A Secure Content Sharing Scheme Based on Blockchain in Vehicular Named Data Networks

Chen Chen, *Senior Member, IEEE*, Cong Wang, Tie Qiu, *Senior Member, IEEE*, Ning Lv, and Qingqi Pei, *Senior Member, IEEE*

***Abstract*—Vehicular named data networking (VNDN) has recently emerged as a novel paradigm to facilitate content-centric data sharing for Internet of Vehicles. However, an information holder can spread fake data to clients for malicious purposes, which may affect the driving decision of the recipient, or even worse, cause traffic congestion and accidents. In this article, we build a data-sharing system that consists of a double-layer blockchain. The nodes at the bottom layer request for service by announcing their requirements in the NDN paradigm. For the upper layer, the nodes submit their demands and supplies to the nearest roadside unit for further matching. We model the balance between the demand and supply as a matching game. To encourage nodes to provide positive services, a reputation management mechanism that combines negative and positive transaction records is proposed. Simulation results verify the validity of our system, and the data-sharing mechanism fosters a secure information interaction in the VNDN.**

***Index Terms*—Blockchain, data sharing, matching theory, vehicular named data networking (VNDN).**

I. Introduction

INTERNET of Vehicles (IoV) has emerged as a key architecture that promises to enhance traffic experience with various safety-related (traffic accident, sudden braking, etc.) and nonsafety-related (commercial, entertainment, etc.) applications to a reality. Vehicles in IoV always rely on unique IDs (primarily the IP addresses), regardless of the type of applications, to position termini and to establish end-to-end communications [1]. Due to the very properties of IoV, such as distributed operation, limited bandwidth, node mobility, and dynamic network topology, a persistent and robust connection is difficult to maintain [2], [3]. Furthermore, as the number of electronic devices continues to grow, it becomes increasingly tough to assign an IP address for every device, especially to devices with high mobility. Interestingly, communications among vehicles concentrate more on content, instead of their actual carriers, giving rise to named data networking (NDN) application in IoV [vehicular named data networking (VNDN)] [4]. Fig. 1 shows a request-driven communication model that is officially adopted in the VNDN. A consumer node (the *Requester*) issues an *Interest* packet that contains the content name, instead of naming the end-to-end hosts, when it wants to get service [5]. When a data holder receives the *Interest*, it prepares a *Data* packet and sends the packet to the requester. Compared to the nodes in the traditional IoV, the vehicles in the VNDN are allowed to communicate with each other diametrically, prior to the knowledge of any authentication or IP address.

A. Motivation

In the VNDN, a consumer will broadcast its *Interest* if it desires information. If more than one node has the content that the consumer wants and receives the *Interest*, then all of these nodes will send their *Data* to the requester separately, which may lead to a waste of transmission resources and even a broadcast storm, especially in large-scale networks. An appropriate matching mechanism will be beneficial to the system, that is, find the best match among these nodes for packet reply. Another concern is the authenticity of the propagated information. In content-centric IoV, vehicles may request traffic information, such as traffic accident information. Effective data sharing on traffic conditions will greatly optimize road utilization. However, malicious nodes in the VNDN may disseminate fake messages, which may aggravate the driving efficiency. Many vehicles may receive such false information and lead to traffic congestion or cause an accident. Therefore, it is necessary to establish a reputation evaluation scheme (RES) to encourage nodes to publish reliable information during data sharing.

More practically, vehicles with traffic or entertainment information may be not willing to participate as suppliers in a service trading market due to their concerns over the transmission

Manuscript received June 1, 2019; revised August 13, 2019 and October 20, 2019; accepted November 11, 2019. Date of publication November 19, 2019; date of current version February 6, 2020. This work was supported in part by the National Key Research and Development Program of China under Grant 2017YFE0121400; in part by the National Natural Science Foundation of China under Grant 61571338, Grant U1709218, Grant 61672132, and Grant U1636209; in part by the Key Research and Development Plan of Shaanxi Province under Grant 2017ZDCXL-GY-05-01, Grant 2019ZDLGY13-04, and Grant 2019ZDLGY13-07; in part by the Key Laboratory of Embedded System and Service Computing (Tongji University) under Grant ESSCKF2019-05; in part by the Xi'an Key Laboratory of Mobile Edge Computing and Security under Grant 201805052-ZD3CG36; and in part by the Innovation Fund of Xidian University under Grant 5001-20109195456. Paper no. TII-19-2234. *(Corresponding author: Tie Qiu.)*

C. Chen, C. Wang, N. Lv, and Q. Pei are with the State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China (e-mail: cc2000@mail.xidian.edu.cn; xidcongw@163.com; nlv@mail.xidian.edu.cn; qqpei@mail.xidian.edu.cn).

T. Qiu is with the School of Computer Science and Technology, Tianjin University, Tianjin 300350, China (e-mail: qiutie@ieee.org).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2019.2954345

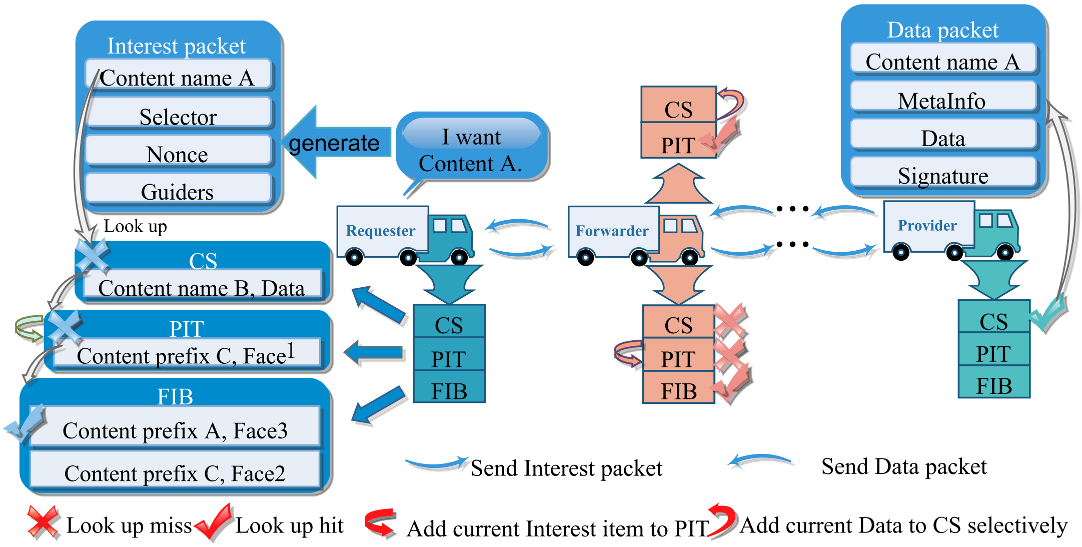


Fig. 1. Communication model in VNDN.

energy consumption or privacy. In this case, information supply and demand are unbalanced among vehicles. Moreover, privacy leakage [6], [7] is also an important issue. The traditional centralized interactive information trading relies on a trusted third party such as Base Station (BS), which suffers from problems including single point of failure and privacy leakage. Therefore, it is imperative to design a proper incentive mechanism and privacy protection scheme to encourage more vehicles to share their resources while preserving the privacy of vehicles during the trade.

