New Trust Management Scheme Based on Blockchain and KNN Reinforcement Learning Algorithm

Ahdab Hulayyil Aljohani, Abdulaziz Al-shammri
Computer Science-Information Security Department
Imam Muhammed ibn Saud Islamic University (IMISIU)
Riyadh, Saudi Arabia

***Abstract*—There has been a continual rise in the quantity of smart and autonomous automobiles in recent decades. the effectiveness of communication among vehicles in Vehicular Adhoc Networks (VANET) is critical for ensuring the safety of drivers' lives. the primary objective of VANET is to share critical information regarding life-threatening events, such as traffic jams and accident alerts in a timely and accurate manner. Nevertheless, typical VANETs encounter several security issues involving threats to confidentiality, integrity, and availability. This paper proposes a new decentralized and tamper-resistant scheme for privacy preservation. We designed a new trust management system that utilizes blockchain technology. We strive to establish trust between vehicles and infrastructure and preserve privacy by guaranteeing the authenticity and integrity of the information exchanged in VANETS. Our proposal adopts the principles of reinforcement learning to dynamically evaluate and allocate trust scores to vehicles and infrastructure based on their behavior. The scheme's performance has been evaluated based on key metrics. The results show that our new system provides an effective behavior management technique while preserving vehicle privacy.**

***Keywords*—Vehicular Ad hoc Networks (VANETs); Blockchain; trust management; reinforcement learning algorithm; privacy preservation; network security**

I. Introduction

Intelligent transportation system (ITS) refers to the implementation of several technologies including sensing, analysis, control, and communications in the domain of ground transportation. The primary objective of ITS is to enhance safety, mobility, and efficiency within the transportation system. ITS encompasses a diverse array of applications that facilitate the processing and dissemination of information. These systems aim to alleviate congestion, enhance traffic management, mitigate environmental consequences, and amplify the advantages of transportation for both business customers and the general public [1].

VANET (Vehicular Ad hoc Network) is a subcase of an intelligent transportation system where vehicles can communicate and exchange information with each other (vehicle-to-vehicle), with fixed Road Side Units (Vehicle-To-Infrastructure), or with any communication entities (Vehicle-To-Everything). Vehicle communication improves traffic control and public safety. This is done by the detection and sharing of traffic flow information, driver behavior, locations, and trajectories [2]. VANET expanded its areas of use and It has become a fertile field for scientific research. New and innovative applications have emerged to offer better driving experiences and provide value-added user-oriented services [3], [4].

The predictable vehicle movement, the constantly changing network topology and density, the frequent hand-offs between on-board units (OBUs) and RSUs, and the ease of reading the radio signals are some of the distinctive features of VANETs [5] As result, cars are highly exposed to various types of attacks and security risks [6], [7]. Denial of service, Blackhole, Wormhole, Eavesdropping, False position information, and Man In The Middle attacks are among the most known attacks in VANET [8], [9]. Various solutions are proposed to deal with each kind of threat [10]–[13].

In this work, we focus on privacy protection in VANET. This means preserving legal vehicle information, user personal information, user locations, and all data leading to user or vehicle identification and activity tracking [6], [7], [14]. Preserving privacy is complex and controversial. It must guarantee the authenticity of each vehicle on the network. While, at the same time, the true identity of the requested vehicle must not be revealed.

To tackle those issues, we introduce the use of blockchain technology [15]. It's confirmed to be a distributed and secure solution for data protection. It's able to provide a highly protected ledger to store authentication information and offers interesting features to check the stored data validity called consensus algorithms [15]–[17]. Proof of Existence (PoE)and Proof of Work (PoW) are the basic two features that guarantee data integrity and authenticity.

Our proposal introduces a new privacy protection solution based on blockchain mechanisms and a trust evaluation system to detect malicious behaviors and prevent their harm to network communications. Furthermore, we enhanced our trust management technique by adopting the Reinforcement learning technique. RL is based on trial-and-error discovery and delayed reward [18]. The more the vehicle is learning from the current state, the better will be its decision.

The contributions of our research work can be summarized as follows:

- A full registration process that allows vehicles to request network join and be authenticated by a central trust authority (TA). Cars use a secured channel to exchange sensitive identity information with the TA and obtain permanent credentials.

- The TA maintains a public blockchain to store authentication information and trust scores. That will provide vehicles with a reliable mechanism to check their interlocutor authenticity and trust scores.
- We develop a novel trust management scheme for VANETs. Our scheme dynamically assesses and assigns trust scores to vehicles. We propose the introduction of three different trust levels: Direct Trust Score (DTS), Indirect Trust Score (ITS), and Historical Trust Score (HTS). These levels are attributed respectively by the vehicles to encountered nodes, RSUs, and the Trust Authority (TA).
- We empowered the trust evaluation by integrating the reinforcement learning technique. The TA uses the algorithm KNN (K-Nearest Neighbors) to predict the candidate's behavior and compute the HTS value for each node in the network.
- A configurable acceptance system where vehicles can decide to accept, or not new incoming data based on the sender scores and the data types.

The remainder of this paper is organized as follows. In Section II, we review the related work related to privacy preservation and trust management in VANET. Section III presents the solution backgrounds. Our proposal is detailed in Section IV. Section V exposes our experimentation and gives a performance evaluation of our scheme. Finally, we conclude the proposal in Section VI.

II. Related Work

Waheeb et al. [19] introduced the framework to ensure the security of the communication in VANETs, this framework integrates a blockchain to support privacy-preserving authentication with a context-aware trust management system. It comprises a blockchain system that allows for anonymity and mutuality authentication of vehicle nodes and their messages. On the other hand, the aware trust management scheme allows for evaluating the reliability of sender vehicles by identifying and blocking the unauthorized nodes and their deceptive messages from the network. The scheme outweighs basic methods in robustness and efficiency while improving security in-vehicle communication. It is crucial to examine elements such as processing and communication overhead, as well as real-world implementation challenges.

In [20], authors introduced a system called TrCoin for VANETs, to conduct the trustworthiness of data providers, enhance traffic efficiency, and prevent malicious data providers from sharing false information. It applies a calculation algorithm with honest value to distinguish honesty from malicious data users and refine feedback shared by malicious users. The algorithm works by assuming that most data users are honest and estimates the weighted consistency (WC) of each user by evaluating their feedback consistency with the majority of users. The honesty value (HV) of data users is adjusted according to their (WC) where a greater (WC) signifies a more truthful user. This framework calculates also the count values of data providers based on truthful observations from honest users. TrCoin's effectiveness is shown by thorough simulations involving different attack scenarios, including fraudulent data injection and dishonest feedback. While blockchain technology is inherently transparent which means it allows all transactions and trust-related information to be available to network participants. We think privacy issues in VANETs might occur if confidential information or user identities are revealed on the blockchain.

The author in [21] introduced decentralized architecture utilizing blockchain technology to tackle the issues related to implementing decentralized architecture and safeguarding privacy in VANETs. The study suggests implementing a scalable and tamper-proof distributed trust management system for VANETs by utilizing blockchain technology. An innovative validation approach based on Bayesian inference is presented to counteract the impact of misleading signals in VANETs. Also, the suggested method removes the requirement for a trusted third party (TTP) by leveraging the decentralized and distributed characteristics of blockchain technology. Their work introduces a sharding consensus mechanism to enhance scalability in the VANET system. The experimental findings demonstrate that the suggested system is efficient, adaptable, and reliable in collecting, processing, organizing, and retrieving trust values in VANETs. In our opinion, first: the study doesn't discuss the potential scalability challenges that could occur with extensive VANET implementations, second the proposed approach assumes that all vehicles in the network would correctly validate and upload their calculated rates to the RSUs which may not happen in real-world situations. third, the study doesn't account for the influence of network latency and communication delays on the dependability and trust management mechanism in VANETs. Lastly, the suggested Bayesian formula for trust management relies on the precise calculation of confidence scores and distances between sender messages and event locations, which may not always be achievable in real-world scenarios.

Another proposal is presented by Inedjaren et al. [22]. It introduces a blockchain-powered distributed management system for trust in VANETs to tackle security and reliability concerns in message sharing between vehicles. The suggested solution attempts to establish a safe and unalterable architecture for routing in VANETs by utilizing blockchain technology. the solution utilizes the optimized link state routing (OLSR) protocol along with blockchain technology to address security issues and redundant procedures in the OLSR routing mechanism, moreover, the system uses the proof of trust (PoT) consensus mechanism in a dynamic and resource-limited context. The system incentivizes vehicles together and prevents redundant detection procedures by providing rewards using blockchain. the simulation results demonstrated that the suggested approach is effective in resource-constrained contexts such as VANETS. It reduces detection time and overhead by isolating hostile nodes, thus enhancing the efficiency of the detection process. At the same time, the system seeks to reduce overhead by isolating hostile nodes and streamlining routing methods. However, the incorporation of blockchain itself introduces additional overhead in terms of storage, computation, and communication. this overhead could offset some of the gains achieved by the proposed solution.

Cong Pu [23] introduces trust management called trust block MCDM for VANETs within the Internet of Vehicles (IoV) framework. The trust block MCDM system employs a multi-criteria decision-making model to assess the reliability of road safety messages and produce trust ratings for message senders. The trust values are regularly sent to a neighboring RSU. The RSU computes the reputation value of the message sender based on trust values from the vehicles and includes it in a block for addition to the blockchain. This blockchain works as a decentralized agreement system, where the longest branch of the transaction is accepted as the network's consensus. The trust value computation considers input from nearby validators, the reputation of the message initiator, and the confidence of the validator in the event. The trust block MCDM method enhances the detection rate of fake messages, and the detection rate of hostile vehicles, and reduces the number of dropped fake messages as compared to other blockchain-based trust management methods. the suggested approach improves the assessment of trustworthiness for road safety messages in VANETs, leading to enhanced road safety and travel experience in the IoV. Although the MCDM Scheme demonstrates promising outcomes in enhancing trust management in VANETs, it possesses specific constraints that must be taken into account for its practical use and deployment. We can generalize these limitations first the effectiveness of the trust block MCDM method depends significantly on the precision and dependability of the multi-criteria decision–making model utilized for reputation assessment secondly the MCDM technique doesn't evaluate the influence of network congestion or communication delays on the trust evaluation process

Hui et al. [24] in their study aims to develop a framework that focuses on selecting a reliable relay for service requests by considering the dynamic traffic conditions and vehicle behaviors by introducing a reputation management system to regulate vehicle actions. Vehicles with a high reputation can receive savings on computing services. the paper suggests using a reputation–based auction system to choose relay vehicles (RVs) and lower the cost of the relay services. Each vehicle is granted a reputation value depending on its adherence to the relay system, vehicles can enhance their reputation by utilizing edge computing devices (ECDs) for computing services and engaging in the request relay process, vehicles with a high reputation value qualify for price discounts on computer services. The simulation results show that the suggested reservation service architecture effectively handles vehicles and results in the most cost-effective relay services compared to traditional methods. This framework has potential limitations or areas for improvement in the current system, including the necessity for improved security measures and more precise classification methods for automobiles.

Sonker and Gupta [25] utilize multiple machine learning to detect misbehavior in vehicle ad hoc networks (VANETs) the techniques utilized are Naïve Bayes, decision tree, random forest, K-nearest neighbor (KNN), and stochastic gradient descent (SGD) classifier. The initial stage of the research includes examining the algorithms on various attack kinds by binary categorization, the second part concentrates on developing a novel process for identifying attacks by utilizing several machine learning classification algorithms and entropy calculation and information gain methods for selecting decision nodes. Stochastic gradient descent is an optimization approach commonly used in research for addressing linear problems with support vector machines and logistic regression moreover the paper utilizes the VeReMi dataset a public repository created for identifying malicious nodes in VANETs. The dataset is utilized to assess machine learning algorithms in identifying various forms of attacks and test their detection techniques' efficiency. However, it's vital to note that the algorithms' efficiency may change when used in a wider range of assault scenarios, and using this amount of algorithms addresses drawbacks like the need for large amounts of labeled data, computational complexity, and generalization to new and unseen attacks.

Anti-Attack Trust Management Strategy named AATMS is proposed in [26]. It assesses the reliability of vehicles in different application scenarios and withstands diverse attacks. The research work introduces social elements such as diverse factors, vehicle factors, and behavior factors to filter out untrustworthy automobiles and indicate the level of public trust in vehicles. They are utilizing Bayesian inference to determine local trust levels from past encounters and choosing trustworthy seed vehicles depending on local trust and societal considerations. Moreover, they are introducing an adaptive forgetting factor to update local trust values and an adoptive decay factor to update global trust values to prevent a sudden increase in trust levels and enable a rapid decrease. The Bayesian inference's accuracy relies on the quality and trustworthiness of historical evidence, making it not a failsafe. Unreliable trust judgments might result from inaccurate or insufficient data.

