Edge Server Deployment Scheme of Blockchain in IoVs

Liya Xu, Mingzhu Ge, and Weili Wu, *Senior Member, IEEE*

***Abstract*—In the Internet of Vehicles (IoVs), vehicles generate and disseminate information, which makes the related vehicular services realized. However, the IoVs is an untrusted environment. Vehicles cannot evaluate the credibility of the received information, which makes it a challenge to implement data sharing in IoVs. Blockchain, constantly directed main attention, are considered as a feasible solution to address the challenge, due to its advantages of decentralization, unforgeability, and collective maintenance. The consensus mechanism of blockchain requires the miners in the system with strong computing power for mining, while the computing power of nodes in IoVs is limited, which restricts the application of blockchain in IoVs. In fact, the application of blockchain in IoVs can be implemented by employing edge computing. The key entity of edge computing is the edge servers(ESs). Roadside nodes (RSUs) can be deployed as ESs of edge computing in IoVs. In this article, we study the ESs deployment scheme for covering more vehicle nodes in IoVs, and propose a randomized algorithm to calculate approximation solutions. Finally, we simulated the performance of the proposed scheme and compared it with other deployment schemes.**

***Index Terms*—Approximation calculation, blockchain, edge computing, edge server (ES) deployment, Internet of Vehicles (IoVs).**

I. Introduction

THE Internet of Vehicles (IoVs) takes the moving vehicles as the perceived object. Through information and communication technology, it realizes the network connection between vehicle and X (i.e., vehicle and vehicle, people, road, and service platform). Therefore, IoVs consists of vehicle nodes and include roadside nodes, passengers' smartphones, laptops, iPods, and other devices. Due to the high self-organization of nodes in IoVs, nodes can freely join and leave a IoVs. Therefore, it is an incomplete trusted network. Data sharing and interaction between vehicles and other smart devices are the key components of information transmission in IoVs. When there are malicious nodes in the network, it means that the data transmitted in IoVs is in danger of being maliciously tampered with, which will bring great losses to users. For example, a malicious node may tamper with and broadcast a message claiming that a certain road is unblocked, but in fact the road is seriously damaged. If this maliciously tampered information is released into IoVs, it will attract many vehicles to choose to drive on this road, which will cause serious traffic accidents and endanger people's lives. In addition, when passengers work in vehicles, important personal information such as personal accounts and passwords, are relayed and transmitted through these nodes in the vehicle network. Once this information is tampered with or forged, it will bring great risks to personal finance. Therefore, how to guarantee the secure and reliable data transmission is an arduous challenge to the realization of the IoVs [1] [2].

For data security, the current IoVs adopts the traditional centralized storage mechanism, that is, the service provider provides an authoritative platform, and all nodes pass the registration and are audited by the platform. If the verification is positive, the node can obtain a legal ID to join the IoVs. The transmission of data in the network is encrypted, and the data is stored in the server of the platform. However, the centralized storage mechanism has some shortcomings: the capacity cannot be flexibly expanded, and the execution efficiency is low when users have personalized needs. In addition, when the central server receives an attack, all data in the network will face problems such as being tampered with and being lost. The emergence of blockchain technology has provided us with a new idea of solving the abovementioned problems. The blockchain is essentially a distributed database. The nodes in the blockchain network are composed of distributed and decentralized nodes. All nodes participate in data management and jointly maintain a unique ledger database [3] [4]. Blockchain has the advantages of "unforgeability," "traceability," "openness and transparency," and "collective maintenance." These advantages have laid a solid "trust" foundation.

A blockchain is a chain of linearly linked blocks. The block is mainly composed of block header and block body. The header of each block contains the hash of the previous block, so that the blocks are linked one by one to form a blockchain. The block header keeps some basic information, such as version number, hash of the previous block header, the Merkle tree root hash, timestamp, computing difficulty, and random number.

Manuscript received June 26, 2021; revised September 16, 2021 and December 1, 2021; accepted January 7, 2022. Date of publication January 26, 2022; date of current version March 2, 2022. This work was supported in part by the NSF under Grant 1907472, in part by the National Science Foundation of China under Grants 62062045 and 61662039, in part by the Science and technology project of Jiangxi Provincial Department of Education under Grant GJJ211842, in part by the Jiangxi Natural Science Foundation under Grants 20202BAB202023, 20192ACBL20031, in part by the Project of Teaching Reform in Jiujiang University under Grant XJJGYB-19-47. Associate Editor: Ruizhi Gao. *(Corresponding author: Mingzhu Ge.)*

Liya Xu and Mingzhu Ge are with the School of Information Science and Technology, Jiujiang University, jiujiang 332005, China (e-mail: xuliya603@whu.edu.cn; mingzhug@whu.edu.cn).

Weili Wu is with the Department of Computer Science, University of Texas at Dallas, Richardson TX 75080 USA (e-mail: weiliwu@utdallas.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TR.2022.3142776.

Digital Object Identifier 10.1109/TR.2022.3142776

0018-9529 © 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Univ of Texas at Dallas. Downloaded on August 15,2022 at 19:55:20 UTC from IEEE Xplore. Restrictions apply.

Each node can form its own block. When a node has formed a complete block, it needs to compute the hash value that meets the requirements by modifying the nonce. The block will be broadcast to other nodes in the network until the node computes the nonce. Additionally, these nodes verify the block, and if the verification is positive, the first node who computed the nonce gets the right to add its block to the blockchain. This computing process is called mining, and the nodes are called miners. It is a competitive process among all nodes in the whole blockchain network.

A block body consists of the transactions (i.e., data). The transactions (i.e., data) in the block body are organized through a Merkle tree. If any of them is modified, it will cause a change in the root hash of the Merkle tree, which will lead to a change in the block header, at which point the nonce of the block will become illegitimate and will need to be remined. Suppose an organization with a large number of computers remines this nonce, which will cause the hash of the block header to change. The hash of the previous block is recorded in the header of the block, so that this block header also changes, additionally, the nonce of the block becomes illegitimate, then, the nonce of the block needs to be mined again. It will cause a chain reaction where any modification will cause the data to collapse and require remining, making it extremely costly to tamper with data of block. To illustrate, in Bitcoin, if six blocks are added to the back of a block, then that block can be considered to never be modified. (Unless all the miners in the world deny the previous block and start mining again). Therefore, the blockchain can prevent the data on the chain from being tampered with or forged [5]. It is very suitable for secure data delivery and storage in IoVs environment.

There are many challenges to apply blockchain to IoVs, such as the choice of blockchain miners, the design of consensus mechanism and so on. The first challenge that needs to be addressed is the choice of IoVs blockchain miners, that is, to find qualified nodes in IoVs as miners to form block and compete for mining. However, vehicle nodes and mobile smart devices of IoVs have low computing power. In addition, their fast moving speed leads to frequent changes in the network topology, making its connection with other nodes extremely unstable. Therefore, they are not qualified as miner nodes in IoVs blockchain. It seriously restricts the application of blockchain in mobile Internet such as the IoVs [6]. Since the computing power of a single mobile device, i.e., a vehicle, cannot undertake this critical assignment. Edge computing, considered to an extension of cloud computing, has seen its attention remarkably increase [7] [8]. Edge computing offers an open platform integrating network computing and network storage for the real-time nearest service [9], [10]. Moreover, through producing faster a response to network service and satisfying real-time requirements, edge computing can undertake various services such as computing power, data storage, application services, etc [11].

