This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3279950

A Computational Model for Reputation and Ensemble-Based Learning Model for Prediction of Trustworthiness in Vehicular Ad Hoc Network

Abdullah Alharthi, Qiang Ni, Richard Jiang and Mohammad Ayoub Khan

***Abstract*—Vehicular ad hoc networks (VANETs) are a special kind of wireless communication network that facilitates vehicle-to-vehicle(V2V) and vehicle-to-infrastructure(V2I) communication. This technology exhibits the potential to enhance the safety of roads, efficiency of traffic, and comfort of passengers. However, this can lead to potential safety hazards and security risks, especially in autonomous vehicles that rely heavily on communication with other vehicles and infrastructure. Trust, the precision of data, and the reliability of data transmitted through the communication channel are the major problems in VANET. Cryptography-based solutions have been successful in ensuring the security of data transmission. However, there is still a need for further research to address the issue of fraudulent messages being sent from a legitimate sender. As a result, in this study, we have proposed a methodology for computing vehicle's reputation and subsequently predicting the trustworthiness of vehicles in networks. The blockchain records the most recent assessment of the vehicle's credibility. This will allow for greater transparency and trust in the vehicle's history, as well as reduce the risk of fraud or tampering with the information. The trustworthiness of a vehicle is confirmed not just by the credibility, but also by its network behavior as observed during data transfer. To classify the trust, an ensemble learning model is used. In depth tests are run on the dataset to assess the effectiveness of the proposed ensemble learning with feature selection technique. The findings show that the proposed ensemble learning technique achieves a 99.98% accuracy rate, which is notably superior to the accuracy rates of the baseline models.**

***Index Terms*— Reputation, Trust, VANET, Machine Learning**

I. INTRODUCTION

VANET is a mobile ad hoc network whose topology is continuously changing as vehicles join and leave the network. VANETs are designed to help with the following kinds of applications: safety and non-safety. The safety applications are meant to alert in order to avoid harm and reduce risk [1, 2]. Non-safety applications include details about products and services, the position of the closest restaurant, petrol facility, or the fastest path to the intended location. The two primary kinds of VANET equipment are road-side units (RSUs) and on-board units (OBUs). RSU is located on the roadside, and OBUs are installed within vehicles. Vehicle-to-vehicle communications (V2V) refer to connectivity among vehicles, whereas vehicle-to-infrastructure communications (V2I) refer to links between vehicles and infrastructure [3, 4]. Current VANET addresses privacy and security concerns, however they fail to specify methods to evaluate the characteristics of registered vehicles. A legitimate vehicle, for example, can send incorrect information to a central supervision unit, leading to generate an incorrect action. Consequently, VANETs necessitate the creation of a reputable and trustworthy system. A vehicle's interaction to other vehicles could be determined via a decentralized trust management system [5]. Through the implementation of a trust management framework that relies on reputation and identity evaluation, it is possible to compensate trustworthy vehicles and warn malicious vehicles in VANETs, ensuring message transmission that is trustworthy. The centrally located and decentralized trust models are two broad types. A centralised server manages confidence in the centralised topology [6-7]. In contrast, the management of a centralized server requires significant resources and is susceptible to malicious attacks that can result in significant issues due to the presence of single-points-of-failure (SPOF). Many authors [8–10] have attempted to overcome these concerns by utilizing a decentralized design whereby trust is evaluated through RSUs instead of a centralized supervision unit. By developing a system where each RSU's communication ranges are mainly tasked with trust management, the decentralized approach has overcome the problem of single-points-of-failure. In their efforts to ensure the reliability of disseminated data, VANETs face crucial and complex security challenges [11, 12]. Several investigations aimed at enhancing VANET security have been undertaken [13-16], however there has been an improvement into examinations and studies into strategies for identifying fraudulent information. A node that is

Abdullah Alharthi is with the College of Computing and Information Technology, University of Bisha, Bisha, Saudi Arabia (amallharthy@ub.edu.sa). He was a doctoral candidate with the School of Computing and Communication, Lancaster University, Lancaster, United Kingdom (e-mail: a.m.alharthi@lancaster.ac.uk).

Qiang Ni is with the School of Computing and Communication, Lancaster University, Lancaster, United Kingdom (e-mail: q.ni@lancaster.ac.uk).

Richard Jiang is with the School of Computing and Communication, Lancaster University, Lancaster, United Kingdom (e-mail: r.jiang2@lancaster.ac.uk).

Mohammad Ayoub Khan, is with the College of Computing and Information Technology, University of Bisha, Bisha, Saudi Arabia (e-mail: ayoub.khan@ieee.org).

Authorized licensed use limited to: Lancaster University. Downloaded on June 09,2023 at 14:46:21 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

deemed legitimate within a VANET has the potential to disseminate erroneous information to its neighboring nodes. This type of data can be sent at breakneck speed [17] and possibly used to forecast driving behaviour. Therefore, for the purpose to prevent inaccurate data from influencing driving decision, a system for assessment is required. Consequently, the system that has been proposed has the capability to efficiently manage trust within vehicular networks, allowing vehicles to evaluate the trustworthiness of their peers and the credibility of incoming messages.

The following is a summary of the contributions of the research:

- A computational model for reputation is proposed. The reputation of the vehicle and network behaviour has been developed to efficiently expect the trustworthiness of the vehicles in the VANET, which exploits spatial, temporal, and behavioural parameters.
- The network behaviour has been proposed to effectively predict the trustworthiness of the vehicles in the VANET. The dataset has been created, trained and tested to predict trustworthiness of the vehicle.
- The data related to vehicle is saved in a blockchain in order to guarantee non-repudiation.
- For trustworthiness prediction, a feature-selected random forest (RF) algorithm within an ensemble learning framework is devised. An extensive simulation has been developed for reputation computation and trust prediction.

The rest of the paper is structured as follows. Section II discusses the related work in the area of trust and reputation in VANET. The proposed methodology for computing reputation is presented in Section III. While Section IV discusses the outcomes of the simulation and performance analysis. Section V provides concluding remarks and outlines potential future research directions.

II. Related Work

In each type of vehicular network, the trust and reputation models are used to eliminate compromised communications and fraudulent vehicles, allowing for more reliable data sharing [18]. The VANET model described by Yang et al. [19] proposed a trust and reputation which is based on similarity features. This model calls for post-reception message verification. Another approach to managing trust is the blockchain-based anonymous reputation system which is exists in the literature. Both presence-based and absence-based forms of blockchain authentication are utilized in this technique. To protect vehicle’s privacy, pseudonyms are associated with public keys, and a vehicle's reputation is established using the messages it has broadcasted and recorded using a shared blockchain. Based on the research results, the implementation of BARS has the potential to enhance the reliability of disseminated messages, while simultaneously securing the confidentiality of driver’s personal data. Liu, Z. et al. [20] suggested securing VANET communications by implementing a lightweight, and self-organized trust (LSOT) architecture. In this paradigm, nodes that are capable of self-organization gather trust credentials and recommendations. Li, W. et al. [21] proposed the implementation of a mechanism known as attack-resistant trust (ART) in order to evaluate the reliability of data and vehicles within VANETs. In VANETs, data trust is employed to authenticate information, while node trust is utilized to establish the reliability of individual nodes. In another work [22], authors have proposed trustworthiness indicators based on three characteristics: credibility, longevity, and expertise. The vehicle's reputation is a direct result of its successful data transmissions with all key units. The trustor's past interactions with the trustee are evaluated here to assess their level of trust. Primiero, G. et al. [23] proposed a natural deduction calculus extension using a proof-theoretic technique for reputation and trust in VANET. The algorithm's efficacy was verified by performing consistency checks during each encounter between vehicles. As a result, this reputation system gave weight to the most important aspects of the service as determined by a temporal evaluation of the parametric feedback messages [24].

