International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/218518 Volume 10, Issue 1, January – February (2023)

RESEARCH ARTICLE

Towards Blockchain-Based Secure IoT Communication for 5G Enabled Intelligent Transportation System

Sakthi Kumaresh
Department of Information Technology, M.O.P. Vaishnav College for Women, Chennai, Tamil Nadu, India.
sakthi.kma@gmail.com

Received: 17 January 2023 / Revised: 15 February 2023 / Accepted: 18 February 2023 / Published: 26 February 2023

Abstract – Intelligent Transportation System (ITS) with the internet of things (IoT) plays an integral role in smart city developments and enables substantial developments in modern human lifestyles. With the emergence of Fifth-Generation (5G) communication technologies, high-speed communications are enabled among multiple internet-connected devices. However, security, reliability, and scalability are significant factors that affect the communication performance of ITS. The conventional security models are mostly centralized and unsuitable for distributed low-powered IoT-enabled 5G ITS. The new-age distributed ledger technology blockchain can improve the security and reliability of ITS services. Therefore, this paper investigates a blockchain-based security mechanism, Blockchain-based Secure IoT Communication (BSIC), that protects the 5G-ITS from potential security threats. The BSIC utilizes a consortium blockchain model with Improved Proof of Reputation (IPoR) to achieve its objectives. It handles the resource limitation issues of IoT by integrating Vehicular Edge Computing (VEC) services. Further, the BSIC design includes two main components: reputation computation strategy and the IPoR mining process. The proposed model successfully builds a secure IoT communication system by integrating multi-criteria factors in subjective logic-based reputation estimation. It selects the miners by adjusting the consensus pool size according to network density and reputation and improves the consensus efficiency with minimum delay. Moreover, the experimental evaluations are carried out to analyze the efficiency of BSIC using performance metrics such as attack detection rate, consensus delay, and reputation estimation accuracy.

Index Terms – Intelligent Transportation System (ITS), Internet of Things (IoT), 5G Communication, Blockchain Security, Improved Proof of Reputation (IPoR), Optimized Consensus Pool Selection.

1. INTRODUCTION

Intelligent transportation plays a prominent role in developing human living standards and accessing fundamental services [1]. Rapid urbanization with better employment has recently escalated the usage of smart vehicles, increasing the challenges of Intelligent Transportation Systems (ITS). Constructing effective intelligent transportation is no longer a vision but a reality. Smart ITS endeavors to improve driving quality and safety levels by effectively solving driving hazards with the assistance of the Internet of Things (IoT) and modern communication technologies such as 4G and 5G [2] [3]. Smart ITS services depend on observed data streams of various vehicles, and it is crucial to develop a secure connected environment among the vehicles to accomplish the desired ITS application. Principally, the IoT is a promising technology to combine the data of intelligent sensor devices, actuators, moving vehicles, and various machines [4].

Thus, it seamlessly connects heterogeneous sensing devices through 4G/5G without human intervention and establishes a well-connected environment to accomplish desired operations in ITS. Therefore, the digital technologies adopting 4G/5G, cloud computing, edge computing, and cybersecurity are crucial elements and ubiquitous terms in IoT-based ITS applications.

The blockchain is a digital immutable ledger technology that constructs block sequences for each transaction and time-stamped information [5]. The blocks are tamper-resistance and immutable, and such property makes the blockchain more promising in many secure and trustworthy application environments. Based on the design, blockchain is mainly classified under three categories: public, private, and consortium [6] [7]. The private and consortium blockchains receive high attention than public blockchains, as anyone easily accesses the public blockchain. The blockchain employs various consensus protocols to block construction; hence, it is imperative to develop an adaptive consensus protocol with a suitable blockchain model to accomplish better secure communication in ITS environments. Moreover, the blockchain and IoT are promising technologies to effectively address the security and communication issues of the 5G-connected ITS environment.

The primary purpose of this work is to design fair, efficient, secure, and intelligent transportation by integrating the IoT and adaptive blockchain technology.

RESEARCH ARTICLE

1.1. Main Contributions

The main Contributions of the proposed Model are as follows.

- The blockchain is a new-age technology that can mitigate various security risks over IoT. The main intention of the proposed model is to design an efficient blockchain-based security model for IoT-enabled 5G intelligent transportation systems.
- The security model enables the nodes to recognize and communicate with each other through blockchain and also gives communication responses. Thus, it protects user privacy and considerably improves the security level of IoT communication systems.
- To efficiently minimize the establishing cost of the blockchain network, the proposed model exploits consortium blockchain and IPoRto construct secure data communication on an edge-based vehicular environment.
- The proposed model utilizes a multi-weight subjective logic-based reputation system to select the high-quality communication vehicles among the entire vehicles and improves the communication performance with high security.
- Finally, the experimental evaluation analyses the efficiency of the proposed BSIC model using various metrics: attack detection rate, consensus delay, and reputation estimation accuracy.

1.2. Paper Organization

The remaining part of the paper is organized as follows. Section 2 reviews the literature related to blockchain and IoT-enabled ITS. Section 3 describes the problem statement and system model of the BSIC model. Section 4 provides the proposed methodology and the mechanisms of BSIC in detail. Consequently, section 5 demonstrates the performance evaluation of BSIC with various metrics and scenarios. Finally, section 6 concludes this paper.

2. LITERATURE SURVEY

The attention towards constructing intelligent transportation has been escalating day by day. Intelligent transportation services must be distributed, autonomous, adaptive, scalable, decentralized, more efficient, and secure to maximize road users' experience [8] [9]. In intelligent transportation, truthful communication and decentralized security services are major issues.

The blooming technology blockchain with IoT promises to meet current intelligent transportation security and routing issues [10]. To study the existing research gaps, the survey is divided into two parts that are 5G for smart transportation and blockchain for ITS.

