



HAL
open science

Assessing trustworthiness of V2X messages: a cooperative trust model against CAMand CPM-based Ghost Vehicles in IoV

Runbo Su, Yujun Jin, Ye-Qiong Song

► To cite this version:

Runbo Su, Yujun Jin, Ye-Qiong Song. Assessing trustworthiness of V2X messages: a cooperative trust model against CAMand CPM-based Ghost Vehicles in IoV. 10th Vehits (International conference on vehicle technology and intelligent transport systems), May 2024, Angers, France. hal-04620893

HAL Id: hal-04620893

<https://hal.science/hal-04620893v1>

Submitted on 22 Jun 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Assessing trustworthiness of V2X messages: a cooperative trust model against CAM- and CPM-based Ghost Vehicles in IoV

Runbo Su, Yujun Jin and Ye-Qiong Song

{runbo.su, yu-jun.jin, ye-qiong.song}@loria.fr, LORIA, CNRS, Université de Lorraine, France



Background and proposed model

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). However, containing safety-related information makes V2X messages susceptible to malicious insider attacks from compromised vehicles after the PKI authentication step [2], such as Ghost Vehicles (GV) [3], passively or actively reaching a 'ghost' state in terms of communication, position, etc.

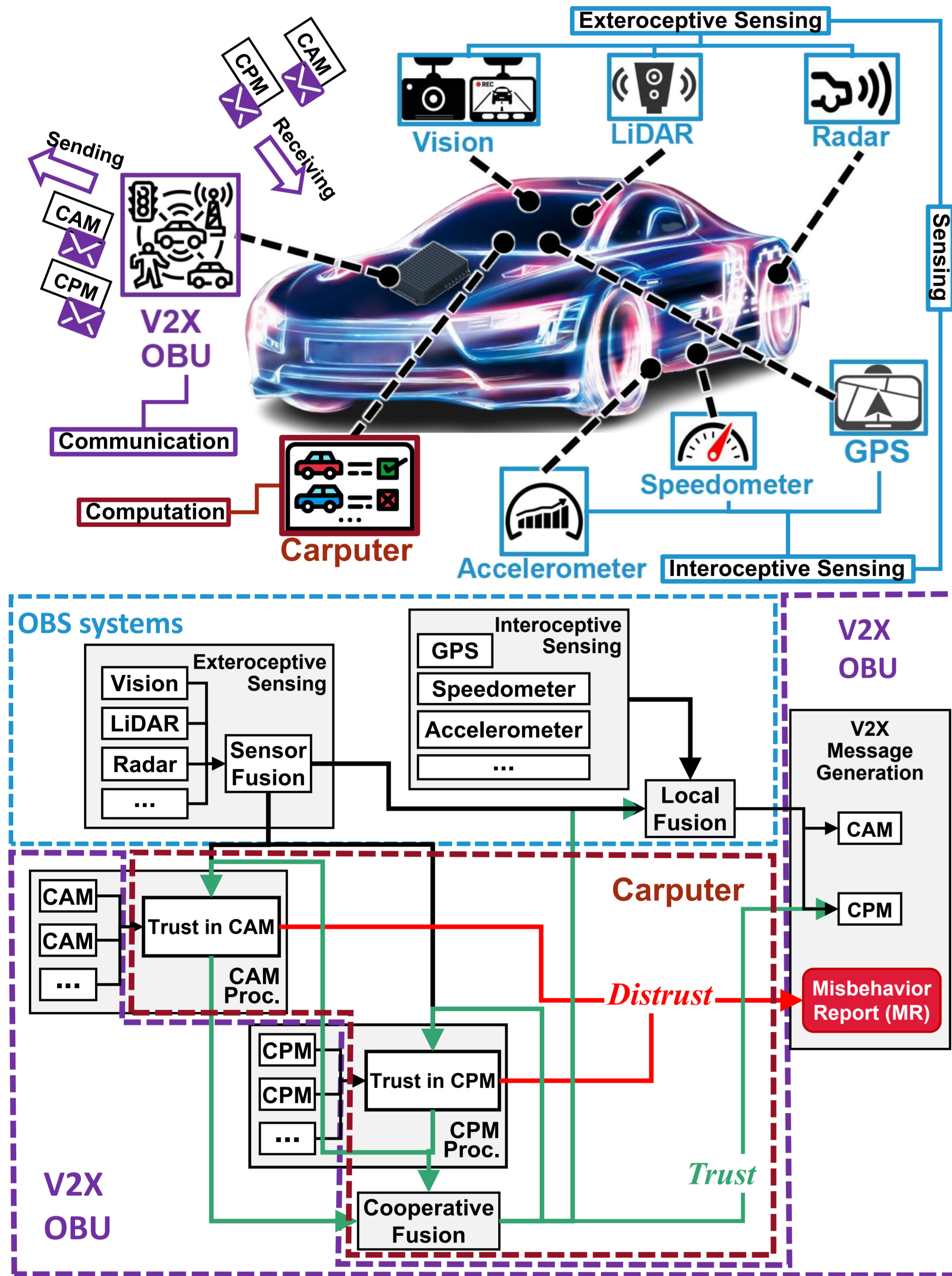


Figure 1. IoV on-board equipment and the functional flows showing how the trust model interacts with OBS (On-Board Sensor) and V2X OBU (On-Board Unit).

Considered Traffic Scenario in Simulation

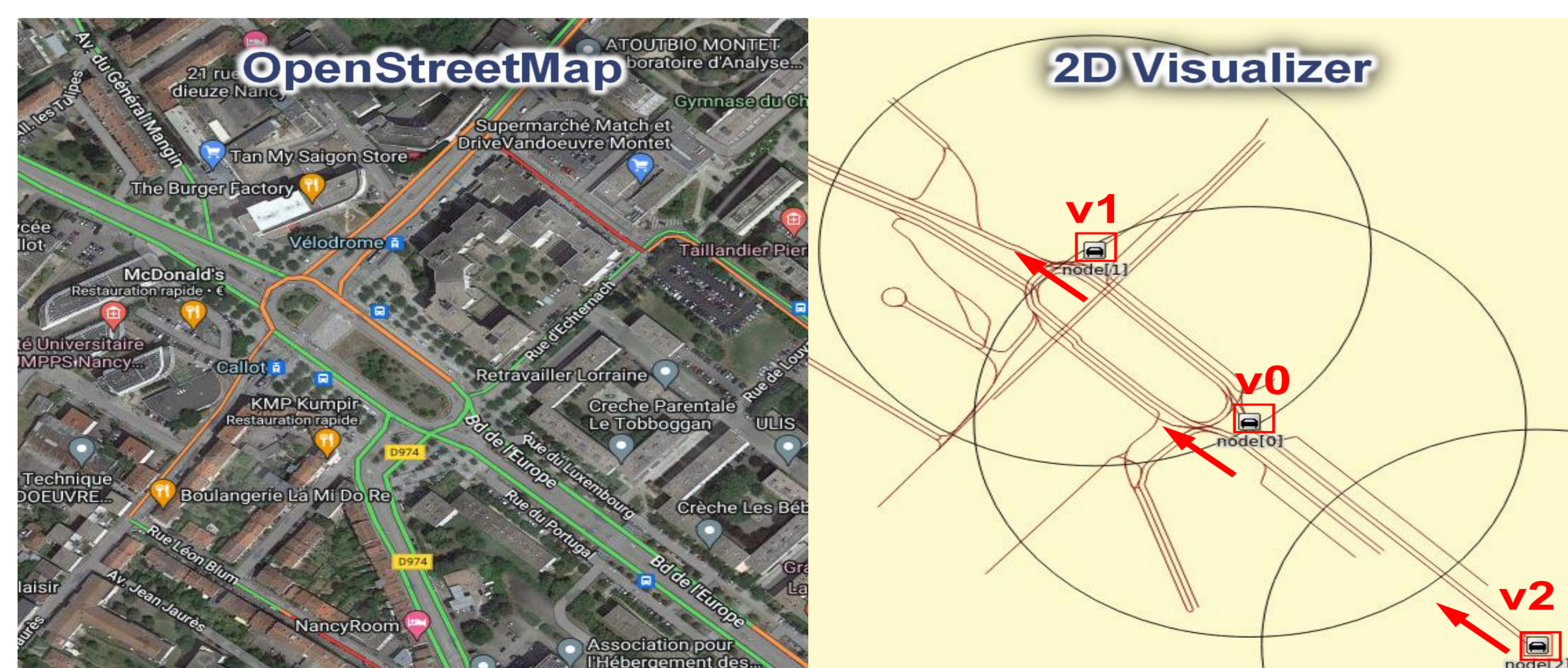


Figure 2. Considered Traffic Scenario

GV attacks

-CAM-based GV Attack Model [4]:

- OOA (On-Off): Attacker switches between good and bad to mislead the trust evaluation, by intentionally doubling its original communication frequency.
- NCA (NewComer): The attacker vehicle fabricates a new identity to convey CAM with the purpose of refreshing its trust.