The increasing complexity of intelligent transport system systems makes the existing VANET topologies inadequate, which are based on centralized administration model. Javaid, U. et al. [25] have developed a blockchain model to facilitating information exchange and the management of trust in VANETs. Using the DrivMan method, a unique cryptographic fingerprint is generated for each vehicle and used to verify data. Vehicle privacy is protected when infrastructure unit issued certificates are used.

The exponential growth of the IoV presents formidable difficulties in terms of data storage, smart administration, and safe data management [26]. Using blockchain, the BARS technology as suggested by Lu, Z. et al. [27, 28]) allows for reliable administration of VANETs. In their theory, vehicle’s dependability is determined using a reputation value strategy that takes into account prior events. Nisha et al. [29] have created a protocol for utilizing blockchain technology in VANET authentication and revocation. While the privacy of the vehicle is maintained, the security of the communications is not considered in the design of these systems. To protect the confidentiality of information passed between vehicles on the same network, Singh, M. et al. [30] propose utilizing a blockchain model for crypto trust point. A message delivery technique for VANETs was proposed using blockchain technology [31], similar to that proposed by [30]. Both methods are safe enough for use in vehicular communication.

Concerned with VANET’s data output, Xiaodong et al. [32] demonstrated how blockchain-based VANETs may make use of mobile edge computing (MEC) to reduce their load on central servers. Blockchains still aren't completely decentralized even though MEC helps with the computing burden. Trust Bit, an incentive-based vehicle communication system which is uses a unique crypto ID [33].

Authorized licensed use limited to: Lancaster University. Downloaded on June 09,2023 at 14:46:21 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3279950

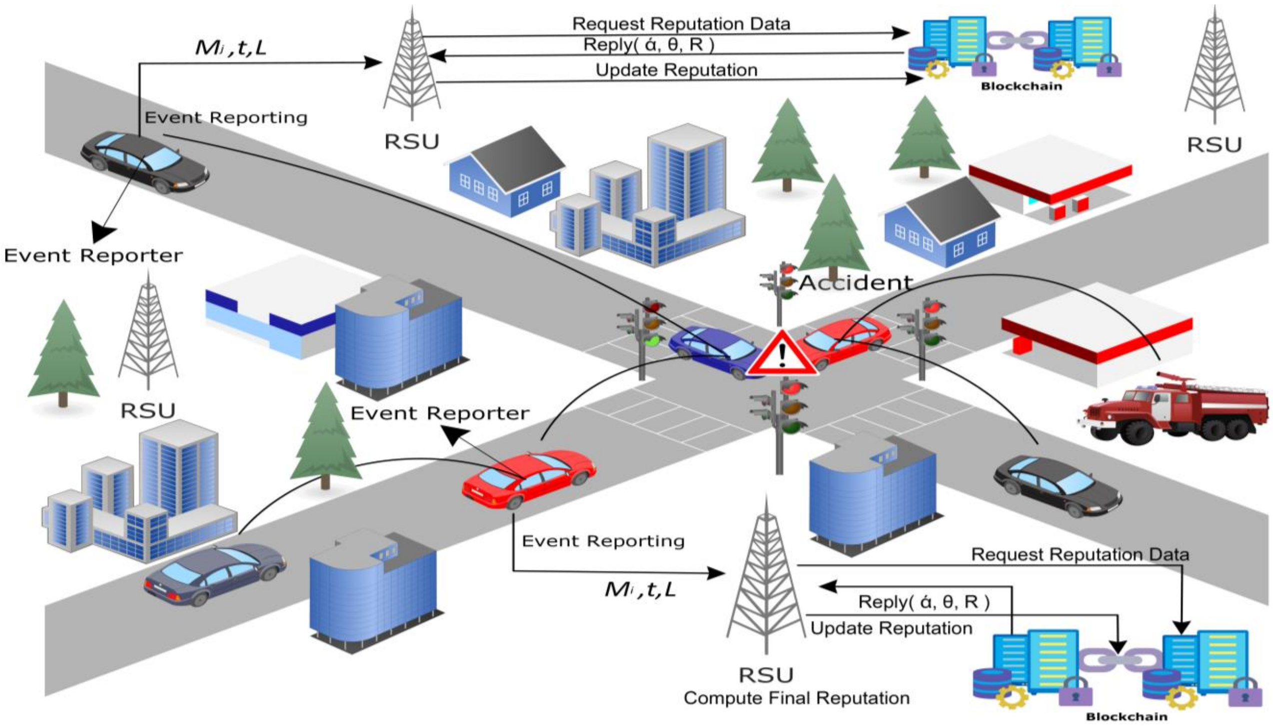


Fig. 1. Proposed Reputation Model

III. Computational Model For Reputation and Trust

The proposed computational approach introduces the basic components that comprise reputation and analyses how the blockchain may be utilized to maintain vehicle reputation values. Fig. 1. depicts the framework recommended to fulfil the goal of reputation computation. VANET is built on the sharing of data among vehicles. Every vehicle will be equipped with biometric data. When the vehicle detects an event, it creates and broadcasts a message to peers in the network that includes RSUs and vehicles. The event has numerous information containing biometric details of the authorized user, which includes the event description and vehicle biometric ID. The age of the vehicle, the level of involvement, message's accuracy, and the reporter's current reputation are all factors that go into determining the reputation of the event reporter when a vehicle/RSU receives the message. The technique under consideration integrates the existing reputation of the vehicle with the trustworthiness of the message to derive the vehicle's reputation score. If the score of the vehicle's reputation surpasses a specific threshold, the authorized user's biometric identifier will be given bonus credit that can be utilized toward the establishment of reward system. The reputation value of a vehicle is recorded in a distributed ledger, which provides both non-repudiation and privacy.

The proposed reputation model will offer a method for determining the trustworthiness of individual vehicles, which will result in improved safety and precision of the information that is communicated over VANETs. In the proposed trust prediction model as shown in Fig. 2., after interaction to a vehicle the reputation is computed based on the proposed reputation model. Along with the reputation features, the other features that constitute network behaviour such as *source IP*, *destination IP*, *destination_port*, *total number of packets forwarded*, *length of the packets*, *network flow*, *average packet size*, *time stamp*, and *time to live* are also extracted from this interaction [34]. Thereafter, these two datasets are merged into one called as reputation dataset after fetching existing reputation value from blockchain. Once the dataset is merged then pre-processing will be performed to balance the class. Thereafter, feature selection and model building are performed to predict the trustworthiness. The following Section B contains a more in-depth overview of machine learning employed in the proposed model.

A. Computational Method

Reputation values are immediately updated following each new interaction with a vehicle. A new communication is assessed, calculated, and observed during the reputation computation. Only information produced by the vehicle may be utilized immediately to calculate the reputation value.

Trust - The vehicle's trust T can be defined as $T \in [0, 1]$, that is assessed based on the average reputation value computed by all the vehicles and network behaviour of the vehicle which is captured during the interaction. Based on the reputation score and network behaviour the vehicle may be classified as trustworthy or non-trustworthy [35].

