

A Conditional Privacy-Preserving, Lightweight V2I and V2V Authentication Framework for IoV using VANETs

Mubarak Almutairi

College of Computer Science and Engineering,
University of Hafr Albatin, Saudi Arabia

ABSTRACT

intelligent transportation systems (ITS) along with internet of vehicles (IoV) have been widely used to improve road safety, comfort, security and flow of traffic. Connected and autonomous vehicles interact with their surroundings, including infrastructure, sensors, computing nodes, etc. via IoV. Communication security has been always a serious concern. Vehicular ad hoc networks (VANETs) can increase driving efficiency and safety while at the same time meet the necessary security requirements through the use of cryptographic techniques. Because VANETs rely significantly on processing efficiency, a speeding car when entering the VANET's service area may reduce communication quality and raise the risk of traffic accidents. The certification authority (CA) is able to predict the vehicle's route in order to send a message to the roadside unit (RSU) in advance. An intelligent vehicle-to-infrastructure (V2I) authentication system that is both privacy-preserving and lightweight is proposed in this work. Boneh, Goh, and Nissim (BGN), a homomorphic encryption approach based on the Moore curve, is used to determine route information before a vehicle sets off on its journey. All roadside units in a region are converted to a vector by CA even if they have no knowledge of the route plan. Using the data acquired from the RSUs, a vehicle's connection to each RSU along its route can be quickly verified.

Keywords: Intelligent transportation systems, blockchain, vehicle to vehicle communication

INTRODUCTION

In general, intelligent transportation systems (ITS) offer a wide range of applications that improve road safety, comfort, security, and traffic flow. Rapid advances in a wide range of sensing and communication technologies have been noticed recently as a result of the human desire to travel in safety, comfort, and on time. Front sensors, controllers, actuators, and other devices are mounted in the car and incorporate modern communication and communication technologies for the implementation of transactions and exchange of information between the vehicle and the vehicle, methods, and resources. ITS has a deep grasp of the environment, can make sensible decisions, and conduct a number of other functions. [1]. The Internet of Things (IoT) is projected to serve a number of modern ITS applications. Easy driving, safety, and assistance technology are the primary objectives. It is common for automobile internet technology systems to integrate machine learning, the automotive industry, electronic mapping and installation, IoT, intelligence management, big data management, secure data sharing, intelligent navigation, graphics, and mobile device connectivity [2]-[8]. Recent advancements

in vehicle technology, high throughput satellite communication, the IoT, and cyber physical systems have made Internet of Vehicles research an important area of study with practical applications.

The IoT will reduce traffic accidents and improve security, performance, and other benefits as a result of data closure services and the integration of traffic, road, and environmental information. Using the IoT, drivers are required to constantly update their position, speed, and other vehicle related data [9]-[15]. By monitoring the relationship between the message and the sender, defective vehicles can gather personal data (such as position, data, etc.) from the driver. Privacy issues, increased data leakage risk, and possible danger to passengers are all possible consequences [16]-[22]. Because of rapid app and service growth in the automobile industry, there will be a huge volume of data and network traffic to deal with. In addition, IoV's mobility, low latency, contextual complexity, and heterogeneity will make typical cloud storage and management difficult [23]-[28]. The interoperability and compatibility of IoV entities held by different service providers is similarly complex. For IoV data exchange and storage to fulfil future growth requirements and deliver on its promises, a decentralised, distributed, interoperable, and scalable platform is required. Security, privacy, and reliability of the IoV data must be ensured because the network is decentralised and distributed. Blockchain technology, modern encryption techniques, and edge computing have already been used in a number of IoV applications [29].

In the ITS business, blockchain has the ability to solve numerous difficulties [30], and its basic architecture can be applied to social interactions as well. The security of communication is a major issue for ITS, and blockchain offers a perfect answer to this problem [31]-[34]. Intelligent systems use a variety of incoming vehicle data as input tables in order to develop the most efficient traffic planning. Due to a lack of real time processing and central algorithms and data centres, vehicle information in the input table is vulnerable to malicious assaults. A simple but reliable security authentication technique is required for ITS communication security. This work comes up with an innovative approach to this problem and provides the following contributions:

1. A blockchain-based authentication scheme is proposed for ITS having the capabilities of a viable option for the transportation industry.
2. An advanced blockchain based authentication protocol is proposed for ITS. Blockchain is integrated into the current intelligent transportation system design and procedures. Users' privacy is protected by the planned blockchain-aided transportation system (Ba-ITS), but the system is also backwards compatible with the old intelligent transportation system, making it a viable option for the transportation industry.
3. Consideration is given to the interoperability of different blockchain layers. Extensive examples of how smart contracts and blockchain related messaging might be coupled to create efficient new services will be presented.
4. The proposed framework provides Pseudonym based authentication that is fast and secure, balancing security with performance, which is another big challenge for the researchers

The rest of the paper is structured as follows. The literature review is presented in Section 2. Section 3 discusses the proposed approach with description of its different phases and their

implementation. Results are discussed in Section 4 while Section 5 concludes this study.

RELATED WORK

For ITS solutions, a reliable, secure and efficient service is required. As the number of vehicles grows large data leakage problem may rise also, in addition to introducing data delays due to large amount of data. To overcome these problems, new solutions have been developed. Using hash encrypted block chain technology, authentication and authentication numbers can be used to set up keys used to report the history and accuracy of data [6]. The lightweight authentication protocol is studied in [7]. A lightweight identity authentication protocol (LIAP) was presented where a vehicle and RSUs first share a unique authentication sequence, and then mutual authentication is established using a dynamic secret session process (DSSP).

The study [8] proposes a hardware free conditional privacy-preserving authentication (CPPA) approach for VANETs based on elliptic curve cryptography. The method satisfies VANET security and privacy requirements, solves the problem of private key compromise, and prevents privilege escalation. According to the findings, the proposed technique is more efficient in VANETs than previous schemes. Similarly, a privacy-preserving, cross-domain group authentication mechanism is proposed in [9]. The system offers higher security features and better performance than previous authentication protocols. The study [10] offers a block chain-based authentication protocol with lower packet delivery ratio (PDR) and latency. The authentication procedure, on the other hand, requires minimal storage and generates low computational overhead. Authors present the enhanced certificate less and provably secure conditional privacy-preserving authentication (ECPS-CPPA) protocol for automotive settings [11]. It satisfies both privacy and security requirements in the VANETs system.

Scalability is also a big concern for VANETS and efforts have been made along these directions correspondingly. [12] provides a scalable, privacy-preserving authentication protocol for safe VANETs. The protocol employs hybrid cryptography. Extensive simulations are done and compared to existing work based on PKI and HMAC to validate the proposed ESPA protocol. ESPA is a more efficient, scalable, and secure protocol than earlier protocols. The authors present a scalable and privacy-preserving authentication protocol in [13]. It requires single authentication when entering a region of roadside unit gateway. Results indicate that the approach reduces the amount of authentication packets and MAC/PHY overhead, while being robustness against various types of attacks.