2.1. 5G for Smart Transportation

In today's world, the number of roadside vehicles is constantly increasing daily. Thus, it leads to casualties worldwide due to traffic accidents, inexperienced drivers, and the deteriorated driving environment. FundamentalITS rectifies the problems of transportation based on Information and Communication (ICT) technologies [11]. The works in [12] [13] aim to prioritize ITS applications that have the potential to enhance road safety, traffic efficiency, fuel economy, and riding comfort. In recent years, the ITS mostly comprises modern vehicles and sensor platforms that absorb information from the vehicular environment in various aspects. Further, the onboard computers process the observed information to assist with navigation, road safety, pollution control, and traffic management. However, ITS requires the most powerful onboard computers to process data rapidly. It is the main reason behind the high cost of luxury vehicles with intelligent driver assistance systems. To neglect the usage of expensive equipment for internet-based data collection and to avoid the burden issues of cloud platforms, the traffic management centers exploit IoT, which can contribute to gathering additional information, complementing the information already absorbed by onboard devices of vehicles. Thus, it makes as easy to test future 5G capabilities. In IoT smart city applications, the vehicles can share information with other vehicles, roadside infrastructures, and pedestrians through the internet [14]. Autonomous driving can benefit from intelligent vehicular communication and rapidly react to maneuvers and collision prevention [15]. It is expected that autonomous vehicles with teleoperation mode can control the vehicle moving using an external operator. This kind of mode is very useful during the failure of the automation mode of intelligent vehicles that necessitates human assistance to recover from the unsafe scenario. Since the external operator remotely performs the driving task and increases driver safety in hazardous environments [16]. The ITS also incorporates a wide range of road users like pedestrians, cyclists, and powered two-wheelers. The research works [17] tackle vulnerable roadside user safety, mainly focusing on determining the pedestrians and avoiding accidents based on vehicular cloud computing. Finally, autonomous vehicles will exploit digital maps with geo-positioning systems to enable navigation guidance to the drivers. Thus, it maximizes driving efficiency by selecting the most suitable routes regarding online traffic information. This information is generally obtained from information gathered by the vehicles in the vicinity, road infrastructure, or traffic management center. More useful data will be collected with the 5G using the IoT and big data, allowing for more value-added services and complementing navigation [18]. A driver will receive notifications with personalized information about interest points like tourist attractions, restaurants, parking places, and gas stations.

RESEARCH ARTICLE

2.2. Blockchain and IoT for ITS

The work in [19] proposes a consortium blockchain-based traffic signal control strategy that can efficiently protect different materials and financial resources. It can minimize human interventions in managing traffic signals and overcome centralization problems. Such work is a step towards building an effective ITS for vehicular networks. It can aptly handle and control traffic signals. If any congestion occurs, the vehicles forward the road condition information to the traffic department to optimally manage and update the traffic signal duration. It can control the status of the vehicles through a smart contract. Furthermore, it exploits an encryption algorithm named El-Gamalto to ensure data privacy and confidentiality. However, the simulation results demonstrate that it cannot handle massive traffic volume in urban vehicular scenarios. The complex vehicular structure also increases the security demands in the conventional centralized traffic management system. However, several security attacks like ghost cars and Sybil are serious threats to the security of legacy intelligent signal control models.

To overcome the issues of existing signal control strategies, the work in [20]introduces a blockchain-based distributed intelligent traffic light control system. It can control traditional traffic light systems and maximize security with distributed blockchain ledger technology. It also runs smart contracts by introducing edge intelligence and minimizes the data transmission rate of distributed ledger technology to an extent. The work in [21] incorporates a consortium blockchain-based platform to securely share the data and enable customized network services. It guarantees security by exploiting the ciphertext policy-based data re-encryption model and securely shares the information. It provides a trustworthy and secure environment for vehicular communication. Service organizations such as traffic police, insurance, and maintenance companies can obtain the corresponding ciphertext using specific authentication and decrypt it. Finally, it applies smart contracts to enable customized services to the vehicular onboard units.

The work in [22] introduces a smart parking system that intends to provide customers with one-stop parking services information in a smart city. To accomplish this intention, the smart parking system brings a lot of parking providers to one unified platform in a smart city environment. There are some concerns related to trust, performance, and security; to make this kind of parking system, a massive amount of vehicular information is shared among multiple entities. Hence, security is a major concern in building a smart parking system. To efficiently handle challenges like security, privacy, and trust, the work in [23] integrates blockchain technology to construct an integrated smart parking system. In [24], the security threats using data sharing are prevented by introducing a blockchain-based outlier detection model for ITS. It employs the advantages of machine learning strategies with a blockchain model to determine the data anomalies. It benefits different ITS applications such as criminal activity detection, accident prevention, user profile maintenance, reporting, controlling traffic lights, and monitoring. Another similar work in [25] rectifies the data security and privacy problems through blockchain ITS and encourages the vehicles to share their observed information with ITS systems. Blockchain technology is a promising platform to provide secure and trustworthy transactions and communications in the ITS system. It also can able to work with fundamental ITS and infrastructure. The smart contract design of the blockchain ITS system is more scalable and pliable enough to introduce novel ITS services anytime. The work in [26] introduces a blockchain-enabled reputation model in which only validated users can access the traffic data from the ITS system. It implements a routing algorithm and a blockchain network to effectively guide the validated cars on free routes even though malicious data was stored in the blockchain network. Moreover, the reputation model determines the malicious information and gives precise route information to the vehicles. However, blockchain technology is usually not well-suited for resource-constrained IoT devices.

3. PROBLEM STATEMENT AND SYSTEM MODEL

Intelligent transportation has to enable sustainable driving behaviors through secure and efficient communication. Although blockchain technology has clear benefits and novel opportunities to maximize ITS efficiency, researchers face several challenges in implementing the blockchain widely among various ITS applications. Additionally, it is impossible to replace the existing ITS using blockchain completely. Hence, partially replacing the fundamental ITS with blockchain and IoT is essential. It incurs different time and cost challenges in the network. Thirdly, the open environment and device heterogeneity pose different attacks; hence, securing the ITS with an adaptive blockchain model is crucial. No effective consensus algorithms are highly suitable for ITS, and it is imperative to select the consensus with minimum cost and time complexity. This work aims to integrate consortium blockchain to address the security and communication issues of the 5G enabled IoT based ITS environment.

3.1. System Architecture

The BSIC constructs the ITS using intelligent vehicles equipped with onboard sensors and smart communication technologies, a base station, a 5G cellular network, VEC devices, and a cloud server. In the proposed model, different types of communications are enabled that are vehicle to vehicle (V2V), Vehicle to Base Station (V2B), Vehicle to Pedestrian (V2P), Vehicle to Network (V2N), and Vehicle to Everything (V2X). In each communication, the data is transferred in the form of messages. The messages are

RESEARCH ARTICLE

categorized into two major types that are emergency and non-emergency. The messages carry the event or security-related data like reputation in BSIC. As presented in figure 1, the proposed IoT-based 5G intelligent transportation comprises three layers: IoT-enabled vehicular layer, edge layer, and cloud Layer.