Reputation - The reputation of a vehicle can be influenced by its interactions with other vehicles within the network [35]. If two vehicles have distinct experiences after interacting with one another, their reputations may differ. Consequently, the score of a reputation is a composite of attributes that are specific to the vehicle and factors related to interactions. The degree of trustworthiness is influenced not just by the quality of the interaction but also by the reputation score.

Authorized licensed use limited to: Lancaster University. Downloaded on June 09,2023 at 14:46:21 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3279950

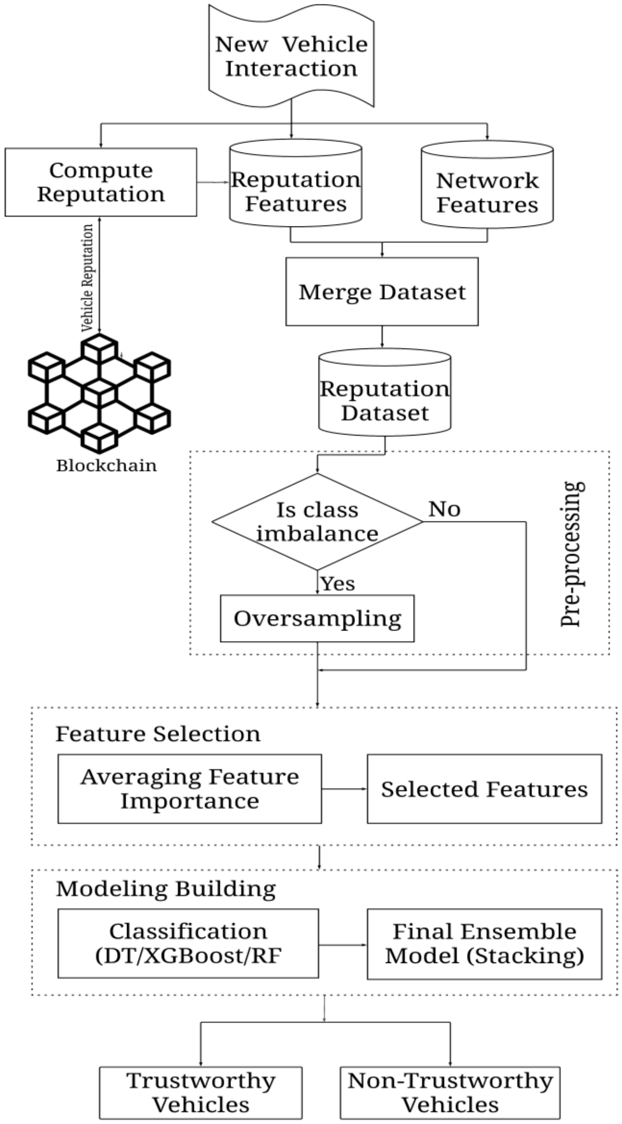


Fig. 2. Proposed trust prediction model

TABLE I

SYMBOL USED IN MODEL

C_t^i	Message correctness at specific time *t*
f_c	Function deriving correctness of message
M	Message
M_p	Set of all messages classified as positive or correct
M_n	Set of all messages classified as negative or correct
N^+, N^-	Total number of messages classified as positive and negative respectively
N	$(N^+ + N^-)$ Number of messages received by any vehicle
S	Function deriving similarity between messages
$R_{xy}^{(t)}$	Reputation at specific time assessed by specific vehicle
w_i	Specific weight assigned for balancing
f_f	Function deriving message freshness
f_d	Function deriving distance among two vehicles
α	Vehicle real age
θ	Degree of participation
t_{Reg}	Vehicle timestamp of registration
n	Fleet size
m	Total number of messages
V_x	Specific vehicle x in the network
R	Average of reputation of a vehicle
v	Speed of the vehicle

Table 1 contains a description of each symbol utilized in the proposed model. Therefore, the average reputation R for vehicle x is represented by equation (1) [35].

$$R = \frac{\sum_{y=1}^{N} R_{xy}^{(t)}}{N}, y = 1,2,3, \dots, n \tag{1}$$

The reputation model that has been developed takes into account many parameters to spatial, temporal, and behavioral, such as the involvement level, the age of the vehicle, and the computation of vehicle reputation.

The $R_{xy}^{(t)}$ represents reputation of a specific vehicle x, assessed by another vehicle y at specific time t is the summation of C_t^i, α, θ, β and $R_{xy}^{(t-1)}$ which is message correctness, vehicle age, degree of participation, coefficient for smoothing and existing reputation. The reputation $R_{xy}^{(t)}$ can be computed by equation (2) and (3) [35].

$$R_{xy}^{(t)} = \begin{cases} \beta R_{xy}^{(t-1)} + (1-\beta)\big((\alpha + \theta + C_t^i)/3\big), & \alpha > 0 \\ (\beta)\big((\alpha + \theta + C_t^i)/3\big) & \alpha = 0 \end{cases} \tag{2}$$

$$C_t^i = \frac{(S\,(M_i,M_j).w_1 + f_f\,(M_i)\,.w_2 + f_d\,(M_i,M_j))\,.w_3)}{3} \tag{3}$$

$$\text{Where} \begin{cases} \alpha = \big(\,(\,t - t_0\,)/((\,t - t_{Reg}\big) + (\,t - t_0\,)) \\ \theta = \dfrac{N^+}{N}\,, 0 \le \theta \le 1 \\ N = N^+ + N^- \\ N^+ = \big|\{\,M_p\}\big|, N^- = \big|\{\,M_p\}\big|, N > 0 \\ C_t^i \in [0,1] \end{cases}$$

The β, is assigned depending on experience, is an integer between zero and one. For instance, if the initial weight placed on established trust is 0.3, then (1- β) is 0.7. Each characteristic's significance can be represented by a weight, such as $w_1, w_2,$ and w_3. Keeping track of each vehicle's standing, the reputation is stored in the following nxn matrix as shown below:

$$\begin{array}{c|ccccc} & V_1 & V_2 & V_3 & \dots & V_n \\ \hline V_1 & R_{11} & R_{12} & R_{13} & \dots & R_{1n} \\ V_2 & R_{21} & R_{22} & R_{23} & \dots & R_{2n} \\ V_3 & R_{31} & R_{32} & R_{33} & \dots & R_{3n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ V_n & R_{n1} & R_{n2} & R_{n3} & & R_{nn} \end{array}$$

The level of involvement in the network is indicated by the participation degree. Greater engagement can be inferred from a higher level of activity exhibited by the vehicle, which can be ascertained by comparing the count of accurately designated messages to the total number of messages transmitted. Here, N^+ denotes the whole count of messages categorized as correct while N^- indicates as incorrect. The vehicle age shows the vehicle's actual age as well as its time in the network. The actual lifetime α is the date a vehicle obtained a registration with the motor vehicle department; however, the network age is the amount of time that has passed from the first activity time t_0 and the present participation time t. Equation (2) demonstrates that the age of the vehicle is represented as a standardized numerical value ranging from 0 to 1. The α =0, indicates that the vehicle has only recently entered the network and hence has no established reputation. The message's correctness C_t^i, as

Authorized licensed use limited to: Lancaster University. Downloaded on June 09,2023 at 14:46:21 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

determined by formula in equation (3). To determine the message correctness, a function f_c is defined across numerous variables such as message similarity, freshness of the message, sender proximity, and message credibility [35]. The $f_c(M)$ value ranges from 0 to 1. If $f_c(M) < t_h$ then C_t^i will be categorized as 0, else it will be categorized as 1.

