Traffic-Aware Agentic AI Framework for Semantic Validation of V2X Safety Messages

Ravi Babu Devareddi[1]*, Shiva Shankar Reddy*[2]

[1] Post Doctoral Researcher, Lincoln University College, Petaling Jaya, Selangor-47301, Malaysia.

[2] Department of Computer Science and Engineering, Lincoln University College, Petaling Jaya, Selangor-47301, Malaysia.

Email ID: pdf.ravibabu@lincoln.edu.my; pdfsv.shiva@lincoln.edu.my

Abstract: V2X communication is used to exchange safety information in real time manner in intelligent transport systems, but current methods of securing the V2X communication network are only concerned with ensuring the legitimacy of the message, without validating whether the alert itself is valid from a behavioral point of view. In order to resolve this problem, we proposed Score–Driven Adaptive Threshold Optimization for V2X Alert Validation approach to detect fake V2X alerts based on multi-vehicle behavior. An adaptive threshold calculation is conducted for evaluating the semantic consistency score with respect to varying traffic conditions and evidence. To mitigate the risk from any possible attack by a node, a trust-based evidential integration technique is included in the process for accurate decision making. An agentic feedback cycle is also implemented in this framework, allowing for dynamic adaptation of the threshold and the trust scores. Experimental analysis in low, moderate, and heavy traffic conditions shows that the framework achieves high detection accuracy, increased recall, F1-score balance, low false positives, and resilience to replay, spoofing, and Sybil attacks.

Keywords V2X, Agentic AI, Fake Alert Detection, Semantic Validation, Adaptive Threshold, Intelligent Transportation.

Introduction

Vehicle to Everything (V2X) technology [1] is reshaping our modern transport system in terms of exchange of real-time information through different types of vehicles and networks. As per the communications process, some of these ideas can be categorized into Vehicle to Vehicle calledV2V, Infrastructure to Vehicle named as I2V, Vehicle to Infrastructure named such as V2I, Communication with pedestrian called Vehicle to Pedestrian-V2P, Vehicle to Network namedV2N [2], [3]. It has become an essential feature of intelligent transportation systems nowadays since it allows real-time sharing of information that is crucial for road safety [4], [5] between vehicles, infrastructure, and cloud computing facilities. The combination of such a system can have enormous benefits, from improved road safety to improved traffic flow and development in autonomous driving [6]. Examples include accident warnings, collision avoidance, and traffic management that depend on V2X messages delivery in time [7], [8]. Still, because of its distributed and open architecture, V2X networks are extremely susceptible to the injection [9], [10], [11] of fake alerts that can cause serious consequences, such as traffic congestion, unnecessary braking, or even secondary collisions [12]. Typical view of V2X Communications in real time scenarios shown in Figure 1.

Figure 1 Typical view of V2X Communications in real time scenarios.

Recent studies also emphasize that developing robust ML-based misbehavior detection systems remains an open research challenge, particularly in the presence of intelligent and adaptive attackers are illustrated in Table 1.

Table 1: Literature Review

Ref.no.	Year	Model Name	Outcome	Disadvantages
[13]	2025	Transformer-Based V2XFormer Detection Approach.	Detects V2X anomalies using deep contextual learning with higher detection accuracy.	It does not validate semantic traffic behavior by braking behavior.
[14]	2025	ML-Based Anomaly Detection in V2V and V2X Networks.	Improved anomaly detection capability using machine learning and anomaly detection for V2X environments.	Focused mainly on Detects anomalies but cannot verify semantic truthfulness of alerts.
[15]	2025	Trustworthy Semantic Communication for Vehicular Networks.	Enhances reliability and trustworthiness of communication in vehicular networks.	Lacks adaptive threshold optimization and semantic traffic scoring.
[16]	2026	Semantic Event Validation for Connected Vehicles.	It is well performed for validation of events using vehicle behavior.	It is not considered adaptive threshold optimization mechanisms.
[17]	2026	Adaptive Federated Learning for Vehicular Intrusion Detection.	This model improved the Distributed intrusion detection by collaborative learning across vehicular systems.	It focused mainly on distributed IDS rather than traffic behavior analysis.

