Liang *et al.*
EURASIP Journal on Advances in Signal Processing (2023) 2023:115
https://doi.org/10.1186/s13634-023-01075-2

EURASIP Journal on Advances in Signal Processing

RESEARCH Open Access

Fairness resource allocation based on blockchain for secure communication in integrated IoT

Wei Liang[1], Jun Zhao[1*], Yan Liu[1], Yan Liang[2] and Jingwen Li[1]

*Correspondence:
zhaojun202308@163.com

[1] China Telecom Research Institute, Beijing, China
[2] School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing, China

Abstract

The emerging Space-Air-Ground, Artificial intelligence, blockchain and Vehicle-to-everything technology in Integrated Internet of Things (IoT) enables vehicles to communicate with other vehicles and roadside units (RSU), which improves communication efficiency and driving safety. Due to the rich data in the Integrated IoT, it is easy for illegal persons to steal data or deceive users. While reasonably allocating resources to complete the transmission task, it is still a challenge to ensure the communication security of vehicle users in Integrated IoT. In this paper, we study the cost of vehicle users transmitting tasks by Vehicle to Infrastructure and Vehicle to Vehicle (V2V) in Integrated IoT. In order to protect the information security, we establish the identity authentication and matching model to obtain a better channel environment of Integrated IoT. Moreover, we consider dynamic pricing based on bandwidth resource occupancy to ensure user experience and server load in Integrated IoT. Under the constraints of task tolerable delay, we fix the bandwidth on the V2V side and decouple the task decomposition and bandwidth allocation in Integrated IoT. Then, we propose algorithms Blockchain-based Vehicle Identity Authentication (BVIA) and Delay Weight Fairness Bandwidth Allocation (DWFBA). In this way, vehicle users and RSUs entering the Integrated IoT system are authenticated and matched with devices with good trust value, and the fairness of users resource allocation is guaranteed. Simulation results show that BVIA algorithm can reduce communication overhead, and DWFBA algorithm can control user costs and effectively reduce the number of task failures in Integrated IoT.

Keywords: Integrated IoT, Information security, Resource allocation, Blockchain, Identity authentication

1 Introduction

With the continuous evolution of industrial production, the number of connected devices in IoT business will continue to increase, which will promote the development of Integrated IoT [1]. The combination of automobile and Integrated IoT industry has formed a new important research field, that is, V2X communication [2]. In the early days, vehicles in IoT provided voice navigation, diagnosis and rescue, as well as road information and entertainment services. In the future, V2X communication of

Integrated IoT could interact with the information of external elements of the vehicle. At present, road safety and data transmission efficiency are the key problems that need to be solved urgently [3]. V2X is a feasible solution to this problem. It can enable networked vehicles to communicate with other vehicles and roadside infrastructure in real time, ensure road safety and improve traffic conditions [4].

At present, many authors have combined V2I and V2V technology to research the transmission delay, throughput, power consumption and other aspects of vehicle system in Integrated IoT, and achieved good optimization results. In [5, 6], considering the user Quality of Service (QoS), Y. Saleem and M. Sepulcre et al. combined V2I and V2V technology to provide offloading services for vehicles, which reduced the task transmission delay, and verified the rationality of the coordination of the two technologies. X. Liu, B. L. Nguyen and L. Su et al. proposed V2V and V2I collaboration strategies in [7–9], respectively, which improved the throughput of the Integrated IoT system. H. Yahya and S. Guo conducted in-depth research on power and spectrum, and proposed the power control scheme to reduce vehicle transmission energy consumption [10, 11].

With the rapid development of Integrated IoT technology, vehicle users are also increasing, and the network is gradually huge. As more and more vehicles join this network, the amount of information in Integrated IoT vehicle communication increases, which attracts attackers to obtain this information illegally, resulting in network security problems of Integrated IoT system [12]. And the Integrated IoT system has the characteristics of scattered users and rapid changes in network topology. The emerging blockchain technology can meet the needs of the distributed characteristics of Integrated IoT and shows good performance in terms of security. Compared with the traditional cryptographic algorithm, it has low complexity and low overhead [13, 14].

In order to solve the data security problem of Integrated IoT, many scholars have proposed blockchain safe communication strategies to improve the reliability and security in Integrated IoT networks. The most common security method is authentication mechanism. Son et al. [15] designed a V2I handover authentication mechanism to ensure the security of data transmission between vehicles and roadside units in. The advantage of this authentication method is that it will not cause load to the vehicle, but it does not consider the safety of V2V data transmission. H. Cheng et al. proposed a reputation evaluation mechanism to solve the security problems in service quality evaluation in [16]. Such a security policy is simple and effective, but it cannot prevent identity forgery. In [17], Wei et al. proposed an authenticated key protocol, which is divided into two stages: authentication and key negotiation, to protect the communication security of V2V and V2I in Vehicular Ad-Hoc Network (VANET) at the same time. At present, many security mechanisms are two stages of authentication and consensus, which is one of the mainstream solutions to the problem of communication security. Moreover, many authors have also improved the performance of blockchain consensus mechanism. In [18–20], J. Cui, J. Shi and H. N. Abishu et al., respectively, proposed improved consensus algorithms such as DPoS and PBFT in combination with mechanisms such as reputation proof to reduce the cost of users, and ensure data security. Thus, we consider adding blockchain authentication and consensus mechanism to the V2X communication in Integrated IoT process to ensure the security of data transmission.

Resource usage cost is an aspect in Integrated IoT that users pay close attention to. Its pricing strategy affects user costs and operator resource load pressure. Many scholars have studied the resource pricing mechanism and proposed solutions. In [21], based on the game method, C. Roy et al. proposed to use dynamic differential pricing scheme, which effectively improved the income of the operator, but does not take into account the user cost. In [22, 23], considering the comfort of users, K. M. K. Ramamoorthy et al. established a pricing model centered on quality of experience (QoE), and maximized economic utility by using Stackelberg game. Such a game market bidding mechanism can dynamically adjust pricing, which can improve the profits of operators and have higher resource utility. However, the game mechanism requires vehicle users and network operators to confirm the price through bidding for many times, which is difficult to meet the urgency requirements of time delay sensitive vehicle tasks. User requests for resource packets with bidding will also lead to additional overhead.

Additionally, in combination with the blockchain framework, X. Wang et al. considered that the servers have different capacities and prices, and integrated task offloading, block propagation and miner mobility to maximize the utility of miners in [24]. And Zhang et al. formulated a joint bandwidth and computing resource allocation problem under the blockchain framework. In order to reduce the complexity of the problem, they decomposed the problem into two sub-problems to maximize the long-term utility of all mobile devices in [25, 26].

For the characteristics of vehicle delay sensitivity, M. Siew et al. proposed the dynamic pricing scheme of decentralized shared resources, which maximized social welfare profits, and verified that the effect of dynamic pricing is better than static pricing [27, 28]. Further, Y. Yang et al. found that the pricing scheme of nonlinear relationship is more suitable for distributed V2X IoT system in the pricing problem of edge resources driven by blockchain [29]. After consulting a large number of literatures, we found that more research focuses on the profit of operators rather than the user cost. Vehicle user cost is an important indicator to evaluate the quality of resource pricing schemes. Hence, we will design a nonlinear dynamic pricing scheme more suitable for the V2X Integrated IoT system to control user costs.

We believe that every vehicle entering the Integrated IoT has the same resource allocation rights and equal status, which is also in line with the idea of blockchain decentralization. Many scholars have solved many problems based on max-min fairness algorithm, such as utility, power, throughput, load and user cost. So the fairness of the target users of resource allocation has been greatly guaranteed.

In [30, 31], the authors Z. Jing and L. Shi, respectively, proposed the improved maximum and minimum fairness algorithm to maximize the user offloading utility and computing energy efficiency, considering the fairness of user resource allocation. Authors Y. Ye and A. Ahmadian, respectively, proposed the resource allocation scheme based on maximum minimum throughput to ensure the fairness of each node in the scenario of wireless powered Internet of things [32, 33]. In [34], X. B. Zhai et al. proposed an improved maximum and minimum rate fairness algorithm to ensure network fairness and effectively control energy consumption. In addition, the authors in [35–37] proposed improved the maximum and minimum fairness algorithm in terms of power

control, reducing the load of the Integrated IoT and user costs, so as to achieve the optimization goal and effectively ensure user fairness.