Therefore, it is a good solution to implement the application of blockchain by adopting edge computing in IoVs [12], [13]. In order to obtain qualified miners, we deploy RSUs as ESs and consider ESs as the miners of IoVs. The ESs perform the creation and verification of the block data. Compared with mobile nodes, the deployed ES has large computing power and stable topology, which can undertake the tasks of miners in IoVs blockchain. Blockchain miners receive data and bundle it into blocks, which need to be connected with other nodes. In addition. As miners, RSUs need to compete for mining and mutually verify relevant mining block information, etc. This mining process is that all miners in the blockchain network compete with each other. After the miners obtain the required nonce, broadcast the block to the other miner nodes of the whole network for verification. If the verification is positive, the first miner that obtain the required hash value can add its own block to the blockchain [14]. This process requires high network connectivity and low information transmission delay. ESs not only participate in mining as a miner, but also assist in the information transmission of the vehicle blockchain network. Therefore, it is critical to effectively deploy the ESs. The deployment scheme proposed in this article is to make the deployed ES satisfy the connectivity with other nodes in IoVs, and meet the requirement that the ES can be qualified as a miner IoVs blockchain.

The main contributions of this work are summarized as follows.

1) This article introduces the important role of blockchain technology in information security transmission, as well as the challenges of blockchain application in IoVs. Furthermore, we analyze the feasibility of employing edge computing to realize the application of blockchain in IoVs.
2) We consider the roadside unit as the ES, and propose a random deployment algorithm of the ES for the blockchain in IoVs to satisfy the coverage of the ES to the vehicle nodes.
3) A simulation algorithm that contains a rigorous analysis is developed for performance evaluation. In addition, we simulated our scheme and compared it with another scheme.

The rest of this article is organized as follows. Related work is briefly introduced in Section II. The randomized algorithm is presented in Section III. We develop a simulation algorithm that contains a rigorous analysis in Section IV. The performance evaluation is given in Section V.

II. Related Work

The integration of edge computing and blockchain is an inevitable way to broaden the application of blockchain in mobile Internets. The scenarios used in the existing blockchain technology do not take into account the scenarios, where the network topology changes rapidly (i.e., vehicle blockchain network). The architecture of edge computing or ES deployment scheme is one of the essential components to implement edge computing. Derived from this conception, only a bounded number of works have been exploited on the architecture for edge computing in IoT.

Zheng *et al.* [15] proposed a blockchain based distributed architecture known as MicrothingsChain. The ESs, with strong computing and storage capabilities, can implement the distributed storage of massive data. Moreover, due to the distributed storage and nontampering features of blockchain, data

Authorized licensed use limited to: Univ of Texas at Dallas. Downloaded on August 15,2022 at 19:55:20 UTC from IEEE Xplore. Restrictions apply.

security, and cross domain access of users can be guaranteed. The authors in [16] analyzed the challenges for the design of mobile blockchain edge computing architecture, as well as the differences with the traditional blockchain architecture, and then proposed an original architecture not only reducing the storage capacity requirements of IoTs devices, but also enhancing the overall performance. Likewise in [17], a secure distributed fog node architecture based on blockchain technology is designed. Fog nodes, taking as the ESs in edge computing, are deployed on the edge of the IoTs to respond to the access requirements of IoT devices in real-time, which provides low-cost and secure computing services for devices in IoTs. Yang *et al.* [18] considered blockchain as service publisher and evidence recorder by taking advantage of its the nontampering and forgery. They proposed a nonrepudiation service supply scheme in IIoT environment. Bera *et al.* [19] analyzed the challenges and problems faced by applying blockchain to UAV environment in 5 G IoT. They proposed a blockchain based security framework for data management during UAV communication. The security framework can resist several potential attacks essential in the Internet of drones environment, such as replay, impersonation, man-in-the-middle, privileged-insider, etc. In [20], the authors analyzed that the traditional centralized unilateral authentication has the security risk of authentication failure or collapse due to external attack or internal deception in the edge network and Internet of things environment. To address this challenge, the authors designed a blockchain based decentralized authentication protocol and implemented a complete blockchain based authentication platform. Gupta *et al.* [21] proposed a secure decentralized connected autonomous vehicles (CAVs) architecture based on blockchain to address security and privacy problems, such as denial of service, GPS spoofing, and replay attacks. In this architecture, the authors designed an Ethereum blockchain layer, which stores the data captured from CAVs as transactions in the chain of immutable blocks. Kaile *et al.* [22] proposed a resource trading architecture based on blockchain, which uses the trust mechanism of blockchain to eliminate dependence on third parties and solve the problems of network economy and resource allocation.

The strategy proposed in [23] exploits the security of blockchain to construct a mobile edge computing based architecture in VANETs. Composed of three layers, from bottom to top namely perception layer, edge computing layer, and service layer, the security architecture ensures the security of VANETs data during transmission. In the bottom layer, a blockchain network constituted by vehicles and RSUs ensures the security of data in VANETs, it even collects and uploads data to the upper layer. The middle one, designated as the edge computing layer, is responsible for processing and storing data, as well as providing data services to the top layer. So, as to maintain the security of cloud data, the service layer in the top, applies blockchain technology to store tamper-proof and traceable data, while adopting the cloud original storage method to store other data for ensuring security through the cloud computing architecture. Furthermore, an edge architecture named edgechain in blockchain, based on minimizing the deployment cost of mobile ESs, is proposed in [24]. The authors employed random programming scheme to study the deployment cost of ESs in order to provide users with edge computing services. In addition, in order to better provide assistance for blockchain research, Androulaki *et al.* [25] designed a Hyperledger fabric that is a blockchain system for distributed applications written in a standard general programming language. It is the first extensible open-source blockchain system that runs distributed applications and supports modular consensus protocols. Compared with the existing blockchain platform, the "smart contract" of this platform does not rely on local cryptocurrency or written in domain specific language.

Enlightened by the aforementioned thoughts, we consider the roadside units as the ESs of edge computing in mobile blockchain to improve security services for sharing critical information under the environment of IoVs. With this strategy, the deployment of ESs, in turn, is equivalent to the RSUs deployment in IoVs. On this issue, considerable scholars have made prominent contributions. Under the precondition of proving that the RSUs deployment problem is NP-hard, Peng and Qin [26] obtained an approximate optimal solution, exploiting a greedy idea and two-phase scheme to deploy the RSUs. In contrast, deploying the RSUs in intersections, A GSC algorithm in [27] is developed to choose the intersections of roads. Undoubtedly, the scheme of the RSUs placement is the selection of intersection in roads. Similar is the scheme in [28]. However, due to restrictions on the deployment location of RSUs, the occasions where these strategies are applied are also restricted.

III. Approximation Scheme

In vehicular blockchain network, miners should compete with each other for add its own block to blockchain, verify other blocks, etc., all of which require high network connectivity. However, in IoVs, fast moving vehicle nodes can lead to low connectivity of the network. Therefore, we study the deployment scheme of edge servers(ESs) and consider ESs as miners to meet the application requirements of vehicular blockchain network. On the one hand, ESs, with high computational power compared with vehicle nodes, can meet the computing power demand of miners competing for mining in blockchain; on the other hand, the network topology of ESs is stable, which can participate in the transmission of information in IoVs and improve the connectivity of the network.

This section demonstrates the deployment scheme of the ESs to address the above challenges of the vehicle blockchain network. Due to the problem of ESs placement in vehicular networks is NP-hard [26]. Therefore, we propose an approximate algorithm to deploy ESs for the vehicle blockchain network.