1) Message Freshness

According to the equation (4), the message's freshness f_f is computed as the elapsed time between its transmission (t_t) and receipt (t_r).

$$f_f = t_r - t_t \quad s.t \begin{cases} \text{TRUE}, f_f \geq t_h \\ \text{FALSE}, f_f \leq t_h \end{cases} \tag{4}$$

In the event that the value of f_f is lower than the threshold value t_h, then the message is considered fresh. In a congested traffic scenario, the predicted packet delivery time is used to set the threshold t_h. If the communication is delayed by more than the threshold, it portends poorly for the vehicle's reputation. If sender vehicle has a good reputation, the f_f will have a high value.

2) Similarity of Messages

The exact message may be obtained by several vehicles at the exact moment and position for the same event. Considering each vehicle transmitting a high number of messages/second, then delivery rates of messages may soon outpace verification capability of the signature. Because, approving all the interactions is not possible, therefore, techniques for determining which messages to investigate becomes very important. The suggested technique reduces the number of unrelated messages validated by utilizing originator location, orientation, reputation, and time. Messages with the closest distance are considered as similar, and hence becomes the best candidate for signature verification. The degree of similarity between two messages may be determined using a variety of methods, including the Euclidean distance, the Manhattan distance, the Jaccard similarity, and the cosine-similarity. Each technique possesses set of benefits and drawbacks. Table II illustrates that all of the messages are generated by different vehicles and represent the same incident. The vehicle's geolocation (latitude and longitude) at a certain moment is saved. In order to determine how similar two vehicles are, we will take into account their reputation value, speed, and direction. Each pair of messages (M_i, M_j) undergoes a similar computation using the Jaccard distance method to choose the most likely legitimate message.

TABLE II
MULTIPLE-MESSAGE-EVENT SCENARIO

M	*V*	*Timestamp*	*Location*	v	$\vec{v}$	*R*
M_1	V_1	00:01:23	(21° 32' 49.4772",39° 13' 3 3.5496")	50	180	0.8
M_2	V_2	00:01:24	(21° 32' 49.4772",35° 13' 3 3.5486")	49	181	0.6
M_3	V_3	00:01:23	(21° 33' 49.4772",39° 13' 3 3.5496")	50	175	0.7
M_4	V_4	00:01:25	(21° 32' 49.4772",39° 13' 3 3.5496")	48	200	0.5
M_n	V_n	00:01:24	(21° 33' 49.4772",39° 13' 3 3.5496")	50	180	0.8

Similarity may be determined using the objects listed in Table II, which include the message (M), the sender's vehicle (V), a timestamp, a location, a speed(v), a direction ($\vec{v}$), and a reputation (R) as shown in equation (5) [36].

$$D(X,Y) = 1 - J(X,Y); J(X,Y) = |X \cap Y|/|X \cup Y| \tag{5}$$

3) Sender Proximity and Event Location

The distance is a key factor in determining how close the event was to the vehicle that witnessed it. Accuracy can only be determined by collecting messages delivered by three or more vehicles. Using equation (6) and (7) to determine latitude and longitude will give you the distance from the incident [36].

$$d = R * C, \text{where} \begin{cases} C = 2.atan\,2(\sqrt{a}, \sqrt{(1-a)}) \\ a = Sin^2\left(\frac{\Delta\emptyset}{2}\right) + cos\,\emptyset_1\,.\emptyset_2.Sin^2\left(\frac{\Delta\lambda}{2}\right) \end{cases} \tag{6}$$

$$D = Min\,\{d_1, d_2, d_3, \dots, d_n\},\ n > 0 \tag{7}$$

Here, $\emptyset$ is latitude, λ is longitude and R is Earth's radius. If d_i is smaller, then it is more likely that the message is correct.

4) Storing Reputation in Blockchain

The reputation derived from a communication is recorded in a blockchain. The aforementioned, ensures non-repudiation and privacy. The blockchain has no single point of authority due to the network's decentralized structure. As a result of this mechanism, a miner is selected at predetermined intervals across all RSUs to generate new offset blocks. In blockchain-based systems, the miner selection procedure based on proof-of-work (PoW) is often used. Nodes in the network regularly update the nonce as part of the process of computing the block's hash parameters, which also includes the nonce. The miner is the individual whose hash number falls below a particular threshold and whose block can be published. The score of the vehicle's reputation is stored within the body of the block. The nodes with the most processing power will win the election since they will be the first to find the correct nonce, despite the fact that the threshold is the same for all nodes due to the difficulty shown as in equation (8).

$$Hash(\rho\,, t\,, prev_{Hash}\,, RSU_{id}) \leq Hash\ threshold \tag{8}$$

The nonce is represented by ρ and time is defined by t. Upon receipt of a block from a miner, the RSU is obligated to verify the validity of the nonce prior to disseminating the block to its respective blockchain. In the unlikely event that the RSU acquires a large number of blocks all at once, the blockchain may fork to facilitate a more rapid transaction. In order to find a solution to this issue, a method known as distributed consensus is put into practice. Every RSU votes on a fork and contributes to add blocks. In addition, it must store the blocks generated by each RSU so that they may be added to the blockchain at a later time. As a direct consequence of this, each RSU possesses an identical and immutable copy of the blockchain.

B. Learning Model

In the first phase, a large quantity of data is gathered from network traffic which is mixed of normal/abnormal cases. Packet sniffers are used to collect the data which is required to develop a predictive model, but for maximum efficiency, these sniffers must possess certain particular network attributes or qualities. We have generated simulated data that takes into account a wide variety of simulated network characteristics such as length of packet, overall packets forwarded, overall packets backward, kind of failure in transmission, selection type, highway circumstances, TTL, vehicle speed, GPS location

Authorized licensed use limited to: Lancaster University. Downloaded on June 09,2023 at 14:46:21 UTC from IEEE Xplore. Restrictions apply.

© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3279950

etc. [35] The custom dataset is generated based on the network characteristics as there are no publicly available VANET datasets that include reputation-related characteristics.

However, the large dimensionality of the data may increase the computational cost of the recommended forecast. Therefore, it's important to look into the external network data for any additional features. The development of prediction models can be aided by first pre-processing the collected network data. To begin, removing possible bias induced by the data's measurement makes it easier to train a machine learning model with normalized data. To do this, the data must be adjusted such that it is inside a smaller range, for example [0.0, 1.0]. The lowest X_{min} and highest X_{max} values of the original value of attribute X are substituted into equation (9) to get the mapped new attribute $X^{'}$.

$$X' = \frac{X - X_{min}}{X_{max} - X_{min}} \tag{9}$$

In order to determine whether or not the system can be relied upon, a problem involving binary classification is analyzed, and machine learning methods are used to provide accurate prediction results [35]. Several distinct approaches to machine learning are incorporated into the system, including random forest, XGBoost, and decision trees. The classification of data using the decision tree is popular because it uses a divide and conquer method. Each node in a decision tree makes a value judgment about one of the traits, and each leaf node in the tree represents one of the classes that resulted from that evaluation. XGBoost is a method of ensemble learning that combines a number of decision trees through the use of an approach called gradient descent. This drastically boosts both speed and efficiency. In addition to these ensemble learning classifiers, random forest is another popular option since it utilizes majority voting rule that chooses those decision tree class which receives the most votes.