Out of above motives, we consider vehicle delay sensitive transmission tasks in the scenario of Integrated IoT. In order to ensure communication security of Integrated IoT, we have added the blockchain identity authentication model, established the communication and resource model, and solved the problem of minimizing the cost of bandwidth resources. The main contributions are as follows:

- We studied the scenario that V2I and V2V transmit data in Integrated IoT at the same time. A variety of basic bandwidth constraints and trust value matching are considered to ensure data legitimacy. Transmission tasks can be completed within tolerable delay with better channel resources.
- For the coupling problem of bandwidth allocation and task decomposition, we fixed the V2V bandwidth, discussed the user bandwidth resource requests based on the user cost, and took the reciprocal of delay as the task emergency weighted value.
- We proposed algorithms Blockchain-based Vehicle Identity Authentication (BVIA) and Delay Weight Fairness Bandwidth Allocation (DWFBA). The goal of these two algorithms is to find the optimal scheme of bandwidth allocation and ensure the fairness of user resource allocation and data security. Compared with the other two algorithms, BVIA algorithm has lower communication overhead, DWFBA algorithm has better cost control effect and fewer task failures.

The rest of the paper is structured as follows: In Sect. 2, we introduce the system model and describe formal problem. In Sect. 3, we narrate the process of the proposed BVIA and DWFBA algorithm. In Sect. 4, we explore experimental parameter settings, analyze the performance of BVIA and DWFBA algorithm by comparing different algorithms, and then draw conclusions in Sect. 5.

2 System model

In this section, we first introduce the data transmission application scenario for block chain authentication in V2X Integrated IoT and vehicle task model. Next, we establish an identity registration and authentication model to ensure the security of transmission tasks, and obtain the trust value between vehicles. Then, the transmission rate and transmission task time of vehicles are calculated according to the user coordinates of the mobile communication model. In addition, we design the bandwidth resource pricing model based on the server resource occupancy, which dispersed the server pressure. Finally, we combine the above models, consider some constraints, and propose the goal of user cost control.

2.1 Vehicle task model

As shown in Fig. 1, we consider a scenario where there is a gnodeb (gNB) and $\mathcal{M} = \{1, 2, ..., j, ..., M\}$ RSUs around the intersection. Both of them are equipped with edge servers, which can be used to formulate resources scheduling strategies, deal with urban road congestion, traffic accidents and other emergencies, and timely report road conditions to vehicles.

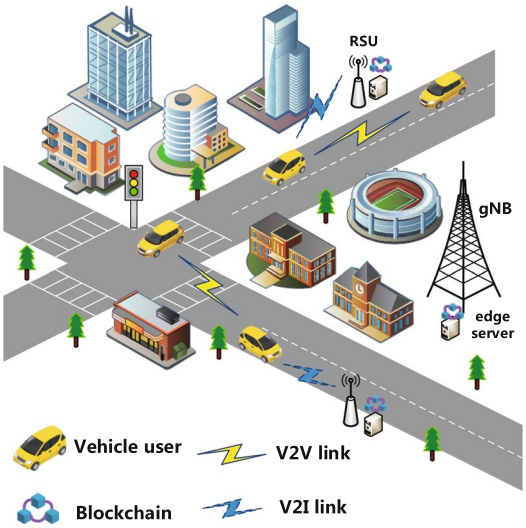

Fig. 1 Transmission system with blockchain in V2X Integrated IoT

Suppose there are $\mathcal{N} = \{1, 2, ..., i, ..., N\}$ V2V users (VUs) driving on the road, and the number of VU with time slot t entering the cellular network coverage follows the Poisson distribution. Let ϑ be the average arrival value of the sample vehicle, then the probability density function is

$$Pn\{X = N(t)\} = \frac{\vartheta^{N(t)}}{N(t)!} e^{-\vartheta} \tag{1}$$

Some data files are needed to process the computing tasks during the driving process of the vehicle. To reduce the pressure on the gNB servers, users can simultaneously use V2V and V2I technologies to obtain cache files from other vehicles and RSUs, respectively. In the V2V communication system of Integrated IoT, the two sides of the pairing of Internet of vehicles users are divided into V2V transmitter (V2V-S) and receiver (V2V-R), and the uplink with less cellular network traffic is used between vehicles to exchange information. To reduce the interference among multiple users, it is restricted that multiple V2V pairs cannot share the same channel, and one VU can only be paired with one V2V. Meanwhile, the VU can communicate with one RSU at most [38].

Due to the high-speed mobility and dynamics of vehicles, the network topology is constantly changing and vulnerable to external node intrusion and attack. The peer-to-peer interaction mode of vehicles is difficult to resist the monitoring and deception of internal malicious nodes, which affects the security of the entire V2X Integrated IoT. Thus, before the vehicle data transmission and caching tasks begin, the vehicles identity needs to be authenticated to ensure data security.

For the user, the vehicle needs the cache resources of other vehicles or RSUs during driving. We use triples $\langle \delta, S, D \rangle$ to describe these tasks, where δ represents the complexity factor of the task, S represents the size of the data, and D represents the maximum tolerable delay of the task. Computing tasks have many forms such as text, voice or video, so the computational complexity factor, data size and maximum tolerable delay of these tasks are different. To complete these data transmission tasks, VUs

need the gNB to schedule bandwidth resources and pay different prices according to different resources.

2.2 Identity authentication model

The whole identity authentication system is composed of certificate authority (CA), RSUs and VUs. The gNB acts as the CA, registers legal identity for vehicle users entering the system, generates public and private keys, and issues certificates. RSUs provide cache files for vehicles and uploads the collected data to the block. Vehicles can communicate with each other to transmit data and report their own conditions to RSUs. Then, we divide the Integrated IoT secure communication of blockchain into three stages: identity registration, identity authentication and trust value calculation.

2.2.1 identity registration

RSUs and VUs entering the system for the first time need to register with CA. We record the j-th RSU in the system as RSU_j, which makes a registration request to CA and sends its own ID Rid_j and 256 bit random number Rk_j information. And the expression is

$$\mathrm{RSU}_j : \{\mathrm{Rid}_j, \mathrm{Rk}_j\} \rightarrow \mathrm{CA}, \forall j \in M, \tag{2}$$

CA receives the registration information of RSU_j and generates the authorization certificate Rc_j after confirmation. Then, CA generates a ellipse curve cryptography function as

$$\begin{aligned} C(a,b) : y^2 &= x^3 + ax + b \ (\mathrm{mod}\ \ p) \\ s.t. \& 4a^3 &+ 27b^2 \neq 0 \end{aligned} \tag{3}$$

where p is a prime number, a and b are non-negative integers.

CA takes the random number Rk_j of RSU_j as the private key, and the expression is

$$Rpr_j = Rk_j, \forall j \in M, \tag{4}$$

The public key of RSU_j can be obtained by randomly selecting a base point $G_j^r(x_j, y_j)$ on the conical section, then the expression is

$$Rpu_j = Rpr_j \times G_j^r, \forall j \in M, \tag{5}$$

where $\times$ is the multiplication symbol of conical section.

Next, CA broadcasts the RSU_j registration completion timestamp Rts_j and public key Rpu_j to the whole network. Meanwhile, RSU_j receives the certificate Rc_j, private key Rpr_j, public key Rpu_j and registration timestamp Rts_j information through secure transmission channel.

$$\mathrm{CA} : \{\mathrm{Rc}_j, \mathrm{Rpr}_j, \mathrm{Rpu}_j, \mathrm{Rts}_j\} \rightarrow \mathrm{RSU}_j, \forall j \in M. \tag{6}$$

And RSU registration diagram is shown in Fig. 2.

Nodes in decentralized blockchain network need to maintain the order of blockchain network operation through consensus mechanism. The consensus mechanism is used to prove which block has obtained the accounting right and reward, which solves the trust problem in the blockchain network. In order to safeguard the data security of blockchain

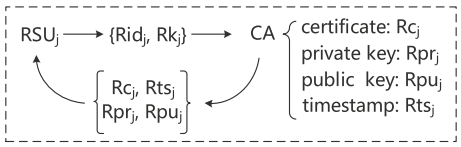

Fig. 2 RSU registration diagram

and adapt to the changing characteristics of the network structure of V2X Integrated IoT, we use the consensus mechanism based on Raft algorithm to elect leaders in RSUs to manage blockchain.

Roles include Follower, Candidate and Leader, in the distributed algorithm Raft. At the initial time, all RSU nodes are Follower. If there is no response from Candidate or Leader within one term, it becomes Candidate. In each term, the candidates can vote for the trusted node to manage the blockchain, and the one who gets more than half of the votes is Leader in that term.