B. Contribution

To address security, a promising blockchain technology with the advantages of decentralization, security, and trust has been introduced in recent years [8], [9].

It has been successfully applied in many fields, such as smart contracts, public key infrastructure (PKI), domain name server (DNS), decentralized Internet of Things (IoT), and IoV [10].

Considering that the computational complexity in matching execution increases with the number of nodes and allocating supply and demand for all nodes is time consuming, we exploit the blockchain technology to develop a regionalized secure information transaction trading system in the VNDN.

The contributions of this article are summarized as follows.

1) We exploit a double-layer blockchain for data sharing, which ensures data transmission security. And incentives have been developed to encourage information sharing between nodes.
2) To prevent malicious nodes from spreading false messages, we design a reasonable RES, which scores the quality of service of different providers by combining negative and positive sharing records.
3) A trading system that is modeled as a one-to-many matching problem to balance the client requirements with the server's supply. We define different utility functions for both server and client to maximize social welfare.

The rest of this article is organized as follows. The system elements is described in Section II. Section III presents the system model of our information trading system. Section IV defines and mathematically formulates the matching problem. Section V presents the assignment game algorithm. Section VI is the numerical analysis of our proposed protocol. Finally, Section VII concludes of this article.

II. System Elements

A. Core System Components

The model for information-centric data trading among vehicles is shown in Fig. 2. The core system components are as follows.

1) On-Board Units (OBUs): We assume that each vehicle is equipped with OBU for data trading. There are three kinds of OBU in localized content trading in our system: client OBU, server OBU, and relay OBU. Each OBU chooses its own character based on its demand status and network demand.

2) Roadside Units (RSUs): RSUs aggregate local transactions or wireless communication services for OBUs. They can also act as information exchange brokers, i.e., they collect the supply and demand of different clients and servers for allocation.

3) Prerequisites for the Realization of VNDN Data Trading: Each wireless access point with a built-in ledger records the transactions history of traded information among OBUs. The client OBUs pay to the server OBUs according to the records in the smart ledger. Each OBU and RSU has storage space to hold the transaction record. OBUs can cache the information downloaded from the cellular network or gets it from other nodes. To make the transaction more convenient, we present a new digital cryptocurrency, vehicle coins, as the virtual currency to trade data.

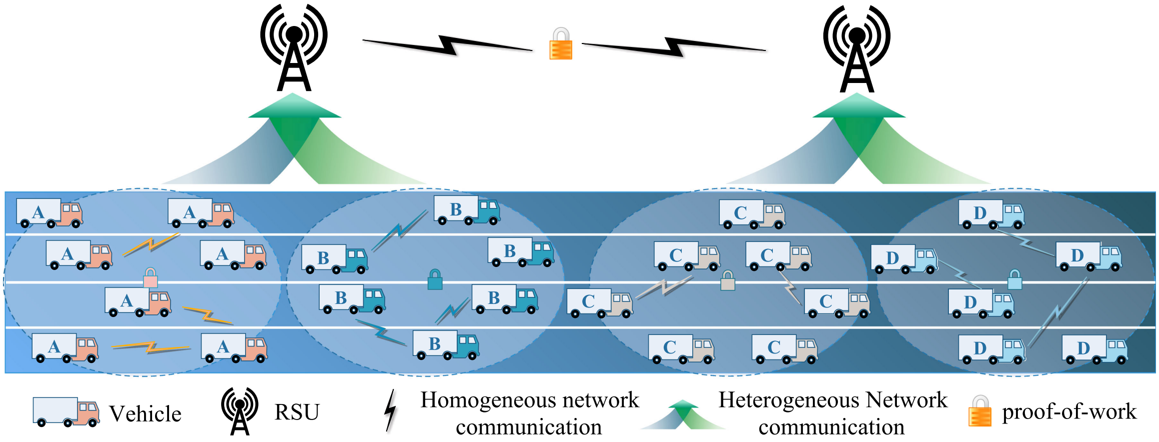

A
B
C
D
Vehicle
RSU
Homogeneous network communication
Heterogeneous Network communication
proof-of-work

Fig. 2. System model: Double-layer blockchain.

B. Double-Layer Blockchain in VNDN

In this article, a double-layer blockchain is built for secure content sharing in the VNDN. A content retrieval in a large-scale VNDN may be difficult due to the number of vehicles on a road section. Besides, the aggregation of forwarding information base (FIB) is troublesome because of the OBUs' mobility. During data trading, we divide the OBUs into several groups. The grouped OBUs (GOs) will request for data within its group by diffusing their *Interests*, i.e., with NDN. However, some of the requests may not be satisfied within the scope of the current group, in which case, each group will send their unsatisfied requests to RSU seeking services.

1) Blockchain Selection: We treat different groups as separate companies. The request from a GO of a *company* will first be transmitted to the members within the *company*. If the request is satisfied, the client will pay for the server, and this transaction will be recorded. The transaction is completed faster within a group compared to spreading the *Interest* to a large-scale network. Obviously, the members in a different *company* are different, and the content they request may be different, so the transaction records maintained by different *companies* are also different. Considering these characteristics of the GOs, we built a private blockchain for OBUs (PBO) to guarantee transaction security. A private blockchain is an important technology in achieving an encrypted transaction. The biggest benefit of a private blockchain compared to a centralized database is the ability to encrypt audits and publicly identifiable information. No one can tamper with the data, and when an error occurs, the source of the error can be traced. The private chain is faster and cheaper than the public chain, while still respecting the client's privacy.

If there are requests that cannot be satisfied by other GOs within the group, the group will seek for help from RSUs. The RSUs will collect the demands and data available of different PBOs and make further matching. In a consortium blockchain, the generation of each block is determined by all preselected nodes. Other nodes can participate in transactions, but they do not participate in the consensus process [11]. A consortium blockchain can shorten blocks' creation time [12]. In this article, we build a consortium blockchain for RSUs (CBR), which can be seen as intermediary agents for balancing supply and demand of PBOs, to release the high cost while processing consensus.

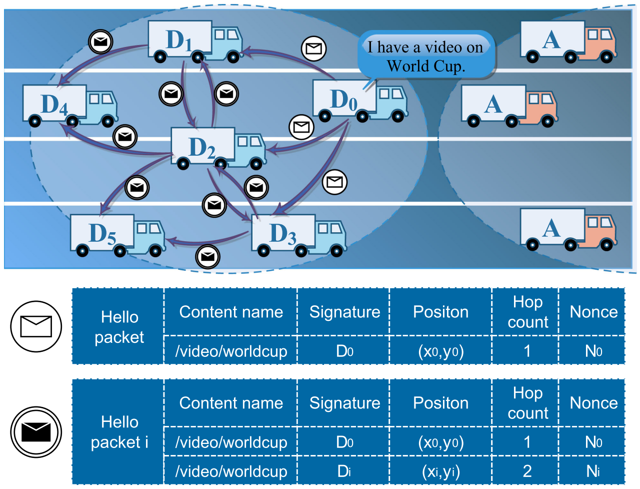
2) Transaction Record and Block Preparation: The transaction records of the data exchange are stored in smart ledgers. The OBUs' anonymities, location information, transacted data, deal price, and the timestamp of transaction generation are included in trading information. For security and authenticity, the transactions are encrypted with the digital signatures of the transactors. After recording the transaction, these records are encrypted and structured into blocks in a linear chronological order, after being audited by the consensus process. For traceability and verification, each block contains information, such as the digital signature of the primary node and the hash value of the block. After the transaction have been packed in blocks and added to the blockchain, the data become accessible to OBU and RSU in the blockchain.