1) *Proposed Ensemble Learning Model*

As opposed to using a single model like linear regression or the K-nearest neighbors (KNN) technique, vast majority of tree topology learning models make use of ensemble learning. Features are selected with the help of estimated importance of such features during the model-building process. In random forest, the feature vector is $\{f_i\}_{i=1}^{N}$and and we look at N instances at a time.

$D = \{(f_1, O_1)\ldots,\ (f_N, O_N)\}$ describes the data, and $f_k = (f_{k1}, \ldots, f_{xd})$ describes every feature vector. The selection of features f_i and threshold t at each node is aimed at reducing the diversity. The Gini criterion, which is commonly employed, serves as a measure for evaluating diversity.

Gini criterion: What is the optimal method for determining the frequency of instances in a node for class C_1, which is deemed untrustworthy, and class C_2, which is considered trustworthy? Assuming the set S as an illustrative example in this context, it can be expressed as the concatenation of two subsets, namely S_1 and S_2. Given a set S, where $|S|$ denotes the cardinality of S, we can establish the definition of $\hat{P}$ as presented in equation (10).

$$\hat{P}(\dot{S_\jmath}) = \frac{|S_j|}{|S|} \text{ and } \hat{P}(C_\imath \dot{|} CS_\jmath) = \frac{|S_j \cap C_i|}{|S_j|} \tag{10}$$

The variation and Gini index can be defined as shown in (11) and (12):

$$g(S_j) = \textstyle\sum_{i=1}^{2} \hat{P}(C_i | CS_j)\left(1 - \hat{P}(C_i | CS_j)\right) \tag{11}$$

$$G = \hat{P}(S_1)g(S_1) + \hat{P}(S_2)g(S_2) \tag{12}$$

$$D = \{(f_1, O_1)\ldots, (f_N, O_N)\} \tag{13}$$

Ensemble learning is a technique in which a set of weak learners, or models, are trained on identical training data and subsequently combined to yield enhanced outcomes. Insufficiently coupled models have the potential to generate predictions of higher precision when properly integrated. The methodology of meta-model training, which involves combining several feeble models, enables the stacking approach to produce a forecast that consolidates the opinions obtained from all the models that underwent training. Equation (13) provides a description of the input data utilized by the random forest. The algorithm's result is an ensemble learning, which is presented in equation (14) and (15):

$$h = \{h_1(f), \ldots, h_{\mathrm{k}}(f)) \tag{14}$$

$$h_k(f) = h(f | \Theta_k) \tag{15}$$

$$\widehat{M}(\dot{F}, o) = \hat{P}_k(h_k(f) = o) - \underbrace{max}_{j \neq o} \hat{P}_k(h_k(f) = j \tag{16}$$

In ensemble learning, the margin function is described in equation (16). The margin function refers to the percentage difference between the proportion of votes received by the proper class and proportion received by the second-best class. The ensemble's efficacy of the RF can be characterized as shown in equation (17) [35]:

$$s = \mathbb{E} \in_{x,y} M(F \dot{,} o) \tag{17}$$

In equation (18), the error using Chebyshev inequality is described as follows:

$$e = P_{x,y}(M(F, o) < 0 \leq P_{x,y}(|m(F, o) - s| \geq s) \leq \frac{V(M)}{s^2} \tag{18}$$

2) *Algorithm Complexity*

Considering that there are N occurrences in the dataset, f characteristics, and T trees, the temporal complexity of the decision tree can be calculated as $O(N^2 f)$. XGBoost's complexity will be $O(NfT)$. The level of difficulty of random forest, on the other hand, can be calculated as $(N^2\sqrt{f}T)$. A multi-processing capacity may be utilized to reduce the duration required for computation. The random forest's complexity in terms of time will be $(O\,\frac{(N^2\sqrt{f}T)}{P})$ if the total amount of processors available for processing is P.

IV. Results and discussion

A. Simulation Setup

To demonstrate the efficacy of our methodology, we generated synthetic data pertaining to Vehicular Ad Hoc Networks comprising 24 distinct attributes. This dataset is widely recognized as a standard benchmark for trust identification and we contend that it represents a highly suitable choice for our purposes. A comprehensive definition of the dataset is presented in Table III [35]. A dataset comprising 100,000 records was generated for the purpose of simulation. Based on the available statistics, the rate of non-trustworthiness is 2.08661%. The min-max normalization technique, which is

Authorized licensed use limited to: Lancaster University. Downloaded on June 09,2023 at 14:46:21 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3279950

widely used, is employed to standardize all of the features. Each attribute is normalized by mapping the minimum value to 0, the maximum value to 1, and rest mapping between greater than 0 and less than 1. The computational simulation was executed on an Intel Pentium central processing unit utilizing Python 3.6 programming language. The operating system used was Windows 10, and the hardware specifications included a 2.6 GHz Intel Core i7 processor with 16.0 GB of random-access memory.

TABLE III
DATASET DESCRIPTION

Features	Description
source	The IP address associated with the originating vehicle.
destination	Target vehicle address (IP)
detection_target	Detecting vehicle address (IP)
destination_port	Endpoint IP address
Total_Fwd_Packets	Sum of all packets that were forwarded
Total_Bkwd_Packets	Sum of all packets sent backward
Total_Length_of_Fwd_Packets	Sum of the length of all packets forwarded
Total_length_of_Bkwd_Packets	Sum of the length of all packets in backward
Flow_Packet_Per_Sec	Flow rate
Average_packet_Size	Average packet size
Time_Stamp	Packet's origin timestamp
TTL	Live time in the network
Reputation	Reputation of the transmitter
OT	Indicators range from 0 (default) to 3 (transmission outcome)
Failure	Failure due to non-malicious conduct is a 1, whereas malicious behavior is a 0. Relating to Transmission result, Number 3 is assigned
Road_Condition	Dry, wet, and icy.
Speed Scenario	The three distinct phases of speed, namely acceleration, constant speed, and deceleration.
Time_Scenario	The temporal scenario includes four distinct phases: "Dawan," "Day," "Dusk," and "Night."
Weather Scenario	The weather conditions can be classified into five scenarios, namely 'Clear', 'Foggy', 'Raining', 'Snowing', and 'Windy'.
Lane_Type	The various types of lanes
Traffic_Scenario	The possible scenarios for the presence of cars
Packet_Type	Possible packets types as 'General', 'Safety', and 'Traffic'.
Latitude, Longitude	GPS coordinates of vehicle

The datasets underwent minor data manipulation procedures such as data merging, removal of missing values, elimination of irrelevant features, and creation of new data labels to enhance their suitability for classification purposes. For simulation the data has been samples which includes 39,567 trustworthy and 6,260 untrustworthy instances. This 4.5% data was used to train the model.

B. Evaluation Metrics

In this paper, we assess the efficacy of the proposed technique, which utilizes feature selection in conjunction with random forest, by comparing its performance against that of the baseline techniques. Two criteria are employed for evaluating the random forest based on feature selection.

Area Under Curve (AUC)- This is a commonly used metric in statistical analysis and machine learning. It refers to the area under a curve that represents relationship among variables, typically a predictor and a response variable. AUC is often used to evaluate the performance of predictive models, particularly in binary classification problems, where the goal is to classify observations into one of two categories. The AUC metric is utilized to assess the efficacy of a model, where a higher value indicates superior performance. A value of 1 represents perfect classification, while a value below 0.5 suggests inadequate classification.

