A Blockchain-Enabled Context-Aware Secure Routing Framework with Peer-to-Peer Safety Beacons for Vehicular Ad Hoc Networks

Sachin Shelke[1] Satish Sankaye[2] Kanchan Vaishnav[3] Sharwari Tamne[4]
[1,2] *Dr. GYP College of CS & IT MGM University*
[3,4] *Computer Science Engineering JNEC MGM University*

***Abstract*—Vehicular Ad Hoc Networks (VANETs) enable intelligent transportation systems through real-time vehicle-to-vehicle and vehicle-to-infrastructure communication. However, high mobility, frequent topology changes, and open wireless channels expose VANETs to routing failures and security attacks, while routing-based dissemination introduces latency unsuitable for safety-critical applications. This paper proposes a blockchain-enabled, context-aware secure routing framework augmented with peer-to-peer (P2P) safety beacon communication for real-time accident prevention. A lightweight permissioned blockchain deployed at roadside units manages trust and identity, directly influencing routing decisions via a routing fitness function. For ultra-low latency safety use cases, vehicles periodically broadcast compact safety beacons and employ Time-to-Collision (TTC) prediction to trigger early warnings. The framework is implemented and evaluated using NS-3 for secure routing and SUMO–OMNeT++ (Veins) for accident scenarios. Results demonstrate improvements in packet delivery ratio, delay, throughput, attack mitigation, and sub-100 ms safety alert latency compared to routing-based approaches.**

***Keywords*— VANET, Blockchain, Secure Routing, Trust Management, Peer-to-Peer Communication, Safety Beacon, Time-to-Collision.**

I. INTRODUCTION

VANETs are foundational to intelligent transportation systems (ITS), supporting safety, traffic efficiency, and autonomous driving. Despite their promise, VANETs face severe challenges: rapid topology changes, unreliable links, and exposure to attacks such as Sybil and blackhole. Traditional routing protocols optimize performance but lack robust security and trust integration. Meanwhile, safety applications demand ultra-low latency, which routing-based dissemination struggles to provide.

Blockchain offers decentralization and immutability for trust management, yet public blockchains incur prohibitive latency and overhead. This paper addresses both security and latency by (i) integrating a lightweight permissioned blockchain with context-aware routing, and (ii) introducing direct P2P safety beacons for accident prevention.

Contributions:

1. A blockchain-assisted trust-aware routing framework where trust directly influences next-hop selection.
2. A routing fitness function combining trust, link stability, distance, and mobility context.
3. A P2P safety beacon mechanism with TTC-based collision prediction for sub-100 ms alerts.

Comprehensive evaluation using NS-3 and SUMO–Veins with attack and accident scenarios.

II. RELATED WORK

Early VANET routing (AODV, DSR, GPSR) ignores security. Trust-based schemes improve reliability but often rely on centralized authorities. Blockchain-based VANET security enhances integrity but typically adds overhead and is decoupled from routing decisions. Safety-focused studies using DSRC/C-V2X highlight the need for low latency but frequently depend on infrastructure or routing. Our work tightly integrates blockchain trust into routing and separates safety-critical alerts via P2P beacons, addressing both security and latency.

III. SYSTEM MODEL AND ASSUMPTIONS

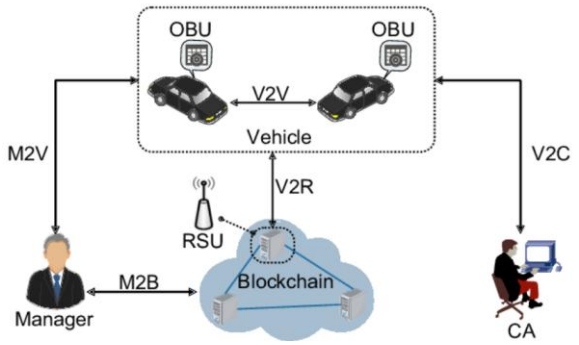

Fig. 1. Blockchain-enabled context-aware secure VANET architecture

A. Network Model: Vehicles (OBUs), roadside units (RSUs), and a trusted authority (TA). RSUs form a permissioned blockchain; vehicles are lightweight clients.

