Blockchain and AI-Enabled Trust Management Model for Internet of Vehicles

Mahalinoro Razafimanjato, Haishan Yang, Seri Park, Sunghyun Kim, Dongkyun Kim
School of Computer Science and Engineering, Kyungpook National University, Republic of Korea
{*mahaly, yanghs158, psr0527, sunghyunkim, dongkyun*}@knu.ac.kr

***Abstract*—The Internet of Vehicles (IoV) is a distributed network where connected vehicles and roadside units communicate seamlessly with one another and surrounding infrastructure. While this network facilitates enhanced inter-vehicular communication, its open and dynamically changing topology makes it vulnerable to the presence of malicious vehicles. These vehicles can transmit false and inaccurate messages, leading to severe, potentially life-threatening consequences for road users and compromising overall network security. Furthermore, the temporary and unreliable vehicle interaction can aggravate trust issues, hindering effective decision-making. However, existing trust management systems fall short of meeting the evolving demands of IoV, particularly in terms of accuracy, scalability, and real-time performance. We propose a novel trust management model for IoV to address these challenges. The model employs a Random Forest-based vehicle trust model to detect misbehavior and a data trust model using the Dempster-Shafer Theory to aggregate trust ratings from neighboring vehicles, comprehensively assessing event credibility. The final trust scores are securely stored on a permissioned blockchain using Hyperledger Fabric, ensuring the integrity of the trust scores while optimizing latency and throughput. The model's scalability and efficiency are validated through rigorous testing, significantly advancing IoV trust management.**

***Index Terms*—Blockchain, trust management, internet of vehicles, machine learning**

I. Introduction

In recent years, the advancement of technologies such as next-generation wireless communication, sensor technology, and intelligent transportation technology has paved the way for the emergence of the Internet of Vehicles (IoV) to enhance traffic efficiency, driving safety, and convenience for road users. IoV is a self-organizing and inter-vehicular communication network in which the nodes consist of roadside units (RSU) and vehicles equipped with onboard units (OBU) [1]. These vehicles can communicate and exchange messages with other vehicles through vehicle-to-vehicle (V2V), with RSUs through vehicle-to-infrastructure (V2I), or with pedestrians through vehicle-to-pedestrian (V2P) communications.

Vehicles and RSUs periodically send messages that generally contain road conditions (such as road congestion, accident conditions, and hazardous weather conditions) and vehicle conditions (such as vehicle location, speed, and direction) to help awareness of the current road situation and improve safety [1], [2]. However, due to the open nature and dynamically changing topology characteristics of IoV, the presence of malicious vehicles can cause the transmission of false and inaccurate messages, which may result in severe life-threatening consequences for road users and compromise the security of the network [3]. Additionally, the communication between vehicles is temporary and unreliable, which may result in a lack of trust between entities and affect normal decision-making of the vehicles [4], [5].

Although cryptographic-based security mechanisms can address security issues and resist external attackers through authorization and authentication, they cannot protect against internal attackers that bypass security checks [6]–[8]. In addition, they cannot assess the trustworthiness of the entities or verify the reliability of the exchanged messages. Therefore, to ensure the trustworthiness of vehicles and the reliability of messages, many researchers have proposed various trust management systems [2], [3], [9]–[11] for IoV to detect malicious or selfish nodes by assigning and evaluating entities and messages through trust scores.

Among proposed solutions, blockchain and learning approaches have been employed for robust and adaptive trust models. Blockchain is a distributed ledger technology with several properties, such as decentralization, consistency, tamper-proofing, and transparency, making it suitable for trust management in IoV [12], [13]. Due to the blockchain's tamper-proofing nature, any data tampering attempt made by malicious nodes is effectively prevented (e.g., intentionally modifying the trust score of a vehicle). On the other hand, given the highly dynamic environment of IoV, an accurate assessment of messages and vehicles' trustworthiness is a foremost requirement. Consequently, learning approaches can effectively increase the accuracy of the trustworthiness computation (e.g., inferring the trust score of a vehicle based on its vehicular data or broadcast messages) [8].