The Leader node packs the received information in the form of blocks and broadcasts it to other nodes. After the block is accepted, other nodes verify the timestamp and term in the block content, and copy files. Half of the nodes responded, followed by the Leader to chain the block. The role judgment expression of RSU $_j$ is

$$\text{RSU}_j \text{ as } \begin{cases} \text{Follower}, & \text{initialization role}, \\ \text{Candidate}, & \text{if without response}, \\ \text{Leader}, & \text{if get more than half votes}. \end{cases} \tag{7}$$

Vehicle users also need to register when entering the network coverage for the first time, and provide their own ID Vid $_i$ and application timestamp Vts $_i$ to CA. Then, the expression is

$$\text{VU}_i : \{\text{Vid}_i, \text{Vts}_i\} \rightarrow \text{CA}, \forall i \in N, \tag{8}$$

CA generates a random number Vk_i and uses it as the private key Vpr_i of VU_i. After the request is received.

$$\text{Vpr}_i = \text{vk}_i, \forall i \in N, \tag{9}$$

According to Equ. (3), the base point $G_i^v(x_i, y_i)$ on the conical section is selected, and the public key Vpu_i of VU_i can be calculated as

$$\text{Vpu}_i = \text{Vpr}_i \times G_i^v, \forall i \in N, \tag{10}$$

If users need privacy protection, pseudonyms are generated to protect users' anonymity. The pseudonym Vpd_i of VU_i is

$$\text{Vpd}_i = H(\text{Vid}_i || \text{Vk}_i), \forall i \in N, \tag{11}$$

where $||$ is the string connector and $H(\cdot)$ is the hash operation.

Next, CA issues the certificate Vc_i with valid time for VU_i and sets the initial trust value $\text{Vtv}_i^{\text{init}}$. Thus, the information sent by CA to VU_i through secure channel includes private key Vpr_i, public key Vpu_i, pseudonym Vpd_i, certificate Vc_i and trust value Vtv_i.

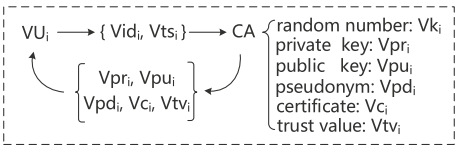

Fig. 3 VU registration diagram

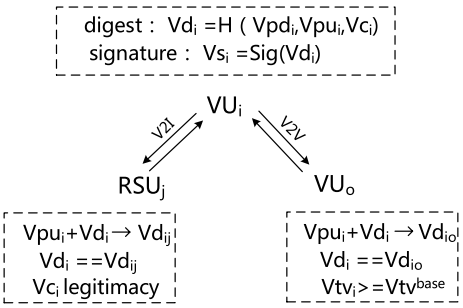

Fig. 4 The schematic diagram of VU_i authentication

$$\mathrm{CA} : \{\mathrm{Vpr}_i, \mathrm{Vpu}_i, \mathrm{Vpd}_i, \mathrm{Vc}_i, \mathrm{Vtv}_i^{init}\} \rightarrow \mathrm{VU}_i, \forall i \in N. \tag{12}$$

And VU registration diagram is shown in Fig. 3.

2.2.2 Identity authentication

Vehicles can obtain the file content they need through V2V or V2I. Before communication transmission, they need to verify the identity of the other party to ensure information security. Assume that the vehicle user preparing to communicate is VU_i, and send the request to RSU_j and VU_o at the same time. VU_i hashes its pseudonym Vpd_i, public key Vpu_i and certificate Vc_i to form a digest Vd_i, and digitally signs Vs_i the digest. Then, the expression is

$$\begin{aligned} \mathrm{Vd}_i &= H\left(\mathrm{Vpd}_i, \mathrm{Vpu}_i, \mathrm{Vpd}_i, \mathrm{Vc}_i\right), \forall i \in N, \\ \mathrm{Vs}_i &= \mathrm{Sig}(\mathrm{Vd}_i), \forall i \in N. \end{aligned} \tag{13}$$

RSU_j uses the received public key Vpu_i to unlock the digital signature Vs_i, get the digest Vd_{ij}, and verify whether the Vd_{ij} is the same as Vd_i. Then, RSU_j queries the validity of the certificate Vc_i in the blockchain and returns the authentication success message to VU_i.

Similar to the RSU_j verification method, VU_o uses the public key Vpu_i to decrypt the signature Vs_i and get the digest Vd_{io}. Next, VU_o verifies whether Vd_i and Vd_{io} are the same, and queries that the trust value Vtv_i is not less than the threshold $\mathrm{Vtv}^{\mathrm{base}}$, then it can notify VU_i of successful authentication. Consequently, the schematic diagram of VU_i authentication is shown in Fig. 4.

2.2.3 Trust value calculation

After the registration of identity is completed, the vehicle node may still carry out malicious attacks to destroy the information system of Integrated IoT. In order to solve this problem,

they need to exchange mutual trust values before data is transmitted between vehicles. The calculated trust value will be transmitted by the vehicle to the nearby RSU, and the trust value and other information will be uploaded to the blockchain for storage through the consensus mechanism.

If the two different vehicle users VU_i and VU_o have interacted before, their historical interaction is used for consideration, and the direct trust value can be calculated as

$$\begin{aligned} \mathrm{Vtv}^d = \alpha \frac{\mathrm{Suc}(i,o)}{\mathrm{Suc}(i,o)+\mathrm{Fai}(i,o)} + \beta \frac{\mathrm{Rea}(i,o)}{\mathrm{Suc}(i,o)} \\ - \gamma \frac{\mathrm{Fal}(i,o)}{\mathrm{Suc}(i,o)}, \forall i \in N, \end{aligned} \tag{14}$$

where $Suc(\cdot)$ and $Fai(\cdot)$ are the number of successful and failed communications between VU_i and VU_o in the past. $Rea(\cdot)$ and $Fal(\cdot)$ are the number of times real data and false data are sent during successful communication. α, β and γ are coefficients, which, respectively, reflect the impact on channel state, user situation and false data punishment.

When two vehicle users VU_i and VU_o do not interact directly or the number of interactions is too small, VU_i needs to calculate the indirect trust value by obtaining the trust evaluation of other nodes that interact with VU_o in Integrated IoT. Assuming that there are K vehicles have interacted with VU_i, the expression of indirect trust value of VU_i is

$$Vtv^i = \frac{\sum_{k=1}^{K} Eva(k,i)}{K}, \forall i \in N, \tag{15}$$

where $Eva(\cdot)$ is the evaluation of other vehicles.

Thus, we combine the direct Vtv^d and indirect Vtv^i trust values, and get the calculation expression of the trust value as

$$Vtv = \theta Vtv^d + (1-\theta) Vtv^i, \tag{16}$$

where θ is the weight factor of trust adjustment, which can adjust the proportion of direct trust value and indirect trust value. Then, the vehicle transmits the pseudonym, trust value and timestamp to the nearby RSU to write it into the block.

2.3 Mobile communication model

After the vehicle completes the identity authentication, it can normally transmit data to other vehicles or RSUs. Suppose there are a total of T time slots, and the set is expressed as $\mathcal{T} = \{1, 2, ..., T\}$. Among multiple communication candidates, VU_i selects the one VU_o with the highest trust value to initiate the data transmission request. Two VUs authenticate with each other and form a V2V pair. VU_o sends the required data to VU_i, So VU_o is the transmitter (V2V-S) and VU_i is the receiver (V2V-R).

At time slot t, we mark the coordinates of i-th V2V-S and V2V-R are $(x_{Si}^v(t), y_{Si}^v(t))$ and $(x_{Ri}^v(t), y_{Ri}^v(t))$, respectively. In addition, the RSU_j coordinate communicating with VU_i is marked as $(x_j^r(t), y_j^r(t))$. Next, we use Euclidean distance formula to calculate the distance between the i-th pair of V2V-S and V2V-R as

$$d_i(t) = \sqrt{(x_{Si}^v(t) - x_{Ri}^v(t))^2 + (y_{Si}^v(t) - y_{Ri}^v(t))^2}, \forall i \in N. \tag{17}$$

The channel power gain between the i-th V2V pair is

$$g_i(t) = g_0 \varrho^2 d_i(t)^{-\alpha_p}, \forall i \in N, \tag{18}$$

where g_0 is the channel gain at the reference distance d_0, ϱ represents an exponential distribution random variable with mean value, and α_p is the path loss exponent in V2V link.