A. Network Model

The ESs are deployed on the side of a road. Vehicles node are distributed randomly on a road and the speed of vehicles is within the given range. There are two connection ways for each vehicle to communicate with ESs: 1) access directly to ESs; 2) access to ESs by multihop relaying. Vehicles forward information to the ES in the same direction of vehicle moving rather than the opposite direction. We assume that all vehicle nodes and ESs

Authorized licensed use limited to: Univ of Texas at Dallas. Downloaded on August 15,2022 at 19:55:20 UTC from IEEE Xplore. Restrictions apply.

have the same transmission scope m_0. It is similar to the network model in [29].

B. Problem Description

Due to the high dynamic topological structure in IoVs, the frequent breakage of links disrupts the transmission of information. The deployed ESs should be able to receive the information uploaded by vehicles and assist information transmission. For simplicity, the distance of deploying ESs is equal in this article. We need to get the optimal deploying distance of ESs, which can transmit information in IoVs with the connectivity probability p_0 within the time t_0.

Assume that a message can be transmitted to a vehicle of distance at most m_0, the speed on the road is v_0, the average number of vehicles is d_0 per kilometer. The Chernoff bound [30] will be adopted to analyze this algorithm.

Proposition 1: (see[30]). Define $X_1, \ldots, X_n$ to be independent random variables, and the value of each variable is 1 or 0. X_i takes 1 with probability p_i. Let $X = \sum_{i=1}^{n} X_i$, and $\mu = E[X]$. Then, for any $\delta > 0$

1) $\Pr(X < (1-\delta)\mu) < e^{-\frac{1}{2}\mu\delta^2}$
2) $\Pr(X > (1+\delta)\mu) < [\frac{e^{\delta}}{(1+\delta)^{(1+\delta)}}]^{\mu}$.

Proposition 2: (see[31]). Define $X_1, \ldots, X_n$ to be independent random variables, and the value of each variable is 1 or 0, and $X = \sum_{i=1}^{n} X_i$.

1) If $P_i(X_i = 1) \leq p$, then for any $\epsilon > 0$, $\Pr(X > pn + \epsilon n) < e^{-\frac{1}{3}n\epsilon^2}$.
2) If $P_i(X_i = 1) \geq p$, then for any $\epsilon > 0$, $\Pr(X < pn - \epsilon n) < e^{-\frac{1}{2}n\epsilon^2}$.

Definition 1: Assume that each ES has a unique identification number x.

1) A *connection topology* of a set of ESs is defined by a function $g : N \to N$ such that for two ESs with identification numbers x and y, they are connected if and only if $g(x) = g(y)$.
2) If all ESs are connected with wires, then they can use the function $g_c(x) = 1$ for each ES with identification x.
3) If all ESs are isolated without wire connection, then they can use the function $g_u(x) = x$ for each ES with identification x.

Definition 2: The M is a set that contains the parameter of road traffic property such as node transmission range m_0, vehicle speeds range $[v_1, v_2]$, the average number b of nodes per unit, etc.

Definition 3: Let M be a set of parameters. Parameters $d > 0, q \in [0,1], D > 0$. Let $g(.)$ be a connection topology. Define the following random events. Let $\mathrm{R}_g(d, q, M, D)$ be a random event within interval ES distance d, and has function $g(.)$ for its ES connection topology. It returns 1 if one packet can be transmitted to qn vehicles. The n indicates the number of vehicle nodes that exist in the area of distance D to the given site.

Definition 4: Let $p, q \in [0,1]$. Let n_D be the number of vehicle nodes with the distance D to the source that sends a message. Let M be a parameter set for the road. Let $g : N \to N$ be a connection topology. Let $f_g(p, q, M, D)$ be the largest distance $d_{\max}$ such that for each $d \in [0, d_{\max})$, if ESs are arranged with distance d between two consecutive ESs via connection topology $g(.)$ on a road, it guarantees that with at least probability p, at least qn_D vehicles within distance D receive the message.

Algorithm 1: Randomized Algorithm.

Input: A parameter set M (see definition 2, probability parameter p, maximum transmission range m_0, initial vehicle speed v_0, time threshold t_0, average number of vehicles density b, parameters $\gamma, \epsilon \in (0,1)$.

Output: d

```
Let d_1 = m_0, i = 1, λ_0 = 0.1, and δ = γ/3;
Select the least integer h such that (1+ε)^h m_0 ≥ 2D;
Select the least integer t such that h e^{-tδ^2/2} ≤ λ_0;
Repeat
    Let X_j = R_g(d_i, q, M, D) for j = 1, 2, ..., t;
    Compute S = Σ_{j=1}^{t} X_j;
    Let d_{i+1} = d_i(1+ε) and i = i + 1;
Until S < (p − δ)t or d_i > 2D;
d = d_{i−1};
```

C. Randomized Algorithm

In this section, we introduce a random algorithm to calculate an approximate distance for deploying edge servers. Its correctness and computational complexity are proved.

We discuss an algorithm framework that is suitable for both connected ESs via some wired network and unconnected ESs network. We propose an approximation scheme for edge servers placement and configuration in IoVs. The algorithm iteratively calculates an approximate deployment distance for ESs by approaching the optimal distance from the initial distance m_0. The m_0 is the maximum distance of node wireless transmission. If the IoVs cannot meet the conditions, then increase sequentially the distance to $m_0(1+\theta), m_0(1+\theta)^2, \ldots, m_0(1+\theta)^i, \ldots$ until the IoVs meets the conditions at distance $m_0(1+\theta)^{i+1}$, where ϵ is a precision parameter adopted to regulate the approximation to the optimal deployement distance for ESs. Then $m_0(1+\theta)^i$ is the approximate optimal deployment distance for ESs. For each distance $d_i = m_0(1+\theta)^i$, We sample the sufficient number t of random events, which exist in the area of distance D to the given site. The events that meet the condition of information transmission on the road will be counted. We make that with probability close to p, at least qn_D vehicles can receive the message (n_D indicates the number of vehicles that exist in the area of distance D to the given site), the Chernoff bound is adopted to ensure the probabilistic approximation to p. The algorithm returns a distance d in the range $[\frac{f_g(p+\gamma,q,M,D)}{1+\epsilon}, f_g(p-\gamma,q,M,D)]$ as an approximation to $f_g(p,q,M,D)$.

Definition 5: Let M be a parameter for the road, and let $g(.)$ be a connection topology. They satisfy *monotonic condition* if $f_g(p_1,q,M,D) \geq f_g(p_2,q,M,D)$ for all $0 \leq p_1 \leq p_2 \leq 1$, $D > 0$, and $q \in [0,1]$.

We have the following algorithm for variant connection topologies for ESs.

Authorized licensed use limited to: Univ of Texas at Dallas. Downloaded on August 15,2022 at 19:55:20 UTC from IEEE Xplore. Restrictions apply.

Theorem 1: Assume that M is a parameter set, and $g(.)$ indicates the ES connection topology. They satisfy the monotonic condition. Let D be the parameter that controls the range for message transmission from the accident site. Let parameters p, q be in [0,1], and γ be in $[0, p]$. Then, it exists a given probability meet the connectivity of IoVs under following condition. It gives a distance d with $\frac{f_g(p+\gamma,q,M,D)}{1+\epsilon} \leq d \leq f_g(p-\gamma,q,M,D)$ in time $O(\frac{1}{\epsilon\gamma^2}(\ln\frac{D}{m_0})(\ln\ln(\frac{D}{m_0})+\ln\frac{1}{\epsilon})\cdot T(M,n_D,\frac{2D}{m_0}))$, where n_D is the number of vehicles on the road to the first message site of distance at most D, and $T(M, n_D, h_D)$ is the time of generation and simulation of a random event $R_g(.)$ for the system of parameters M, n_D vehicles, and h_D is the number of ESs to the accident site of distance at most D. Furthermore, $T(M, n_D, h_D)$ is not decreasing for both n_D and h_D.

