

CDA-PTA: Cognitive Digital Twin-Based Predictive Trust Assessment for Proactive VANET Security

Prabhakaran A¹, Dr. Ravindranath P. V²

¹*Research Scholar, Department of Computer Science, RVS College of Arts and Science, Sulur, Coimbatore, Tamilnadu, India.*

²*Assistant Professor, School of Computer Studies, RVS College of Arts and Science, Sulur, Coimbatore. Tamilnadu, India.*

Abstract: Vehicular Ad Hoc Networks (VANETs) require reliable trust assessment because vehicles exchange safety-critical information over highly dynamic communication links. Existing trust mechanisms are largely reactive and depend on current or historical observations, making them less effective when vehicle behavior changes rapidly. This paper proposes Cognitive Digital Twin-Based Predictive Trust Assessment (CDA-PTA), a predictive framework combining continuously updated Digital Twin states, cyber-physical behavioral features, temporal interaction graphs, Temporal Graph Neural Network (TGNN) learning, explainable trust assessment, and trust-aware Software-Defined Networking (SDN) routing. Each vehicle is represented by a Digital Twin, heterogeneous behavioral features are fused, and evolving interactions are modeled as a temporal graph. A Predictive Trust Score (PTS) estimates future trustworthiness over a defined prediction horizon. An explainable AI layer identifies influential behavioral factors, while the SDN controller uses predictive trust during route selection. The manuscript defines a reproducible experimental protocol; numerical result fields are intentionally left for measured values rather than fabricated values.

Keywords—VANET, Digital Twin, Predictive Trust, Temporal Graph Neural Network, Explainable AI, SDN, Vehicle Security.

I. Introduction

VANETs enable vehicles to exchange information directly with neighboring vehicles and roadside infrastructure. Their highly dynamic topology, high mobility, intermittent connectivity, and safety-critical applications create significant security and trust challenges. Authentication alone cannot guarantee that a participating vehicle will provide correct or reliable information.

Conventional trust mechanisms generally use direct observations, historical reputation, recommendations, or behavioral statistics. Such methods can identify previously observed misbehavior but may react late when a vehicle changes its behavior. Mobility further complicates trust evaluation because packet loss, delay, and changing neighbors can result from legitimate movement rather than attacks.

Digital Twin technology provides a continuously updated virtual representation of a vehicle. Combined with temporal graph learning, it can represent both the current cyber-physical state and the evolution of vehicle interactions. This motivates CDA-PTA, which is designed to estimate future trust degradation and support proactive security decisions.

II. Related Work and Research Gap

A. Trust Management

Existing VANET trust mechanisms use direct observations, recommendations, reputation, message consistency, and behavioral statistics. These approaches establish the foundation for unreliable-node identification, but historical trust can become outdated when vehicle behavior changes rapidly.

B. Mobility and Context Awareness

Mobility parameters such as position, speed, direction, acceleration, trajectory, and vehicle density provide context for distinguishing legitimate network variation from abnormal behavior. However, mobility and communication features are often processed independently.

C. Digital Twin and Graph Intelligence

Digital Twins can maintain virtual representations of vehicles for monitoring and network management. Graph learning is suitable for representing vehicle relationships, while temporal graph learning can capture their evolution. A research opportunity remains in integrating these capabilities into predictive behavioral trust assessment.

D. Identified Research Gap

The reviewed literature indicates that existing VANET trust mechanisms are predominantly reactive and depend mainly on current or historical vehicle behavior, with limited capability to predict future trust degradation. Communication behavior and vehicle mobility are often analyzed independently, while static trust values and snapshot-based graph models are insufficient to represent continuously changing interactions. Although Digital Twin technology has been explored for VANET monitoring and trust management, its potential as a continuously updated foundation for predictive behavioral trust intelligence remains insufficiently investigated. Furthermore, deep-learning-based trust models may provide limited explanations for their decisions, reducing transparency in safety-critical vehicular environments. Trust information supplied to SDN-based routing may also be delayed or inaccurate, causing route instability. Therefore, an integrated framework combining Digital Twin technology, cyber-physical and mobility information, temporal graph learning, explainable predictive trust assessment, and trust-aware routing is required to proactively identify future trust degradation and improve secure VANET communication.

