Asynchronous Reputation Management Framework For V2X Networks Under Intermittent Connectivity

Hope Leticia Nakayiza, Love Allen Chijioke Ahakonye †, Dong-Seong Kim, Jae Min Lee,
IT Convergence Engineering, † ICT Convergence Research Center,
Kumoh National Institute of Technology Gumi, South Korea
hopeleticia, loveahakonye, dskim, ljmpaul@kumoh.ac.kr

***Abstract*—Vehicular networks depend on continuous connectivity for reputation management, but disruptions compromise reliability. This paper proposes a decentralized V2X trust system that operates during offline periods using a hashed trust lock protocol to generate secure local trust logs and synchronize them with IPFS and blockchain upon reconnection. Experiments show an average processing latency of $1.2s$ per vehicle with reliable detection of replayed and conflicting logs prior to on-chain anchoring.**

***Index Terms*—Blockchain, IPFS, Offline communication, Trust and Reputation management, V2X**

I. Introduction

Vehicle-to-everything (V2X) networks enable communication among vehicles, infrastructure, and other road users [1]. They employ both IEEE 802.11p-based direct short-range communication (DSRC) and cellular V2X (C-V2X) technologies [2], supporting both direct exchange and broadband-assisted connectivity. These systems depend on roadside units (RSUs), base stations, cloud-edge infrastructure, and the internet for trust management and incentive mechanisms [3]. Yet, coverage gaps in rural areas, tunnels, or during disasters can disrupt connectivity [4]. Without effective fallback measures, such outages may be exploited by malicious actors, threatening system integrity [5].

This paper, therefore, introduces a system for continuous trust management that does not require constant internet or infrastructure access. Our key contributions include the Hashed Trust Lock Protocol (HTLP) for secure offline trust log generation and storage, a robust conflict detection and replay prevention mechanism, and the integration of the Interplanetary File System (IPFS) with blockchain for decentralized storage and reputation verification.

II. Methodology

Vehicles equipped with connectivity technologies such as C-V2X or Wi-Fi interact with RSUs and infrastructure to synchronize trust management data with IPFS and blockchain nodes. In the absence of internet connectivity, vehicles can communicate with each other through V2V links over DSRC. Figure 1 depicts the proposed offline reputation management architecture. The proposed HTLP ensures verifiable cryptographic commitments of trust logs during offline operations. A vehicle V_a observing the behavior of a peer vehicle V_p initiates the trust evaluation, logging the trust events locally

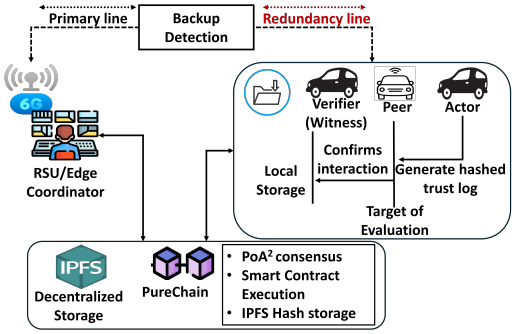

Fig. 1: HTLP-Based Offline Reputation Management Architecture

and creating a hash lock to commit to the trust assessment cryptographically. A witness vehicle, V_w, endorses this interaction by appending its signature to the log, thereby boosting its credibility. The trust log L is defined in Equation 1.

$$L = \{V_a, V_p, s_{ap}, h_i, t, \sigma_a, V_k, \sigma_k\}, \qquad h_i = H(n_i) \quad (1)$$

where s_{ap} is the trust score assigned by V_a to V_p, $H(n_i)$ is the SHA-256 hash of the secret nonce n_i and locks the log, t is the timestamp, σ_a and σ_k are the ECDSA signatures of V_a and V_w, respectively. Trust scores are updated incrementally, where $T_{ap}(t)$ at time t is given by Equation 2.

$$T_{ap}(t) = T_{ap}(t-1) + \Delta s_{ap}(t), \quad (2)$$

with $\Delta s_{ap}(t) \in [-0.3, +0.2]$, where negative values denote malicious behavior and positive values indicate cooperation.

A conflict detection algorithm ensures consistency by checking if the same vehicle logs contradictory trust scores for the same peer within a short time window Δt. Two logs, L_1 and L_2, are deemed conflicting as shown in Equation 3.

$$|s_1 - s_2| > \theta \quad \text{and} \quad |t_1 - t_2| \leq \Delta t, \quad (3)$$

where $\theta = 0.3$ and $\Delta t = 60$ seconds. To prevent replay attacks, which involve resubmitting old logs to manipulate reputation, each log is assigned a unique identifier ID_i as in Equation 4.

$$\text{ID}_i = H\big(V_a \parallel V_p \parallel t \parallel H(n_i)\big), \quad (4)$$

Logs are flagged as replayed if their ID_i matches any previously observed identifiers stored in set $\mathcal{S}$.

Once connectivity is restored, vehicles upload filtered logs to IPFS, generating a content identifier (CID) that is recorded on the blockchain. The Edge Coordinator retrieves the CID from the blockchain, verifies the logs, and checks for duplicates or conflicts before updating trust scores. Replay attack protection is also enforced at the blockchain level, and after validation, the Edge Coordinator triggers reward distribution via a smart contract, advancing the reputation system.