We note that a concrete computational time complexity for $T(M, n_D, h_D) = O(n^2 \log n)$ with $n = n_D + h_D$ will be given at section IV, where we develop a simulation algorithm.

Proof: Let parameters m_0, i, λ_0, i, $\delta = \gamma/3$, and X_j be defined as in Algorithm.1.

The number of cycles of the loop (lines 4–8 in the algorithm) is bounded by h with $(1+\epsilon)^h m_0 \geq 2D$. Thus,

$$h = \left\lceil \frac{\ln(2D/m_0)}{\ln(1+\epsilon)} \right\rceil = O\left(\frac{1}{\epsilon}\ln\frac{D}{m_0}\right). \tag{1}$$

Select parameter t for the number of random events on a road as follows:

$$t = \left\lceil \frac{2\ln\left(\frac{h}{\lambda_0}\right)}{\delta^2} \right\rceil \tag{2}$$

$$= O\left(\frac{1}{\delta^2}\left(\ln\ln\left(\frac{D}{m_0}\right)+\ln\frac{1}{\epsilon}\right)\right) \tag{3}$$

$$= O\left(\frac{1}{\gamma^2}\left(\ln\ln\left(\frac{D}{m_0}\right)+\ln\frac{1}{\epsilon}\right)\right). \tag{4}$$

By equation (2), the selection of parameters h and t makes

$$he^{-\frac{1}{2}t\delta^2} \leq \lambda_0. \tag{5}$$

If $d_i < f_g(p+\gamma, M, D)$, then with probability at most $e^{-\frac{1}{2}t\delta^2}$, $\sum_{i=1}^{t} X_i < (p+\gamma-\delta)t = (p+2\delta)t$ by Proposition 2. If $\sum_{i=1}^{t} X_i \geq (p+\gamma-\delta)n = (p+2\delta)t$, it fails the test of line 8 in the algorithm and enters cycle $i+1$ for testing d_{i+1}. Thus, with probability at most $he^{-\frac{1}{2}t\delta^2}$, we fail to have an output $d \geq \frac{f_g(p+\gamma,M,D)}{1+\epsilon}$.

If $d_i \geq f_g(p-\gamma,q,M,D)$ (note $f_g(p-\gamma,M,q,D) \geq f_g(p+\gamma,M,D)$ by the monotonic condition of M), then we have $\sum_{i=1}^{t} X_i > (p-\gamma+\delta)t = (p-2\delta)t$ with probability at most $e^{-\frac{1}{2}t\delta^2}$ (by Proposition 2). If $\sum_{i=1}^{t} X_i \leq (p-\gamma+\delta)t = (p-2\delta)t$, it passes the test at line 8 of the algorithm, and returns $d = d_{i-1}$. If i is the least integer with $d_i \geq f_g(p-\gamma,q,M,D)$, then $d_{i-1} \leq f_g(p-\gamma,q,M,D)$. Thus, with probability at most $e^{-\frac{1}{2}t\delta^2}$, we fail to have an output $d \leq f_g(p-\gamma,M,D)$.

By inequality 5, with probability at most $(h+1)e^{-\frac{1}{2}t\delta^2} \leq 2he^{-\frac{1}{2}t\delta^2} \leq 2\lambda_0$, we fail to output d with $\frac{f_g(p+\gamma,M,D)}{1+\epsilon} \leq d \leq f(p-\gamma,M,D)$.

Each cycle samples sufficient t random events. The total number of cycles in the loop is at most h. The maximal number of ESs is at most $\frac{2D}{m_0}$ as the distance of two consecutive ESs should not be less than m_0. The total amount time is $t \cdot h \cdot T(M, n_D, h_D)$, which matches the complexity claim in the theorem by equations (1) and (2)–(4).

The monotonic condition is satisfied for both connected ESs and unconnected ESs. The algorithm is applied for connected ESs when $R_{g_c}(d_i, M, D)$ is used in the simulation.

Corollary 1: Assume that M is a parameter set for road traffic with connected ESs with connection topology $g_c(.)$. Let D be the parameter that controls the range for message transmission from the accident site. Let parameters p, q be in [0,1], and γ be in $[0, p]$. Then there is an approximation algorithm that gives a distance d and meets $\frac{f_{g_c}(p+\gamma,M,D)}{1+\epsilon} \leq d \leq f_{g_c}(p-\gamma,M,D)$. The time is $O(\frac{1}{\epsilon\gamma^2}(\ln\frac{D}{m_0})(\ln\ln(\frac{D}{m_0})+\ln\frac{1}{\epsilon})\cdot T(M,n_D,\frac{2D}{m_0}))$, where n_D is the number of vehicles on the road of length D, and $T(M, n_D, h_D)$ is the time of simulation for the system of parameters M, n_D vehicles, and h_D is the number of ESs on a road of length D.

The algorithm is applied for connected ESs when $R_{g_u}(d_i, M, D)$ is used in the simulation.

Corollary 2: Assume that M is a parameter set for road traffic with unconnected ESs with connection topology $g_u(.)$. Let D be the parameter that controls the range for message transmission from the accident site. Let parameters p, q be in [0,1], and γ be in $[0, p]$. Then there is an approximation algorithm that gives a distance d and meets $\frac{f_{g_u}(p+\gamma,M,D)}{1+\epsilon} \leq d \leq f_{g_u}(p-\gamma,M,D)$. The time is $O(\frac{1}{\epsilon\gamma^2}(\ln\frac{D}{m_0})(\ln\ln(\frac{D}{m_0})+\ln\frac{1}{\epsilon})\cdot T(M,n_D,\frac{2D}{m_0}))$, where n_D is the number of vehicles on the road of length D, and $T(M, n_D, h_D)$ is the time of simulation for the system of parameters M, n_D vehicles, and h_D the number of ESs on a road of length D.

IV. Algorithm for Simulation

In this section, we give an algorithm for simulation. It has a rigorous analysis for both correctness and complexity. Our algorithm can simulate an IoV with many vehicles at variant speeds, and multiple lanes on the roads. It has a reasonable computational complexity that makes it implementable by software.

We first give a brief description of the algorithm. Each ES is considered as a vehicle of speed zero. The algorithm is recursive via linear order of the times for the vehicles receiving the message. Two B-trees T_T and T_N hold the list of vehicles to receive the message within time t_0. T_T is used to hold the set of vehicles by their time to receive the message, and T_N is used to hold the set of vehicles by their names. Our algorithm identifies the set of vehicles P_i that can receive the message from the vehicle c_i after c_i has got the message. A vehicle c_i in T_T with the least time t_i is put into the output list L_2. For each vehicle c_i, calculate the time t_j to receive the message directly from c_i for each $c_j \in P_i$. Delete c_i from both T_T and T_N. If T_T and T_N already contain $c_j \in P_i$, it will be replaced by the new time t_j if it is earlier than the old time to receive the message for c_j. The set of vehicles in P_i will be inserted into two B-trees T_T (by the

Authorized licensed use limited to: Univ of Texas at Dallas. Downloaded on August 15,2022 at 19:55:20 UTC from IEEE Xplore. Restrictions apply.

Algorithm 2: Simulation Algorithm.