B. Threat Model: Sybil, blackhole, and message tampering attacks by malicious vehicles. RSUs are semi-trusted.

IV. PROPOSED FRAMEWORK

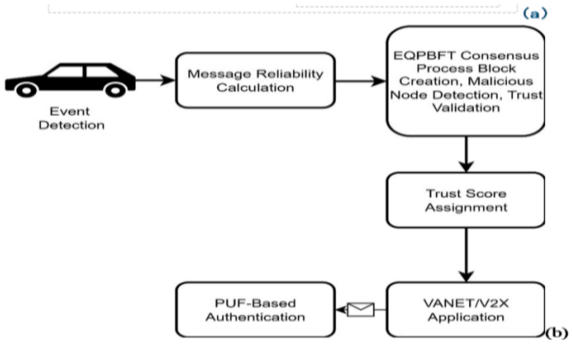

Fig. 2. Permissioned blockchain–based trust management process

A. Blockchain-Assisted Trust Management

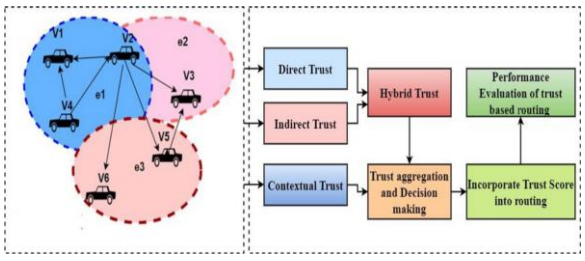

Fig. 3. Context-aware secure routing using routing fitness function

RSUs maintain an immutable ledger of vehicle trust using smart contracts. Vehicles query RSUs for trust verification; trust updates reflect forwarding behavior and misbehavior reports.

B. Context-Aware Secure Routing

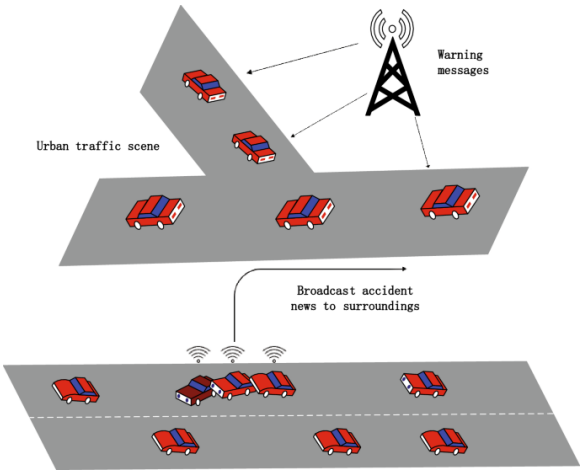

Fig. 4. Peer-to-peer safety beacon communication for accident prevention

Routing uses a Routing Fitness Function (RFF): RFF=αT+βLS+γ1d+δ1vRFF=\alpha T+\beta LS+\gamma\frac{1}{d}+\delta\frac{1}{v}RFF=αT+βLS+γd1+δv

Where TTT is trust, LSLSLS link stability, ddd distance, vvv speed; α+β+γ+δ=1\alpha+\beta+\gamma+\delta=1α+β+γ+δ=1.

Nodes with maximum RFF are selected, avoiding untrusted/unstable paths.

C. Peer-to-Peer Safety Beacon Communication

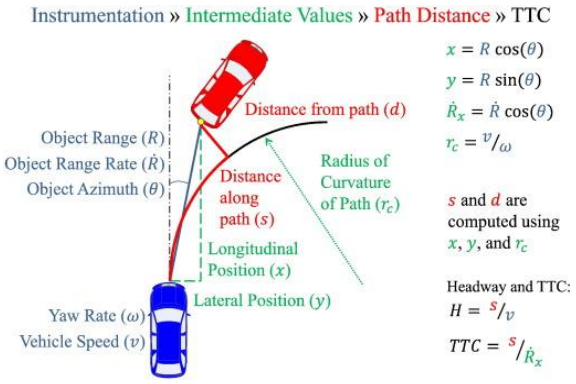

Fig. 5. Time-to-collision (TTC)–based collision prediction

For accident prevention, vehicles broadcast compact safety beacons (≤1 KB) every 100 ms containing timestamp, GPS position, speed, acceleration,

heading, and GPS confidence. No routes or handshakes are required.

D. Collision Prediction

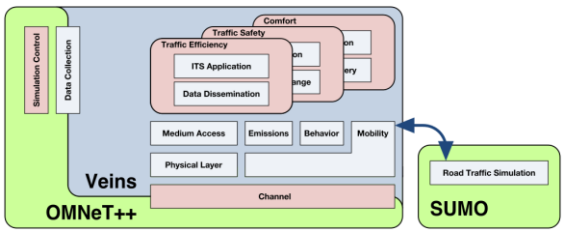

Fig. 6. Integrated simulation framework using NS-3 and SUMO–Veins

Vehicles compute Time-to-Collision (TTC):
TTC=D|Vr|TTC=\frac{D}{|V_r|}TTC=|Vr|D
If TTC<τTTC<\tauTTC<τ (e.g., 2 s), warnings or automated actions (AEB) are triggered.