Combined with learning approaches, blockchain presents several advantages and is widely considered to enhance security and trust within IoV. However, existing blockchain-based and AI-integrated trust models prioritize the learning model capabilities while overlooking the impact of the blockchain's performance within their scheme. This emphasis often leads to insufficient testing and optimization of critical blockchain performance scalability metrics, including throughput and latency. As a result, the blockchain's ability to handle large volumes of transactions and data in real-time scenarios is compromised, limiting their applicability in IoV [14]. In addition, existing solutions are heavily relying on learning approaches to determine trust scores automatically. Although

they have shown promising results, these approaches often do not capture sufficient features to compute accurate trust score values for individual nodes, affecting the reliability of trust assessments, thus leading to a discrepancy between the computed trust values and the actual trustworthiness of the nodes [8].

This paper proposes a novel trust management model to address the above challenges. Its main contributions can be summarized as follows.

- We leverage HyperLedger Fabric (HLF) for secure and immutable storage of vehicle trust scores, utilizing its high throughput and low latency capabilities to ensure efficient and reliable trust management in dynamic environments. Our model uses smart contracts to automate the verification and update of trust scores.
- We use a Random Forest Classifier in our vehicle trust model for effective misbehavior detection, chosen for its high accuracy, resilience to overfitting, and capability to handle complex datasets common in vehicular networks. This model enables our system to accurately and swiftly identify malicious or misbehaving vehicles.
- We incorporate the Dempster-Shafer Theory (DST) in our data trust model to further enhance the credibility assessment of events from neighboring vehicles. DST provides a flexible and robust framework for reasoning under uncertainty, allowing our model to assess the credibility of events with high precision, even in the presence of conflicting evidence.

The remainder of this paper is structured as follows. Section II reviews the related works. Section III introduces the overview of the architecture and the threat model. Section IV presents the trust management model in detail. Section V discusses the experimental results and analysis in more detail in Section VI. Finally, Section VII concludes this paper.

II. Related Works

Various research studies have recently been conducted on trust management systems in the IoV environment. Many researchers have already combined blockchain with learning-based approaches in trust management.

Zhao et al. [5] proposed a trust model using a Gaussian Naive Bayes classifier to detect malicious vehicles and active detection technology to update trust values through collaboration between vehicles and RSUs. Their solution employs a hybrid consensus algorithm that merges Delegated Proof of Stake with Byzantine Fault Tolerance, aiming to enhance the efficiency of block generation and updating trust within the blockchain. HS in [15] proposed a blockchain-based reputation management system that employs a self-sovereign digital identity management system using HLF, ensuring interoperability and privacy through verifiable pseudo-identities. They propose a 'Proof of Trust' (PoT) consensus mechanism, combining Proof of Stake with random leader election, where RSU grades serve as the stake. Additionally, Bayesian inference is employed to estimate the truthfulness of nodes, enabling distributed reputation management within the network. Zhang et al. [2] proposed a blockchain-based trust management system that employs a Feedforward Neural Network to dynamically and automatically assess the trust scores of vehicles, RSUs, and messages, which does not rely on a traditional fixed formula. Wang et al. [3] utilize a public blockchain combined with a fully connected network (FCN) deep learning model. The system uses a Proof-of-Trust consensus algorithm to enhance blockchain performance by prioritizing high-trust vehicles and speeding up data processing. The FCN model, implemented on roadside units (RSUs), efficiently verifies message authenticity by analyzing vehicle attributes and historical behavior to detect malicious activities. Haddaji et al. [16] proposed FBTM, a blockchain-based trust model combined with Federated Learning (FL), to improve data quality for model training. The Proof of Reputation consensus assigns reputation scores to RSUs while motivating them to generate and aggregate global FL models.

These solutions address key challenges in trust management systems by ensuring accurate and efficient trust evaluation, enhancing security, and promoting participation by integrating blockchain and learning techniques.

III. Architecture Overview

This section introduces the overall architecture, HLF, and the threat model adopted in this paper. The network architecture follows a typical IoV network consisting of entities such as RSUs and vehicles depicted in Fig. 1. The IoV entities are assumed to perform local data processing and have storage capabilities. They can communicate wirelessly through IEEE 802.11p/DSRC. Additionally, RSUs represent nodes that maintain the blockchain. They verify and evaluate the vehicles' trust scores.