Beside security, efficiency in terms of processing time is another important perspective for VANETs. A privacy-preserving vehicle safety approach, vehicular safety message based on chaos is proposed in [14]. It meets transmission requirements with a high probability of 85 percent and low round trip duration of 50 milliseconds. With a processing time of only 2-3 milliseconds, the suggested chaos-based encryption method achieves quicker speeds, demonstrating its lightweight qualities appropriate for time critical applications. The study [15] presents scheme to ensure legitimacy of a safety message while maintaining anonymity. Results indicate that it take less than 100 miliseconds to broadcast a safety group message, and less than 150 milliseconds to transmit a non safety group message. A multizone authentication and privacy-preserving protocol is presented in [16]. When compared to earlier methods, the

proposed methods considerably cut signature creation time by 16 to 80 times. Furthermore, the new method dramatically reduces signature verification time by 10 to 16 times.

The authors propose the use of batch confirmation for V2I authentication in [17] to lower the burden and increase efficiency. For this purpose, aggregate signature technology is adopted and authors present a new certificate less aggregate signature system for VANETs. Similarly, [18] proposes an V2I authentication scheme including crucial insulation. Vehicles might update their own secret keys using an assistance device on a regular basis. Forward and backward secrecy can be been achieved in this manner. The V2I authentication protocol in [19] uses symmetric encryption, group communication, and proactive authentication to design a lightweight authentication system. The results reveal that the proposed protocol works effectively in both high- and low-density traffic environments. Similarly, [20] proposes a lightweight authentication protocol for V2G, especially for protection of electric vehicle identities, vehicle tracking prevention, and data confidentiality. The lower resource consumption contributes to signaling congestion reduction and bandwidth savings. The protocol guards against a variety of known threats, and security analysis reveals that it meets the standard's security objectives.

SYSTEM ARCHITECTURE

We classify the protocols used in VANETs that are used to protect privacy, authenticate users, and distribute secure messages into several categories and examine the advantages and disadvantages of each protocol within each category. Because several protocols might be classified in more than one category, it is impossible to give a definitive classification of them all. This is merely a generalization.

Network Model

There are three key players in the VANET system model: an authentication server (AS), a large number of (RSUs), and a large number of vehicles. The AS is presumed to be completely trustworthy, while RSUs are thought to be just somewhat trustworthy while the vehicles are presumed to be completely untrustworthy. As a result, each vehicle is expected to contain an on-board unit (OBU) with limited processing and storage capabilities that communicates with the RSUs. The OBU will be used to designate a specific vehicle in the following sections. Furthermore, with VANET, neither the wired nor the wireless channels are expected to be secure. A hacker can therefore intercept messages being delivered and use them to conduct various attacks.

System Model:

Fig. 1 depicts a simple model made up of three components: a CA, an RSU, and a vehicle. A semi trusted certificate authority (CA) may try to derive valuable information from legally received messages. In addition, CA manages VANETs and helps RSU verify the vehicle by storing RSU information. It receives and passes on the information from a vehicle within its range via RSU. OBU and TPD modules installed in a vehicle communicate information with RSU and CA, while TPD keeps private data for secure computing.

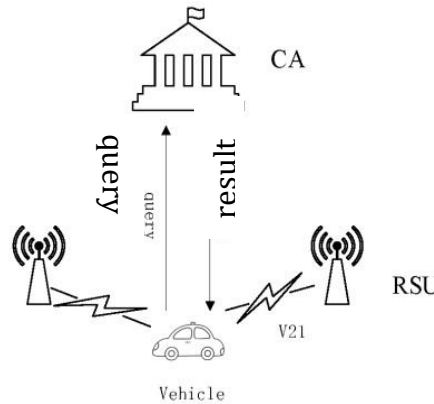


Figure 1: System model used in this study.

Design Goals for ITC:

Message Integrity:

One of the most important considerations in the design process is message integrity, which means that any changes made to an open channel message should be detected by the receiver.

Message Confidentiality:

The eavesdropped message is useless to an attacker.

Route Plan Privacy:

If all RSUs are compromised, the genuine identification of the vehicle cannot be deduced because the RSU and CA cannot collaborate.

Ride Sharing Anonymity:

CA assists a vehicle in obtaining RSUs' information on its route, but does not know which RSUs' information has been gleaned.

New ITS design is proposed that incorporates blockchain technology. Overlays of hierarchical blockchain are built on top of the vehicular network infrastructure in this architecture. Because no new network entities are added, the ITS's existing services can be used with confidence. Protecting user privacy while reducing the likelihood of a system or service failing due to a single point of failure is made possible by the block chain's decentralization and anonymity. Because of the immutability of the blockchain, data integrity and evidence of hostile activity in the intelligent transportation systems are both guaranteed. New intelligent transportation system services can be launched quickly and easily using blockchain's smart contracts. Meanwhile, legacy vehicle networks can continue to analyze and transmit data efficiently. Ultimately, we want to encourage vehicles and ITS users to actively participate in the intelligent transportation system by providing and utilizing data. The ITS oriented blockchain model with proposed seven layers is shown in Fig. 2.

