mathematics

MDPI

Article

Intelligent Proof-of-Trustworthiness-Based Secure Safety Message Dissemination Scheme for Vehicular Ad Hoc Networks Using Blockchain and Deep Learning Techniques

Fuad A. Ghaleb [1,*], Waleed Ali [2,*], Bander Ali Saleh Al-Rimy [1] and Sharaf J. Malebary [2]

[1] Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru 81310, Johor, Malaysia
[2] Information Technology Department, Faculty of Computing and Information Technology-Rabigh, King Abdulaziz University, Jeddah 25729, Saudi Arabia
* Correspondence: abdulgaleel@utm.my (F.A.G.); waabdullah@kau.edu.sa (W.A.); Tel.: +966-563887947 (W.A.)

Abstract: Vehicular ad hoc networks have emerged as the main building block for the future cooperative intelligent transportation system (cITS) to improve road safety and traffic efficiency and to provide passenger comfort. However, vehicular networks are decentralized, characterized by high mobility and dynamicity, and vehicles move in a hostile environment; such characteristics make VANET applications suffer many security and communication issues. Recently, blockchain has been suggested to solve several VANET issues including the dissemination of trustworthy life-threatening information. However, existing dissemination schemes are inefficient for safety messages and are vulnerable to malicious nodes and rely on the majority of honest assumptions. In the VANET context, adversaries may collude to broadcast false information causing serious safety threats. This study proposes an intelligent proof-of-trustworthiness-based secure safety message dissemination scheme (PoTMDS) to efficiently share only trustworthy messages. The consistency and plausibility of the message were evaluated based on a predictive model developed using a convolutional neural network and signal properties such as the received signal strength and angle of arrival. A blockchain-based data dissemination scheme was developed to share critical messages. Each vehicle calculates the proof of trustworthiness of the disseminated messages by comparing the received message with the output of the prediction model. The results showed that the proposed scheme reduced the consensus delay by 58% and improved the detection accuracy by 7.8%. Therefore, the proposed scheme can have an important role in improving the applications of future cITS.

Keywords: blockchain; consensus; convolutional neural network; Kalman filter; VANET

MSC: 68-00

Citation: Ghaleb, F.A.; Ali, W.; Al-Rimy, B.A.S.; Malebary, S.J. Intelligent Proof-of-Trustworthiness -Based Secure Safety Message Dissemination Scheme for Vehicular Ad Hoc Networks Using Blockchain and Deep Learning Techniques. *Mathematics* **2023**, *11*, 1704. https://doi.org/10.3390/math11071704

Academic Editors: Daniel Ramotsoela, Adnan M. Abu-Mahfouz, Bruno Silva, Umair Mujtaba Qureshi and Zuneera Umair

Received: 24 February 2023
Revised: 19 March 2023
Accepted: 31 March 2023
Published: 2 April 2023

1. Introduction

Vehicular ad hoc networks (VANETs) are a promising technology to enhance road safety, traffic efficiency, and enhance passenger comfort for future intelligent transportation systems. According to the World Health Organization (WHO) [1], millions of people lose their lives and possessions every year as a result of traffic accidents. Accidents lead to the loss of billions of dollars in treatment costs, property damage, wasted time in traffic, increased fuel consumption, and pollution [2]. These problems have a direct or indirect impact on economic activity and sustainability [3]. Studies have shown that more than 90% of road accidents are attributed to human errors and most of these accidents can be avoided if drivers are warned a few seconds before the collision [4–7]. VANETs are considered a key enabler for future intelligent transportation systems (ITS) applications, as it extends the range of awareness beyond that of the driver and conventional sensors. Numerous VANET applications have been developed and investigated, including but not limited

to cooperative active safety systems (CASS) [8], cooperative collision warning systems (CCWS) [7], and driver assistance systems (ADAS) [9].

VANETs have unique characteristics compared to other wireless network technologies in terms of mobility, scalability, security, message descriptions, and types of equipment. With the high mobility and density of vehicles, many VANET applications required that the data produced by vehicle sensors needs to be shared with the neighboring vehicles. Thus, vehicles in VANETs are equipped with several hundred sensors controlled by on-board units (OBUs). The OBUs provide vehicles the ability to sense information related to car status, driving situation, and road features and status and communicate this information with the neighboring vehicles. Vehicles use the dedicated short-range communication protocol (DSRC) and the Wireless access in vehicular environments (WAVE) architecture [10] to share safety and traffic information such as (e.g., traffic jams, accidents, and natural disasters) with other vehicles. The OBU can communicate with road side units (RSU) for disseminating information to extended areas. Vehicles also broadcast real-time traffic messages such as (speed, location, braking, etc.) with nearby vehicles. However, due to the sparse and disconnected environment, VANET applications assume an honest majority of participants. Unfortunately, such an assumption may not be always true in the presence of malicious vehicles which send false information. Thus, the trustworthiness of the information shared in VANETs is a major security concern. There are many solutions that try to disseminate trustworthiness information in VANETs based on data-centric approaches by checking the consistency and plausibility of information such as those in [5,11,12] or based on entity-centric approaches which solely depend on entity trust using cryptographic techniques such as those in [13]. Cryptographic techniques are essential for message integrity [14,15]. However, a compromised vehicle can send false yet authenticated messages. Both entity- and content-centric approaches either apply basic security checks that assume an honest majority or are based on static trust values. Both approaches are ineffective in hostile VANET environments where the colluded vehicles can spread fake information related to its status, road conditions, or traffic situations causing serious life safety threats. Accordingly, disseminating trustworthiness information is challenging due to the VANET's unique requirements in terms of distribution, scale, mobility, density, and hostile environments for a reliable communication and trustworthiness messages.

Recently, blockchain has been used in various fields related to VANETs due to its exceptional characteristics such as distribution, decentralization, tamper-resistance, immutability, availability, and transparency which fit VANET application requirements [16–19]. A blockchain is a decentralized ledger that allows transactions to be securely recorded in a trustworthy environment, without the need for a central authority [20,21]. Jiang and Fang [22] suggested using blockchain to achieve decentralization, data security, and privacy in VANETs. The authors in [23] proposed a trust model based on blockchain for preserving vehicles' privacy. A pseudonym public key was suggested to achieve anonymity while the trustworthiness messages were evaluated based on the entity's reputation which is stored in the blockchain. In [24], blockchain is recommended as a solution for privacy preservation and efficient database management in railway vehicles. One of the ways blockchain is also being used is for storing and distributing messages and event information. Zhang and Chen [25] employed a consortium blockchain to store critical data including the position, direction, location, and authentication information of vehicles. According to [26], blockchain and VANETs can potentially result in secure and reliable vehicle-to-vehicle (V2V) communication.

In a VANET-based blockchain, the main challenge is the selection of a consensus algorithm that ensures that the validity of the message as a false message can disrupt any VANET potential application and is a threat to people's lives. Consensus algorithms can be used for massage validation, distribution, and security preservation. Before adding a transaction to the blockchain, nodes go through a validation procedure, which is referred to as "consensus". In the blockchain, the nodes that participate in this consensus are called the mining nodes, and the node that successfully creates a block is called the "leader" [27].

Proof of work (PoW) is a popular consensus algorithm in which mining nodes compete to find a nonce that solves the hash puzzle. The node that finds the solution first generates the block and receives the incentive. However, PoW is not suitable for VANET-critical applications because it needs around 10 min to solve the hash puzzle [26]. Proof of stake (PoS) is another consensus algorithm that is proposed to reduce the consensus time [28]. In PoS, the node which has the highest trust value called the stack should generate the block and receive the incentives. However, PoS does not provide fairness as the nodes with high trust values always win. Proof of elapsed time (PoET) was proposed to improve fairness. PoET requires nodes to perform a busy-waiting operation for a randomly generated period. Due to the randomness of PoET, nodes may need to wait for a significant amount of time before generating proof. In VANETs, where fast communication is often critical, this can lead to increased latency, which can be problematic for applications that require low latency such as safety applications. In addition, PoET is not secure against malicious nodes. The practical Byzantine fault-tolerant (PBFT) [29] consensus algorithm determines the number of nodes needed to reach an agreement in presence of malicious nodes. However, PBFT requires a significant amount of message exchanges between nodes, which can result in high message overhead. A proof-of-quality-factor (PoQF) [26] consensus algorithm uses a voting mechanism to validate the message. However, PoQF has a high verification delay and assumes an honest majority. Several other blockchain solutions have been proposed [25,30,31] for permissioned blockchains. Most of these solutions have high validation delays and are vulnerable to colluding attacks.

Although many consensus algorithms have been proposed for data dissemination in VANETs [25,27–31], most of these algorithms suffer in terms of security and efficiency. That is, most of the algorithms assume an honest majority assumption among vehicles. This is not a valid assumption because malicious vehicles can collide and create non-existing events causing leader vehicles to endorse false information and add to the blockchain. However, many existing dissemination schemes rely on consensus algorithms that use basic checks to validate the message resulting in consensus on uncertain trustworthiness information. This study proposes an intelligent proof of trustworthiness-based secure safety message dissemination scheme (PoTMDS). A consensus algorithm called proof of trustworthiness in which the trustworthiness of the messages neither relies only on the majority nor the trust value given to a vehicle in the past is used. Alternatively, the mobility information of vehicles is validated by fusing sensor information received from sender vehicles with their signal properties such as received signal strength and angle of arrival using the Kalman filter algorithm. The innovation error of the Kalman filter which represents the inconsistencies of the information was used to train a deep learning event prediction model. A convolutional neural network (CNN)-based prediction model was designed and developed to assist vehicles at the event location to autonomously detect the event. Vehicles at the event location extract the proof of the event based on the mobility patterns of the vehicles passing the event location. The proposed consensus algorithm allows vehicles at the event location to compete validating the event based on the plausibility and consistency of the event as witnessed by the neighboring vehicles. The results show that the proposed consensus algorithm is robust against malicious vehicles which share false mobility information or event messages. The results also show that the proposed solution outperforms the related work in terms of consensus time, verification delay, and communication overhead. The contributions made in this study can be summarized as follows:

- A proof of trustworthiness (PoT) consensus method is proposed, where the mining nodes compete to validate the trustworthiness of the event. Instead of relying on a voting algorithm, nodes independently validate the messages based on the properties of the event message signal (physical evidence) collected by the miner nodes.
- A CNN-based prediction model was designed and developed to autonomously identify the events on the road and used as evidence of the message's correctness. The distribution of innovation errors of the Kalman filter was used to represent traffic

status. An image like grid cells containing the accumulative errors of the vehicles in each cell was used as proof of the event.
- A blockchain-based message dissemination scheme called PoTMDS is proposed to securely share critical messages that are effective and efficient for VANET application requirements.

The remainder of this paper is organized as follows. Section 2 presents the related work. Section 3 describes the proposed solution. The procedures of validation and evaluation are presented in Section 4. The results and performance analysis are discussed in Section 5 while Section 6 concludes the paper.