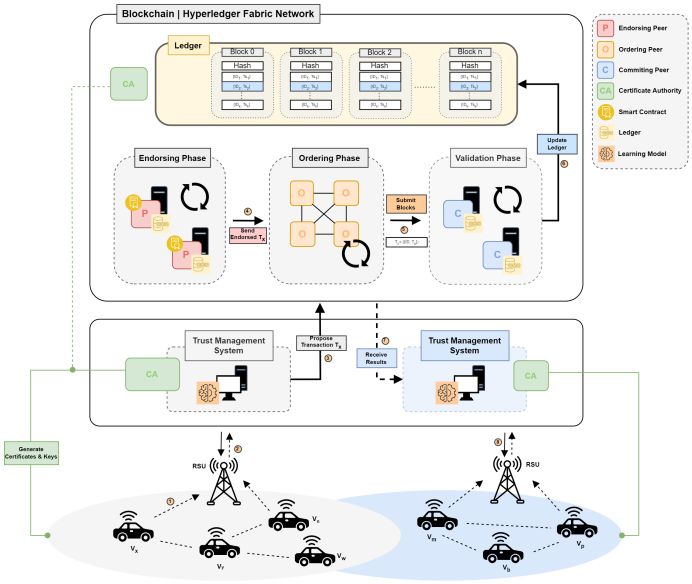

Fig. 1. System model

A. HyperLedger Fabric Network (HLF)

HyperLedger Fabric (HLF) is a permissioned blockchain platform with a highly configurable architecture for executing, ordering, and validating transactions. Fig. 1 illustrates the structure and flow of HLF-enabled IoV, where trust score updates are managed through the following phases:

- Endorsing Phase: A transaction proposal is generated to update the trust score of a vehicle. Selected peers execute the specified smart contract to assess the proposal, producing signed responses. These responses are aggregated into a transaction envelope, along with read-write sets that capture the state of the ledger before and after the transaction.
- Ordering Phase: The transaction envelope is submitted to the ordering service. In our case, we use the Raft consensus mechanism. The ordering service sequences the transactions, packages them into blocks, and distributes these blocks to all peers in the network.

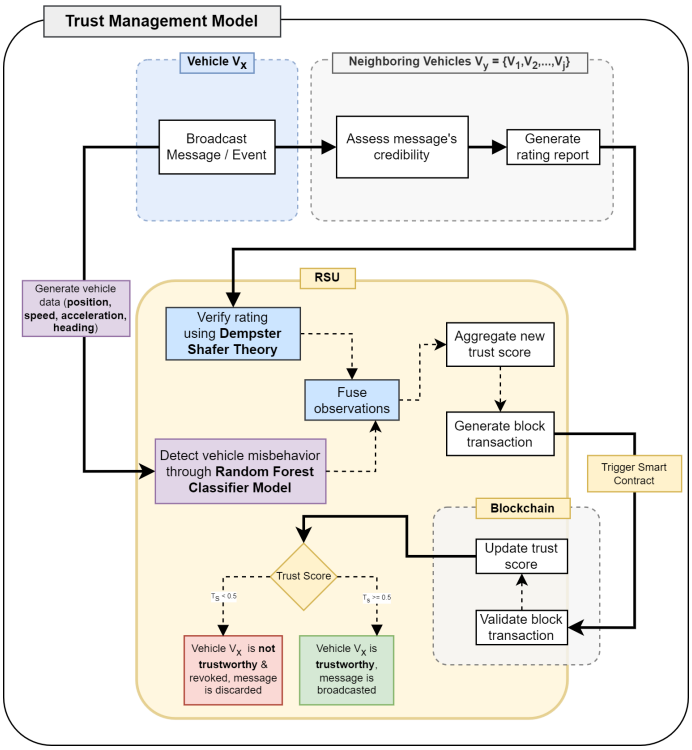

Fig. 2. Trust Management Process

- Validation Phase: Each peer validates the transactions by verifying the endorsements and ensuring compliance with endorsement policies. Valid transactions are committed to the channel ledger, updating the world state. Then, a commit status is communicated to confirm the ledger update.

