Trust-Aware Relay Selection for Message Delivery to Isolated Malicious Vehicles in V2X Networks

Hope Leticia Nakayiza [1], Love Allen Chijioke Ahakonye [2], Dong-Seong Kim [1] *, Jae Min Lee [1]
[1] IT-Convergence Engineering, *Kumoh National Institute of Technology*, Gumi, South Korea
* NSLab Co. Ltd., Gumi, South Korea, *Kumoh National Institute of Technology*, Gumi, South Korea
[2] ICT Convergence Research Center, *Kumoh National Institute of Technology*, Gumi, South Korea
(hopeleticia, loveahakonye, dskim, ljmpaul)@kumoh.ac.kr

***Abstract*—Compromised vehicles are often quarantined by intrusion detection systems (IDS) to prevent further attacks. Previous research has been done to ensure that compromised vehicles continue to receive time-critical safety updates in this state by using benign vehicles as relays but does not address how to securely select reliable relays. This paper presents a hybrid trust-based relay selection framework that enables safe and verifiable message forwarding using trustworthy benign vehicles selected as relays.**

***Index Terms*—Malicious Vehicles, Relay, Trust Model, Vehicle-to-Everything (V2X)**

I. Introduction

Vehicle-to-Everything (V2X) networks enable critical real-time communication for intelligent transport systems [1]. However, they face reliability challenges under adversarial or disconnected scenarios, particularly when intrusion detection systems (IDS) isolate compromised vehicles, thereby preventing them from receiving mission-critical updates [2]. Building on our previous work [3] that introduced message relaying to compromised vehicles via benign vehicles, this study proposes a trust-based relay selection framework to evaluate candidate vehicles using dynamic, off-chain trust scores anchored on-chain via a permissioned blockchain network, PureChain that is based on a proof of authority and association (PoA^2) consensus mechanism [4]. Figure 1 shows the proposed system model and workflow.

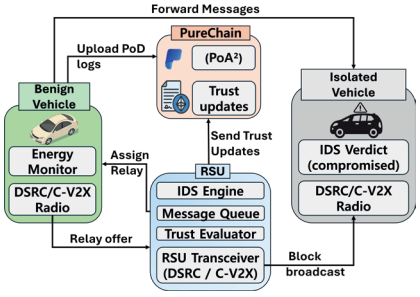

Fig. 1: Proposed System Model and Workflow

II. System Methodology

A. Message Broadcast and Queuing

Vehicles, V_i periodically broadcast safety messages signed using their private ECDSA key k_i to the nearest roadside unit (RSU). When a vehicle is determined to be malicious by the IDS, it is flagged as compromised V_c and temporarily isolated from the network with direct participation revoked. The RSU queues all incoming messages for V_c and leverages benign vehicles V_i to deliver messages to V_c since V_c can only receive messages but not send.

B. Relay Offer, Off-Chain Trust Score Computation, and Relay Selection

Benign vehicles, V_i overhear the RSU's relay-request beacon and respond with a relay-offer frame containing their pseudonym VID_i, current battery level E_i, and a signed timestamp. Every RSU maintains a time-varying trust score $\tau_i \in [0,1]$ for each candidate relay. Five normalized evidences considered so that recent, reliable behavior dominates long-term reputation using the Equation 3.

$$\tau_i = w_1\,\mathrm{SR}_i + w_2(1-\mathrm{PLR}_i) + w_3\,\mathrm{PoD}_i + w_4\,\mathrm{IND}_i - w_5\,e^{-\lambda\,\mathrm{AGE}_i} \tag{1}$$

where SR_i is the successful-relay ratio, PLR_i the packet-loss rate, PoD_i the fraction of valid proofs of delivery, IND_i indirect feedback from neighbouring RSUs, and AGE_i the time since the last interaction.

The RSU evaluates all relay candidates based on a composite score as shown in Equation 2.

$$s_i = \alpha \cdot \tau_i + \beta \cdot \mathrm{LQ}_i - \gamma / E_i. \tag{2}$$

where τ_i is the current trust score of candidate V_i, LQ_i is predicted link quality, and E_i is the remaining energy. The weights α, β, and γ allow prioritization between trustworthiness, communication efficiency, and energy preservation.

