Peer-to-Peer Networking and Applications (2023) 16:554–570
https://doi.org/10.1007/s12083-022-01432-2

Blockchain-enabled solution for secure and scalable V2V video content dissemination

Hang Shen[1] · Xin Liu[1] · Ning Shi[2] · Tianjing Wang[1] · Guangwei Bai[1]

Received: 26 April 2022 / Accepted: 29 November 2022 / Published online: 17 December 2022

Abstract
Vehicle-to-vehicle (V2V) video content dissemination is fundamental for many emerging services (e.g., on-road entertainment and roadside surveillance). However, many security, privacy, and trust issues hinder the large-scale promotion of this service. Malicious entities may spread incomplete and illegal content or defraud the requester to obtain rewards. Moreover, resource consumption and possible privacy leakage issues decrease the participation of many vehicle users. To address these issues, we propose a blockchain-based trust and scalable V2V video content dissemination framework to create an excellent content caching and sharing ecosystem with resistance to diverse attacks and adaptation to high mobility. Under a decentralized framework, a fair reward strategy is designed to price each video content transaction as a V2V service fee. A vehicle-group selection policy for many-to-one video content delivery is developed to minimize service fees subject to the constraints of the number of video layers, vehicle reputation, V2V connection duration, and achievable transmission rate. Smart contracts are designed to regulate transaction triggering, verification, and rewards, with a traceable punishment mechanism against malicious behaviors. We provide the proposed scheme's security analysis and simulation results, demonstrating our scheme's security, feasibility, and superiority.

Keywords Video content dissemination · Blockchain · Trustworthy · Security · Privacy preservation · V2V communication

1 Introduction

The fifth-generation (5G) mobile networks can provide a high capacity to support bandwidth-intensive video applications [1]. One of the most promising 5G cases that shape and revolutionize transportation systems is cellular vehicle-to-everything (C-V2X), a key enabling technology for Internet-of-Vehicles (IoV) [2]. V2V communications refer to data dissemination among vehicles where vehicles are equipped with on-board units (OBUs) and exchange information with each other via direct C-V2X or the dedicated short-range communication (DSRC) technology. The former allows physically similar vehicles to communicate directly via a licensed cellular band, bypassing base stations (BSs) [3]. Compared to DSRC, C-V2X/V2V can achieve higher data rates and longer transmission ranges [4].

In the 5G era, data traffic produced by video-rich services has been predominant in IoV [1, 5]. Video content dissemination among cars enables innovative services, such as on-road video entertainment and roadside surveillance. Video services are resource-consuming with large file volumes, long transmission duration, with strict quality-of-service (QoS) demands. Supporting stable video transmission quality over IoV raises challenges to service and resource provisioning. Due to the scarcity of communication and computing resources, relying solely on cellular infrastructure cannot support large-scale vehicular video delivery. Moreover, because of limited BS coverage and the high-speed movement of vehicles, conventional vehicle-to-infrastructure

✉ Tianjing Wang
wangtianjing@njtech.edu.cn

Hang Shen
hshen@njtech.edu.cn

Xin Liu
liuxin990224@njtech.edu.cn

Ning Shi
shining@newspiral.net

Guangwei Bai
bai@njtech.edu.cn

[1] College of Computer Science and Technology, Nanjing Tech University, Nanjing 211816, China

[2] Nanjing Trusted Blockchain and Algorithm Economics Institute, Nanjing 211899, China

communication may generate frequent video freezing resulting from frequent reconnections.

Scalable video coding (SVC) [6] offers a layered approach to scalability. This technique can encode video data frames into multiple layers, consisting of a base layer of low-quality video and multiple enhancement layers representing the same video with gradually increased quality. The video layers are dynamically adjusted to accommodate channel conditions or quality requirements. SVC-based V2V video content delivery advances in 1) Layered V2V video delivery improves the elasticity of video distribution, which can satisfy strict video quality level requirements; 2) Exchanging video content among vehicles helps reduce the network infrastructure load and extend the coverage scope of video content services; 3) SVC-enabled many-to-one collaboration helps decrease content delivery delay and improve reliability [7].

SVC-based V2V video delivery depends on collaboration, in which many security, privacy, and trust issues exist that may destroy the network ecology for financial gain [8]. First, connected vehicles are vulnerable to Sybil attacks subverted by forging identities in peer-to-peer networks [9], and potential attackers may collude with cars to obtain transaction records and speculate on sensitive information (e.g., interest preferences [10] and account [11]) for drivers, causing some customers to refuse to participate in video caching and distribution. Second, malicious vehicles may tamper with video content or spread incomplete content without content detection and tracking [12], destroying the ecology of V2V mutual assistance. Third, V2V video distribution requires vehicles to contribute a certain amount of cache space and communication resources. Thus, designing an effective reward and punishment mechanism is essential to incentivize more users to participate in V2V distribution.

Conventional centralized security management has low storage efficiency, vulnerability to attacks, and poor credibility and thus fails to adapt to large-scale V2V content distribution scenarios. Blockchain is a distributed, immutable database that stores transactional records, i.e., blocks in several databases, known as the "chain", in a peer-to-peer (P2P) network. The decentralized, tamper-resistant, and traceable feature regulates participants' behavior and ensures reliable content delivery over IoV [13, 14]. Smart contracts [15] on a blockchain network permit trusted transactions and agreements to be executed among disparate, anonymous parties and transform them into some final state. As is closely associated with infrastructure since its birth, blockchain can facilitate secure content and delivery, consensus computing, and trust verification in IoV [16, 17].

1.1 Related works

Investigators have proposed blockchain-based content dissemination schemes and corresponding security mechanisms that prevent identity theft, cyberattacks, or criminality in transactions [18]. Li et al. develops a trust-enhanced content delivery solution in blockchain-based information-centric networking, where malicious nodes can be located by tracing the content delivery process in an implicitly trusted way [19]. He et al. propose the FairDownload and FairStream solutions based on blockchain, ensuring that the content consumers and providers can be fairly treated when the other two parties collude to misbehave arbitrarily [20]. Considering that vehicles may collude to defraud the advertiser to obtain rewards without disseminating ads, Li et al. propose a fair and anonymous ad dissemination solution based on blockchain, preventing free-riding and distributed denial of service (DDoS) attacks, and privacy leakage [21]. A blockchain-based auditable access control model is proposed in [22] that combines access records in the blockchain network to manage private data and realize auditable access.

Due to high mobility and network dynamics, V2V video delivery is prone to transmission interruption, unstable video quality, and low cache hit rate. Zaidi et al. propose an enhanced user datagram protocol, which adopts the unequal protection of video frame types to improve the quality of video delivery in vehicular networks [23]. An efficient video streaming mechanism is proposed in [24], which selects a minimum subset of rebroadcaster vehicles for interference reduction and achieves high-quality video dissemination in vehicular ad hoc networks (VANETs). An SVC-based adaptive video streaming scheme is presented in [25] to support video services in a highway scenario. Via vehicle relay, a vehicle can obtain video data through an adjacent car or a multi-hop path to the BSs.

Cooperative V2V video delivery requires vehicles to contribute a certain cache and communication resources. Thus, it is necessary to design an incentive mechanism for content caching to improve vehicle participation and cache utilization. Shi et al. explore an incentive scheme for pricing the contributions of device-to-device (D2D) based on the Stackelberg game, where each competition side can maximize their profits [26]. Xu et al. establish a pricing mechanism to improve the quality-of-experience (QoE) of mobile users and increase the utility of edge nodes, considering the social characteristics of user groups and the caching capabilities of edge nodes [27]. By applying the Kelly and Stackelberg game mechanism to the shared cache of mobile network operators (MNOs), De Pellegrini et al. derive the optimal price configuration that maximizes the revenue of MNOs [28]. Simply pricing policy can only drive vehicles to cache content but cannot incentivize vehicles to distribute video content. Selfish vehicles may no longer deliver content after obtaining a reward. Therefore, incentives are essential for building an ecosystem.

1.2 Main contributions

This paper proposes a blockchain-based trust and scalable V2V video content dissemination framework that can adapt to high-speed movement and resist diverse network attacks. The goal is to create a sound V2V ecology for video caching and sharing, reducing the network infrastructure burden and enhancing video service flexibility. Our main contributions are three folded:

- A decentralized framework for V2V content dissemination is presented to enhance service availability and flexibility with resistance to content tampering and poisoning, Sybil attacks, DDoS attacks, and other types of attacks. Under this framework, vehicles from different operators can safely share video content through V2V mode.
- We construct a fair pricing strategy for V2V content transactions. Based on the strategy, we mathematically formulate the problem of minimizing the total V2V service fees paid by a content-requester under the constraints of the number of video layers, vehicle reputation, the achievable transmission rate, and the duration of V2V connections. An adaptive vehicle-group selection algorithm for problem-solving is then developed that supports SVC-based many-to-one video content delivery.
- Smart contracts are deployed for transaction triggering, verification, and rewards, with a fair reward strategy to price each video content service and a traceability mechanism to punish malicious behaviors. Security analysis and simulation results demonstrate our scheme's security, feasibility, and superiority.

The rest of the paper is organized as follows. Some preliminary knowledge used is introduced in Section 2. The system scheme and problem analysis are presented in Section 3. We explain the key steps of credible and fair V2V content delivery in Section 4 and provide a safety and reliability analysis in Section 5. We present the simulation experiment results in Section 6. Finally, the conclusion is given in Section 7.

2 Preliminaries

This section introduces some key technologies used in the proposed blockchain-based V2V content delivery scheme.