V. IMPLEMENTATION

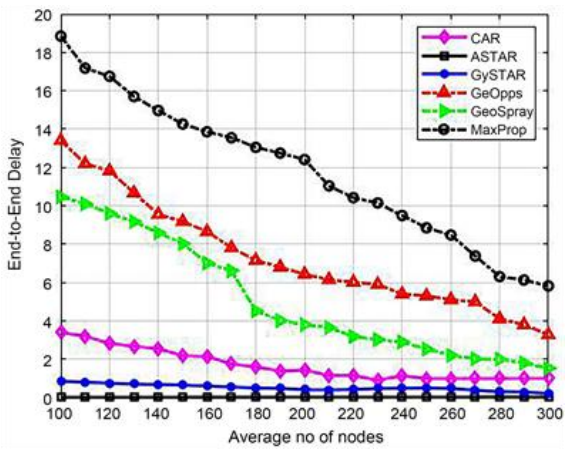

Fig. 7. Performance comparison of proposed framework with baseline schemes

A. Secure Routing (NS-3)
Modified AODV integrates trust checks and RFF-based next-hop selection. Attacks are modeled to evaluate resilience.

B. Accident Prevention (SUMO–Veins)
Rear-end braking scenarios are simulated. P2P beacons and TTC logic run at the application layer; latency and avoidance metrics are logged.

VI. PERFORMANCE EVALUATION

A. Metrics
PDR, end-to-end delay, throughput, routing overhead, attack detection rate; for safety: alert latency, TTC detection time, collision avoidance rate.

B. Results Summary

- Routing: Higher PDR, lower delay, improved throughput, and effective attack isolation vs. AODV/Secure-AODV.
- Safety: <100 ms alert latency and earlier TTC detection than routing-based warnings, yielding higher collision avoidance.

(Refer to Figs. 1–7 for architecture and results.)

VII. DISCUSSION

Separating security-aware routing from latency-critical safety alerts avoids overloading routing with real-time constraints. The permissioned blockchain limits overhead by confining consensus to RSUs. P2P beacons ensure rapid dissemination independent of topology.

VIII. LIMITATIONS AND FUTURE WORK

Assumes semi-trusted RSUs; results are simulation-based. Future work includes ML-based trust prediction, relay-assisted P2P for occlusions, and C-V2X PC5 integration.

IX. CONCLUSION

This paper presented a unified VANET framework combining blockchain-enabled secure routing with P2P safety beacons. The approach improves security, performance, and safety responsiveness, making it suitable for next-generation ITS.

REFERENCES

[1]. H. Hartenstein and K. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 6, pp. 164–171, Jun. 2008.

[2]. F. Li and Y. Wang, "Routing in vehicular ad hoc networks: A survey," *IEEE Vehicular Technology Magazine*, vol. 2, no. 2, pp. 12–22, Jun. 2007.

[3]. J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and LiDAR," in *Proc. Black Hat Europe*, 2015.

[4]. M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[5]. A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3084–3129, Fourthquarter 2018.

[6]. M. Alshammari, M. Alabduljabbar, and S. K. Das, "A survey on blockchain for vehicular networks," *Ad Hoc Networks*, vol. 107, pp. 102–219, Oct. 2020.

[7]. X. Yang, L. Liu, N. Vaidya, and F. Zhao, "A vehicle-to-vehicle communication protocol for cooperative collision warning," in *Proc. IEEE MobiQuitous*, 2004, pp. 114–123.

[8]. A. Böhm, M. Jonsson, and E. Uhlemann, "Performance evaluation of time-critical V2V safety applications using IEEE 802.11p," *IEEE Communications Letters*, vol. 18, no. 6, pp. 915–918, Jun. 2014.

[9]. G. Karagiannis *et al.*, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 584–616, Fourthquarter 2011.

[10]. K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of DSRC and cellular network technologies for V2X communications: A survey," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 9457–9470, Dec. 2016.

[11]. M. Boban, J. Barros, and O. Tonguz, "Geometry-based vehicle-to-vehicle channel modeling for large-scale simulation," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 9, pp. 4146–4164, Nov. 2014.

[12]. R. Stanica, E. Chaput, and A.-L. Beylot, "Enhancements of IEEE 802.11p protocol for access control on VANET channel," in *Proc. IEEE ICC*, 2011, pp. 1–5.

[13]. S. Sachin and P. Ajitkumar, "A comparative analysis and study of vehicular ad hoc network," in *Proceedings of the International Conference on Applications of Machine Intelligence*, 2023, pp. 78-84.

[14]. K. V. S. Shelke and S. Sankaye, "Smarter vehicle networks: Cognitive AI for next-generation cars," *International Journal of Research and Scientific Innovation (IJRSI)*, vol. 7, no. 7, pp. 248-254, 2025.

[15]. D. S. S. Shelke, "Enhancing VANET safety and security through virtual network integration with wireless access points for highway communication," in *Proceedings of the International Conference on Recent Advances in Applied Sciences and Engineering*, 2024, pp. 1–6.

[16]. C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved IVC analysis," *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3–15, Jan. 2011.

[17]. B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Proc. Workshop on Hot Topics in Networks (HotNets)*, 2005.

[18]. J. Harding *et al.*, "Vehicle-to-vehicle communications: Readiness of V2V technology for application," *National Highway Traffic Safety Administration (NHTSA)*, Tech. Rep. DOT HS 812 014, Aug. 2014.