There is channel interference when the vehicle communicates with RSU and another vehicle at the same time, and the signal-to-interference-plus-noise ratio (SINR) of i-th VU pair can be calculated as

$$\gamma_i^v(t) = \frac{p_i^v(t) g_i^v(t)}{\sigma^2 + \delta_i p_j^r(t) g_j^{rv_R}(t)}, \forall i \in N, \forall j \in M, \tag{19}$$

where p^v and p^r represent the transmit power of VU pair and RSU, respectively. g_i^v and $g_i^{rv_R}$ denote the channel gain between i-th VU pair link, and RSU_j to $V2V\text{-}R_i$ link, respectively. δ_i is whether VU_i uses V2V and V2I to transmit data at the same time, and σ^2 represents the power of additive white Gaussian noise.

One RSU can serve multiple VUs at the same time, so there is channel interference g_{jl}^{rv} from other VUs when communicating with VU_i. Assuming that RSU_j serves L VUs at the same time, the SINR from RSU_j to $V2V\text{-}R_i$ is

$$\gamma_{ij}^{rv_R}(t) = \frac{p_j^r(t) g_{ij}^{rv_R}(t)}{\sigma^2 + \delta_j \Sigma_{l=1}^{L} p_j^r(t) g_{jl}^{rv}(t)}, \forall j \in N, \forall j \in M, \tag{20}$$

where δ_j is whether RSU_j serves multiple vehicle users. Factor δ represents whether there are multiple users multiplex channel, and the expression is

$$\delta = \begin{cases} 1, & \text{if multiple users multiplex channel,} \\ 0, & \text{otherwise.} \end{cases} \tag{21}$$

Then, we set W_i^v and W_j^r are the bandwidths of VU pair $V2V_i$ and RSU_j, respectively, and $W_{ij}^{rv_R}$ denotes the bandwidth allocated by RSU_j to communicate with $V2V\text{-}R_i$. The transmission rates of the i-th VU pair are

$$R_i^v(t) = W_i^v log_2\left(1 + \gamma_i^v(t)\right), \forall i \in N. \tag{22}$$

Similarly, the transmission rate between RSU_j and $V2V\text{-}R_i$ is

$$R_{ij}^{rv_R}(t) = W_{ij}^{rv_R} log_2\left(1 + \gamma_{ij}^{rv_R}(t)\right), \forall j \in M. \tag{23}$$

We measure the instantaneous data transmission rate of the vehicle once in each time slot, and the calculated $V2V_i$ pair and $RSU_j - V2V\text{-}R_i$ average transmission rates are, respectively,

$$\overline{R_i^v} = \frac{\sum_{t=1}^{T} R_i^v(t)}{T}, \forall i \in N. \tag{24}$$

$$\overline{R_{ij}^{rv_R}} = \frac{\sum_{t=1}^{T} R_{ij}^{rv_R}(t)}{T}, \forall i \in N, \forall j \in M. \tag{25}$$

The data transmission task of the vehicle consists of two parts, from other vehicles and RSU. The two parts are carried out at the same time, which can reduce the overall transmission delay.

Suppose the data size obtained by VU_i from $V2V_i$ and RSU_j are s^v and s^r, respectively, we can calculate the times spent by the $V2V_i$ and RSU_j on the transmission task are

$$t_i^v = \frac{s^v}{\overline{R_i^v}}, \forall i \in N, \tag{26}$$

$$t_i^r = \frac{s^r}{\overline{R_{ij}^{rv_R}}}, \forall i \in N, \forall j \in M. \tag{27}$$

Two parts of data are transmitted at the same time, and the larger value is the final time consumption. Thus, the total time of data transmission task is

$$t_i = \max\left\{t_i^v, t_i^r\right\}, \forall i \in N. \tag{28}$$

2.4 Resources pricing model

The vehicle obtains the data and pays the cost for the provider accordingly. Referring to [39], in order to ensure the rational utilization of resources and good user experience, we propose a pricing scheme based on utilization of bandwidth resources as follows:

$$P^{\text{unit}}(t) = \lambda e^{\mu x(t)} + \omega, \tag{29}$$

where λ is the size of bandwidth allocated to users. $x(t)$ is the independent variable related to the bandwidth resources occupancy rate under slot t, which affects the variation range of unit price. μ affects the rate at which the unit price changes with x, indicating the degree of unit price change. ω denotes the lowest unit price offered by the infrastructure provider. λ and ω jointly determine the initial price of bandwidth resources. And these parameter values are positive.

This function is obviously monotonically increasing. The characteristic of this pricing function is that the higher the server bandwidth resources occupancy rate is, the higher the resource unit price is. Higher resource prices may allow users to choose bandwidth resource from other RSUs or vehicles. When resources utilization is high, this can reduce congestion and help improve the user experience. For vehicles, in addition to the trust value, we also need to consider the resources occupancy rate of the server. Affected by the resources cost, the trust value here needs to be greater than a certain threshold.

Thus, the user cost can be calculated by the bandwidth resources occupation time of other vehicles and RSU

$$P = P^{\text{unit}V} t^v + P^{\text{unit}R} t^r. \tag{30}$$

Combined with blockchain security authentication and vehicle task transmission model, the user cost can be controlled under the premise of ensuring secure communication. It

is assumed that $\frac{N}{2}$ pairs of V2V are formed in the system. Then, the user cost minimization problem in V2X Integrated IoT can be formally expressed as

$$\begin{aligned}
\mathbf{P1}: \quad & \min_{s_i^v, s_i^r, W_i^v, W_{ij}^{rv_R}} \sum_{i=1}^{\frac{N}{2}} P_i \\
s.t. \quad & C1: t_i \leqslant D_i, \forall i \in N/2, \\
& C2: s_i^v + s_i^r \geqslant s_i, \forall i \in N/2, \\
& C3: Vts_{io} \geqslant Vts^{base}, \forall i \in N/2, \\
& C4: \delta_{ij} \leqslant 1, \forall i \in N/2, \forall j \in M, \\
& C5: W^{min} \leqslant W_{ij}^{rv_R} \leqslant W^{max}, \forall i \in N/2, \\
& C6: \sum W_i^v \leqslant W^v, \forall i \in N/2, \\
& C7: \sum W_{ij}^{rv_R} \leqslant W_j^r, \forall i \in N/2, \forall j \in M.
\end{aligned} \tag{31}$$

where $C1$ represents that the total delay for VU_i to complete the transmission task does not exceed the tolerable delay. $C2$ ensures that the data obtained from RSU and V2V can form a complete file. $C3$ represents that the trust value of both vehicles constituting V2V is greater than the threshold. $C4$ indicates that one VU is paired with at most one RSU and another vehicle. $C5$ represents that the bandwidth allocated by RSU to single vehicle is limited. $C6$ illustrates that the total bandwidth of V2V pairs is limited. And $C7$ means that the bandwidth allocated by each RSU to the service VU is limited.

3 Proposed solution scheme

In this section, we solve the problem of minimizing the transmission cost of user tasks. According to the characteristics of the decision variables and constraints of the problem, it can be solved in three parts: the vehicle and RSU that meet the constraints $C3$, $C4$ to communicate with VU; the bandwidth resources allocation that meets the constraints $C5$, $C6$, $C7$; and the decomposition of two-way data transmission that meets the constraints $C1$, $C2$.

3.1 Identity authentication matching

Due to delay sensitivity, vehicle tasks can be obtained directly from other vehicles or RSUs to reduce transmission delay. Before they establish transmission links, in order to ensure data security, they need to authenticate each other's identities and select vehicles with better channel resources that meet the constraint $C3$, $C4$ to form a pair.

The environment is initialized, and the CA, that is gNB, registers the RSU and vehicle entering the system for the first time. As shown in Equ. (2), RSU sends its own ID and random number information to CA, and the latter returns certificate, private key, public key and registration timestamp to complete registration according to Equ. (6). Then, the role of RSU is determined refer to Equ. (7). And the leader who manages blockchain is elected in each term.

Similarly, according to Equ. (8) and (12), the vehicle ready for registration provides its own ID and application timestamp to the CA, which returns the information including private key, public key, pseudonym, certificate and initial trust value

to complete the registration. Next, the important parameter trust value of vehicle matching communication is generated according to Equ. (16).

Refer to Equ. (13), the vehicle or RSU to be communicated needs to complete the identity authentication with digest and signature. For the VU, he hopes that the vehicle matching the communication has a better channel environment to obtain a higher network speed. According to Equ. (14), the trust value, that takes into account the channel environment, is an appropriate reference index, so the VU selects the vehicle with the highest trust value in the current time slot to match into a V2V pair. Our optimization goal is to reduce user costs, and the resources pricing function is related to the server resources occupancy. Thus within the communication coverage, the RSU with the lowest server resources occupancy is paired with the V2I of the vehicle. And we proposed Blockchain-based Vehicle Identity Authentication (BVIA) algorithm is shown in Alg. A1.