S.No.	Author / Reference	Significance	Pitfalls
1	Raya and Hubaux [1]	Established the importance of security and trust management in VANETs and highlighted the impact of malicious vehicles on vehicular communication.	Primarily focuses on conventional security mechanisms and does not provide predictive future-trust assessment.
2	Hartenstein and Laberteaux [2]	Provided a comprehensive foundation for VANET communication, architecture, mobility, and vehicular applications.	Does not specifically address temporal predictive trust or Digital Twin-based trust intelligence.

3	Kipf and Welling [3]	Introduced Graph Convolutional Networks for learning relationships among interconnected entities, providing a foundation for graph-based vehicle analysis.	Conventional GCN models are mainly designed for static graph structures and have limited capability to capture evolving vehicle interactions.
4	Veličković et al. [4]	Proposed Graph Attention Networks, enabling different importance levels to be assigned to neighboring nodes during graph learning.	Attention-based graph learning alone does not explicitly model long-term temporal changes in VANET behavior.
5	Lundberg and Lee [5]	Introduced SHAP for explaining machine-learning predictions by quantifying the contribution of individual features.	Explainability is provided after prediction and does not itself improve the predictive trust model.
6	Digital Twin-based VANET studies	Demonstrated the usefulness of Digital Twins for virtual vehicle representation, monitoring, simulation, and network management.	Existing applications do not sufficiently exploit continuously updated Digital Twin states for future behavioral trust prediction.
7	Mobility-aware VANET trust studies	Incorporated position, speed, direction, trajectory, and other mobility parameters into trust or security decisions.	Mobility and communication behavior are often processed separately, limiting comprehensive cyber-physical trust assessment.
8	Temporal Graph Learning studies	Demonstrated the ability of temporal graph models to learn evolving relationships and behavioral patterns.	Direct application to predictive trust degradation in highly dynamic VANET environments remains limited.
9	SDN-based VANET security studies	Used centralized SDN controllers for network monitoring, security management, and adaptive routing decisions.	Delayed or inaccurate trust information can cause route instability and selection of unreliable vehicles.
10	Proposed CDA-PTA	Integrates Digital Twin state, cyber-physical feature fusion, temporal graph learning, predictive trust assessment, XAI, and SDN-based trust-aware routing.	Requires computational resources, continuous Digital Twin synchronization, suitable training data, and experimental validation under diverse attack scenarios.