2. Related Work

Disseminating safety information in VANETs has been a major concern of researchers in the last few years [11,12,26,32–35]. A misbehaving vehicle can generate false mobility patterns and disseminate wrong safety messages. Many researchers use blockchain in various fields related to VANETs because of its exceptional characteristics such as distribution, decentralization, tamper-resistance, immutability, availability, and transparency which meet VANET application requirements [16,19,36–43]. Zhang et al. in [25] used a consortium blockchain to store important information about vehicles such as their position, direction, location, and authentication information. Similarly, Javaid et al. in [44] utilized a blockchain to store registration information and vehicle status. Akhter, Ahmed [45] also used a blockchain to store authentication information and ensure vehicle privacy. It is a common belief that blockchains and VANETs can potentially result in secure and reliable vehicle-to-vehicle (V2V) communications [9]. However, in a VANET-based blockchain, the main challenge is the selection of a consensus algorithm that ensures the validity of the message as a false message and can disrupt any potential VANET application and threats to people's lives.

Many studies have utilized blockchains to validate and disseminate safety messages in VANETs [18,25–27,32–35,38,40,43,46,47]. Most of these studies rely on an extended version of the existing consensus algorithms proposed for conventional blockchains. For permission-less (or public) blockchains, proof of work (PoW), proof of stack (PoS), and proof of elapsed time (PoET) are commonly suggested for VANETs. The consensus algorithms can be categorized into two approaches: proof-based or voting-based. The proof-based approach tries to find proof of either action or situation such as PoW and PoS while the voting-based tries to validate the message based on the entity voting such as in the practical Byzantine fault tolerance (PBFT) [36]. In [17], PoS is compared to PoW and recommended as a promising consensus algorithm for VANETs due to its computational complexity and reduced time delay. Meanwhile, the authors in [33] proposed a blockchain-based approach for message dissemination in vehicular ad hoc networks (VANETs) which uses edge computing and PoW. This approach achieves a reduction in block generation latency by offloading complex computations to capable edge devices. The blockchain in this approach is used to store the trust values of nodes, which are updated based on the validity of the messages initiated by each node. In [48], Khan et al. proposed a blockchain to store trust values and message ratings, where RSUs perform hash computations. However, Wagner and Mcmillin [49] demonstrated that implementing a completely distributed peer-to-peer (P2P) blockchain in VANETs with minimal reliance on RSUs and infrastructure is not possible with PoW and that an RSU-dependent network would be expensive. To address this, ref. [50] proposed a joint PoW and PoS consensus managed by RSUs to store trust values and evaluate message credibility based on the sender's trust value while Liu, Teng [51] used deep reinforcement learning (DRL) to address these technical difficulties by adjusting the block size and interval.

Xie, Ding [52] proposed a message dissemination scheme based on software-defined networks and blockchains. The SDN is used for improving network connectivity while the blockchain is used for decentralization. However, PoW and PoS mechanisms were used for consensus; such mechanisms are inefficient for time-critical applications. Chukwuocha,

Thulasiraman [46] proposed a blockchain-based message exchange scheme for VANETs. The trustworthiness of a message is calculated based on the prior event distribution in the event location. The vehicle trust value is obtained from a hyperledger constructed to hold the trust values of vehicles. A smart contract was developed to query and update vehicle trust values in the hyperledger. However, it is not clear what the consensus is about adding a new block to the blockchain. Moreover, the proposed scheme is vulnerable to the bogus messages that originate in the subject vehicles' OBUs by malicious software. Haddaji, Ayed [53] constructed a blockchain to prevent and detect Sybil attacks. Sybil vehicles are detected using three trust-based mechanisms, namely horizontal trust management (HTM), vertical Trust Management (VTM), and distributed trust management (DTM). In the HTM, vehicles are classified using the support vector machines algorithm (SVM) into malicious or benign. In the VTM, each vehicle sends the classification results to the RSU, and based on the majority voting scheme, the malicious vehicles are identified. Meanwhile, in the DTM, an RSUs-based blockchain is constructed that contains a smart contract to exchange the decision about the vehicles. The proof of work (PoW) consensus mechanism was used to mine and add transactions to the blockchain. However, a predefined and static threshold was used to classify the vehicles into malicious or benign which does not hold for the dynamic vehicular environment. In addition, the proposed blockchain depends on the infrastructure RSU which is impractical for realistic deployment. The authors in [54] proposed a message validation scheme based on a blockchain-enabled trust establishment. However, the Byzantine fault-tolerant consensus mechanism was used for validation. Such mechanisms are vulnerable to colluding attacks.

Shrestha, Bajracharya [33] proposed a message dissemination scheme based on a public blockchain to store the trustworthiness of nodes and their messages in a distributed ledger. However, the proposed scheme assumes the availability of RSUs in the communication range of the vehicles which requires heavy infrastructures costs. Ahmed, Moustafa [40] proposed a message transmission protocol based on the Ethereum blockchain. A local location database is suggested to store the proof of presence. However, the proposed protocol assumes the availability of a centralized server to store the location information of the vehicles to protect against malicious nodes which generate false positioning information. In addition, the mechanisms of the evaluation of the validity of the message have not been discussed. The server may store false location information regarding a vehicle. Table 1 summarizes the consensus mechanisms, trustworthiness assessment methods, and limitations of the existing solutions.

Table 1. Summary of the related solutions.

Scheme	Consensus	Verification Method	Limitations
[33]	PoW	Proof of the location	• High latency due to the use of PoW
[48]	PoW	Entity-centric trust	• Vulnerable to compromised vehicles and RSUs • High latency due to the use of PoW
[50]	PoW & PoS	Distance-based voting	• Heavily depends on the RSUs • Vulnerable to malicious attack • High latency
[51]	PBFT	Majority voting	• (Two/three) of replicas are honest • Crypto-based message validation
[52]	PoS	Entity-centric trust	• The large message size relies on a centralized trusted authority • Crypto-based message validation

Table 1. *Cont.*

Scheme	Consensus	Verification Method	Limitations
[46]	Voting consensus	Bayesian-based inference	• Relies on the voting scheme with a majority honest • No validation of the message content was proposed
[53]	PoW	Distance and spead consistency	• Heavily depends on the infrastructure • Basic consistency and plausibility checks • High latency
[54]	PBFT	Witness scheme	• Heavily depends on the infrastructure • Vulnerable to colluding attacks
[40]	PoS	Proof of presence	• Relay in a centralized server • No content validation

Although there are many solutions proposed for validating and disseminating safety messages in VANETs, these solutions have several drawbacks. As can be seen in Table 1, most of the current solutions suffer from two main concerns: vulnerability to colluding attacks and inefficiency in safety message dissemination. Due to the honest majority assumption, a misbehaving vehicle can create and disseminate false safety messages. The existing consensus algorithms use basic security checks for validating the correctness of the safety message. These basic checks can be bypassed by misbehaving vehicles. In addition, most of the existing mechanisms are inefficient in terms of consensus time or require heavy communication overhead for consensus. In VANETs, where fast communication is often critical, this can lead to increased latency, which can be problematic for applications that require low latency. To this end, this study proposes an efficient yet secure event message dissemination scheme for VANETs that is based on blockchain technology and convolutional neural network techniques. A new consensus method, named PoT, is developed, which includes several proofs, such as proof of location, proof of mobility, and proof of the event, to verify the accuracy of the emergency message before adding it to the blockchain. A proof of event is created using a convolutional-neural-network-based prediction model that is trained by correlating the mobility pattern extracted from the cooperative awareness messages with the event occurrence using the Kalman filter algorithm. A detailed description of the proposed scheme is presented in the subsequent section.

3. Proposed Scheme

The components of the proposed intelligent proof-of-trustworthiness-based secure safety message dissemination scheme (PoTMDS) are illustrated in Figure 1. The proposed scheme consists of three main parts: the event ledger blockchain, the trust ledger blockchain, and the on-board units (OBU) and roadside units (RSU) nodes. A detailed description of each part is in the following subsections.

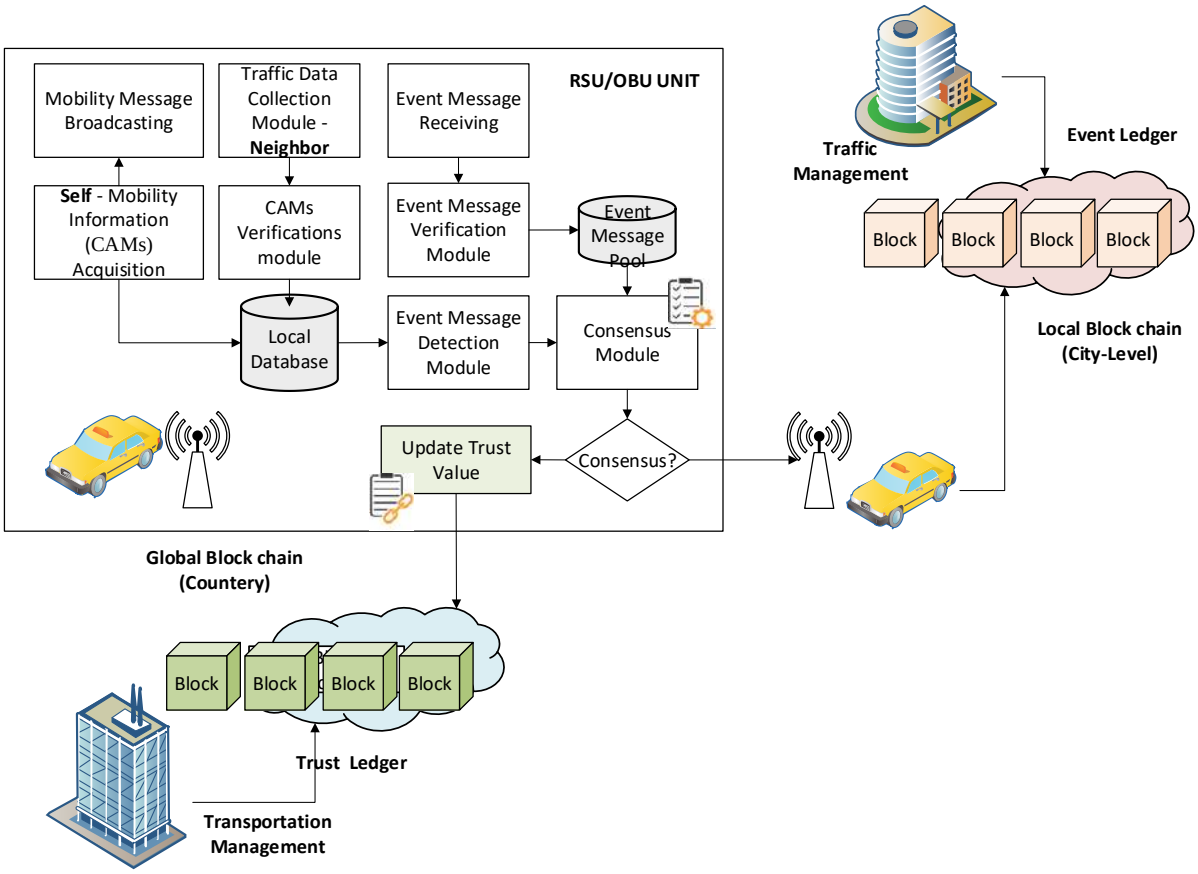


Figure 1. The architecture of the proposed PoTMDS.