III. Information Trading System With Double-Layer Blockchain

Fig. 2 illustrates the system model of the double-layer blockchain built for secure content sharing in the VNDN. At the bottom layer, we divide the vehicles into several group blockchains based on the movement trends similarity, i.e., PBO. Then, at the top layer, the consensus process is executed by the preselected RSUs, i.e., CBR. We assume that all vehicles that tend to participate in information sharing systems are legitimate entities after registering with a trusted authority.

A. Operation Details on PBO

1) Group Initialization in Data Trading: In the data trading system, we divide the vehicles into several groups. To achieve a higher data trading efficiency, we concentrate more on the robustness of the group when grouping the OBUs, i.e., balance the number of each group and have fewer entries or departures. We take the *mobility value* defined in mobility-based metric



Hello packet	Content name	Signature	Positon	Hop count	Nonce
	/video/worldcup	D0	(x0,y0)	1	N0

Hello packet i	Content name	Signature	Positon	Hop count	Nonce
	/video/worldcup	D0	(x0,y0)	1	N0
	/video/worldcup	Di	(xi,yi)	2	Ni

Fig. 3. Operation details of PBO.

for clustering (MOBIC) [13] as a foundation to initialize the PBO. The main idea of the MOBIC is to take into account the current position and mobility of the individual nodes with respect to its neighbors. The relative mobility metric $M_Y^{\mathrm{rel}}(X) = 10\log_{10}\frac{RxPr^{\mathrm{new}}_{X\to Y}}{RxPr^{\mathrm{old}}_{X\to Y}}$ denotes the relative mobility between X and Y, where $RxPr_{X\to Y}$ indicates the distance between the transmitting and receiving node pair (X, Y). The subscripts new and old indicate the parameter with current time slot and previous slot, respectively. After that, the mobility value M_Y can be found by calculating the variance of relative mobility samples

$$M_Y = \mathrm{var}_0(M_Y^{\mathrm{rel}}(X_1), M_Y^{\mathrm{rel}}(X_2), \ldots, M_Y^{\mathrm{rel}}(X_m)) \quad (1)$$

where $\mathrm{Neighbor}_Y = \{X_1, X_2, \ldots, X_m\}$. The vehicle with the largest mobility value is selected as the first PBO center, which act as a representative to negotiate with RSU. Then, this center and its neighbors form the first group. The vehicle with the largest mobility value among the unclassified nodes is selected as the second PBO center. This process is executed until all vehicles are grouped.

2) System Preparation: After the grouping, each center will first register with the RSU, and publish its information, including electronic signature, location, group number, and so on, to other members. The node receiving the information from the central node will get its own public/privacy key, certificate, and wallet address. Each vehicle will issue the content that it holds by announcing its content name, position, and signature periodically. A node will follow the process, as shown in Fig. 3 for new content creation: D_0 first prepares a *hello packet*, and then, broadcasts the packet to its neighbors (D_1, D_2, D_3) within its group. Receiving a *hello packet* with its hop count equals 1, the recipients would update its FIB and append its signature, position, and hop count information in the *hello packet*. In this way, the *hello packet* i is created. Then, D_i will broadcast *hello packet* i to its neighbors. Upon receiving a *hello packet* with hop count equals 2, the receivers (D_4, D_5) would add the new item $(\mathrm{content}, \mathrm{forwarder})$ to its FIB if the newly received nonce did not exist previously; otherwise, this packet will be dropped.

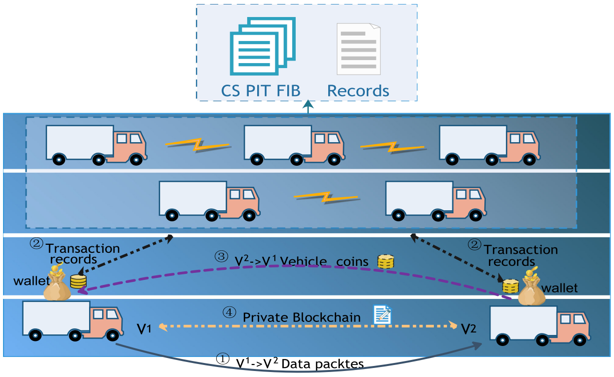


Fig. 4. Data trading.

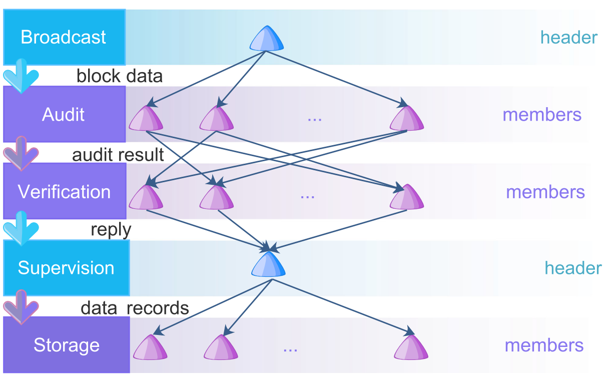


Fig. 5. Consensus process.

3) Data Trading Among OBUs: Client OBUs prepare *Interest* that specifies the content name and send out the *Interest*. After data trading, the client pays for the data transaction through a wallet address of the server, as shown in Fig. 4. The consumer generates transaction records, and the server verifies them for further audit.

4) Building Blocks and Carrying Out Consensus Process: After trading, PBO centers collect all local data transaction records and pack them into a block within its group. The block is stored in the system after being confirmed. It is difficult for the vehicles in our system to *mine* a block by calculating the hash value based on a random nonce value because vehicles have limited computing power and proof-of-work (PoW) imposes a high level of computational cost on the transaction verification process. Therefore, the center selected to pack the block will act as the leader of the current consensus process, as shown in Fig. 5. During the consensus process, the center first broadcasts the block data to its members. After a series of audits, the header will send the transaction record to other members if the majority of the members agree on the blocks. Then, the leader will be awarded with vehicle coins and the current block will be stored in the blockchain.