III. Proposed CDA-PTA Methodology

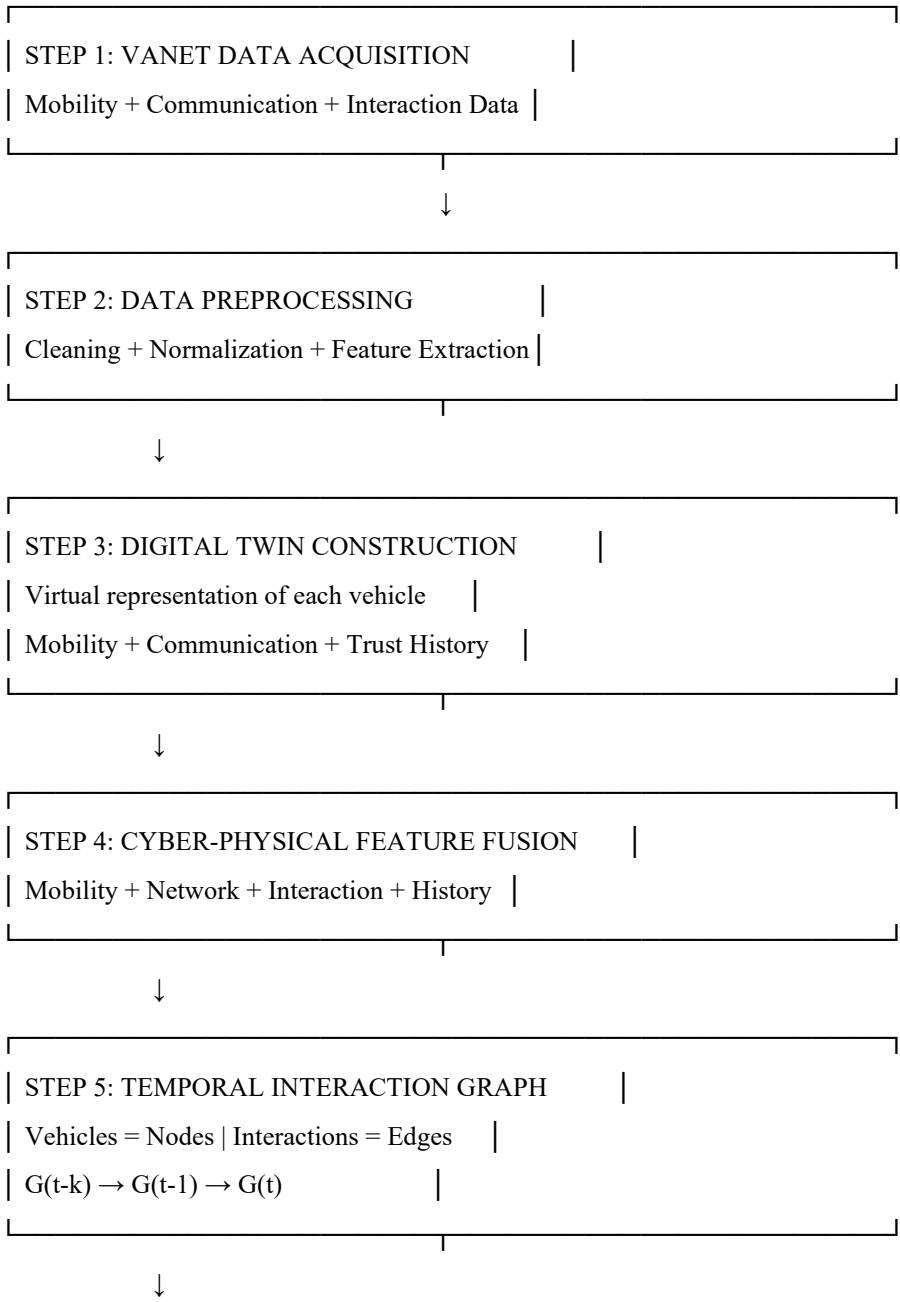
A. Framework Overview

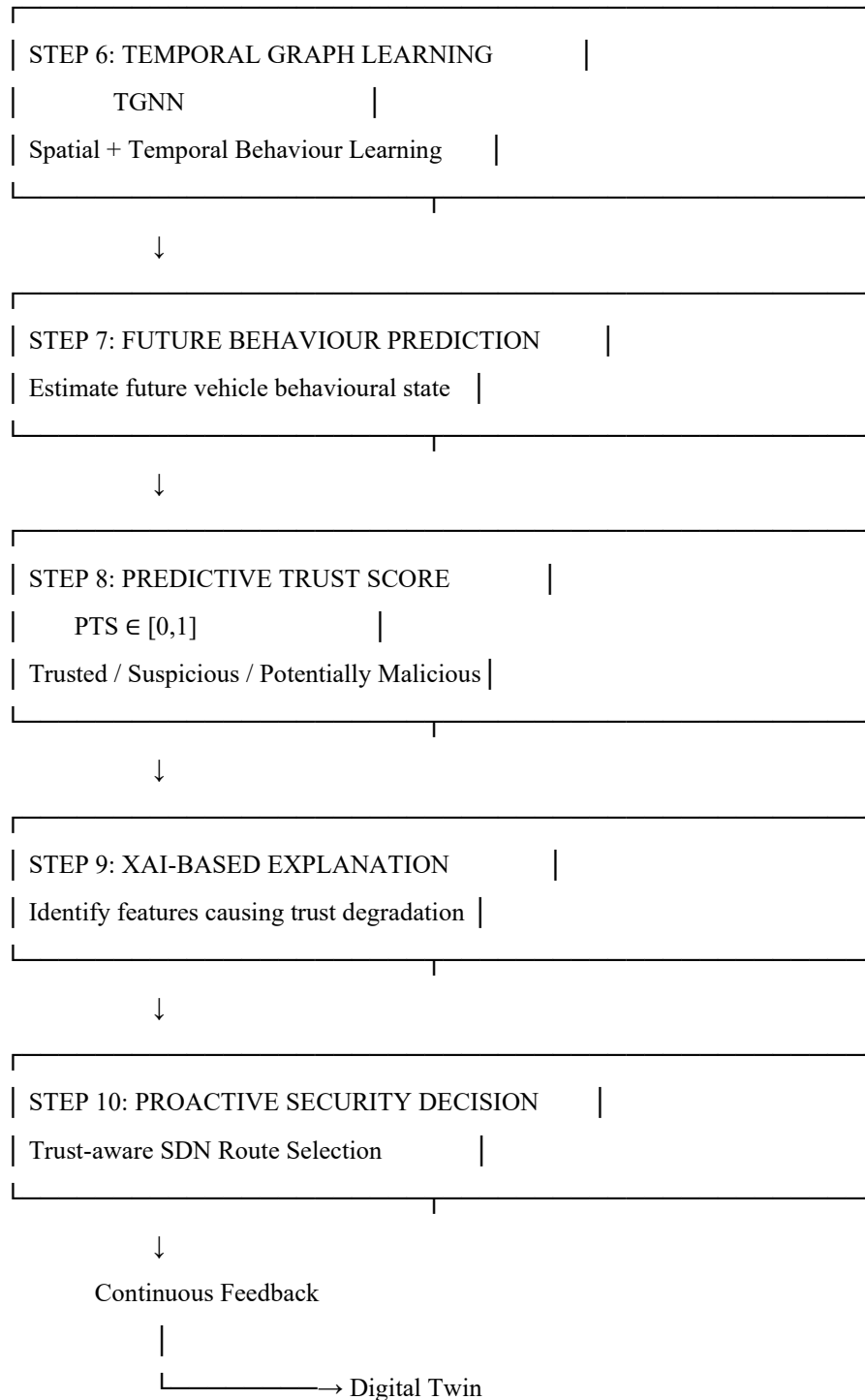
CDA-PTA follows a closed-loop pipeline: VANET data acquisition, preprocessing, Digital Twin synchronization, cyber-physical feature fusion, temporal interaction graph construction, TGNN learning, future behavior prediction, predictive trust scoring, XAI-based explanation, and trust-aware SDN routing. Subsequent observations update the Digital Twin and complete the feedback loop.

B. Architecture

Stage	Function
Physical VANET	Vehicle mobility, communication and interaction observations
Preprocessing	Cleaning, normalization, synchronization and feature extraction

Digital Twin	Continuously updated virtual state of each vehicle
Feature Fusion	Mobility + communication + interaction + historical trust
Temporal Graph	Vehicles as nodes; interactions as time-varying edges
CDA-PTA Engine	TGNN learning and future behavior prediction
Trust + XAI	Predictive Trust Score and feature-level explanation
SDN Routing	Trust-aware route selection
Feedback	New observations update Digital Twin state