3.1. Event Ledger Blockchain

The distributed event ledger is created and managed by the traffic management center. It stores the event message information. VANET applications can use smart contracts to trigger actions related to road safety, traffic efficiency, and passenger comfort. An event such as traffic congestion, accidents, road hazards, slippery roads, etcetera can be stored in the event ledger. Vehicles continuously check the blockchain for any new block added to the area of interest. As vehicles move, the area of interest is updated and thus the related emergency messages will be considered. Because all the messages added to the blockchain are trusted vehicles, it just needs to verify the integrity and origin of the message by validating the certificate and the signature of the message.

3.2. Trust Ledger Blockchain

Similar to [44], this ledger is created to hold the registration information of the vehicles with their trust values. It is created and managed by the transportation authority. Vehicles and RSUs are registered and the initial trust value is given based on the trustworthiness of the messages broadcasted by the vehicles. The trust value of the vehicle is inherited from the trust value given to the owner of the vehicle. If the owner has multiple vehicles, then the trust values are aggregated. Vehicles obtain their pair of public and private keys with pseudonyms IDs. Vehicles use pseudonymous IDs to hide their privacy from pairs. Only trusted RSUs or authorities can resolve the pseudonym ID to the public key of the vehicle. Vehicles request to change their pseudonyms in specific areas and situations such as mix-zone. Thus, vehicles are anonymous but all the important information can be retrieved by pairs from the trust blockchain using a trust-based smart contract.

3.3. RSU/OBU Nodes

The OBU/RSU comprises five modules, namely, a traffic data collection module, a CAMs verifications module, an event message detection module, a block generation module, and a consensus module.

3.3.1. Traffic Data Collection Module

The purpose of this module is to collect the mobility information of the neighboring vehicles. In VANETs, vehicles receive a continuous update of recent mobility information from neighboring vehicles in a range of two kilometers in the form of cooperation awareness messages (CAMs). The CAM messages are essential for safety applications and traffic data collection. They play an important role in validating the event messages because they contain the mobility patterns needed to validate the event [55]. The CAM message contains information that includes vehicle position (e.g., GPS coordinates), speed, acceleration, and direction. According to the IEEE standard, CAMs are broadcasted every 100 ms (10 Hz) [10]. Thus, vehicles can autonomously predict and detect any road events, autonomously by analyzing the mobility information of the neighboring vehicles in terms of time and space. However, misbehaving vehicles which share false mobility information can cause high false alarms and low detection rates and lead to serious safety threats. Therefore, CAMs should be evaluated before they are stored in the local mobility dataset. To evaluate the correctness of the CAM messages, the following steps are suggested based on our previous studies:

1. CAMs Acquisition: In every 100 ms, each vehicle acquires mobility information from onboard sensors and forms its CAM message.
2. CAMs Noise Removing: The vehicle uses the Kalman filter algorithm to fuse sensor information to achieve accuracy. Because vehicle sensors are independent of each other's, e.g., GPS, speedometer, and gyroscope, the Kalman filter is effective noise removal to obtain unified but accurate CAMs. The Kalman filter has been used to fuse information from different sensors to obtain accurate information [56,57].
3. CAMs Broadcasting: A vehicle broadcasts its mobility information to neighboring vehicles. Because CAMs messages contain information regarding vehicle mobility, CAMs are highly predictable. Thus, to reduce communication overhead, vehicles broadcast CAMs messages only if necessaryt, e.g., during maneuvering, acceleration, or deceleration. More precisely, vehicles predict their future CAMs using a vehicle mobility model, and based on the prediction error of the broadcasting, a decision is made [3,58].

3.3.2. CAMs Verifications Module

Once a CAM message is received by neighboring vehicles, vehicles evaluate the correctness of the information using pliability and consistency models such as those proposed in [5]. To detect sophisticated false message attacks, sent by misbehaving vehicles, a vehicle uses physical evidence such as the received signal strength indicator of the received CAM Kalman and signal direction to check the validity of the CAM message [59]. The Kalman filter algorithm is used to fuse the signal properties with CAM information and the innovation error of the Kalman filter is used as an indicator of false messages. Because signal strength can be noisy in high-density scenarios, the noise covariance of the RSSI can be dynamic by aggregating uncertainties of neighbouring vehicles to reduce the false alarm rate. The RSSI is measured by the antennas using the antennas array. RSSIs from different sensors are averaged to remove the noise and obtain more accurate readings. The distance between the receiving and sending vehicles (physical evidence) is calculated using Equation (1):

$$\varphi_k = 10^{(\delta-\omega)/10n} \tag{1}$$

where δ denotes the antenna gain, ω denotes the RSSI value, and n denotes n to the propagation constant or path-loss exponent (this study assumes free space with $n = 2$). The

predicted distance between the receiving and sending vehicles $\hat{\varphi}_k$ is calculated using the position information of the received CAM message (as claimed by the sender) as shown in Equation (2):

$$\hat{\varphi}_k = \sqrt{\left(x_{s(k)} - x_{r(k)}\right)^2 - \left(y_{s(k)} - y_{r(k)}\right)^2} \tag{2}$$

where $x_{s(k)}$ and $x_{r(k)}$ denote the latitude of the sending and receiving vehicles at time epoch k, respectively. $y_{s(k)}$ and $y_{r(k)}$ are the longitude of the sending and receiving vehicles, respectively. The angle of arrival θ_k of vehicle CAM at time k is calculated using array antennas occupied in the receiver vehicle (at least two antennas) as shown in Equation (3):

$$\theta_k = sin^{-1}\frac{\varphi_2 - \varphi_1}{\alpha} \tag{3}$$

where φ_1 and φ_2 denote the distance between receiving and sending vehicles as received by the first and second antennas, respectively, while α denotes the distance between the antennas in the receiving vehicle. The predicted angle of arrival $\hat{\theta}_k$ can also be calculated using the following formula.

$$\hat{\theta}_k = tan^{-1}\frac{x_{s(k)} - x_{r(k)}}{y_{s(k)} - y_{r(k)}} \tag{4}$$

The measurements vector of the Kalman filter is represented as shown in Equation (5):

$$CAM = \begin{bmatrix} x_{s(k)} & y_{s(k)} & vx_{s(k)} & vy_{s(k)} & \theta_k & d_k \end{bmatrix} \rightarrow f_k \tag{5}$$

where $x_{s(k)}$, $y_{s(k)}$, $vx_{s(k)}$, and $vy_{s(k)}$, denote the position and speed of the sender vehicle in both the latitudal and longitudal direction at time epoch k, while θ_k and d_k are the angle of arrival and the distance between sending and receiving vehicles as measured using array antennas and RSSI, respectively. The transition matrix of the Kalman filter $F_{k|k-1}$ which holds the prediction models used to predict the upcoming CAM message at time k from the CAMs estimated at the previous time epoch $k-1$ is formulated as shown in Equation (6):

$$F_{k|k-1} = \begin{bmatrix} x_{s(k)} + Tvx_{s(k)} + \frac{T^2 ax_{S(k)}}{2} \\ y_{s(k)} + Tvy_{s(k)} + \frac{T^2 ay_{S(k)}}{2} \\ vx_{s(k)} + Tax_{S(k)} \\ vy_{s(k)} + Tay_{S(k)} \\ tan^{-1}\frac{x_{s(k)} - x_{r(k)}}{y_{s(k)} - y_{r(k)}} \\ \sqrt{\left(x_{s(k)} - x_{r(k)}\right)^2 - \left(y_{s(k)} - y_{r(k)}\right)^2} \end{bmatrix} \tag{6}$$

where T denotes the broadcasting rate of the sender vehicle in the second while $ax_{s(k)}$ and $ay_{s(k)}$ are the acceleration of the sender vehicle. Thus, for each time epoch, the receiving vehicle predicts the $\widehat{CAM}$ messages of all neighboring vehicles using $F_{k|k-1}$ and once the actual CAM message is obtained. The innovation error Z of the Kalman filter can be calculated using Equation (7):

$$Z_k = CAM - \widehat{CAM} \tag{7}$$

The innovation error of the Kalman filter is used to update the CAM message in the update phase of the Kalman filter. However, in this study, Z_k is used to measure how consistent the information sent by the sender vehicle is with the information perceived by the receiver vehicle using the signal properties. If the discrepancy between the actual CAM

and the predicted $\widehat{CAM}$ between cannot be tolerated, the message is considered false. The box and whisker plot technique was used to detect the outliers as follows:

$$I_k = Q_{75\%} - Q_{25\%} \tag{8}$$

where I_k is the inter quartile range while $Q_{25\%}$, and $Q_{75\%}$ denote to the 25th and the 75th percentile of the innovation sequence, respectively. Let β and γ denote the upper and lower bounds of the innovation sequence error, respectively. The detection rule is formulated as follows:

$$CAM_{Status_k} = \begin{cases} true & \gamma < z_k < \beta \\ false & \beta < z_k \; or \; \gamma > z_k \end{cases} \tag{9}$$

The upper bound β and lower bound γ of the box plot can be calculated as follows:

$$\gamma_k = Q_{25\%} - 1.5 I_k \tag{10}$$

$$\beta_k = Q_{75\%} + 1.5 I_k \tag{11}$$

Each vehicle stores the true CAMs messages received from neighbouring vehicles in the local database (LDB); additional information such as Kalman filter innovation errors are attached with each CAM.

3.3.3. Event Message Detection Module

The event message is generated based on traffic anomalies by analysing the local database collected in the data collection phase. Mobility information (or CAMs) patterns can be used as evidence of the event happening [60]. Each vehicle v has an innovation error associated with specific road position $p(i,j)$ and time epoch k. As shown in Figure 2, the road is represented as a grid. The grid consists of square cells with each square equipped with an area size of one meter squared. The road event area is represented by a sub-grid consisting of $m \times n$ where m is the width length in meters and n is the event area length in meters. In this study, the event area is represented by 10×30 m^2 and each meter squared is represented by a position coordinate $p(x,y)$. When a vehicle $z_{v(k)}$ passes the cell $p(x,y)$, its Kalman innovation error is aggregated with the innovation error of the other vehicles which have passed the same position. The aggregated innovation error of each position $p(x,y)$ in time window w is calculated as follows:

$$z_{t,p(i,j)} = \sum_{t=k}^{w} z_{v(k)} \tag{12}$$

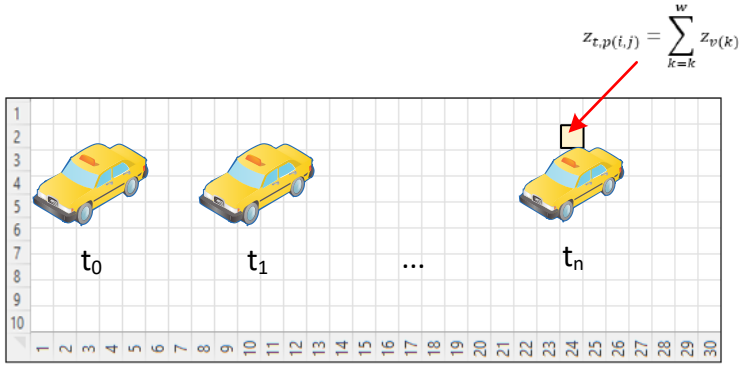


Figure 2. The traffic event area represented as a grid image.

