Reliable Vehicle-to-Vehicle Information Sharing in Smart Cities

Vincenzo Agate*, Giuseppe Lo Re*, Marco Morana* and Antonio Virga*
*Department of Engineering, University of Palermo, Palermo, Italy.
Email: vincenzo.agate@unipa.it, giuseppe.lore@unipa.it, marco.morana@unipa.it, antonio.virga01@unipa.it

***Abstract*—The proliferation of Vehicle-to-Everything (V2X) technologies is reshaping vehicular communication, enabling decentralized and real-time data exchange to enhance safety and traffic efficiency. However, the lack of centralized control in Vehicular Ad Hoc Networks (VANETs) exposes them to risks such as the spread of fake or malicious information. This work presents a lightweight, fully distributed architecture for reliable event dissemination that operates without roadside infrastructure. Vehicles directly perceive events occurring in their immediate surroundings through onboard sensors, while they acquire knowledge of events occurring elsewhere via communication with neighboring vehicles. Each vehicle autonomously evaluates the trustworthiness of both received messages and their sources by combining its own sensory perception with information shared through localized interactions. A dynamic reputation mechanism enables timely adaptation to changing network conditions and enhances resilience against adversarial behavior.**

***Index Terms*—VANETs, Reputation Management, Event Dissemination, Trust Evaluation, Urban Mobility, Intelligent Transportation Systems**

I. Long Abstract

Recent analyses estimate that approximately 60% of the global population currently resides in urban environments, with projections indicating an increase to 70% by the year 2050. This accelerated urbanization trajectory poses substantial challenges for future metropolitan areas, particularly concerning transportation infrastructure, traffic safety, and the pursuit of sustainable mobility solutions [1]. In this regard, Intelligent Transportation Systems (ITS) alongside advanced vehicular communication paradigms are widely regarded as pivotal enablers for the evolution of next-generation urban mobility. Among these technologies, Vehicle-to-Everything (V2X) communication and Vehicular Ad Hoc Networks (VANETs) [2] exhibit considerable promise in supporting cooperative services, including but not limited to traffic situational awareness, congestion alleviation, and collision avoidance [3].

Despite these opportunities, the full deployment of VANETs remains a complex task due to the dynamic and infrastructureless nature of vehicle-to-vehicle (V2V) communications. While vehicle-to-infrastructure (V2I) models offer reliability through fixed entities like Road Side Units (RSUs), their widespread implementation is often hampered by high deployment costs and practical limitations [4]. On the other hand, V2V communications offer greater flexibility and scalability but raise concerns regarding the reliability and integrity of the exchanged information, especially in the absence of a trusted central authority. High-speed mobility, varying network densities, and the presence of malicious actors pose additional challenges to the trustworthy dissemination of data [5].

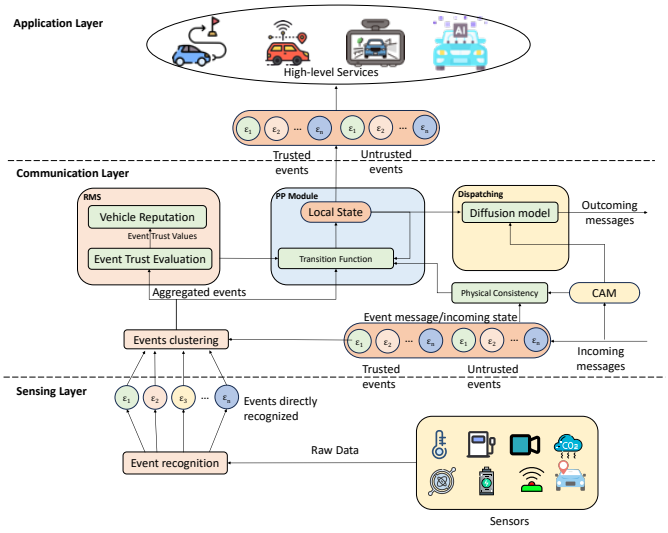

Fig. 1. Architecture of the proposed framework.

To address the issues of communication reliability in fully distributed environments, this work introduces a three-layered architecture where the central layer focuses on robust and trustworthy event dissemination based on a reputation mechanism [6]–[8]. An overview of the proposed architecture is presented in Figure 1. The system assumes that event information is obtained from the *sensing layer*, which processes onboard sensor data to detect relevant occurrences. Events are described by a tuple containing their type, time, location, and the identifier of the detecting vehicle. Events locally perceived by a vehicle through its sensing capabilities are considered reliable by default. In contrast, events received via the *communication layer*, through interactions with neighboring vehicles, are subject to a trust evaluation mechanism, which determines their eligibility for integration and further propagation within the network.

To handle data redundancy caused by overlapping event reports, the system adopts DBSCAN clustering to aggregate similar events based on spatial and temporal features. This approach significantly reduces processing overhead and enhances data consistency in dense traffic scenarios. Aggregated events then undergo trust evaluation and classification based

on a novel reputation management system (RMS).

The proposed reputation model includes three key components: trust scoring for events, estimation of vehicle reputation, and dynamic decay adjustment. Event trust is computed using feedback from other vehicles, but only opinions from trusted nodes are considered. The trust value reflects the balance of positive and negative reports, normalized over the number of distinct source vehicles.

Each vehicle maintains local reputations of others, updating them using an exponentially weighted moving average. A key innovation of the system is the dynamic decay factor, which reacts asymmetrically to trust fluctuations. Reputation drops rapidly in response to suspicious or incorrect data, while increases are more gradual. This asymmetry helps the system quickly identify and isolate malicious behavior, yet avoids penalizing honest nodes excessively for occasional errors.