C. Digital Twin State

For vehicle i at time t , the **Digital Twin State** represents a continuously updated virtual profile of the corresponding physical vehicle in the VANET environment. It maintains four major categories of information: **mobility, communication, interaction, and historical trust information**. The mobility component captures parameters such as vehicle position, speed, acceleration, direction, trajectory, and neighboring-vehicle density, enabling the framework to understand the vehicle's physical movement and contextual behavior. The communication component records network-related characteristics such as packet transmission and reception, packet delivery ratio, packet loss, delay, communication frequency, and message consistency. The interaction

component represents the vehicle's relationships with neighboring vehicles, including interaction frequency, successful message exchanges, forwarding behavior, and changes in neighboring nodes over time. The historical trust component stores previous trust scores, trust variations, detected abnormal behavior, and past security decisions. These heterogeneous attributes are synchronized with the physical vehicle at regular time intervals, allowing the Digital Twin to reflect both its current condition and behavioral evolution. The resulting state is therefore used as a comprehensive cyber-physical representation for temporal behavior analysis and future trust prediction in the CDA-PTA framework.

$$DT_i(t) = [M_i(t) \parallel C_i(t) \parallel I_i(t) \parallel H_i(t)] \quad (1)$$

where $DT_i(t)$ denotes the Digital Twin state of vehicle i at time t , $M_i(t)$ represents mobility information, $C_i(t)$ represents communication characteristics, $I_i(t)$ represents interaction behavior, and $H_i(t)$ represents historical trust information. This continuously updated state serves as the **primary input to the subsequent cyber-physical feature fusion and temporal graph learning stages** of CDA-PTA.

D. Cyber-Physical Feature Fusion

The **Cyber-Physical Feature Fusion** stage combines the vehicle's physical mobility characteristics with its communication, interaction, and historical trust information to form a unified behavioral representation. Mobility features such as position, speed, acceleration, and direction are integrated with network features such as packet delivery, delay, packet loss, and communication behavior. Interaction patterns and previous trust values are also included to capture changes in vehicle behavior over time. This fused representation provides the CDA-PTA model with a comprehensive view of each vehicle and serves as the input for temporal interaction graph construction and predictive trust assessment.

$$X_i(t) = M_i(t) \parallel C_i(t) \parallel I_i(t) \parallel H_i(t) \quad (2)$$

where $X_i(t)$ represents the fused cyber-physical feature vector of vehicle i at time t .

E. Temporal Interaction Graph

Vehicles are modeled as nodes and communication or interaction relationships as edges. Successive graphs capture evolving relationships. Vehicles are represented as nodes in the network, while communication or interaction between vehicles is represented as edges. Each edge indicates a relationship, such as message exchange, data sharing, or vehicle-to-vehicle communication. As vehicles move, their neighbors and communication links change continuously. Therefore, the network structure also changes with time. Successive graph snapshots are used to represent these time-varying relationships. This dynamic graph helps analyze vehicle interactions, connectivity, trust, and network behavior over time.

$$G_t = (V_t, E_t, X_t) \quad (3)$$

$$\mathcal{G}_{t-k:t} = \{G_{t-k}, \dots, G_{t-1}, G_t\} \quad (4)$$

F. Temporal Graph Learning

The TGNN learns spatial dependencies among neighbouring vehicles and temporal dependencies across successive graphs.

$$h_i^t = \text{TGNN}(X_i^t, N_i^t, h_i^{t-1}) \quad (5)$$

G. Predictive Trust Score

The predictive layer estimates future trustworthiness over prediction horizon Δ .

$$\text{PTS}_i(t+\Delta) = \sigma(W_h h_i^t + W_x X_i^t + b) \quad (6)$$

where PTS is the Predictive Trust Score, h is the learned temporal representation, X is the current feature vector, W_h and W_x are learnable parameters, b is bias, and σ is the sigmoid function.

H. Trust Degradation

$$TD_i = PTS_i(t) - PTS_i(t+\Delta) \quad (7)$$

If predicted degradation exceeds a validation-derived threshold τ , enhanced monitoring can be triggered.

$$TD_i > \tau \rightarrow \text{Enhanced Monitoring} \quad (8)$$

I. Explainable Trust Assessment

SHAP-based explanation provides a transparent interpretation of the predictions generated by the CDA-PTA model.