2.1 Smart contract

Smart contracts are self-executing programs stored on a blockchain, which are a reliable way to build tamperproof agreements among disparate, anonymous parties without a central authority. As an immutable computer program, smart contracts have the characteristic that its code cannot be changed once deployed. This paper builds a solution based on the Ethereum platform. Smart contracts on Ethereum are written in solidity high-level language, which supports direct execution in a decentralized environment. The contract code is compiled into the underlying bytecode executable by the Ethereum virtual machine (EVM), and then deployed on the Ethereum blockchain through contract creation transactions.

2.2 Merkle hash tree

Merkle hash tree with smart contracts is utilized to improve the efficiency of content integrity and validity verification. Storing the content hash value after Merkle tree processing on the blockchain can reduce the storage cost on the chain. Each video layer is divided into multiple fragments to facilitate integrity verification. Each leaf node is the hash value of a fragment. When a vehicle needs to verify the integrity of the content, only a few content fragments with corresponding path values need to be uploaded.

2.3 Elliptic curve cryptography

Elliptic curve cryptography (ECC) is a public-key generation technique based on the algebraic structure of elliptic curves. Ethereum uses an ECC-based scheme called the elliptic curve digital signature algorithm (ECDSA) for signing transactions. This scheme uses public and private keys generated by ECC to ensure that each user is unique and every transaction is secure. It has been applied to IoV to verify the information exchange among vehicles [29].

A couple of public and private keys determine an Ethereum account. The private key creates a digital signature, while the public key is made available to anyone who verifies the signature. An Ethereum public key corresponds to a point on an elliptic curve. It is almost impossible to perform inverse operations since elliptic curve scalar multiplication is a trapdoor function.

Ethereum and Bitcoin adopt elliptic curve $secp256k1$. The curve is generated by

$$y^2 \bmod \gamma = (x^3 + 7) \bmod \gamma. \tag{1}$$

Given private key k, the public key in Ethereum is generated by performing elliptic curve multiplication on k, i.e.,

$$K = k * G \tag{2}$$

where G is coordinate generation point and $*$ is the multiplication symbol in the elliptic curve function that is different from the normal multiplication operator. Without division operations in elliptic curve, it is complicated to get private key k when public key K is known. The address in the Ethereum platform is converted from the public key, in

which the conversion depends on the cryptographic hash function *keccak*256 in Ethereum. The Ethereum account address corresponds to the last 20 digits after hashing the account's public key by running $keccak256(K)$.

The execution of the elliptic curve algorithm for signing and verifying is depicted as follows (To distinguish, # represents the multiplication symbol in the elliptic curve function):

Sign:

① Generate a random number r by a cryptographically secure pseudo-random number generator (CSPRNG).
② Calculate a coordinate point M through r and G.
③ Calculate the hash of the message $H = keccak256(m)$.
④ Calculate $s = (H + k * x)/r$ (Algebraic operation, x is the abscissa of G).
⑤ Send (m, r, s, M) to verifier.

Verify:

① Calculate the hash of m $H = keccak256(m)$.
② Calculate the coordinate point based on the content sent by signer $D = H\#G/s + x\#k/s$.
③ Compare M and D. If M and D are equal, the verification is passed.

3 System scenario and problem statement

In this section, we first introduce the model of the blockchain-based V2V content delivery framework in IoV, and then present the threat model and our design goals. The main notations and variables are listed in Table 1.

3.1 System model

As shown in Fig. 1, the blockchain-based V2V content dissemination framework includes five main entities: register authority (RA), video sevice providers, operators, vehicles, and BSs. The roles of the five entities are introduced as follows:

- **RA**, an authorized audit agency, manages vehicles that join the platform and undertakes account registration and payment record audit. RA maintains a certificate repository for vehicle identity and installs a blockchain client to maintain a global ledger that contains all payment records. Vehicles with RA signature certification can be qualified to obtain or send content. Each payment record contains transaction and account information. The transaction information is public, but the account is anonymous to the outside, preventing privacy leaks. RA can obtain the account information of cars.
- **Video Service Providers**, such as YouTube and Facebook, have a large amount of video content and can directly interact with operators. They have the right to distribute content by renting the blockchain-based video content distribution platform.
- **Operators**, provide network infrastructure such as BSs. All operators follow the unified rules and standards deployed on the blockchain. It can record and track content sharing between vehicles through the blockchain.
- **Vehicles** refer to the entities with an OBU [30], which can actively cache the most popular content with the help of BSs. Each vehicle is equipped with a trusted platform module to store private information (e.g., private key) and perform predefined calculations [31]. Each vehicle informs surrounding vehicles of its speed, direction, and content cache through a beaconing mechanism [32]. A vehicle can either initiate a content request to surrounding vehicles (as a content requester), or share cached content with surrounding vehicles (as a content provider). Vehicles pay a service fee to purchase the desired content. Nevertheless, a vehicle may have to obtain content from BSs if no nearby vehicles have cached the required content.
- **BSs**, deployed by operators, play the role of access points for vehicles to obtain original video contents. BSs recommend appropriate content to vehicles based on the cognitive engine to increase their cache hit rate. More intelligent and more efficient content caching can be realized by receiving the prediction results provided by a cognitive engine.

Table 1 Notations and Variables

Symbols	Definition
c_n	video content n
$c_{n,m}$	mth video layer of c_n
$c_{n,m,e}$	eth fragment of $c_{n,m}$
$\mathcal{C}_n$	Set of video layers for c_n
$E_{n,m}/\mathcal{E}_{n,m}$	Number/Set of fragments of $c_{n,m}$
$\mathcal{G}_j$	Index set of adjacent vehicles of vehicle j
$\mathcal{G}_{j,n}$	Index set of vehicles in $\mathcal{G}_j$ carrying c_n
K_x^P/K_x^S	Public/Private key of account x
$M_n/\mathcal{M}_n$	Number/Set of video layers of c_n
$\mathcal{N}$	Set of video content indexes
$p_{n,m}$	Price of $c_{n,m}$
r_i	Reputation of account i
$s_{n,m}$	Size of $c_{n,m}$
$v_{j,n}$	Quality requirement of vehicle j requesting c_n
$\kappa_{i,n,m}$	Service fee earned by vehicle i delivering $c_{n,m}$

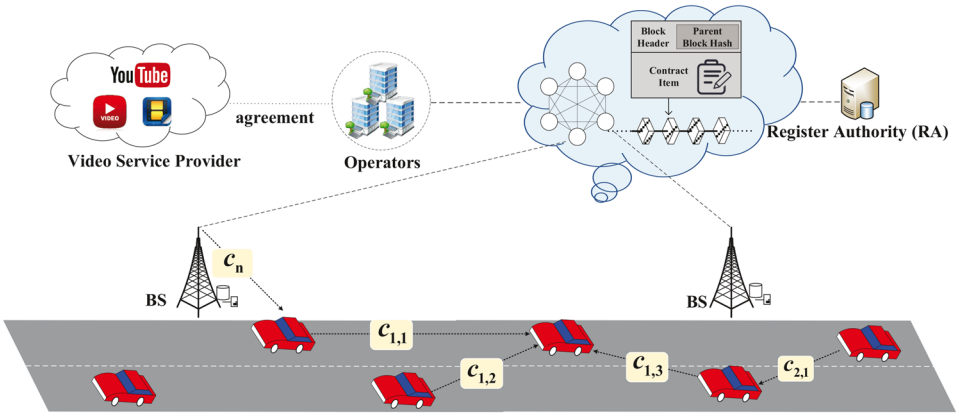


Fig. 1 Blockchain-based V2V content delivery scenario

3.2 Layered video

SVC can encode video data into multiple layers. The basic unit of content request is the video layer. Vehicles can request multiple video layers simultaneously according to their video quality requirements. A vehicle user can decide the number of video layers to acquire according to the quality requirement and channel condition.

Based on SVC, video content n is encoded as M_n layers, the set of which is denoted as $\mathcal{M}_n$. Let $c_{n,m}$ denote the mth video layer in content n. Denote $\mathcal{C}_n = \bigcup_{m\in\mathcal{M}_n} c_{n,m}$ as the set of video layers for c_n. Denote $\mathcal{C} = \bigcup_{n\in\mathcal{N}} \mathcal{C}_n$ as the set of video contents in the system, with $\mathcal{N}$ being the set of video content indexes. The video quality requirement is related to the number of video layers. Let $s_{n,m}$ be the size of $c_{n,m}$. The total size of content n is calculated as

$$S_n = \sum_{m\in\mathcal{M}_n} s_{n,m}. \tag{3}$$

3.3 Threat model

There are privacy and security issues in the open blockchain network. We specify these threats in the V2V video dissemination scenario as follows:

- *Privacy Leakage*: Since transaction records are shared among traders, potential attackers can infer the content preferences of the vehicle. In addition, attackers can also collude with selfish vehicles to obtain private information about related vehicles.
- *Content Integrity Attack*: Due to resource consumption, dishonest vehicles may send incomplete content to content requesters. Requesters' interests may be lost without effective integrity detection because they cannot get the complete content.
- *Poisoning Attack*: An attacker may tamper with the original content and plant unauthorized, illegal content even phishing links.
- *Sybil Attack*: Since a vehicle's transaction relies on an account, an attacker may virtualize multiple account identities and send a request to the same vehicle using a different account to interfere with content delivery.
- *DDoS Attack*: When multiple attackers attack a target vehicle or base station, the attacked equipment will not be able to be used normally, and it will also cause serious economic losses.
- *Double-Spending Attack*: A content requester may use the same amount of money to obtain multiple contents when the payment has not been deducted.