5) System Maintenance: It is generally known that the topology in IoV is not stable, even in highway environments. Therefore, we must take into account the effect of the topological dynamics on the group changes. When an OBU drives away from the current leader, it will leave the current PBO. After that,

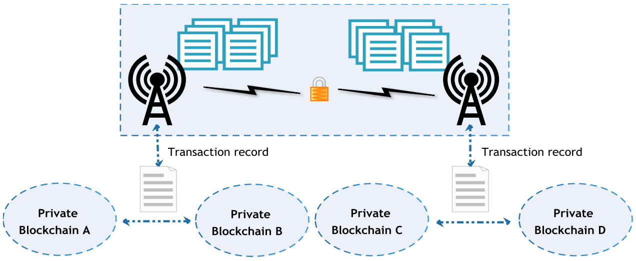


Fig. 6. Data transactions record among PBOs.

if there is another PBO center within its communication range, the node will submit an application for certification to the leader to join this new group. Otherwise, this node will regard itself as the center of a new group. Note that the cluster and maintenance method are not the focus of this article.

B. Operation Details on CBR

1) System Preparation: After registering with the nearest RSU, each header becomes a legitimate entity and a member over which the RSU has jurisdiction. After that, the RSU works as a supervisor of the headers and treats each group as an individual. All RSUs in a certain area constitute a CBR.

2) Data Trading Among PBOs: Each PBO header would collect all unsatisfied requests (demand) and the name of available data (supply) periodically. Then, these request/content name will be packaged and sent to the nearest RSU. The RSU matches the data supply and demand among the PBOs. Here, we take the matching theory to execute data negotiation and transactions among PBOs. (Details of the matching mechanism will be given in Section IV.) After matching, as shown in Fig. 6, the RSU will create the transaction record.

3) Building Blocks and Finding Proof-of-Work: The process of building blocks is identical to that of the PBO. RSUs within a CBR need to verify (mine) a block by solving a computationally difficult PoW puzzle [14]. Every RSU competes to find a hash value that meets a preset difficulty [15]. The fastest RSU is selected as the header of the CBR.

4) Carrying Out Consensus Process: The fastest RSU with a valid PoW becomes the leader of the current consensus process. The details of the consensus process of the CBR is the same as that of the PBO.

IV. Problem Definition for Trading

In this section, we present the problem definition in the network to maximize social welfare about data sharing.

A. Reputation Management in CBR

In data sharing, the vehicle may diffuse false information because of faulty sensors, virus infection, or even for selfish reason [16], [17]. To alleviate the impact of such malicious messages on system deterioration, we must endeavor to suppress the spread of these false messages. As a general rule, requesters are reluctant to request information from providers who always spread falsehood. To improve the transmission availability, it is essential to design a mechanism that quantifies the vehicle's reputation.

We propose an RES for high-quality data sharing in this section. $\mathrm{provider}_j$ toward $\mathrm{requester}_i$, i.e., $R_{j\to i}$, by taking their interaction history into consideration. This consists of the requester's satisfaction and interaction time. If a positive sharing (PS) arises between the node pair, i.e., an interaction occurs where $\mathrm{requester}_i$ found the data sent by $\mathrm{provider}_j$ is useful, the reputation of the provider toward the consumer is enhanced. Conversely, an occurrence of negative sharing (NS) will lead to a decrease in reputation value. Nodes with higher reputation indicates that data with higher quality will be provided. Consumers prefer providers with higher reputation values.

1) Confidence Level (CL): In an RES, a higher (CL between $\mathrm{requester}_i$ and $\mathrm{requester}_i$ means that the $\mathrm{requester}_i$ has more prior knowledge about the $\mathrm{provider}_j$, leading to more accurate and reliable reputation calculation. The CL of $\mathrm{requester}_i$ toward $\mathrm{provider}_j$ can be calculated as $\mathrm{CL}_{j\to i} = \frac{\mathrm{IT}_{j\to i}}{\sum_{j\in N}\mathrm{IT}_{j\to i}}$, where $\mathrm{IT}_{j\to i}$ indicates the number of interactions between $\mathrm{requester}_i$ and $\mathrm{provider}_j$, and N is a set of all the providers that interacted with $\mathrm{requester}_i$. Since there are two kinds of interactions, i.e., PS and NS, we classify CL into the following two categories:

$$\mathrm{CL}_{P_{j\to i}} = \frac{\mathrm{IT}_{P_{j\to i}}}{\sum_{j\in N}\mathrm{IT}_{P_{j\to i}}}, \mathrm{CL}_{N_{j\to i}} = \frac{\mathrm{IT}_{N_{j\to i}}}{\sum_{j\in N}\mathrm{IT}_{N_{j\to i}}} \tag{2}$$

where $\mathrm{IT}_P/\mathrm{IT}_N$ indicates the number of PS/NS interaction. In this way, $\mathrm{CL}_P/\mathrm{CL}_N$ denotes the positive/negative CL.

2) Interaction Frequency and Event Timeliness: A CBR is not always reliable or always unreliable, and the trustfulness between data provider and requester varies over time [15]. It is common sense that recent events have a larger impact on the accurate and reliable reputation calculation. The credit value of $\mathrm{provider}_j$ toward $\mathrm{requester}_i$ can be calculated as $\mathrm{r}_{j\to i} = \sum_{t=1}^{n}\mathrm{F}(T_c - T_{t_{j\to i}})$, where T_c denotes the current time and $T_{t_{j\to i}}$ indicates the time when the $\mathrm{provider}_j$ shared data with $\mathrm{requester}_i$ for the tth time. n is the total interaction times from j to i. $\mathrm{F(x)}$ is a weight function that adjusts the relative importance of frequency and timeliness. Similar to the CL, the credit value can also be classified into positive reputation value and negative reputation value

$$\mathrm{r}_{P_{j\to i}} = \sum_{t=1}^{n_P}\mathrm{F}(T_c - T_{P_{t_{j\to i}}}) \tag{3}$$

$$\mathrm{r}_{N_{j\to i}} = \sum_{t=1}^{n_N}\mathrm{F}(T_c - T_{N_{t_{j\to i}}}). \tag{4}$$

3) Reputation Management: A PS interaction between two vehicles would strengthen the reputation of the $\mathrm{provider}$ toward the $\mathrm{requester}$. On the contrary, a NS interaction would deteriorate the credit value. Therefore, we can calculate the reputation as $\mathrm{R}_{j\to i} = \mathrm{CL}_{P_{j\to i}}\mathrm{r}_{P_{j\to i}} - \mathrm{CL}_{N_{j\to i}}\mathrm{r}_{N_{j\to i}}$.

B. Data Transmission Rate

In a transaction, the client considers not only the credibility of the server, but also the time required to receive the message. Therefore, we have to evaluate the data transmission rate during a data trading. The signal-to-interference-noise ratio of the PBO header H_k that is registered to RSU_j at the fth subchannel is given by

$$\mathscr{S}_k^j(f) = \frac{\mathcal{P}_k^f \mathcal{L}_{kj}^f}{\sum_{k' \in \mathcal{K}_j, k' \neq k} \mathcal{P}_{k'}^f \mathcal{L}_{k'j}^f + \sigma^2} \tag{5}$$

where $\mathcal{P}_k^f$ is the uplink transmission power from H_k^j in the subchannel f, $\mathcal{L}_{kj}^f$ is the propagation loss from H_k to the RSU_j in the subchannel f, and σ^2 denotes the noise variance. $\mathcal{K}_j$ is the set of indices of PBO headers subscribed to RSU_j. Therefore, the uplink data transmission rate from H_k to RSU_j is $\mathcal{T}_r^{kj} = B \sum_{f \in \mathcal{C}_{kj}} \log_2(1 + c_3^k \mathscr{S}_k^j(f))$, where $\mathcal{C}_{kj}$ is the subchannel set that allocated to PBO header H_k by RSU_j, $c_3^k = -(c_2^k \ln(\mathrm{BER}_k^f / c_1^k))$, and BER_k^f is the bit error rate [18].