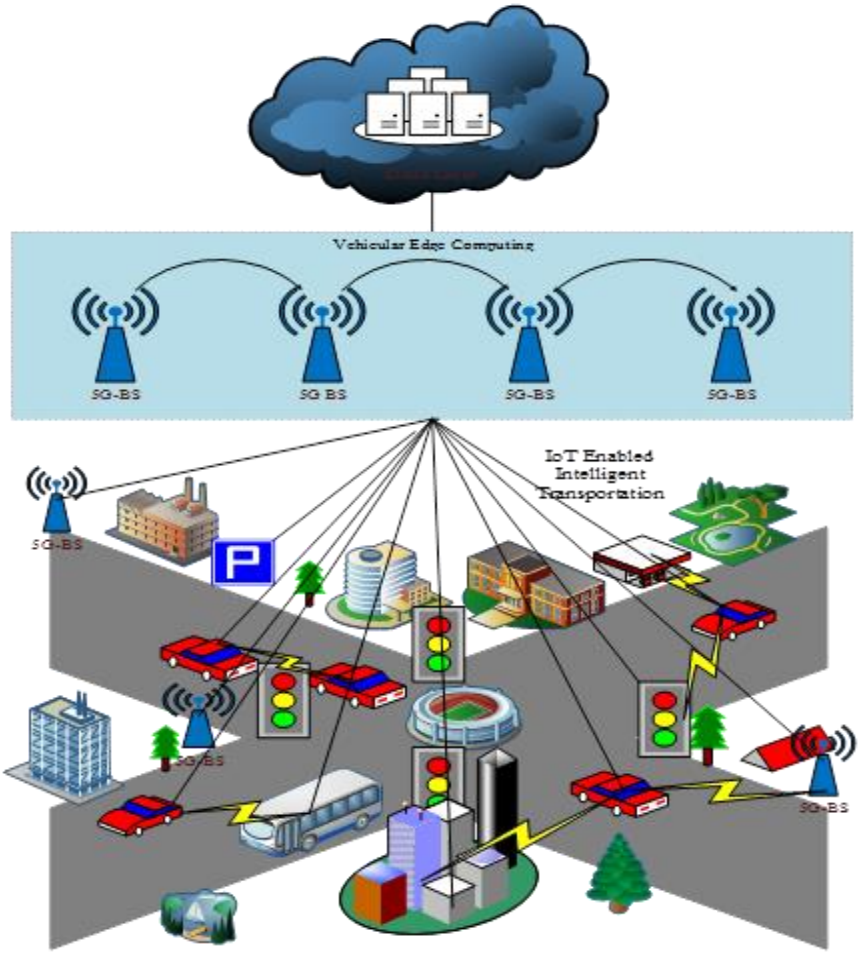

Figure 1 IoT Enabled 5G Intelligent Transportation

3.1.1. IoT Enabled Vehicular Layer

This layer comprises intelligent vehicles, buses, traffic lights, smart buildings, pedestrians, parking areas, petrol stations, and 5G base stations. Vehicular-to-Everything (V2X) communications are mainly enabled in IoT-enabled intelligent transportation. The vehicles comprise various sensors, onboard units, and communication technologies to enable V2X communication.

3.1.2. Edge Layer

It consists of 5G base stations coupled with VEC. The 5G BS receives and has adequate high-speed spectrums to connect the IoT-enabled vehicular layer and cloud. The 5G BSs transmit intelligent transportation information to the cloud to enable various services like security and communication.

3.1.3. Cloud Layer

It stores, analyses, and accesses the data related to intelligent transportation services. The devices in intelligent transportation can access the information stored in cloud services anywhere, anytime.

3.2. Attack Model

Due to the nature of the open wireless medium and high vehicle mobility, it is vulnerable to newcomer attacks, on-off, man-in-the-middle, and ballot stuffing.

3.2.1. New Comer Attack

In this type, the malicious entities erase their bad historical interactions through new identity registration. The malicious nodes create fake identities and send new registration request

RESEARCH ARTICLE

messages to the vehicle registration center and try to prove it as genuine behavior. In this way, it launches the attack again and again in the network. The proposed model integrated a blockchain-based reputation system in which it is very hard to obtain new identities from malicious nodes.

3.2.2. On-off Attack

With aiming to confuse the attack detection model, the on-off attacker behaves as benign in some time intervals and as malicious in some time intervals. That means the on-off attacker gives true reputation opinions to others in some intervals and provides false reputations to others in some intervals. Thus, the alternative performance of well and poor attackers neglects to be detected. The proposed model integrates an adaptive forgetting factor with smart contracts to strengthen the bad behavior histories of on-off attackers.

3.2.3. Man-in-the-Middle

In this type, the attacker launches attacks by modifying, forging, tampering, delaying, and dropping the sensitive messages of the vehicular system. It is very dangerous in IoT-based vehicular systems. The man-in-the-middle attacker can compromise the network entities and obtain their reputation values to launch their attack behaviors. The proposed system exploits efficient smart contracts and consensus to detect such attack behavior.

3.2.4. Ballot Stuffing Attack

In this type, the malicious vehicles give a good reputation to the other malicious vehicles and improve their reputation by launching the attacks with a group of vehicles. In such a situation, most of the received reputation packets are untrue, making it very difficult to determine the attacker. The group of malicious vehicles increases their benefits by participating in the consensus process. Reputation maintenance using the consortium blockchain model reduces the impact of such attacks in the proposed system.