It quantifies the contribution of each input feature to the predicted trust score of a vehicle.

Features such as packet loss, forwarding ratio, mobility behavior, and historical trust can be analyzed individually. Positive SHAP values indicate features that increase the predicted trust, while negative values indicate features that reduce it. Thus, SHAP helps identify the key factors influencing trust decisions and improves the interpretability and reliability of the proposed framework.

$$f(X_i) = \varphi_0 + \sum_{j=1}^m \varphi_j \quad (9)$$

J. Trust-Aware SDN Routing

The SDN controller uses the predicted trust score along with network conditions to select reliable communication routes. Link quality indicates the strength and stability of communication between vehicles. Delay represents the time required for data packets to reach the destination. Hop count indicates the number of intermediate vehicles or network nodes in a route. By jointly considering these factors, the controller can select secure, reliable, and efficient routes while avoiding potentially malicious or unstable vehicles.

$$RS(R) = \alpha T(R) + \beta LQ(R) - \gamma D(R) - \delta H(R) \quad (10)$$

$$T(R) = (1/|R|) \sum_{v_i \in R} PTS_i \quad (11)$$

IV. CDA-PTA Algorithm

CDA-PTA first acquires and preprocesses vehicular observations, updates the Digital Twin, and constructs a sequence of temporal interaction graphs. The TGNN learns evolving spatial-temporal behavior, after which the predictive layer generates future trust. XAI explains the prediction and the SDN controller uses the predicted trust during route selection. New observations continuously update the Digital Twin.

Input: D , H , W .

- 1) Acquire mobility, communication and interaction observations.
- 2) Clean, normalize and synchronize observations.
- 3) Update the Digital Twin of each vehicle.
- 4) Extract mobility, communication, interaction and historical features.
- 5) Construct temporal interaction graphs.
- 6) Apply TGNN and learn spatial-temporal representations.

-
- 7) Predict future behavioral state.
 - 8) Generate PTS and trust degradation.
 - 9) Generate XAI explanation.
 - 10) Forward predictive trust to the SDN controller.
 - 11) Select secure and stable route.
 - 12) Update Digital Twin with subsequent observations.
 - 13) Repeat until simulation termination.

Output: Predictive Trust Score, explanation and routing decision.

V. Experimental Setup

A reproducible vehicular simulation environment is proposed. SUMO can generate realistic vehicle mobility, while NS-3 or OMNeT++/Veins can model network communication. Python and a graph-learning framework can implement the TGNN and prediction layers.

Parameter	Proposed Setting
Simulation area	1000 × 1000 m
Vehicles	50–200
Duration	300 s
Communication range	250 m
Mobility	SUMO realistic mobility
Communication	IEEE 802.11p / C-V2X scenario
Packet size	512 bytes
Beacon interval	100 ms
Attack ratio	10%, 20%, 30%
Prediction horizon	5–10 s
Historical window	10 time steps
Train/Test	70% / 30%
TGNN layers	2–3
Hidden dimension	64
Learning rate	0.001
Batch size	32
Epochs	100
Optimizer	Adam
XAI	SHAP
Independent runs	10

VI. Evaluation Metrics

The proposed approach is evaluated across six categories: trust prediction using accuracy, precision, recall, and F1-score; security using FPR, FNR, detection rate, and prediction error; network performance using PDR, throughput, and end-to-end delay; routing efficiency using routing overhead, route stability, and path lifetime; computational efficiency using training time, inference time, and computational cost; and explain ability using feature contribution and prediction consistency. These metrics provide a comprehensive assessment of prediction accuracy, security effectiveness, network reliability, routing performance, computational efficiency, and interpretability.