C. Matching Function Definitions

An RSU divides all PBOs into two disjoint finite sets of players for a particular content $\gamma_k \in \Gamma = \{\gamma_i\}_{i=1}^{|\Gamma|}$ in a time interval T, i.e., clients $\Theta^k = \{\theta_i^k\}_{i=1}^{|\Theta^k|}$ and servers $\Xi^k = \{\xi_i^k\}_{i=1}^{|\Xi^k|}$. The server can provide data for multiple clients; however, each requester only needs one provider offering the data. In addition, considering the selfishness of the node, clients pay servers with vehicle coins in exchange for information. Therefore, it can be modeled as a one-to-many matching with transfer [19]. The one-to-many matching is defined as $\Psi^k : \{\Theta^k\} \bigcup \{\Xi^k\} \to (\{\Theta^k\} \bigcup \{\Xi^k\}) \times \mathbb{R}^+, k \in \phi^\gamma$ that satisfies the conditions described as follows (where $\phi^\gamma = \{1, \ldots, |\Gamma|\}$ indicates the index sets of Γ):

1) $\Psi^k(\theta_i^k) \subseteq \{\xi_{j' \in \phi^{\theta^k}} \in \Xi^k\}$ and $|\Psi^k(\theta_i^k)| \leqslant q_k^i$ imply that member θ_i^k can be matched to multiple members of Ξ^k. Where $\phi^{\theta^k} = \{1, \ldots, |\Theta^k|\}$ denotes the index sets of Θ^k and $q_i^k \in \mathbb{N}$ indicate the maximum of θ_i^k may fill.
2) $\Psi^k(\xi_i^k) \subseteq \{\theta_{i' \in \phi^{\xi^k}}^k \in \Theta^k\}$ and $|\Psi^k(\xi_j^k)| \in \{0, 1\}$ denote that each client $\xi_i^k \in \Xi^k$ can be matched to at most one server. Similarly, ϕ^{ξ^k} denotes the index sets of Ξ^k.
3) $\Psi^k(\theta_i^k) = (\xi_j^k, p_{ij}^k) \Leftrightarrow \Psi^k(\xi_j^k) = (\theta_i^k, p_{ij}^k)$ indicates that if $\theta_i^k \in \Theta^k$ is matched to $\xi_j^k \in \Xi^k$ with unit transaction price p_{ij}^k for data γ_k, ξ_j^k is also matched to θ_i^k with p_{ij}^k.

We denote our matching function Ψ^k with a three-tuple $\Psi^k : (\Theta^k, \Xi^k, \mathbf{q}^k)$, where $\mathbf{q}^k = \{q_k^1, q_k^2, \ldots, q_k^{|\Theta|}\}$. For notational purposes, θ_0 and ξ_0 are defined as the dummy members of Θ and Ξ, respectively. θ_0 and ξ_0 can be matched to multiple members with no transaction [19]. Then, the (i, j)th element ζ_{ij}^k in the matching matrix $\mathcal{M}$ is defined as $\zeta_{ij}^k = 1$, if $\Psi^k(\xi_i) = (\theta_j, p_{ij}^k)$, $i \in \phi^\theta$, $j \in \phi^\xi$. Otherwise, $\zeta_{ij}^k = 0$.

D. Problem Definition

The purpose of our matching system is to maximize the overall welfare of data sharing. In a transaction, what a client cares about are the vehicle coins, the cost of energy, the quality of the data received, and the wait time to receive the message. We define the satisfaction level of $\mathrm{requester}_i$ while requesting for data γ_k from $\mathrm{provider}_j$ as

$$\mathscr{Q}_{\xi_i^k}(\theta_j^k, \gamma_k) = \frac{1}{1 + e^{-\vartheta[\mathcal{R}_{\xi_i^k}(\theta_j^k, \gamma_k) - \mathcal{R}_{\xi_i^k}^{\mathrm{EXP}}(\gamma_k)]}} \tag{6}$$

where $\mathcal{R}_{\xi_i^k}(\theta_j^k, \gamma_k) = \varsigma \mathrm{R}_{j \to i} + \tau \frac{S_{\gamma_k}}{\mathcal{T}_r^{kj}}$ implies the combination of information reliability and delay, where ς and τ represent the weights of information reliability and transmission delay, S_{γ_k} is the size of γ_k. $\mathscr{Q}_{\xi_i}(\cdot)$ is the Sigmoid function [20] that has been widely used for estimating the satisfaction level of users with respect to service quality in wireless communications [18]. The utility of $\mathrm{requester}_i$ is defined as

$$\mathcal{U}_{\xi_i^k}^{\mathrm{REQ}}(\theta_j^k, \gamma_k, p_{ij}^k) = \mu \mathscr{Q}_{\xi_i^k}(\theta_j^k, \gamma_k) - p_{ij}^k S_{\gamma_k} - \upsilon \mathcal{P}_r^i S_{\gamma_k} \tag{7}$$

where $\mathscr{Q}_{\xi_i}$ is the satisfaction level, p indicates the cost, $\mathcal{P}_r$ is the reception power, and $\mu, \upsilon \in \mathbb{R}^+$ are coefficients with unit revenue per requester satisfaction and reception power cost.

The utility of a server is related to the vehicle coins it receives and the energy it consumes per trade. Therefore, the utility function of $\mathrm{provider}_j$ is defined as

$$\mathcal{U}_{\theta_j^k}^{\mathrm{PRO}}(\xi_i^k, \gamma_k, p_{ij}^k) = p_{ij}^k S_{\gamma_k} - \nu \mathcal{P}_t^j S_{\gamma_k} \tag{8}$$

which reflect the monetary gain of the $\mathrm{provider}_i$ and transmission cost. $\mathcal{P}_t$ is the transmitting power, $\mu \in \mathbb{R}^+$ is a fixed coefficient with unit revenue per provider transmission cost. Therefore, the objective function of our trading system is