4. PROPOSED METHODOLOGY

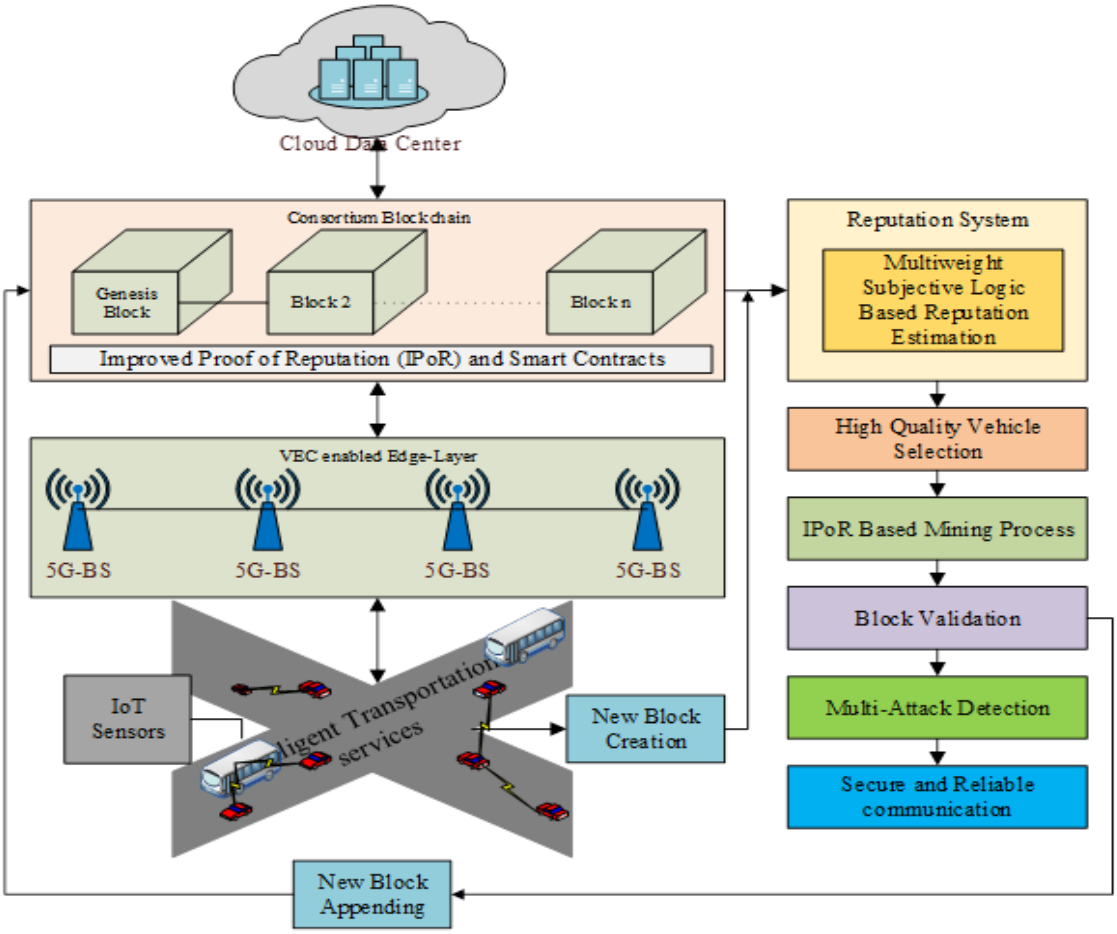

Figure 2 Designing Process of the Proposed System

RESEARCH ARTICLE

The drastically generating heterogeneous IoT data in a smart vehicular environment enriches vehicular services through intelligent transportation. However, a secure and reliable communication model is highly challenging in such environment due to dynamic environment changes and massive heterogeneous data generation at vehicle sensors. To achieve a reliable and secure communication model among intelligent vehicles, the proposed model integrates the advantages of consortium blockchain in vehicular communication. The blockchain model stores the transactions using immutable ledgers and allows high-quality vehicles with more accurate onboard data to the mining process, resulting in optimized block generation. Further, it instructs the vehicles to recognize the communicating parties through blockchain and improves the security of the vehicular environment. To select the enriched vehicles for mining, the proposed model employs a reputation system in which multi-weight-based subjective logic is used to estimate the rewards of vehicles during communication. Moreover, the proposed model increases the efficiency of ITS through IoT data collection and blockchain-based communication. Figure 2 shows the design process of the proposed BSIC model. The proposed model includes five main steps: block generation, reputation estimation model, IPoR mining process, block validation, and block appending.

4.1. Block Generation

Initially, the vehicles joined the network by registering their identities with an ITS-trusted authority. After validating their identity, the authority center provides public and private key pairs, pseudonyms, and digital certificates to the corresponding vehicle. The ITS entities are the blockchain members in the proposed system. The information like public and private key pairs, pseudonyms, and digital certificates for each vehicle is stored in the form of immutable ledger blocks with particular hash values. Whenever an ITS entity arrives at a coverage of a 5G base station, it sends its identification information to the BS for validation. After validation, the vehicle can access ITS service information and is also eligible to generate new blocks. Each entity observes different driving experiences and records information such as road traffic status, roadside incidents, travel time of corresponding routes, and improper behavior of other entities as blocks to sharing the service information with other entities in ITS. If a vehicle observes any event in the network, it needs to generate a block generation request and initiates the reputation estimation process to perform mining for block validation.

4.2. Reputation Estimation Model

The proposed model estimates the reputation value of the vehicles based on three reputation factors: local reputation estimated according to the interactions through the vehicle-to-everything communication, opinion-based reputation, and global reputation estimated based on the historical behavior data stored in the blockchain structure.

The proposed model calculates the reputation of a targeted vehicle V (R_V)using the following equation (1).

$$R_V = \frac{(W_L * R_L(V)) + W_G(R_G(V))}{W_L + W_G} \ldots\ldots\ldots (1)$$

In equation (1), the terms $R_L(V)$ and $R_G(V)$ refer to vehicle V's local and global reputation values calculated based on local interactions and blockchain ledger information, respectively. The terms $W_L$and W_G are the weighting factors of local and global reputation values, respectively, where $W_L + W_G = 1$. Firstly, the proposed system estimates the local reputation using two pieces of information: vehicle direct interaction and opinions collected from neighboring vehicles at a t time interval. The direct interaction of vehicle local reputation values is estimated based on multi-criteria communication, vehicle to vehicle, vehicle to pedestrian, vehicle to base stations, and vehicle to IoT devices such as roadside sensors and mobile devices. The presence of more than one malicious vehicle may lead to an inaccurate local reputation in many situations. The proposed model neglects the uncertainty and malicious impacts using a subjective logic method which is a probabilistic logic method that estimates the uncertainty of local reputation estimation $R_L(V)$ of communication entities based on belief vectors. It collects subjective opinions from other entities to evaluate the truthful level of the targeted entity [27]. Also, the proposed model assigns a lower $W_L$according to subjective opinions to reduce the impact of malicious contributions in $R_L(V)$ estimation. Secondly, the proposed system estimates the global reputation value based on the historical data provided by the consortium blockchain model. However, a malicious node may intend to increase its reputation by genuinely participating in the consensus process and impacting global reputation estimation. Therefore, the proposed model integrates a reliability factor on $\rho(R_V)$ with the assistance of subjective logic to evaluate the final reputation value. The BSIC model estimates the $\rho(R_V)$ using equation (2).

$$\rho(R_V) = \rho_e(R_V).\rho_d(R_V) \quad \ldots\ldots\ldots (2)$$

In equation (2), the terms $\rho_e(R_V)$ and $\rho_d(R_V)$ denote the expected and deviated reliability values on R_V respectively. The term $\rho(R_V)$belongs to 0 to 1. If the term$\rho(R_V)$ is 1, then the term $\rho(R_V)$ is reliable, and no malicious behaviors contribute to reputation estimation. Otherwise, the term $\rho(R_V)$ is 0, and the proposed model gives a low reputation to the targeted vehicle and neglects its performance in the consensus process.

4.3. IPoR Mining Process

The PoR consensus protocol includes highly reputed entities as miners during consensus [28]. Thus, the PoRcan maintain

RESEARCH ARTICLE

fair consensus in blockchain-based security systems, even the number of attackers presented in the network. However, the fundamental PoR applies random miner election in which sometimes there is no mining opportunity for highly reliable nodes. That means the malicious nodes frequently participate in mining, aiming to increase their economic benefits. Hence, it is very crucial to give consensus participation chances to the genuine nodes that have high reputation values. Therefore, the IPoRincludes the reputation values to select the miners and optimizes the fundamental PoR.The consensus process of IPoR is explained in figure 3. Initially, the IPoRestimates reliable reputation values to the node that creates a novel block. If a reputed node generates a new block, the proposed model selects highly reputed miners among the available miner nodes using PSO. Already, the reputation value $\rho(R_V)$ of any vehicle is given by the reputation system, and the IPoR exploits such value to select the highly reliable mining nodes. The integration of blockchain data in $\rho(R_V)$estimation increases the accuracy level, and thus, it also impacts the miner selection efficiency, resulting in an optimized IPoR consensus pool and high consensus efficiency.