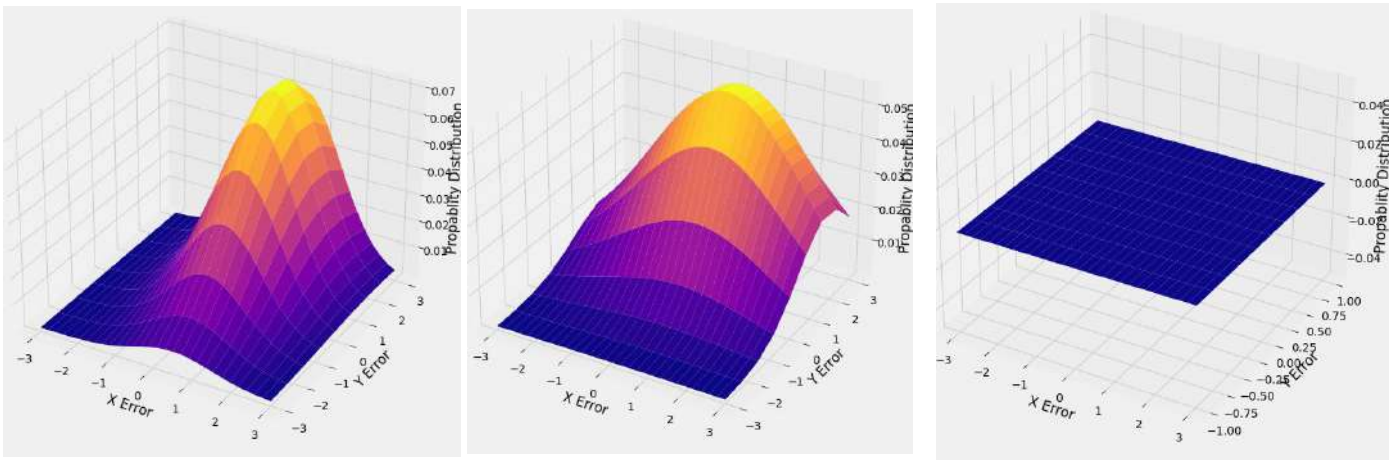
To detect road events, a deep learning classifier based on a convolutional neural network was designed and developed for detecting traffic anomalies. CNNs can effectively capture the patterns and structures in the data, making them useful for identifying anomalies. They can automatically learn and extract features from the input data, which can

be useful in identifying anomalies [61]. CNNs can capture the hierarchical structure in the input data, such as patterns and shapes, by using convolutional and pooling layers. This is useful in anomaly detection as anomalies often have different shapes and patterns compared to normal data [62]. The CNNs are also robust to noise and can handle missing values, making them well suited for real-world anomaly detection tasks where data can be noisy and incomplete such as VANET environments. Figure 3 shows the architecture layers of the proposed classifier. The normal data were collected by simulating vehicle movement using SUMO traffic simulation. The mobility information was generated and stored in the database using Traci in the Python programming environment. The grid of size 10×30 is represented by a two-dimensional array in the Python programming language and stored in the form of images. The traffic anomalies were generated by simulating hard deceleration and stopping in the middle of the road. To represent misbehaving vehicles that send false mobility information, 15% of the vehicles were designed to send false mobility information.

```
Model: "sequential_1"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 conv2d_2 (Conv2D)           (None, 8, 28, 32)         896
 max_pooling2d_2 (MaxPooling 2D)  (None, 4, 14, 32)    0
 conv2d_3 (Conv2D)           (None, 2, 12, 64)         18,496
 max_pooling2d_3 (MaxPooling 2D)  (None, 1, 6, 64)     0
 flatten_1 (Flatten)         (None, 384)               0
 dense_2 (Dense)             (None, 64)                24,640
 dense_3 (Dense)             (None, 10)                650
=================================================================
Total params: 44,682
Trainable params: 44,682
Non-trainable params: 0
_________________________________________________________________
```

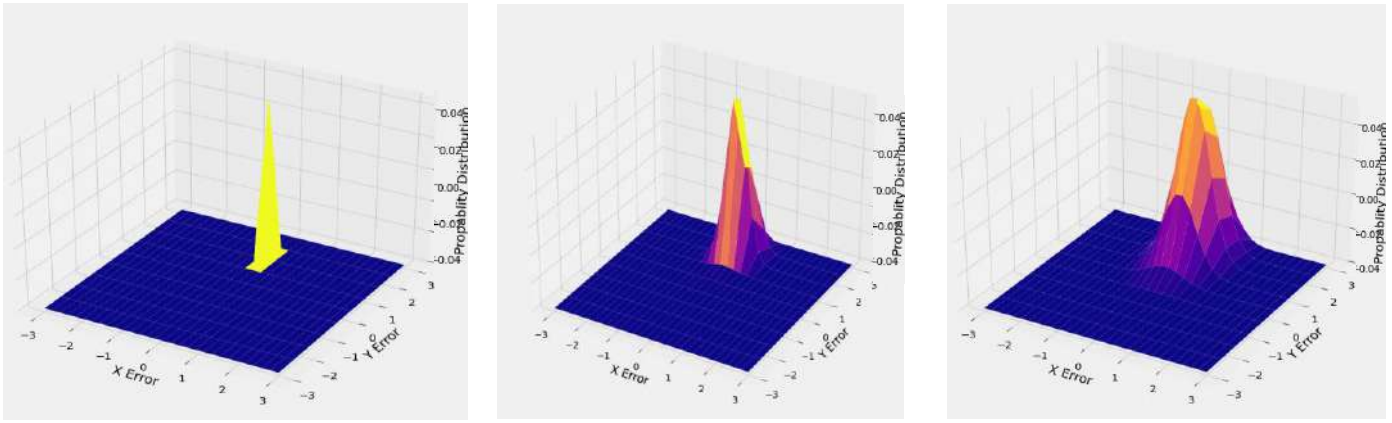
Figure 3. The architecture layers of the proposed CNNs classifier.

To autonomously detect traffic anomalies, a classifier was trained based on the innovation errors of the Kalman filter. As shown in Figure 2, the innovation errors in specific time windows are represented as grid images and thus used as instances for the CNN model to learn from. The normal grid images were constructed for normal traffic scenarios to represent normal situations while the event grid images were constructed during the events to represent the traffic anomalies. The event grid image encompasses information before the event and during the event. The traffic event is centralized in the grid image. That is, the grid image is the aggregated innovation errors of Kalman filters of vehicles before the event until some period after the event happens. The classifiers should learn how to distinguish between grid images that represent normal situations from the grid images that represent traffic anomalies. The hypothesis is that the distribution of the innovation error during the normal event may follow a uniform distribution while there will be a spike at the event position which leads to disturbance in the uniform. The following example demonstrates how innovation errors are utilized as an indicator of traffic anomalies. If a vehicle stops in the middle of the road, other vehicles will slow down and change their lanes. This disturbance in traffic causes the prediction model to wrongly estimate the feature position of the vehicle which leads to high innovation error. The error will be gradually reduced as the vehicles leave the event area. Thus, the change in the error distribution indicates a traffic event. Figure 4 shows the disturbance of the innovation errors during the ideal traffic events: (a) deceleration and stopping, (b) congestion, and (c) normal traffic situations. Figure 5 shows the disturbance of the errors during the ideal traffic events: (a) 1 s, (b) 5 s, and (c) 10 s.



(**a**) (**b**) (**c**)

Figure 4. Probability distribution: (**a**) deceleration and stopping, (**b**) congestion, and (**c**) normal traffic situations.



(**a**) (**b**) (**c**)

Figure 5. The disturbance of the errors during the ideal traffic events: (**a**) 1 s, (**b**) 5 s, and (**c**) 10 s.

3.3.4. Block Generation Module

Upon detection of a traffic anomaly, an event message is generated. The message comprises the following information:

1. Block Header: The header contains the previous hash in the blockchain.
2. Block ID: A random number
3. Vehicle Certificate: The certificate contains the temporal public key of the vehicle which generated the message signed by the certificate authority.
4. Time Stamp: Date and time.
5. Position Coordinate: Position where the event happened.
6. Grid Event Image: This contains a grid of the probability distribution of the Kalman filter innovation error $z_{t,p(i,j)}$.
7. Witnesses List: List of surrounding vehicles that are potential witnesses. The list contains the temporal public keys of the witnesses.
8. Location Certificate: Once a vehicle approaches an RSU or a special vehicle, the vehicle requests a certificate of location. The certificate of location is used to prove the trustworthiness of the vehicle on the road. The certificate is valid for a specific period. An RSU uses a CAMs verification module to evaluate the trustworthiness of the location information of the vehicle.

9. Message Hash: RSA-1024 is used for the message signature. According to the studies in [40,63], ECDSA needs around 10.8 ms for signing and verification while RSA-1024 requires less than 3.10 ms. Due to the availability of mobility information of a vehicle n, vehicles in the area will generate the event message. However, none of the vehicles will add the event message to the blockchain. Thus, the vehicles share the event message with RSUs, special vehicles such as police vehicles, or public vehicles such as public buses. If there are no public trusted vehicles within the event area, a vehicle with the highest trust value will generate the block.

3.3.5. Consensus Module

Upon generating the event message, the vehicle broadcasts the generated block. Each vehicle collects a list of event messages produced by neighboring vehicles in the event location. Then, a collective mining process is performed where all neighboring vehicles try to validate the correctness of the message in parallel. Then, each vehicle in the event area (the region of interest) should sign and then broadcast the predicted event message to the vehicles in its vicinity. Each vehicle validates the trustworthiness of the message according to the consensus method presented in Figure 6. Vehicles start to verify the integrity and authenticity of the message by validating the signature of the event message with the help of the temporary certificate obtained from RSUs. If the certificate is not valid or the signature is not true, then the message will be discarded. Otherwise, the vehicles verify the proof of location using the CAM verification module and the latest location certificate. A vehicle cannot deny sending a message signed by its private key or claim a location outside the communication range of the receiving vehicles. The proof of mobility of the vehicles which send the event message should also be presented in the local database (LDB). Because the nodes in the event position are witnessed vehicles, then they should also detect the event pattern using the CNN prediction module. Then, a vehicle should verify if the event pattern matches the event pattern in the event message, then the message is added to the consensus list. Otherwise, the sender vehicle will be reported as a misbehaving vehicle and its trust value will be updated. If the average trust values of the messages of the consensus vehicles are greater than the average trust of the potential witness vehicles, then a block is generated and signed and then sent to the nearest RSUs using a reliable connection. Both vehicles that generate the event message and will receive an incentive and their trust will be updated. If the trust value of the recipient vehicle is less than the trust value of the sender vehicle, the recipient vehicle compares the represented grid image that contains the event with its own generated grid image. The comparison is performed based on the root mean square error as shown in Equation (13). Another potential strategy for comparison can be used based on the image retrieval used in [64]. The message with the lowest RMSE is added to the blockchain.

$$RMSE = \sqrt{\frac{\sum_{i=1}^{n}(x_s - x_r)^2}{n}} \tag{13}$$

where n is the number of cells in the grid image and x_s and x_r are the cell values of the sent and received grid images, respectively. The RMSE of the message, however, should not exceed a certain threshold. The threshold can be selected based on the lower quartile Q_1 (Q_1 is the 25th percentile) of the box and whisker plot. The threshold value of the consensus trust value (in Figure 6) can be calculated as in Formula (14):

$$\frac{\sum_{i=1}^{C} T_i}{C} > \frac{\sum_{i=1}^{W} T_i}{W} \tag{14}$$

where C and W denote the set of censuses and witness vehicles, respectively, and T_i the trust value of vehicle i as extracted from the blockchain. The wittiness vehicles at the event location with high trust values are eligible for consensus. In another words, a vehicle with a trust value higher than the average trust value of wittiness vehicles is eligible for

consensus. Suspicious vehicles that have high innovation errors from the CAM verification module are excluded from the consensuses. Figure 6 shows the flowchart of the proposed consensus method.