$$\begin{aligned}
&\max_{\mathcal{M}} \sum_{k=1}^{|\Gamma|} \sum_{i=1}^{|\Xi^k|} \sum_{j=1}^{|\Theta^k|} \zeta_{ij}^k \left[\mathcal{U}_{\xi_i^k}^{\mathrm{REQ}}(\theta_j^k, \gamma_k, p_{ij}^k) + \mathcal{U}_{\theta_j^k}^{\mathrm{PRO}}(\xi_i^k, \gamma_k, p_{ij}^k)\right] \\
&= \max_{\mathcal{M}} \sum_{k=1}^{|\Gamma|} \sum_{i=1}^{|\Xi^k|} \sum_{j=1}^{|\Theta^k|} \zeta_{ij}^k \Big[\mu \mathscr{Q}_{\xi_i^k}(\theta_j^k, \gamma_k) - p_{ij}^k S_{\gamma_k} - \upsilon \mathcal{P}_r^i S_{\gamma_k} \\
&\qquad + p_{ij}^k S_{\gamma_k} - \nu \mathcal{P}_t^j S_{\gamma_k}\Big] \\
&= \max_{\mathcal{M}} \sum_{k=1}^{|\Gamma|} \sum_{i=1}^{|\Xi^k|} \sum_{j=1}^{|\Theta^k|} \zeta_{ij}^k \Big[\mu \mathscr{Q}_{\xi_i^k}(\theta_j^k, \gamma_k) - \upsilon \mathcal{P}_r^i S_{\gamma_k} + \nu \mathcal{P}_t^j S_{\gamma_k}\Big]
\end{aligned} \tag{9}$$

$$\begin{aligned}
\text{s.t.}: \quad &(a) \sum_{\theta_j^k \in \Theta^k} \zeta_{ij}^k \leq 1 \quad \forall i \in \phi^{\xi^k}, k \in \phi^\gamma \\
&(b) \sum_{\xi_i^k \in \Xi^k} \zeta_{ij}^k \leq q_k^j \quad \forall j \in \phi^{\theta^k}, k \in \phi^\gamma \\
&(c)\ \zeta_{ij}^k = \{0, 1\} \quad \forall i \in \phi^{\xi^k} \forall j \in \phi^{\theta^k}, k \in \phi^\gamma.
\end{aligned} \tag{10}$$

Restrictive condition (a) guarantees that each requester can be matched with only one provider, condition (b) states that at most q clients can be matched with one provider, and condition (c) guarantees that the value of ζ will be either one or zero. Note that if a provider is matched with n multiple clients for message γ_k, providers only need to send ONCE, instead of n times.

Algorithm 1: Assignment Game.

```
1  for All $\gamma_k \in \Gamma$ do
2      Set $t = 1, p_{i,j}^{k,t} = p_{\min j}^{k,t}, b_{i,j}^{k,t} = 0 \forall i \in \phi^{\xi}, j \in \phi^{\theta}$;
3      Set $\mathrm{MATLIST}_c = \{\theta_j\}_{j=1}^{|\Theta|}$, $\mathrm{SLIST}_s = \{\xi_i\}_{i=1}^{|\Xi|}$.
4  for All $\gamma_k \in \Gamma$ do
5      $\theta_j \in \mathrm{MATLIST}_c$ announces $p_{i,j}^{k,t}$ to $\xi_i \in \mathrm{SLIST}_s$;
6      for Each unmatched requester $\xi_i$, $\forall i \in \phi^{\xi}$ do
7          Calculate its demand set $\mathcal{S}_i(p_{i,k}^t)$;
8          if $\mathcal{S}_i(p_{i,k}^t) = \theta_0$ then
9              Set $b_{i,j}^{k,t} = 0, j \in \phi^{\theta}$, $\Psi^k(\xi_i) = \{\theta_0\}$;
10             Remove $\xi_i$ from $\mathrm{SLIST}_s$;
11         else
12             $\xi_{i,k}^t$ bids for $\theta_j$, set $b_{i,j}^{k,t} = 1, j \in \mathcal{S}_i(p_{k,t}^t)$;
13 for All $\gamma_k \in \Gamma$ do
14     for all $\theta_j \in \mathrm{MATLIST}_c$ do
15         if $\sum_{i=1}^m b_{i,j}^{k,t} = 0$ and $p_{i,j}^{k,t} > p_{\min,j}^{k,t}$ then
16             $\Psi^k(\theta_j) = (\xi_{i^*}, p_{i^*,j}^{k,t-1})$, $i^* = \arg\max R_{j\to i}$
17             Remove $\xi_i$ from $\mathrm{SLIST}_s$;
18             if $|\Psi^k(\theta_j)| = q_j^k$ then
19                 Remove $\theta_j$ from $\mathrm{MATLIST}_c$;
20                 Set $b_{i^*,j^+}^{k,t} = 0$, where $j^+ = \mathcal{S}_{i^*}(p_{i^*}^{k,t})$;
21         else if $\sum_{i=1}^m b_{i,j}^{k,t} > 1$ then
22             Set $p_{i,j}^{k,t+1} = p_{i,j}^{k,t} + \epsilon$;
23         else
24             $(\sum_{i=1}^m b_{i,j}^{k,t} = 1)$
25             $\Psi^k(\theta_j) = (\xi_i, p_{i,j}^{k,t}), i = \arg_{i^-} b_{i^-,j}^{k,t} = 1$;
26             Remove $\xi_i$ from $\mathrm{SLIST}_s$;
27             if $|\Psi^k(\theta_j)| = q_j^k$ then
28                 Remove $\theta_j$ from $\mathrm{MATLIST}_c$;
29 for All $\gamma_k \in \Gamma$ do
30     if $\mathrm{MATLIST}_c = \emptyset$ or $\mathrm{SLIST}_s = \emptyset$ then
31         End;
32     else
33         set $t = t + 1$ and go to line 6;
```

Therefore, our one-to-many assignment problem is updated as

$$\max_{\mathcal{M}} \sum_{k=1}^{|\Gamma|} \sum_{i=1}^{|\Xi^k|} \sum_{j=1}^{|\Theta^k|} \zeta_{ij}^k \left[\mu \mathscr{Q}_{\xi_i^k}(\theta_j^k, \gamma_k) - \upsilon \mathcal{P}_r^i S_{\gamma_k} \right] + \sum_{k=1}^{|\Gamma|} \sum_{j=1}^{|\Theta^k|} \mathrm{sign}\left(\sum_{i=1}^{|\Xi^k|} \zeta_{ij}^k \right) \nu \mathcal{P}_t^j S_{\gamma_k} \Bigg] \tag{11}$$

where $\mathrm{sign}(\cdot)$ is the signum function that indicates whether there are nodes requesting for content γ_k from $\mathrm{provider}_j$.

V. Assignment Game Algorithm

In this section, we will introduce the assignment algorithm, which is an improved version of the algorithm proposed in [19], to solve the optimization problem in (11).

The system initialization is depicted in Algorithm 1 lines 1–3. Note that not only is the requester selfish, but also the provider. The provider matches the requester only if its utility is greater than 0, that is, $\mathcal{U}_{\theta_j^k}^{\mathrm{PRO}}(\xi_i^k, \gamma_k, p_{ij}^k) = p_{ij}^k S_{\gamma_k} - \nu \mathcal{P}_t^j S_{\gamma_k} > 0$. Consider the initial price is set as $p_{\min j}^{k,t} \geq \nu \mathcal{P}_t^j$. To judge whether the matching is complete or not, we construct the list of all the servers and clients that remain to be matched denoted by $\mathrm{MATLIST}_s = \{\theta_j\}_{j=1}^{|\Theta|}$, $\mathrm{MATLIST}_c = \{\xi_i\}_{i=1}^{|\Xi|}$, whenever a node completes its matching, it will be moved out of the set.