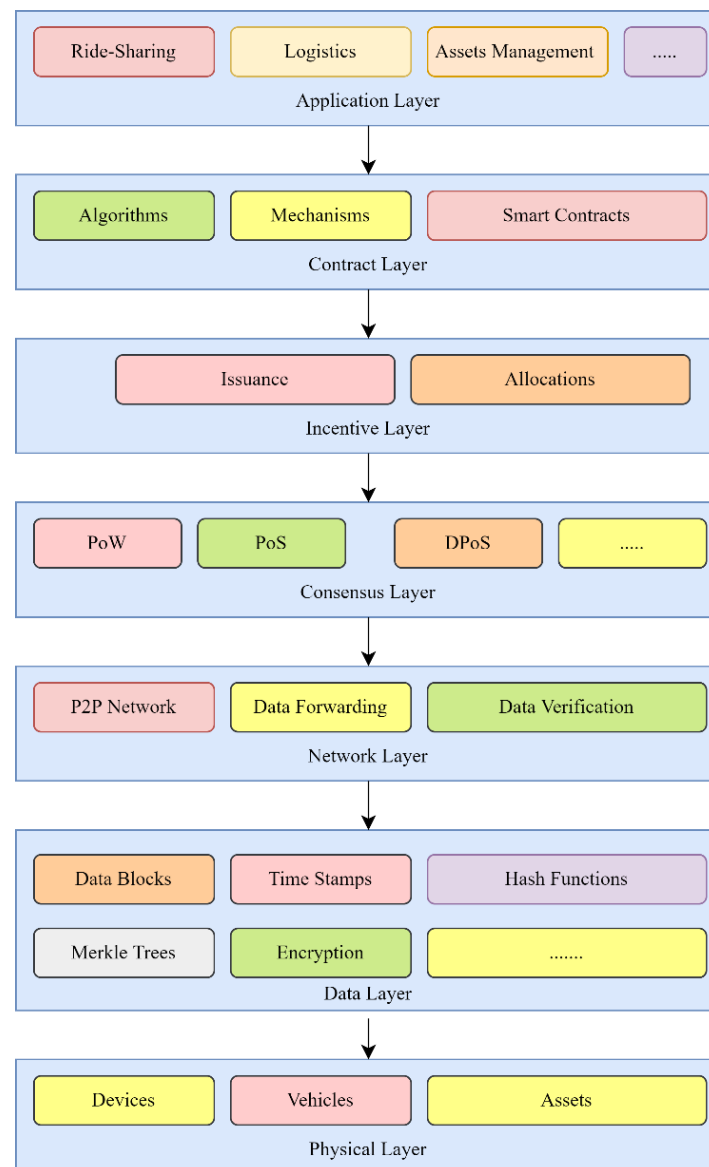


Figure 2: Intelligent transportation system oriented blockchain framework.

Privacy Preserving Lightweight Architecture

PLV scheme has four stages: initialization, registration, query, and authentication. California automobile association (CA) produces and publishes security parameters, as well as RSU information, during the first phase. This information is exchanged when registration with CA. Vehicle queries CA during the query phase and deduces the information of RSUs along its route; nevertheless, CA is unaware of which RSUs' information has been deduced by the vehicle during this phase. After that, vehicle and RSU rapid authentication is achieved.

Initial Phase:

In the initial phase, following steps are carried out

- CA generates a Public and Private Key to RSU,
- RSU selects its symmetric encryption key,
- CA uses Moore Curve to process the map (actual),

- CA then creates the actual map using Moore curve and keep its security,
- Registration phase,
- TDP of vehicle will create some composite bilinear parameters,
- TDP will be send to CA,
- CA create a chain of ids,
- CA will create a hash train for PWD

Query Phase:

In order to anticipate a vehicle's path on the actual map, the TPD utilizes the Dijkstra algorithm. Cells that are passed are set to 1; otherwise, they are set to 0. The map is then transformed into a sequence L using Moore curves by TPD. When $cell_0$, $cell_1$, and $cell_2$ are all 1, and $cell_3$ is a 0, the path L is represented as 1, 1, 1, and 0. In this case, the trajectory of the vehicle may readily be deduced by CA from its prior requests if EL is sent straight to it. CA gets no information regarding the vehicle's trajectory because TPD chooses a random number and spins EL by d .

Vehicle to Vehicle and Vehicle to Infrastructure Communications

V2V communications are used between vehicles, while V2I communications are used between vehicles and the roadside infrastructure. Designing a VANET while considering vehicular mobility is a difficult task. This study provides a fundamental understanding of how vehicular mobility affects the density of VANET networks and the connectivity between V2V and V2I. Valet mobility is required for VANET designers in the future. Examples of this mobility include connectivity under specific road traffic situations inside specific geographic locations, routing protocols for multi hop based applications, or security and privacy threats and mitigations. To test connectivity and network performance, tools that make building and visualizing VANET scenarios easy are needed.

First and second phases of this study are separate. In the first phase, we simulate highway mobility to evaluate the network densities available for V2V connectivity under various traffic volumes. In the second phase, we visualize and evaluate two different VANET situations like V2V communication and a vehicle-to-remote sensing unit (RSU) V2I communication.

Blockchain Based Service Sharing via Road Side Units

Vehicles in this model have already been registered by the revocation authority. In addition, blockchain includes vehicle data and a timestamped record of prior car sharing services. RSU assists vehicles in requesting services from other vehicles in accordance with their needs. Whenever a vehicle sends out a request, the RSU receives it. Response vehicles' services have already been entered into RSU's database. This request will be sent to the network by RSU. Messages will be sent out to every car connected to the network. After that, the car that is available will contact the one that was requested. Smart contracts will be generated between the respondent and responding cars if both vehicles agree to their terms of the smart contract when they agree to share their services with each other. To mine the blocks, proof of work (POW) is needed, and it is also included in each transaction. Consensus mechanisms are then utilized to verify the block's validity and add it to the blockchain. In order to add on blockchain, the transaction must be validated by at least 51% of the nodes.

In addition, according to the terms of the smart contract, the car that reacted will be rewarded. In exchange for an incentive, the responding vehicle will provide its services to the requested vehicle. It is assumed that this is a specific RSU-to-vehicle sharing scenario. There are many examples of this, such as when a vehicle is running low on gas. Vehicles are also congregating at the gas station. In order to get out of the wait sooner, the vehicle will make a request. RSU will be notified of this request. As a result, RSU will issue a follow up request to the network to see if any vehicles are available to react to that particular request. If any car agrees to share their service, the requested vehicle will receive a response. After that, a smart contract between the two vehicles will be activated. Transactions on blockchain will be included to the consensus mechanism. Furthermore, in order to reap the benefits of smart contracts, both vehicles must agree on the rules. Responding vehicles will then be rewarded for sharing their services and moving on to the next gas station. The requested vehicle takes the place of the vehicle that answered. The model of blockchain used service sharing is given in Fig. 3.

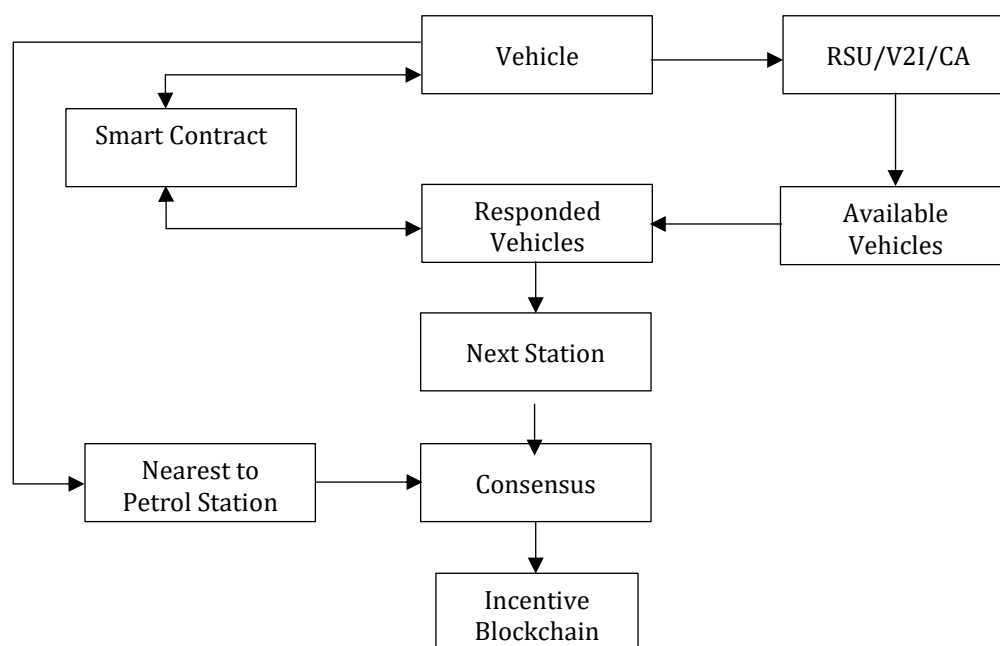


Figure 3: Proposed model of blockchain based service sharing in ITS.