Input: parameter t_0 for the time delay, the positions of ESs, and vehicles with speed.

Output: the list L of vehicles and ESs that receive the message within time t_0.

1: Let each ES is treated as a vehicle of speed zero.
2: For each car c_i, find the set of vehicles P_i that can receive message from c_i within time t_0.
3: Identify the first vehicle c_k to receive the message, put it into T_N and T_T, and set up a link from T_N to T_T for this vehicle in both trees.
4: Build a B-tree T_N to save the cars by the linear order of their names.
5: Build a B-tree T_T to save the cars by the linear order of their time to receive message.
6: Let L_2 be an empty list.
7: Put the car in L_1 into T_N and T_T, and set up a link from T_N to T_T for the same vehicle.
8: Repeat
9: for each vehicle c_i with least time to receive the message in T_T,
10: delete c_i from T_T and T_N, and put it into a list L_2.
11: put all vehicles in P_i into T_N and T_T, set up a link from T_N to T_T for the same vehicle, and delete the existing vehicle if its time to receive the message is later, and insert the new time.
12: Until T_T is empty.
13: $L = L_2$.

order of t_j) and T_N (by the order of their IDs). There is a two directional link for the two nodes of each vehicle in T_T and T_N.

Definition 6: Let $g(.)$ be a connection topology for ESs on a road. A ES *xdirectly connects* to another ES y if they are connected $g(x) = g(y)$, and there is no ES z between x and y with $g(x) = g(z)$.

By the definition of direct connection, one ES connects at most two ESs on a road.

Theorem 2: There is an $O(P(t_0)n \log n)$ time algorithm to determine the set of vehicles that will receive message, where $P(t_0)$ is the largest number of vehicles that one vehicle or ES can directly pass the message to other vehicles or ESs on the road, and n is the total number of vehicles and ESs.

We only let at most two ESs directly receive message from one node. They can continue pass the message to the others connected to them. This controls the $P(t_0)$ to be small.

Proof: The correctness of this algorithm can be obtained by a simple induction for the number of vehicles on the road. Each ES is treated as a vehicle of speed zero in the algorithm. Each ES passes the message directly to its neighbor ESs if they are connected, or those vehicles and ESs in the range radio transmission. It is trivial when there is only one vehicle on the road. Assume that the algorithm works for the case that there are n vehicles such that each vehicle is added to the list L_2 by the earliest time receiving the message. Consider the case of $n + 1$ vehicles. Let c_{n+1} be the rightmost vehicle on the road. We discuss the following cases.

Case 1: The vehicle c_{n+1} is reachable by neither ES nor other vehicles. It follows from the inductive hypothesis.

Case 2: The vehicle c_{n+1} is reachable first by another vehicle c_i at time t_{n+1}. It will be considered in P_i. When c_i is added to L_2, c_{n+1} will be in P_i and will be added to the list L_2 according to time t_{n+1}. After vehicle c_i is added L_2, it will be added to neither L_2 nor B-tree. It becomes the case of n vehicles on the road. The other vehicles with message passed from c_{n+1} follows from the inductive hypothesis.

Therefore, the algorithm works for the case with $n + 1$ vehicles. This proves the correctness of the algorithm.

Each vehicle can forward message to at most $P(t_0)$ vehicles. The B-tree operation takes $O(\log n)$ time for inserting and deleting. Each vehicle has at most $O(P(t_0)$ times to do B-tree operations. Therefore, the total time is $O(P(t_0)n \log n)$.

Corollary 3: It exists an $O(n^2 \log n)$ time algorithm to determine the set of vehicles that will receive message, where $P(t_0)$ is the largest number of vehicles that one vehicle or ES can directly pass the message to other vehicles or ESs on the road, and n represents the total number of vehicles and ESs.

The generation of a random traffic takes $O(n)$ for a piece of road with n vehicles and ESs according to a system of parameters M for road traffic.

Theorem 3: Assume that M is a parameter set, and $g(.)$ is the ES connection topology. They satisfy the monotonic condition. Let parameters p, q be in [0,1]. Then there is an approximation algorithm such that it gives a distance d with $\frac{f_g(p+\gamma,q,M,D)}{1+\epsilon} \leq d \leq f_g(p-\gamma,q,M,D)$ in time $O(\frac{1}{\epsilon\gamma^2}(\ln \frac{D}{m_0})(\ln\ln(\frac{D}{m_0}) + \ln \frac{1}{\epsilon}) \cdot n^2 \log n)$, where D is the length to be considered for the message transmission, n_D is the number of vehicles on the road of length D, and $T(M, n_D, h_D)$ is the time of simulation for the system of parameters M, n_D vehicles, and h_D is the number of ESs on a road of length D. Furthermore, $T(M, n_D, h_D)$ is not decreasing for both n_D and h_D.

Proof: It follows from Theorem 1 and Corollary 3.

V. Simulation Results

There is no algorithm that can calculate the optimal solution during the polynomial running time since the problem of ESs placement in vehicular networks is NP-hard [26]. What we can do is approaching the approximation optimal solution as much as possible. It is unnecessary to cover all the nodes to complete connectivity in practical application. We focus on the relation about the placement distance of ESs or the number of ESs according to the connection probability of the vehicular network.

For each vehicular network, we can calculate the approximate optimal solution of ES deployment by this scheme. This experimental scenario is set as follows. According to the daily traffic volume of WUE highway in China, we calculate the average vehicle capacity of the highway. That is 1060. It means that there are 1060 vehicles on the highway. We consider two scenarios of vehicle density. When the vehicle node is 1060, it is a general scenario, and when the vehicle node is 530, it is a sparse scenario. Where vn is the number of vehicles and vES is the number of

Authorized licensed use limited to: Univ of Texas at Dallas. Downloaded on August 15,2022 at 19:55:20 UTC from IEEE Xplore. Restrictions apply.

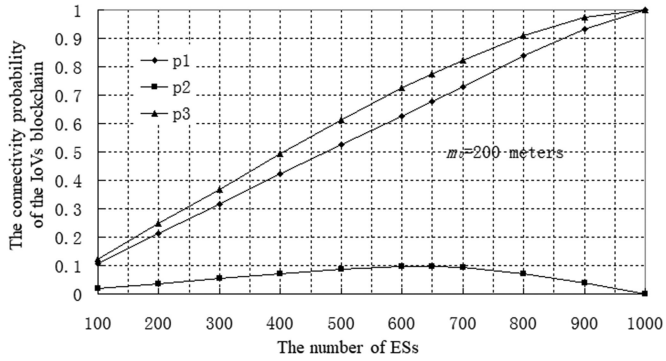

Fig. 1. Connectivity probability of IoVs for the number of ESs with vn = 530. p1:The probability of vehicles directly connected ESs. p2: The probability of vehicles indirectly connected ESs. p3: The total probability of vehicle connected ESs.