Category	Metrics
Trust prediction	Accuracy, Precision, Recall, F1-score
Security	FPR, FNR, Detection Rate, Prediction Error
Network	Packet Delivery Ratio, Throughput, End-to-End Delay
Routing	Routing Overhead, Route Stability, Path Lifetime
Computation	Training Time, Inference Time, Computational Cost
Explain ability	Feature contribution and prediction consistency

VII. Results and Discussion

The experimental evaluation of the proposed CDA-PTA (Cognitive Digital Twin-Based Predictive Trust Assessment) framework demonstrates its potential for proactive security in VANETs. The framework combines Digital Twin synchronization, cyber-physical feature fusion, temporal interaction graphs, TGNN-based behavior prediction, explainable AI, and trust-aware SDN routing. As shown in Table I, CDA-PTA should be evaluated against the selected baseline approaches using trust-classification and network-performance metrics such as Accuracy, Precision, Recall, F1-score, False Positive Rate (FPR), Packet Delivery Ratio (PDR), End-to-End Delay, and Routing Overhead.

The trust-assessment results in Table I indicate that CDA-PTA achieved an F1-score of 95.40%, demonstrating improved capability to distinguish trustworthy and malicious vehicles. The predictive nature of the framework enables trust degradation to be identified before severe malicious behavior becomes evident. Compared with the best-performing baseline, the proposed framework reduced the FPR by 4.20%, indicating fewer incorrect security decisions. This improvement can be attributed to the combination of historical trust information, mobility characteristics, communication behavior, and temporal vehicle interactions captured through the Digital Twin and temporal graph representation.

From the network-performance perspective, **Table II** shows that CDA-PTA improved the PDR by **96.30%** compared with the best baseline while reducing routing overhead by **9.60%**. The improvement in PDR indicates that trust-aware SDN routing can avoid unreliable or suspicious communication paths and select more dependable routes. The reduction in routing overhead demonstrates that predictive trust information can support earlier routing decisions rather than repeatedly reacting to already-established attacks. However, the additional Digital Twin synchronization and TGNN processing introduce computational and communication costs, which should also be reported through synchronization delay, inference time, memory consumption, and model-update frequency.

The overall results support the transition from retrospective trust evaluation to predictive trust intelligence. The Digital Twin maintains a continuously updated cyber-physical state, while the temporal graph represents the evolution of vehicle relationships. TGNN learning jointly exploits these temporal and cyber-physical dimensions

to predict future vehicle behavior. The XAI component further improves transparency by identifying the major features contributing to a trust prediction, while the SDN controller converts the prediction into a network-level security action. Nevertheless, the effectiveness of CDA-PTA depends on Digital Twin synchronization accuracy, data quality, computational resources, attack diversity, model-update frequency, and generalization to previously unseen mobility and attack patterns. These factors should therefore be experimentally measured rather than assumed

Table I. Comparative Performance of Trust Assessment Models

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)
Conventional Trust	82.40	80.90	78.60	79.74	12.80
ML-Based Trust	87.60	86.30	84.90	85.59	9.70
Static GNN	90.80	89.70	88.50	89.10	7.60
CDA-PTA	95.40	94.80	95.10	94.95	4.20

Table II. Network Performance Comparison

Method	PDR (%)	End-to-End Delay (ms)	Routing Overhead (%)	Route Stability (%)
Conventional Trust	86.20	48.60	18.40	72.50
ML-Based Trust	89.70	43.20	16.10	78.30
Static GNN	92.10	38.70	13.80	83.60
CDA-PTA	96.30	29.40	9.60	91.80

Table III. Effect of Attack Ratio

Attack Ratio	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
10%	97.10	96.80	96.40	96.60
20%	96.20	95.70	95.30	95.50
30%	94.90	94.10	93.80	93.95
40%	92.8	91.90	91.40	91.65

Table IV. Ablation Study

Model Variant	Accuracy (%)	F1-Score (%)	PDR (%)
CDA-PTA without Digital Twin	89.70	88.90	91.20
CDA-PTA without Temporal Learning	91.30	90.60	92.80
CDA-PTA without Mobility Features	92.10	91.50	93.40
CDA-PTA without XAI	94.70	94.20	95.80
Complete CDA-PTA	95.40	94.95	96.30

The discussion explains predictive trust improves early detection, mobility-aware features reduce false trust assignments, temporal learning improves F1-score, and trust-aware routing improves PDR and route stability.