3.2 Task decomposition and bandwidth allocation

Based on the decision variables are multidimensional, we originally intended to use Deep Reinforcement Learning (DRL) or Genetic Evolution Algorithm (GEA) to solve the sub-problem of bandwidth allocation, in which the optimization goal of problem **P1** is the reward function of DRL or the fitness function of GEA, so we need to get the decomposition amount of transmitted data first. In fact, the transmission task decomposition needs to meet the tolerable delay requirements, and the transmission rate is the key index, but the premise is to find out the bandwidth allocation strategy according to Equ. (22). Thus, DRL or GEA algorithm leads to the coupling of two sub-problems, and they are not suitable to solve problem **P1**.

Algorithm 1 Blockchain based Vehicle Identity Authentication (BVIA) Algorithm

Require: Vehicle and RSU initial information in Integrated IoT.

Ensure: Vehicle trust value Vtu in Integrated IoT.

1: Initialize the Integrated IoT environment;
2: Stage 1: RSUs and Vehicles registration.
3: RSUs send their own ID Rid and random number Rk to CA according to Equ.(2);
4: CA returns certificate Rc, private key Rpr, public key Rpu and registration timestamp Rts to RSUs according to Equ.(6);
5: Refer to Equ.(7), the role of RSUs are determined, and the blockchain leader is elected in each term;
6: Vehicles provide their own ID Vid and application timestamp Vts to the CA for registration according to Equ.(8);
7: CA returns private key Vpr, public key Vpr, pseudonym Vpd, certificate Vc and initial trust value Vtv^{init} to vehicles according to Equ.(12);
8: Stage 2: Communication identity authentication.
9: Refer to Equ.(13), the vehicle or RSU to be communicated needs to complete the identity authentication with digest Vd and signature Vs;
10: Trust value Vtu of the vehicle is generated according to Equ.(16);
11: VUs match the vehicle with the highest trust value and the RSU with the lowest resource occupancy within the signal range.

In order to solve the coupling problem, we treat every VU in V2X Integrated IoT as equal, when the bandwidth resources is allocated. Meanwhile, the delay requirement of each transmission task is taken into account. Consequently, based on the improved max-min fairness algorithm, we proposed Delay Weight Fairness Bandwidth Allocation (DWFBA) algorithm is shown in Alg. 2.

In the problem of dynamic task transmission in V2X Integrated IoT, we lock the unit that processes the task each time to a slot. In this time slot, the total amount of bandwidth resources is certain, which meets the constraints *C*5, *C*6, *C*7. Turn the task into two-dimensional variables $< Ur_i, Ud_i >$, where Ur_i and Ud_i are the required bandwidth resources and delay weight of the *i*-th V2V, respectively.

The problem solved by DWFBA algorithm needs to meet three conditions:

- The order of allocating bandwidth resources is arranged according to the increasing demand, and the number of allocated resources is determined according to the delay weight.
- If some vehicle users get more resources than their own needs, the more resources will be allocated to other users who do not meet their needs.
- Unsatisfied vehicle users allocate resources for the second time according to the delay weight.

Algorithm 2 Delay Weight Fairness Bandwidth Allocation (DWFBA) Algorithm

Require: Coordinates and trust values Vtv_i of Vehicles at time slot t; Task complexity factor δ_i, data size S_i and tolerable delay D_i of VU_i.

Ensure: Total bandwidth cost of vehicles ΣP_i.

1: According to Equ.(34), the bandwidth resource requirements of each VU are determined and the queue $< Ur_i >$ is arranged in ascending order.
2: The weight queue $< Ud_i >$ is sorted according to the order of the resource queue, according to Equ.(37);
3: **while** Number of cycles not reached **do**
4: The amount of resource per-weight is calculated according to Equ.(38) ;
5: Bandwidth resources are allocated to VUs according to the delay weight;
6: **if** the amount of resources allocated is not less than the demand **then**
7: The extra resources are collected for the next round of allocation to unsatisfied VUs;
8: **else**
9: Unsatisfied VUs are marked;
10: **end if**
11: **if** there are no remaining resources or VUs have completed resource allocation **then**
12: break;
13: **end if**
14: **end while**
15: Total cost ΣP_i of VUs is calculated according to Equ.(30).

According to this principle, if the unit price of V2V is cheaper, first determine the amount of data that V2V can complete within the tolerable delay, and the rest is transmitted by V2I. In this way, the expected amount of data transmitted by V2V channel of VU_i is

$$s_i^v = R_i^v D_i, \forall i \in N/2, \tag{32}$$

And the expected amount of data transmitted by V2I channel of VU_i is

$$s_{ij}^r = S_i - s_i^v, \forall i \in N/2, \forall j \in M. \tag{33}$$

It is worth noting that the tolerable delay decreases as the time slot advances. At time slot t, the amount of resources requested by VU_i is

$$Ur_i(t) = \frac{s_{ij}^r}{D_i(t) log_2\left(1 + \gamma_{ij}^{rv_R}(t)\right)}, \forall i \in N/2, \forall j \in M. \tag{34}$$

Firstly, we focus on the resources required queue $< Ur_i >$ and delay weight queue $< Ud_i >$ of VUs.

Here, we decompose the transmission task to determine $< Ur_i >$, and satisfy the constraints $C1$, $C2$ at the same time. We set the bandwidth W_i^v of V2V to a fixed value, and consider the bandwidth allocation of RSU. For VUs, there are two transmission channels, V2V and V2I. Our goal is to control user costs, so the RSU and the vehicle with cheaper resources should be fully utilized first, and the part of task beyond the delay range should be completed by another device.

On the contrary, if the unit price of V2I is cheaper, V2I channel needs to be used as much as possible, and the expected task volume should be the size of the whole task. If it fails to meet the requirements, the part that cannot be completed will be transmitted by V2V. So, the expected amount of data transmitted by V2V channel is

$$s_{ij}^r = S_i, \forall i \in N/2, \forall j \in M. \tag{35}$$

Then, the amount of resources requested by VU_i is same as Equ. (34). If V2I fails to complete the transmission task within the tolerable delay, the expected amount of data transmitted by V2V channel of VU_i is

$$s_i^v = S_i - s_{ij}^r, \forall i \in N/2. \tag{36}$$

Because the greater the tolerable delay, the lower the urgency of the task. Thus, we take the reciprocal of the delay as the weight to make the urgent task get more resources. Then, the delay weight queue $< \mathrm{Ud}_i >$ expression of $V2V_i$ is

$$\mathrm{Ud}_i(t) = \frac{1}{D_i(t)}, \forall i \in N/2. \tag{37}$$

Specifically, the demand queue of VUs under slot t is arranged in ascending order, and the corresponding weight queue is adjusted. The bandwidth resource amount of each weight is calculated as

$$Ur^{\mathrm{avg}}(t) = \frac{\mathrm{Ur}^{\mathrm{total}}(t)}{\mathrm{Ud}^{\mathrm{total}}(t)}, \tag{38}$$

where $\mathrm{Ur}^{\mathrm{total}}$ and $\mathrm{Ud}^{\mathrm{total}}$ are the total amount of remaining resource and the total weight of VUs in slot t, respectively.

The RSU bandwidth resource in the first round are allocated, according to the delay weight. If some vehicle users get more resources than their own needs, the system collects the extra resources and assigns them with weight to the unsatisfied VUs in the next round, and cycles until the resources are used up.

4 Simulation results

In this section, we give the simulation results of algorithms *BVIA* and *DWFBA*, and analyze their performance through comparative experiments. First, we set a variety of parameter combinations to find the appropriate direct and indirect trust values, as well as the parameters of the pricing model. Then, we compare the bandwidth overhead of *BVIA* and the other two blockchain authentication algorithms, and observe that our proposed algorithm is more stable and has lower overhead. Finally, compared with greedy algorithm and random algorithm, we verify the controllability of *DWFBA* algorithm in user cumulative cost and the number of failed tasks. Refer to [40, 41], and some parameters are listed in Table 1.

4.1 Parameters analysis

Firstly, we analyze the four parameters of trust value. Among them, α, β and γ affect the channel quality, message quality and false message penalty weight of direct trust value, respectively. Parameter θ is the weight of direct and indirect trust value, which affects whether users pay more attention to historical direct communication scores or scores from others.

In order to find the best parameter setting, we compare four groups of data with the experimental set. According to Equ. (14), we calculate the success, failure, real, false times and indirect trust values of the four groups of interactive message data, as shown in Table 2. These four groups of data represent four communication situations, that is, good channel sends more real data, good channel sends more false data, poor channels sends more real data and poor channels send more false data, and they are marked as Data A, B, C and D.