Confusion metrics - This refers to a set of performance evaluation measures used in machine learning and statistical classification tasks. These accuracy and effectiveness of a classification is measured by comparing the predicted outcomes with the actuals. This includes accuracy, precision, recall, and F1 score.

Time measurement - The effectiveness of the proposed trust classifications is evaluated using runtime as a measure to benchmark the efficacy of the proposed technique. In the present study, the duration required to detect untrustworthy data will be denoted as the processing time of an individual data instance. Models with lower values are comparatively more efficient than others.

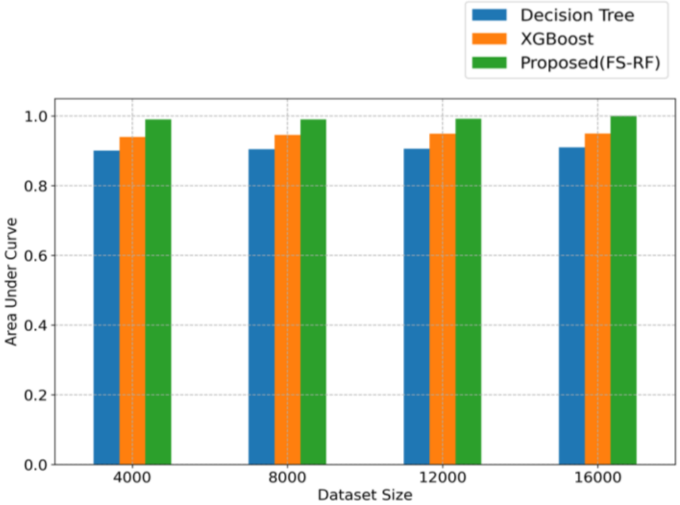


Fig. 3. AUC performance Vs Dataset

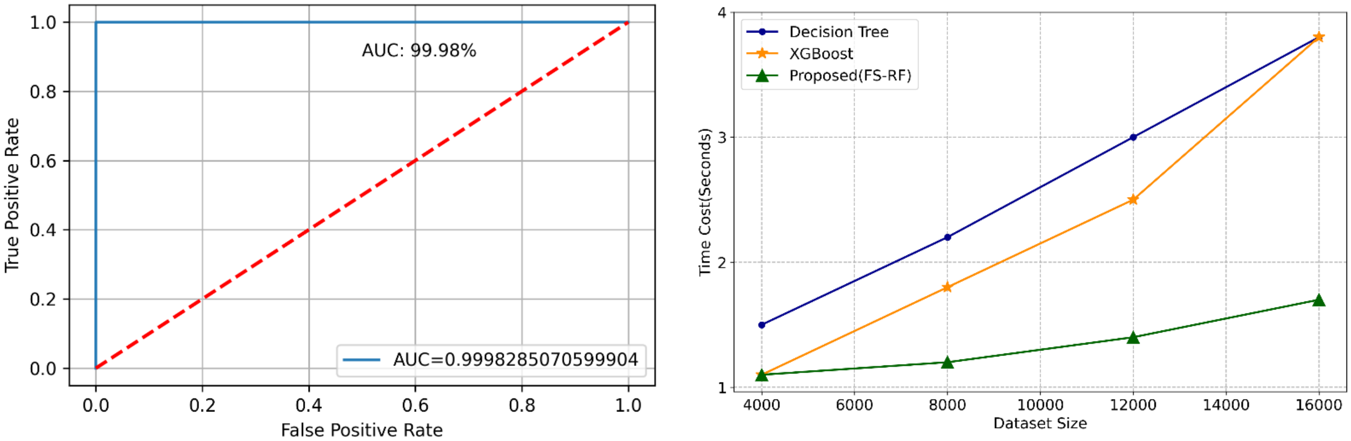
C. Experimental Results

The efficacy of the proposed random forest methodology is assessed based on its accuracy and efficiency. The outcomes are subsequently verified through the utilization of ensemble learning and feature selection. The findings and examination of the experiment are presented below.

AUC Measurements – This is measured for baseline and proposed featured selection random forest (FS-RF) for different size of subset as illustrated in Fig. 3. The dataset was subjected to random selection, with subset sizes ranging from 4,000 to 8,000 and 12,000 to 16,000. The aforementioned data has been derived from the recorded measurements of various variables as documented in previous publications, in conjunction with the outcomes of our own conducted experiments. Despite the variable's capacity to accommodate values within the specified ranges, empirical evidence suggests that the efficiency of FS-RF is higher and exhibits significant variability. The results depicted in Fig. 3 demonstrate that the AUC value increases when the subset size is modified using the FS-RF approach. The AUC metric of the XGBoost model is marginally lower than that of the decision tree model.

Authorized licensed use limited to: Lancaster University. Downloaded on June 09,2023 at 14:46:21 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3279950



(a) ROC analysis of proposed FS-RF

(b) Timing analysis for datasets

Fig. 4. ROC and Timing Analysis

In addition, Fig. 4(a). illustrates the true positive rate (TPR) and false positive rate (FPR), along with the AUC measuring which is about 99.98%.

Analysis of Computation Time - The computation time of all methods in relation to the subset size ranging from 4,000 to 16,000 is illustrated in Fig. 4(b). The duration of the decision tree falls within the range of 1.5 to 3.8 seconds, whereas the time for XGBoost ranges from 1.1 to 3.8 seconds. According to the findings presented in Fig. 4(b), the proposed FS-RF method exhibits a significant level of effectiveness when compared to the baseline methods. The baseline methods, which are associated with time costs ranging from 1.1 to 1.7 seconds, are outperformed by the FS-RF method. The variability in duration can be attributed to the utilization of ensemble learning and feature selection algorithms within our system, which have been shown to significantly decrease time expenditure. Fig. 5 displays the confusion matrix of multiple machine learning models.

Analysis of feature selection - The efficiency of the proposed feature selection technique was evaluated by utilizing data subsets for analysis. Table IV illustrates that the reputation holds a feature score 0.4681, that is highest among all to indicate trustworthiness. This finding indicates that reputation is a crucial aspect in predicting the reliability of vehicles, alongside other network parameters. The TTL exhibits the minimum characteristic selection value of 0.0107. The mean packet size is a crucial element of the dataset. A larger packet is commonly perceived as being unreliable. Additional criteria for showcasing trustworthiness include the option and failure types.

Table V demonstrate that the ensemble learning technique, utilizing FS based on RF, exhibits superior performance compared to the baseline. The FS-RF model achieved a high accuracy of 99.9812, whereas the other models, namely decision tree, XGBoost, random forest, Feature selection-based decision tree, and feature selection based XGBoost, obtained accuracies of 98.1281, 99.0352, 99.8354, 99.3983, and 99.7961, respectively.

Given the limitations of decision trees in terms of accuracy and processing time, the stacking ensemble model was developed using XGBoost and random forest algorithms. The final meta-classifier selected for this model was RF. The employment of stacking to combine the models has resulted in achieving a 99.98% accuracy and F1 precision, enabling the detection of all the trained untrustworthy vehicles.