GAPS Identified

- Existing V2X work covers misbehavior detection, validity checks, and backend support, but a gap remains in cloud-assisted semantic validation of accident alerts using spatial and temporal qualities of multi-vehicle identification.
- There is no physical confirmation that the appropriate vehicles passed through that location to validate real-world traffic conditions.

Objectives

- Detection of fake accident alerts in V2X communication stack is used to avoid malfunctioning system problems like emergency braking and traffic disruption of self-driving vehicles.
- Validation of multiple vehicles crossed in that area like upcoming or down-coming directions to identify the physical presence of that vehicle.

Methodology

The proposed Semantic-Adaptive Threshold Optimization V2X (SATO-V2X) framework for reliable V2X safety alert validation methodology is designed to identify the fake or real alerts from V2X communities stack to all receiving ends in the network, addressing limitations such as lack of semantic validation. The modifications involved adding a layer called Trust & Event Validation Layer to Security Layer in V2X Communication Stack. The SATO-V2X framework is illustrated in Figure 2.

Block 1: Verification of vehicles

Whenever alert is generated from V2X stack, Verification of vehicles block from this framework extracting multi-vehicle behavioral features such as speed variation, braking intensity, local traffic density from the surrounding environment.

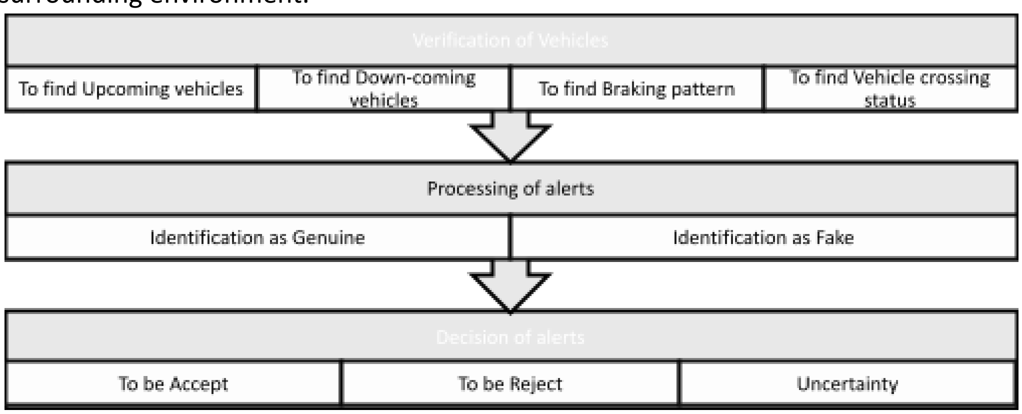


Figure 2. Semantic Score–Driven Adaptive Threshold Optimization Framework

Block 2: Processing alerts

The initial classification phase gives a means of determining whether the V2X warning should be classified based on a preset threshold value.

Block 3: Decision of alerts:

After calculating the optimal threshold Th_optimal then this system calculates again that alerts is genuine or fake by applying optimized threshold and $Score\_Label\_Optimal$ is generated by using equation (1).

$$Score\_Label\_Optimal = \begin{cases} 1, & s_i \geq Th\_optimal \\ 0, & s_i < Th\_optimal \end{cases} \qquad equation\ (1)$$

Finally, this approach predicts this alert is genuine or fake or uncertain.

Algorithm	Semantic Score–Driven Adaptive Threshold Optimization for V2X Alert Validation.

INPUT:	Incoming alert as Accident ahead
OUTPUT:	Detection of Real alert or Fake alert or Unstable
Step1:	Identification of Up-Coming vehicles data and Down coming vehicles data And Vehicle behavior as speed variation and braking frequency
Step2:	Calculate trust score by combing all the episodes of step1 data
Step3:	Predict the alert trust by using Score =>Threshold_Optimal then identified as Real alert. If Score =<Threshold_Optimal, then predicted as Fake alert. Else it is unknown alert.
Step4:	Calculate Optimal Threshold by using evaluation metrics FPR, FNR and Goto Step3.
Step5:	If threshold is optimal then Goto Step 6 Else Goto Step 3
Step6:	Decision is classified as Accept or Reject or Uncertain.