B. Threat Model

In this paper, we assume the vehicles could be vulnerable to attacks performed by malicious nodes within the network.The main attacks we considered within our proposed scheme are as follows:

- Bogus Information Attack: Malicious attackers' primary goal is to broadcast false messages. Attackers might flood the network with an excessive number of false messages, which can affect the stability and security of the network. In our trust model in Section IV, the assessment of event credibility limits malicious vehicles from sending false messages to the network.
- Bad-Mouthing Attack: Attackers might try to provide false ratings to messages to promote or discredit other vehicles. This type of attack could revoke genuine vehicles, disrupting the normal flow within the network. To avoid such behavior, assessing behavior and events to derive the final trust score provides fair judgment.
- Tampering Trust Data: Malicious vehicles might attempt to tamper with trust values to undermine the integrity of the network. This type of attack could compromise the reliability of the trust assessments, which can destabilize the network's security. To avoid such attacks, we leverage blockchain in our architecture. Its decentralized and immutable characteristics ensure that tampering with trust data is nearly impossible.

IV. Trust Management Model

In this section, we present a comprehensive step-by-step explanation of our proposed trust management model, as depicted in Fig. 2.

A. Data Trust Model - Event Rating

Let v_i be the vehicle broadcasting an event/message E and $\{v_1, v_2, \ldots, v_n\}$ be its neighboring vehicles providing a set of reports $\{R_1, R_2, \ldots, R_n\}$ about the message's trustworthiness. Each neighbor vehicle v_j provides a report $r_j \in \{0, 1\}$, where 1 indicates that E is trustworthy and 0 indicates that E is untrustworthy. Each vehicle v_j also has a trust score $t_j \in [0, 1]$, which represents its reliability.

DST is used to compute and aggregate the reports from all the neighboring vehicles. From this, DST includes a frame of discernment θ containing two elements, namely $\Theta = \{T, \bar{T}\}$. T indicates that E is trustworthy. $\bar{T}$ indicates that E is untrustworthy. Hence, there are three propositions:

$$H = \{T\} \quad (E \text{ is trustworthy}) \tag{1}$$

$$\bar{H} = \{\bar{T}\} \quad (E \text{ is untrustworthy}) \tag{2}$$

$$U = \{T, \bar{T}\} \quad (E \text{ is trustworthy or untrustworthy}) \tag{3}$$

For vehicle v_j, the basic probability assignment is adjusted based on its report and trust score as follows:

$$m_j(H) = t_j \cdot r_j \tag{4}$$

$$m_j(\bar{H}) = t_j \cdot (1 - r_j) \tag{5}$$

$$m_j(U) = 1 - t_j \tag{6}$$

If the RSU receives k event rating reports on vehicle v_i, to combine the evidence from all neighboring vehicles, Dempster's rule of combination is used whereby the trustworthiness of the E is defined by the belief function as follows:

$$\text{Bel}(H) = m(H) = \oplus_{j=1}^{k} m_j(H) \tag{7}$$

In this case, the received reports k from the set of neighbors is calculated from:

$$\text{Bel}(H) = m_1(H) \oplus m_2(H) \oplus \cdots \oplus m_j(H) \tag{8}$$

Further, using the Dempster's rule of combination to combine the trustworthiness is given by:

$$m(H) = \frac{\sum_{H_1 \cap H_2 \cap \cdots \cap H_j = H} \prod_{j=1}^{k} m_j(H)}{1 - \sum_{H_1 \cap H_2 \cap \cdots \cap H_j = \emptyset} \prod_{j=1}^{k} m_j(H)} \tag{9}$$

In this paper, we assumed that if $Bel(H) > Bel(\bar{H})$, the event E is considered trustworthy, while $Bel(H) < Bel(\bar{H})$, the event E is considered untrustworthy.