3.4 Design goals

For building a good V2V video content sharing ecosystem, our scheme should achieve the following design goals:

- *Trustiness*: 1) Content providers should provide trusted and reliable delivery. Each content-requesting vehicle can identify neighbor vehicles to avoid communicating with historically irregular behaviors; 2) The content disseminated over IoV should be authorized and credible. Operators need to ensure that the content is traceable and prevent the content from being maliciously changed after multiple disseminations.
- *Security*: 1) Our scheme should prevent the disclosure of vehicle privacy information and avoid participants' preferences from being acquired by malicious entities; 2) The system should trace back to abnormal vehicles to prevent the further spread of unsafe content; 3) The system should resist DDoS attacks and Sybil attacks.
- *Fairness*: 1) The system needs to provide fair rewards for content-providing vehicles for each content transaction;

2) and should prevent content requesters from refusing to pay rewards after vehicles successfully disseminate content.

- *Feasibility for high mobility*: Content-providing vehicle selection needs to consider V2V connection duration and achievable transmission rate to account for vehicle mobility.

4 Secure and scalable V2V content delivery

This section discusses the trusted and scalable V2V content delivery scheme, which includes six phases: Registration, Content Publication, Reputation Calculation, V2V Service Fee Calculation, Content-Providing Vehicle-Group Selection, and Smart Contract Based Transaction Verification.

4.1 Registration

In the infrastructure based on the blockchain, vehicles can realize cross-operator content transactions through V2V. However, since there is no mutual trust between vehicles, vehicles are easily deceived by unidentified traders around them. V2V content distribution is often vulnerable to Sybil attacks, against which an identity verification mechanism is embedded into the content delivery scheme to resist fake identity fraud. Vehicles joining the video content delivery platform need to perform account verification in RA in advance. Each vehicle must submit the generated account information (public key, account ID, driving license and reputation value signed by the private key) to RA for identity verification and registration. The account of vehicle i is expressed as $account_i = \left(Sign\left(K_i^P, timestamp\right)_{K_{RA}^S}, r_i, address_i\right)$, including the legality statement of vehicle identity, reputation value, and vehicle address on the blockchain. As illustrated in Fig. 2, vehicle i being registered needs to generate a pair of public and private keys to ensure interaction and verification between different entities.

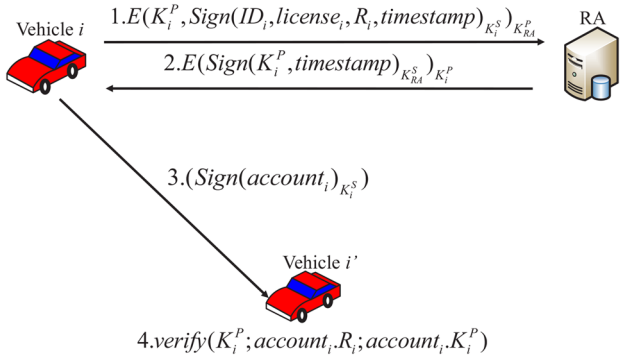


Fig. 2 Account registration

Vehicle i needs to send its public key K_i^P and identity information to RA. After verifying the identity of vehicle i, RA uses its private key K_{RA}^S to sign K_i^P. When vehicles i and i' conduct a transaction, vehicle i sends K_i^P and $Sign\left(account_i\right)_{K_i^S}$ to vehicle i'. Vehicle i' uses RA's public key K_{RA}^P to verify $account_i.K_i^P$ and $account_i.r_i$, determining whether vehicle i is a legal transaction account. Since payment records are publicly shared among all participants, attackers may speculate on vehicles' sensitive information. The system allows vehicles to apply for multiple public-key signatures from RA at once to protect their privacy and reapply when the accounts generated by these public key signatures are exhausted [31]. The payment records include transaction information and account information. Account privacy information is maintained by RA, while transaction information is public.

4.2 Content publication

While publishing an authorized video content encoded by SVC, operators initialize the video content's attributes and identification. Merkle hash tree is introduced to detect and trace incomplete video content. Before video content injection, operators generate a hash of the content layer and record it in the blockchain, which reduces the storage space and facilitates transaction verification.

The basic unit of content transactions among vehicles is the video layer. To facilitate verification, $c_{n,m} = \bigcup_{e \in \mathcal{E}_{n,m}} c_{n,m,e}$ is divided into $E_{n,m}$ fragments, the set of which is denoted as $\mathcal{E}_{n,m}$. Each video layer constructs a Merkle hash tree according to Algorithm 1 with leaf nodes composed of fragments. Take Fig. 3 as an instance. $root(c_{n,m})$ is stored in the smart contract deployed by the operator, and the occupied storage space is reduced to the size of one hash. After content delivery, a vehicle only needs to upload video layer fragments with path indexes to facilitate subsequent verification.

Data block validation is a bottom-up process. When verifying whether a video layer has been tampered with, the ordinary hash list needs to re-hash each data block with

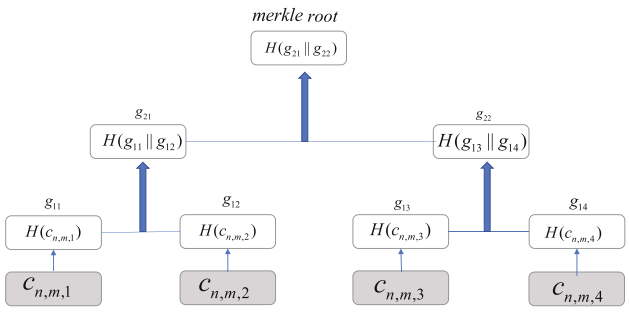


Fig. 3 A merkle tree example for video layer $c_{n,m}$ with $E_{n,m} = 4$

the computational complexity of $O(n)$. Although the first encryption operation is simple, each subsequent verification of this method must repeat the above process. Merkel tree only needs to provide the node's hash value on the specified path when performing data verification. Merkel hash verification can reduce the complexity from linear time to logarithmic time $O(\log_2 n)$ [33].

Algorithm 1: Merkle Hash Tree Generation for $c_{n,m}$.

Input: $c_{n,m} = (c_{n,m,1}, c_{n,m,2}, ..., c_{n,m,E_{n,m}})$.

Output: Merkle hash tree with root value $root(c_{n,m})$.

$c^L_{n,m}$=MerkleTree$(c_{n,m,1}, c_{n,m,2}, ..., c_{n,m,\lceil E_{n,m}/2 \rceil})$;

$c^R_{n,m}$=MerkleTree$(c_{n,m,\lceil E_{n,m}/2 \rceil+1}, c_{n,m,\lceil E_{n,m}/2 \rceil+2}, ..., c_{n,m,E_{n,m}})$;

$root(c_{n,m})=H(c^L_{n,m}c^R_{n,m})$;

final;

return $root(c_{n,m})$;

Operators need to deposit in advance when deploying the smart contract. Once a contract expires, the remaining deposit gets automatically returned. If the transaction verification fails, reward distribution is not performed. Suppose a contract receives a certain number of valid vehicle signatures declaring that one video content is illegal. In that case, the pre-deposit of operators is confiscated and issued to these declared vehicles.

Operator o submits the corresponding transaction to the blockchain network and records the content's digest information as

$$\tilde{c}_{n,m} = \{root(c_{n,m}), t_d, u_{n,m}, p_{n,m}, g, s_{n,m}\} \tag{4}$$

when issuing video content. After that, the reward contract is broadcast by BSs. In (4), $root(c_{n,m})$ represents the root hash of video layer $c_{n,m}$; t_d is the deadline for content delivery to obtain a reward: is contract lifetime; $u_{n,m}$ is the identifier of content layer $c_{n,m}$; $p_{n,m}$ is the price of $c_{n,m}$; g represents deposit locked in the contract by operator o; $s_{n,m}$ is the size of content $c_{n,m}$. Operator o uses K^S_o to sign $\tilde{c}_{n,m}$, to realize content authorization. Any content recipient can verify $Sign(\tilde{c}_{n,m})_{K^S_o}$ through K^P_o. V2V content delivery can trigger the transaction by calling the corresponding contract according to the contract address.

4.3 Reputation calculation

To provide security for content requesters, we set a reputation value for each vehicle calculated from the score of historical transactions. Let $z_i^{(q)} \in [0, 1]$ denote the service rating of vehicle i when providing the qth service to a content-requester. Generally, $z_i^{(q)} \in [0, 0.5]$ belong to a lower level. When the vehicle is found to have malicious behavior in the qth service, the service rating of vehicle i is rated $z_i^{(q)} = (1 + \varpi)z_i^{(q)}(\varpi \in [0, 1])$, otherwise $z_i^{(q)} = \varpi z_i^{(q)}$. Compared with the early behavior, the current behavior of a vehicle has a more significant impact on its current reputation. We characterize the effect of the qth service rating on positive and negative trust degrees via $z_i^{(q)}e^{-u(t-t^{(q)})}$ and $(1 - z_i^{(q)})e^{-u(t-t^{(q)})}$, where u is a decay factor, t is current time, and $t^{(q)}$ is the time of the qth interaction. Let Q_i denote the number of content deliveries of vehicle i. The cumulative positive trust degree and negative trust degree are expressed as

$$P(Q_i) = \sum_{q=1}^{Q_i} z_i^{(q)} e^{-u(t-t^{(q)})} \tag{5}$$

and

$$N(Q_i) = \sum_{q=1}^{Q_i} (1 - z_i^{(q)}) e^{-u(t-t^{(q)})}. \tag{6}$$

Then, the trustworthiness and untrustworthiness of vehicle i are defined as

$$a(Q_i) \triangleq \frac{P(Q_i)}{P(Q_i) + \vartheta_i N(Q_i) + \eta} \tag{7}$$

and

$$b(Q_i) \triangleq \frac{\eta}{P(Q_i) + \vartheta_i N(Q_i) + \eta} \tag{8}$$

where η is the uncertain factor and ϑ_i is the punishment factor for vehicle i. To prevent vehicles from destroying the transaction ecology, we increase the penalties for vehicles with low reputation ($r(Q_i) < 0.6$) by adjusting the penalty factor. Normally, ϑ_i is set to 1. Suppose that a vehicle currently has ℓ cumulative abnormal transactions. ϑ_i will be increased in future $2^\ell + \hbar$ transactions. Repeatedly being found to have malicious behaviors will lead to increased punishment. It is unlikely for these vehicles to return to a normal credit level within a short period. In what follows, the impact of the adjustment of ϑ_i on the score will be tested by simulation. Based on (5)–(8), the cumulative reputation value of vehicle i is calculated as

$$r(Q_i) = a(Q_i) + \theta b(Q_i) \tag{9}$$

where θ is a parameter to adjust the untrustworthiness.