Javaid et al. [27] introduced a trust management system named DrivMan (VANETs) that utilizes blockchain and a certificate authority (CA) to guarantee secure communication and data exchange. The scheme uses physical unclonable functions (PUFs) to guarantee the data dependability and privacy of intelligent vehicles (IVs) in (VANETs). It also utilizes the SHA-265 cryptographic hash method for authentication and verification. the system design includes initializing the nodes, composing and deploying contracts on RSUs nodes, and utilizing a genesis block for DrivMan that expands with subsequent blocks. blockchain is utilized as a decentralized digital ledger in DrivMan to guarantee the secure and dependable functioning of the system, it's offers an immutable and transparent record of all transactions and data exchanges. Moreover, the blockchain technology in DrivMan ensures high security by necessitating a minimum of 51% of the network's processing power to tamper with data. Smart contracts, and autonomous computer algorithms, are utilized with blockchain to ensure data provenance and integrity in DrivMan. The asymmetric public key infrastructure in blockchain guarantees secure communication between the IVs and the network. Since the security implies that an adversary would require a minimum of 51% of the total processing power of the DrivMan network to manipulate data, a feat that may be achievable in some situations, also using a blockchain network hosted by RSUs could lead to centralization and reliance on an entity for network operations.

A decentralized trust management strategy for vehicular networks, specifically for decentralized VANETs is proposed by Gulen et al. [28]. The approach utilizes a fuzzy logic-based method to calculate trust and assess direct trust between trustor and trustee nodes within the transmission range. The system utilizes a reinforcement learning method to estimate indirect trust, especially when the actions of trustee nodes are not explicitly observable, in their scheme they propose a method for evaluating trust among multiple agents is suggested, and direct trust is determined through a fuzzy logic algorithm that considers factors such as cooperativeness, honestness, and responsibility. Indirect trust is assessed using a reinforcement learning technique that adjusts trust levels based on the number of intermediaries involved. This technique efficiently integrates knowledge from several nodes by evaluating indirect trust to handle complex circumstances. This strategy has some drawbacks like the trust evaluation process depending on fuzzy logic and indirect trust estimation through reinforcement learning, which could lead to limits in accurately assessing and determining the trustworthiness of nodes. The scheme doesn't address the potential obstacles or restrictions in attaining precise trust evaluation in dynamic and unreliable vehicle networks. Moreover, the proposed architecture is based on nodes being situated within each other's transmission range. This reliance on closeness could restrict the effectiveness of the plan in situations where nodes are widely spread out or when the communication range is restricted.

In [29] a new study introduces an innovative trust structure for vehicle networks to tackle the problem and an innovative trust structure for vehicle networks, the problem of rouge nodes, and inaccurate information which can make the system unreliable for safety and emergency purposes. The trust architecture enables nodes to recognize and screen out recommendations from malicious nodes and distinguish genius events. The system successfully detects malicious nodes and true events with a probability over 0.92, while maintaining the trust computation error under 0.03. The network model is created to evaluate the framework in situations including malevolent nodes where nodes move collectively along specific routes and encounter notable occurrences. Nodes communicate changes using messages, allowing nodes not directly involved to be informed by received messages. Simulation studies are conducted to confirm the trust framework's validity. A circular road is created in a simulation where accidents or traffic hazards occur randomly at various points. Proximal nodes encounter the event before distal nodes, who perceive it subsequently. The framework effectively detects events in incoming messages and excels in determining the actual characteristics of nodes. However, the suggested trust architecture operates under the assumption that there is a singular authentic event in the network at every moment, which may not align with the complexities of real-world situations. The system depends on nodes detecting the incident and notifying their neighboring nodes within the $300m$ range, which aligns with the conventional DSRC range. This restricted range may hinder the framework's efficacy in bigger network deployments. The approach assumes that malicious nodes transmit inaccurate information with a constant probability, without accounting for the potential adaptive or dynamic actions of malicious nodes. The system prioritizes safeguarding nodes against certain assaults but does not offer privacy or anonymity for the messages shared between nodes.

III. Solution Background

A. VANET Basic Fundamentals

Wireless access in vehicular environment (WAVE) is the name of the system that lets vehicles and RSUs talk to each other. The exchange of security messages is described by the WAVE design [30]. The WAVE communication keeps passengers safe by updating information about vehicles and traffic flow. This app makes sure that both pedestrians and drivers are safe. It also makes the traffic move better and the traffic management system work better. The VANETs are made up of different groups, such as OBUs, RSUs, and Trusted Authority (TA). In particular, the OBU is attached to each vehicle and collects useful data about the vehicle, such as its speed, acceleration, and fuel consumption. The RSU usually hosts an application that is used to interact with other network devices. After that, these data are sent to nearby cars through wireless signals. All RSUs that are linked to each other are also wired to connect to TA. In addition, the TA is in charge of managing the VANETs and is the leader of all the parts.

- Road Side Units (RSU): A roadside unit is a computing device that is located next to the road or in a certain place like a parking lot or an intersection [2]. Its job is to connect passing cars to the internet locally. The RSU is made up of network devices that use IEEE 802.11p radio technology for dedicated short-range communication (DSRC). It is more specific that RSUs can also talk to other network devices in other core networks [5].
- On-Board Unit (OBU): can share information about a car with RSUs and other OBUs. It does this by using a global positioning system (GPS) to track the vehicle. The OBU is made up of many electronic parts, including a resource command processor (RCP), sensor devices, a user interface, and read/write storage for getting information from storage. The main job of an OBU is to connect to an RSU or other OBUs through an IEEE 802.11p [31] wireless link and send information to other OBUs or RSUs. The car battery also gives power to the OBU, and each car has a (GPS), an event data recorder (EDR), and forward and backward devices that send information to the OBU.
- Trusted Authority (TA): The trusted authority is in charge of running the whole VANET system and recording the RSUs, OBUs, and vehicle users. In addition, it is its job to make sure that VANETs are secure by checking the vehicle identification, user ID, and OBU ID to make sure that no vehicles are harmed. The TA uses a lot of power and has a lot of memory [1]. It can also show the OBU ID and information if it receives a malicious message or notices strange behavior. In addition to these, TA additionally provides an approach for identifying the attackers [2]. ITS is always trying to improve traffic flow and road safety by making communication more secure and using different networking methods, like MANETs and VANETs, to get around traffic jams. To make traffic flow more smoothly, keep people safe, and make driving more enjoyable, Vehicle-to-Everything (V2X) communications are very impor-

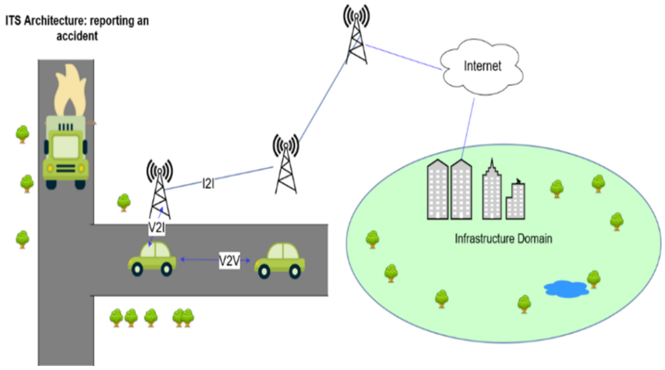

Fig. 1. VANETs communication architecture.

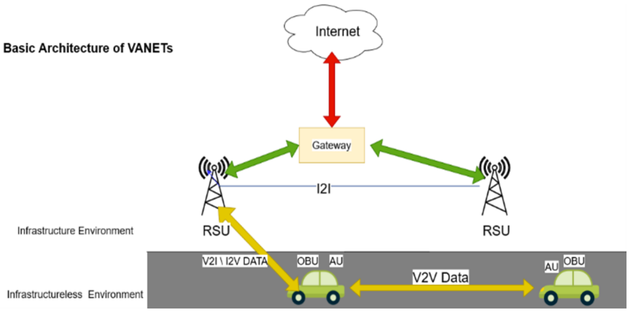
Basic Architecture of VANETs
Internet
Gateway
I2I
RSU
RSU
Infrastructure Environment
Infrastructureless Environment
V2I \ I2V DATA
OBU
AU
V2V Data
AU
OBU

Fig. 2. Communication types in VANETs.

tant. They do this by sending very accurate and up-to-date information about things like accidents, traffic jams, emergencies, and other transportation services as shown in Fig. 1.

B. Communication Techniques Utilized in VANETs

The transmission medium in V2V communication has a high transmission rate and a small latency [31] In V2V, a vehicle can send important data to another vehicle, like emergency braking, collision detection, and traffic conditions. V2I lets vehicles and network infrastructures send important data to each other The car built a link with RSUs in this area so it could share data with other networks, like the Internet. V2I also needs more data than V2V because it communicates with infrastructure, but it is less likely to be attacked [5]. Cellular vehicle to everything (C-V2X) technology was just released. It's a unified connectivity platform that's meant to serve V2X communications [2]. C-V2X was created as part of the third-generation partnership project (3GPP), and it is thought to be the most reliable communication system that can handle V2X communications [2].

It links all the cars together and makes it possible for co-operative intelligent transport systems (C-ITS) to work, which eases traffic and makes it run more smoothly. Fig. 2 illustrates the on-board unit (OBU) and one or more applications units (AUs) make up the in-vehicle area. They often use wired links, but sometimes they use wireless ones. On the other hand, the ad hoc domain is made up of cars with OBUs and RSUs. An OBU is like a mobile node in an ad hoc network, and an RSU is like a fixed node. The gateway can connect an RSU to the Internet. RSUs can also talk to each other directly or through multi-hop. Access to the infrastructure can be done through two different types of points: RSUs and hot spots (HSs). OBUs can talk to the Internet through either RSUs or HSs. Cellular radio networks (GSM, GPRS, UMTS, WiMAX, and 4G) can also be used by OBUs to talk to each other when RSUs and HSs are not available. Furthermore, VANET communications can be broken down into four groups, which are shown below [32].

C. Trust Concepts and Trust Components

Trust in the context of VANET (Vehicular Ad-Hoc Network) denotes the level of confidence that one entity has in another entity [4]. It relies on the anticipation that the other party will carry out a specific action as anticipated by the initiator. Trust is predicated on the assurance that the trusted entity will not engage in malevolent behavior in a given circumstance. Since exact certainty is unattainable, trust relies entirely on the trustor's conviction. An entity refers to a tangible device that actively engages in the process of communication, such as OBUs (OnBoard Units) and RSUs (Road Side Units) utilized in VANET (Vehicular Ad hoc networks). Trust refers to the extent to which a node is considered trustworthy, secure, or reliable while engaging with other nodes. For a node to engage in the communication process of VANET, it must be considered trustworthy by other nodes and meet the trust criteria. A node's trust values can vary when assessed by different nodes due to variations in the trust evaluation criteria for each particular node. Trust is contingent upon the passage of time, as it has the potential to both flourish and deteriorate. Trust levels are established based on specific acts that the trusted party can carry out on behalf of the trustee. Moreover, the following elements comprise the character of interactions between two entities upon which the concept of trust is predicated:

- Direct Trust: It is demonstrated through the interaction between a trustor and a target vehicle, as evidenced by the trustor's direct observations [33]. Certain scholars employ the term "knowledge" to denote the explicit data acquired by the trustor to assess the trustee by specific criteria that depend on the nodes and services involved. Although it is commonly held that direct trust is more significant than indirect trust, when evaluating a vehicle, the combination of the two is considered. Fig. 3, demonstrates the difference between direct and indirect vehicle trust. Where vehicle number 2 recommends that vehicle 4 trust the vehicle.
- Indirect trust: It refers to the viewpoints of trusted entities in the vicinity of a trustor, regarding a specific node (trustee). These viewpoints are based on past experiences with the node in question. Researchers often explain indirect observation through the combination of reputation and experience. Reputation is the collective record of previous interactions with a certain entity, which reflects the overall perception of that entity. On the other hand, experience refers to the relationship between a person who trusts and another who is trusted, based on the trustor's belief in the trustee's ability to complete a task.