The four parameter schemes in which each parameter is significantly considered are shown in Table 3. Then, these four schemes are named Set1, Set2, Set3 and Set4,

Table 1 Simulation parameters

Parameter	Value
Transmission power p^c of a single CU	20dBm
Transmission power p^v of a V2V pair	25dBm
Power of Gaussian white noise σ^2	-118dBm
Single RSU total bandwidth W^r	100MHz
Max-bandwidth W^{max} RSU to a vehicle	20MHz
Bandwidth allocated W^v to V2V pair	10MHz
Vehicle speed	60km/h
The number of voting nodes N_v	500
The number of consensus nodes N_c	[0,20]
Size of block $Size_{block}$	1024KB
Size of vote data $Size_{vote}$	0.25KB

Table 2 Data status in each experiment(Unit:times or points)

Data	Suc.	Fai.	Rea.	Fal.	Indirect Tru.
Data A	82	28	68	14	1.325
Data B	34	66	26	8	0.837
Data C	82	28	14	68	0.462
Data D	34	66	8	26	0.112

Table 3 Direct trust value parameters in each experiment

Set	α	β	γ
Set1	1	1	1
Set2	1.2	1	1.5
Set3	1	1.2	1.5
Set4	1.8	1.2	1.5

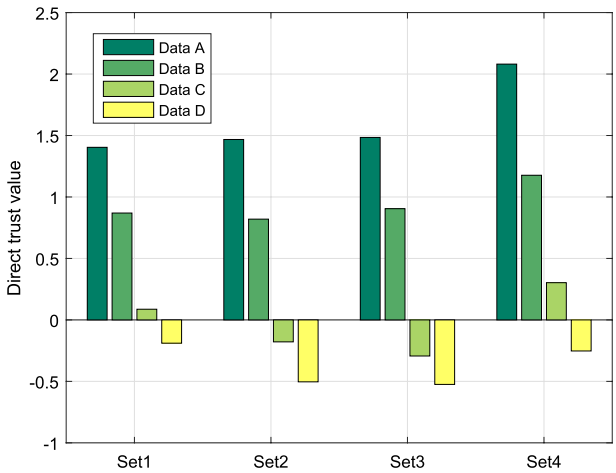

Fig. 5 Comparison of direct trust values under different parameters

respectively. Here, Set1 balances the parameters. Set2 pays attention to channel quality and large false data penalty. Set3 focuses more on the authenticity of data sent by users. In Set4, the channel quality weight is greater than the penalty weight, and other parameters are similar to Set3.

Now, we analyze the three parameters α, β, γ of the direct trust value, and the direct trust values under different parameter schemes are shown in Fig. 5. In these four cases, the groups that send false data should not have a positive score, and the group with better channel will get a higher score. According to this principle, Set1 and Set4 are eliminated because the Data C score is positive. There is a small difference between Set2 and Set3, but Set3 score is more differentiated, we choose Set3 configuration to set the parameters of direct trust value.

Then, as shown in Fig. 6, we compare the comprehensive trust values under different parameter θ in V2X Integrated IoT. Based on the parameters of the direct trust value Set3, the indirect trust value is added to analyze the parameter of the comprehensive

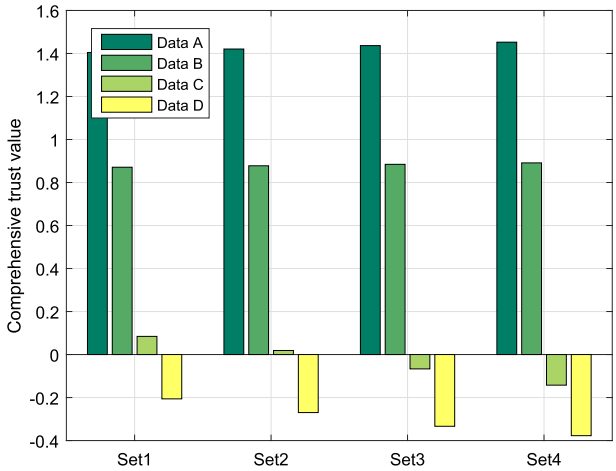

Fig. 6 Comparison of comprehensive trust values under different parameter

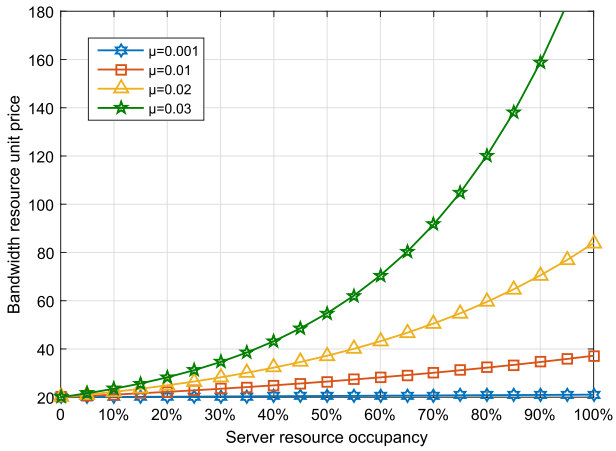

Fig. 7 Comparison of resource unit price under different parameters

trust value. The parameter θ in each experiment Set is set as 0.5, 0.6, 0.7 and 0.8, respectively. According to the screening principle, Set1 and Set2 do not meet the condition that the Data C should be negative, and Set4 has a slightly larger discrimination than Set3, so we set the parameter θ as 0.8.

Next, we analyze the parameters μ and ω of the resource pricing model in V2X Integrated IoT. According to Equ. (29), we fix the bandwidth $\lambda = 10MHz$ to make the resource occupancy x from 0 to 100%, and observe the change trend of bandwidth resources unit price under the four values of μ. When the server resources are too busy, the price of the exponential pricing scheme rises faster, which helps guide users to choose another server, and balance the load pressure among multiple servers.

It can be seen from Fig. 7 that the unit price of schemes μ=0.001 and μ=0.01 increases slowly when the resource occupation rate is large, which is not conducive to relieving the pressure on the server. On the whole, scheme μ=0.03 rises rapidly, which is difficult for users to accept. In order to balance the interests of the network operator and users, we choose a moderate parameter setting scheme μ=0.02. In addition, ω affects the function

to move up and down, which is set as 10 here, and works together with λ to make the Y-axis of the image start from 20.

4.2 Performance comparison

Our optimization goal is to control user costs, and bandwidth overhead is an important factor. We apply three methods to compare the bandwidth overhead of different consensus algorithms in V2X Integrated IoT. These three algorithms are *BVIA*, *PBFT* and *PoW*. Among them, *BVIA* is our proposed Blockchain IoT authentication algorithm, which is based on RAFT algorithm in terms of election and consensus, and generates broadband overhead in both two aspects. Specifically, the election includes two stages: request and response for votes, and consensus includes four stages: client request, leader forward, nodes response and leader reply. Then, the bandwidth overhead of *BVIA* is defined as

$$\begin{aligned} rmBO_{\mathrm{BVIA}} &= N_v(N_v-1)+N_v(N_v-1)\mathrm{Size}_{\mathrm{block}} \\ &\quad +(1+N_c+N_c+1)\mathrm{Size}_{\mathrm{vote}} \\ &= 2\Big((N_v^2-N_v)\mathrm{Size}_{\mathrm{block}}+(N_c+1)\mathrm{Size}_{\mathrm{vote}}\Big) \end{aligned} \tag{39}$$

where N_v and N_c are the number of voting nodes and consensus nodes, respectively, $Size_{block}$ and $Size_{vote}$, respectively, are the size of block and voting data.

PBFT algorithm has only consensus, and its four stages include request, pre-prepare, prepare, commit and reply. Its bandwidth overhead is defined as

$$\begin{aligned} BO_{PBFT} &= (1+(N_c-1)+(N_c-1)(N_c-1) \\ &\quad +N_c(N_c-1)+N_c)Size_{block} \\ &= (2N_c^2-N_c+1)Size_{block} \end{aligned} \tag{40}$$

Similarly, *PoW* algorithm has only consensus, which is divided into two stages: broadcast transaction and broadcast block, and its bandwidth overhead is

$$\begin{aligned} BO_{PoW} &= (N_c-1)(N_c-1)Size_{block} \\ &= (N_c^2-2N_c+1)Size_{block} \end{aligned} \tag{41}$$

Thus, it can be seen that the bandwidth overhead of algorithm *BVIA* is mainly in election, and the overhead of algorithm *PBFT* and *PoW* is mainly in consensus.