To overcome the trust bootstrap problem for newly encountered events, their initial trust is set based on the reputation of the sender. This enables timely decision-making when historical data is lacking. The dissemination of information across the network is governed by a lightweight one-way population protocol [9], which ensures compatibility with the asymmetric and intermittent nature of vehicular communication.

The population protocol model supports local state synchronization among vehicles through unidirectional exchanges, and is used to integrate both self-perceived and received information into a vehicle's internal knowledge. A transition function processes this integration, updating the lists of trusted and untrusted events depending on thresholds and the sender's reputation. Only information from positively rated vehicles is considered, and previously trusted events can be invalidated based on new sensory input.

To limit unnecessary bandwidth usage and prevent message flooding, the system employs a dedicated dispatcher module that governs the selective transmission of event messages. Rather than broadcasting continuously, dissemination is triggered only under specific conditions: when a new event is detected by the local sensing layer; when the vehicle's internal knowledge is updated due to interactions governed by the population protocol; or when a previously unknown neighbor is encountered. These triggers ensure that information sharing remains relevant and responsive to the vehicle's context. In parallel, Cooperative Awareness Messages (CAMs), as defined by ETSI standards, are exchanged to maintain mutual awareness among nearby vehicles and to cross-validate data such as position, speed, and heading, thereby enhancing the reliability of received information.

Once events have been validated, either through direct sensing or following successful trust assessment via the communication layer, they are forwarded to the *application layer*. This enables the activation of high-level services aimed at enhancing driving support and traffic safety. For instance, validated accident reports can trigger early braking alerts or rerouting suggestions; similarly, trustworthy congestion information can be used for adaptive navigation, and the detection of hazardous road conditions (e.g., potholes or slippery surfaces) may activate driver assistance systems or contribute to shared warning broadcasts for following vehicles.

The system was tested through simulations based on realistic urban mobility traces. Different adversarial strategies, including stealth attacks and coordinated misinformation injection, were considered. Results demonstrate the effectiveness of the approach compared to state-of-the-art solutions. In particular, the dynamic reputation mechanism shows superior adaptability, maintaining high accuracy and resilience even when a significant portion of the network behaves maliciously.

Furthermore, the analysis of communication overhead reveals that the number of exchanged messages remains limited, thanks to the use of clustering and selective dispatching. The system scales efficiently with the number of vehicles, making it suitable for real-world deployment in complex and dynamic urban settings.

In conclusion, the proposed architecture represents a practical and scalable solution for improving the reliability of information dissemination in VANETs. It achieves this without relying on fixed infrastructure or global coordination, making it particularly well-suited for smart city scenarios. Future work will explore the integration of additional trust indicators, adaptation to heterogeneous environments, and privacy-preserving mechanisms [10] for reputation exchange.

REFERENCES

[1] Z. Cheng, J. Zhu, Z. Feng, M. Yang, W. Zhang, and J. Chen, "Driving Safety Risk Analysis and Assessment in a Mixed Driving Environment of Connected and Non-Connected Vehicles: A Systematic Survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 26, no. 5, pp. 5747–5781, 2025.

[2] A. Alnasser, H. Sun, and J. Jiang, "Recommendation-based trust model for vehicle-to-everything (V2X)," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 440–450, 2019.

[3] Z. Lin, K. Gao, P. Duan, N. Wu, and P. N. Suganthan, "Prediction and Feedback Assisted Evolutionary Algorithms for Scheduling Urban Traffic Signals," *IEEE Transactions on Intelligent Transportation Systems*, vol. 26, no. 5, pp. 6881–6890, 2025.

[4] Y. Wu, X. Fang, G. Min, H. Chen, and C. Luo, "Intelligent Offloading Balance for Vehicular Edge Computing and Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 26, no. 5, pp. 5792–5803, 2025.

[5] D. V. Sri and B. J. Lakshmi, "A review of security infrastructure, protocols, a taxonomy of security threats and intrusion detection in the Internet of Vehicles (IoV)," in *2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC)*, 2024, pp. 1–8.

[6] M. H. Junejo, A. A.-H. B. A. Rahman, R. A. Shaikh, K. M. Yusof, and S. Sadiah, "Trust Model for Reliable Grouping-Based Communications in Vehicular Ad-Hoc Networks," *IEEE Access*, vol. 11, pp. 124 584–124 596, 2023.

[7] H. Amari, Z. A. E. Houda, L. Khoukhi, and L. H. Belguith, "Trust Management in Vehicular Ad-Hoc Networks: Extensive Survey," *IEEE Access*, vol. 11, pp. 47 659–47 680, 2023.

[8] V. Agate, A. De Paola, G. Lo Re, and A. Virga, "Reputation-based dissemination of trustworthy information in vanets," in *Mobile and Ubiquitous Systems: Computing, Networking and Services*, A. Zaslavsky, Z. Ning, V. Kalogeraki, D. Georgakopoulos, and P. K. Chrysanthis, Eds. Cham: Springer Nature Switzerland, 2024, pp. 445–463.

[9] B. Su and L. Tong, "Transmission Protocol of Emergency Messages in VANET Based on the Trust Level of Nodes," *IEEE Access*, vol. 11, pp. 68 243–68 256, 2023.

[10] T. Yoshizawa, D. Singelée, J. T. Muehlberg, S. Delbruel, A. Taherkordi, D. Hughes, and B. Preneel, "A survey of security and privacy issues in v2x communication systems," *ACM Comput. Surv.*, vol. 55, no. 9, jan 2023. [Online]. Available: https://doi.org/10.1145/3558052