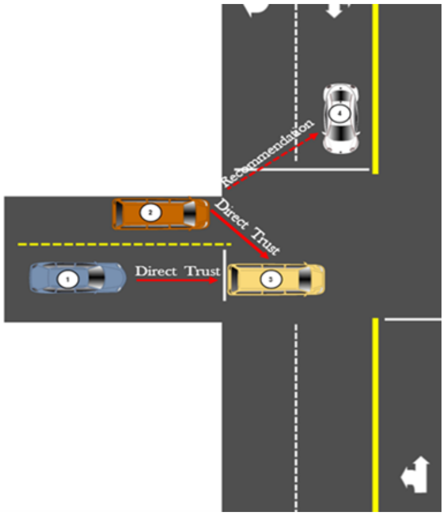

Fig. 3. Difference between direct and indirect trust in VANETs.

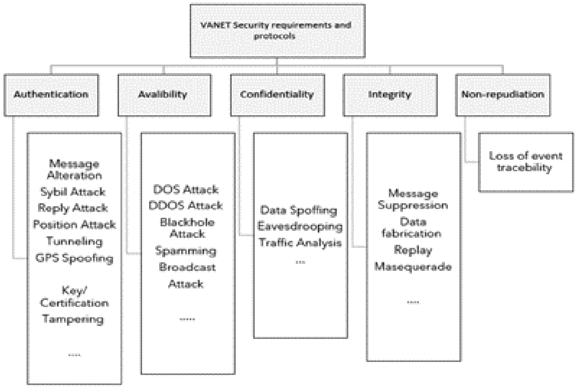

Fig. 4. VANETs security requirements.

D. Requirement for VANETs Security

A system can be vulnerable to a variety of system flaws that can be exploited by unfriendly entities for a variety of reasons. The security requirements of a system must be addressed to make it secure. The VANET system has some security requirements, which are briefly detailed here. Fig. 4 additionally shows the kind of probable assaults that could jeopardize VANET security standards.

- Authentication: It is a critical and unavoidable need of any system. A system must be able to verify the authenticity of all system participants. Authentication and identity are especially crucial and vital in VANET, which is prone to many vulnerabilities. In the event of a VANET attack, a robust authentication strategy can give solid legal proof against the invader. As a result, the authentication procedure is an obvious necessity to defend the VANET system against assaults such as Sybil attacks, location attacks, tunneling, replay attacks, message manipulation, and so on.
- Availability: A system or a system component could be susceptible to failure or attack. This type of malicious system or component condition should not impact other users or system elements. All applications and networks within VANETs must remain operational and accessible, even if one element of the VANET is compromised. Certain infrastructures or nodes within a VANET may be susceptible to attacks or problems that do not affect other nodes. Alternatively stated, VANET resources must be consistently accessible. To meet the availability requirement of a VANET, it is necessary to develop a system that is robust, secure, and tamper-tolerant. A multitude of attacks, including Distributed Denial of Service (DDOS), Denial of Service (DOS), spamming, and Black Hole attacks, can significantly compromise the availability requirements of VANET.
- Confidentiality pertains to the safeguarding of private information associated with a specific node or infrastructure. The communications that transpire between two components in a VANET must not be made public to a third party. The maintenance of confidentiality can be accomplished through the implementation of diverse encryption algorithms. Safety messages in VANETs do not contain any sensitive information; therefore, they are not encrypted. Electronic payment information, the identity of the user, and other personally identifiable data are, nevertheless, protected in confidence through the implementation of diverse cryptographic algorithms. Data surveillance, traffic analysis, and data spoofing are a few of the potential breaches of confidentiality in VANETs.
- Integrity safeguards communications against forgery or interpolation. Messages transmitted and received by various VANET entities must remain intact. Therefore, it is imperative to safeguard the integrity of communications against unauthorized tampering by criminals. Message integrity may be compromised by data alteration attacks, masquerade attacks, and replay attacks, among others. For the protection of communications during transmission and reception, it is necessary to implement a secure protocol. The IEEE1609.2 standard is employed to provide security services in VANETs.
- NonRepudiation: One of the critical security requirements of VANET. It safeguards against the denial of transmitted data by either the sender or the receiver [34]. Fig. 4 outlines the VANET security requirements as well as the potential hazards that could compromise those requirements.

E. Blockchain Overview

A blockchain is a decentralized public database that stores all completed digital transactions and is shared among participating nodes. It has an indisputable and verifiable record of every event that has ever taken place. Every event in the blockchain database is verified through the consensus of the majority of nodes in the network. There are primarily two types of blockchains: public blockchain and private blockchain. The public blockchain is a decentralized blockchain that allows

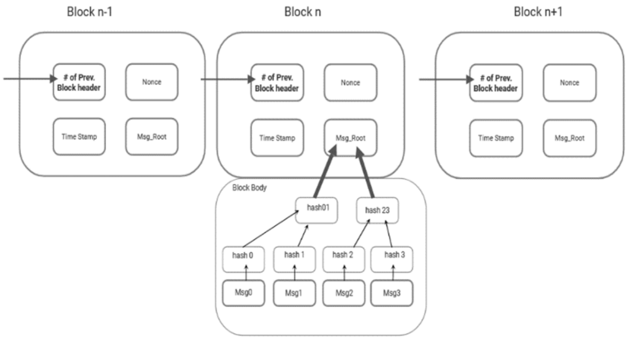

Fig. 5. Blockchain Concept.

unrestricted participation and interaction without requiring approval from a central authority. The starting point of the blockchain is a genesis block, which serves as the initial block in the blockchain. The genesis block serves as the shared starting point for all blocks and stores information that is universally accessible to all nodes [35]. The block comprises cryptographic hashes of records, each block containing the previous block's hash information, making a data chain and producing a blockchain, as illustrated in Fig. 5.

Features of using blockchain are:

1) Immutability: is a crucial aspect of blockchain technology. Once information is recorded and authenticated on the blockchain, it becomes immutable and cannot be altered or removed from the network. Additionally, information cannot be inserted randomly.
2) Distributed and trustless environment: In a blockchain system, any node that is added can synchronize and validate all data in a distributed way without the need for central control, creating a trustless environment. It offers security and guards against a single point of failure. It establishes trust in an atmosphere where trust is typically absent.
3) Privacy and anonymity: The blockchain offers privacy to its users. Users can join the network without revealing their identity. That is, the user's information is kept private from other users. It signifies that personal information is confidential, protected, and unidentified.
4) Faster Transactions: Setting up a blockchain is straightforward, and transactions are swiftly confirmed. Processing transactions or events only takes a few seconds to a few minutes.
5) Reliable and accurate data: The blockchain's decentralized network ensures that the data is reliable, accurate, consistent, timely, and publicly accessible. It is resilient to malicious assaults and lacks a single point of failure.
6) Transparency: It is fully transparent as it records information about each transaction or event that takes place in the blockchain network. Transactions are visible to all members of the network.

IV. Solution Presentation

Users can benefit from VANET communication to exchange different kinds of messages. Public safety, road traffic enhancement, and even entertainment and social applications are becoming VANET's basic use cases. Due to those heterogeneous usages, privacy preservation has become an urgent issue. To ensure that, we propose a new trust management process to detect and reject any malicious attacks. Our proposal defines a scoring mechanism to reward legitimate and punish malicious nodes. Our scheme introduces blockchain as a public ledger to save authenticated vehicle information and a reinforcement learning algorithm to enhance the trust score attribution. In this section, we will present the details of our solution. First, we will introduce the solution architecture and involved entities. Then, we will detail the authentication mechanism defined to integrate different network nodes. Finally, we will describe our trust management process and its score calculation procedures.

A. The Vehicle Registration and Authentication Mechanism

We propose a new authentication solution based on blockchain technology to ensure vehicle authentication and preserve user privacy. We define a trust management system to assess the trust of different vehicles in the network. As mentioned in Fig. 6, the network will contain the following entities: MVAC, TA, RSUs, and vehicles.

1) Motor and Vehicle Authority Centre (MVAC): The MVAC represents the legal authority or any delegated service to manage vehicles and transportation engines. It has the authority to store real documentation and to provide the car's valid registration numbers. It can also revoke those numbers and pull any given transportation license. Owners submit real documentation to register their vehicles. Accepted engines will receive a unique Identifier (ID) which will be stored with all identity information in the "Vehicle Information Base". This base is highly protected and managed only by the MVAC. In our scheme, we consider that MVAC is fully trusted. They are impossible to hack. Their operations and data cannot be compromised. They can resist any external attack and will never encounter internal attacks. DMV or TA can be held by the government or any authorized service provider.

2) The Trust Authority (TA): The trust authority is allowed by the MVAC to access the Vehicle Information Base and to read real identity information about all registered vehicles. To do so, it has a secure communication channel with the MVAC. The TA receives network registration requests from vehicles. It checks their information and generates all necessary parameters. It provides anonymous pseudo and various cryptographic parameters for each newcomer.

3) The Roadside Units (RSU): RSUs are small and wireless units deployed all over roads. They will offer different network services for registered vehicles. They can communicate with cars to share messages and service-related information. They need to register with the TA and get valid pseudonyms and security parameters. RSUs will correctly perform the proposed solution and provide reliable information and parameters. However, they are not allowed to access vehicle private information.

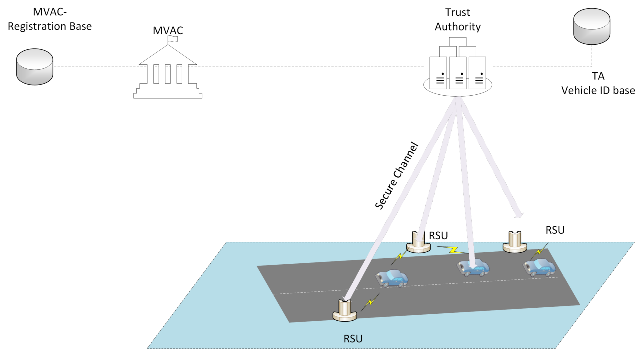

Fig. 6. Solution network architecture.

4) Vehicles: In VANET, vehicles are automobile engines equipped with wireless communication devices. They can use the WAVE standard to communicate with other network members. They can exchange messages with each other or with the network infrastructure. Vehicles are wireless mobile nodes. They are the most vulnerable units in the network. They can be hacked or receive compromised data. They can also act maliciously to threaten the network safety. They will be able to generate false data and compromise offered services

B. The used Blockchain Specifications

We propose the use of a dedicated blockchain structure for vehicle authentication. For each new registered car, a new block will be created. Its corresponding transaction contains its time of issue. So any participant can access the chain searching for the latest and newest information. When it finds the desired data, it will not need to continue reading.

1) The blockchain structure: Each time a new vehicle is registered and accepted by the MVAC, the TA will add its information to the Authentication Blockchain. The required information includes:

- The unique vehicle pseudonym
- The generated certificate: a public key and hash algorithm
- Universal issuing time
- Initial trust score
- Validity period
- Signature of the TA
- The certificate state (Valid or Not)

All that information constitutes a new block and will be added by the TA to the blockchain. The blocks are organized chronologically. Any reading operation will start with the newest inserted blocks to minimize the necessary research time.

2) The blockchain implementation approach: The use of blockchain technology has evolved tremendously since its first proposition with the concept of “bitcoin” in 2008 [36]. Different domains are introducing it to benefit from its valuable characteristics: transparency and non-tampering which can provide high security and privacy protection. Two basic formats are mainly used: the permissioned and permissionless. The permissioned blockchain authorizes any community member to access and add new blocks. This feature guarantees decentralized storage. On the other hand, the permissionless version is often used with centralized management to enhance the trustworthiness of the proposed operations. In our proposal, we introduce the permissionless blockchain. The trust authority (TA) is the only network member authorized to create and add new blocks which makes it impossible for the attackers to tamper with the public ledger.

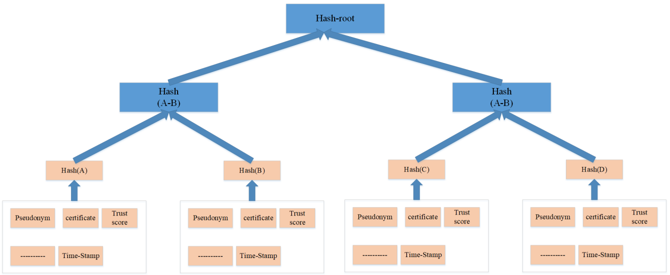

Fig. 7. The used blockchain architecture.

We also use the chronological Merkle tree (CMT) structure for our blockchain [37]. The CMT is the traditional underlying structure used for blockchain implementation. Fig. 7 shows this structure. All transactions will be hashed and stored chronologically in a binary hash tree. The leaves are the transaction data. In our case, a transaction represents a new block created after adding a newly registered vehicle to the network. Then, each pair of leaves is hashed to construct a new level of internal hashes. Pairwise hashing continues until we get a single hash as the root of the tree. Network members: vehicles or RSUs, are permitted to read the blockchain to verify their communicator credentials. They search the tree leaves using the communicator’s pseudonym starting with the last added data block. When the corresponding block is found, the proof of working concept (POW) [38] permits the validation of the communicator’s information. We need only to check the hashing branch between the root hash and the targeted node block.