4.4 V2V service fee calculation

Consider a transaction model with a video layer as a request unit. The requester can simultaneously trade with multiple

adjacent vehicles for different video layers. Since the decoding of the enhancement layer is dependent on the base layer, the reliability and safety requirements of a car providing the base layer are higher than that of a vehicle providing the enhancement layer. Note that RA can only guarantee whether a public key is owned by a registered car but cannot guarantee the credibility of the vehicle's behavior. By observing the reputation value of surrounding vehicles, content requesters tend to select cars with good historical behavior for transactions.

The higher the probability that a video layer is requested, the more likely it is to be exploited by malicious attackers. Therefore, it is necessary to adjust the reputation value of the content-providing vehicle according to the request probability. Denote $h_{n,m}$ as the popularity ranking of $c_{n,m}$. The distribution of content requests follows a Zipf distribution [34], and the probability of $c_{n,m}$ being requested is expressed as

$$f_{n,m} = \left(h_{n,m}^{\iota} \sum_{n \in \mathcal{N}} \sum_{m \in \mathcal{M}_n} \frac{1}{h_{n,m}^{\iota}} \right)^{-1} \tag{10}$$

with $\sum_{n \in \mathcal{N}} \sum_{m \in \mathcal{M}_n} f_{n,m} = 1$, where $\iota \in [0, 1]$ represents the skewness of video layer distribution.

Let $r^{(\max)}$ represent the upper bound of vehicle reputation value in a area. Based on (9) and (10), if vehicle i acts as the provider of content layer $c_{n,m}$, the reputation value of the vehicle needs to satisfy

$$r(Q_i) \geq \alpha r^{(\max)} + \beta \log(1 + f_{n,m}) \tag{11}$$

where α is used to adjust reputation value and β is weight factor for content popularity. The request probability of $c_{n,m}$ is positively associated with the reputation requirement.

After sharing content $c_{n,m}$ and passing the transaction verification, content-providing vehicle i can obtain reward depending on the contract. Different video layers contribute differently to the improvement of video quality. The utility of obtaining $c_{n,m}$ from vehicle i is calculated as

$$\omega_{i,n,m} = \frac{\chi}{1 + e^{-\delta f_{n,m}}} \log(1 + \frac{\varphi}{1 + e^{-\tau(\frac{s_{i,n,m}}{\bar{s}})}}) \tag{12}$$

where χ, δ, φ, and τ are adjustable parameters. The service fee that can be obtained by vehicle i delivering content $c_{n,m}$ is paid by the requester, which is calculated as

$$\kappa_{i,n,m} = r(Q_i)\omega_{i,n,m} + \lambda p_{n,m} \tag{13}$$

where $p_{n,m}$ is the price of video layer $c_{n,m}$ and λ is an adjustable parameter. After being verified, this service fee is issued to vehicle i as a reward. The higher the value of $\omega_{i,n,m}$ obtained by the content requester from vehicle i, the higher the reward for vehicle i. The ratio of $s_{i,n,m}$ to the average size, $\bar{s}$, of video is positively correlated with the service fee. According to (12) and (13), a vehicle can obtain considerable benefits by keeping a good reputation while caching popular content.

4.5 Vehicle-group selection

A vehicle can simultaneously initiate requests for different video layers to multiple neighboring vehicles to conduct video content transactions. The purpose is to minimize V2V service fees paid by the requester under the constraints of the number of video layers, reputation, V2V connection duration, and the achievable transmission rate.

Let $y_{i,n,m}$ be 1 if vehicle i has cached $c_{n,m}$, otherwise be 0. The set of the indexes of vehicle j's adjacent vehicles is denoted as $\mathcal{G}_j$. The index set of vehicles in $\mathcal{G}_j$ carrying c_n is denoted as $\mathcal{G}_{j,n} = \{i \in \mathcal{G}_j \mid y_{i,n,m} = 1, m \in \mathcal{M}_n\}$. We use $v_{j,n}$ to represent the number of video layers required by vehicle j for c_n, reflecting the quality requirement.

For ease of understanding, we next present a simple example to explain the impact of the constraints on content-providing vehicle-group selection,assuming that:

1. Vehicle j requests video c_1 with $v_{j,1} = 4$ and $\mathcal{G}_{j,1} = \{1, 2, 3, 4\}$;
2. Under connection duration and transmission rate constraints, each vehicle can only provide one video layer;
3. Vehicle reputation status, V2V service fees for video layers cached by vehicles, and reputation requirements are shown in Fig. 4.

For this case, a common approach is choosing content providers starting from the base video layer based on minimizing V2V content service fee. Take Fig. 5 as an example, which includes the following two consecutive steps:

Step 1 Requester j selects vehicle 1 with the second lowest service fee to provide $c_{1,1}$, because vehicle 2 cannot meet the reputation requirement ($r_2 < r_{1,1}^{(\min)}$).

	$\kappa_{i,1,1}$	$\kappa_{i,1,2}$	$\kappa_{i,1,3}$	$\kappa_{i,1,4}$	r_i
$i=1$	90	86	\	\	0.8
$i=2$	100	88	\	\	0.9
$i=3$	\	85	84	79	0.79
$i=4$	88	\	82	76	0.76

	$r_{1,m}^{(\min)}$
$m=1$	0.8
$m=2$	0.79
$m=3$	0.77
$m=4$	0.75

Fig. 4 Service fee for content from different vehicles (empty means the content is not cached by the corresponding vehicle) and vehicle reputation requirements

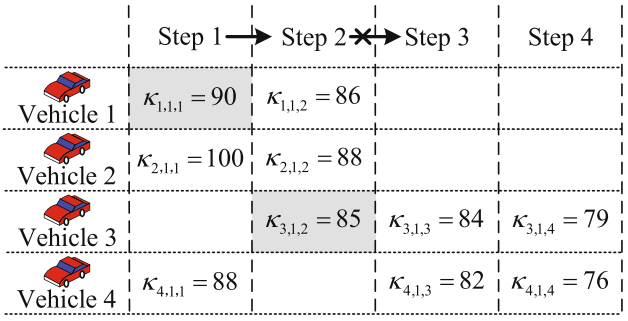


Fig. 5 Vehicle-group selection (Case 1)

Step 2 Requester j decides vehicle 3 with the lowest service fee to provide $c_{1,2}$.

Since the reputation requirement ($r_4 < r_{1,3}^{(\min)}$) cannot be satisfied, vehicle 4 cannot serve as a provider of $c_{1,3}$. Vehicle 3 also fails to provide $c_{1,3}$ in Step 3. The vehicle selection for subsequent video layers has to be terminated, and the video quality requirement ($v_{j,1} = 4$) of vehicle j cannot be satisfied.

Let $x_{i,j,n,m}$ be 1 if vehicle j chooses to obtain $c_{n,m}$ from neighbor vehicles i, otherwise be 0. Given $\mathcal{G}_{j,n}, \mathcal{C}_n, v_{j,n}$, the content-providing vehicle selection problem of vehicle j with respect to $\mathcal{C}_n$ is formulated as $\mathcal{P}1$.

$$\mathcal{P}1: \min_{\{\mathcal{X}_{j,n}\}} : \sum_{i\in\mathcal{G}_{j,n}} \sum_{m\in\mathcal{M}_n} x_{i,n,m}\kappa_{i,n,m} \tag{14}$$

$$s.t.\begin{cases} \sum\limits_{i\in\mathcal{G}_{j,n}} y_{i,n,m} \geq 1, \forall m \in \mathcal{M}_n & \text{(15a)} \\ \sum\limits_{i\in\mathcal{G}_j} \sum\limits_{m\in\mathcal{M}_n} x_{i,n,m} = v_{j,n} & \text{(15b)} \\ \prod\limits_{m=1}^{v_{j,n}} \left(\sum\limits_{i\in\mathcal{G}_{j,n}} x_{i,n,m} \right) = 1 & \text{(15c)} \\ r_i \geq \alpha r^{(\max)} + \beta \log(1+f_{n,m}), \forall i \in \mathcal{G}_{j,n}, m \in \mathcal{M}_n & \text{(15d)} \\ d_{i,j} \geq \frac{\sum_{m\in\mathcal{M}_n} x_{i,n,m} s_{n,m}}{w_i}, \forall i \in \mathcal{G}_{j,n} & \text{(15e)} \\ x_{i,n,m} \in \{0,1\}, y_{i,n,m} \in \{0,1\}, i \in \mathcal{G}_{j,n}, m \in \mathcal{M}_n & \text{(15f)} \end{cases} \tag{15}$$

The essence of objective (14) is to find a group of vehicles (determined by $\mathcal{X}_{j,n} = \bigcup_{m\in\mathcal{M}_n} x_{i,n,m}$) in $\mathcal{G}_{j,n}$ to provide the required $v_{j,n}$ video layers with the least service fee. Constraint (15a) guarantees that vehicles in $\mathcal{G}_{j,n}$ can provide every video layer required by vehicle j. Constraint (15b) states that the content-providing selection should meet the requester's video quality requirement. Due to the decoding dependencies, constraint (15c) ensures the reception of the base video layer. The vehicle that provides $c_{n,m}$ needs to meet the reputation requirement, which corresponds to (15d). Suppose that the achievable transmission rate of vehicle i is w_i. Under (15e), vehicle i needs to complete the transmission of the relevant video layer(s) within duration $d_{i,j}$.