RESULTS

In this section, the proposed system is scrutinized to ensure that message integrity, message confidentiality, vehicle anonymity, and route plan secrecy are all met. Authentication, TPD pre computation, and CA computation all play a role in determining the overall performance. Analysis and discussion of the results are the focus of this section. This section describes the results of the experiments for the DM prediction.

Blockchain Based Services Sharing via RSU

One RSU and numerous vehicles are assumed in this paper as part of a proposed model. There are requests from various cars, as well as communication between vehicles and RSU. Results are given in Fig. 4.

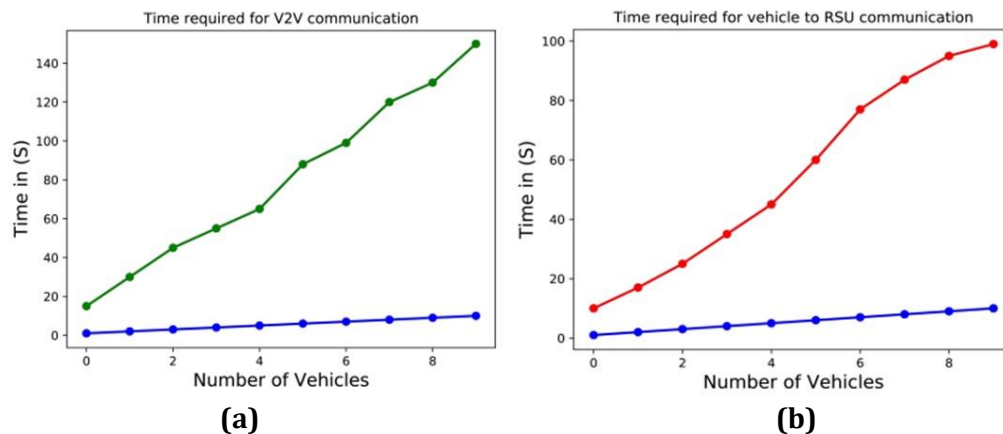


Figure 4: Results for time delay, (a) Vehicle to vehicle communication, and (b) Vehicle to RSU communication.

Both have the same initial latency, but it steadily increases. However, the delay between vehicles is increasing more quickly than the delay between vehicles and RSUs. Time delays rise as the quantity of requests increases. In addition, as the number of vehicles increases, the network grows. There is a rise in demand for automobiles as the number of networks grows large. There has been a gradual increase in the time it takes for vehicles to communicate with each other. Increases in traffic volume will inevitably result in longer delays. A single request will result in less delay if it is made by a single vehicle. Vehicles are experiencing delays due to the fact that they are receiving several requests at the same time

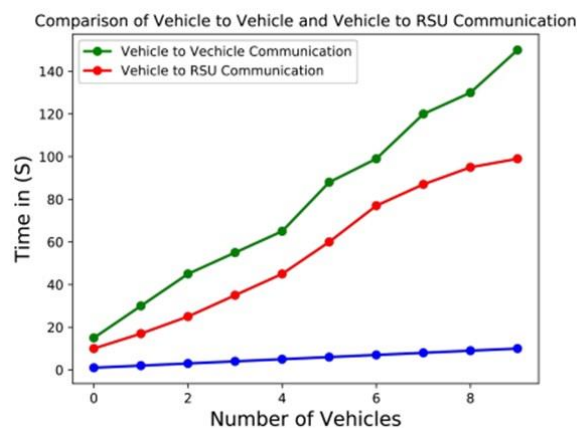


Figure 5: Comparison between Vehicle to Vehicle and Vehicle to RSU.

In Fig. 5, we examine the time delays for both communications. It takes longer for vehicles to communicate with each other than it does for vehicles to communicate with RSUs. The amount of time it takes to complete a task grows gradually. V2V communication has a lower throughput than RSU. This shows that the delay rate in both communication channels is growing. However, the delay from a vehicle to an RSU is minimal.

In Fig. 6, the x-axis shows the number of blocks, while the y-axis shows the cost. As the number of blocks increases, so does the operational expense. Operational costs rise as the number of

blocks grows. Operating costs rise when contracts are signed. On the other side, when a smart contract function is called, operational costs are reduced.

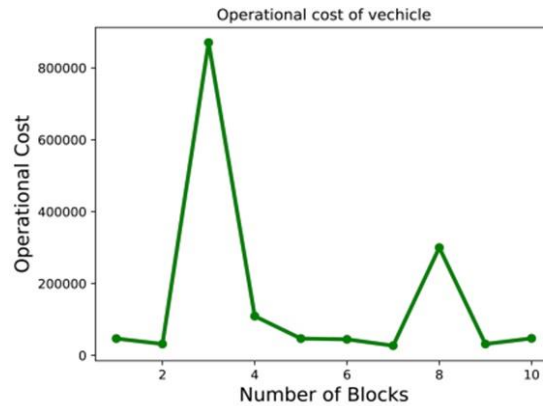


Figure 6: Operational cost.

Message Integrity

The reliability of a communication that has been sent needs to be examined. 'Message integrity' states that there should be no tampering with or alteration to the message. Typically, a hash function is used to create a message digest by combining all the message's bytes with a secret key. This is difficult to reverse. There are several components to an information security programme, and one of them is integrity checking.

Vehicle Mobility Models

Using the freeway mobility model, we look at the spatial restriction, spatial dependence, and temporal dependence that come with driving on freeways. Another thing that is needed to capture how a car moves behind another car in the road or how a car changes lanes to pass the car ahead of it are behavior models for car following and changing lanes. The following sections provide information on these three models.

Model of Freeway Transportation:

For example, in the model described here, each vehicle is spatially constrained to a single lane of the freeway, and its speed is time dependent on its previous velocity. In the same way, if two vehicles are traveling in the same lane within a safety distance (D_s), then a car following it, is spatially dependent on that car ahead of it, which we call the leading vehicle. The speed of the vehicle following must not be greater than the speed of the vehicle leading. As a result, for a vehicle I the intra vehicle relationship is

$$new_{speed} = current_{speed} + random() * acceleration \quad (1)$$

where $random()$ returns a value uniformly distributed in range of $[-1, 1]$ and equally probable vehicle deceleration or acceleration. Additionally, if vehicle j is ahead of vehicle I in its lane and inter vehicle distance D_s , then speed i speed j is the resulting inter vehicle relationship.