C. The Network Initialization

During the initialization of the network, infrastructure components must be configured and prepared to accept the vehicle’s join requests. Later, they must ensure secure communication. Our proposal defines two basic network infrastructure elements: the Trust Authority (TA) and the Roadsides Units (RSUs).

1) The trust authority configuration: The TA is the central management unit. It stores the identification information of all allowed vehicles. It’s supposed to be fully functional all the time. For each vehicle, the TA proposes a unique pseudonym and a couple of public and private keys. Therefore, a pseudonym generation function will be initialized and started to wait for any incoming vehicle request. Then, the cryptographical process [7] will ensure the creation of the couple: public and private keys

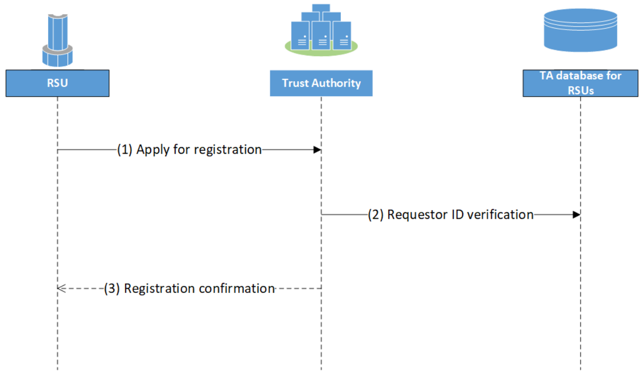
RSU
Trust Authority
TA database for RSUs
(1) Apply for registration
(2) Requestor ID verification
(3) Registration confirmation

Fig. 8. RSU network join.

2) The RSU network join: When a new RSU is installed and launched, it needs to contact the TA to obtain its security parameters: pseudonym, a private and public key. Like vehicles, RSUs are authenticated by the trust authority to avoid any malicious infiltration. Furthermore, they use pseudonyms and encryption during their communication to guarantee sensitive data preservation.

The RSU begins by sending a join request to the TA Fig. 8. The request includes a unique identifier given to the RSU upon its setup. The TA checks its database to confirm the RSU identity. Then, it generates new parameters for the requestor, signs them, and sends back the response. When the RSU receives the TA message, it adopts the new parameters. Finally, its configuration is completed, and it can participate in any message exchange. It also starts the vehicle trust management process.

3) The vehicle registration process: When a new vehicle is registered Fig. 9, the owner physically submits the required documents to the MVAC. The latter checks the vehicle's identity documents validity and approves the registration. An acceptance notification will be sent from the MVAC to the TA. The real identity of the vehicle will also be sent to be stored in the TA dedicated database. As a second step, the vehicle will be allowed to communicate with the TA through a secure channel Fig. 10. The vehicle sends its identity information and asks for a certificate generation. The TA generates for the new vehicle a new "unique pseudonym" and a couple of public and private keys and sends it to the vehicle using the secure channel. Also, the newly generated public key will be stamped and added to the authentication blockchain among other relative information: the initial value of the trust score and the certification issuing time, validity duration, etc.

D. The Certificate Creation and Management

We use the PKI (Public Key Infrastructure) as the basic mechanism for car identification and secure communication. The TA is the only unit allowed to issue couples (public, private) vehicle keys. Consequently, no computational charge will be on the vehicle. The certificate will be used in any communication with other vehicles. Also, the TA generates a "unique pseudonym" as an identifier for the participant car and it guarantees that the pseudonyms remain unique for all vehicles and during all communications. There will be no possibility of relaying the pseudonym to the real vehicle identity or any private information.

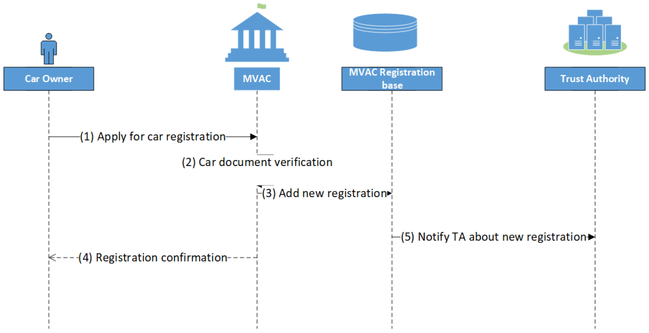
Car Owner
MVAC
MVAC Registration base
Trust Authority
(1) Apply for car registration
(2) Car document verification
(3) Add new registration
(5) Notify TA about new registration
(4) Registration confirmation

Fig. 9. The Vehicle's physical registration in the MVAC.

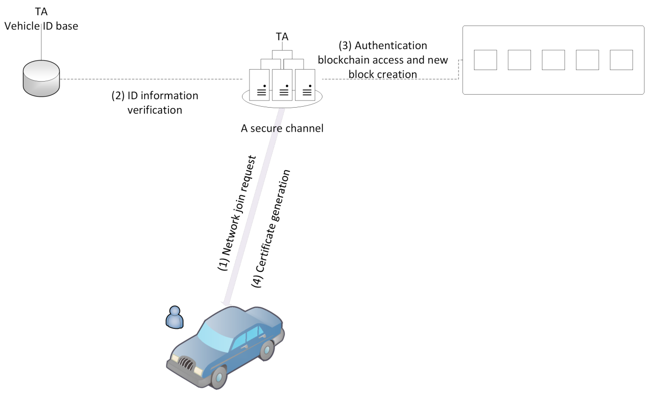
TA
Vehicle ID base
TA
(3) Authentication blockchain access and new block creation
(2) ID information verification
A secure channel
(1) Network join request
(4) Certificate generation

Fig. 10. Vehicle network join.

Each participant will receive his certificate generated by the TA at its first connection. The certificate has a validity period specifying the duration attributed by the TA and the MVAC to the requesting car. Vehicles can ask for new certificates anytime due to compromised data or any eventual attack. The new certificate is requested and received through the secure channel. Upon receiving the request, the TA starts by invalidating the previous certificate and adding a new block to the authentication blockchain to announce it. Then, a new certificate is created for the requestor and added to the blockchain along with the car other's information. Especially, using the same old pseudonym and trust score Eventually, a new pair of public and private keys will be generated to avoid any eventual new threat.

E. Vehicle Authentication During V2V or V2I Communication

When a Vehicle or RSU receives a new message from another vehicle, it starts by authenticating the communicator Fig. 11. It extracts the vehicle certificate from the message and determines the corresponding public key and pseudonym. Then, it accesses the Authentication Blockchain and checks the car registered certificate and its validity duration. We remain that the blockchain is built chronologically. Therefore, the verification process starts with the newest block and goes on until the oldest one Fig. 11. Eventually, the requestor will be able to find out the most recent state of the targeted node information. For example, if the communicating node was

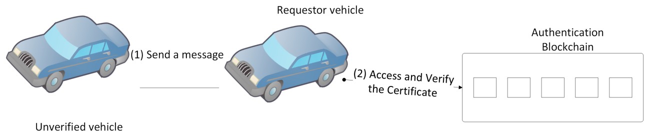
Requestor vehicle
(1) Send a message
Authentication Blockchain
(2) Access and Verify the Certificate
Unverified vehicle

Fig. 11. Vehicle authentication during V2V or V2I communication.

banned by the TA or has an un-renewed expired certificate, the requestor will reach in the first place the block announcing that state. This verification process allows the requesting vehicle or RSU to authenticate its communicator. So, it will be able to accept the new communication. Furthermore, the requestor has the new arrival's last known historical trust score. So, it will be able to decide better about its communicator's behavior.

F. The Trust Management System

We propose a trust management system based on the following elements.

- A historical trust score HTS: defined in the interval $[0..1]$. The TA attributes an initial HTS value to each new vehicle registered. The TA collects the trust scores of the targeted vehicle from the RSUs and other vehicles. Then, the TA uses a reinforcement algorithm (KNN) to recalculate the new HTS value for the vehicle and announces it by creating a new block.
- A direct trust score DTS: defined in the interval $[0..1]$ and attributed by a vehicle to each other. When vehicle A encounters for the first time vehicle B, it will generate a new DTS value for it and keep updating the B score when any new communication happens.
- An indirect trust score: ITS: defined also in the interval $[0..1]$ and attributed by the RSUs to different encountered vehicles. Periodically, the RSU receives different DTS measurements from neighboring vehicles. Then, it aggregates them to recalculate the new ITS for the targeted vehicles.

1) The DTS update algorithm: The algorithm in Fig. 12 defines the process used to manage the DTS for each vehicle. When vehicle A encounters vehicle B for the first time, it starts with attributing a first score $DTS(B) = 0.5$ and initializing 2 counters: counter for bad communication with B (Negative Behaviour Count: $NBC(B)$). It will count all cases of misbehavior of vehicle B: Lost packets and false information. And a counter for successful communication (Positive Behaviour Count: $PBC(B)$). Each new communication between them will increment the Bad or the Good counter and the total number of communications achieved. When a maximum threshold number is reached, vehicle A will calculate a new DTS for vehicle B using the formula 1

$$DTS(B)_{i+1} = \begin{cases} DTS(B)_i + DirectReward * \frac{PBC(B)-NBC(B)}{MaxThreshold} \\ = 0 \text{ if } DTS(B)_{i+1} < 0) \\ = 1 \text{ if } DTS(B)_{i+1} > 1) \end{cases} \tag{1}$$

Later, the counters for vehicle B will be re-initialized to zero. Thereby, the defined algorithm will allow to increase or decrease of the DTS of the communicating vehicle periodically depending on its behavior until reaching a minimum of 0 or a maximum of 1. The "Direct Reward" is a weight defined in the interval $[0..1]$. It's used to update the direct trust score DTS. In our experimentation presented later in the next section, we chose a value of 0.2.

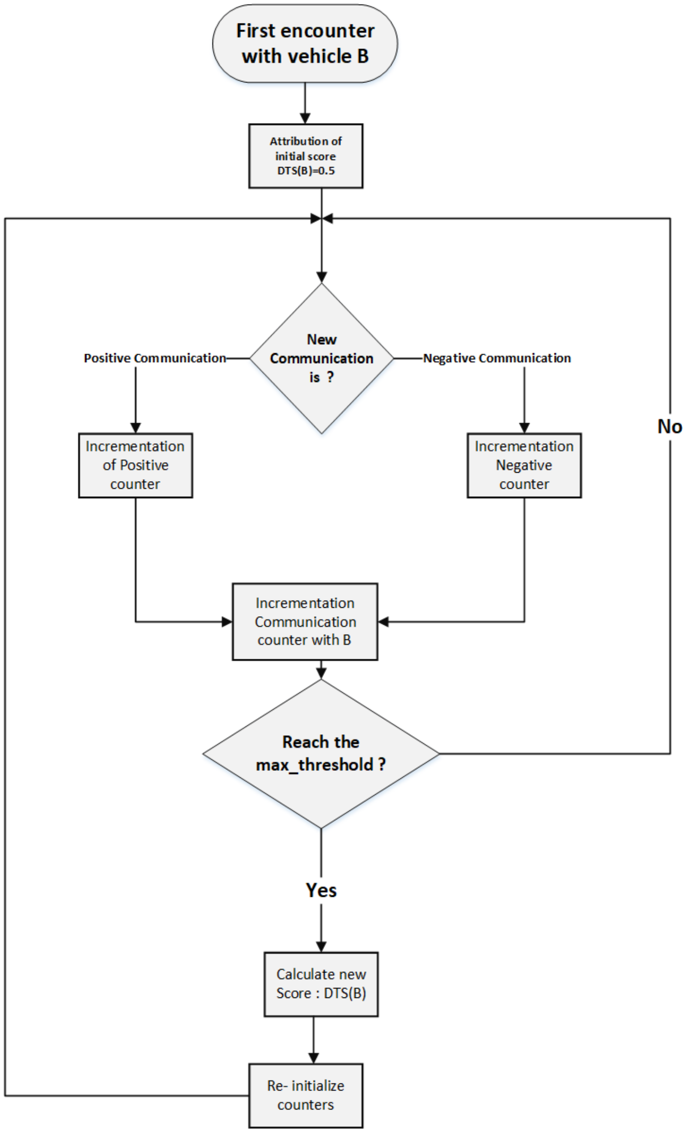
First encounter with vehicle B
Attribution of initial score DTS(B)=0.5
New Communication is ?
Positive Communication
Negative Communication
Incrementation of Positive counter
Incrementation Negative counter
No
Incrementation Communication counter with B
Reach the max_threshold ?
Yes
Calculate new Score : DTS(B)
Re- initialize counters

Fig. 12. DTS update algorithm.