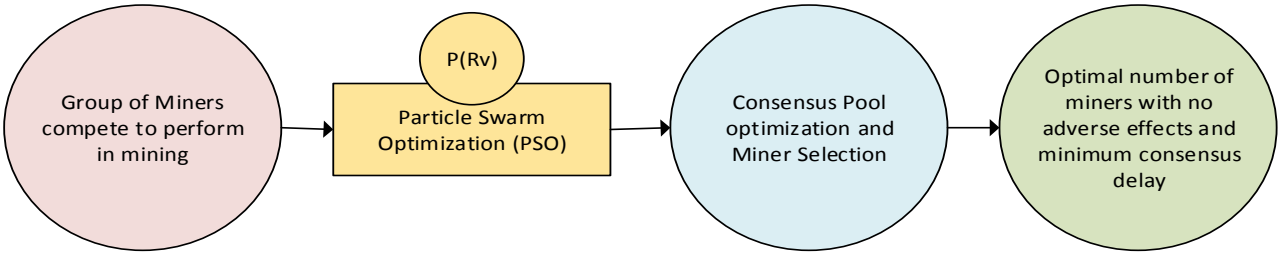

Figure 3 IPoR Consensus Process

The data communicated in the vehicle to everything comprises not only individual information like transaction information and reputation but also roadside events. Before creating emergency responses, it is essential to perform consensus verification using IPoR at the edge layer, computing the severity and status of the roadside event. The IPoR consensus protocol adaptively adjusts the next consensus group size based on the observed data communication, like emergency and non-emergency. It is very worthwhile and essential in emergency ITS services. Instead of random selections, the proposed system IPoR can encourage entities to accumulate the overall reputation of genuine behavior to compete in nominations for miners. All benign entities in the ITS are eligible to participate in miner competition, but the proposed IPoR permits the selected nodes using stochastic filtering to participate in consensus.

4.3.1. PSO for Consensus Pool Optimization and Block Validation

In this section, the consensus pool selection is optimized using the reputation values of a competed miner node and network size. The proposed model decides the number of optimal miners according to the size of the network. By reducing the consensus pool size without decreasing the performance efficiency, the IPoR effectively handles the consensus complexity and delay in the network. Also, the miner selection with reward value mitigates the effect of security threats in the mining process and boosts the accuracy of block generation. The proposed IPoR exploits the PSO on the consensus pool construction process [29].In the proposed model, The PSO is used to select the consensus pool members in which the members who compete for consensus are selected based on their reputation estimated using local iterations and blockchain data. Let us consider i number of initial miners competing to participate in consensus, and the PSO selects an optimal number of consensus nodes according to their reputations.

$$S_{cp} \alpha S_N, \quad \begin{cases} \text{if } S_N = \text{high then the } S_{cp} \geq 0.5 \\ \text{Otherwise } S_{cp} < 0.5 \end{cases} \quad \ldots\ldots(3)$$

$$S_{fcp} = \int_{\min R}^{\text{Max } R} \sum_{n=1}^{k} S_{icp} \ldots\ldots\ldots(4)$$

Equation (3) depicts the relationship between the consensus pool size (S_{cp}) and the network size (S_N). If the network compromises a huge number of devices, then the term S_{cp} is also large. Otherwise, it is reduced. Simple, the term S_{cp} is directly proportional to S_N. Consequently, the BSIC decides the final consensus pool set (S_{fcp}) using equation (4). Here, the term S_{icp} refers to the initial consensus pool set.

//IPoR Mining Process//

Input: n number of vehicles in consensus pool

Output: K number of miner selection using PSO and block validation

During IPoR the entity do{

Initiates the consensus pool selection process;

$S_{cp} \in S_{icp}$;

Estimates the S_{cp} based on the S_N using equation (3);

RESEARCH ARTICLE

Calculate the values of $\rho(R_V)$ to each vehicle inS_{icp};

Selects the high quality vehicles using PSO;

Decides S_{fcp} using equation (4);

Starts mining process;

If (consensus is achieved) {

Block is valid;

Increase the$\rho(R_V)$;

Else {

Block is invalid and there are some malicious activities;

Decrease the$\rho(R_V)$ according to malicious behavior;

}}

};

Algorithm 1 Steps of IPoR Consensus

The proposed model applies the PSO on the initial consensus pool and selects the final consensus pool based on the R-value estimated using multi-criteria data. Further, the consensus nodes are involved in the block validation process and neglect the effect of an adversary from the consensus process. The IPoR consensus pool selection is explained in algorithm 1. After consensus pool selection, the nodes in the final consensus pool are allowed to participate in consensus. The block is valid and will be appended to the blockchain network if the consensus is reached successfully. Otherwise, there is any attack behavior, and the proposed model initiates the attack detection process.

4.4. Attack Detection

Assume that each node has reputation value $\rho(R_V)$ as one during network initialization. After, the reputation $\rho(R_V)$ is reduced according to the behavior of the node in V2X communication interactions. The proposed model detects the attack behaviors by fixing the threshold for attack activities, and it is explained using equation (5).

$$V \in \begin{cases} \text{If the } \rho(R_V) \geq 0.9 \text{ and } \leq 1; \text{the node's behavior is genuine and } \rho(R_V) \text{is increased} \\ \text{If the } \rho(R_V) \geq 0.7 \text{ and } < 0.9; \textit{the node is suspicious and } \rho(R_V) \text{ is decreased} \\ \text{Otherwise, the node is purely malicious and } \rho(R_V) \text{ is reset to 0} \end{cases} \quad \ldots (5)$$

A node V should satisfy any of the conditions in equation (5). If the node behavior is genuine, the value of reputation $\rho(R_V)$ is greater than 0.9 up to 1, and the reputation $\rho(R_V)$ of the vehicle V is further increased in the corresponding round. If the value of reputation $\rho(R_V)$is greater than 0.7 and less than 0.9, then the node behavior is suspicious, and the value $\rho(R_V)$ is decreased. Otherwise, the node is purely an attacker and the value $\rho(R_V)$ is reset to zero. The node V has to behave as genuine for a long period to reach the high value$\rho(R_V)$. Likewise, the proposed model detects and terminates the attack behaviors from the network. With the assistance of blockchain, the proposed model stores and maintains the reputation in the form of immutable ledgers, contributing to succeeding block generations. Moreover, the secure block appending with IPoR in consortium blockchain maximizes the security and effectively handles the resource limitation issues of IoT-enabled 5G ITS with high security.

5. EXPERIMENTAL EVALUATION

To show the efficiency of the proposed BSIC, it is evaluated using Network Simulator 3 (NS-3). The BSIC is implemented using machine Ubuntu 18.04 LTS with the Intel i3 2.5GHZ CPU and 4 GB memory. The BSIC comprises intelligent vehicles connecting with IoT sensors and VEC-enabled 5G BSs using intelligent communication technologies. The ITS is constructed using many IoT-connected vehicles exchanging safety and non-safety messages through base stations and V2X Communication. The realistic ITS street data is extracted from OpenStreetMap and can simulate numbers of intelligent vehicles in a realistic simulation environment. The BSIC can enable secure V2X communication in intelligent ITS by integrating the multi-criteria reputation model with blockchain technology. The consortium blockchain with the IPoR consensus model is used for implementation. The proposed BSIC model kept the block size 1 Mb, and each block comprises 516 maximum numbers of transactions to prevent the block size from going beyond 1 MB. The simulation parameters are shown in table 1. For evaluation, the proposed BSIC is compared with the existing Blockchain-based Reputation (BbR) model [26], and the proposed IPoR is compared with the existing PoR algorithm [29]. Further, the results are obtained under different scenarios like node density and the number of attackers (NoA).