B. Vehicle Trust Model - Misbehavior Detection

Once the vehicle transmits a message to neighboring vehicles, this module collects the state of the vehicle data in this step to build the behavior feature of the vehicle. Then, it uses the trained Random Forest classifier to determine whether the vehicle is misbehaving or genuine. The vehicle behavior feature is formatted as follows:

$$X = (p_x, p_y, s_x, s_y, v_x, v_y, h_x, h_y) \tag{10}$$

where p represents the position, s the speed, v the acceleration, h the heading of the vehicle on the x and y axis.

C. Trust Value Computation

Upon receiving the results from the classification from Random Forest and analysis from DST, the observations will be fused to form a new trust score. The updated trust value T_new for a vehicle is calculated based on its previous trust value T_old, the classification results C from the vehicle trust model, the probability D from the data trust model, and defined thresholds β and α.

For $C = 0$ (Normal Behavior):

$$T_{\text{new}} = \begin{cases} T_{\text{old}} + w_{\text{H}} & \text{if } D \geq \alpha \\ T_{\text{old}} + w_{\text{L}} & \text{if } \beta < D < \alpha \\ T_{\text{old}} + p_{\text{M}} & \text{if } D \leq \beta \end{cases} \tag{11}$$

For $C = 1$ (Misbehavior Detected):

$$T_{\text{new}} = \begin{cases} T_{\text{old}} + p_{\text{L}} & \text{if } D \geq \alpha \\ T_{\text{old}} + p_{\text{M}} & \text{if } \beta < D < \alpha \\ T_{\text{old}} + p_{\text{H}} & \text{if } D \leq \beta \end{cases} \tag{12}$$

where:

- w_{H} and w_{L} are weights for increasing trust (high, low).
- $p_{\text{L}}, p_{\text{M}}, p_{\text{H}}$ are penalties for decreasing trust (low, moderate, high).
- α and β are high and low thresholds, respectively.

D. Trust Score Storage through HLF

Once the classification and DST analysis results are available, transactions are proposed on the blockchain, which triggers the smart contract in the HLF. Algorithm 1 displays the detailed procedure for updating the trust score function of the smart contract. In addition, we employ the Raft consensus algorithm designed for efficiency and scalability, using a leader-based approach for consensus. Transactions, submitted as proposals, are automatically routed by the ordering node to the channel's current leader. After validation, they are ordered, packaged into blocks, consented upon, and distributed. These blocks are then sent to committing peer nodes for validation and recorded in the ledger. These processes align with the second and third phases of our transaction flow, ensuring the system can quickly and reliably update trust values while maintaining security and integrity.

Algorithm 1 Update Trust Score

Require: Vehicle ID id, Trust Score $tscore$
Ensure: Update the trust score of the vehicle with ID id in the ledger
Check if the vehicle with ID id exists in the system
if vehicle does not exist **then**
  return "The vehicle with ID id does not exist"
end if
Update the vehicle record with the new trust score
Store the updated vehicle record in the ledger
if storing fails **then**
  return "Failed to update the vehicle's trust score in the ledger"
end if
return "Trust score updated successfully"

V. Experimentation & Results

A. Experimental Setup

To evaluate the feasibility of our proposed solution, we implemented the HLF blockchain network on a virtual machine with a 2.50-Ghz Intel Core i5-12400 processor, 32 GB 3200-MHz DDR4 RAM, and Ubuntu-22.04.4 LTS(64-bit), which consists of 4 ordering nodes and 5 peer nodes. The smart contract was developed using the Go language and deployed on HLF. Hyperledger Caliper was used to measure the performance of our blockchain implementation. The vehicular simulation and misbehavior detection were conducted using Python.

To train and test our random forest model, we used the VeReMi extension dataset [17]. The VeReMi dataset comprises various position and speed malfunctions as well as attacks. This dataset is generated using VEINS, based on the OMNET++ network simulator and the SUMO road traffic simulator. The dataset utilizes vehicle traces from a subsection of the Luxembourg SUMO Traffic (LuST) scenario, with an area size of 1.61 km² and a vehicle density of 67.4 vehicles/km². The dataset was further processed and formatted to fit our machine

learning model. The source code for our implementation can be found in our GitHub repository [18].