The clients' demand for information is depicted in lines 4–12. Providers that remain to be matched issue their price allocation offer $\mathbb{P}_j^{k,t} = \{p_{1,j}^{k,t}, p_{2,j}^{k,t}, \ldots, p_{n,j}^{k,t}\}$ to the unmatched requesters in each interaction t. After that, all the requesters determine their demand set as follows:

$$\mathcal{S}_i(\mathbf{P}_i^{k,t}) = \begin{cases} \arg\max_{\theta_j^k \in \mathrm{MATLIST}_p^k} \mathcal{U}_{\xi_i^k}^{\mathrm{REQ}}(\theta_j^k, \gamma_k, p_{i,j}^{k,t}) \\ \text{if } \max_{\theta_j^k \in \mathrm{MATLIST}_p^k} \mathcal{U}_{\xi_i}^{\mathrm{REQ}}(\theta_j^k, \gamma_k, p_{i,j}^{k,t}) \geqslant 0 \\ \theta_0, \qquad \text{otherwise} \end{cases} . \tag{12}$$

Each requester prefers to request content from a provider that maximizes its utility function. Therefore, the demand set for $\mathrm{requester}_i$ is defined as the $\mathrm{provider_j}$ that maximize the utility. Note that the acceptable utility of a provider is greater than 0, which indicates that all the dealer will not trade at a loss. If $\mathrm{provider_j} = \mathcal{S}(p_{i,j}^{k,t})$, the $\mathrm{requester_i}$ will bid for the $\mathrm{provider_j}$ with price $p_{i,j}^{k,t}$, i.e., $b_{i,j}^{k,t} = 1$.

After the requester indicates its wish, the information provider makes a matching choice. To maximize social welfare, in each iteration, we make a match decision for only one requester. The providers' decision making is shown in Algorithm 1 lines 13–20. During each interaction, a provider may receive no bids from any requesters (case 1), receive bids from multiple requesters (case 2), or receive one bid (case 3).

Case 1 (lines 15–20) indicates that there are no requesters that choose current $\mathrm{provider}_j$ as their best match, but there are several requesters ($\Re_j^k = \{\xi_i^k\}, i = \arg_{i^* \in \Xi^k} b_{i^*,j}^{k,t} = 1$) bid for $\mathrm{provider}_j$ in the last interaction. In case 1, the provider will choose $\mathrm{requester}_{i^*}$ that with highest reputation toward $\mathrm{provider}_j$, i.e., $i^* = \arg\max_{\xi_i \in \Re_j^k} R_{j\to i}$ as its *customer*, in this way, $\mathrm{provider}_j$ is matched with $\mathrm{requester}_{i^*}$, $\Psi^k(\theta_j^k) = (\xi_{i^*}^k, p_{i^*,j}^{k,t-1})$. Case 2 (lines 21 and 22) indicates that there are multiple requesters that choose current $\mathrm{provider}_j$ as their best match. The provider will increase its price by ϵ. Case 3 (lines 23–28) indicates that there is ONE requester that chooses current $\mathrm{provider}_j$ as their best match, i.e., $|\Re_j^k| = 1$. In this algorithm, it is different from the one-to-one matching, providers will not leave the matching system until $|\Psi^k(\theta_j^k)| = q_j^k$.

The main differences between Algorithm 1 and the algorithm proposed in [19] are as follows.

1) We created collections for both the requester $\mathrm{MATLIST}_c$ and the provider SLIST_s. Once a node pair is matched, the two nodes will move out of the collection.
2) When multiple requesters compete for a node at the same time, the competing node will select the requester with

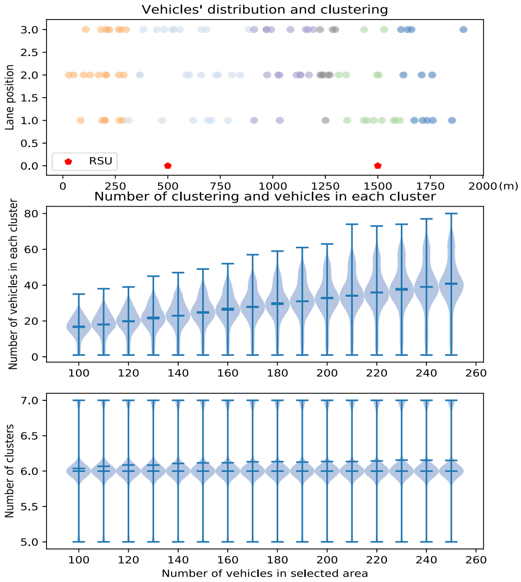


Fig. 7. Cluster changes with different vehicle densities.

the higher reputation value to match, instead of randomly selecting

3) The end condition of the algorithm is simpler than the previous version: as long as one of the two sets is empty, the match is completed.

VI. Rationality Analysis

A. Vehicle Group Division

We deploy our simulation on a three-line scenario, assuming that the initial position of the vehicles on the lane $i (i = 1, 2, 3)$ follows a uniform distribution with average node density λ_i. Then, the number of vehicles located in an interval of length l on the lane i follows the Poisson distribution. To evaluate the number of vehicles in each group, we conduct a statistical experiment on a specific road segment with a length of 2 km. Fig. 7 shows the cluster changes with different vehicle densities. These vehicles are divided into 5–7 consortia, and the number of vehicles in each cluster increase with the increase in density. To make the clustering structure more intuitive, we drew a schematic diagram of the vehicle distribution and clustering result. From the violin diagram, it can be seen that the variances of the number of clusters and the number of users in each group was small, and the clustering result of the system was relatively stable.

B. Matching Stability and Complexity

In a matching game, there are two kinds of obstruction that may impact the stability of the system: `individual block` and `pair block` [21]. A matching Ψ^k is *block by an individual* if

$$\begin{aligned} &\exists\, i, j, \quad \mathcal{U}^{\text{PRO}}_{\theta^k_j}(\xi^k_i, \gamma_k, p^k_{ij}) < 0, \Psi^k(\theta^k_j) = (\xi^k_i, p^k_{ij}) \\ \text{or } &\exists\, i, j, \quad \mathcal{U}^{\text{REQ}}_{\xi^k_i}(\theta^k_j, \gamma_k, p^k_{ij}) < 0, \Psi^k(\xi^k_i) = (\theta^k_j, p^k_{ij}) \end{aligned} \tag{13}$$

which indicates that a match is completed with $\mathcal{U}^{\text{PRO}} < 0$ or $\mathcal{U}^{\text{REQ}} < 0$. But, in fact, a node has a disposition to remain single if $\mathcal{U} < 0$. A matching Ψ^k is *block by pair* if