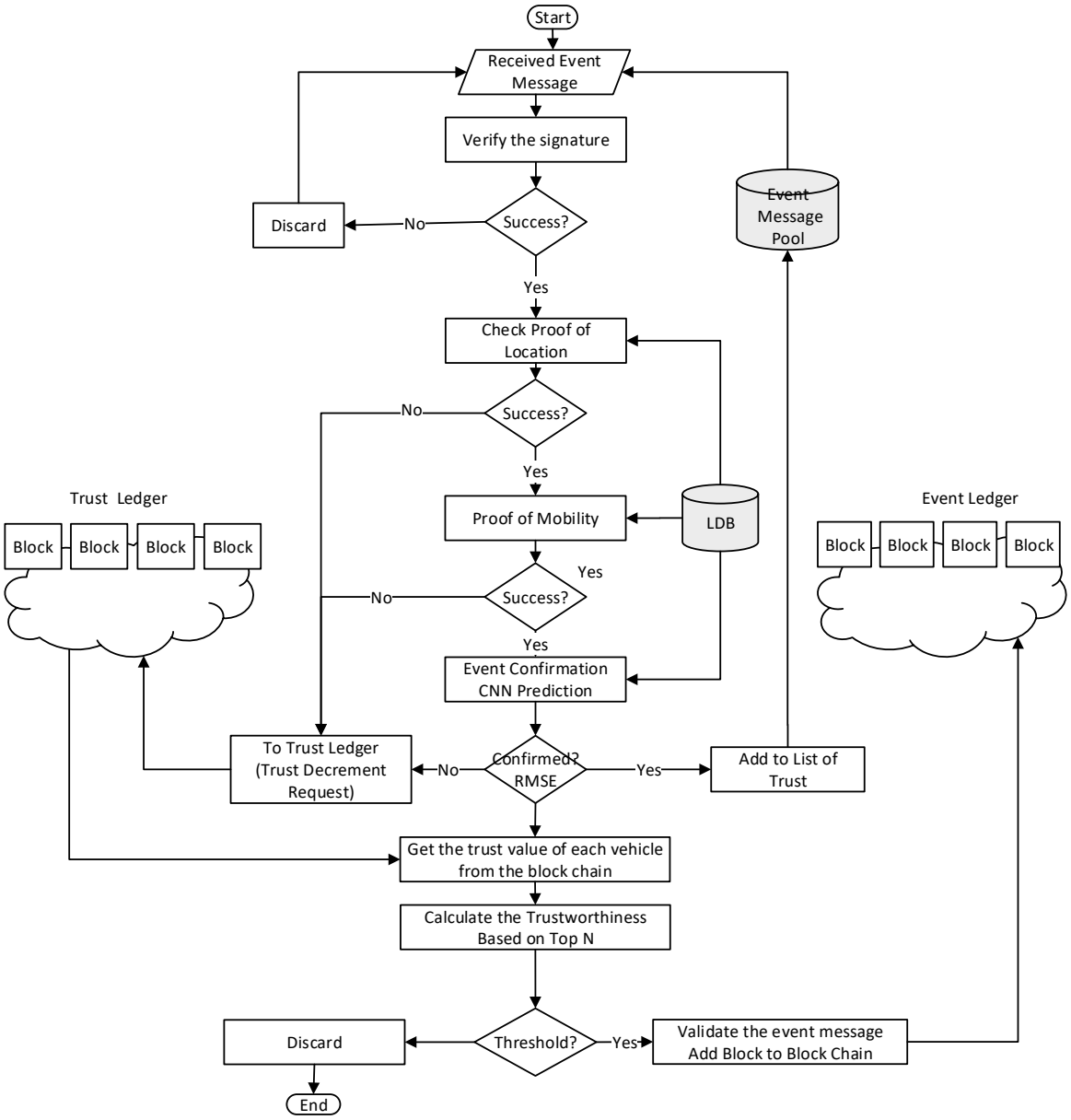


Figure 6. The flowchart of the proposed consensus scheme.

4. Performance Evaluation

Proof of concept based on the simulation has been conducted to validate and evaluate the proposed consensus method. Detailed information about the simulation setup and performance measures are presented in the following subsections.

4.1. Experimental Environment

The simulation of urban mobility (SUMO) has been used in this study to generate vehicle traffic. SUMO is a common simulation tool used to evaluate VANET solutions in related studies. The map that was used in the experiment (see Figure 7) was extracted from open street maps and fed into SUMO to generate traffic data. Vehicles are generated randomly and directed to different destinations on the map. Two scenarios were created: a low traffic scenario (50 vehicles in each square kilometer) and a high traffic scenario

(200 vehicles in each square kilometer). The dataset used in the study was extracted from a three km-length and three-lane road. The SUMO simulator is connected to the Python programming environment through the Traffic Control Interface TraCI Python library. Vehicle positions, speeds, acceleration, direction, and road lane numbers are extracted. For each simulated vehicle, a dataset that represents vehicle movement was extracted and stored in the local database (LDB) in the form of CAMs for each row. LDB contains the mobility information of the vehicle within 2 km (the communication range is assumed to be one km according to the IEEE standard). Table 2 shows the simulation parameters used in the experiment.

Figure 7. Simulation scenarios.

Table 2. Simulation parameters.

Parameter	Value	Parameter	Value
Simulation Time	3600 s	Communication Protocol	IEEE 802.11 p
Average Speed	50 km per hour	Communication Range	1000 m
Max Vehicle Density	200 vehicles per km^2	Data Rate	3 Mbps
Min Vehicle Density	50 vehicles per km^2	CAM Size	500 Byte
Mobility Model	Freeway	Max CAM Broadcasting Rate	10 per second
Road Length	3 km	Propagation Model	Two-ray path-loss

4.2. Event Detection Model Training and Testing

As explained in the previous section, two scenarios were simulated, one for high-density and the other for low-density scenarios considering the parameters in Table 2. Vehicle movements were simulated using SMO software based on the map obtained from the OpenStreetMap (https://www.openstreetmap.org/ (accessed on 13 February 2023)) (See Figure 7). To simulate the traffic events, some vehicles were selected randomly in different time epochs to slow down and stop in the middle of the road. In response, the following

vehicles also decelerate or change lanes accordingly to avoid collisions. Such sudden deceleration and stopping make a disturbance in the traffic follow and produce traffic anomalies. To simulate misbehaving vehicles, 15% of the vehicles were programmed to send false mobility information. The attacks include the basic and sophisticated creation of fake mobility information such as fake deceleration, fake stopping, and fake maneuvering. A homogenous noise environment with a normal distribution of a 1.8 m error average was assumed in the GPS noise information. The CAM messages are appended gradually in every time epoch. In each time epoch, each vehicle verifies the correctness of CAM messages using the aforementioned CAMs verifications module. The dataset consists of a total of 16,657 images created and used for training and testing. As explained in Section 3.3.3, the innovation error of the Kalman filter was aggregated to generate the grid images (see Figure 2). The total number of images with traffic anomalies is 8387; meanwhile, 8270 images contain normal traffic. The CNN model was trained based on 70% of the dataset, while 30% was used for testing. The CNN model was constructed using the Keras framework in Python. Then, the constructed model was used for online operation by integrating the trained classifier into the SUMO scenarios through the Traffic Control Interface TraCI Python library.

4.3. Evaluation Measures

We used some common measures in this study such as the event detection accuracy, recall, precision, false positive rate, false negative rate, success rate, average consensus time, and average delay. The event detection accuracy is calculated using Equation (15):

$$Acc = \frac{n_t}{N} \tag{15}$$

where n_t is the number of traffic images correctly classified divided by the number of total classified images. The recall is defined as the number of traffic anomalies correctly identified n_{tp} divided by the total number of actual traffic anomalies N_p.

$$recall = \frac{n_{tp}}{N_p} \tag{16}$$

The precision is the number of traffic anomalies correctly identified n_{tp} divided by the total number of predicted traffic anomalies N_{pp}.

$$\text{precision} = \frac{n_{tp}}{N_{pp}} \tag{17}$$

The false positive rate (FPR) is the number of traffic anomalies wrongly identified n_{fp} divided by the total number of actual traffic anomalies N_p.

$$\text{FPR} = \frac{n_{fp}}{N_p} \tag{18}$$

The false negative rate (FNR) is the number of normal traffic images wrongly identified n_{fn} divided by the total number of actual normal traffic images N_n.

$$\text{FPR} = \frac{n_{fn}}{N_n} \tag{19}$$

The average message success rate is the total number of event messages that have been successfully added to the blockchain. It is the ratio of the number of verified messages m_i by a consensus node i and the received message. It is equivalent to the message delivery ratio when the source is the vehicles that generate the block.

$$\text{SR} = \frac{m_i}{N_p} \tag{20}$$

The message failure rate FR is calculated based on SR as follows. $FR = 1 - \text{SR}$. The average delay is the time spent since the event was detected until it is received by the destination.

$$average\ delay = \sum_{i=1}^{N} \frac{\left(T_{p(i)} + T_{s(i)} + T_{c(i)} + T_{v(i)} + T_{td(i)}\right)}{N} \tag{21}$$

where $T_{p(i)}$, $T_{s(i)}$, $T_{c(i)}$, and $T_{td(i)}$ denote to the time of processing, signature time, consensus time, verification, and transmission latency, respectively.

5. Results and Discussion

The security analysis and performance evaluation are discussed in this section to show the advantages of the proposed PoT scheme.

5.1. Security Analysis

In the following subsections, the security analysis of the proposed PoT dissemination scheme is presented.

Decentralization: A blockchain is stored in multiple nodes in the network such as RSUs, special vehicles such as police and emergency vehicles, and also in public vehicles such as buses. The rationale behind these selected vehicles is that those vehicles can have enough resources that are needed for scalability and also so they are easy to maintain by trusted parties. Because the storage is distributed on multiple nodes (police cars, emergency vehicles, buses, etc.), the proposed solution does not rely on vulnerable centralized or trusted third-party storage. That is, a compromised node will be disclosed and thus it is not possible to disseminate fake messages. Assuming an event message size of 800 bytes as computed based on the event message generation module, the message size is consistent with the related studies [5,25] as it is assumed to be between 500 bytes and 1500 bytes in the basic safety messages (BSM) in the United Sates' WAVE standards [10]. Table 3 shows the maximum expected size of the blockchain in gigabytes. Even with 1000 years, the blockchain can only be 292 GB. Such a size is reasonable for VANETs.

Table 3. The maximum message size is 800 bytes (including the signature).