C. On-Chain Trust Anchoring, Encrypted Message Forwarding and proof-of-delivery (PoD) Generation

Once the new trust score τ_i is computed, the RSU sends it to the blockchain as $setTrust(\mathrm{VID}_i, \tau_i)$. The new trust score triggers a trust change event on the blockchain, allowing other RSUs to verify the update. This ensures a consistent, auditable, and tamper-resistant view of trust values across the network.

Upon selection as a relay, V_i becomes V_r and receives an encrypted message $C = \mathrm{AES}k_s(M)$, to forward to V_c. Upon receipt, V_c verifies the V_r's authenticity and message integrity using V_r's public ECDSA key. Once successfully verified, V_c

returns a PoD signed with its own private key k_c as shown in Equation 3.

$$\text{PoD} = \text{ECDSA}k_c(\text{hash}(C)||\text{timestamp}) \quad (3)$$

The RSU validates this PoD for authenticity using V_c's public key and timeliness if the delivery delay is within bounds.

III. Experimentation and Performance Evaluation

The system is evaluated in a discrete-event simulation environment using SimPy, with blockchain interactions implemented via Web3.py on the PureChain network. Other simulation parameters considered are depicted in Table I.

TABLE I: Simulation Parameters

Parameter	Value
Simulation Duration	600 s
Fleet size (Benign Vehicles)	100
Initial Energy (E_i)	1000kJ
Relay Cost (Energy drain)	50 kJ per relay forwarding
Energy Penalty	0.5
Link Quality (LQ_i)	0.5∼1
Relay Selection Weights (α, β, γ)	0.5, 0.35, 0.15
Trust weights w1 - w5	0.35, 0.25, 0.20, 0.15, 0.05
Trust-age decay rate (λ)	0.02
Latency deadline	500 ms

The top five relay vehicles were analyzed across energy consumption (Figure 2), trust evolution (Figure 3), and Successful Delivery Rate (SDR) (Table II). Vehicle V34 was the most active relay, with 46 attempts and a 73.91% SDR, resulting in a sharp trust increase but significant energy depletion. In contrast, V29 had only two attempts and was able to maintain energy but gained little trust due to limited involvement. These results show that the system effectively rewards consistent, reliable relays while discouraging inactivity or overuse.

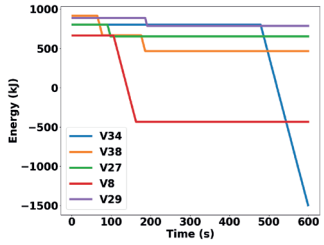

Fig. 2: Energy Consumption by Relays

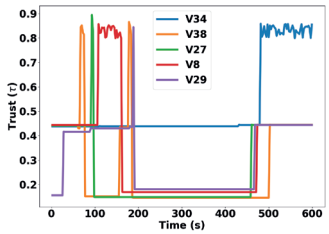

Fig. 3: Relay Trust Evolution

The average time taken to log trust updates on the blockchain using the $setTrust$ function and to retrieve them using $getTau$ was also evaluated to assess PureChain's efficiency. As shown in Figure 4, both exhibited low latency, supporting near real-time relay decisions.

TABLE II: SDR for the Top 5 Relay Vehicles

Vehicle ID	Attempts	Successes	SDR (%)
V34	46	34	73.91
V38	9	8	88.89
V27	3	2	66.67
V8	22	19	86.36
V29	2	2	100

Fig. 4: Average Blockchain Latency

IV. Conclusion

This study proposed a hybrid on-chain reputation trust-based framework system that selects reliable relays for forwarding critical messages to isolated malicious vehicles to improve message availability and timeliness. Future work will integrate mobility-aware trust decay and empirical evaluation using real-world simulation tools..

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 & Coummunications 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, "Homomorphic encryption for privacy-preserving misbehavior detection in the internet of vehicles," in *2025 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, 2025, pp. 0320–0324.

[2] H. Nakayiza, L. Ahakonye, D.-S. Kim, and J. M. Lee, "Blockchain-Enabled Intrusion Detection System for Distributed Vehicular Networks," in *The Korean Institute of Communications and Information Sciences Summer Conference (KICS)*, 11 2024, pp. 463 – 464.

[3] H. N. Leticia, L. Ahakonye, D.-S. Kim, and J. M. Lee, "Secure Message Delivery Protocol for Isolated Compromised Vehicles in V2X Networks," in *The 35th Joint Conference On Communications And Information (JCCI)*, 04 2025.

[4] 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.