2) The ITS update algorithm : RSUs are responsible for attributing and updating the indirect trust score for each vehicle that has joined the network. Fig. 13 shows the IDS computing algorithm. Vehicles calculate continuously the direct trust score for each encountered node and broadcast their measurement to all nearest RSUs. Periodically, RSUs will use the received DTS measurements to compute a new indirect trust score for each targeted node X. RSUs use the following formula 2

$$ITS(X)_{i+1} = \alpha * ITS(X)_i + \beta * \frac{\sum_{j=1}^{j=N} DTS(X)_j}{N} \tag{2}$$

With $\alpha + \beta = 1$ and N is the number of nodes that have sent their DTS measurement for vehicle X. α and β are weights

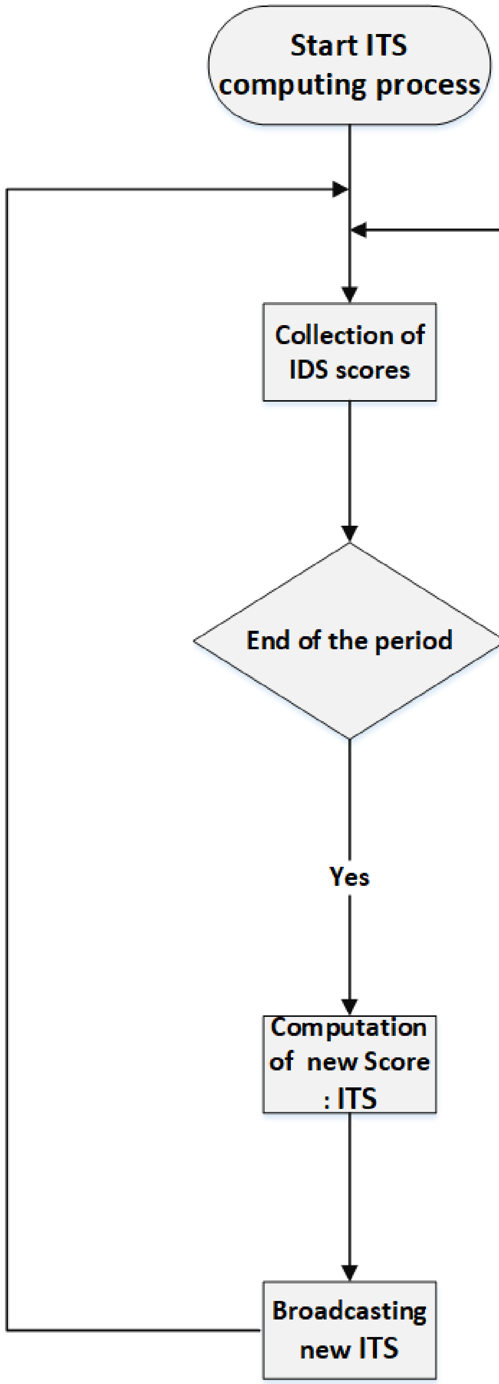

Fig. 13. ITS update algorithm.

used to moderate the combination. The new ITS measurement aggregates all the direct scores measured during the current period with the old indirect score. This formula will tie the estimated behavior of the targeted node to its location. Thus, vehicles will have a better view of communicating over the same region.

3) The HTS update algorithm: The historical trust score is attributed and updated by the TA. It is worth noting that a HTS equal to 0 is the lowest allowed value and a vehicle reaching this level will be banned. A dedicated block will be created and added to the blockchain to announce the expiration of the targeted node certificate. A vehicle with good behavior can reach a maximum value of 1. The algorithm in Fig. 14 explains the HTS management process. When a new car asks for network join, the TA will attribute an initial HTS=0.5 and mention this value in the Authentication Blockchain. The update of the historical score is based on the following features:

- The direct score in the different vehicles: The TA collects direct scores attributed to vehicles encountering the candidate car. The collection is done slowly and passively over a long period. Independently, cars can deposit their local scores on the RSUs during their travel. Later, the TA will contact RSUs periodically and ask for new deposits.
- The indirect score is calculated by all RSUs deployed in the network. The TA also receives the collection of IDS. Periodically, each RSU computes the IDS of all encountered vehicles. Then, it sends the results to the TA.
- The TA uses the reinforcement algorithm KNN (K-Nearest Neighbours) to predict the candidate's behavior. The DTS measurements for each vehicle constitute the KNN algorithm inputs. A new "judgment" about the candidate's behavior will be the algorithm's output.

Depending on the new judgment: malicious or legitimate node, the TA computes the new value of the historical trust score. The new HTS is calculated using the following formula 3

$$HTS_{i+1} = \begin{cases} \alpha * (HTS_i + HReward) + (1-\alpha) * \frac{\sum_{j=1}^{j=N} HTS_j}{N} \\ = 0 \text{ if } HTS_{i+1} < 0) \\ = 1 \text{ if } HTS_{i+1} > 1) \end{cases} \tag{3}$$

Where N is the number of RSUs having an ITS measurement for the candidate. α, is a weight defined in the interval $[0..1]$. The $HReward$ is a weight given depending on the output of the KNN algorithm. If the algorithm finds out that the candidate vehicle is a legitimate node, a positive reward will be given. Otherwise, the attributed value will be negative. We chose a value of 0.2 for this weight. It means:

- $HReward = 0.2$ if the candidate is judged legitimate.
- $HReward = -0.2$ if the candidate is judged malicious.

Thereby, the TA will be able to update vehicle historical scores according to their behavior seen by other nodes (vehicles and RSUs). The better the car behaves during its communications the better will be its HTS. The KNN is an efficient classification reinforcement learning algorithm [39]. Therefore, it helps the TA to predict the candidate's vehicle behavior efficiently.

G. The Final Trust Score and Message Acceptance Decision During V2V or V2I Communications

We have defined three different types of trust score measurement. Direct, indirect, and historical trust score. In this section, we will present how those scores will be combined and used to compute a "Final trust score" which will be used

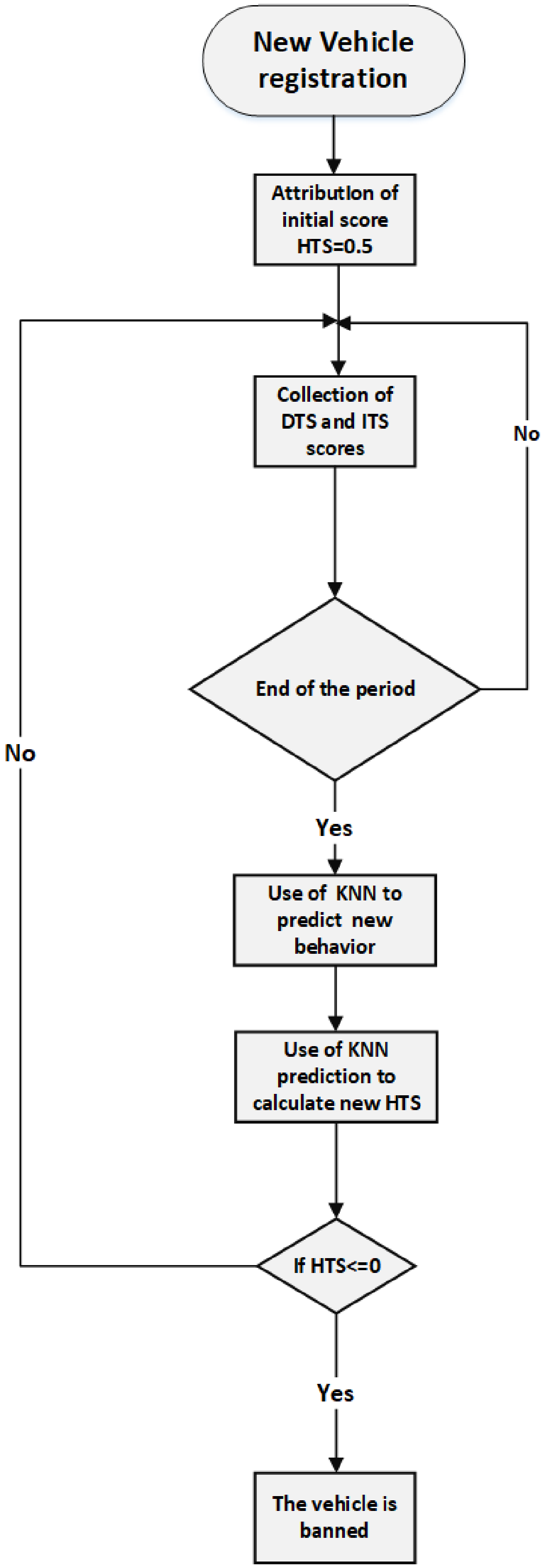
New Vehicle registration
Attribution of initial score HTS=0.5
Collection of DTS and ITS scores
No
End of the period
No
Yes
Use of KNN to predict new behavior
Use of KNN prediction to calculate new HTS
If HTS<=0
Yes
The vehicle is banned

Fig. 14. HTS update algorithm.

TABLE I. WEIGHT ATTRIBUTION CASES FOR FTS

Communication Case	Weight attribution
Public Safety and urgent data	$\alpha = 0$, $\beta = 0$, $\gamma = 1$
User application or ordinary data (general case)	$\alpha = 0.5$,$\beta = 0.2$,$\gamma = 0.3$
Non -important Data	$\alpha = 1$, $\beta = 0$, $\gamma = 0$
Location-based application	$\alpha = 0$, $\beta = 1$, $\gamma = 0$

to decide during the message exchange. Upon receiving a new message from another vehicle, the car can decide whether to continue the communication or not based on the node "Final trust score". Vehicles, during their travel, will face different cases of communication. The exchanged data type can vary from urgent and important data to non-important or advertisement ones. Therefore, nodes can evaluate the sender's behavior differently depending on the communication case.

To face different cases, we introduce the following formula (4) for the final trust score (**FTS**):

$$FTS(X) = \alpha * DTS(X) + \beta * ITS(X) + \gamma * HTS(X) \quad (4)$$

Where $\alpha + \beta + \gamma = 1$. This formula permits the cover of all cases mentioned below by defining various values for the used weights.

In Table I, we introduce examples of weight attribution. In each case, nodes can compute differently the final trust score. We chose to rely on the TA's judgment when dealing with important data. So, the vehicle will neglect the direct and indirect measurements and use only the historical score which will increase the trustworthiness of the exchanged data. In the general case, we combine all the three measurements. For non-important data, vehicles can use only their measurements. Finally, for the location-based data, the trust evaluation done by RSUs will be more convenient to decide about the received messages.

V. PERFORMANCE EVALUATION

1) The evaluation scenario parameters : To evaluate the performance of our solution, we conducted two different experiments. In the first experiment, we aim to study the blockchain's basic operations: new block creation upon a vehicle network join and the proof of existence (POE) during message authentication. The second experiment will study our trust management process to show its accuracy in distinguishing between legitimate and malicious behaviors and its influence on transmission quality. we used the simulators Veins [40], OMNet++ [41], and SUMO [42] . OMNet++ is a well-known C++ event-based simulator for building network simulations. Simulation of Urban Mobility (SUMO) is an open-source, road traffic package for scenario creation. Veins is a framework that includes OMNet++ and SUMO to create and run vehicular network simulations. Table II presents the basic technical parameters.

We used the map of the "Riyadh City" Fig. 15 for the solution performance evaluation. It was generated using the open-source mapping platform "open-street-map" [43]. The covered area is (10 000m,10 000m). The traffic generator SUMO generates random trips for all the vehicles defined in the scenario.