B. Experimental Results & Analysis

To test the efficacy of our machine learning model in detecting misbehaving vehicles, the analysis was carried out on different network sizes and proportions of malicious vehicles. We evaluated the performance of the model in networks of 100, 200, and 400 vehicles with varying percentages of malicious vehicles: 20%, 30%, and 50%. The primary metric for evaluating model performance was the True Positive Rate (TPR), which shows the proportion of correctly predicted malicious vehicles to the total number of actual malicious vehicles. As shown in Fig. 3, we can see that the model performs well in scenarios where the proportion of malicious vehicles exceeds 50% across all network sizes. This suggests that the model is particularly effective when malicious behavior is more prevalent.

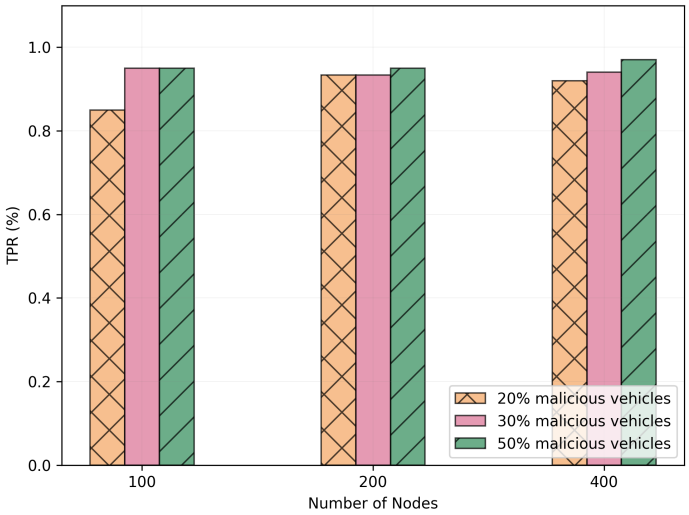

Fig. 3. TPR with different number of vehicles under different ratio of malicious vehicles

To validate the efficacy of our trust model (integrated scheme using DST and Random Forest Classifier), we also simulate the change in average trust scores over a time span of 200 units. During each time span, we assumed that 10 distinct events occurred, and for each event, 5 neighboring vehicles evaluated the broadcasting vehicle's message. The simulation involved a network of 400 vehicles subjected to varying ratios of malicious vehicles: 20%, 30%, and 50%. The initial trust score of each vehicle is set between 0.7 to 0.8. The weight parameters used for the final trust computation function are described in Table I. As shown in Fig. 4, the simulation outcomes demonstrate the trust scores for genuine vehicles remained high and stable, indicating the system's accuracy in preserving the reputation of genuine vehicles. In the case of malicious vehicles spreading false messages, their trust scores consistently decrease over time, reflecting the model's ability to detect and penalize malicious vehicles.

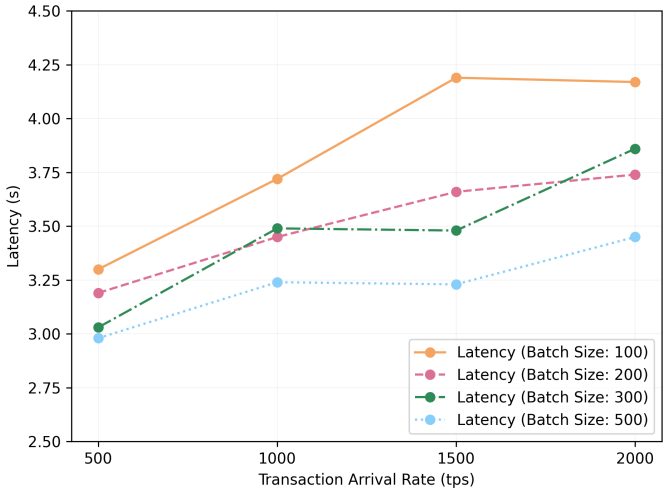

Fig. 4. Latency with different transaction arrival rate under different batch size

To assess the scalability of the blockchain network, we evaluated two key performance metrics: latency and throughput. These were measured across four different batch sizes (100, 200, 300, 500) and transaction arrival rates ranging from 500 to 2000 transactions per second. During this experiment, due to the limitation of our computer, we limited the number of vehicles accessing the blockchain to 20. As shown in Fig. 5, smaller batch sizes result in higher latency as more transactions are processed progressively. This is likely due to the increased complexity and time required to validate larger batches of transactions. As for the throughput depicted in Fig.

