ is inferior to the threshold with a sufficient V2X communication, the evaluated vehicle's trustworthiness is considered not to meet the minimum security requirement, and then MR generation will be triggered. In such a manner, misbehaving vehicles will be identified and reported.

## III. Preliminary Results and Future Work

Fig. 2 shows the scenario simulated by using Veins: vehicle 2 (v2) is overtaking vehicle 0 (v0), and vehicle 1 (v1) is at a short distance in front of them. v0 disseminates DENM informing v2's coming, all nodes broadcast CAM periodically, and CPM will be transmitted if other vehicles are detected. By varying v2's behavioral types, we visualize the changes in v2's trust values evaluated by v0: **a)** known and cooperate, i.e., v2's identity has been recorded by v0 and thus known in IoV, and it cooperates for V2X communication; **b)** unknown but cooperate, i.e., v2 may hide its true identity to reconnect as a newcomer; and **c)** known but misbehave by intentionally doubling its original communication frequency, where the latter two types are described as potential newcomer and on-off attackers in [8]. We can observe that the former two types

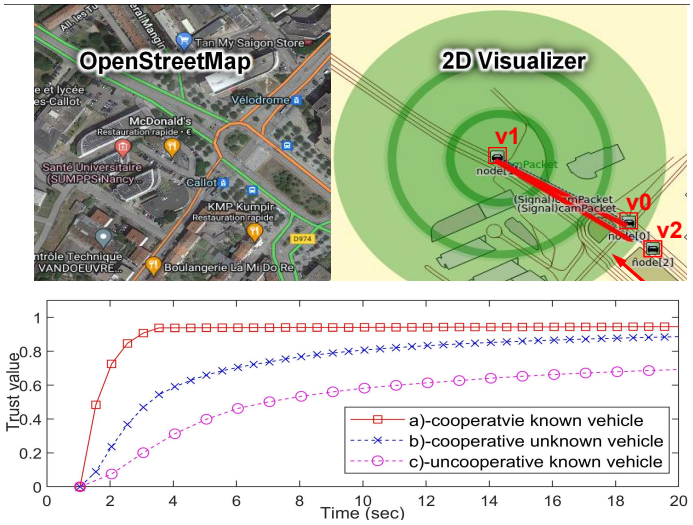


Fig. 2: Scenario with OpenStreetMap and 2D visualizer, and the changes in trust value by varying v2's behavioral types.

(a and b), performing cooperation, reach a higher trust level, while the unknown one (b) increases slowly. The misbehaving of the uncooperative vehicle (c) is reflected in a lower trust level despite its known identity in the IoV. Consequently, a MR will be transmitted to MA. We note that the threshold can be dynamic depending on real-time traffic conditions instead of a predefined value [9]. The preliminary results show the effectiveness of our proposal through a three-vehicle scenario simulation considering two misbehavior kinds.

Since real-world traffic and related threats remain complex, the simulation scenarios and attack models will be explored and further discussed in our future work.

## References


[1] T. Yoshizawa *et al.*, "A survey of security and privacy issues in v2x communication systems," *ACM Computing Surveys*, vol. 55, no. 9, pp. 1–36, 2023.

[2] W. Li and H. Song, "Art: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE trans. ITS*, vol. 17, no. 4, pp. 960–969, 2015.

[3] F. Gai, J. Zhang, P. Zhu, and X. Jiang, "Trust on the ratee: A trust management system for social internet of vehicles," *Wireless Communications and Mobile Computing*, 2017.

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

[5] M. Tsukada, S. Arii, H. Ochiai, and H. Esaki, "Misbehavior detection using collective perception under privacy considerations," in *2022 19th CCNC*, IEEE, 2022, pp. 808–814.

[6] *Veins*, https://veins.car2x.org/, Accessed: 04.27.2023.

[7] "Intelligent transport systems (its); security; pre-standardization study on misbehaviour detection; release 2," *ETSI TR 103 415 V1. 1.1 (2020-10)*, 2020.

[8] R. Su, A. R. Sfar, E. Natalizio, P. Moyal, and Y.-Q. Song, "Ensuring trustworthiness in ioit/aiot: A phase-based approach," *IEEE IoT Magazine*, vol. 5, no. 2, pp. 84–88, 2022.

[9] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Trust model for secure group leader-based communications in vanet," *Wireless Networks*, vol. 25, pp. 4639–4661, 2019.