The calculated semantic scores using the data will act as inputs for threshold-based optimization and classification purposes. Furthermore, performance comparison can be carried out using simulated data and sample of synthetic semantic traffic dataset is shown in Table 2.

Table 2: Sample records of Synthetic semantic traffic dataset for maintain Alerts

Alert_id	Sender_id	Event_time	Event_zone	Claimed_Type	Reputation_ Sender-Score	Truth- Flag
A1	Vh_1	2/10/2026 10:00:02	Zone-X	accident	0.87	accident
A2	Vh_13	2/10/2026 10:00:03	Zone-X	accident	0.79	accident
A3	Vh_19	2/10/2026 10:10:11	Zone-P	accident	0.72	No accident
A4	Vh_28	2/10/2026 10:10:11	Zone-P	Congestion	0.75	No congestion

Result analysis

To compare the efficacy of the proposed model SATO-V2X with existing methods are ML Based Anomaly Detection in V2X Networks, Transformer Based V2XFormer Detection approach, AI-Driven IoV Security approach, Semantic Traffic Flow Validation Model and Adaptive Threshold Detection Framework. Figure 3(a) and 3(b) showed the output simulation for the generation of the proposed SATO-V2X based alert validation for the true V2X accident alert. The ADR and false positive rate comparison is furnished in Figure 4 and Graph for various metrics illustrated in Figure 5, it clearly shows that the proposed SATO-VTX Framework performs very well with existing models mentioned in literature. Hence, the resulting semantic similarity score becomes low (0.24), which is lower than the optimized threshold score value of 0.58. The comparison of proposed models with existing models of various metrics values is shown in Table 3.

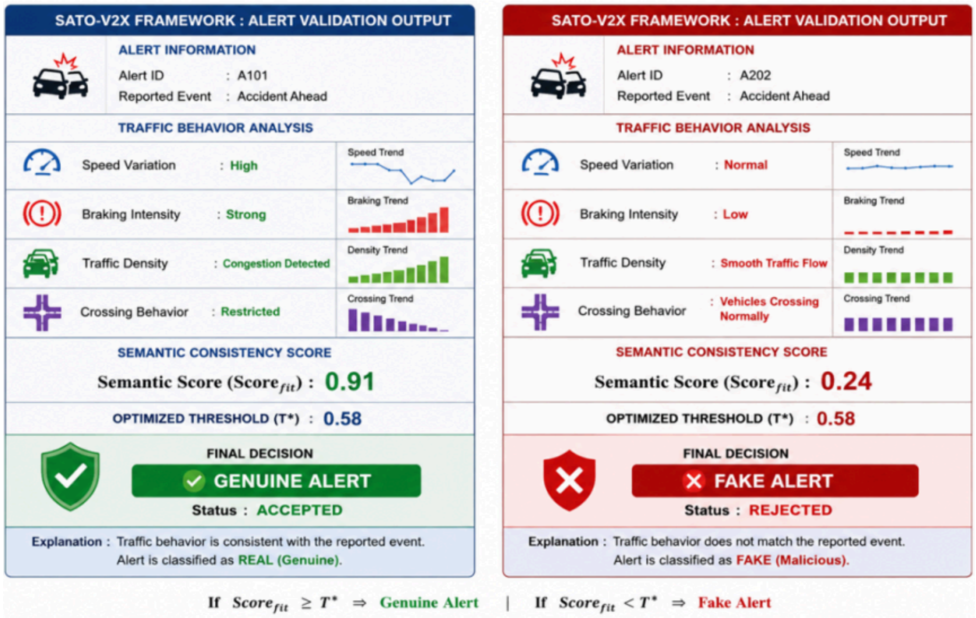
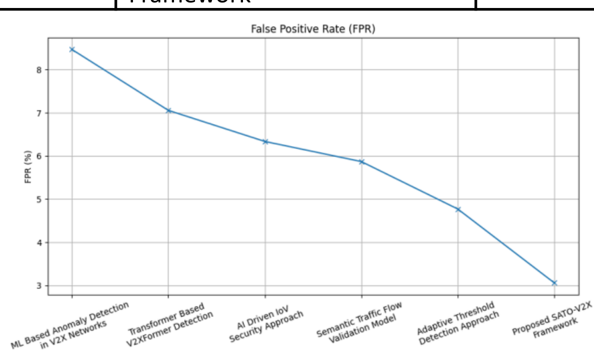


Figure 3 a)Genuine Alert Figure 3 b)Fake alert

It is illustrated the comparison of SATO-V2X framework with models by metrics accuracy as 96.90, precision as 97.05%, recall as 96.86%, F1-score as 96.96%, AD rate is 96.94% and false positive rate is 3.06.