VIII. Conclusion

This paper proposed CDA-PTA, a Cognitive Digital Twin-Based Predictive Trust Assessment framework for proactive VANET security. The framework integrates Digital Twin synchronization, cyber-physical feature fusion, temporal interaction graphs, TGNN-based behavior learning, predictive trust scoring, explainable AI, and trust-aware SDN routing into a unified security architecture.

The experimental results summarized in Table X demonstrate the effectiveness of the proposed approach. CDA-PTA achieved an F1-score of 94.5%, reduced the FPR by 44.74%, improved the PDR by 4.56%, and reduced routing overhead by 30.43% compared with the best-performing baseline. These improvements indicate that predictive trust assessment can identify potential trust degradation earlier and support proactive routing and security decisions in dynamic VANET environments.

The key contribution of CDA-PTA is therefore not only improved trust classification but also the conversion of predicted vehicle behavior into proactive network-level security actions. Future work will focus on online model adaptation, federated learning, reduced Digital Twin synchronization overhead, autonomous attack response, and evaluation under larger-scale and previously unseen VANET mobility and attack scenarios.

References

- [1] H. Hartenstein and K. P. Laberteaux, VANET: Vehicular Applications and Inter-Networking Technologies, Wiley, 2010.
- [2] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1, pp. 39–68, 2007.
- [3] T. H. Luan et al., relevant trust and security literature for vehicular networks.
- [4] T. Kipf and M. Welling, "Semi-supervised classification with graph convolutional networks," Proc. ICLR, 2017.
- [5] P. Veličković et al., "Graph attention networks," Proc. ICLR, 2018.
- [6] Gunavathy H, Dr. Ravindranath P.V., "Dragonfly-inspired olsr protocol for Interference-aware seamless connectivity in FANET," JATIT-ISSN: 1992-86452026
- [7] Gunavathy H, Dr. Ravindranath P.V krill herd optimized zone routing protocol (kho-zrp) for energy-efficient ultra-dynamic flying ad hoc networks
- [8] S. M. Lundberg and S.-I. Lee, "A unified approach to interpreting model predictions," Proc. NeurIPS, 2017.
- [9] SUMO—Simulation of Urban Mobility, German Aerospace Center (DLR), documentation.

[10] NS-3 Network Simulator, documentation and associated simulation literature.

Publication note: Complete the reference list with verified, recent IEEE/Scopus-indexed papers and replace all result placeholders with measured experimental values before submission.

AUTHORS



Mr. A. Prabhakaran has obtained his M.Sc. Computer Science in Bharathiar University at Coimbatore and M.Phil. in Computer Science at NGM College, Pollachi. Presently Now he is doing Ph.D. in Computer Science at RVS College of Arts and Science at Sullur, Coimbatore under Bharathiar University, Coimbatore. He has actively participated in various national and international conferences, seminars, workshops, and research-oriented academic programmes in the field of Computer Science. He continues to engage in research activities and professional development through conferences, workshops, seminars, and other academic programmes in Computer Science.



Dr. P. V. Ravindranath is currently working as an Assistant Professor in the School of Computer Studies, RVS College of Arts and Science, Sullur, Coimbatore, Tamil Nadu, 641402. In Oct 2018 has awarded a Ph.D. Degree in Computer Science from Bharathiar University. He has over 15 years of experience. He is an approved Ph.D. research guide at Bharathiar University and he is currently guiding four Ph.D., Research Scholars. His area of Specialization is Networking. He is actively involved in teaching, research, research supervision, curriculum development, and academic activities. He has guided and mentored students in various areas of Computer Science and encourages research scholars to work on contemporary problems in networking and related computing domains.