-CPM-based GV Attack Model [5]:

Table 1. CPM-based GV Attack Parameters

GV Type	Parameters/Description
Constant	$x = 461.937, y = 414.526$
Constant Offset	$\Delta x = -100, \Delta y = -50$
Random	Uniformly random in playground
Random Offset	d uniformly random from $[0, 150]$ θ uniformly random from $[0, 2\pi]$ $\Delta x = d * \cos\theta, \Delta y = d * \sin\theta$

Trust in CAM

We set T^i representing the trust of evaluated CAM sender vehicle i :

$$p_1^i = (1 - \rho) \sum \rho^{t - t_n^i}$$

$$p_2^i = \rho^{\lambda/n}$$

$$T^i = (p_1^i * p_2^i)^{1/2}$$

Figure 3. Composition of Trust in CAM

t is the current time and t_n^i is the timestamp of n^{th} CAM from i , $\rho \in [0, 1[$ is the decay factor, and λ in p_2 is a scale factor. To summarize, p_1 calculates the freshness of the received CAM message, and p_2 determines the level of acquaintance of the CAM sender vehicle.

Trust in CPM

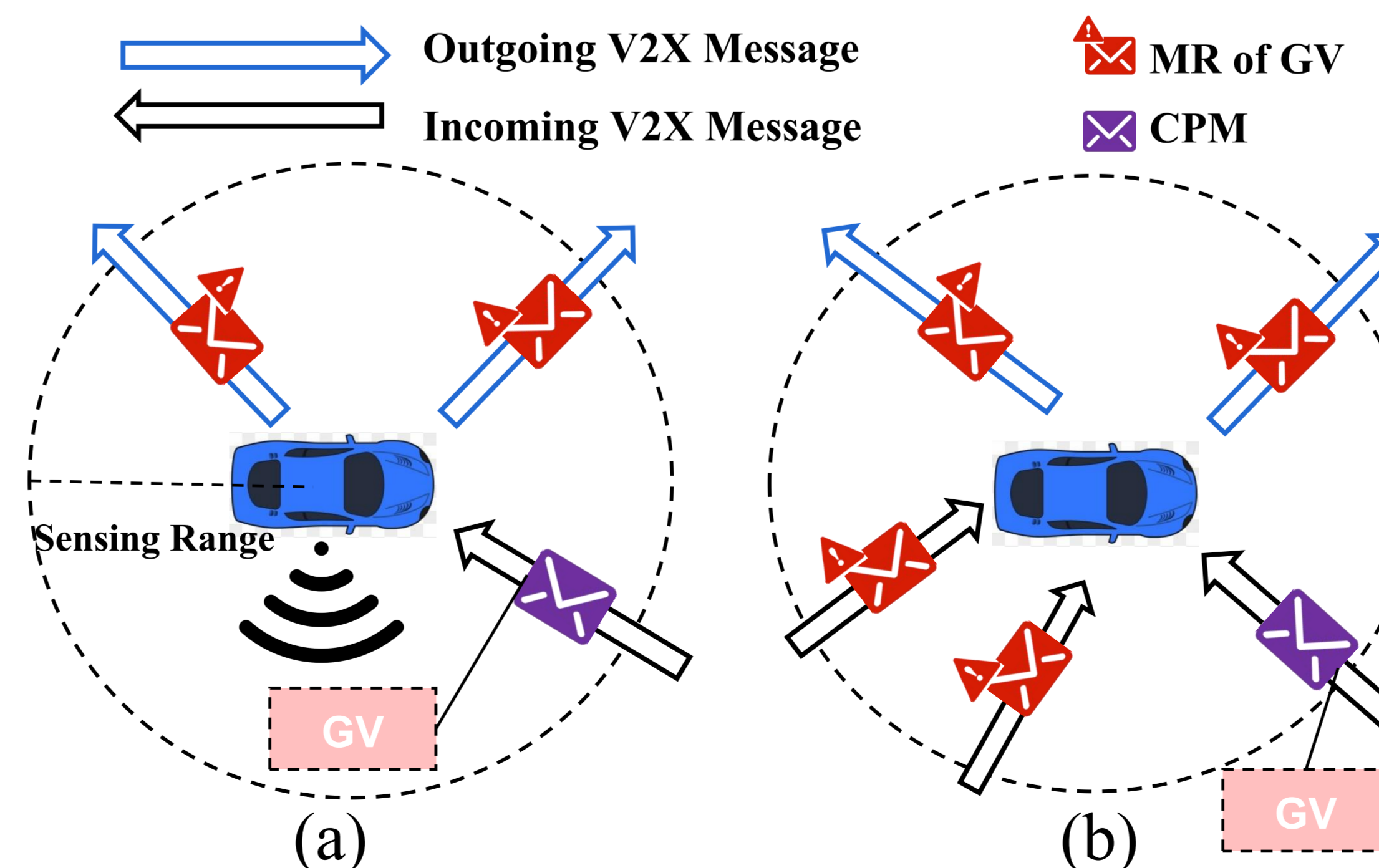


Figure 4. Two GV detection cases: in (a) or out (b) of the evaluator vehicle's perception range

Simulation results by using Veins Simulator [1]