The experimental results of Fig. 8 are completed with voting nodes size $N_v = 500$ ($N_v \gg N_c$). The bandwidth overhead of algorithm *BVIA* is mainly in election, so it is significantly higher than that of the other two algorithms when there are few consensus nodes. Because the election voting data is much smaller than the block data, with the increase in consensus nodes, the overhead of algorithm *PBFT* and *PoW* gradually increases and exceeds that of algorithm *BVIA*.

The time complexity of algorithm *BVIA* is o(n), and the maximum fault-tolerant node supported is (n-1)/2, while the time complexity of algorithm *PBFT* is o(n^2), and the maximum fault-tolerant node supported is (n-1)/3. In these two indicators, algorithm *BVIA* is better than *PBFT*. Algorithm *PoW* has the disadvantage of wasting resources and time due to its mine and account mechanism. According to the experimental results, algorithm *BVIA* is more suitable for the mobility and latency in V2X Integrated IoT when

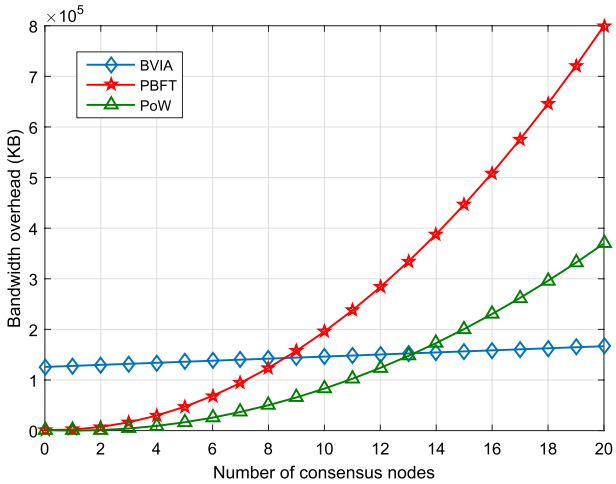

Fig. 8 Comparison of bandwidth overhead of different consensus algorithms

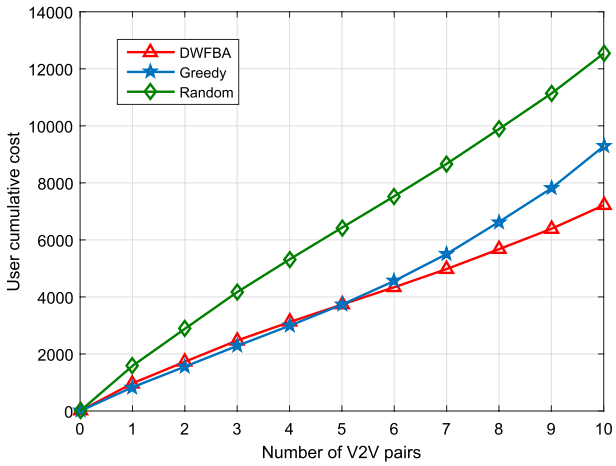

Fig. 9 Compare the number of failed tasks of different algorithms

there are many consensus nodes. Compared with algorithms *PBFT* and *PoW*, it can save 55.49% and 17.62% bandwidth overhead on average, respectively.

Next, we verify the performance of three algorithms for controlling user cost through simulation experiments in V2X Integrated IoT. These three algorithms are *DWFBA* algorithm we proposed, *Greedy* algorithm that pays attention to the current benefit and *Random* allocation algorithm.

Figure 9 shows the trend of the user cumulative cost with the growth of the number of user pairs in V2X Integrated IoT. *Random* algorithm allocates more random bandwidth, which leads to poor performance and makes it difficult to control user cost. *Greedy* algorithm focuses more on current benefit and performs better in the early stages when V2V pairs is less. But *Greedy* algorithm is easy to fall into local optimal solution with the increase in Integrated IoT V2V users, and the user cumulative cost gradually exceeds that of *DWFBA* algorithm. Moreover, *DWFBA* algorithm considers the long-term benefit, and the performance gradually reflects after the increase

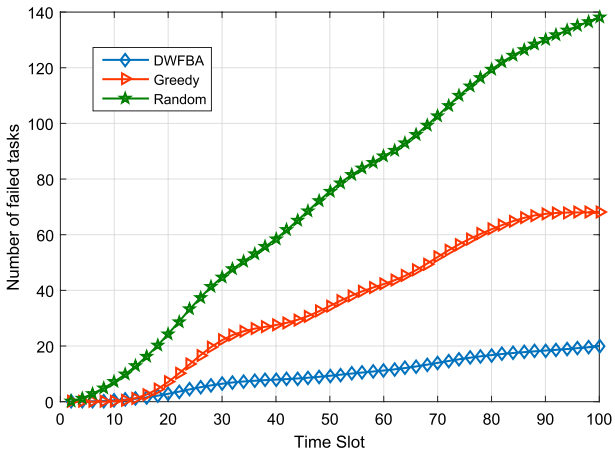

Fig. 10 Compare the number of failed tasks of different algorithms

in users. It keeps the distance from the other two algorithms in terms of cost control. Compared to algorithms *Greedy* and *Random*, *DWFBA* is able to, respectively, save 22.28% and 42.45% of user cumulative cost in the case of more users in V2X Integrated IoT.

Finally, we compare the long-term effects of the three algorithms to finish the transmission task in V2X Integrated IoT. The vehicles drive fast and the transmission tasks is delay sensitive, so it is still possible to fail to complete the transmission task. We, respectively, apply algorithms *DWFBA*, *Greedy* and *Random* to observe the number of failed tasks.

As shown in Fig. 10, the number of failed tasks of the three algorithms increases with the increase in time slots in V2X Integrated IoT. Due to its randomness, *Random* allocation algorithm shows poor performance, and the number of failed tasks grows rapidly out of control. *Greedy* algorithm has local optimality, which shows that the first 20 time slots perform well, and the subsequent defects gradually appear, with general performance. Different from these two algorithms, our proposed *DWFBA* algorithm considers long-term benefits. The resource allocation principle is based on weighted delay, and the urgency of the task is met. Meanwhile, it can maximize the resource fairness of unfinished tasks, and the performance is relatively stable. In addition, the task failure rate is much lower than the other two algorithms in V2X Integrated IoT.

5 Conclusion

In this paper, we study the cost of V2V users to complete the transmission task in Integrated IoT with blockchain identity authentication. In order to solve this problem, we propose a task transmission scheme with identity registration and authentication. In this scheme, *BVIA* algorithm is used to authenticate the equipment in V2X Integrated IoT and calculate the vehicle trust value to ensure the legitimacy of users. Then, we combine V2V and V2I, and apply *DWFBA* algorithm to solve the task transmission strategy to minimize vehicle users cost to complete the transmission task. Simulation results show

that compared with the other two algorithms, our proposed algorithm can reduce the number of transmission failed tasks and save users' cumulative cost.

Acknowledgements
Not applicable.

Author contributions
The authors equally contributed to the paper. All authors read and approved the final manuscript.

Funding
Not applicable.

Data Availability
Please contact author for data requests.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
The picture materials quoted in this article have no copyright requirements, and the source has been indicated.

Competing interest
The authors declare that they have no competing interests.

Received: 1 September 2023 Accepted: 20 October 2023
Published online: 09 November 2023