	Assuming 1000 Events	**Assuming 2000 Events**	**Assuming 5000 Events**
#Year	**Block Chain Size (GB)**	**Block Chain Size (GB)**	**Block Chain Size (GB)**
1	0.292	0.584	1.46
10	2.92	5.84	14.6
100	29.2	58.4	146
1000	292	584	1460
10,000	2920	5840	14,600

Privacy Protection: To preserve the vehicles' real identity, the vehicles generate a temporal pseudonym public key and obtain certification for their temporal pseudonym public key. Vehicles are allowed to change their public keys in mix zones only where there are RSUs or special vehicles such as police vehicles. The authorities authenticate the vehicles and sign the temporal pseudonym public key. Attackers cannot identify the real vehicle identified as the vehicle uses a temporal key. Even if the attacker analyzes the event messages stored in the blockchain, it is impossible to link the pseudonyms keys to each other. The event messages in the blockchain that are generated by the vehicle are rare. It might be very difficult to find them unless the attacker carries out brute force attacks. In this case, the attacker may have $p = \frac{m}{n}$ where m is the number of event messages generated by a vehicle and n is the total number of messages. Given that m is less than 10 per day for some vehicles such as taxis and the total events may reach 5000, the probability of finding a two-message generated by the same vehicle is 0.2%. Even if the worst case happens it is

impossible to retrieve the true identity from the pseudonym's ID. The proposed solutions rely on temporal IDs so that it is impossible for an attacker to access the encrypted keys in a short time by brute force. Only the authorities can identify the true identity of the vehicle by linking the pseudonyms of a vehicle with its true identity so that incentives and trust values can be identified.

Integrity Protection: Vehicles sign their generated messages using their private keys. To verify the signature vehicles, it is required first to verify the certificate using the public authority key. If the certificate is valid then the signature is verified. It is difficult for an attacker to reuse the certificate of other vehicles because the digital signature is generated using the private key of the vehicles. In addition, vehicles that sign the message cannot deny the signature, so the non-repudiation service is achieved. If verification is not successful, the message will not be endorsed during the consensus. The time verification of the signature is averaged at 0.51 ms. That means within 100 ms which is the period of communication in the IEEE standard [10]; a vehicle can verify around 196 vehicles.

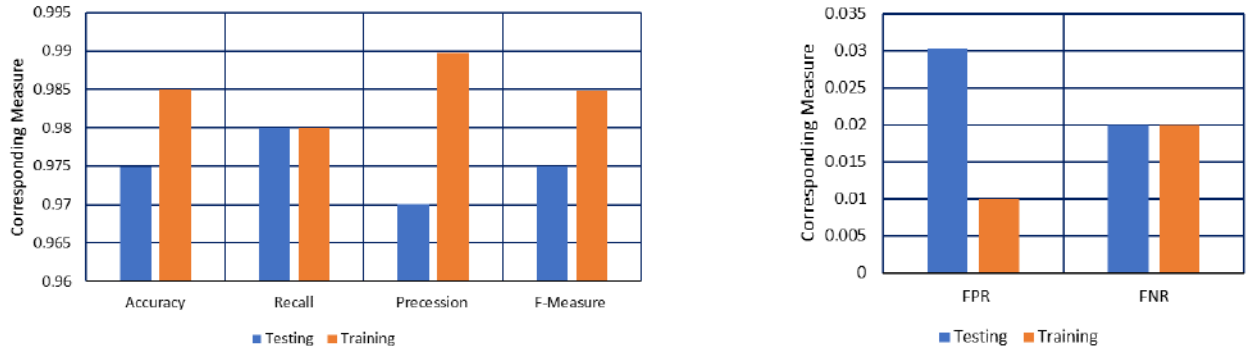
Security Against Malicious Vehicle: An adversary can generate two types of messages: basic safety message part 1 (CAM or mobility information) or an event message (EM or basic safety message part 2). Vehicles that generate false CAMs will be detected by neighboring vehicles using the CAMs detection module. The CAMs detection module uses the signal properties and Kalman filter algorithm to fuse sensor information generated from both sender and receiver vehicles. The signal properties are out of the attacker's control because they are measured by the receiver which verifies the message's trustworthiness. The event message should carry the error map which should be consistent with the error map that is generated by the verifier. Thus, the CAM detection model is robust against malicious vehicles which send false information. Similarly, if the event message is fabricated, it will be detected easily as proof that the event did not occur. All neighboring vehicles will detect the fake event message. With integrity protection, a vehicle cannot send a message on behalf of other vehicles. A vehicle uses its private key to generate the digital signature of the message to ensure no attacker can sign on behalf of the legitimate vehicle. An attacker which controls multiple vehicles should be able to avoid the existence in the range of the trusted verifiers and should be able to compromise more than 50% of the trusted verifiers which have high trust values. Such a condition is challenging to be satisfied in practical situations. Thus, the proposed event dissemination scheme can easily detect false messages.

5.2. Simulation Results Analysis

The performance in terms of event detection accuracy, the efficiency of the message dissemination, and the message success and failure rate are presented in the following subsections.

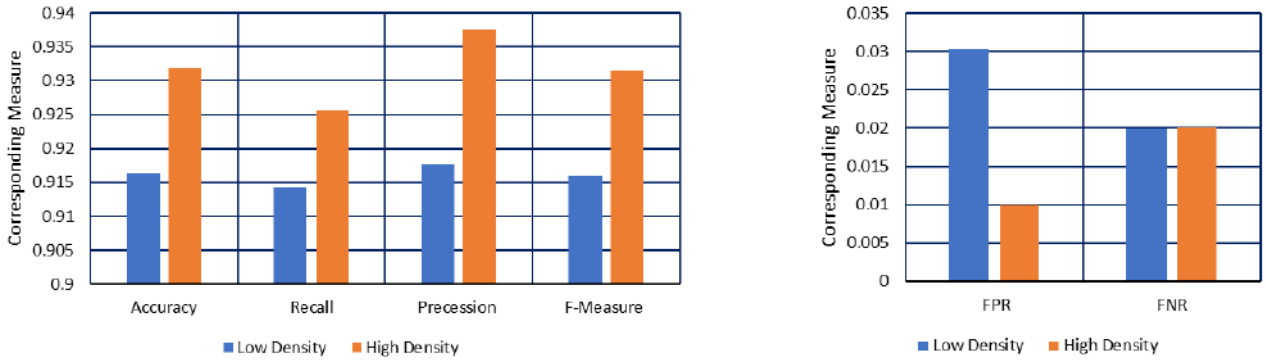
Event Prediction Model Performance: The performance of the proposed consensus method depends on the performance of the event prediction model because the event prediction model carries the proof of the road incident. Figure 8 shows the training and testing performance of the proposed model. Meanwhile, Figure 9 shows the testing performed in the two simulated scenarios: high density and low density.

As shown in Figure 8, the performance of the prediction model on the training set reaches 98.5%, 98%, 99%, and 98.5% in terms of accuracy, detection rate, precession, and F-measure, respectively. Meanwhile, the performance achieved on the testing set reached 97.5%, 98%, 97%, and 97.5%, respectively. The constructed model is also applied during the simulation run time and a prediction is conducted at every time epoch to detect the event as early as possible. As shown in Figure 9, the performance achieved in terms of accuracy, detection rate, precession, and F-measure in the low-density scenario is 91.6%, 91.4%, 94.18%, and 91.6%, respectively, while it is 93.2%, 92.6%, 93.8%, 93.2%, respectively in the high-density scenario.



(**a**) (**b**)

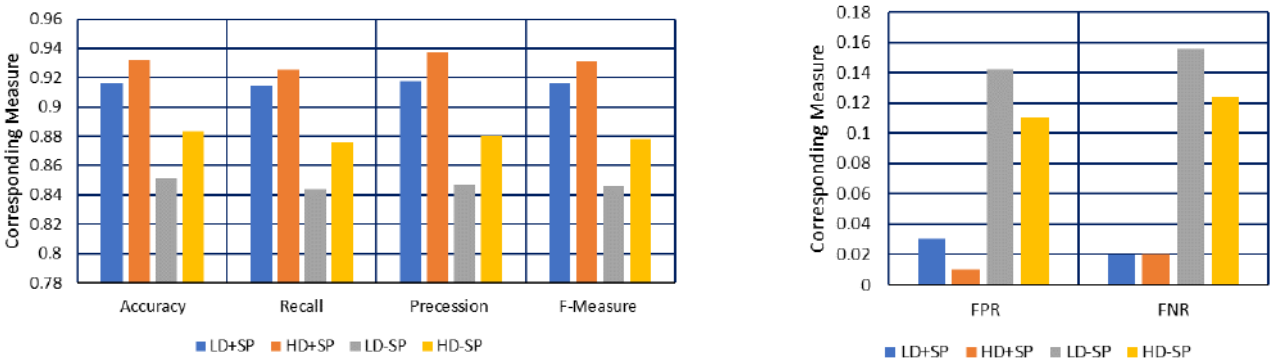
Figure 8. Event prediction performance of training and testing offline in terms of (**a**) Accuracy, Recall, Precession, and F-Measure, and (**b**) False Positive Rate (FPR) and False Negative Rate (FNR).



(**a**) (**b**)

Figure 9. Event prediction performance of testing during the run Time in terms of (**a**) Accuracy, Recall, Precession, and F-Measure, and (**b**) False Positive Rate (FPR) and False Negative Rate (FNR).

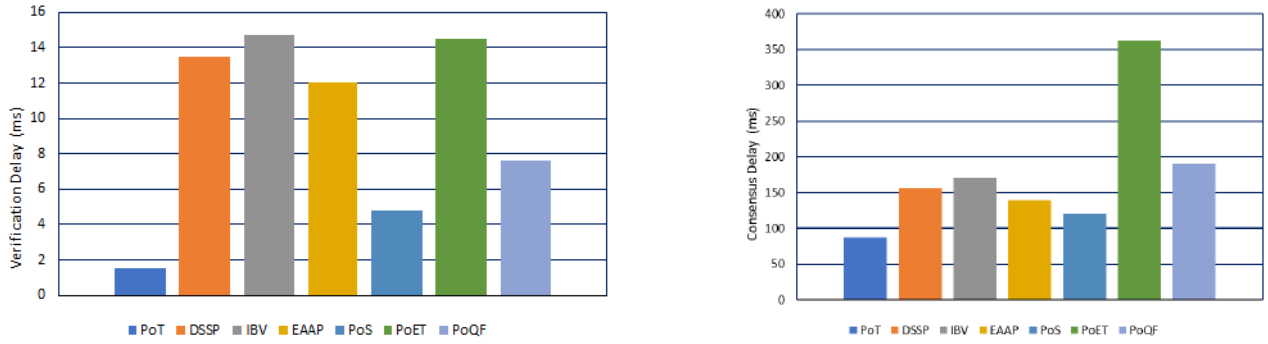
Figures 8 and 9 show the performance of the proposed event detection model while Figure 10 shows the gains when the signal properties (RSSI and AoA) were utilized for improving false CAMs detection. In Figure 10a,b, LD+SP and HD+SP denote the low and high-density scenarios, respectively, with signal properties included (AoA and RSSI) for CAMs detection while LD-SP and HD-SP denote the same scenarios without including the signal properties. In the absence of RSSI and AoA, attackers can send fake movement information with a wide scope. However, the attack scope is eliminated using these two features leading to high detectability of fake CAM messages and thus the exclusion from the grid image which represents the event messages (see Figure 8a). As can be seen in testing, the performance of the event detection model is 97.5%. Both highly dynamic mobility and misbehaving vehicles contribute to degrading the quality of the grid image that represents the traffic anomalies. In the low density scenario, it is difficult to distinguish due to a lack of sufficient information. Similarly, misbehaving vehicles collude and send false CAM messages aiming at generating fake mobility patterns to trigger the event detection model in the benign vehicles to generate fake event messages. Without the AoA and RSSI features, such misbehavior influences the event detection performance. As can be seen in Figure 10a,b, the inclusion of RSSSI and AoA leads to improving the accuracy of the event detection in both scenarios. The accuracy improvements achieved are 6.5% and 4.9% for low and high-density scenarios, respectively (see Figure 10a). Meanwhile, the false positive rate and the false negative rate dropped by 6% and 7% for the low-density scenario and 5% for the high-density scenario, respectively. Although the false CAMs detection module can correct the false messages, attackers can still impact the event detection accuracy.