For solving $\mathcal{P}1$, a vehicle-group selection algorithm is developed, as shown in Algorithm 2. Due to V2V connection duration constraint (15e), the following two situations make vehicle i' with the lowest service fee (line 2) not selected as the provider of $c_{n,m}$:

1. Vehicle i' may also act as an alternate provider for other video layers after completing the delivery of the content of volume $s_{i',n} = \sum_{m\in\mathcal{M}_n} x_{i',n,m} s_{n,m}$. If the transmission of $c_{n,m'}(m' > m)$ cannot be completed in $d_{i,j}$, the number of providers for $c_{n,m'}$ is updated to $V_{n,m'} = V_{n,m'} - 1$ (line 6). If $V_{n,m'} = 0$ ($c_{n,m'}$ has no optional provider), $x_{i',n,m}$ is set to 0 (lines 7-8).
2. If candidate providers are insufficient to deliver all remaining video layers, $x_{i',n,m}$ is set to 0 (lines 10-11).

Apart from the connection duration constraint, the reputation constraint also prevent vehicle i' from becoming the provider of $c_{n,m}$. Take Fig. 6 as an example, which includes the following four consecutive steps:

Step 1 Vehicle 1 with the second lowest service fee is selected as the provider of $c_{1,1}$ because vehicle 4 cannot meet the reputation requirement ($r_4 < r_{1,1}^{(\min)}$).

Step 2 The two vehicles with the lowest service fee, vehicles 2 and 3, cannot complete the transmission of $c_{1,2}$ within the given connection duration, and therefore, vehicle 2 becomes the content provider.

Step 3 Vehicle 3 is selected as the provider of $c_{1,3}$ due to $r_4 < r_{1,3}^{(\min)}$.

Step 4 Vehicle 4 with the lowest service fee is selected as the provider of $c_{1,4}$.

From the above steps, the proposed algorithm helps to discover more vehicles to participate in many-to-one content transmission, thereby reducing the occurrence of content acquisition from BSs at a higher cost due to improper vehicle selection.

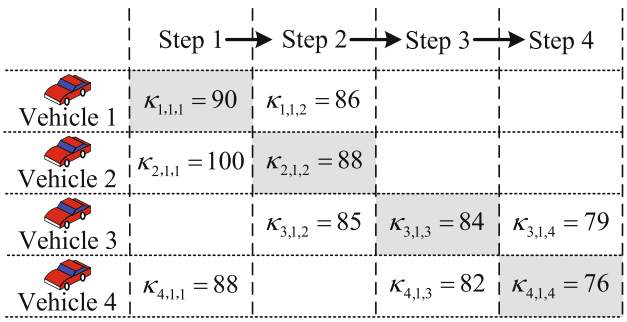


Fig. 6 Vehicle-group selection (Case 2)

Algorithm 2: Vehicle-Group Seleciton.

Input : $\mathcal{G}_j, \kappa_{i,n,m}, \upsilon_{j,n}, d_{i,j}, r_i, w_i, y_{i,n,m}$
Output: $\mathcal{X}_{j,n}$
Init: $m \leftarrow 1$, $V_{n,m} = \sum_{i \in \mathcal{G}_j} y_{i,n,m}$
while $m < \upsilon_{j,n} + 1$ **do**
  $i' \leftarrow \arg\min_{i \in \mathcal{G}_{j,n}} \kappa_{i,n,m}$, s.t.(18) (19);
  if $i' = 0$ **then**
    break;
  $x_{i',n,m} \leftarrow 1$;
  $a \leftarrow 0$;
  for $m' \leftarrow m+1$ *to* $\upsilon_{j,n}$ **do**
    if $d_{i',j} w_{i'} - s_{i',n} < y_{i',n,m'} s_{n,m'}$ **then**
      $V_{n,m'} \leftarrow V_{n,m'}$-1;
    if $V_{n,m'} = 0$ **then**
      $x_{i',n,m} \leftarrow 0$;
      break;
    $a \leftarrow a + V_{n,m'}$;
  if $a < \upsilon_{j,n} - m \| !x_{i,n,m'}$ **then**
    $x_{i',n,m} \leftarrow 0$;
    $\kappa_{i',n,m} \leftarrow +\infty$;
    for $m' \leftarrow m+1$ *to* $\upsilon_{j,n}$ **do**
      if $d_{i',j} w_{i'} - s_{i',n} < y_{i',n,m'} s_{n,m'}$ **then**
        $V_{n,m'} \leftarrow V_{n,m'}$+1;
  else
    $m \leftarrow m + 1$;
  $i' \leftarrow 0$;
return $\mathcal{X}_{j,n}$;

4.6 Smart contract based transaction verification

Take Fig. 7 as an example. The transaction process between requester *j* and provider *i* (included in $\mathcal{X}_{j,n}$) is as follows:

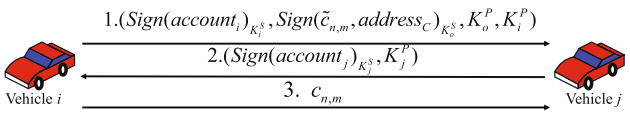


Fig. 7 V2V transaction process

1. Vehicle *j* can obtain the identity of vehicle *i* through $account_i$, and use K_{RA}^P to verify the legitimacy of $account_i$. K_{RA}^P is public, known to any account. Operators generate a digest for each published content for verification during the dissemination process. The receiver can inquire about the legality of content with K_o^P, and determine whether it is the requested content through the identifier.
2. Vehicle *j* sends its public key K_j^P and $Sign(account_j)_{K_j^S}$ to vehicle *i*, along with the dispatched contract address, indicating that vehicle *j* wants content from vehicle *i*.
3. Upon receiving a request from vehicle *j*, vehicle *i* generates a transaction record. Video content delivery is carried out after vehicle *j* verifies and signs the transaction record [35].

A smart contract is deployed for trusted interactions among various vehicles. The implementation details are summarized in Algorithm 3. Once the content-providing vehicle-group, included in $\mathcal{X}_{j,n}$, is determined by Algorithm 2, the smart contract verifies the behavior of all parties in a transaction. Although video content provisioning is a many-to-one transmission mode, the smart contract must verify each video layer in $\mathcal{X}_{j,n}$ separately. For a group of content provider vehicles, the behavior of anyone will not affect the credibility and the service fee calculation of other cars.

Algorithm 3: Content Transaction.

Input: $account_i$, $account_j$, $deposit_i$, $deposit_j$, t, $\tilde{c}_{n,m}$, $x_{i,n,m} \in \mathcal{X}_{j,n}$
Sign($account_i$) and Sign($account_j$) on the smart contract;
if $(t_d \geq t$ *&&* $deposit_j \geq p_{n,m})$ **then**
  Vehicle i send $c_{n,m}$ to vehicle j;
  Vehicle i broadcasts content transaction;
  Calculate $\kappa_{i,n,m}$ of vehicle i;
  $Penalty() \rightarrow (Penalty_o, Penalty_i, Penalty_j)$;
  Send$(account_i, deposit_i + \kappa_{i,n,m} + Penalty_i)$;
  Send$(account_j, deposit_j - p_{n,m} - \kappa_{i,n,m} + Penalty_j)$;
  $g = (g + p_{n,m} + Penalty_o)$;
  return true;
else
  Fail to initiate the transaction;
  return false;

Content delivery is performed if a vehicle initiates a content request within the preset broadcast time and the deposit has been locked to the contract. Miners validate the new transaction and record it on the global ledge. After completing the consensus, the contract executes rewards and punishments according to the behavior record of each participant.

5 Security analysis

This section explains how the design goals on trustiness, security, a fairness against different types of attacks is achieved.

- *Trusted V2V Interaction*: Since only transaction information can be obtained between vehicles and account information cannot be obtained, the disclosure of vehicle privacy information can be avoided. Vehicle i certified by RA gets a public key information, $Sign(K_i^P)_{K_{RA}^S}$, signed by the RA. When other vehicles interact with vehicle i, K_{RA}^P can verify the legality of vehicle i to ensure its authenticity. The scoring mechanism for content transactions also evaluates vehicles' transaction behavior to ensure that it is credible. Each vehicle can evaluate the historical behavior of surrounding vehicles based on reputation to avoid connecting with malicious vehicles.
- *Trusted Video Content Dissemination*: Operator o digests key information of authorized content and uses its private key K_o^S to sign $\tilde{c}_{n,m}$, indicating that the content is authorized to disseminate. Any operator' vehicle can verify the validity of $Sign(\tilde{c}_{n,m})_{K_o^S}$ through K_o^P. The pre-deposit mechanism used by an operator when issuing a smart contract can also ensure that its content is supervisable. When vehicles find that the published content is illegal information, they can sign and report it. Suppose the smart contract receives a certain number of valid signatures from vehicles declaring that its content is illegal. In that case, the operator's deposit is treated as a fine to distribute to cars as a reward. This contract-based reward and punishment mechanism can realize the distribution of rewards and punishments across operators in the blockchain environment.
- *Security Against Sybil Attack*: When interacting with other vehicles, vehicle i needs to provide the identity information that RA has authenticated. RA's authentication can prevent malicious vehicles from virtualizing multiple accounts to do evil since these accounts can be located in RA when malicious behavior occurs.
- *Security Against Poisoning Attack*: The blockchain records the input and output of each vehicle transaction in IoV, which can easily track transaction activities and ensure the traceability of content dissemination.
- *Security Against DDoS Attack*: A vehicle needs to deposit in advance before the transaction occurs, reducing the possibility of malicious attackers frequently sending many requests, effectively preventing DDoS attacks.
- *Non-repudiation*: By recording the behavior of each transaction party on the blockchain, any participant who spreads illegal content can be traced back to. Combining this feature, we have set a time-locked deposit in the smart contract along with reward and punishment mechanisms, which can effectively prevent the occurrence of double-spending and account fraud.