References

1. X. Cheng, Z. Huang, S. Chen, IOT security privacy protection mechanism and mechanical structure design simulation optimization. EURASIP J. Adv. Signal Process. **2021**(52), 1–14 (2021)
2. K. Sehla, T.M.T. Nguyen, G. Pujolle, P.B. Velloso, Resource allocation modes in C-V2X: from LTE-V2X to 5G–V2X. IEEE Internet Things J. **9**(11), 8291–8314 (2022)
3. V. Maglogiannis, D. Naudts, S. Hadiwardoyo, D. van den Akker, J. Marquez-Barja, I. Moerman, Experimental V2X evaluation for C-V2X and ITS-G5 technologies in a real-life highway environment. IEEE Trans. Netw. Serv. Manag. **19**(2), 1521–1538 (2022)
4. W.-D. Shen, H.-Y. Wei, Distributed V2X sidelink communications with receiver grant MAC design. IEEE Trans. Veh. Technol. **71**(5), 5415–5429 (2022)
5. Y. Saleem, N. Mitton, V. Loscri, A QoS-Aware Hybrid V2I and V2V Data Offloading for Vehicular Networks, 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), (2021)
6. M. Sepulcre, J. Gozalvez, Heterogeneous V2V communications in multi-link and multi-rat vehicular networks. IEEE Trans. Mob. Comput. **20**(1), 162–173 (2021)
7. X. Liu, Z. Xu, Y. Meng, W. Wang, J. Xie, Y. Li, An elastic-segment-based V2V/V2I cooperative strategy for throughput enhancement. IEEE Trans. Veh. Technol. **71**(5), 5272–5283 (2022)
8. B.L. Nguyen, D.T. Ngo, N.H. Tran, M.N. Dao, H.L. Vu, Dynamic V2I/V2V cooperative scheme for connectivity and throughput enhancement. IEEE Trans. Intel. Transp. Syst. **23**(2), 1236–1246 (2022)
9. L. Su, Y. Niu, Z. Han, B. Ai, R. He, Content distribution based on joint V2I and V2V scheduling in mmWave vehicular networks. IEEE Trans. Veh. Technol. **71**(3), 3201–3213 (2022)
10. H. Yahya, A. Al-Dweik, Y. Iraqi, E. Alsusa, A. Ahmed, A power and spectrum efficient uplink transmission scheme for QoS-constrained IoT networks. IEEE Internet Things J. **9**(18), 17425–17439 (2022)
11. S. Guo, B.-J. Hu, Q. Wen, Joint resource allocation and power control for full-duplex V2I communication in high-density vehicular network. IEEE Trans. Wirel. Commun. **21**(11), 9497–9508 (2022)
12. L. Xu, M. Ge, W. Wu, Edge server deployment scheme of blockchain in IoVs. IEEE Trans. Reliab. **71**(1), 500–509 (2022)
13. M.B. Mollah et al., Blockchain for the internet of vehicles towards intelligent transportation systems: a survey. IEEE Internet Things J. **8**(6), 4157–4185 (2021)
14. L. Vishwakarma, A. Nahar, D. Das, LBSV: lightweight blockchain security protocol for secure storage and communication in SDN-enabled IoV. IEEE Trans. Veh. Technol. **71**(6), 5983–5994 (2022)
15. S. Son, J. Lee, Y. Park, Y. Park, A.K. Das, Design of blockchain-based lightweight V2I handover authentication protocol for VANET. IEEE Trans. Netw. Sci. Eng. **9**(3), 1346–1358 (2022)
16. H. Cheng, Q. Hu, X. Zhang, Z. Yu, Y. Yang, N. Xiong, Trusted resource allocation based on smart contracts for blockchain-enabled internet of things. IEEE Internet Things J. **9**(11), 7904–7915 (2022)
17. L. Wei, J. Cui, H. Zhong, Y. Xu, L. Liu, Proven secure tree-based authenticated key agreement for securing V2V and V2I communications in VANETs. IEEE Trans. Mobile Comput. **21**(9), 3280–3297 (2021)
18. J. Cui, F. Ouyang, Z. Ying, L. Wei, H. Zhong, Secure and efficient data sharing among vehicles based on consortium blockchain. IEEE Trans. Intel. Transp. Syst. **23**(7), 8857–8867 (2022)
19. J. Shi, J. Du, Y. Shen, J. Wang, J. Yuan, Z. Han, DRL-based V2V computation offloading for blockchain-enabled vehicular networks. IEEE Trans. Mobile Comput. (2022). https://doi.org/10.1109/TMC.2022.3153346

20. H.N. Abishu, A.M. Seid, Y.H. Yacob, T. Ayall, G. Sun, G. Liu, Consensus mechanism for blockchain-enabled vehicle-to-vehicle energy trading in the internet of electric vehicles. IEEE Trans. Veh. Technol. **71**(1), 946–960 (2022)
21. C. Roy, S. Misra, J. Maiti, F. Nait-Abdesselam, Diff-Price: differential pricing scheme for provisioning safety-as-a-service in vehicular IoT applications. IEEE Trans. Veh. Technol. **71**(8), 8189–8198 (2022)
22. K.M.K. Ramamoorthy, W. Wang, A QoE-driven pricing scheme for inter-vehicular communications with four-stage Stackelberg game. IEEE Trans. Veh. Technol. **71**(3), 3121–3130 (2022)
23. M. Tao, K. Ota, M. Dong, H. Yuan, Stackelberg game-based pricing and offloading in mobile edge computing. IEEE Wirel. Commun. Lett. **11**(5), 883–887 (2022)
24. X. Wang, Z. Ning, L. Guo, S. Guo, X. Gao, G. Wang, Mean-field learning for edge computing in mobile blockchain networks. IEEE Trans. Mobile Comput. (2022). https://doi.org/10.1109/TMC.2022.3186699
25. Z. Ning, S. Sun, X. Wang, L. Guo, S. Guo, Blockchain-enabled intelligent transportation systems: a distributed crowd-sensing framework. IEEE Trans. Mobile Comput. **21**(12), 4201–4217 (2022)
26. Z. Ning, S. Sun, X. Wang, L. Guo, G. Wang, Intelligent resource allocation in mobile blockchain for privacy and security transactions: a deep reinforcement learning based approach. Sci. China Inf. Sci. **64**(6), 168–183 (2021)
27. M. Siew, D. Cai, L. Li, T.Q.S. Quek, Dynamic pricing for resource-quota sharing in multi-access edge computing. IEEE Trans. Netw. Sci. Eng. **7**(4), 2901–2912 (2020)
28. M. Siew, D. Cai, L. Li, T. Q. S. Quek, A sharing-economy inspired pricing mechanism for multi-access edge computing, GLOBECOM 2020 - 2020 IEEE Global Communications Conference, (2020), 1-6
29. Y. Yang, Z. Liu, Z. Liu, Y. Xie, K.Y. Chan, X. Guan, Joint optimization of edge computing resource pricing and wireless caching for blockchain-driven networks. IEEE Trans. Veh. Technol. **71**(6), 6661–6670 (2022)
30. Z. Jing, Q. Yang, M. Qin, J. Li, K.S. Kwak, Long-term max-min fairness guarantee mechanism for integrated multi-RAT and MEC networks. IEEE Trans. Veh. Technol. **70**(3), 2478–2492 (2021)
31. L. Shi, Y. Ye, G. Zheng, G. Lu, Computational EE fairness in backscatter-assisted wireless powered MEC networks. IEEE Wirel. Commun. Lett. **10**(5), 1088–1092 (2021)
32. Y. Ye, L. Shi, X. Chu, G. Lu, Throughput fairness guarantee in wireless powered backscatter communications With HTT. IEEE Wirel. Commun. Lett. **10**(3), 449–453 (2021)
33. A. Ahmadian, W. Shin, H. Park, Max-min throughput optimization in FDD multiantenna wirelessly powered IoT networks. IEEE Internet Things J. **8**(7), 5866–5880 (2021)
34. X.B. Zhai, X. Liu, C. Zhu, K. Zhu, B. Chen, Fast admission control and power optimization with adaptive rates for communication fairness in wireless networks. IEEE Trans. Mobile Comput. **20**(3), 1017–1026 (2021)
35. A. Gupta, D. N. Amudala, E. Sharma, R. Budhiraja, Max-min fairness for wireless-powered spatially correlated massive mimo multi-way relaying, ICC 2021 - IEEE International Conference on Communications, (2021)
36. Y. Wu, J. Wu, L. Chen, J. Yan, Y. Han, Load balance guaranteed vehicle-to-vehicle computation offloading for min-max fairness in VANETs. IEEE Trans. Intell. Transp. Syst. **23**(8), 11994–12013 (2021)
37. J. Feng, L. Liu, Q. Pei, K. Li, Min-max cost optimization for efficient hierarchical federated learning in wireless edge networks. IEEE Trans. Parallel Distrib. Syst. **33**(11), 2687–2700 (2022)
38. O.A. Amodu, M. Othman, N.K. Noordin, I. Ahmad, A primer on design aspects, recent advances, and challenges in cellular device-to-device communication. Ad Hoc Netw. **94**, 101938 (2019)
39. Y. Liang, X. Chen, T. Ma, S. Ma, L. Jiao, Power Control and Evolutionary Strategy Based Slicing Resource Allocation for V2V Communication, 2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS), (2021), 96-101
40. A. Kumar, D. Das, EIoVChain: towards authentication and secure communication based blockchain for internet of vehicles (IoV). IEEE Int. Conf. Blockchain (Blockchain) **2021**, 47–54 (2021)
41. S. Raza, S. Wang, M. Ahmed, M.R. Anwar, M.A. Mirza, W.U. Khan, Task offloading and resource allocation for IoV using 5G NR-V2X communication. IEEE Internet Things J. **9**(13), 10397–10410 (2022)

Publisher's Note