TABLE II. Basic Simulation Parameteres

Parameter	Values
Hardware platform	Speed 3200Mhz, 8GRAM
Operation System	Debian9.4
Traffic Generator	SUMO
Network basic simulator	Omnet++ 5.0 with inet v4.2.8
Vanet Simulator	Veins 5.2
Simulation Area	(10000mx10000m)
Simulation time	500s
Data Rate	6Mbps
Transmission power	20mW

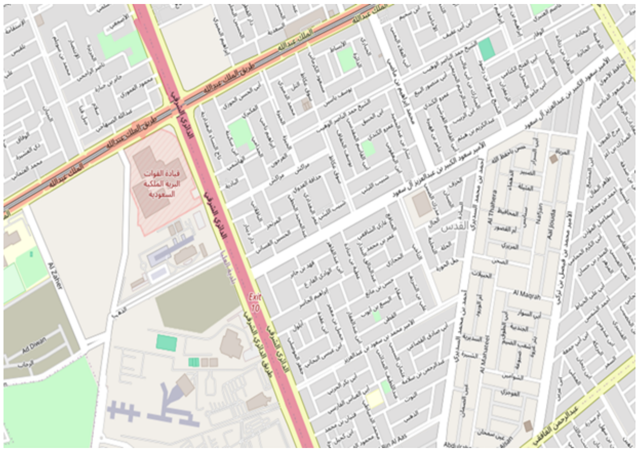

Fig. 15. Riyadh city map.

To evaluate the performance of our trust management approach, we defined the following parameters as mentioned in Table III. In our experiment, we varied the number of traveling vehicles from 20 to 200. We also varied the percentage of malicious vehicles from 20% to 80%. Each vehicle will periodically broadcast data messages. The broadcasting delay is selected randomly depending on the vehicle's behavior. We made the malicious broadcasting delay shorter than the legitimate one to emulate real cases where attackers try to overcharge the network with their forged messages. Fig. 16 shows the Roadside Units deployment. After testing different locations to choose the best positions to cover the entire trajectory used in the vehicle's trips, we selected positions as mentioned in the figure. We observed that more than half of RSUs are placed all along the road "King ABDALLAH street".

TABLE III. Basic Simulation Parameters

Parameter	Values
Number of Vehicles	Varying from 20 to 200
Number of RSU	8
Malicious vehicles rate	Varying20% -40% -60%-80%
Certificate Validity period	3600s
The trust threshold	0.5
The initial trust score	0.5
The direct trust reward	0.2
The historical trust reward	0.2
The direct max count	2
The direct trust broadcasting period	15s
The indirect trust computing and broadcasting period	20s
The historical trust updating period	25s
Legitimate vehicle broadcasting delay	Random in the interval [5—10] s
Malicious vehicle broadcasting delay	Random in the interval [2—6] s

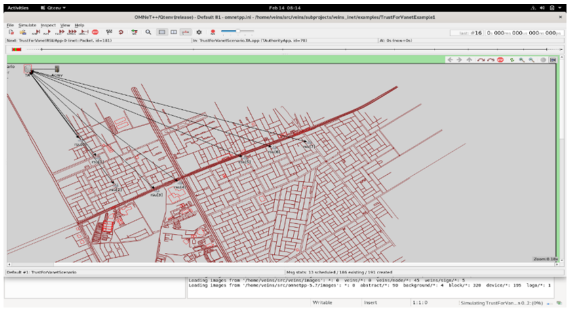

Fig. 16. RSU Deploymemt.

2) The evaluation metrics : We used two types of metrics. Metrics related to the network performance and others focused on the trust estimation. We presented the following metrics:

- PDR: the packet delivery rate. It evaluates the success rate of data packet reception. We consider the PDR for both kinds of transmitted messages: legitimate and malicious.
- Average Transmission Delay: it measures the average delay to successfully transmit legitimate data packets from sender nodes to the receivers.
- Detection accuracy: it measures the ratio of the correctly detected legitimate and malicious messages to the total received messages.
- Average of different trust scores: We evaluated the averages of different trust scores for both kinds of behaviors. Those scores are:
    - ○ Direct trust scores
    - ○ Indirect trust scores
    - ○ Historical trust scores
    - ○ Final trust scores

3) Blockchain computational cost: In our first experiment, we aim to study the performance of our blockchain structure. we implemented the Authentication blockchain in a Python environment using a virtual machine with a speed of 3200Mhz and 8GRAM. We want to evaluate the computational time needed for a vehicle to be registered by the Trust Authority and the time to authenticate received messages.

a) The evaluation of the average registration delay: In Fig. 17, we represented the average registration delay versus the number of vehicles in the network. We varied the network population from 50 to 10,000 vehicles. We observe that the average delay varies in the interval [1...2] seconds. It is worth remembering that TA will create a new block for each new vehicle at its first attempt to join the network. The block contains the vehicle information as mentioned in the previous section. Each block will have a total size of 60 bytes. We use SHA-256 for the blockchain implementation. SHA-256 generates the hash code used as a block identifier citeyoshida2005analysis. The Chronological Merkel Tree (CMT) is the basic chaining structure [37] which minimizes the needed time for block checking. The average time of PoW (Proof Of Work) operation is estimated at around 1 second [44] and it varies depending on the block size and the used technology. In our experiment, results show that the block creation time varies from 1.04 to 1.84

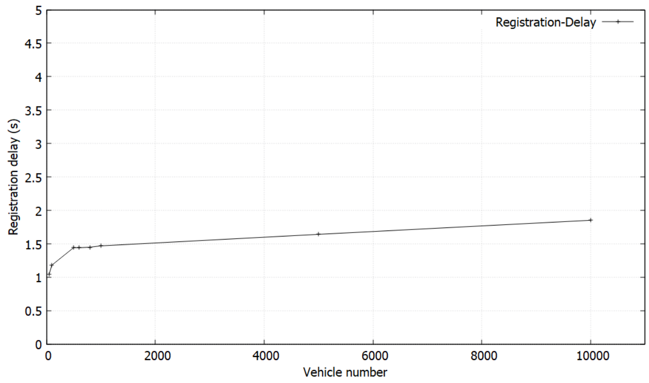

Fig. 17. Average registration delay versus vehicle number.

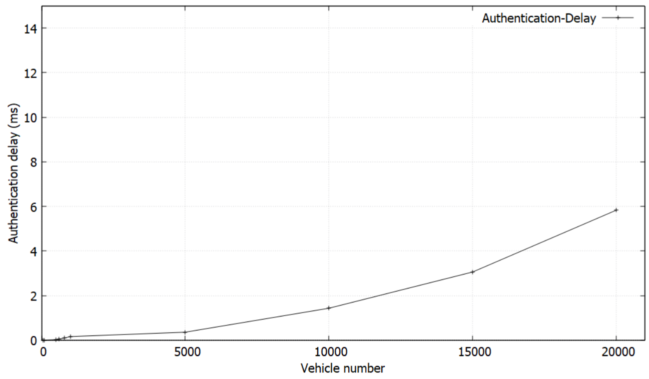

Fig. 18. Message authentication delay versus vehicle number.

seconds with the largest vehicle's number. The delay increases slowly with the number of requestors. Therefore, processing a large number of vehicle registrations will not penalize the network performance. Moreover, TA has exclusive permission to write new blocks and it has sufficient computation resources to perform its tasks without any issues. Consequently, the integration of blockchain as a public ledger in VANET will not affect the network latency.

b) The evaluation of the message authentication: In Fig. 18, we represented the average authentication delay versus the number of vehicles in the network. The message authentication delay is the needed time to verify the message sender's identity during V2V or V2I communications. Vehicles or RSUs will access the used blockchain and search for a corresponding block. The average authentication delay is the needed time to access the Authentication blockchain or other structures and verify the existence of a block for a specific vehicle. It's the elapsed time to perform a proof of presence operation. Our solution uses the algorithm SHA in the blockchain operations whose computational time is around 0.001ms per KB [45].

We varied the network population size from 50 to 20,000 vehicles. Results show that the consumed time increases from 0.0014 to $5.83ms$. Thus, with the largest number of vehicles in the network, an extra delay of $6ms$ will be observed in each message exchange. With less dense network populations, the added delay is less than $2ms$. Consequently, communications between different kinds of nodes will not be gravely affected, and vehicles can quickly authenticate each other's.

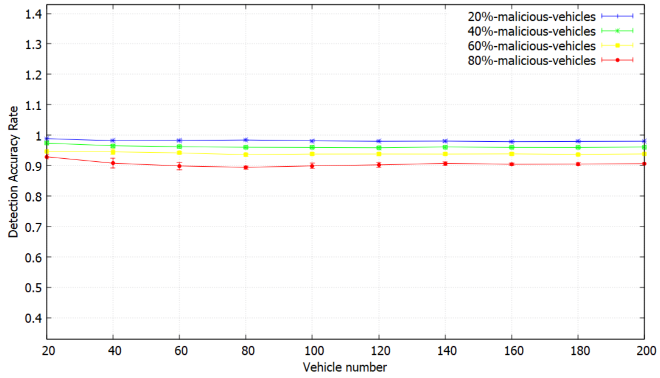

Fig. 19. Detection accuracy rate versus vehicle number.

4) Trust management system evaluation: Our second experiment defines simulation scenarios to evaluate the trust management process. We aim to study the efficiency and correctness of our scheme and its effects on network performance and communication quality.

a) The evaluation of the detection accuracy: Fig. 19 shows the detection accuracy rate over vehicle number variation. We used four different malicious percentages: from 20% to 80%. We see clearly that whatever the number of malicious nodes in the network, our scheme distinguishes correctly between the two behaviors. The detection accuracy rate is always greater than 0.9. With only 20% of malicious vehicles, the detection accuracy is stable around 0.98. With the highest malicious rate (80%), the detection accuracy rate decreases and is stable around 0.9. We also observe that the vehicle number slightly affects the detection accuracy. With fewer vehicles, the detection is less precise than with a bigger network population. It means, that when legitimate nodes are a minority in the network, communications and trust information exchange between them is difficult. But, with a denser network, vehicles have more opportunities to recognize malicious messages.

b) The evaluation of the direct trust score: Fig. 20 and 21 illustrate the measurement of the average direct trust score for both behaviors with various malicious percentages. We also plotted the trust score threshold used by our scheme for a clear comparison. We observe that our proposal successfully recognizes the legitimate nodes. The average attributed direct score varies between 0.68 and 0.83 which is always greater than the defined threshold.

With the smallest malicious cars percentage (20%), the average score was stable at around 0.8 whatever the number of vehicles in the network. Legitimate nodes are more likely to communicate with each other which increases the number of exchanged messages and makes the direct evaluation more precise. With a Higher malicious percentage, the communication opportunities between legitimate cars will be less often because the network will be overwhelmed by malicious messages. Nevertheless, our scheme can correctly identify good behavior and attribute a direct score always greater than $.68$. The direct score attributed to malicious vehicles is presented in Fig. 21. We see that the average score is stable around

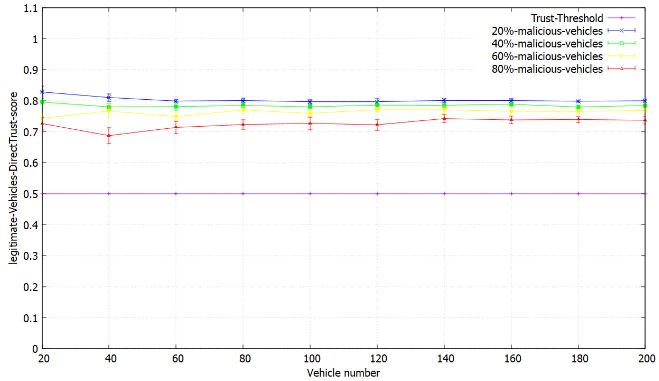

Fig. 20. Average direct score for a legitimate vehicle versus vehicle number.

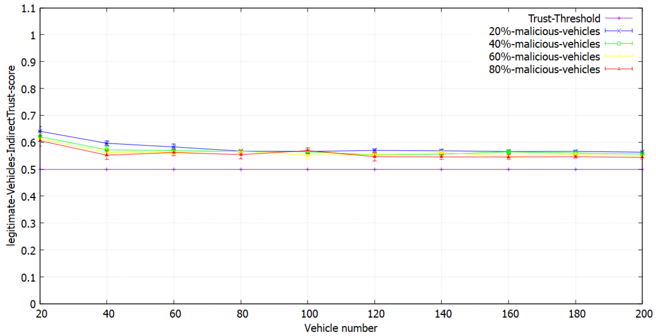

Fig. 22. Average indirect score for a legitimate vehicle versus vehicle number.

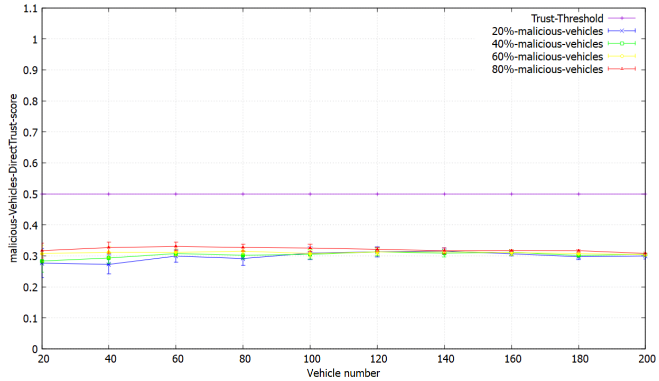

Fig. 21. Average direct score for a malicious vehicle versus vehicle number.