Table 1 Simulation Parameters of BSIC

Parameters	Values
Simulator	NS-3
Simulation Area	1Km*1Km
Number of Vehicles	100
Vehicle Communication Range	300m
Maximum vehicle speed	40 km/hr

RESEARCH ARTICLE

Maximum vehicle Acceleration	3.5 k/m^2
Number of Base Stations	10
Base Station Coverage	0.5 Km
Blockchain Model	Consortium Blockchain
Consensus Protocol	IPoR
Block Size	1MB
Maximum number of transactions of a block	516
Mobility Model	RandomWayPoint
Map	OpenStreetMap

5.1. Performance Metrics

The performance of the proposed BSIC model is estimated using the following metrics.

Attack Detection Rate: It is the ratio of successfully detected attacks to the total number of attackers.

Consensus Delay: It is the amount of time taken to reach a consensus.

Reputation Estimation Accuracy: The accuracy percentage improved due to the adoption of blockchain technology.

5.2. Simulation Results

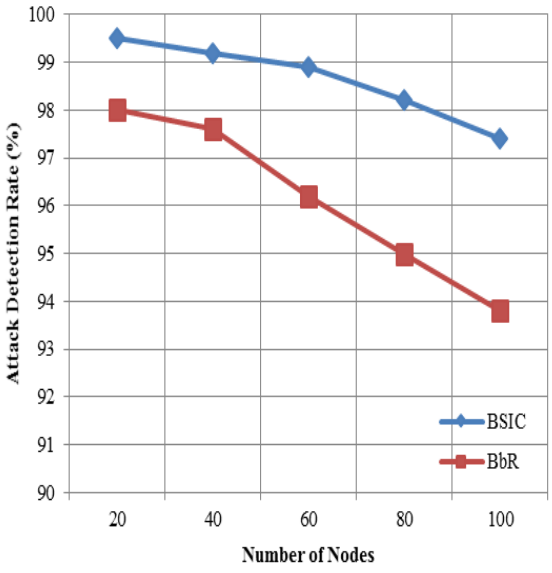

Figure 4 Number of Nodes Vs. Attack Detection Rate

Figure 4 demonstrates the attack detection rate comparison results of BSIC and BbR obtained by adjusting the number of nodes from 20 to 100. Both methods decrease the attack detection rate by increasing the number of nodes from low to high. For example, the BSIC accomplishes 99.5% and 97.4% attack detection rates for 20 and 100 nodes presented in the network. It is caused due to some reputation opinions that may sound inaccurate due to the high number of attackers present under the high-density scenario. However, the attack detection rate of BSIC is higher than the BbR system. The main reason behind this is that the proposed model includes subjective reputation estimation that collects opinions from various nodes in reputation estimation and feeds the previous reputation round as input to the next round of reputation estimation and consensus process. Thus, it effectively determines the attack behaviors and neglects the attack activities by resetting the reputation of malicious vehicles as zero in each consensus round. For instance, the proposed BSIC increases the attack detection rate by 3.6% more than the BbR when 100 nodes are present in 5G-ITS.

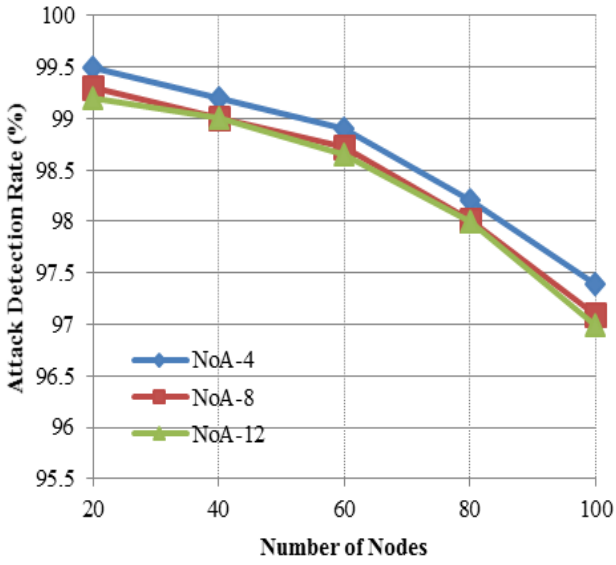

Figure 5 Number of Nodes Vs. Attack Detection Rate

Figure 5 demonstrates that the attack detection rate results of the proposed BISE were obtained for various nodes and Number of Attacks (NoA) scenarios. The attack detection rate decreases with increasing the number of nodes. The reason is that the number of communications enabled among vehicles is high under high node density scenarios, increasing the complexity of the proposed BSIC reputation model. Hence, the consensus pool size is increased, in which most nodes are attackers. The reputation results may be inaccurate in such scenarios due to node mobility and a huge number of attack present. Therefore, the proposed model decreases the attack detection rate when high numbers of nodes are presented in the network. For example, the detection rate of BSIC is 99.2%

RESEARCH ARTICLE

and 97% for 20 and 100-node density scenarios, respectively, when 12 attackers are presented in the network.

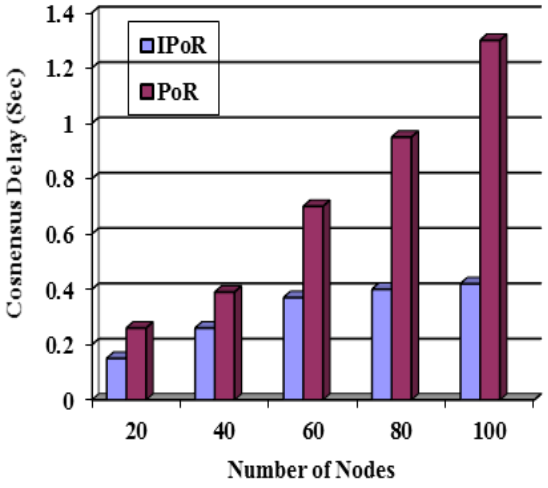

Figure 6 Number of Nodes Vs. Consensus Delay

Figure 6 depicts the consensus delay comparative results of both IPoR and PoR consensus algorithms. The results are obtained by adjusting the number of nodes from 20 to 100. IPoR and PoR escalate the consensus delay by varying the number of nodes from low to high. For example, the proposed IPoR attains 0.15 and 0.42 seconds delay for 20 and 100-node density scenarios, respectively. It is mainly due to a huge number of nodes participating in the consensus process under high-density scenarios, resulting in increased consensus delay. However, the consensus delay of IPoR is reduced when compared with fundamental PoR. The main reason is that the proposed IPoR optimizes the consensus pool size with an adequate number of miners based on the network size and reputation value. Thus, it contributes to minimizing the consensus delay with no adverse effects. Unlike IPoR, the existing PoR not adjusts the consensus pool size according to node density. For instance, the IPoR and PoR attain 0.42 and 1.3 of consensus delay, respectively, when 100 nodes are presented in the network.