TABLE IV
SCORE OF DATASET FEATURES [35]

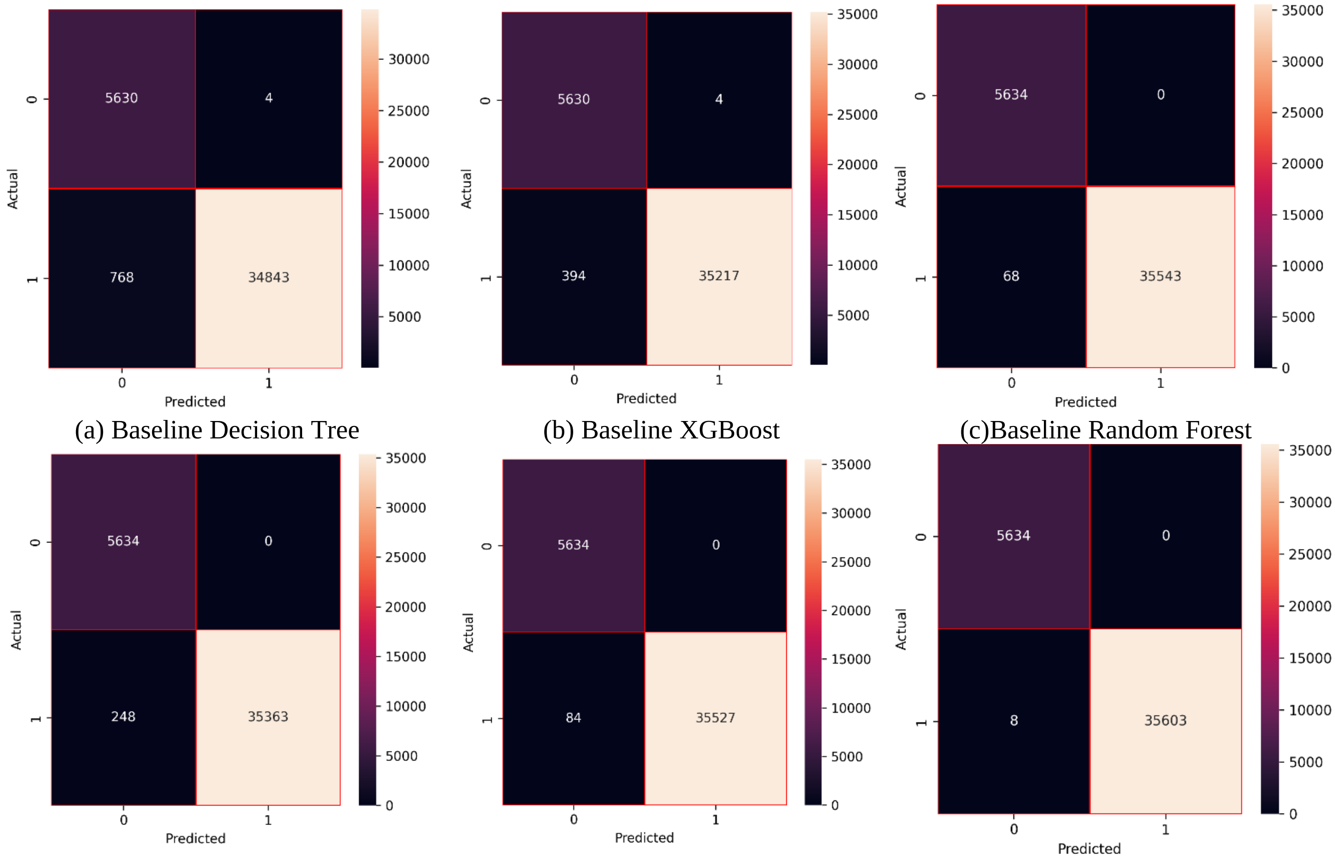
Reputation	0.4681
Average_packet_Size	0.3732
Option Type	0.0202
Failure Type	0.0183
Total_Bkwd_Packets	0.0152
Total_length_of_Bkwd_Packet	0.0151
Destination_port	0.0147
Latitude	0.0143
Longitude	0.0115
Total_Fwd_Packets	0.0134
Flow_Packet_Per_Second	0.0131
Total_Length_of_Fwd_Packets	0.0127
TTL	0.0107

TABLE V
COMPARATIVE ANALYSIS

Approach	Methods	Accuracy	Precision	Recall	F1
Baseline	Decision Tree	98.1281	98.3505	98.1284	98.1771
	XGBoost	99.0352	99.0964	99.0353	99.0452
	Random Forest	99.8354	99.8373	99.8352	99.8353
Feature Selection	Decision Tree	99.3983	99.4242	99.3981	99.4044
	XGBoost	99.7961	99.7991	99.7965	99.7965
	Random Forest	99.9812	99.9801	99.974	99.8912

Authorized licensed use limited to: Lancaster University. Downloaded on June 09,2023 at 14:46:21 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3279950



(a) Baseline Decision Tree (b) Baseline XGBoost (c)Baseline Random Forest

(d) Feature Selection – Decicison Tree (e) Feature Selection – XGBoost (f) Feature Selection – Radom Forest

Fig. 5. Confusion matrix of approaches (baseline and feature selection)

V. Conclusion

The present study introduces a methodology for trust computation and classification for vehicular networks based on blockchain technology. The process of trust value aggregation in the RSU is reliant on the reputation feedback received from message recipients. The collaboration of RSUs results in the establishment of a reliable and uniform database through the application of blockchain principles. A variety of simulations are run in order to assess the overall system's performance. According to simulation results, the proposed method for decentralised trust management is effective and viable. The trust and reputation data are dynamic rather than static, and they present certain challenges for existing classification algorithms due to their unboundedness, correlations and distribution changes. Therefore, a trust classification using ensemble learning and feature method is proposed, namely FS-RF, that can achieve an accurate classification with better dataset scalability. An extensive test on the dataset has been carried out, and the results of these studies demonstrate the practicality of FS-RF. Future work will study the impact of reputation and trust prediction on minimizing the incidents of erroneous decision due to inaccurate messages from non-trustworthy vehicles.

References

[1] J. Xu, S. H. Park, X. Zhang and J. Hu, "The Improvement of Road Driving Safety Guided by Visual Inattentional Blindness," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 6, pp. 4972-4981, June 2022, doi: 10.1109/TITS.2020.3044927.

[2] J. Xu, X. Zhang, S. H. Park and K. Guo, "The Alleviation of Perceptual Blindness During Driving in Urban Areas Guided by Saccades Recommendation," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 9, pp. 16386-16396, Sept. 2022, doi: 10.1109/TITS.2022.3149994.

[3] X. Dai et al., "A Learning-Based Approach for Vehicle-to-Vehicle Computation Offloading," in IEEE Internet of Things Journal, vol. 10, no. 8, pp. 7244-7258, 15 April15, 2023, doi: 10.1109/JIOT.2022.3228811.

[4] Yao Z, Yoon H-S, Hong Y-K., "Control of Hybrid Electric Vehicle Powertrain Using Offline-Online Hybrid Reinforcement Learning," in Energies. 2023; vol. 16, no. 2, 652. https://doi.org/10.3390/en16020652

[5] Yanyu Chen, Research on collaborative innovation of key common technologies in new energy vehicle industry based on digital twin technology, in Energy Reports, Vol. 8, 2022, pp. 15399-15407, https://doi.org/10.1016/j.egyr.2022.11.120.

[6] Y. Fang, H. Min, X. Wu, W. Wang, X. Zhao and G. Mao, "On-Ramp Merging Strategies of Connected and Automated Vehicles Considering Communication Delay," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 9, pp. 15298-15312, Sept. 2022, doi: 10.1109/TITS.2022.3140219.

[7] N. Bißmeyer, J. Njeukam, J. Petit, and K. M. Bayarou, "Central misbehavior evaluation for VANETs based on mobility data plausibility," in Proc. 9th ACM Int. Workshop Veh. Inter-Netw., Syst., Appl. ACM, 2012, pp. 73–82.