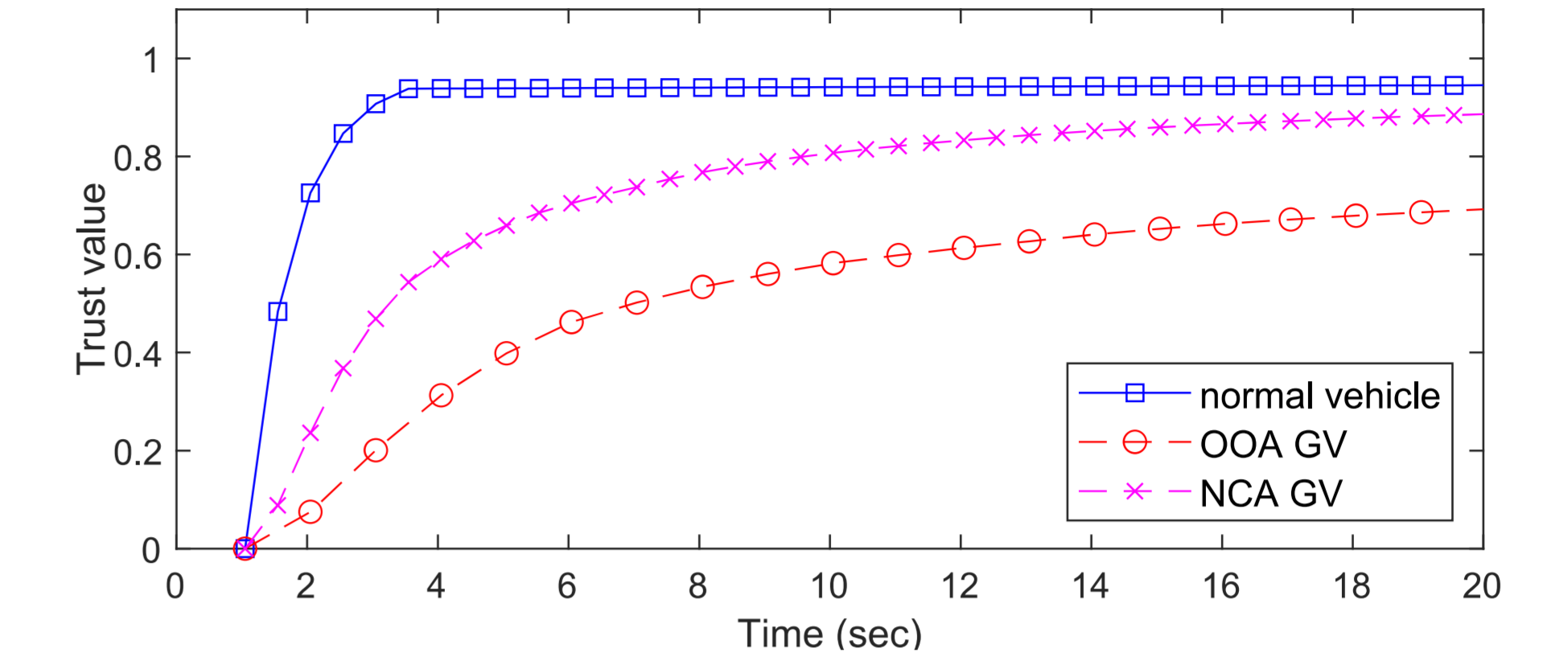


Figure 5. Changes in vehicles' trust values in the presence of OOA and NCA

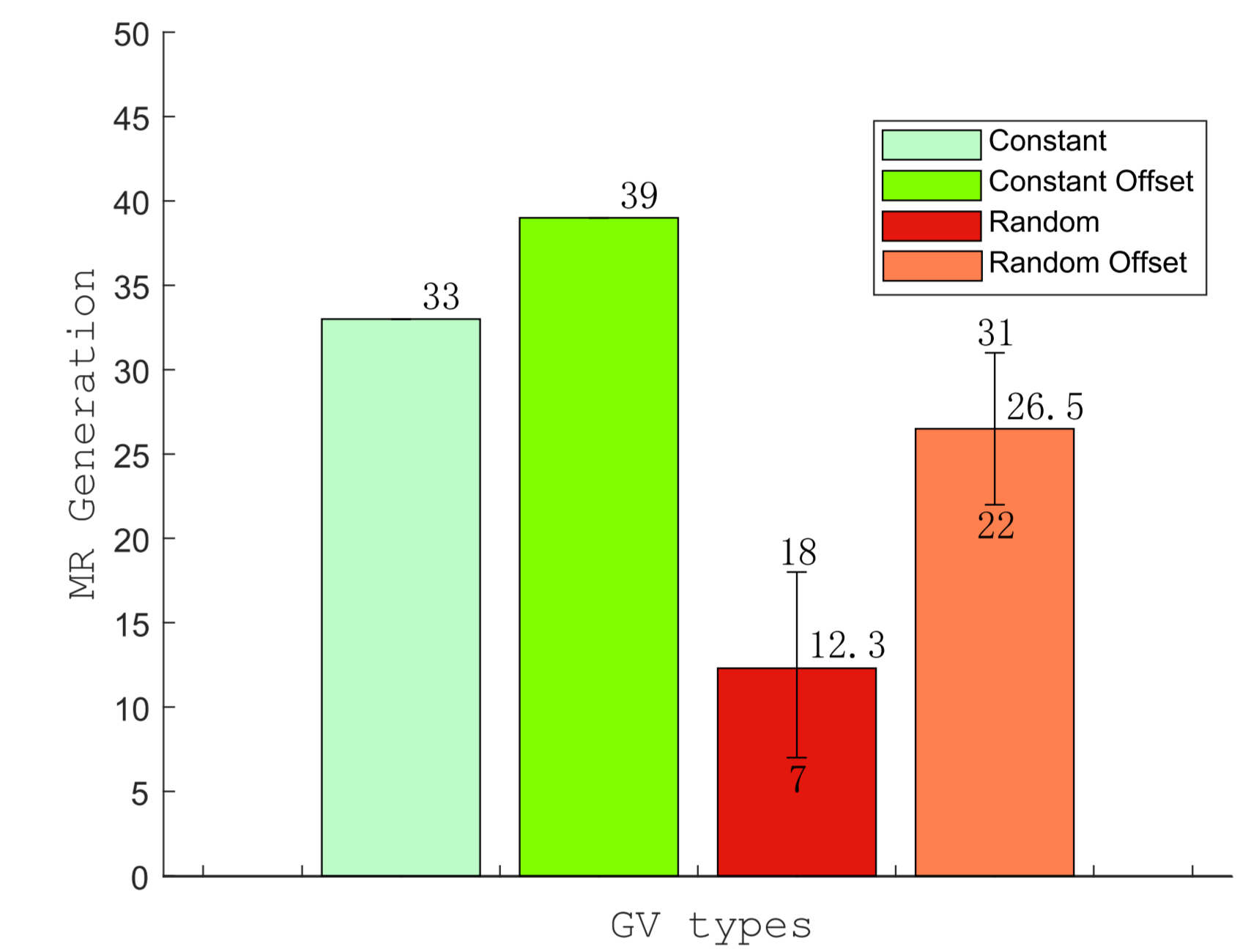


Figure 6. Comparison of detection rate of four CPM-based GV types

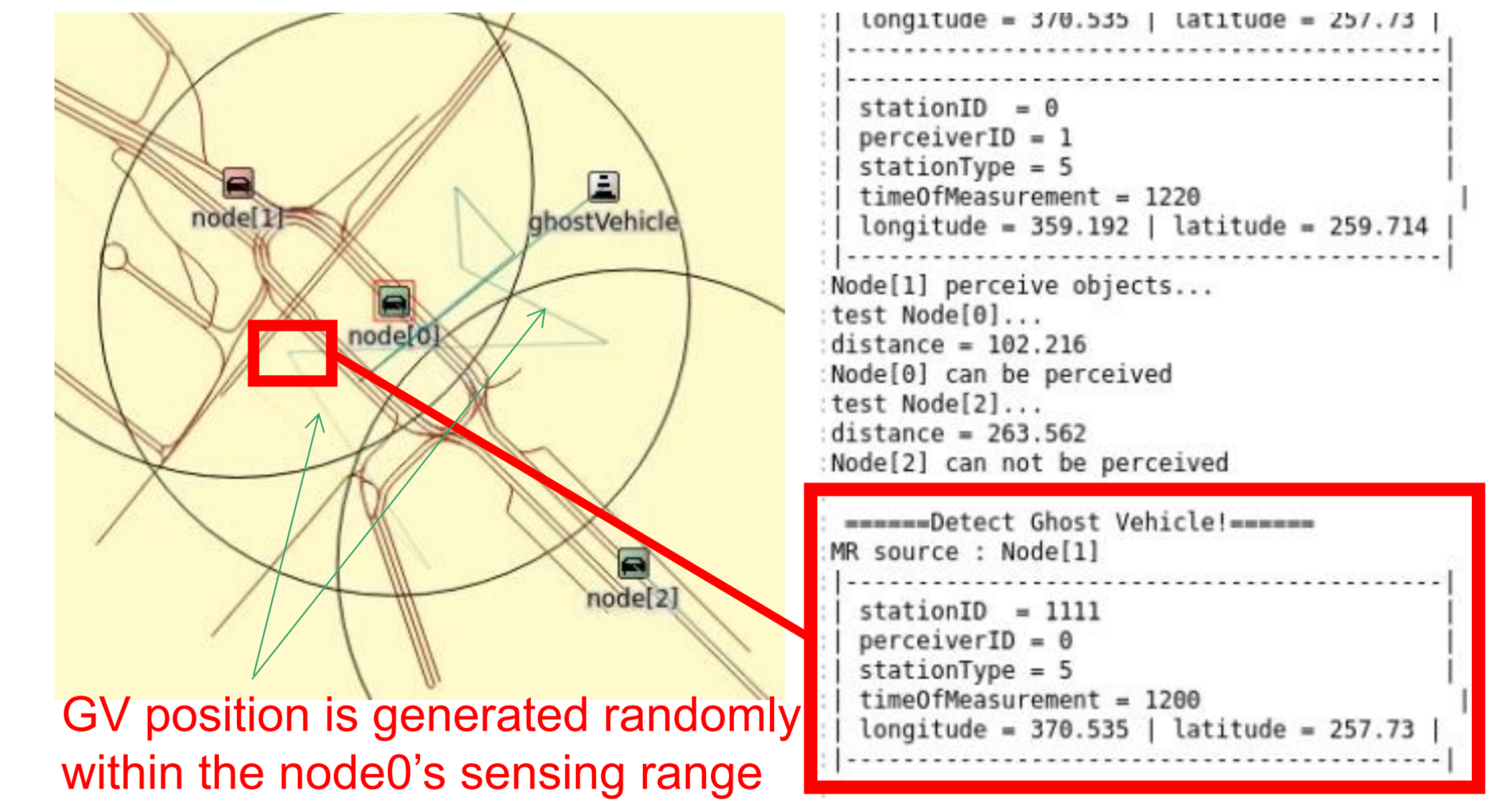


Figure 7. Random Offset GV and MR Generation

References

- [1] Veins Accessed: 03.13.2024. <https://veins.car2x.org/>.
- [2] Hassan Farran and David Khoury. Performance improvements of vehicular pki protocol for the security of v2x communications. In 2023 46th TSP, pages 177-182, 2023.
- [3] Sohan Gyawali and Yi Qian. Misbehavior detection using machine learning in vehicular communication networks. In 2019-2019 IEEE ICC, pages 1-6, 2019.
- [4] Runbo Su, Arbia Riahi Sfar, Enrico Natalizio, Pascal Moyal, and Ye-Qiong Song. Ensuring trustworthiness in iot/aiot: A phase-based approach. IEEE IoT Magazine, 5(2):84-88, 2022.
- [5] Rens W Van Der Heijden, Thomas Lukaseder, and Frank Kargl. Veremi: A dataset for comparable evaluation of misbehavior detection in vanets. In 14th SecureComm 2018, Proceedings, Part I, pages 318-337. Springer, 2018.