III. Experimentation and Result Discussion

We validated the system using a simulated vehicular network of 50 vehicles, each generating 50 interactions with unique blockchain addresses and ECDSA key pairs. Vehicles recorded 1–6 offline events before uploading logs to a local IPFS node. A Solidity smart contract was deployed on a custom proof-of-authority and association blockchain [6]. Figure 2 shows part of a hashed trust log stored locally and uploaded to IPFS.


```
{
  "actor": "V1",
  "peer": "V7",
  "score": 0.2,
  "hash_lock": "b31baf04e267c3603cb88b5ae3d07128cc
  "timestamp": 1754970486,
  "signature": "c30dd249486498d2040e76962795bfc642
  "nonce": "1660c6ab7e1c4cd0af8f267c8f5cdc79",
  "verifier": "V10",
  "verifier_signature": "094e4f7a52c0e0dbe46e3ad76
},
```


Fig. 2: Hashed Trust Log Stored on IPFS

A. Computation Overhead Analysis

The computational costs, including IPFS upload latency, ECDSA signing/verification on vehicle onboard units, blockchain transaction latency, and total end-to-end latency from connectivity to on-chain confirmation, are shown in Figure 3.

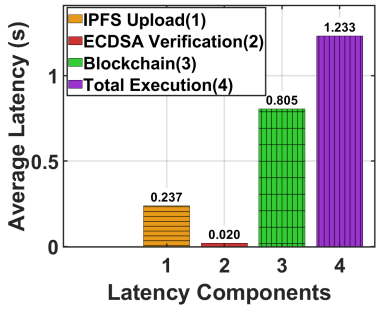

Fig. 3: Average Vehicle Communication System Latency Analysis

B. Security Analysis

We evaluated robustness against replay and conflict attacks during simulated interactions. Table I shows system totals, retained logs, and security filter removals. The smart contract prevents replay attacks by rejecting reused hash locks and duplicate IPFS CIDs, while an offline detector identifies conflicting entries. Invalid logs are filtered before IPFS storage, preventing malicious data from reaching distributed storage or blockchain, thus maintaining data integrity.

TABLE I: System-Wide Performance Summary.

	Initial logs	Filtered logs	Conflicts	Replays	Logs Removed
Total	60	44	6	10	16

IV. Conclusion

The proposed offline trust management for vehicular networks ensures continuity of trust during connectivity disruptions. HTLP, IPFS-based decentralized storage, and blockchain anchorage enable the system to securely maintain and verify trust logs without requiring continuous network access. Experimental results demonstrate its efficiency, with an average processing latency of $1.2s$ and strong security guarantees. Future work aims to develop a fully offline blockchain channel for reputation management.

Acknowledgment

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the IITP grant funded by the Korean government(MSIT) (IITP-2025-RS-2020-II201612, 25%) and by Priority Research Center's Program through the NRF funded by the MEST(2018R1A6A1A03024003, 25%) and by the MSIT, Korea, under the ITRC support program(IITP-2025-RS-2024-00438430, 25%), and by the IITP(Institute of Information & Communications Technology Planning & Evaluation)-ICAN(ICT Challenge and Advanced Network of HRD) grant funded by the Korea government(Ministry of Science and ICT)(IITP-2025-RS-2022-00156394, 25%).

References

[1] H. L. Nakayiza, L. A. C. Ahakonye, D.-S. Kim, and J. M. Lee, "Trust-Aware Relay Selection for Message Delivery to Isolated Malicious Vehicles in V2X Networks," in *Proceedings of Symposium of The Korean Institute of Communications and Information Sciences Summer Conference (KICS SUMMER 2025)*, 06 2025.

[2] S. A. Yusuf, A. Khan, and R. Souissi, "Vehicle-to-Everything (V2X) in The Autonomous Vehicles Domain–A Technical Review of Communication, Sensor, and AI Technologies For Road User Safety," *Transportation Research Interdisciplinary Perspectives*, vol. 23, p. 100980, 2024.

[3] H. L. Nakayiza, L. A. C. Ahakonye, D.-S. Kim, and J.-M. Lee, "Blockchain-Enhanced Feature Engineered Data Falsification Detection in 6G In-Vehicle Networks," *IEEE Internet of Things Journal*, vol. 12, no. 15, pp. 30 036–30 048, 2025.

[4] R. Xing, Z. Su, T. H. Luan, Q. Xu, Y. Wang, and R. Li, "UAVs-Aided Delay-Tolerant Blockchain Secure Offline Transactions in Post-Disaster Vehicular Networks," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 11, pp. 12 030–12 043, 2022.

[5] C. Li, H. Jin, W. Wu, M. Yang, Q. Wang, and Y. Pei, "Path Loss and Auxiliary Communication Analysis of VANET in Tunnel Environments," *Symmetry*, vol. 15, no. 6, 2023.

[6] D.-S. Kim, I. S. Igboanusi, L. A. C. Ahakonye, and G. O. Anyanwu, "Proof-of-Authority-and-Association Consensus Algorithm for IoT Blockchain Networks," in *The 43rd IEEE International Conference on Consumer Electronics (ICCE 2025)*, 2025.