Table 3: Comparison of SATO-V2X with existing models.

Ref.No.	Model Used	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	ADR (%)	FPR (%)
[13]	Transformer Based V2X Former Detection Approach	91.40	92.83	89.88	91.33	92.94	7.06
[14]	ML Based Anomaly Detection in V2X Networks	89.60	91.32	87.70	89.47	91.53	8.47
[15]	AI Driven IoV Security Approach	92.30	93.36	90.91	92.12	93.66	6.34
[16]	Semantic Traffic Flow Validation Model	93.20	94.15	92.29	93.21	94.13	5.87
[17]	Adaptive Threshold Detection Approach	94.20	95.07	93.16	94.11	95.23	4.77
	Proposed SATO-V2X Framework	96.90	97.05	96.86	96.96	96.94	3.06



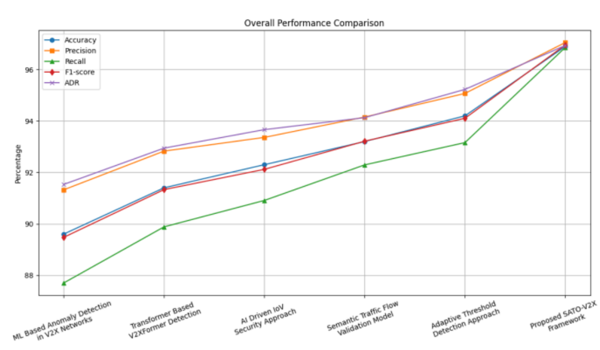


Figure 4. Graph for FPR reduction comparison Figure 5. Graph for various metrics

The proposed SATO-V2X approach outperforms in terms of all metrics because of semantic consistency calculation and adaptive threshold optimization.

Conclusion

Proposed SATO-V2X framework, it detects fake alerts using multi-vehicle behavior, focused on validating the sematic consistency of the received alerts instead of its dependent on traditional authentication approaches. Multi-vehicle behavior attributes speed, baking density and traffic density changes with respective to the alert intimated zone are analyzed. Experimental results determined that is proposed model obtained an accuracy of 96.90%, precision of 97.05%, recall of 96.86%, and F1-score of 96.96%, while maintaining a low false positive rate of 3.06% with existing models. These results confirm the effectiveness of the proposed semantic-aware adaptive validation mechanism for intelligent V2X communication systems with a very low false positive rate then leads to fake alerts not wrongly accepted. This proposed model achieves high recall and minimizes missed real alerts and ensures safety. Further research can be directed towards the real-time deployment based on SUMO for autonomous, self-learning V2X security models that can keep pace with changing cyber-attacks and traffic conditions.

References

[1] HAMID, Firas Shawkat, Jasim, Teba Ali, Alsultan, Raghad Ghalib, Vehicular-to-Everything (V2X) Communication Using 5G NR for Autonomous Vehicles, Journal of Engineering, 2026, 8643947, 9 pages, 2026. https://doi.org/10.1155/je/8643947.

[2] Weihao Feng, Bohui Wang, Stability analysis and delayed feedback control for platoon of connected automated vehicles with V2X and V2V infrastructure, Physica A: Statistical Mechanics and its Applications, Volume 658, 2025, 130258, ISSN 0378-4371.