Vehicle Model:

This model calculates the following vehicle's speed based on the safety gap between it and the leading vehicle. We will slow down to the speed required to maintain the safety distance D_s with the leading vehicle when it is directly in front of another vehicle in a lane.

Lane Change Model:

After waiting a certain amount of time and if room is available in an adjacent lane (i.e., no other vehicle is within the safety distance D_s of the new position in the chosen adjacent lane), the following vehicle can change lanes and pass the leading vehicle in this model.

Simulation Parameters

The above models must be put into action under the simulation conditions outlined in the following section. These simulation conditions are summarized in Tab. 1.

Table 1: Simulation parameters used in this study.

Parameters	Value
Safety distance (D_s)	10 m
Vehicle speed S_{min}	50 miles/hour = 22.35 m/s, $S_{max} = 70$
miles/hour	31.29 m/s
Vehicle acceleration	$a_{min} = 0 \text{ m/s}^2$, $a_{max} = +(-) 5 \text{ m/s}^2$
Road Traffic Volume	vol = 3000 vehicles/hour/lane
Vehicle Arrival rate/Departure rate	0.833
Road Traffic Density	100-500 vehicles/lane
minutes	2
range	50

The simulated freeway map is shown in Fig. 7 below. Each lane on the motorway must be 5000m long, and there must be three entry ramps and three exit ramps that are used by vehicles on all four lanes. Vehicles on freeways, on the other hand, move solely in one direction. Four lanes are used because a motorway with four lanes going in one direction is a frequent sight in North America, Europe, and elsewhere. The horizontal gap between neighboring lanes should be 3 meters (10 feet) for programmatic and computational simplicity.

The average number of vehicles per motorway lane might range from [100, 500] depending on the freeway's density of vehicular traffic. The initial placements of automobiles in each lane must be spread evenly before the simulation is started. In addition, vehicles' starting speeds and acceleration must be distributed uniformly. It is assumed that freeway traffic flow is 3000 vehicles/hours per lane, thus the inter arrival and interdeparture process for each lane is kept exponential at $3000/(6060)=0.833$. To be clear, we are using actual traffic density and volume statistics.

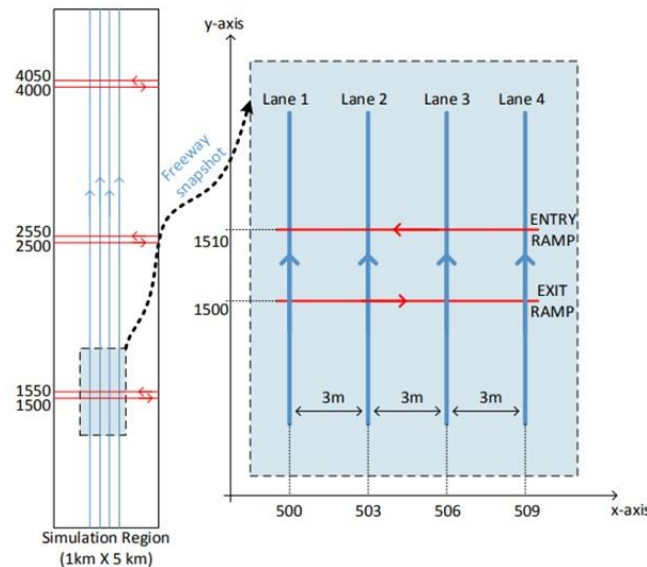


Figure 7: A simulated four lanes, five-kilometer motorway with a three meter inter lane separation and a one direction separation.

The expressions random arrival rate and random departure rate to calculate the arrival and departure rates of new vehicles (also known as nodes in the rest of the document) and current nodes per lane using exponential distribution. In the simulation, these expressions produce a random value of 0 or 1, depending on how they are applied. An entry ramp is chosen by chance only if there is no existing node on the highway; otherwise, it is chosen by chance only if there is an existing node on the motorway and an exit ramp is selected by chance alone.

Vehicle-to-Vehicle Broadcasting

V2V broadcasting of safety warnings with a transmission range of 50 meters results in the network data traffic. It is also possible to employ a non-safety application in which vehicles are required to join a group of nodes connected by V2V for a short time period (seconds or less). As a result of these network applications, the following two simulation settings have emerged: a vehicle's radio communication range is 50 meters, and the simulation iteration step must be at least 100 milliseconds.

An example of a simulator's generated visual interface for taking user input and visualizing the results is depicted in Fig. 8a, 8b, and 8c where 3 automobiles are simulated on the user's two crossing roadways, each traveling at a random speed and approaching the intersection. While moving, V2V linkages form between nodes that are within radio communication range. Some V2V linkages fail as nodes travel towards the end of the roads and are no longer in communication range.

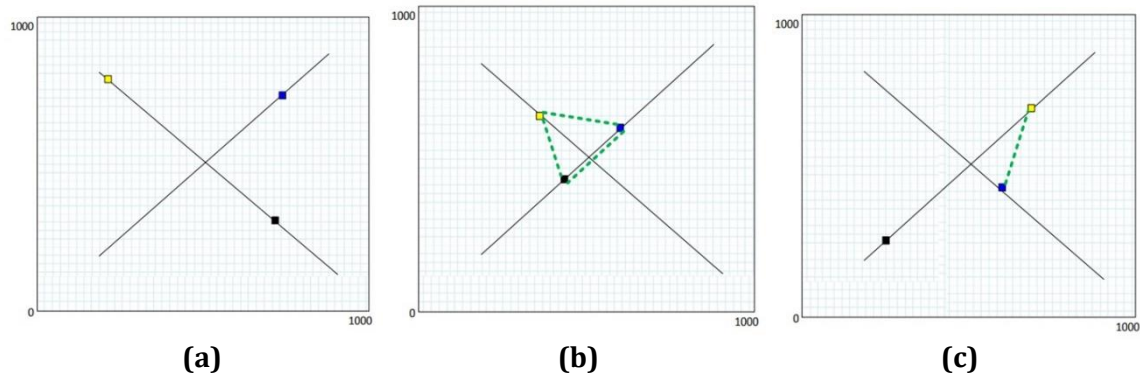


Figure 8: Simulations involving 3 vehicles, (a) Vehicles are simulated on the user's two crossing roadways, (b) All vehicles communicate with each other, and (c) Two vehicles are connected and communicate.

VANET Visualization and Assessment Tool Simulation

We build a high level simulator to see how V2V and V2I communication works on roads and freeways in this simulation. Advanced networking and wireless analysis should not be done using the simulator's output. To be innovative, the simulation tool is designed so that a user can grasp V2V and V2I communication as well as the applications and issues associated with it. There are two sections to this design: a 4 way road intersection with user provided V2V connectivity may be visualized and assessed and V2I coverage difficulties for a user provided road and RSU deployment can be visualized and assessed.