Figure 7 portrays the comparative results of reputation estimation accuracy of BSIC and BbR systems. Both models decrease the reputation estimation accuracy by increasing the number of attackers from 20 to 100. The reason is that both models estimate the reputation values based on the blockchain data and local reputations. Hence, the reputation collected from others may be inaccurate under a high number of attacker scenarios in which most of the miners are attackers, and it decreases the reputation estimation accuracy. For instance, the proposed model attains 99.6% and 98.5% of reputation estimation accuracy for 4 and 20 numbers of attackers in the network. However, the BSIC accomplishes high reputation accuracy than the BbR model. Unlike BbR, the proposed BSIC adaptively increases and decreases the reputation of nodes based on the local-global reputation and consensus participation behaviors and resets the reputation of malicious nodes as one after attack detection. Hence, the attacker must behave as genuine for a long time to obtain a high reputation. By feeding the previous round reputation values as input to the next round of reputation estimation, the BSIC successfully neglects the adversary effects and improves the reputation estimation accuracy. For instance, the proposed BSIC increases the reputation estimation accuracy level by 6.5% than the BbR for 20 numbers of attackers' scenarios.

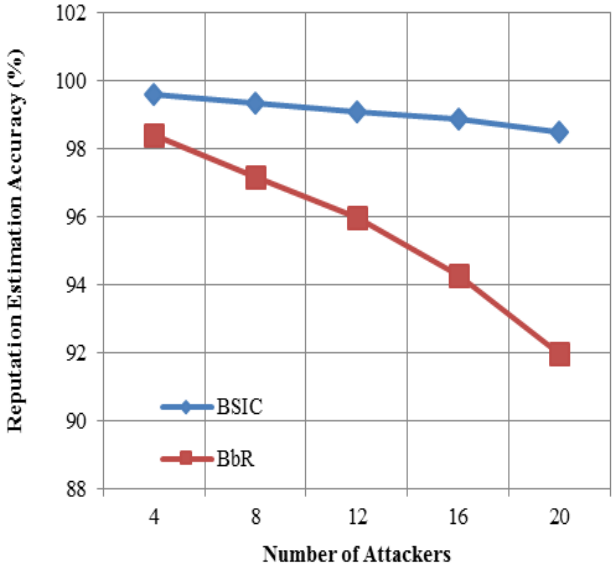

Figure 7 Number of Attackers Vs. Reputation Estimation Accuracy

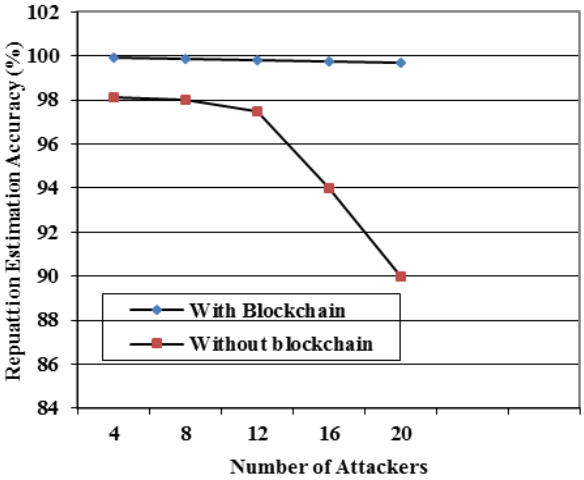

Figure 8 Number of Nodes Vs. Reputation Estimation Accuracy

RESEARCH ARTICLE

The reputation accuracy results of BSIC with and without blockchain technology are depicted in figure 8. Generally, reputation estimation accuracy decreases with increasing the number of attackers from low to high. The reason is that most of the nodes are attackers under high attack scenarios, and the attackers may provide bad reputations to the genuine nodes aiming to increase their benefits in the environment. For example, the BSIC with blockchain technology accomplishes 99.9% and 99.7% of reputation estimation accuracy, respectively, when four numbers of attackers are presented in the network. It is high when compared with BSIC without blockchain, as the immutable ledgers of the blockchain model significantly contribute to each level of reputation computation and improves the accuracy of BSIC with blockchain. Moreover, the BSIC with and without blockchain attain 99.7% and 90% of reputation estimation accuracy, respectively, when a high number of attackers 20 are presented in the network.

6. CONCLUSION

In this paper, a consortium blockchain with an IPoR-based reputation system has been designed to improve the security of IoT-enabled 5G intelligent transportation. By exploiting the VEC at the edge layer, the proposed BSIC efficiently handles the resource limitation issues of IoT-based components. Further, the reputation estimation model considers different reputation factors at the local and global levels with the subjective logic model. Thus, it increases reputation estimation accuracy considerably. Storing and maintaining the reputation values of vehicles in the blockchain system increases the security level of the proposed BSIC. Also, the consensus pool optimization of IPoR reduces the consensus delay by improving the miner selection according to network size and reputation values. From experimental evaluation, the IPoR decreases the consensus delay by 0.88 seconds more than the fundamental PoR. Moreover, the simulation results demonstrate that the proposed BSIC increases the attack detection rate and reputation estimation accuracy by 3.6 and 6.5% than the existing BbR under a high number of nodes and a high number of attackers' scenarios, respectively.

REFERENCES

[1] Gholamhosseinian, Ashkan, and Jochen Seitz, "Vehicle Classification in Intelligent Transport Systems: An Overview, Methods and Software Perspective", IEEE Open Journal of Intelligent Transportation Systems, Vol. 2, pp. 173-194, 2021

[2] Patel, Palak, ZunnunNarmawala, and AnkitThakkar, "A survey on intelligent transportation system using internet of things", Emerging Research in Computing, Information, Communication and Applications, pp. 231-240, 2019

[3] Yu, Miao, "Construction of Regional Intelligent Transportation System in Smart City Road Network via 5G Network", IEEE Transactions on Intelligent Transportation Systems, 2022

[4] Painuly, Sakshi, Sachin Sharma, and PriyaMatta, "Future trends and challenges in next generation smart application of 5G-IoT", In 2021 5th International Conference on Computing Methodologies and Communication (ICCMC)IEEE, pp. 354-357, 2021

[5] Balasubramaniam, Anandkumar, Malik Junaid Jami Gul, Varun G. Menon, and Anand Paul, "Blockchain for intelligent transport system", IETE Technical Review, Vol. 38, No. 4, pp. 438-449, 2021