6 Analysis of simulation results

We simulate a road network environment where multiple optional video content providers coexist. Each vehicle improves the cache profit rate as much as possible based on the recommendation of the cognitive engine. Vehicles tend to contribute extra cache space for content distribution. Under the recommendation of the cognitive engine, vehicles cache the most popular content in the area with a high cache utilization. It is assumed that the cache space size contributed by a vehicle is in the range of [10,70] GBs, and each vehicle can serve up to four adjacent vehicles simultaneously. To achieve a more realistic simulation effect, we use the real-world video trace [36] to randomly generate 80 video contents with larger sizes, each of which uses SVC to achieve a quality level of $M = 4$. Among these 80 videos, there are three types of videos: CREW, FOOTBALL, and SOCCER. The content requests issued are all randomly generated according to the Zipf distribution. Some other parameter settings are given in Table.2.

The proposed vehicle-group selection scheme supports SVC-based many-to-one video content transmission. For comparison, two baselines are selected:

- **Independent video delivery**: Without SVC-based video layering, the requester selects a unique vehicle to transmit the entire video content as in [37, 38].

Table 2 Simulation Settings

Parameter	Value
Decay factor for trust (u)	0.001
Uncertain factor of trust (η)	0
Zipf parameter (ι)	0.6
Number of abnormal transaction ($\hbar$)	100
Weight parameters ($\{\alpha,\beta,\rho,\varpi\}$)	0.8,0.9,0.5,0.1
parameters to quantize κ ($\{\chi,\delta,\varphi,\tau,\lambda\}$)	1.6,0.2,1,1,0.1

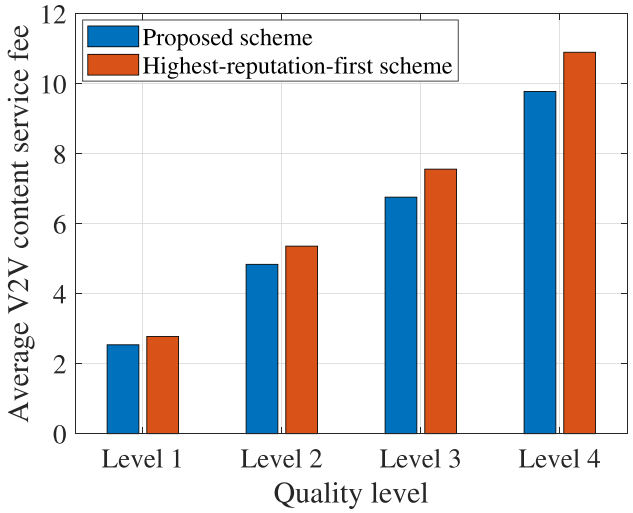


Fig. 8 Comparison of V2V content service fee

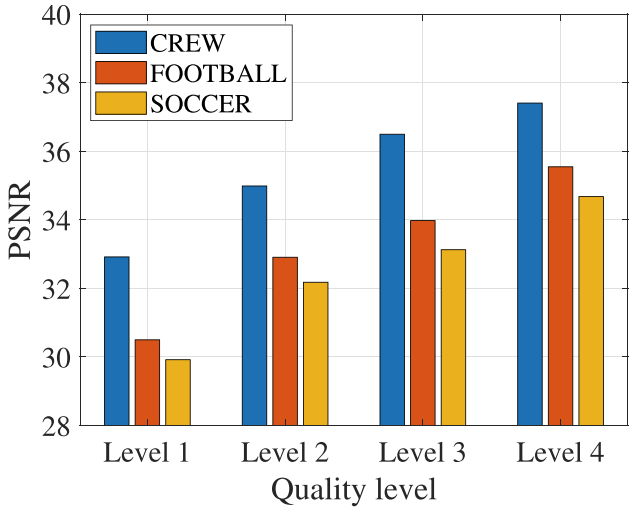


Fig. 9 Average PSNR for different quality levels

- **Highest-reputation-first scheme**: With SVC-based video layering, the vehicle with high reputation value is preferred as the video layer provider [39].

6.1 Impact of the number of video layers

We examin the difference in V2V content service fee when the average quality levels of content requests are set to 1, 2, 3, and 4, respectively. It is assumed that each vehicle maintains a high reputation status.

In addition to vehicles reputation, the selection of content providers should consider the service fee paid for V2V services. As shown in Fig. 8, with the increase in the video quality level, the proposed scheme can save more service fee for the requester than the highest reputation first scheme. Using the highest-reputation-first scheme, a requester must have priority to connect to vehicles with a high reputation. High V2V service fees often accompany a high reputation. Besides, due to constraints, traditional heuristic schemes may cause the requester to face the dilemma of having no option, and the algorithm terminates early. This situation results in the requester having to connect with high-cost BSs.

Figure 9 illustrates the changes in peak signal-to-noise ratio (PSNR) when video content is received at different quality levels. The lack of some enhancement layers does not have much impact on video playback.

6.2 Comparison of content delivery delay

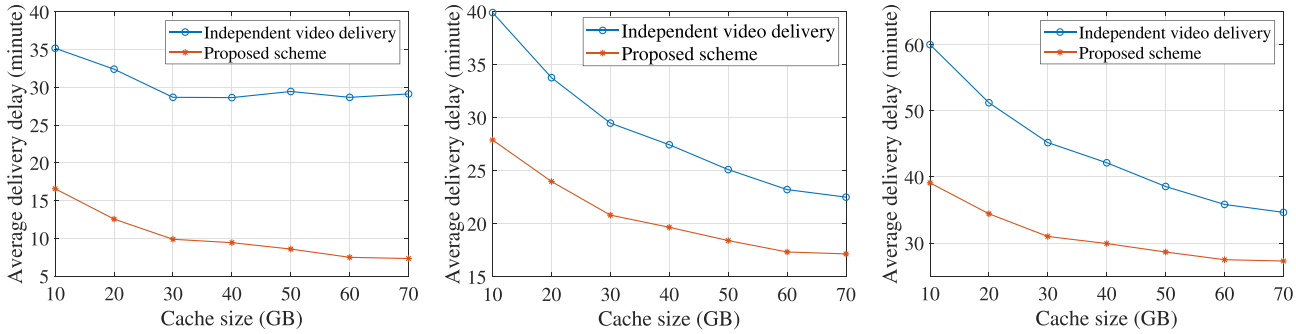
Figure 10a–c compare the average delivery delay between proposed scheme and the independent video delivery. In the simulation, we assume that each vehicle has a high reputation. The average video quality levels are set to 2, 3, and 4, respectively.

As expected, in Fig. 10a–c, the average delay decreases as the average cache size increases. The proposed scheme has a lower transmission delay than the independent video delivery because independent video delivery cannot transmit different video layers simultaneously. The high delay caused by independent video content transmission cannot be well adapted to the dynamic network topology. The proposed content delivery scheme uses the video layer as the transaction unit. When a vehicle requests the content of multiple video layers, it can obtain services by connecting different vehicles. By comparing the two schemes in Fig. 10a–c, we can see that when vehicles request high-quality video content, collaborative content delivery can significantly reduce the delay. For example, when a car requests content with a quality level of 3, three different vehicles can transmit different layers. The delivery delay is equal to the video layer with the longest delivery time, not the sum of the transmission time of the entire content.

6.3 Rewards under different strategies

Figure 11a shows the overall vehicle reward variation over time under different reputation statuses. The reputation status of vehicles are divided into three categories (namely, high-reputation, general-reputation, and low-reputation). Assuming that the vehicle can randomly initiate content requests, the average cache space contributed by each vehicle is set to 60G.

From Fig. 11a, the total reward of vehicles with high and medium reputation status gradually increases with



(a) Quality level: 2 **(b)** Quality level: 3 **(c)** Quality level: 4

Fig. 10 Scheme comparison for average delivery delay

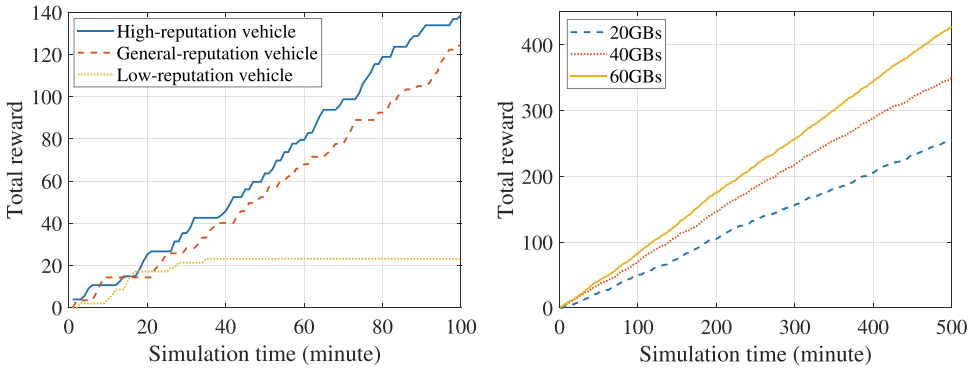
time. The revenue growth rate for vehicles with medium reputation status is slightly lower than high reputation vehicles. The revenue of vehicles with low reputation status has increased quickly in a short period, and then there are no more revenue changes. All vehicles have the same reputation value initially, and they are all likely to be selected. Vehicles with high (low) reputation status will receive high (low) scores. As the number of content deliveries increases, the reputation value of vehicles continues to update. A vehicle with a higher reputation value is more likely to be selected by neighboring vehicles, obtaining higher returns under the same transaction conditions. Vehicles with low reputation status are connected in the initial stage. However, as time changes, content services provided by vehicles with low reputation status are given low scores because they do not meet the requester's needs even harm the benefit of the requester. When multiple neighboring vehicles give lower scores to the services provided by malicious vehicles, their reputation value gradually decreases. Vehicles with low reputation status cannot continue to receive revenue after being identified because vehicles whose reputation values drop below the minimum threshold are not chosen as content providers.