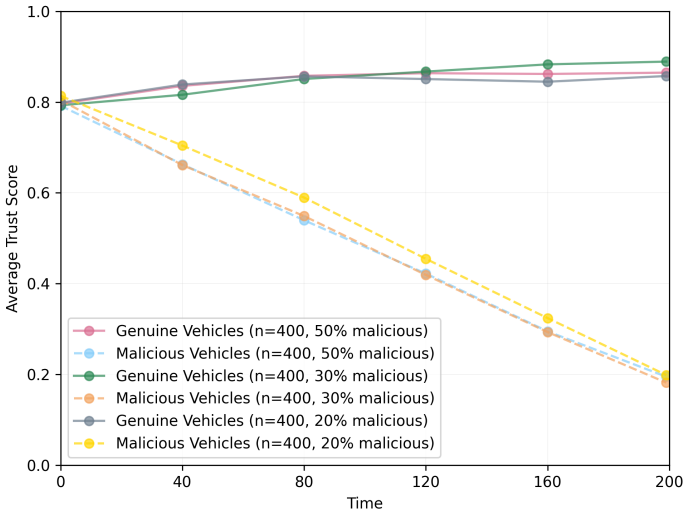

Fig. 5. Change of average trust scores under different ratio of malicious vehicles

6, we can see that the throughput consistently rises with the batch size, which illustrates that the blockchain can handle more transactions as batch size increases and transaction rates are higher. This suggests the blockchain network may

work efficiently with 600 transactions per second and below. Although the ability of the blockchain to maintain increased throughput with larger batch sizes and higher transaction rates indicates good scalability, it is necessary to find an optimal batch size with quick response time despite a slight reduction in throughput.

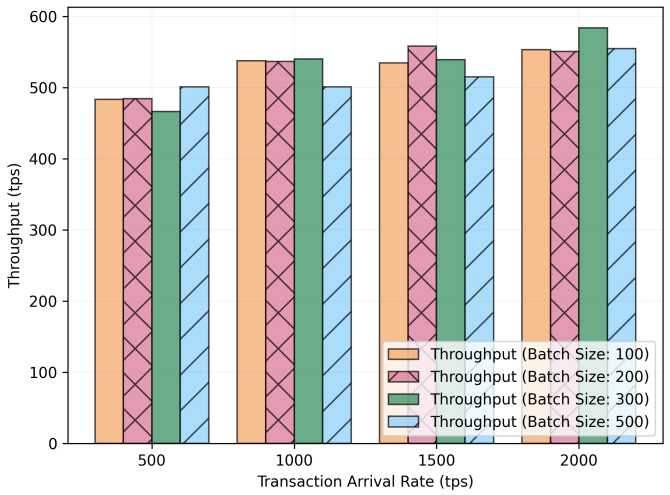

Fig. 6. TPS with different transaction arrival rate under different batch size

VI. Conclusion & Future Works

In this paper, we proposed a novel trust management model for IoV. By leveraging HLF's performance and scalability, our approach addresses the limitations of existing blockchain-based models, ensuring timely and secure data processing critical for the IoV environment. This proposed model integrates a vehicle trust model, employing a random forest classifier for effective misbehavior detection, and a data trust model, utilizing DST for event credibility evaluation. This dual approach provides a comprehensive measure of trustworthiness by integrating the results of classification and DST analysis, thereby overcoming the limitations of previous models that rely solely on learning algorithms. This model effectively captures essential features to compute accurate trust scores, aligning the computed values more closely with the actual trustworthiness of nodes and enhancing the reliability of trust assessments in the IoV environment. Future research will enhance the model's accuracy and efficiency of trust assessments through additional learning techniques, particularly in dynamic and heterogeneous IoV environments with extensive model support for more complex scenarios. Further testing and optimization of the HLF network in large-scale scenarios could further demonstrate and validate its performance under varying traffic conditions.