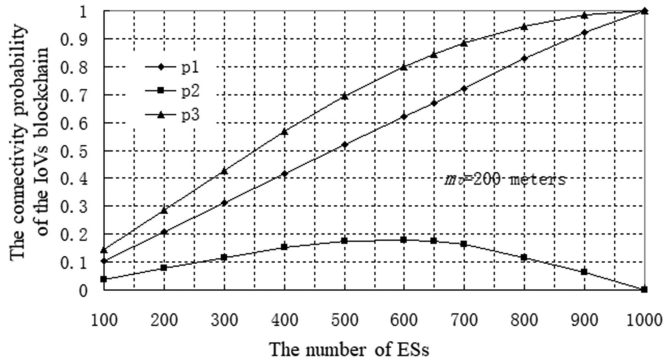

Fig. 2. Connectivity probability of IoVs for the number of ESs with vn = 1060. p1:The probability of vehicles directly connected ESs. p2: The probability of vehicles indirectly connected ESs. p3: The total probability of vehicle connected ESs.

deployed ESs. The node communication adopts the DSRC. The maximum distance of node transmission is 200 m. We take 200 m as the common default value m_0

The ESs deployed have the same interval. The initial position of vehicle nodes is randomly on this vehicular network. They play the role of miners in the vehicular blockchain network. The simulation results show that the vehicular blockchain network connectivity rate increases with the total number of ESs, as shown in Figs. 1, 2, 4, and 6.

Define the *direct connectivity probability* of vehicle with ESs is the number of vehicles on the blockchain network directly connected to ESs divided by the total number of vehicles on the blockchain network.

Define the *indirect connectivity probability* of vehicle with ESs is the number of vehicles on the blockchain network that can communicate with ESs via the relay of some other vehicles divided by the total number of vehicles on the blockchain network.

Define the *connectivity probability* of vehicle with ESs is the number of vehicles on the blockchain network is the sum of direct connectivity probability of indirect connectivity probability.

When m_0 is 200 m, the direct connectivity probability of vehicle to ESs increases almost linearly as the number of ESs

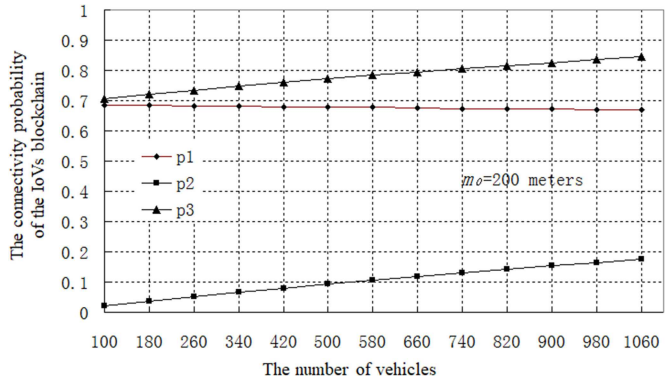

Fig. 3. Connectivity probability of IoVs for the number of vehicles with vES = 650. p1:The probability of vehicles directly connected ESs. p2: The probability of vehicles indirectly connected ESs. p3: The total probability of vehicle connected ESs.

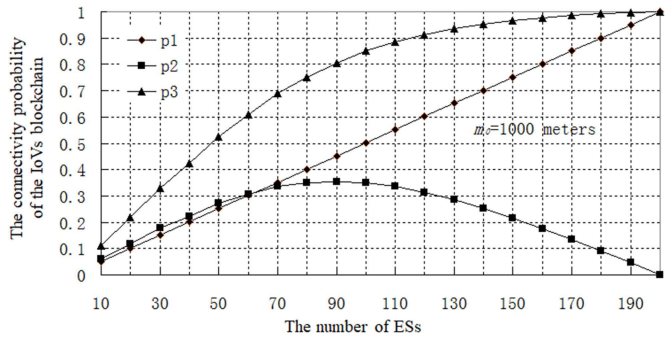

Fig. 4. Connectivity probability of IoVs for the number of ESs with vn = 530. p1:The probability of vehicles directly connected ESs. p2: The probability of vehicles indirectly connected ESs. p3: The total probability of vehicle connected ESs.

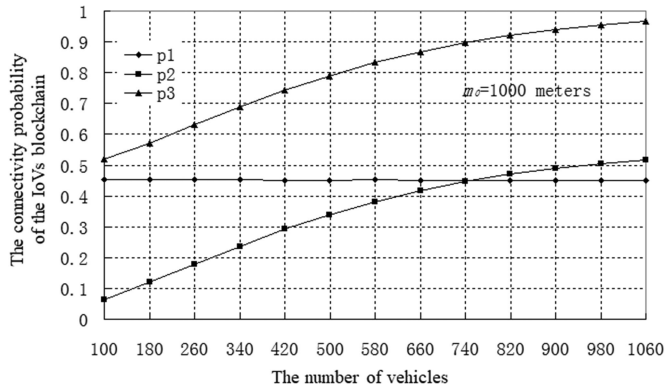

Fig. 5. Connectivity probability of IoVs for the number of vehicle with vES = 90. p1:The probability of vehicles directly connected ESs. p2: The probability of vehicles indirectly connected ESs. p3: The total probability of vehicle connected ESs.

gets larger. The direct connectivity probability of vehicles to ESs is much larger than the indirect connectivity probability of vehicles to ESs. On the other hand, the indirect connectivity probability of vehicles with ESs is not linearly increasing with the increasing number of ESs.

Authorized licensed use limited to: Univ of Texas at Dallas. Downloaded on August 15,2022 at 19:55:20 UTC from IEEE Xplore. Restrictions apply.

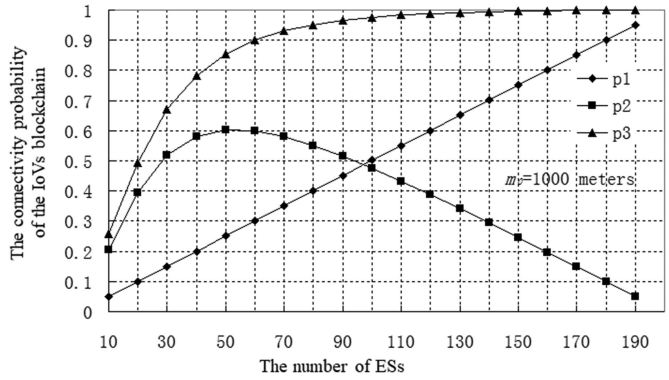

Fig. 6. Connectivity probability of IoVs for the number of ESs with vn = 1060. p1:The probability of vehicles directly connected ESs. p2: The probability of vehicles indirectly connected ESs. p3: The total probability of vehicle connected ESs.

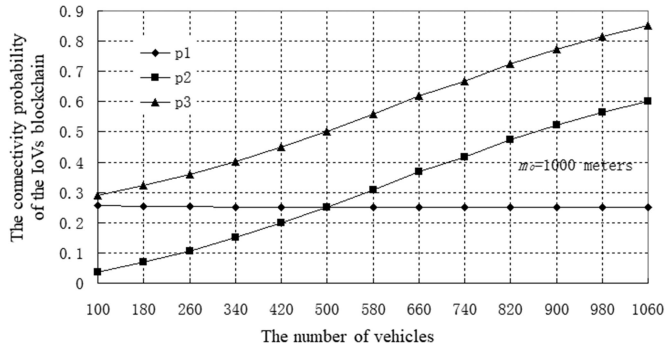

Fig. 7. Connectivity probability of IoVs for the number of vehicle with vES = 50. p1:The probability of vehicles directly connected ESs. p2: The probability of vehicles indirectly connected ESs. p3: The total probability of vehicle connected ESs.

For vn = 530, the indirect connectivity probability of vehicles with ESs becomes maximum when ESs = 650.

The indirect connectivity probability decreases when the number of ESs is increased. The reason is that the number of vehicles directly connected with ESs increases when the number of ESs is increased. The connectivity probability goes up slowly.

When the number of deployed ESs reaches 650, the connectivity probability is 0.775, as shown in Fig. 1. We can consider vES = 650 as an approximation for the optimal solution in the case. For vn = 1060, vES = 600 is an approximation for the optimal solution in the case, which is shown in Fig. 2.