Figure 11b compares the impact of different average cache space contributions from vehicles on vehicle revenue. The average cache capacity is set to 20GBs, 40GBs, and 60GBs respectively (assuming that each vehicle maintains a high reputation status). When the size of the cache space contributed by vehicles is different, there is a different increase in reward. The reason is that vehicles with ample cache space can cache more content, having a higher probability of being selected by neighboring vehicles. When the cache hit rate is high, vehicles can quickly gain revenue. Encouraging vehicles to contribute more extra cache space for content delivery is beneficial.

6.4 Impact of punishment strategy

In Fig. 12, the transaction scores generated for vehicle i during simulation conform to a normal distribution with a mean of 0.5 and a standard deviation of 0.2. Figure 12a shows the probability density function (PDF) of reputation value under different penalty factors. As penalty factor ϑ_i increases, the hump shift to the left, and the distribution of reputation values also be concentrated at a lower level. Figure 12b shows the cumulative distribution

Fig. 11 Total reward over time



(a) Impact of reputation status. **(b)** Impact of cache space.

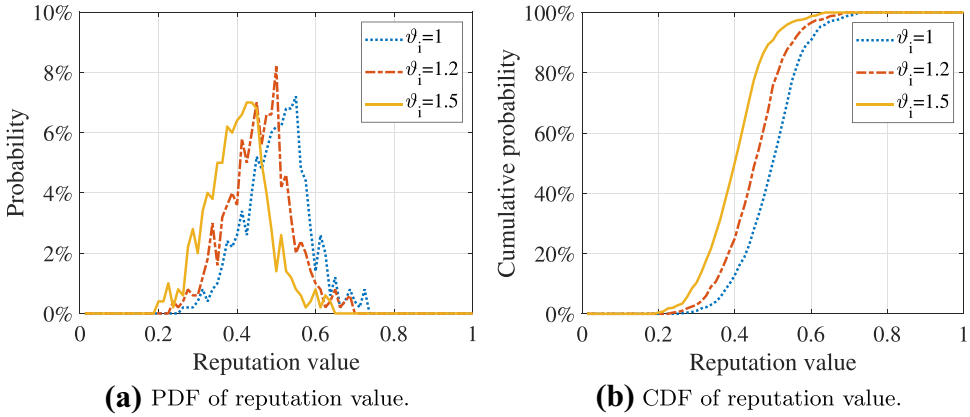


Fig. 12 Case where the probability distribution of transaction scores with a mean of 0.5 and a standard deviation of 0.2

(a) PDF of reputation value. **(b)** CDF of reputation value.

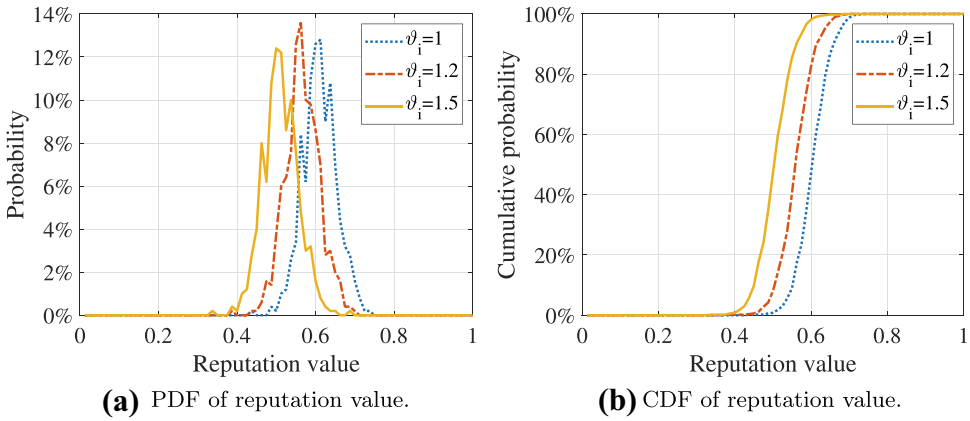


Fig. 13 Case where the probability distribution of transaction scores with a mean of 0.6 and a standard deviation of 0.1

(a) PDF of reputation value. **(b)** CDF of reputation value.

function (CDF) for reputation value. As we can see, the curves of $\vartheta_i = 1.2$ and $\vartheta_i = 1.5$ are to the left of $\vartheta_i = 1$. In Fig. 13, the generated transaction scores conform to a normal distribution with a mean of 0.6 and a standard deviation of 0.1. The mean of the scores from Fig. 13 is higher than Fig. 12, while the distribution of reputation value in Fig. 13a becomes more concentrated than in Fig. 12a. The increase in the penalty factor leads to the rise in the cost of doing evil, forcing vehicle i to regulate its behavior. In other words, only by continuously providing high-quality content services to requesters can a vehicle accumulate a high reputation value.

7 Conclusion

A blockchain-based secure and scalable V2V video content dissemination scheme has been proposed in this paper. The goal is to achieve an excellent V2V content service ecosystem with resistance to different types of attacks. We present a fair reward strategy to price each V2V content transaction. A content-providing vehicle selection policy supporting SVC-based many-to-one video content delivery is designed to realize quality-adjustable, mobility-aware, secure, and trusted video transmission. Smart contracts are deployed to regulate transaction triggering, verification, and rewards. We present the security analysis and simulation results to confirm the feasibility and efficiency of the proposed scheme.

When supporting large-scale V2V video distribution, traditional blockchain frameworks face difficulties such as low transaction consensus efficiency, complex coordination of multi-party trust, high latency, and low throughput. Our ongoing work focuses on consortium blockchain-based IoV service framework, solving the multi-party trust problem in V2V video content transactions and improving system versatility and scalability.

Acknowledgements The authors gratefully acknowledge the financial assistance provided by the National Natural Science Foundation of China, Natural Science Foundation of Jiangsu Province, and other research projects.

Author contribution Hang Shen and Xin Liu wrote the main manuscript text. Ning Shi, Tianjing Wang, and Guangwei Bai provided guiding ideas and suggestions. All authors reviewed the manuscript.

Funding This work was supported in part by the National Natural Science Foundation of China under Grants 61502230 and 61501224,

the National Project Funding for Key R &D Programs under Grant 2018YFC0808500, the Natural Science Foundation of Jiangsu Province under Grant BK20201357, and the Six Talent Peaks Project in Jiangsu Province under Grant RJFW-020.

Data availability Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Declarations

Ethical approval and consent to participate This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication All authors agree to publish the paper and related research results of the paper.

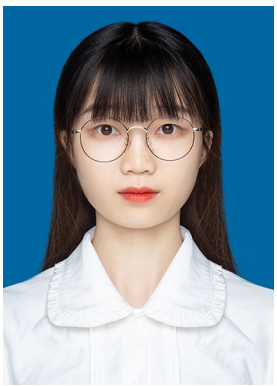
Conflict of interest We have no conflict of interest to declare that are relevant to the content of this article.