Acknowledgment

This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant NRF-2018R1A6A1A03025109. This work was also supported in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant NRF-RS-2018-NR031059.

References

[1] H. Che, Y. Duan, C. Li, and L. Yu, "On trust management in vehicular ad hoc networks: A comprehensive review," *Frontiers in the Internet of Things*, vol. 1, p. 995233, 2022.

[2] C. Zhang, W. Li, Y. Luo, and Y. Hu, "Ait: An ai-enabled trust management system for vehicular networks using blockchain technology," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3157–3169, 2020.

[3] S. Wang, Y. Hu, and G. Qi, "Blockchain and deep learning based trust management for internet of vehicles," *Simulation Modelling Practice and Theory*, vol. 120, p. 102627, 2022.

[4] Y. Zhang, C. Lv, C. Cheong, and Y. Cao, "An introduction to trust management in internet of vehicles," in *Communication, Computation and Perception Technologies for Internet of Vehicles*, pp. 245–260, Springer, 2023.

[5] J. Zhao, F. Huang, L. Liao, and Q. Zhang, "Blockchain-based trust management model for vehicular ad hoc networks," *IEEE Internet of Things Journal*, 2023.

[6] A. Hbaieb, S. Ayed, and L. Chaari, "A survey of trust management in the internet of vehicles," *Computer Networks*, vol. 203, p. 108558, 2022.

[7] S. A. Siddiqui, A. Mahmood, Q. Z. Sheng, H. Suzuki, and W. Ni, "A survey of trust management in the internet of vehicles," *Electronics*, vol. 10, no. 18, p. 2223, 2021.

[8] R. Abidi, N. B. Azzouna, W. Trojet, G. Hoblos, and N. Sahli, "A study of mechanisms and approaches for iov trust models requirements achievement," *The Journal of Supercomputing*, vol. 80, no. 3, pp. 4157–4201, 2024.

[9] C. Zhang, K. Chen, X. Zeng, and X. Xue, "Misbehavior detection based on support vector machine and dempster-shafer theory of evidence in vanets," *IEEE Access*, vol. 6, pp. 59860–59870, 2018.

[10] S. Srivastava, D. Agarwal, B. K. Chaurasia, and M. Adhikari, "Blockchain-based trust management for data exchange in internet of vehicle network," *Multimedia Tools and Applications*, pp. 1–19, 2024.

[11] S. Gyawali, Y. Qian, and R. Q. Hu, "Machine learning and reputation based misbehavior detection in vehicular communication networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 8871–8885, 2020.

[12] Y. Liu, J. Wang, Z. Yan, Z. Wan, and R. Jäntti, "A survey on blockchain-based trust management for internet of things," *IEEE internet of Things Journal*, vol. 10, no. 7, pp. 5898–5922, 2023.

[13] E. Alalwany and I. Mahgoub, "Security and trust management in the internet of vehicles (iov): Challenges and machine learning solutions," *Sensors*, vol. 24, no. 2, p. 368, 2024.

[14] S. Abbasi, N. Khaledian, and A. M. Rahmani, "Trust management in the internet of vehicles: a systematic literature review of blockchain integration," *International Journal of Information Security*, pp. 1–24, 2024.

[15] J. HS, "Reputation management in vehicular network using blockchain," *Peer-to-Peer Networking and Applications*, vol. 15, no. 2, pp. 901–920, 2022.

[16] A. Haddaji, S. Ayed, and L. Chaari, "Federated learning with blockchain approach for trust management in iov," in *International Conference on Advanced Information Networking and Applications*, pp. 411–423, Springer, 2022.

[17] J. Kamel, M. Wolf, R. W. Van Der Hei, A. Kaiser, P. Urien, and F. Kargl, "Veremi extension: A dataset for comparable evaluation of misbehavior detection in vanets," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2020.

[18] R. Mahalinoro, "hrdt-tms-bc." 2024, gitHub repository. [Online]. Available: https://github.com/Mahalinoro/hrdt-tms-bc.