When the number of vehicles is fixed, the direct connectivity probability of vehicles with ESs is almost constant regardless of the number of vehicles, which is shown in Figs. 3, 5, and 7. However, the indirect connectivity probability of vehicle with ESs almost linearly increases with the increasing number of ESs.

When vn = 1060, the connected probability has the similar trends with vn = 530. But, the number of ESs need to deploy is a significant reduction. The approximation optimal solution is vES = 50 and vES = 90 with the vn = 1060 and vn = 530, respectively. The connectivity probability is up to 0.806 with vES = 50, vn = 530 according to the m_0 is 200 m, vES = 680, vn = 530.

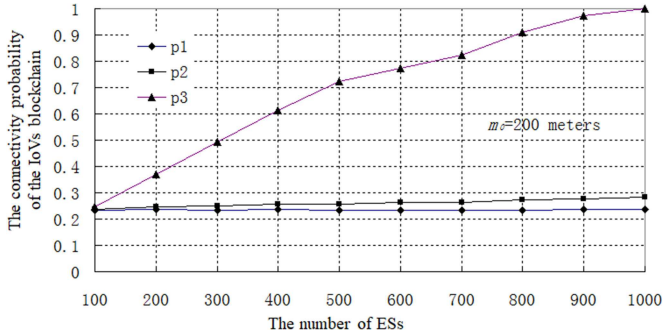

Fig. 8. Connectivity probability of IoVs for the number of ESs with m_0 = 200 meters, vn = 1060, vspeed = 108 km/h, and vspeed = 216 km/h. p1:The connectivity probability of vehicles with vspeed = 108 km/h. p2: The connectivity probability of vehicles with vspeed = 216 km/h.

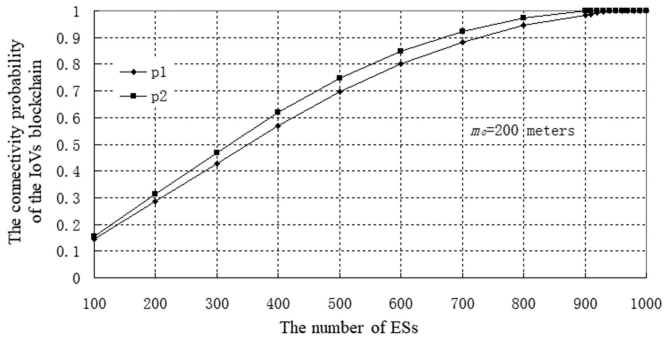

Fig. 9. Connectivity probability of IoVs for the number of ESs with m_0 = 1000 meters, vn = 1060, vspeed = 108 km/h, and vspeed = 216 km/h. p1:The connectivity probability of vehicles with vspeed = 108 km/h. p2: The connectivity probability of vehicles with vspeed = 216 km/h.

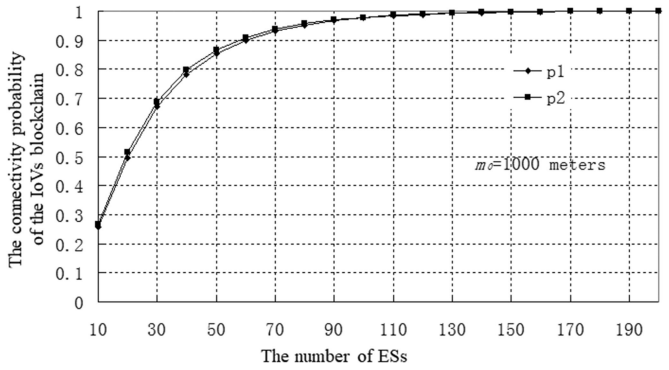

Fig. 10. Number of ESs versus the connectivity probability of IoVs with m_0=200 m. p1: The number of ESs in the proposed scheme. p2: The number of ESs in ODEL.

Figs. 8 and 9 show that the connectivity probability of IoVs for the number of ESs with vn = 1060, vspeed = 108 km/h, and vspeed = 216 km/h: 1) The transmission distance of vehicles is 200 m; 2) The transmission distance of vehicles is 1000 m. We can see that the speed of vehicles has little impact on the connectivity probability.

We compared the proposed scheme with ODEL [32]. As shown in Figs. 10 and 11, we find that the deployment cost

Authorized licensed use limited to: Univ of Texas at Dallas. Downloaded on August 15,2022 at 19:55:20 UTC from IEEE Xplore. Restrictions apply.

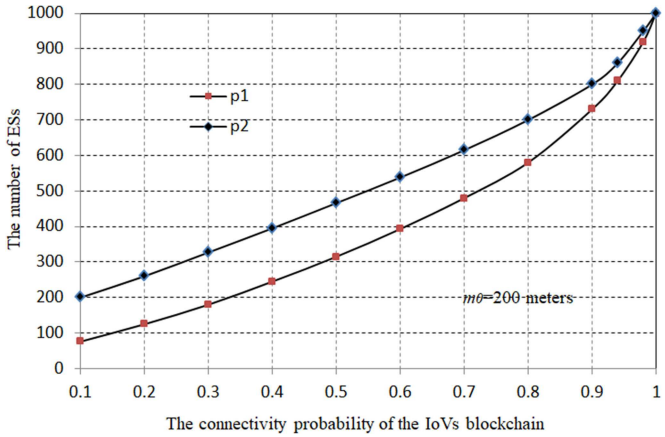

Fig. 11. Number of ESs versus the connectivity probability of IoVs with $m_0 = 1000$ m. p1: The number of ESs in the proposed scheme. p2: The number of ESs in ODEL.

of ODEL scheme is higher than that of the proposed scheme with the same connectivity probability of IoVs. It is because the ODEL method needs to deploy more ESs to satisfy the requirements to reduce the routing delay caused by dynamic network topology in IoVs. The scheme proposed in this article focuses on the fact that the deployed edge servers can cover more segments on the road, so the deployment cost can be reduced.

VI. Conclusion

In this article, we have proposed an edge server deployment scheme for the application of blockchain technology in IoVs. The edge servers are used as miners in vehicular blockchain networks. To address the challenges of the communication delay between miners in vehicular blockchain networks, we introduce a randomized method to design an approximation algorithm for edge server deployment. It achieves an approximation for the optimal deployment distance to ensure the message can be transmitted to ESs via the IoVs. The simulation results show the deployment of edge server can greatly improve the connectivity of vehicular blockchain networks and meet the communication requirements of edge server as a miner of IoVs blockchain. In addition, it shows that in vehicle blockchain network, the number of deployed edge servers and the communication distance of vehicle nodes are two key factors determining the connectivity of vehicle blockchain network. In addition, results show that when the number of edge servers deployed reaches a certain value, the connectivity of vehicle blockchain network reaches a threshold. Since then, more edge servers have a very limited contribution to the connectivity of vehicle blockchain network. However, the scale of the vehicle blockchain network is very large. When the number of edge servers deployed reaches the maximum, in order to further improve the mining efficiency of miners and meet the computing needs of the blockchain network, the edge servers can recruit vehicle nodes to provide services for its competitive mining. In future work, we will investigate the incentive mechanism of edge server recruiting vehicle nodes. The edge server recruits vehicle nodes within its communication range to provide services for mining. It will improve the computing power of the edge server and speed up the competitive mining process. These enable blockchain, a distributed database with the advantages of unforgeability, traceability, and collective maintenance, to be applied to the IoVs.