References

1. Qiao J, He Y, Shen XS (2018) Improving video streassming quality in 5G enabled vehicular networks. IEEE Wireless Commun 25(2):133–139
2. Bagheri H, Noor-A-Rahim M, Liu Z, Lee H, Pesch D, Moessner K, Xiao P (2021) 5G NR-V2X: Toward connected and cooperative autonomous driving. IEEE Commun Stand Mag 5(1):48–54
3. Cheng X, Chen C, Zhang W, Yang Y (2017) 5G-enabled cooperative intelligent vehicular (5genciv) framework: When benz meets marconi. IEEE Intell Syst 32(3):53–59
4. Abbas F, Fan P, Khan Z (2018) A novel low-latency V2V resource allocation scheme based on cellular V2X communications. IEEE Trans Intell Transp Syst 20(6):2185–2197
5. Sun Y, Xu L, Tang Y, Zhuang W (2018) Traffic offloading for online video service in vehicular networks: a cooperative approach. IEEE Trans Veh Technol 67(8):7630–7642
6. Meng J, Lu H, Liu J (2020) Joint quality selection and caching for SVC video services in heterogeneous networks. In: IEEE WCNC, pp 1–6
7. Zhou H, Wang X, Liu Z, Ji Y, Yamada S (2018) Resource allocation for SVC streaming over cooperative vehicular networks. IEEE Trans Veh Technol 67(9):7924–7936
8. Maleh Y, Shojafar M, Darwish A, Haqiq A (2019) Cybersecurity and privacy in cyber physical systems. CRC Press. https://books.google.com.hk/books?id=PVOWDwAAQBAJ
9. Zhang Y, Bai X (2019) Comparative analysis of VANET authentication architecture and scheme. Int Symp Comput Intell Des (ISCID) 2:89–93
10. Liao D, Li H, Sun G, Zhang M, Chang V (2018) Location and trajectory privacy preservation in 5G-Enabled vehicle social network services. J Netw Comput Appl 110:108–118
11. Lu T, Li J, Zhang L, Lam KY (2019) Group signatures with decentralized tracing. In: International Conference on Information Security and Cryptology, Springer, pp 435–442
12. Adhikari M, Munusamy A, Hazra A, Menon VG, Anavangot V, Puthal D (2021) Security and privacy in edge-centric intelligent internet of vehicles: Issues and remedies. IEEE Consum Electron Mag. https://doi.org/10.1109/MCE.2021.3116415
13. Rawat DB, Doku R, Adebayo A, Bajracharya C, Kamhoua C (2020) Blockchain enabled named data networking for secure vehicle-to-everything communications. IEEE Netw 34(5):185–189
14. Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo KKR (2020) A systematic literature review of blockchain cyber security. Digit Commun Netw 6(2):147–156
15. Ahram T, Sargolzaei A, Sargolzaei S, Daniels J, Amaba B (2017) Blockchain technology innovations. In: IEEE TEMSCON, pp 137–141
16. Dinh TTA, Liu R, Zhang M, Chen G, Ooi BC, Wang J (2018) Untangling blockchain: a data processing view of blockchain systems. IEEE Trans Knowl and Data Eng 30(7):1366–1385
17. Zhang R, Xue R, Liu L (2019) Security and privacy on blockchain. ACM Comput Surv 52(3):1–34
18. Maleh Y, Shojafar M, Alazab M, Romdhani I (2020) Blockchain for cybersecurity and privacy: Architectures, challenges, and applications. Security, Audit and Leadership Series, CRC Press. https://books.google.com.hk/books?id=dC7yDwAAQBAJ
19. Li H, Wang K, Miyazaki T, Xu C, Guo S, Sun Y (2019) Trust-enhanced content delivery in blockchain-based information-centric networking. IEEE Netw 33(5):183–189
20. He S, Lu Y, Tang Q, Wang G, Wu CQ (2021) Fair peer-to-peer content delivery via blockchain. Preprint at http://arxiv.org/abs/2102.04685
21. Li M, Weng J, Yang A, Liu JN, Lin X (2019) Toward blockchain-based fair and anonymous ad dissemination in vehicular networks. IEEE Trans Veh Technol 68(11):11248–11259
22. Han D, Zhu Y, Li D, Liang W, Souri A, Li KC (2021) A blockchain-based auditable access control system for private data in service-centric IoT environments. IEEE Trans Industr Inform 18(5):3530–3540
23. Zaidi S, Bitam S, Mellouk A (2017) Enhanced user datagram protocol for video streaming in VANET. In: IEEE ICC, pp 1–6
24. Bradai A, Ahmed T (2014) ReViV: Selective rebroadcast mechanism for video streaming over VANET. In: IEEE VTC Spring, pp 1–6
25. Xing M, Cai L (2012) Adaptive video streaming with inter-vehicle relay for highway VANET scenario. In: IEEE ICC, pp 5168–5172
26. Shi L, Zhao L, Zheng G, Han Z, Ye Y (2019) Incentive design for cache-enabled D2D underlaid cellular networks using Stackelberg game. IEEE Trans Veh Technol 68(1):765–779
27. Xu Q, Su Z, Yang Q (2019) Blockchain-based trustworthy edge caching scheme for mobile cyber-physical system. IEEE Internet Things J 7(2):1098–1110
28. De Pellegrini F, Massaro A, Goratti L, El-Azouzi R (2016) A pricing scheme for content caching in 5G mobile edge clouds. In: IEEE WINCOM, pp 193–198
29. Souri A (2022) Artificial intelligence mechanisms for management of QoS-aware connectivity in internet of vehicles. J High Speed Netw (Preprint) 1–10
30. Shah G, Valiente R, Gupta N, Gani SMO, Toghi B, Fallah YP, Gupta SD (2019) Real-time hardware-in-the-loop emulation framework for DSRC-based connected vehicle applications. In: IEEE CAVS, pp 1–6
31. Gao F, Zhu L, Shen M, Sharif K, Wan Z, Ren K (2018) A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks. IEEE Netw 32(6):184–192
32. Ni Y, Cai L, He J, Vinel A, Li Y, Mosavat-Jahromi H, Pan J (2020) Toward reliable and scalable internet of vehicles: Performance analysis and resource management. Proc IEEE 108(2):324–340
33. Chelladurai U, Pandian S (2021) Hare: A new hash-based authenticated reliable and efficient modified merkle tree data structure to ensure integrity of data in the healthcare systems. J Amb Intel Hum Comp 1–15
34. Zhang X, Zhu Q, Poor HV (2020b) Sequential hypothesis criterion based optimal caching schemes over mobile wireless networks. In: IEEE ISIT, pp 1254–1258
35. Liu Y, Yu FR, Li X, Ji H, Leung VC (2018) Resource allocation for video transcoding and delivery based on mobile edge computing and blockchain. In: IEEE GLOBECOM, pp 1–6

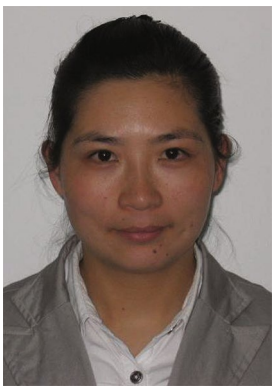
36. Zhu H, Cao Y, Jiang T, Zhang Q (2018) Scalable NOMA multicast for SVC streams in cellular networks. IEEE Trans Commun 66(12):6339–6352
37. Fang S, Mao H (2018) A connectivity-aware caching algorithm for vehicular content centric networks with cache-enabled vehicles. In: IEEE/CIC ICCC Workshops, pp 232–236
38. Zhang K, Cao J, Liu H, Maharjan S, Zhang Y (2020) Deep reinforcement learning for social-aware edge computing and caching in urban informatics. IEEE Trans Ind Informat 16(8):5467–5477
39. Su Z, Hui Y, Luan TH, Liu Q, Xing R (2021) Reputation based content delivery in information centric vehicular networks. In: The Next Generation Vehicular Networks, Modeling, Algorithm and Applications, pp 29–47

Hang Shen is currently an Associate Professor with the Department of Computer Science and Technology, Nanjing Tech University, Nanjing, China. He received the Ph.D. degree (with honors) in Computer Science from the Nanjing University of Science and Technology. He worked as a Full-Time Postdoctoral Fellow with the Broadband Communications Research (BBCR) Lab, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, from 2018 to 2019. His research interests involve space–air–ground integrated vehicular networks, network security, and privacy computing. He serves as an Associate Editor for the IEEE Access and an Academic Editor for the *Mathematical Problems in Engineering*.



Xin Liu received the B.S. degree in Network Engineering from Hunan University of Humanities, Science and Technology, Hunan, China. She is currently an M.S. student at the Department of Computer Science and Technology, Nanjing Tech University, Nanjing, China. Her research interests include blockchain, vehicular networks, and their privacy and security.

Ning Shi holds a bachelor's degree from Tsinghua University and a doctorate from Hong Kong University of Science and Technology. He is a leading domestic researcher in supply chain management and blockchain research. He is also a young and middle-aged leading talent in the field of cybersecurity and informatization of the Internet Information Office of the Jiangsu Provincial Party Committee, a talented person in innovation and innovation of Jiangsu Province, and a top expert in Nanjing. He used to be a senior researcher at IBM China Research Institute and a professor at the School of Management of Sun Yat-sen University. He is currently the dean of Nanjing Trusted Blockchain and Algorithm Economics Institute, the chairman of Nanjing Jinninghui Technology, the visiting professor of Macau University of Science and Technology, the consultant of the Strategy Committee of Nanjing Digital Finance Industry Research Institute, and the chief scientist of the ``Blockchain Industry Finance" laboratory of Foshan Rural Commercial Bank. He has presided over or participated in more than 10 National Natural Science Foundation projects, and published more than 30 high-quality papers. He has 57 invention patents in the blockchain field, and obtained 53 software copyrights. He has served as a member of several academic committees. He was named a highly cited scholar in China's decision science field by Elsevier for six consecutive years, and one of the most influential scholars in China's decision science field.



Tianjing Wang holds a BSc. (2000) in Mathematics at the Nanjing Normal University, an MSc. in Mathematics at the Nanjing University in 2005, and a Ph.D. in Signal and Information Processing at the Nanjing University of Posts and Telecommunications in 2009. From 2011 to 2013, she was a postdoctoral fellow with the School of Electronic Science and Engineering, Nanjing University of Posts and Telecommunications. From 2013 to 2014, she was a visiting scholar with the Department of Electrical and Computer Engineering, State University of New York at Stony Brook. She is now an Associate Professor with the Department of Computer Science and Technology at Nanjing Tech University. Her research interests include integrated sensing and communications for V2X, and artificial intelligence and machine learning for future networking.

Guangwei Bai received the B.Eng. and M.Eng. degrees in computer engineering from Xi'an Jiaotong University, Xi'an, China, in 1983 and 1986, respectively, and the Ph.D. degree in Computer Science from the University of Hamburg, Hamburg, Germany, in 1999. From 1999 to 2001, he worked at the German National Research Center for Information Technology, Germany, as a Research Scientist. In 2001, he joined the University of Calgary, Calgary, AB, Canada, as a Research Associate. Since 2005, he has been working at Nanjing Tech University, Nanjing, China, as a Professor in Computer Science. From October to December 2010, he was a Visiting Professor with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. His research interests include architecture and protocol design for communication networks, multimedia networking, network security, and location-based services. He is a member of the ACM and a Distinguished Member of CCF.