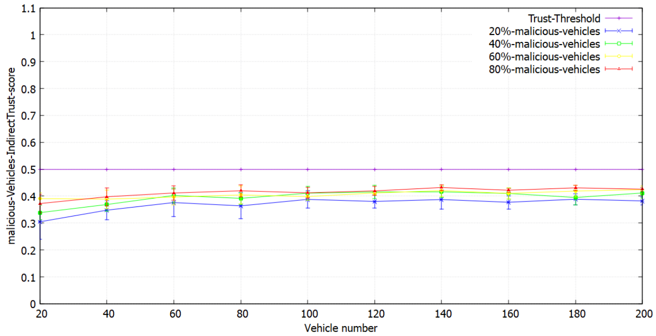

Fig. 23. Average indirect score for a malicious vehicle versus vehicle number.

0.3 less than the threshold score. Our scheme was able to recognize efficiently bad behavior and correctly attributed the corresponding score values. With various malicious rates, our direct score attribution mechanism maintains a clear distinction between behaviors. We remark that in the case of a low network population (less than 60 nodes), the average score with a malicious percentage of 80% is a little higher than with other percentages. The higher density of malicious cars makes their communications with legitimate vehicles less often which leads to fewer opportunities to evaluate their behaviors.

c) The evaluation of the indirect trust score: We represented the measurement of the average indirect score attributed to both behaviors in Fig. 22 and 23. It's worth it to remember that the indirect score is computed and attributed by RSUs. They collect direct scores of network member from their neighborhood and update their score attribution using the formula mentioned in the previous chapter. In Fig. 22, the average indirect score of legitimate nodes is illustrated. We see that the average score is always greater than the defined trust threshold whatever the malicious percentage and the number of cars in the network.

The indirect score is an aggregation of direct scores. The RSUs receive the measurement from nearby nodes and calculate the new value. In doing so, the indirect calculation process reflects the global consensus between nodes in the same neighborhood. With a small percentage of malicious vehicles in the network (20%), the average indirect value is greater than values with higher malicious rates. This means that malicious messages overwhelming the network bandwidth are handicapping behavior evaluation. Nevertheless, our solution is capable of clear recognition of each kind of behavior.

The measurement of average indirect scores for malicious cars illustrated in Fig. 23 confirms our previous observation. Bad behavior is identified in all cases and consequently, lower scores are attributed. The average indirect score for malicious vehicles is always less than the trust threshold value. It was stable between 0.3 and 0.4.

With a high presence of malicious vehicles (percentage over 60%) the average scores were greater than scores with lower rates. As we explained before, the higher presence of malicious cars made it less often for legitimate nodes to encounter them and come up with clear behavior judgments.

d) The evaluation of the historical trust score: We studied the historical trust score attribution process for both behaviors (refer to Fig. 24 and 25). The historical score is attributed by the Trust Authority (TA) using the reinforcement algorithm KNN as defined in the previous section. We observe that the TA manages to efficiently identify node behaviors and correctly attribute the corresponding scores. Legitimate nodes received an average score stable around 0.98 whatever the malicious rate and the vehicle number in the network. While malicious cars received an average score of around 0.1.

We remember that the TA receives direct and indirect score measurements from vehicles and RSUs in the network. All the collected information is cumulated and used as input for

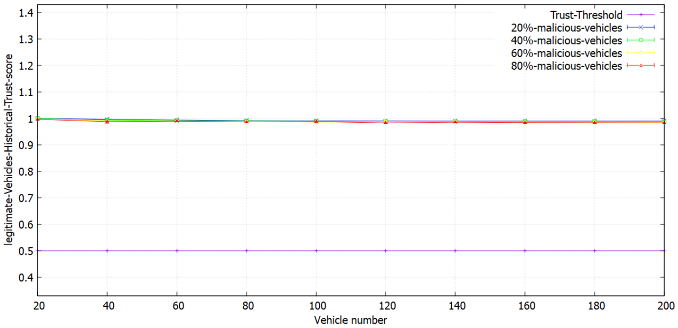

Fig. 24. Average historical score for a legitimate vehicle versus vehicle number.

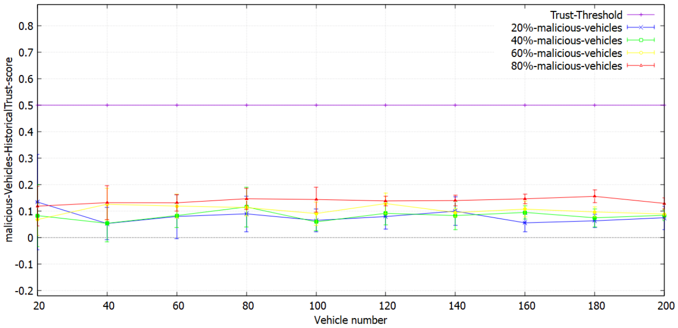

Fig. 25. Average historical score for a malicious vehicle versus vehicle number.

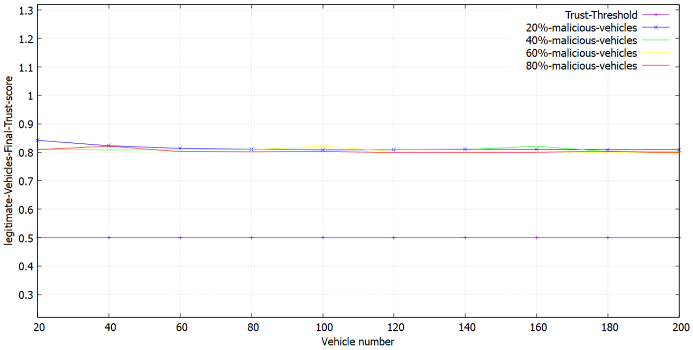

Fig. 26. Average final score for a legitimate vehicle versus vehicle number.

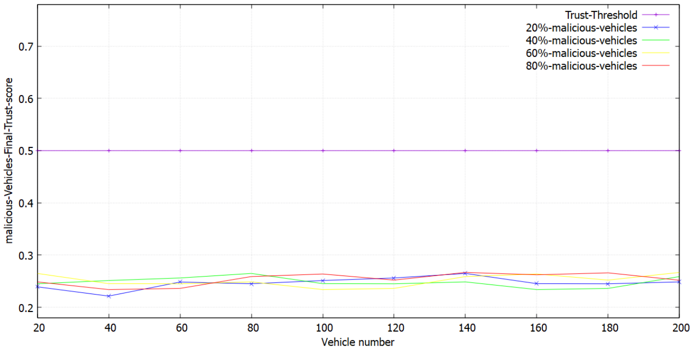

Fig. 27. Average final score for a malicious vehicle versus vehicle number.

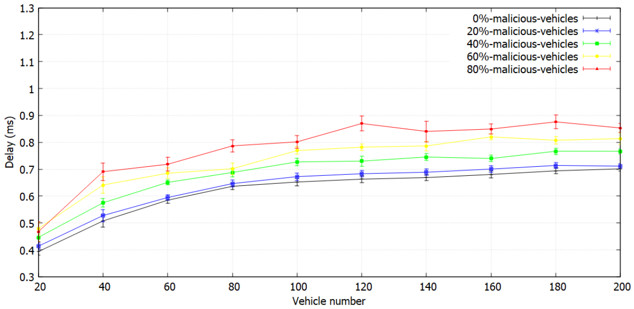

Fig. 28. Average transmission delay versus vehicle number.

the KNN reinforcement learning algorithm. TA successfully recognizes the two kinds of behavior in various situations. Legitimate nodes are identified without any issues. Malicious vehicle rate affects slightly the scores attributed to malicious vehicles. With the highest used rate (80%), the scores given to bad behavior are a little bit greater than scores in the case of a smaller rate (20% or 40%). In a network with a high malicious node density, legitimate nodes are a minority which makes the behavior evaluation more difficult.

e) The evaluation of the final score: Fig. 26 and 27 show the evaluation of the average final score for both kinds of behaviors versus the number of vehicles in the network and using various malicious rates. We remember that the final score formula is defined in the previous chapter. It combines the three evaluated trust score forms (direct, indirect, and historical) with weighted factors.

In this experiment, we studied the case where the weights (0.5, 0.2, 0.3) are respectively given to the score types (direct, indirect, and historical). This situation represents a global communication case without any special needs. We observe that the average final score of legitimate nodes is stable at around 0.8 whatever the used malicious rate and the network population size. Our proposal successfully recognizes the behavior and attributes the correct evaluation. In the case of malicious behavior, the average score is illustrated in Fig. 27 Bad behavior received an average score of around 0.25. As mentioned above, the malicious node density affects the judgment slightly. Legitimate nodes received fewer messages which made their trust evaluation less precise. This handicap leads to a higher score for bad behavior when the malicious rate is greater than 60%.

f) The evaluation of the transmission delay for legitimate data : Fig. 28 shows the data transmission delay versus variation in the number of vehicles with different malicious vehicle rates. We added to the representation a case without any attack (0% malicious vehicles) to compare with a standard transmission situation. We notice that the transmission delay in the attack scenarios is close to the ordinary exchange. First, with 20% malicious vehicles in the network, our proposal generates an extra delay stable of around $0.02ms$ whatever the population size. When the malicious car rates exceed 60%, the gap passes to $0.15ms$. Therefore, our system works without an important impact on the data delivery. The proposed authentication process is fast and efficient and legitimate communications can be carried out with minimum delay.

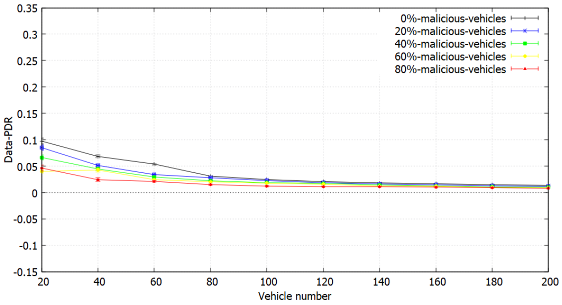

Fig. 29. Average PDR for legitimate data versus vehicle number.

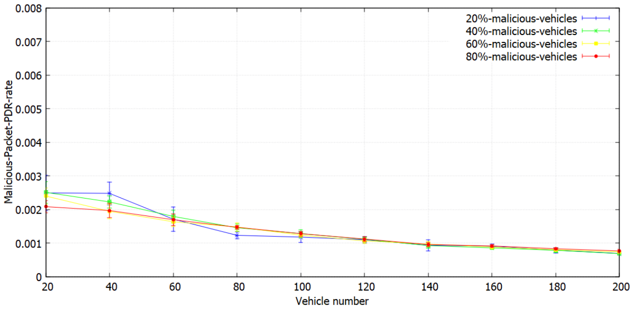

Fig. 30. Average PDR for legitimate data versus vehicle number.

g) The evaluation of PDR: Our second metric to study the impact of our solution on the transmission quality is the evaluation of the Packet Delivery Rate (PDR) which counts the successfully delivered data packet rate. We evaluated the PDR for both kinds of behavior: legitimate and malicious data. Fig. 29 shows the legitimate data PDR versus the variation of vehicle numbers with various malicious vehicle rates. The PDR illustration confirms the result seen in the latency experiment. The PDR for legitimate vehicles is close to ordinary exchange no matter the rate of malicious cars. The highest malicious rate (80%) with the small network size (20 vehicles), shows the lowest successful rate, and the highest gap: 5% with the PDR of the ordinary exchange case. Malicious vehicles outnumber legitimate ones, consequently, they will occupy the network bandwidth and cause high packet loss for legitimate data. With other examples of population, our solution succeeded in reducing the attack overhead and data PDR is always close to ordinary exchange with all used malicious rates.

Fig. 30 illustrates the PDR evaluation for the malicious data to study the amount of harmful packets undetected by our solution. We remark that this amount is almost negligible. Its highest value was 0.0025 when we used 20% of malicious vehicles and a small network population size (20 vehicles). With other malicious rates or population sizes, the accepted malicious packets decrease, and the PDR is stable at around only 0.0015. This result shows that our solution detected efficiently any possible attack and succeeded in blocking and rejecting those packets. The low accepted rate is recorded during the first data exchanges where legitimate nodes were not able to fully evaluate the attacker's behavior. Quickly, our trust management process reveals the packet harm aspect and distinguishes correctly the bad from the good.