An interface is designed to visualize the V2V and V2I coverage with the following objectives. An interface should emerge upon launch that allows the user to create two intersecting roads as straight lines and displays the intersection of those two routes. Randomly two or three vehicles are chosen which are traveling in squares approaching the road intersection at a speed between [10, 20] m/s. The links are shown for V2V as they move. V2V links can be assumed to exist if two vehicles are within 100m of one another and are communicating wirelessly. Also, the graphical window is large enough to depict a 1000 m wide piece of the real world landscape. The RSU deployment should allow the user to create an uninterrupted road plan, i.e. a set of straight lines connected in this visual window, when the simulator is operating. If the user wants to place 1-3 RSUs along the route, they can draw circles around the route on the screen. See a vehicle moving from one end of the user entered road layout to the other at a random speed between [10, 20] m/s. Show the vehicle-to-RSU V2I link, including the RSU's communication range and the user placed RSUs' V2I coverage, while the vehicle is moving. V2I links are assumed to exist when a vehicle is within 100 meters of an RSU. A 1000mx1000m zone must be simulated in the viewing area, therefore plan accordingly.

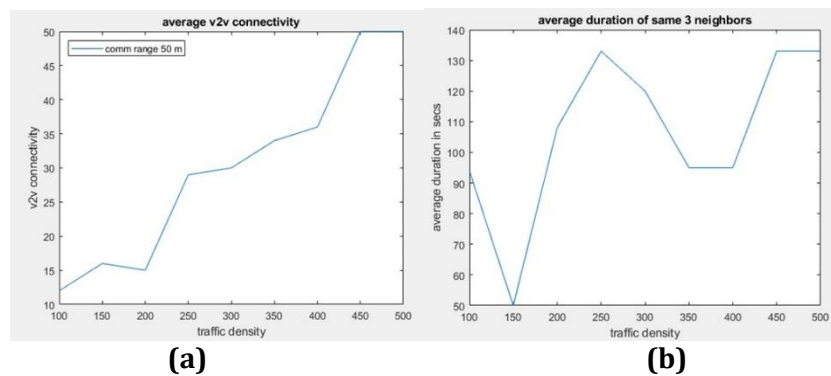


Figure 9: (a) Average V2V connectivity, and (b) Average duration of same 3 neighbors.

When developing a VANET with V2V and V2I connectivity, it's critical to keep vehicular mobility in mind. Initially, we look at how vehicle mobility and traffic volume affect V2V connectivity. The freeway mobility model, the automobile following model, the lane changing model, and the border effects are all effectively implemented in Matlab for a 4 lane scenario with three entry ramps and three exit ramps. For each traffic density, the simulations run for five trials of ten minutes each. These figures appear possible and practical based on our graphs, which show linear variation with increasing traffic density. The output changed when the communication range shifted. The charts that follow represent the results of five simulations, each of which was performed for five minutes. The communication distance is 50m and the results are shown in Fig. 9.

1. Plot shows the average number of communication nodes within 50 meters from the target.
2. Plot shows the average duration the target node maintains the same communication neighbors that are within 50 meters.
3. Plot shows the average number of same neighbors for 30 seconds

Plots at 50m and 100m are shown in Fig. 10. Two-minute simulations are run on a 50m and 100m course. The graphs show the differences when the communication range is increased to 100 meters, which is the result of five simulations for each. The graphs depict the average number of communication nodes within 50 and 100 meters of the target in red and blue, respectively. Fig. 10a shows the average duration the target node maintains the same communication neighbors that are within 50 meters (red) and 100 meters (blue). Fig. 10b shows the average number of same neighbors for 30 seconds for 50 meters (red) and 100 meters (blue) communication ranges. As traffic density rises, so does the number of neighbors, as vehicles are forced to cram themselves closer together to avoid collisions. As a result, traffic density has a linear effect on average V2V connectivity.

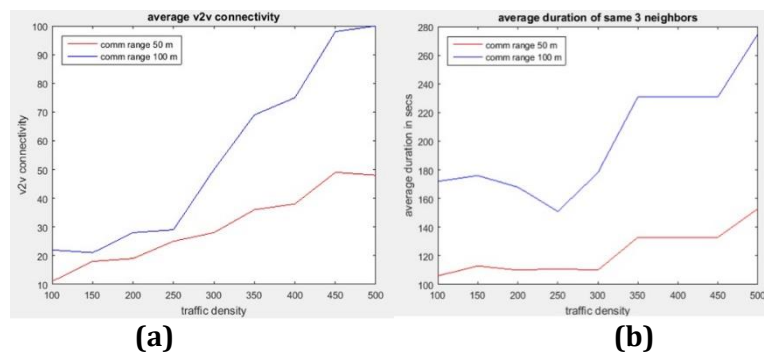


Figure 10: (a)Average V2V connectivity, and (b) Average duration of same 3 neighbors.

When uniformly deployed, each node has connectivity with 8-40 vehicles when considering 100-500 vehicles in a lane of 5km and a communication range of 50 meters. Results indicate that, as expected, the average duration of the same three neighbors grows linearly with traffic density as the same neighbors tend to stay together longer as traffic intensity increases. Increasing traffic would result in congestion and tighter control over how vehicles move around. Because of the congestion in other lanes, drivers change lanes less frequently, reducing the risk of being out of sight. As traffic congestion increases, the duration varies from 1 minute (60 seconds) to 6 minutes.

Abnormalities in the graphs do not happen at the same density every time; they happen at random. Perhaps this is the case because the random distribution of speed and distance changes every 100 millisecond, making the simulation unpredictable even when using average values. The average time of three neighbors at a specific period grows linearly with traffic density, as seen on Fig. 11. Congestion and a reduced ability to change lanes would be caused by increased traffic, as explained previously. The average number of neighbors increases from 4 to 40 in 30 seconds. Results shown in Fig. 9a to 10b show a comparison of plots from 100m and 50m. It's easy to observe that the outcomes have nearly doubled.

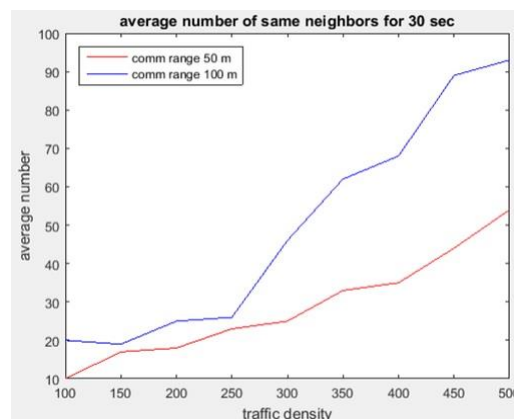


Figure 11: Average duration of the same 3 neighbors for 30 seconds.

V2V Connectivity of Approaching Vehicles at 4 Way Road Intersection Simulation 1

When the user sketches two roads that connect, three random vehicles begin to move towards the intersection at random speeds. A connection is established if the distance between the vehicles is less than 100m.