(**a**) (**b**)

Figure 10. Event prediction performance of testing during run time with and without the AoA and RSSI in the CAM validation (**a**) Accuracy, Recall, Precession, and F-Measure, and (**b**) False Positive Rate (FPR) and False Negative Rate (FNR).

Delay and Communication Overhead: Figure 11a,b and Table 4 show the results in terms of delay and communication overhead. The time needed for validating the event message is 1.51 ms compared to 13.5 ms, 14.7 ms, 12 ms, 4.8 ms, 14.5 ms, and 7.6 ms for DSSP [25], IBV [30], EAAP [31], PoS, PoET, and PoQF [26], respectively. The verification delay of PoS and PoET can vary based on the used signature algorithm. The average delay is directly affected by the validation and consensus delay. Meanwhile, the average consensus time achieved by the proposed PoT scheme is 87.6 ms. Compared to the existing methods of DSSP [25], IBV [30], EAAP [31], PoS, PoET, and PoQF [26], which achieved 156.52 ms, 170.43 ms, 139.13 ms, 119.7 ms, 362.5 ms, and 190.2 ms, respectively, the proposed scheme reduced the consensus delay by 58.9%. The consensus delay includes the time needed for verification and validation of the correctness of the event message. On average, the proposed PoT achieved a 155.2 ms delay. The average delay is the time required for detecting, gaining consensus of, transmitting, and validating the event message.



(**a**) (**b**)

Figure 11. Comparison of verification and consensus delay. (**a**) Validation delay and (**b**) consensus delay.

In VANETs, 155.2 ms for event dissemination is acceptable with most safety and traffic efficiency applications. The average time needed by a human driver to respond to an accident is 1.5 s which is lower than the maximum transmission delay recorded in the experiments. The maximum delay could reach 306.6 ms in some situations such as high-density scenarios. In terms of communication overhead, in each time epoch, a vehicle needs to sign a CAM message and it needs to verify a maximum of 200 vehicles in a high-density scenario (worst-case scenario). The maximum time needed for generating and sending event messages is 105.2 ms assuming 200 vehicles in the communication

range. Although this time is slightly greater than 100 ms, it is not necessary to verify all the messages received from neighboring vehicles as long as the innovation error of the Kalman filter is not consistent with the temporal innovation error of the vehicles. The average delay is 87.6 ms in generating and disseminating event messages.

Table 4. Delay and communication overhead.

Average Performance Measure	Values
Signature delay (RSA-1024)	4.6 ms
Message verification delay	1.5 ms
Message consensus delay	87.6 ms
The average delay	155.2 ms
Max delay	306.6 ms (HD)
Event message communication overhead	105.2 ms (HD)
CAMs communication overhead	25.1 ms (HD)

Compared to the common types of consensus methods such as PoW which needs 10 min to solve the puzzle [26], PoS and PoET achieve more efficient consensus delays of 119.7 and 365.9, respectively. However, the proposed PoT algorithm is more efficient and suitable for critical time applications in VANETs than PoS and PoET. The proposed PoT consensus doesn't require solving a difficult puzzle like PoW, it does not require time to select the relay node or perform voting; in addition, it does not require waiting a random time.

Message Success/Failure Rate: In the proposed PoT, nodes compete to find the consensus nodes with the highest trust values to validate the message and generate the block. Hence, the message success rates for low and high density are 91.43% and 91.96%, respectively, and the message failure rates for low- and high-density scenarios are 8.67% and 8.04%, respectively. As compared to the existing consensus methods such as PoS and PoET, which achieved 21.7%, and 18.1% failure rates, respectively, the proposed PoT consensus algorithm is more effective.

6. Conclusions and Future Work

In this study, an event message dissemination scheme for VANETs is proposed based on blockchain technology and the convolutional neural network technique. An efficient and secure consensus method called PoT was designed and developed that comprises multiple proofs such as proof of location, proof of mobility, and proof of event to validate the correctness of the emergency message before it is added to the blockchain. A proof of event has been created using a convolutional-neural-network-based prediction model that was trained based on correlating the mobility pattern extracted from the cooperative awareness messages. The occurrence of the event is represented by mobility patterns generated using the help of the Kalman filter algorithm and the signal properties such as RSSI and AoA for proof of trustworthiness. The results showed that the proposed dissemination scheme reduced the consensus time by 58.7% while the message failure rate was reduced by 7%. The proposed scheme shows its suitability to meet VANET critical time applications. Although the proposed scheme is highly secure against malicious vehicles, an in-depth investigation is needed. In future work, the authors will explore the robustness of the proposed scheme to different percentages of malicious vehicles. The proposed scheme assumes that the trust establishment mechanisms are ideal for VANETs which needs more investigation. In addition, although the false CAMs detection module can correct false messages, attackers still can impact the event detection accuracy. Such limitations can be improved by improving the estimation capability in the CAM detection model. Moreover, other deep learning techniques may be used to improve event detection accuracy.

Author Contributions: Conceptualization, F.A.G. and W.A.; methodology, F.A.G. and W.A.; software, F.A.G.; validation, W.A., B.A.S.A.-R. and S.J.M.; formal analysis, F.A.G., B.A.S.A.-R. and S.J.M.; investigation, W.A.; resources, F.A.G.; data curation, F.A.G.; writing—original draft preparation, F.A.G.; writing—review and editing, W.A.; visualization, F.A.G.; supervision, W.A.; project administration, W.A.; funding acquisition, W.A. All authors have read and agreed to the published version of the manuscript.

Funding: King Abdulaziz University—Institutional Funding Program for Research and Development—Ministry of Education: IFPIP:408-830-1442.

Data Availability Statement: Not applicable.

Acknowledgments: This research work was funded by Institutional Fund Projects under grant no. (IFPIP:408-830-1442). Therefore, the authors gratefully acknowledge technical and financial support from the Ministry of Education and King Abdulaziz University, DSR, Jeddah, Saudi Arabia.

Conflicts of Interest: The authors declare that no conflicts of interest exist.

References

1. Word Health Organization. 10 Facts about Road Safety. Available online: https://www.who.int/news-room/facts-in-pictures/detail/road-safety (accessed on 22 July 2022).
2. Xu, J.; Zadorozhny, V.; Zhang, D.; Grant, J. FaNDS: Fake News Detection System using energy flow. *Data Knowl. Eng.* **2022**, *139*, 101985. [CrossRef]
3. Ghaleb, F.A.; Al-Rimy, B.A.S.; Almalawi, A.; Ali, A.M.; Zainal, A.; Rassam, M.A.; Shaid, S.Z.M.; Maarof, M.A. Deep Kalman Neuro Fuzzy-Based Adaptive Broadcasting Scheme for Vehicular Ad Hoc Network: A Context-Aware Approach. *IEEE Access* **2020**, *8*, 217744–217761. [CrossRef]
4. Vahdat-Nejad, H.; Ramazani, A.; Mohammadi, T.; Mansoor, W. A survey on context-aware vehicular network applications. *Veh. Commun.* **2016**, *3*, 43–57. [CrossRef]
5. Ghaleb, F.A.; Aizaini Maarof, M.; Zainal, A.; Rassam, M.A.; Saeed, F.; Alsaedi, M. Context-aware data-centric misbehaviour detection scheme for vehicular ad hoc networks using sequential analysis of the temporal and spatial correlation of the consistency between the cooperative awareness messages. *Veh. Commun.* **2019**, *20*, 100186. [CrossRef]
6. Alghamdi, W.; Shakshuki, E.; Sheltami, T.R. Context-Aware Driver Assistance System. *Procedia Comput. Sci.* **2012**, *10*, 785–794. [CrossRef]
7. Huang, C.M.; Lin, S.Y. Cooperative vehicle collision warning system using the vector-based approach with dedicated short range communication data transmission. *IET Intell. Transp. Syst.* **2014**, *8*, 124–134. [CrossRef]
8. Mchergui, A.; Moulahi, T.; Ben Othman, M.T.; Nasri, S. Enhancing VANETs broadcasting performance with mobility prediction for smart road. *Wirel. Pers. Commun.* **2020**, *112*, 1629–1641. [CrossRef]
9. Li, L.; Wen, D.; Zheng, N.-N.; Shen, L.-C. Cognitive cars: A new frontier for ADAS research. *IEEE Trans. Intell. Transp. Syst.* **2011**, *13*, 395–407. [CrossRef]
10. *IEEE Std 1609.0-2013*; IEEE Guide for Wireless Access in Vehicular Environments (WAVE)-Architecture. IEEE: Piscataway, NJ, USA, 2014.
11. Shahwani, H.; Attique Shah, S.; Ashraf, M.; Akram, M.; Jeong, J.; Shin, J. A comprehensive survey on data dissemination in Vehicular Ad Hoc Networks. *Veh. Commun.* **2022**, *34*, 100420. [CrossRef]
12. Oliveira, R.; Montez, C.; Boukerche, A.; Wangham, M.S. Reliable data dissemination protocol for VANET traffic safety applications. *Ad Hoc Netw.* **2017**, *63*, 30–44. [CrossRef]
13. Hussain, R.; Lee, J.; Zeadally, S. Trust in VANET: A Survey of Current Solutions and Future Research Opportunities. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 2553–2571. [CrossRef]
14. Verma, R.; Kumari, A.; Anand, A.; Yadavalli, V. Revisiting shift cipher technique for amplified data security. *J. Comput. Cogn. Eng.* **2022**, 1–7.
15. Namasudra, S.; Devi, D.; Choudhary, S.; Patan, R.; Kallam, S. Security, privacy, trust, and anonymity. In *Advances of DNA Computing in Cryptography*; Chapman and Hall/CRC: London, UK, 2018; pp. 138–150.
16. Dwivedi, S.K.; Amin, R.; Das, A.K.; Leung, M.T.; Choo, K.K.R.; Vollala, S. Blockchain-based vehicular ad-hoc networks: A comprehensive survey. *Ad Hoc Netw.* **2022**, *137*, 102980. [CrossRef]
17. Nguyen, C.T.; Hoang, D.T.; Nguyen, D.N.; Niyato, D.; Nguyen, H.T.; Dutkiewicz, E. Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities. *IEEE Access* **2019**, *7*, 85727–85745. [CrossRef]
18. Patel, A.; Shah, N.; Limbasiya, T.; Das, D.; IEEE. VehicleChain: Blockchain-based Vehicular Data Transmission Scheme for Smart City. In Proceedings of the IEEE International Conference on Systems, Man and Cybernetics (SMC), Bari, Italy, 6–9 October 2019; pp. 661–667.
19. Namasudra, S.; Sharma, P. Achieving a Decentralized and Secure Cab Sharing System Using Blockchain Technology. *IEEE Trans. Intell. Transp. Syst.* **2022**, 1–10. [CrossRef]