5) Result discussion: To study the performance of our solution, we defined two different kinds of experimentation. Firstly, we aim to evaluate the impact of blockchain technology integration on the authentication process. So, we implemented a real structure of the blockchain and tested the different computation operations. We focused on two basic processes: the registration of new vehicles and message authentication during ordinary communications. Our evaluation shows that the consumed time during a new vehicle registration will not exceed 1.84 seconds. This time corresponds to a new block creation and adding to the current ledger. This result remains as expected and lower than the standard time known from a literature review. Our second goal in this experiment was the computation time needed during V2V or V2I message exchange. This time was at around $0.001ms$. it corresponds to the PoE (Proof of Existing) operation. We find out that, the blockchain integration in the VANET authentication process offers transparency and sensitive data preservation without overcharging network members.

Our second experiment used simulation scenarios to evaluate trust management and its impact on communication and network performances. Results show the correctness of our scheme. We observed that the detection accuracy rate was high and stable around 0.98 which demonstrates that node behaviors were recognized effectively. The evaluation of the different defined levels of trust scores: direct, indirect, historical, and final, indicates that the behavior score was quickly reviewed and updated. In a small populated network, the trust management system allows clear differentiation. Legitimate scores have been increased to over 0.8 and malicious scores have been decreased to 0.15. In populated networks, the recorded scores were around 0.75 for good behaviors and 0.3 for bad ones. Analysis of those results shows that the trust score attribution is slightly affected by the encountering probability. In small networks, a few vehicles are more likely to meet than in large networks. Therefore, the trust evaluation process can detect malicious behavior regardless of network size. In addition, it is more effective when vehicles pass each other very often.

Our second interest was the effects on communication quality. Results proved that the proposed scheme did not affect ordinary communications between network legitimate nodes. Data packets are still delivered quickly. In small networks, the identity verification process will add around $0.02ms$ to packet transmission time. While in larger networks the extra delay is around $0.15ms$. Packet delivery rate measurement shows that we maintain high rates close to ordinary exchange without any attack.

VI. Conclusion

In this age of emerging technologies, we have to face these security challenges, specifically in the context of VANETs, which have become a rich field for scientific research. In this paper, we highlighted the concern of privacy protection in VANETs. We proposed a new authentication solution for VANET to ensure private data preservation and distinguish legitimate users from malicious ones. Our proposal introduces the use of blockchain technology as a reliable structure to maintain trustworthy authentication information and provide vehicles with an effective technique to authenticate any received message. We designed also a new trust management process where vehicles evaluate their communicator's behavior and attribute trust scores accordingly. We defined various kinds of scores. Each one reflects different levels of trust evaluation decisions. Direct trust to reflect the node relationships. An indirect score is calculated by TA to reflect a bigger view. And a historical score using the reinforcement algorithm KNN to have a deeper evaluation of the node behavior. Finally, we evaluated the performance of our solution. Our analysis showed that our proposal provides an effective behavior management system and meets all the requirements for security and privacy in VANET. In future research, we will investigate the possibility of designing a new attack mitigation technique and we will focus on testing real attacks to evaluate the performance of our system.

Acknowledgment

The authors extend their appreciation to the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMISIU) for funding and supporting this work through the Graduate Students Research Support Program.

References

[1] R. Suryadithia, M. Faisal, A. S. Putra, and N. Aisyah, "Technological developments in the intelligent transportation system (its)," *International Journal of Science, Technology & Management*, vol. 2, no. 3, pp. 837–843, 2021.

[2] M. S. Sheikh and J. Liang, "A comprehensive survey on vanet security services in traffic management system," *Wireless Communications and Mobile Computing*, vol. 2019, pp. 1–23, 2019.

[3] A. Rasheed, S. Gillani, S. Ajmal, and A. Qayyum, "Vehicular ad hoc network (vanet): A survey, challenges, and applications," in *Vehicular Ad-Hoc Networks for Smart Cities: Second International Workshop, 2016*. Springer, 2017, pp. 39–51.

[4] R. Hussain, J. Lee, and S. Zeadally, "Trust in vanet: A survey of current solutions and future research opportunities," *IEEE transactions on intelligent transportation systems*, vol. 22, no. 5, pp. 2553–2571, 2020.

[5] H. Cheng, X. Fei, A. Boukerche, and M. Almulla, "Geocover: An efficient sparse coverage protocol for rsu deployment over urban vanets," *Ad Hoc Networks*, vol. 24, pp. 85–102, 2015.

[6] S. A. Jan, N. U. Amin, M. Othman, M. Ali, A. I. Umar, and A. Basir, "A survey on privacy-preserving authentication schemes in vanets: attacks, challenges and open issues," *IEEE Access*, vol. 9, pp. 153 701–153 726, 2021.

[7] P. Mundhe, S. Verma, and S. Venkatesan, "A comprehensive survey on authentication and privacy-preserving schemes in vanets," *Computer Science Review*, vol. 41, p. 100411, 2021.

[8] M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in vanets: Communication, applications and challenges," *Vehicular Communications*, vol. 19, p. 100179, 2019.

[9] M. M. Hamdi, L. Audah, M. S. Abood, S. A. Rashid, A. S. Mustafa, H. Mahdi, and A. S. Al-Hiti, "A review on various security attacks in vehicular ad hoc networks," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 5, pp. 2627–2635, 2021.

[10] C. H. Quevedo, A. M. Quevedo, G. A. Campos, R. L. Gomes, J. Celestino, and A. Serhrouchni, "An intelligent mechanism for sybil attacks detection in vanets," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE, 2020, pp. 1–6.

[11] A. Quyoom, A. A. Mir, D. A. Sarwar *et al.*, "Security attacks and challenges of vanets: a literature survey," *Journal of Multimedia Information System*, vol. 7, no. 1, pp. 45–54, 2020.

[12] S. Dong, H. Su, Y. Xia, F. Zhu, X. Hu, and B. Wang, "A comprehensive survey on authentication and attack detection schemes that threaten it in vehicular ad-hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, 2023.

[13] X. Xu, Y. Wang, P. Wang *et al.*, "Comprehensive review on misbehavior detection for vehicular ad hoc networks," *Journal of Advanced Transportation*, vol. 2022, 2022.

[14] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in vehicular ad-hoc networks (vanets)," *Vehicular Communications*, vol. 25, p. 100247, 2020.

[15] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain: research and applications*, vol. 3, no. 2, p. 100067, 2022.

[16] S. K. Dwivedi, R. Amin, A. K. Das, M. T. Leung, K.-K. R. Choo, and S. Vollala, "Blockchain-based vehicular ad-hoc networks: A comprehensive survey," *Ad Hoc Networks*, p. 102980, 2022.

[17] A. R. Javed, M. A. Hassan, F. Shahzad, W. Ahmed, S. Singh, T. Baker, and T. R. Gadekallu, "Integration of blockchain technology and federated learning in vehicular (iot) networks: A comprehensive survey," *Sensors*, vol. 22, no. 12, p. 4394, 2022.

[18] R. S. Sutton and A. G. Barto, "Reinforcement learning: An introduction," *Robotica*, vol. 17, no. 2, pp. 229–235, 1999.

[19] W. Ahmed, W. Di, and D. Mukathe, "Blockchain-assisted privacy-preserving and context-aware trust management framework for secure communications in vanets," *Sensors*, vol. 23, no. 12, p. 5766, 2023.

[20] E. Meamari and C.-c. Shen, "Trcoin: A blockchain-based robust trust management system for vanet," *Authorea Preprints*, 2023.

[21] F. Ghovanlooy Ghajar, J. Salimi Sratakhti, and A. Sikora, "Sbtms: Scalable blockchain trust management system for vanet," *Applied Sciences*, vol. 11, no. 24, p. 11947, 2021.

[22] Y. Inedjaren, M. Maachaoui, B. Zeddini, and J.-P. Barbot, "Blockchain-based distributed management system for trust in vanet," *Vehicular Communications*, vol. 30, p. 100350, 2021.

[23] C. Pu, "A novel blockchain-based trust management scheme for vehicular networks," in *2021 wireless telecommunications symposium (WTS)*. IEEE, 2021, pp. 1–6.

[24] Y. Hui, Z. Su, T. H. Luan, and C. Li, "Reservation service: Trusted relay selection for edge computing services in vehicular networks," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 12, pp. 2734–2746, 2020.

[25] A. Sonker and R. Gupta, "A new procedure for misbehavior detection in vehicular ad-hoc networks using machine learning." *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 11, no. 3, 2021.

[26] J. Zhang, K. Zheng, D. Zhang, and B. Yan, "Aatms: An anti-attack trust management scheme in vanet," *IEEE Access*, vol. 8, pp. 21 077–21 090, 2020.

[27] U. Javaid, M. N. Aman, and B. Sikdar, "Drivman: Driving trust management and data sharing in vanets with blockchain and smart contracts," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*. IEEE, 2019, pp. 1–5.

[28] S. Guleng, C. Wu, X. Chen, X. Wang, T. Yoshinaga, and Y. Ji, "Decentralized trust evaluation in vehicular internet of things," *IEEE Access*, vol. 7, pp. 15 980–15 988, 2019.

[29] S. Ahmed, S. Al-Rubeaai, and K. Tepe, "Novel trust framework for vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9498–9511, 2017.

[30] W. Liang, Z. Li, H. Zhang, S. Wang, and R. Bie, "Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends," *International Journal of Distributed Sensor Networks*, vol. 11, no. 8, p. 745303, 2015.

[31] S. Malik and P. K. Sahu, "A comparative study on routing protocols for vanets," *Heliyon*, vol. 5, no. 8, 2019.

[32] A. A. Taleb, "Vanet routing protocols and architectures: An overview." *J. Comput. Sci.*, vol. 14, no. 3, pp. 423–434, 2018.

[33] H. Chen, R. Zhang, W. Zhai, X. Liang, and G. Song, "Interference-free pilot design and channel estimation using zcz sequences for mimo-ofdm-based c-v2x communications," *China Communications*, vol. 15, no. 7, pp. 47–54, 2018.

[34] M. El Zorkany, A. Yasser, and A. I. Galal, "Vehicle to vehicle "v2v" communication: scope, importance, challenges, research directions and future," *The Open Transportation Journal*, vol. 14, no. 1, 2020.

[35] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new type of blockchain for secure message exchange in vanet," *Digital communications and networks*, vol. 6, no. 2, pp. 177–186, 2020.

[36] I. Roussou, C. Dritsaki, E. Stiakakis *et al.*, "The bitcoin's network effects paradox—a time series analysis," *Theoretical Economics Letters*, vol. 9, no. 06, p. 1981, 2019.

[37] M. Bosamia and D. Patel, "Current trends and future implementation possibilities of the merkel tree," *International Journal of Computer Sciences and Engineering*, vol. 6, no. 8, pp. 294–301, 2018.

[38] A. S. Rajasekaran, M. Azees, and F. Al-Turjman, "A comprehensive survey on blockchain technology," *Sustainable Energy Technologies and Assessments*, vol. 52, p. 102039, 2022.

[39] N. C. Luong, D. T. Hoang, S. Gong, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim, "Applications of deep reinforcement learning in communications and networking: A survey," *IEEE communications surveys & tutorials*, vol. 21, no. 4, pp. 3133–3174, 2019.

[40] C. Sommer, D. Eckhoff, A. Brummer, D. S. Buse, F. Hagenauer, S. Joerer, and M. Segata, "Veins: The open source vehicular network simulation framework," *Recent advances in network simulation: the OMNeT++ environment and its ecosystem*, pp. 215–252, 2019.

[41] C. Sommer, D. Eckhoff, A. Brummer, D. Buse, F. Hagenauer, S. Joerer, M. Segata, A. Virdis, and M. Kirsche, "Recent advances in network simulation: The omnet++ environment and its ecosystem," 2019.

[42] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "Sumo–simulation of urban mobility: an overview," in *Proceedings of SIMUL 2011, The Third International Conference on Advances in System Simulation*. ThinkMind, 2011.

[43] J. Bennett, *OpenStreetMap*. Packt Publishing Ltd, 2010.

[44] F. Wilhelmi, S. Barrachina-Muñoz, and P. Dini, "End-to-end latency analysis and optimal block size of proof-of-work blockchain applications," *IEEE Communications Letters*, vol. 26, no. 10, pp. 2332–2335, 2022.

[45] R. P. Naik and N. T. Courtois, "Optimising the sha256 hashing algorithm for faster and more efficient bitcoin mining," *MSc Information Security Department of Computer Science UCL*, pp. 1–65, 2013.