1. The connection is shown by the green dashed line.
2. Connection is established between all the three vehicles when they are close to the intersection.

V2I Coverage Simulation for a Car in a Road Map with RSU Deployment One

The user creates three roadways and sets two RSUs on each one. A connection is established if the distance between the vehicle and any RSU is less than 100 meters. Paths with no connections are shown in red, whereas paths with connections are shown in green. Figure below shows the coverage of simulation for a car with average V2V connectivity. The connection is shown by the green dashed line. Fig. 12 shows the coverage of simulation for a car with average V2I connectivity.

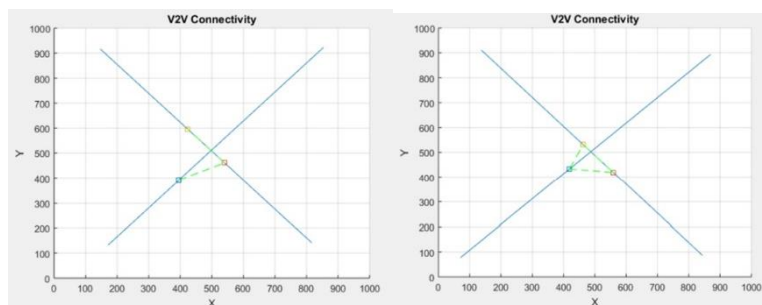


Figure 12: V2I coverage simulation for a car. Connection is established between all the three vehicles when they are close to the intersection.

V2I Coverage Simulation for a Car in a Road Map with RSU Deployment One

The user creates three roadways and sets two RSUs on each one. A connection is established (see Fig. 13) if the distance between the vehicle and any RSU is less than 100 meters. Paths with no connections are shown in red, whereas paths with connections are shown in green.

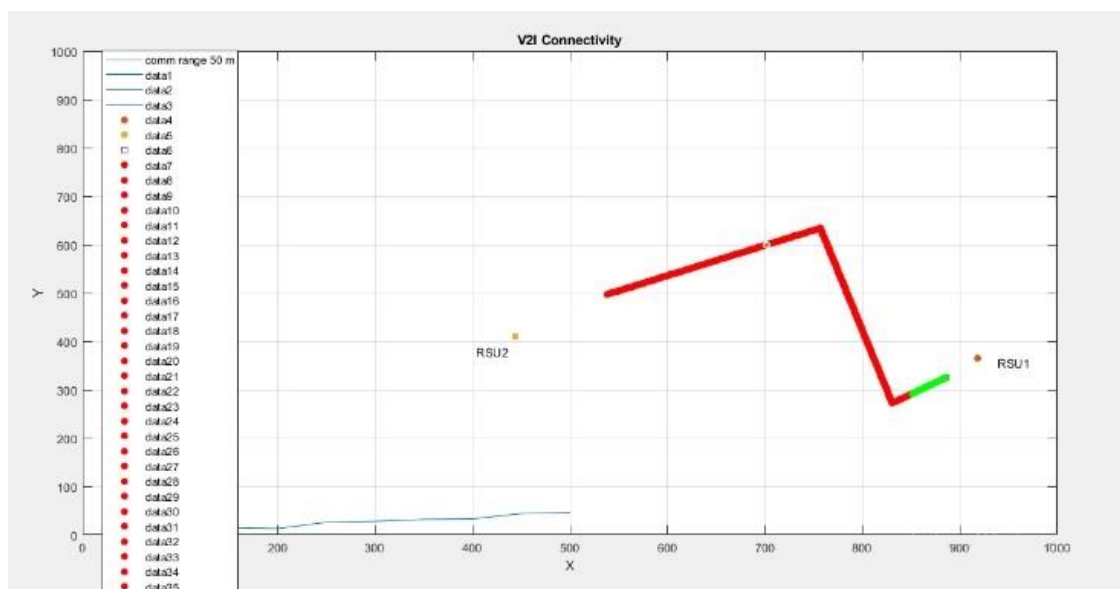


Figure 13: V2I connectivity.

DISCUSSIONS AND CONCLUSIONS

This paper proposes a privacy-preserving and lightweight intelligent vehicle-to-infrastructure (V2I) authentication system. BGN, a homomorphic encryption method based on the Moore curve, determines RSU route information before a vehicle leaves. CA converts all roadside units in a region to a vector without knowing the route plan. The vehicle's connectivity to each RSU along its journey may be quickly verified using RSU data. The proposed technique works well in MATLAB simulations of real world VANETs. The VANETs already has early warning systems for road construction, collisions, weather hazards, merging lanes, curve speed restrictions, and pedestrian crossing warnings. VANETs can give more than simply safety aid; they can also entertain drivers and passengers. VANETs can also help with parking and toll payments, as well as music, video, and software downloads via in car navigation systems with real time traffic information. When designing a V2V or V2I adhoc network, vehicular mobility should also be considered. Starting with mobility and traffic volume, this study investigates V2V connectivity. These models work well in Matlab for a four-lane scenario with three entry ramps and three departure ramps. The simulations run for five ten-minute trials per traffic density. Our graphs demonstrate linear fluctuation with increasing traffic density; thus these values appear feasible. The output widened with the communication range. Communication between vehicles and RSUs is studied in the scenario. Communication between vehicles and RSUs has an average time delay, but communication between vehicles has a high latency rate. As a result, we focused on low latency because increasing average time delay reduces throughput. RSU makes a request to the network when a car requests service. The requested vehicle responded from the available automobiles. We ran simulations to see how effectively the system works. This automobile and RSU have successfully communicated. The results of V2V communication are compared to RSU communication. When the requested car agrees to share its services with the requested vehicle, a smart contract may be made. POW was then used to mine the block and add the transaction. To be included on the blockchain, this transaction must be validated by at least 51% of nodes. In the future, researchers intend to investigate how blockchain technology might be combined with wearable technology to create a secure and reliable transportation architecture. Blockchain will be utilized to solve data sharing and trading issues among vehicles.

References

- [1] Y. Li, K. Ouyang, N. Li, R. Rahmani H. Yang et al., "A blockchain-assisted intelligent transportation system promoting data services with privacy protection," *Sensors*, vol. 20, no. 9, 2020.
- [2] X. Du, Y. Gao, C. H. Wu, R. Wang and D. Bi, "Blockchain-Based Intelligent Transportation: A Sustainable GCU Application System," *Journal of Advanced Transportation*, vol. 2020, 2020.
- [3] M. Waseem, K. A. Ahmed and M. T. Azeem, "Blockchain Based Intelligent Transport System," *Modern Innovations, Systems and Technology*, vol. 1, no. 3, pp. 70-88, 2021.
- [4] Y. Yuan and F. Y. Wang, "Towards blockchain-based intelligent transportation systems," *In Proc. Intelligent Transportation Syststems*, pp. 2663-2668, 2016.
- [5] A. Yaqoube, "Improvement of power quality by shunt active power filter in a three-phase four-wire distribution system," Ph.D. thesis, *University Teknologi Petersonas*, 2011.
- [6] F. Casino, T. K. Dasaklis and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, no. May 2018, pp. 55-81, 2019.