[3] T. Sivanantham and S. C. Sethuraman, "Securing Vehicle-to-Everything (V2X) Communication: Challenges, Mechanisms, and Future Directions," Wireless Personal Communications, vol. 146, no. 2, pp. 537–643, 2026,

[4] Sahu, D., Prakash, S., Pandey, V.K. et al. Edge based distributed framework for real time hazard detection and road safety in smart transportation. Sci Rep 16, 12232 (2026). https://doi.org/10.1038/s41598-026-42899-w

[5] Shi Ye, Tiantian Chen, Oscar Oviedo-Trespalacios, Yasir Ali, Taeho Oh, Inhi Kim, How do the drivers react to different C-V2X-based communication conditions in dilemma zones? A driving simulator study, Accident Analysis & Prevention, Volume 221, 2025, 108208, ISSN 0001-575,https://doi.org/10.1016/j.aap.2025.108208.

[6] Chuan Tian, Yirong Kang, Modeling and optimal congestion control of multi-lane highway traffic with on-ramp and off-ramp under V2X environment, Physica A: Statistical Mechanics and its Applications, Volume 661,2025,130409,ISSN 0378-4371.

[7] Junjie Wu, Benjamin C. M. Fung, Natalia Stakhanova, Faiyaz Khan, Hanbo Yu,Securing automotive data flow: A survey of telematics security across intra-vehicle, V2X, and cloud layers, Vehicular Communications, Volume 59, 2026, 101024, ISSN 2214-2096.

[8] Chuan Tian, Yirong Kang, Modeling and optimal congestion control of multi-lane highway traffic with on-ramp and off-ramp under V2X environment, Physica A: Statistical Mechanics and its Applications, Volume 661,2025,130409,ISSN 0378-4371.

[9] K. V. S. S. Murthy, J. Rajanikanth, S. R. S. Shankar, Ch. Ravi S, and D. R Babu, "GenerativeAI in personal diary

information retrieval for criminal investigation," in Algorithms in Advanced Artificial Intelligence, CRC Press, 2024, doi: 10.1201/9781003529231-76.
[10] D. Lanka, V. Priyadarshini, C. R. S. Shankar, and R. Swaroop, "Verifiable secure vehicle connectivity using machine learning framework for internet of vehicles," in Algorithms in Advanced Artificial Intelligence, CRC Press, 2024. doi: 10.1201/9781003529231-5
[11] Pham, Thinh & Mcloughlin, Ian & Fahmy, Suhaib. (2014). Shaping Spectral Leakage for IEEE 802.11p Vehicular Communications. 2015. 10.1109/VTCSpring.2014.7023089.
[12] Raveena Dangi, Poonam Redhu, Analyzing the impact of nearby information of vehicles on a car-following model in a V2X communication with passing, International Journal of Non-Linear Mechanics,Volume 175,2025,105113,ISSN 0020-7462, https://doi.org/10.1016/j.ijnonlinmec.2025.105113.
[13] H. S. Mavikumbure, V. Cobilean, C. S. Wickramasinghe, D. Drake and M. Manic, "V2XFormer: Transformer-Based Anomaly Detection for Vehicle-to-Everything Communication," 2025 IEEE 101st Vehicular Technology Conference (VTC2025-Spring), Oslo, Norway, 2025, pp. 1-7
[14] Alfardus A, Rawat DB. Machine Learning-Based Anomaly Detection for Securing In-Vehicle Networks. Electronics. 2024; 13(10):1962. https://doi.org/10.3390/electronics13101962
[15] Y. Pan, Y. Wang, S. Guo, C. Yin, R. Li, Z. Su, and Y. Wu, "Trustworthy Semantic Communication for Vehicular Networks: Challenges and Solutions," arXiv preprint arXiv:2509.20830, 2025, doi:10.48550/arXiv.2509.20830.
[16] G. Tong, Y. Tang, W. Zhao, Z. Ge, Q. Li, and D. Peng, "Traffic flow prediction model based on dynamic spatio-temporal feature extraction and semantic association modeling," Computers and Electrical Engineering, vol. 133, p. 111036, 2026, doi: 10.1016/j.compeleceng.2026.111036.
[17] A. Heidari, S. H. Rastegar, and A. Khonsari, "FedIoV: A Secure and Adaptive Federated Framework for Real-Time Intrusion Detection in Vehicular Networks," Future Generation Computer Systems, vol. 181, p. 108448, 2026, doi:10.1016/j.future.2026.108448.