[6] Bhutta, Muhammad NasirMumtaz, Amir A. Khwaja, Adnan Nadeem, Hafiz Farooq Ahmad, Muhammad Khurram Khan, Moataz A. Hanif, HoubingSong,MajedAlshamari, and Yue Cao, "A survey on blockchain technology: evolution, architecture and security", IEEE Access, Vol. 9, pp. 61048-61073, 2021

[7] Dib, Omar, Kei-Leo Brousmiche, Antoine Durand, Eric Thea, and Elyes Ben Hamida, "Consortium blockchains: Overview, applications and challenges", International Journal on Advances in Telecommunications, Vol. 11, No. 1, pp. 51-64, 2018

[8] Rudskoy, Andrey, Igor Ilin, and Andrey Prokhorov, "Digital twins in the intelligent transport systems", Transportation Research Procedia, Vol. 54, pp. 927-935, 2021

[9] Gohar, Ali, and Gianfranco Nencioni, "The role of 5G technologies in a smart city: The case for intelligent transportation system", Sustainability, Vol. 13, No. 9, pp. 1-24, 2021

[10] Jabbar, Rateb, EyaDhib, Ahmed ben Said, MoezKrichen, NooraFetais, EsmatZaidan, and KamelBarkaoui, "Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review", IEEE Access, Vol. 10, pp. 20995-21031, 2022

[11] FantinIrudaya Raj, E., &Appadurai, M, "Internet of things-based smart transportation system for smart cities", In Intelligent Systems for Social Good, pp. 39-50, 2022

[12] Kim, J.; Moon, Y.J.; Suh, I.S. "Smart Mobility Strategy in Korea on Sustainability, Safety and Efficiency Toward 2025" IEEE Intell. Transp. Syst. Mag. Vol. 7, No. 4, pp. 58–67, 2015

[13] Tokody, D.; Mezei, I.J. "Creating smart, sustainable and safe cities", In Proceedings of the IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY), pp. 141–146, 2017

[14] Velez, G.; Quartulli, M.; Martin, A.; Otaegui, O.; Aseem, H, "Machine Learning for Autonomic Network Management in a Connected Cars Scenario", In Proceedings of the International Workshop on Communication Technologies for Vehicles, pp. 111–120, 2016

[15] Marletto, G, "Who will drive the transition to self-driving? A socio-technical analysis of the future impact of automated vehicles", Technol. Forecast. Soc. Chang, Vol. 139, pp. 221–234, 2019

[16] Vulgarakis, A.; Karapantelakis, A.; Fersman, E.; Schrammar, N, "5G Teleoperated Vehicles for Future Public Transport", Available online: https://www.ericsson.com/en/blog/2017/6/5g-teleoperated-vehicles-forfuture-public-transport, 2020

[17] Scholliers, J.; van Sambeek, M.; Moerman, K, "Integration of vulnerable road users in cooperative ITS systems", European Transport Research Review, Vol. 9, No. 15, pp. 1-9, 2017

[18] Amer, H.M.; Al-Kashoash, H.; Hawes, M.; Chaqfeh, M.; Kemp, A.; Mihaylova, L,"Centralized simulated annealing for alleviating vehicular congestion in smart cities, Technol, Vol. 142, pp. 235–248, 2019

[19] X. Zhang and D. Wang, "Adaptive traffic signal control mechanism for intelligent transportation based on a consortium blockchain", IEEE Access, Vol. 7, pp. 97281–97295, 2019

[20] P. Zeng, X. Wang, H. Li, F. Jiang, and R. Doss, "A scheme of intelligent traffic light system based on distributed security architecture of blockchain technology," IEEE Access, vol. 8, pp. 33644–33657, 2020.

[21] D. Wang and X. Zhang, "Secure data sharing and customized services for intelligent transportation based on a consortium blockchain", IEEE Access, Vol. 8, pp. 56045–56059, 2020

[22] S. Ahmed, M. S. Rahman, M. S. Rahaman, and others, "A blockchain-based architecture for integrated smart parking systems", in Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 177–182, 2019

[23] M. M. Badr, W. A. Amiri, M. M. Fouda, M. M. E. A. Mahmoud, A. J. Aljohani, and W. Alasmary, "Smart parking system with privacy preservation and reputation management using blockchain", IEEE Access, Vol. 8, pp. 150823–150843, 2020

RESEARCH ARTICLE

[24] S. R. Maskey, S. Badsha, S. Sengupta, and I. Khalil, "Bits: blockchain based intelligent transportation system with outlier detection for smart city," in Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 1–6, 2020
[25] Y. Li, K. Ouyang, N. Li, R. Rahmani, H. Yang, and Y. Pei, "A blockchain-assisted intelligent transportation system promoting data services with privacy protection", Sensors, Vol. 20, No. 9, pp. 1-22, 2020
[26] L. A. Hˆır¸tan, C. Dobre, and H. Gonzalez-V ´ elez, "Blockchain-based reputation for intelligent transportation systems," Sensors, Vol. 20, 2020
[27] Müller, Johannes, Michael Gabb, and Michael Buchholz., "A subjective-logic-based reliability estimation mechanism for cooperative information with application to IV's safety", In IEEE Intelligent Vehicles Symposium (IV), pp. 1940-1946, 2019
[28] Zhuang, Qianwei, Yuan Liu, Lisi Chen, and Zhengpeng Ai, "Proof of reputation: A reputation-based consensus protocol for blockchain based systems", In Proceedings of the 2019 International Electronics Communication Conference, pp. 131-138. 2019
[29] Jameel, Marwan, and OğuzYayla, "PSO based Blockchain Committee Member Selection",In 2021 6th IEEE International Conference on Computer Science and Engineering (UBMK), pp. 725-730, 2021.

Author

Dr.Sakthi Kumaresh is a self-directed, action-oriented professional with over 22 years of teaching experience. Her aim is to encourage all students to be successful learners and works to create a classroom atmosphere that is stimulating, encouraging, and adaptive to the varied needs of students. She has completed her Ph.D. at Bharathiar University, Coimbatore, in the year 2018 and M Phil at Periyar University, Salem, in the year 2007. She is currently Associate Professor and Head of BCA Programme, Department of Information Technology, M.O.P. Vaishnav College for Women (Autonomous), Chennai, India. She has served as Examiner for Public viva-voce for Ph.D. student and also served as a panel member in the National Conference. She is the Organising Secretary of the International Conference on Computing, Communication and Information Technology ICCCMIT 2012, 2014, 2019 and the convener for ICCCMIT 2017 conducted by MOP Vaishnav College. She has publication in several international journals including IEEE, Springer and Scopus indexed journals, and presented research papers in several International and National conferences. Her areas of specialization include Programming Languages, Software Engineering, Web Programming, Software Quality Management, and Data Mining.

How to cite this article:

Sakthi Kumaresh, "Towards Blockchain-Based Secure IoT Communication for 5G Enabled Intelligent Transportation System", International Journal of Computer Networks and Applications (IJCNA), 10(1), PP: 144-155, 2023, DOI: 10.22247/ijcna/2023/218518.