20. Sharma, P.; Namasudra, S.; Chilamkurti, N.; Kim, B.-G.; Gonzalez Crespo, R. Blockchain-Based Privacy Preservation for IoT-Enabled Healthcare System. *ACM Trans. Sens. Netw.* **2022**, *19*, 1–17. [CrossRef]
21. Namasudra, S.; Akkaya, K. Introduction to Blockchain Technology. In *Blockchain and Its Applications in Industry 4.0*; Namasudra, S., Akkaya, K., Eds.; Springer Nature Singapore: Singapore, 2023; pp. 1–28. [CrossRef]
22. Jiang, T.; Fang, H.; Wang, H. Blockchain-based internet of vehicles: Distributed network architecture and performance analysis. *IEEE Internet Things J.* **2018**, *6*, 4640–4649. [CrossRef]
23. Lu, Z.; Liu, W.; Wang, Q.; Qu, G.; Liu, Z. A Privacy-Preserving Trust Model Based on Blockchain for VANETs. *IEEE Access* **2018**, *6*, 45655–45664. [CrossRef]
24. McMahon, P.; Zhang, T.; Dwight, R. Requirements for big data adoption for railway asset management. *IEEE Access* **2020**, *8*, 15543–15564. [CrossRef]
25. Zhang, X.; Chen, X. Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network. *IEEE Access* **2019**, *7*, 58241–58254. [CrossRef]
26. Ayaz, F.; Sheng, Z.G.; Tian, D.X.; Guan, Y.L. A Proof-of-Quality-Factor (PoQF)-Based Blockchain and Edge Computing for Vehicular Message Dissemination. *IEEE Internet Things J.* **2021**, *8*, 2468–2482. [CrossRef]
27. Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Wen, Y.; Kim, D.I. A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access* **2019**, *7*, 22328–22370. [CrossRef]
28. Kang, J.; Xiong, Z.; Niyato, D.; Ye, D.; Kim, D.I.; Zhao, J. Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2906–2920. [CrossRef]
29. Kudva, S.; Badsha, S.; Sengupta, S.; Khalil, I.; Zomaya, A. Towards secure and practical consensus for blockchain based VANET. *Inf. Sci.* **2021**, *545*, 170–187. [CrossRef]
30. Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K. Where is current research on blockchain technology?—A systematic review. *PLoS ONE* **2016**, *11*, e0163477. [CrossRef]
31. Azees, M.; Vijayakumar, P.; Deboarh, L.J. EAAP: Efficient Anonymous Authentication With Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2467–2476. [CrossRef]
32. Ayaz, F.; Sheng, Z.G.; Tian, D.X.; Guan, Y.L.; Leung, V.; IEEE. A Voting Blockchain based Message Dissemination in Vehicular Ad-Hoc Networks (VANETs). In Proceedings of the IEEE International Conference on Communications (IEEE ICC)/Workshop on NOMA for 5G and Beyond, Dublin, Ireland, 7–11 June 2020.
33. Shrestha, R.; Bajracharya, R.; Shrestha, A.P.; Nam, S.Y. A new type of blockchain for secure message exchange in VANET. *Digit. Commun. Netw.* **2020**, *6*, 177–186. [CrossRef]
34. Shrestha, R.; Bajracharya, R.; Nam, S.Y. Blockchain-based Message Dissemination in VANET. In Proceedings of the 3rd IEEE International Conference on Computing, Communication and Security (ICCCS), Kathmandu, Nepal, 25–27 October 2018; pp. 161–166.
35. Li, X.C.; Yin, X.C.; Ning, J.T. Trustworthy Announcement Dissemination Scheme With Blockchain-Assisted Vehicular Cloud. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 1786–1800. [CrossRef]
36. Arora, S.K.; Kumar, G.; Kim, T.H. Blockchain Based Trust Model Using Tendermint in Vehicular Adhoc Networks. *Appl. Sci.* **2021**, *11*, 1998. [CrossRef]
37. Zhang, B.W.; Wang, X.L.; Xie, R.; Li, C.C.; Zhang, H.Z.; Jiang, F. A reputation mechanism based Deep Reinforcement Learning and blockchain to suppress selfish node attack motivation in Vehicular Ad-Hoc Network. *Future Gener. Comput. Syst.-Int. J. Escience* **2023**, *139*, 17–28. [CrossRef]
38. Gaba, P.; Raw, R.S. B-VANET: A blockchain-based vehicular ad-hoc network for data validation. *Peer-Peer Netw. Appl.* **2022**, *15*, 2650–2669. [CrossRef]
39. Grover, J. Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review. *Veh. Commun.* **2022**, *34*, 100458. [CrossRef]
40. Ahmed, M.; Moustafa, N.; Akhter, A.; Razzak, I.; Surid, E.; Anwar, A.; Shah, A.; Zengin, A. A Blockchain-Based Emergency Message Transmission Protocol for Cooperative VANET. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 19624–19633. [CrossRef]
41. Akhter, A.; Ahmed, M.; Anwar, A.; Shah, A.; Pathan, A.S.K.; Zengin, A. Blockchain in vehicular ad hoc networks: Applications, challenges and solutions. *Int. J. Sens. Netw.* **2022**, *40*, 94–130. [CrossRef]
42. Zhang, X.F.; Xia, W.B.; Wang, X.C.; Liu, J.J.; Cui, Q.M.; Tao, X.F.; Liu, R.P. The Block Propagation in Blockchain-Based Vehicular Networks. *IEEE Internet Things J.* **2022**, *9*, 8001–8011. [CrossRef]
43. Ma, Z.W.; Zhu, L.; Jiang, X.T.; Yu, F.R.; Shafiq, O.; James, J. A practical solution for blockchain-secured sharing of trustworthy traffic information in vehicular ad hoc networks. *Int. J. Sens. Netw.* **2022**, *39*, 18–33. [CrossRef]
44. 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.
45. Akhter, A.S.; Ahmed, M.; Shah, A.S.; Anwar, A.; Kayes, A.; Zengin, A. A blockchain-based authentication protocol for cooperative vehicular ad hoc network. *Sensors* **2021**, *21*, 1273. [CrossRef]
46. Chukwuocha, C.; Thulasiraman, P.; Thulasiram, R.K. Trust and scalable blockchain-based message exchanging scheme on VANET. *Peer-Peer Netw. Appl.* **2021**, *14*, 3092–3109. [CrossRef]

47. Lv, P.; Xie, L.Y.; Xu, J.; Li, T.S. Misbehavior Detection in VANET Based on Federated Learning and Blockchain. In Proceedings of the 21st International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP), Virtual Event, 3–5 December 2021; pp. 52–64.
48. Khan, A.S.; Balan, K.; Javed, Y.; Tarmizi, S.; Abdullah, J. Secure trust-based blockchain architecture to prevent attacks in VANET. *Sensors* **2019**, *19*, 4954. [CrossRef] [PubMed]
49. Wagner, M.; McMillin, B. Cyber-physical transactions: A method for securing VANETs with blockchains. In Proceedings of the 2018 IEEE 23rd Pacific rim international symposium on dependable computing (PRDC), Taipei, Taiwan, 4–7 December 2018; pp. 64–73.
50. Yang, Z.; Yang, K.; Lei, L.; Zheng, K.; Leung, V.C. Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet Things J.* **2018**, *6*, 1495–1505. [CrossRef]
51. Liu, M.; Teng, Y.; Yu, F.R.; Leung, V.C.; Song, M. Deep reinforcement learning based performance optimization in blockchain-enabled internet of vehicle. In Proceedings of the ICC 2019—2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6.
52. Xie, L.; Ding, Y.; Yang, H.; Wang, X. Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs. *IEEE Access* **2019**, *7*, 56656–56666. [CrossRef]
53. Haddaji, A.; Ayed, S.; Fourati, L.C.; Soc, I.C. Blockchain-based Multi-Levels Trust Mechanism Against Sybil Attacks for Vehicular Networks. In Proceedings of the 14th IEEE International Conference on Big Data Science and Engineering (BigDataSE), Guangzhou, China, 29 December 2020–1 January 2021; pp. 155–163.
54. Ahmed, W.; Di, W.; Mukathe, D. A Blockchain-Enabled Incentive Trust Management with Threshold Ring Signature Scheme for Traffic Event Validation in VANETs. *Sensors* **2022**, *22*, 6715. [CrossRef] [PubMed]
55. Ghaleb, F.A.; Razzaque, M.A.; Isnin, I.F. Security and privacy enhancement in VANETs using mobility pattern. In Proceedings of the 2013 Fifth International Conference on Ubiquitous and Future Networks (ICUFN), Da Nang, Vietnam, 2–5 July 2013; pp. 184–189.
56. Ghaleb, F.A.; Maarof, M.A.; Zainal, A.; Al-rimy, B.A.S.; Alsaeedi, A.; Boulila, W. Ensemble-Based Hybrid Context-Aware Misbehavior Detection Model for Vehicular Ad Hoc Network. *Remote Sens.* **2019**, *11*, 2852. [CrossRef]
57. Ghaleb, F.A.; Zainal, A.; Rassam, M.A.; Abraham, A. Improved vehicle positioning algorithm using enhanced innovation-based adaptive Kalman filter. *Pervasive Mob. Comput.* **2017**, *40*, 139–155. [CrossRef]
58. Ghaleb, F.A.; Zainal, A.; Rassam, M.A.; Saeed, F. Driving-situation-aware adaptive broadcasting rate scheme for vehicular ad hoc network. *J. Intell. Fuzzy Syst.* **2018**, *35*, 423–438. [CrossRef]
59. Alzahrani, M.; Idris, M.Y.; Ghaleb, F.A.; Budiarto, R. An Improved Robust Misbehavior Detection Scheme for Vehicular Ad Hoc Network. *IEEE Access* **2022**, *10*, 111241–111253. [CrossRef]
60. Ghaleb, F.A.; Razzaque, M.A.; Zainal, A. Mobility pattern based misbehavior detection in vehicular adhoc networks to enhance safety. In Proceedings of the 2014 International Conference on Connected Vehicles and Expo (ICCVE), Vienna, Austria, 3–7 November 2014; pp. 894–901.
61. Chen, Z. Research on internet security situation awareness prediction technology based on improved RBF neural network algorithm. *J. Comput. Cogn. Eng.* **2022**, *1*, 103–108.
62. Hooshmand, M.K.; Hosahalli, D. Network anomaly detection using deep learning techniques. *CAAI Trans. Intell. Technol.* **2022**, *7*, 228–243. [CrossRef]
63. Akhter, A.F.M.S.; Ahmed, M.; Shah, A.F.M.S.; Anwar, A.; Zengin, A. A Secured Privacy-Preserving Multi-Level Blockchain Framework for Cluster Based VANET. *Sustainability* **2021**, *13*, 400. [CrossRef]
64. Ahmad, F. Deep image retrieval using artificial neural network interpolation and indexing based on similarity measurement. *CAAI Trans. Intell. Technol.* **2022**, *7*, 200–218. [CrossRef]