References

[1] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.
[2] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.
[3] L. Dong, W. Wu, Q. Guo, M. N. Satpute, T. Znati, and D. Z. Du, "Reliability-aware offloading and allocation in multilevel edge computing system," *IEEE Trans. Rel.*, vol. 70, no. 1, pp. 200–211, Mar. 2021.
[4] X. D. Jianxiong Guo and W. Wu, "Reliable traffic monitoring mechanisms based on blockchain in vehicular networks," *IEEE Trans. Rel.*, to be published, doi: 10.1109/TR.2020.3046556.
[5] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.
[6] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2906–2920, Mar. 2019.
[7] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, Jan. 2017.
[8] J. Ren, G. Yu, Y. He, and G. Y. Li, "Collaborative cloud and edge computing for latency minimization," *IEEE Trans. Veh. Technol.*, vol. 68, no. 5, pp. 5031–5044, May 2019.
[9] Z. Li, Z. Yang, and S. Xie, "Computing resource trading for edge-cloud-assisted Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3661–3669, Jun. 2019.
[10] W. Chen *et al.*, "Cooperative and distributed computation offloading for blockchain-empowered industrial Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8433–8446, Oct. 2019.
[11] C. Luo, L. Xu, D. Li, and W. Wu, "Edge computing integrated with blockchain technologies," in *Proc. Complexity Approximation*, 2020, pp. 268–288.
[12] M. Li, N. Cheng, J. Gao, Y. Wang, L. Zhao, and X. Shen, "Energy-efficient UAV-assisted mobile edge computing: Resource allocation and trajectory optimization," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 3424–3438, Mar. 2020.
[13] J. Zhao, Q. Li, Y. Gong, and K. Zhang, "Computation offloading and resource allocation for cloud assisted mobile edge computing in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 7944–7956, Aug. 2019.
[14] H. Sun, F. Zhou, and R. Q. Hu, "Joint offloading and computation energy efficiency maximization in a mobile edge computing system," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 3052–3056, Mar. 2019.
[15] J. Zheng, X. Dong, T. Zhang, J. Chen, W. Tong, and X. Yang, "Microthingschain: Edge computing and decentralized IoT architecture based on blockchain for cross-domain data shareing," in *Proc. IEEE Int. Conf. Netw. Network Appl.*, 2018, pp. 350–355.
[16] A. Damianou, C. M. Angelopoulos, and V. Katos, "An architecture for blockchain over edge-enabled IoT for smart circular cities," in *Proc. IEEE 15th Int. Conf. Distrib. Comput. Sensor Syst.* , 2019, pp. 465–472.
[17] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined FOG node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, Sep. 2017.
[18] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, and Y. Zhang, "A blockchain-based nonrepudiation network computing service scheme for industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3632–3641, Jun. 2019.
[19] B. Bera, S. Saha, A. K. Das, N. Kumar, P. Lorenz, and M. Alazab, "Blockchain-envisioned secure data delivery and collection scheme for 5G-based IoT-enabled internet of drones environment," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 9097–9111, Aug. 2020.
[20] M. Zhaofeng, M. Jialin, W. Jihui, and S. Zhiguang, "Blockchain-based decentralized authentication modeling scheme in edge and IoT environment," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2116–2123, Feb. 2021.

Authorized licensed use limited to: Univ of Texas at Dallas. Downloaded on August 15,2022 at 19:55:20 UTC from IEEE Xplore. Restrictions apply.

[21] R. Gupta, A. Kumari, and S. Tanwar, "A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 6, 2020, Art. no. e4009.
[22] K. Xiao, W. Shi, Z. Gao, C. Yao, and X. Qiu, "Daer: A resource preallocation algorithm of edge computing server by using blockchain in intelligent driving," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9291–9302, Oct. 2020.
[23] X. Zhang, R. Li, and B. Cui, "A security architecture of vanet based on blockchain and mobile edge computing," in *Proc. 1st IEEE Int. Conf. Hot Information-Centric Netw.*, 2018, pp. 258–259.
[24] H. Zhu, C. Huang, and J. Zhou, "Edgechain: Blockchain-based multi-vendor mobile edge application placement," in *Proc. 4th IEEE Conf. Netw. Softwarization Workshops*, 2018, pp. 222–226.
[25] E. Androulaki *et al.*, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. IEEE 13th EuroSys Conf.*, 2018, pp. 1–15.
[26] P. Li, Q. Liu, C. Huang, J. Wang, and X. Jia, "Delay-bounded minimal cost placement of roadside units in vehicular AD HOC networks," in *Proc. IEEE Int. Conf. Commun.*, 2015, pp. 6589–6594.
[27] Y. Jo and J. Jeong, "RPA: Road-side units placement algorithm for multihop data delivery in vehicular networks," in *Proc. IEEE 30th Int. Conf. Adv. Inf. Netw. Appl. Workshops*, 2016, pp. 262–266.
[28] S.-F. Hwang, W.-C. Chen, C.-R. Dow, and N.-L. Nguyen, "Efficient RSU placement schemes in urban vehicular ad HOC networks," *J. Inf. Sci. Eng.*, vol. 35, no. 5, pp. 1045–1060, Sep. 2019.
[29] X. Liya, H. Chuanhe, L. Peng, and Z. Junyu, "A randomized algorithm for roadside units placement in vehicular ad HOC network," in *Proc. IEEE 9th Int. Conf. Mobile Ad-Hoc Sensor Netw.*, 2013, pp. 193–197.
[30] R. Motwani and P. Raghavan, *Randomized Algorithms*. London, U.K.: Chapman & Hall/CRC, 2010.
[31] M. Li, B. Ma, and L. Wang, "On the closest string and substring problems," *J. ACM (JACM)*, vol. 49, no. 2, pp. 157–171, Mar. 2002.
[32] S. Mehar, S. M. Senouci, A. Kies, and M. M. Zoulikha, "An optimized roadside units (RSU) placement for delay-sensitive applications in vehicular networks," in *Proc. 12th Annu. IEEE Consum. Commun. Netw. Conf.*, 2015, pp. 121–127.

Liya Xu received the Ph.D. and M.S. degrees in computer science from the Wuhan University, Wuhan, China, in 2014 and 2010, respectively.

He is currently a Visiting Scholar with the Department of Computer Science, University of Texas at Dallas, Richardson, TX, USA, following the team of Prof. Dingzhu Du. He is also an Associate Professor of School of Information Science and Technology, Jiujiang University, China. His current research interests include blockchain, internet of vehicles, wireless sensor network, and design and analysis of algorithms for optimization problems that occur in wireless networking environments.

Mingzhu Ge received the B.S. and M.S. degrees in computer science from Wuhan University, Wuhan, China, in 2013 and 2015, respectively, and the Ph.D. degree in Computer and Software Engineering from Wonkwang University, Iksan, South Korea, in 2021.

She is currently an Associate Professor of School of Information Science and Technology, Jiujiang University, China. Her current research interests include blockchain, vehicular ad hoc network, wireless sensor network, edge computing.

Weili Wu(Senior Member, IEEE) received the Ph.D. and M.S. degrees in computer science from University of Minnesota, Minneapolis, MN, USA, in 2002 and 1998, respectively.

She is currently a Full Professor with the Department of Computer Science, The University of Texas at Dallas, Richardson, TX, USA. Her current research interests include data communication and data management, and design and analysis of algorithms for optimization problems that occur in wireless networking environments and various database systems.

Authorized licensed use limited to: Univ of Texas at Dallas. Downloaded on August 15,2022 at 19:55:20 UTC from IEEE Xplore. Restrictions apply.