[8] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data centric trust establishment in ephemeral ad hoc networks, " in Proc. IEEE INFOCOM, Phoenix, AZ, USA, Apr. 2008, pp. 1–9.

[9] M. Monir, A. Abdel-Hamid, and M. A. El Aziz, "A categorized trust-based message reporting scheme for VANETs, " in Advances in Security of Information and Communication Networks. Berlin, Germany: Springer, 2013, pp. 65–83.

Authorized licensed use limited to: Lancaster University. Downloaded on June 09,2023 at 14:46:21 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3279950

[10]X. Dai, Z. Xiao, H. Jiang and J. C. S. Lui, "UAV-Assisted Task Offloading in Vehicular Edge Computing Networks," in IEEE Transactions on Mobile Computing, doi: 10.1109/TMC.2023.3259394.

[11]R. G. Engoulou, M. Bellaiche, S. Pierre, and A. Quintero, "VANET security surveys, " in Comput. Commun., vol. 44, no. 5, pp. 1–13, 2014

[12]F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs, " in IEEE Trans. Intell. Transp. Syst., vol. 16, no. 6, pp. 2985–2996, Dec. 2015.

[13]P. Zhao, X. Yang, W. Yu, and X. Fu, "A loose-virtual-clustering-based routing for power heterogeneous MANETs, " in IEEE Trans. Veh. Technol., vol. 62, no. 5, pp. 2290–2302, Jun. 2013.

[14] J.-S. Weng, J. Weng, Y. Zhang, W. Luo, and W. Lan, "BENBI: Scalable and dynamic access control on the northbound interface of SDN-based VANET, " in IEEE Trans. Veh. Technol., vol. 68, no. 1, pp. 822–831, Jan. 2019.

[15]Apostolos Gerodimos et al., IoT: Communication protocols and security threats, in Internet of Things and Cyber-Physical Systems, Vol. 3, pp.1-13, 2023, https://doi.org/10.1016/j.iotcps.2022.12.003.

[16]Y. Zhang et al., "Onionchain: Towards balancing privacy and trace- ability of blockchain-based applications," 2019. [Online]. Available: arXiv:1909.03367.

[17]J. Cheng, P. Qin, M. Zhou, Z. Huang, and S. Gao, "Key properties of connectivity in vehicle ad-hoc network," in Internet and Distributed Computing Systems (IDCS) (LNCS 9864), W. Li et al., Eds. Cham, Switzerland: Springer, 2016, pp. 328–339.

[18]Y. Ren, H. Jiang, X. Feng, Y. Zhao, R. Liu and H. Yu, "ACP-Based Modeling of the Parallel Vehicular Crowd Sensing System: Framework, Components and an Application Example," in IEEE Transactions on Intelligent Vehicles, vol. 8, no. 2, pp. 1536-1548, Feb. 2023, doi: 10.1109/TIV.2022.3221927.

[19]Yang, N. A et al., "Similarity based trust and reputation management framework for vanets," in Int. J. Future Generation Communication Netw. 2013, vol. 6, pp. 25–34

[20]Liu, Z.; Ma, J.; Jiang, Z.; Zhu, H.; Miao, Y., "LSOT: A lightweight self-organized trust model in VANETs, " in Mob. Inf. Syst. 2016, 7628231. https://doi.org/10.1155/2016/7628231

[21]W. Li and H. Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks," in IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 4, pp. 960-969, April 2016, doi: 10.1109/TITS.2015.2494017.

[22]Truong, N.B.; Lee, G.M., "Trust Evaluation for Data Exchange in Vehicular Networks," in Proceedings of the 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), Pittsburgh, PA, USA, 18–21 April 2017; pp. 325–326.

[23]G. Primiero, F. Raimondi, T. Chen and R. Nagarajan, "A Proof-Theoretic Trust and Reputation Model for VANET," 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris, France, 2017, pp. 146-152, doi: 10.1109/EuroSPW.2017.64.

[24]Z. Xiao et al., "Understanding Private Car Aggregation Effect via Spatio-Temporal Analysis of Trajectory Data," in IEEE Transactions on Cybernetics, vol. 53, no. 4, pp. 2346-2357, April 2023, doi: 10.1109/TCYB.2021.3117705.

[25]Javaid, U.; Aman, M.N.; Sikdar, B., "DrivMan: Driving Trust Management and Data Sharing in VANETs with Blockchain and Smart Contracts," in Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 28 April–1 May 2019; pp. 1–5.

[26]T. Jiang, H. Fang, and H. Wang, "Blockchain-based internet of vehicles: Distributed network architecture and performance analysis," in IEEE Internet of Things Journal, pp. 1–1, 2018.

[27]Z. Lu, Q. Wang, G. Qu and Z. Liu, "BARS: A Blockchain-Based Anonymous Reputation System for Trust Management in VANETs," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 2018, pp. 98-103, doi: 10.1109/TrustCom/BigDataSE.2018.00025.

[28]Z. Lu, W. Liu, Q. Wang, G. Qu and Z. Liu, "A Privacy-Preserving Trust Model Based on Blockchain for VANETs," in IEEE Access, vol. 6, pp. 45655-45664, 2018, doi: 10.1109/ACCESS.2018.2864189.

[29]N. Malik, P. Nanda, A. Arora, X. He, and D. Puthal, "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks," in 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Aug 2018, pp. 674–679

[30]M. Singh and S. Kim, "Crypto trust point (ctp) for secure data sharing among intelligent vehicles," in 2018 Int. Conference on Electronics, Information, and Communication (ICEIC), Jan 2018, pp. 1–4.

[31]R. Shrestha, R. Bajracharya, and S. Y. Nam, "Blockchain-based message dissemination in vanet," in 2018 IEEE 3rd Int. Conference on Comput- ing, Communication and Security (ICCCS), Oct 2018, pp. 161–166.

[32]X. Zhang, R. Li, and B. Cui, "A security architecture of vanet based on blockchain and mobile edge computing," in 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Aug 2018, pp. 258–259.

[33]M. Singh and S. Kim, "Trust bit: Reward-based intelligent vehicle commination using blockchain paper, " in 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Feb 2018, pp. 62–67.

[34] A. Alharthi, Ni, Q., Jiang, R., M. A. Khan , "A Formal Method of Trust Computation in VANET: A Spatial, Temporal and Behavioral Approach," In: Arsenyeva, O., Romanova, T., Sukhonos, M., Tsegelnyk, Y. (eds) Smart Technologies in Urban Engineering. STUE 2022. Lecture Notes in Networks and Systems, vol 536. Springer, Cham. https://doi.org/10.1007/978-3-031-20141-7_69

[35]A. Alharthi, "Blockchain Based Security and Trust Mechanisms for Vehicular Ad hoc Networks," [Doctoral Thesis, Lancaster University]. Lancaster University, 2023, https://doi.org/10.17635/lancaster/thesis/1929

[36]Hancock, J.M., Zvelebil, M.J. and Hancock, J.M. (2014). Jaccard Distance (Jaccard Index, Jaccard Similarity Coefficient). In Dictionary of Bioinformatics and Computational Biology (eds J.M. Hancock and M.J. Zvelebil). https://doi.org/10.1002/9780471650126.dob0956

Authorized licensed use limited to: Lancaster University. Downloaded on June 09,2023 at 14:46:21 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.