- [7] P. Wang, Y. Liu and S. Lv, "An improved lightweight identity authentication protocol for VANET," *Journal of Internet Technology*, vol. 20, no. 5, pp. 1491-1504, 2019.
- [8] S. O. Ogundoyin, "An autonomous lightweight conditional privacy-preserving authentication scheme with provable security for vehicular ad-hoc networks," *International Journal of Computer Applications*, vol. 42, no. 2, pp. 196-211, 2020.
- [9] C. Xu, X. Huang, M. Ma and H. Bao, "A privacy-preserving and cross-domain group authentication scheme for vehicular in LTE-A networks," *Journal of Communications*, vol. 12, no. 11, pp. 604-610, 2017, doi: 10.12720/jcm.12.11.604-610.
- [10] Yu Wang and F. Li, "Vehicular AdHoc Network," in *Proc. Guide to Wireless Adhoc Networks*, pp. 503-525, 2009.
- [11] J. Li, "Conditional Privacy-Preserving Authentication Protocols for Vehicular AdHoc Networks Dissertation," PhD thesis, *Niedersächsische Staats-und Universitätsbibliothek Göttingen*, 2019.
- [12] S. Tangade and S. S. Manvi, "Scalable and privacy-preserving authentication protocol for secure vehicular communications," in *Proc. International Conference on Advanced Networks and Telecommunication Systems*, pp. 1-6, 2016.
- [13] M. N. Aman, U. Javaid and B. Sikdar, "A Privacy-Preserving and Scalable Authentication Protocol for the Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 1123-1139, 2021.
- [14] S. Ansari, J. Ahmad, S. Aziz Shah, A. Kashif Bashir, T. Boutaleb et al., "Chaos-based privacy preserving vehicle safety protocol for 5G Connected Autonomous Vehicle networks," *Transactions on Emerging Telecommunication Technologies*, vol. 31, no. 5, pp. 1-16, 2020.
- [15] T. M. Mohamed, I. Z. Ahmed and R. A. Sadek, "Efficient VANET safety message delivery and authenticity with privacy preservation," *PeerJ Computer Science*, vol. 7, pp. 1-21, 2021.
- [16] S. A. A. Hakeem and H. Kim, "Multi-zone authentication and privacy-preserving protocol (mapp) based on the bilinear pairing cryptography for 5g-v2x," *Sensors*, vol. 2, no. 12, pp. 665, 2021.
- [17] H. H. Nie, Y. P. Li and Q. H. Wu, "A privacy-preserving V2I authentication scheme without certificates," *Journal of Informatin Science & Engineering*, vol. 33, no. 4, pp. 1025-1040, 2017.
- [18] Y. Zhou, S. Liu, M. Xiao, S. Deng and X. Wang, "An Efficient V2I Authentication Scheme for VANETs," *Mobile Information Systems*, vol. 2018, 2018.
- [19] Y. Liu, W. Guo, Q. Zhong and G. Yao, "LVAP: Lightweight V2I authentication protocol using group communication in VANETs," *International Journal of Communication Systems*, vol. 30, no. 16, pp. 1-11, 2017.
- [20] L. F. A. Roman, P. R. L. Gondim and J. Lloret, "A lightweight authentication protocol for V2G networks in smart grid," in *Proc. International Joint Conference on Pervasive and Embedded Computing and Communication Systems*, pp. 67-74, 2018.
- [21] J. Wang, B. Wei, J. Zhang, X. Yu and P. K. Sharma, "An optimized transaction verification method for trustworthy blockchain-enabled IIoT," *Ad Hoc Networks*, vol. 119, p.102526, 2021.
- [22] J. Wang, W. Chen, L. Wang, R. S. Sherratt, O. Alfarraj et al., "Data secure storage mechanism of sensor networks based on blockchain," *Computers Materials & Continua*, vol. 65, no. 3, pp. 2365-2384, 2020.
- [23] J. Wang, W. Chen, Y. Ren, O. Alfarraj and L. Wang, "Blockchain based data storage mechanism in cyber

- physical system,” *Journal of Internet Technology*, vol. 21, no. 6, pp. 1681–1689, 2020.
- [24] J. Y. Zhang, S. Q. Zhong, T. Wang, H. C. Chao and J. Wang, “Blockchain-based systems and applications: A survey,” *Journal of Internet Technology*, vol. 21, no. 1, pp. 1–14, 2020.
- [25] J. Zhang, S. Zhong, J. Wang, X. Yu and O. Alfarraj, “A storage optimization scheme for blockchain transaction databases,” *Computer Systems Science and Engineering*, vol. 36, no. 3, pp. 521–535, 2021.
- [26] Z. Xu, W. Liang, K. C. Li, J. Xu and H. Jin, “A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles,” *Journal of Parallel and Distributed Computing*, vol. 149, pp. 29–39, 2021.
- [27] B. Yin and X. T. Wei, “Communication-efficient data aggregation tree construction for complex queries in IoT applications,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3352–3363, 2018.
- [28] S. M. He, K. Xie, K. X. Xie, C. Xu and J. Wang, “Interference-aware multisource transmission in multiradio and multichannel wireless network,” *IEEE Systems Journal*, vol. 13, no. 3, pp. 2507–2518, 2019.
- [29] Y. S. Luo, K. Yang, Q. Tang, J. Zhang and B. Xiong, “A multi-criteria network-aware service composition algorithm in wireless environments,” *Computer Communications*, vol. 35, no. 15, pp. 1882–1892, 2012.
- [30] Z. F. Liao, J. B. Liang and C. C. Feng, “Mobile relay deployment in multihop relay networks,” *Computer Communications*, vol. 112, no. 1, pp. 14–21, 2017.
- [31] B. Yin and J. Lu, “A cost-efficient framework for crowdsourced data collection in vehicular networks,” *IEEE Internet of Things Journal*, vol. 8, no. 17, pp. 13567–13581, 2021.
- [32] D. Cao, B. Zheng, B. Ji, Z. Lei and C. Feng, “A robust distance-based relay selection for message dissemination in vehicular network,” *Wireless Networks*, vol. 26, no. 3, pp. 1755–1771, 2020.
- [33] Z. Xu, W. Liang, K.C. Li, J. Xu and H. Jin, “A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles,” *Journal of Parallel and Distributed Computing*, vol. 149, pp. 29–39, 2021.
- [34] Z. Xu, X. Li, J. Xu, W. Liang and K. K. R. Choo, “A secure and computationally efficient authentication and key agreement scheme for Internet of Vehicles,” *Computers & Electrical Engineering*, vol. 95, p.107409, 2021.