$$\begin{aligned} &\exists\, i, j^1, p^1_{ij}\ \mathcal{U}^{\text{REQ}}_{\xi^k_i}(\theta^k_{j^1}, \gamma_k, p^k_{ij}) > \mathcal{U}^{\text{REQ}}_{\xi^k_i}(\theta^k_j, \gamma_k, p^k_{ij}) \\ &\quad \text{and } \ \mathcal{U}^{\text{PRO}}_{\theta^k_{j^1}}(\xi^k_i, \gamma_k, p^k_{ij}) > \mathcal{U}^{\text{PRO}}_{\theta^k_{j^1}}(\xi^k_{i^*}, \gamma_k, p^k_{ij}) \\ &\qquad \text{where} \quad \Psi^k(\xi^k_i) = (\theta^k_j, p^k_{ij}) \text{ and } j^1 \neq j \\ &\qquad \Psi^k(\theta^k_{j^1}) = (\xi^k_{i^*}, p^k_{ij}) \text{ and } i^* \neq i \end{aligned} \tag{14}$$

which indicates that both parties that complete the matching tend to leave their current partner and match with other nodes. A matching theory tutorial [19] defined that a matching Ψ is defined as stable if it is not blocked by any individual or any pair. Based on this definition, our system converges to stable matching. First, all nodes are self-centered. A transaction can only be completed if the utilities of both sides are positive.

1) Each *buyer* will only match with a *seller* in its demand set, and the demand set is calculated by (12), with restrictive condition $\mathcal{U}^{\text{REQ}}_{\xi^k_i}(\theta^k_j, \gamma_k, p^{k,t}_{i,j}) \geqslant 0$, which ensures that the matching utility is not negative.
2) Each *seller* does not trade at a loss, and $p^{k,t}_{\min j}$ is defined as $p^{k,t}_{\min j} = \nu \mathcal{P}^j_t$ in line 3, by which $\min_p \mathcal{U}^{\text{PRO}}_{\theta^k_j}(\xi^k_i, \gamma_k, p^k_{ij}) = 0$, and their utility increases with the subsequent price increases, i.e., $\inf \mathcal{U}^{\text{PRO}}_{\theta^k_j}(\xi^k_i, \gamma_k, p^k_{ij}) = 0$.

In [18], the theorem *a matching is group stable if it is stable* is proved. Similar, in our model, assume that there exists ξ^k_i and θ^k_j such that

$$\begin{aligned} &\exists p^1_{ij}\ \mathcal{U}^{\text{REQ}}_{\xi^k_i}(\theta^k_j, \gamma_k, p^k_{ij}) > \mathcal{U}^{\text{REQ}}_{\xi^k_i}(\Psi^k(\xi^k_i)_1, \gamma_k) \\ &\text{and } \ \mathcal{U}^{\text{PRO}}_{\theta^k_j}(\xi^k_i, \gamma_k, p^k_{ij}) > \mathcal{U}^{\text{PRO}}_{\theta^k_j}(\Psi^k(\theta^k_j)_1, \gamma_k) \end{aligned} \tag{15}$$

where $\Psi^k(\xi^k_i) = (\theta^k_{j^*}, p^k_{ij}), \Psi^k(\theta^k_j) = (\xi^k_{i^*}, p^k_{ij})$, and $p^1_{ij} \neq p_{ij}$. Here, we have to prove that such p^1_{ij} does not exist. Note that $\mathcal{U}^{\text{PRO}}_{\xi^k_i}$ is a monotone increasing function about p_{ij}, to satisfy condition $\mathcal{U}^{\text{REQ}}_{\xi^k_i}(\theta^k_j, \gamma_k) > \mathcal{U}^{\text{REQ}}_{\xi^k_i}(\Psi^k(\xi^k_i)_1, \gamma_k)$, $p^1_{ij} > p_{ij}$. However, $\mathcal{U}^{\text{REQ}}_{\theta^k_j}$ is a monotone subtraction function about p_{ij}, to satisfy condition $\mathcal{U}^{\text{PRO}}_{\theta^k_j}(\xi^k_i, \gamma_k) > \mathcal{U}^{\text{PRO}}_{\theta^k_j}(\Psi^k(\theta^k_j)_1, \gamma_k)$, $p^1_{ij} < p_{ij}$. Evidently, there is a contradiction between $p^1_{ij} < p_{ij}$ and $p^1_{ij} > p_{ij}$.

Note that ξ_i will bid for θ_j only when $\mathcal{U}^{\text{REQ}}_{\xi^k_i}(\theta^k_j, \gamma_k, p^{k,t}_{i,j}) \geqslant 0$. Conversely, if $\forall j, \mathcal{U}^{\text{REQ}}_{\xi^k_i}(\theta^k_j, \gamma_k, p^{k,t}_{i,j}) < 0$, the demand set of i would be empty, here

$$\begin{aligned} &\forall j, \quad \mu \mathcal{Q}_{\xi^k_i}(\theta^k_j, \gamma_k) - p^k_{ij} S_{\gamma_k} - \upsilon \mathcal{P}^i_r S_{\gamma_k} < 0 \\ &\qquad p^k_{ij} < \mu \mathcal{Q}_{\xi^k_i}(\theta^k_j, \gamma_k)/S_{\gamma_k} - \upsilon \mathcal{P}^i_r S_{\gamma_k}. \end{aligned} \tag{16}$$

Then, we can calculate its upper and lower bound as $\sup p = \max_{i,j} \mu \mathcal{Q}_{\xi^k_i}(\theta^k_j, \gamma_k)/S_{\gamma_k} - \upsilon \mathcal{P}^i_r S_{\gamma_k}$, $\inf p = \nu \mathcal{P}^j_t$. Thus, the maximum iteration times that makes all the providers matched

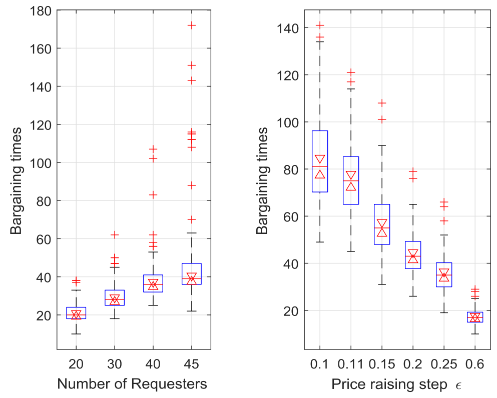


Fig. 8. Bargaining times changes.

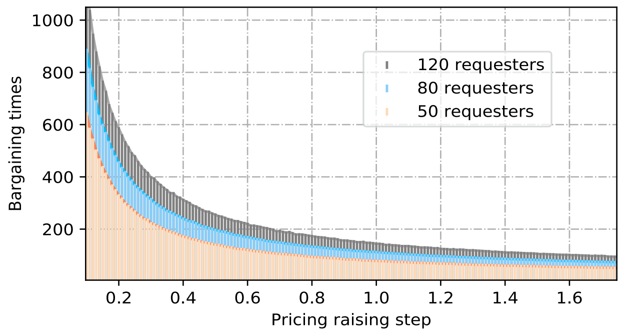


Fig. 9. Impact of ϵ on bargaining times changes.

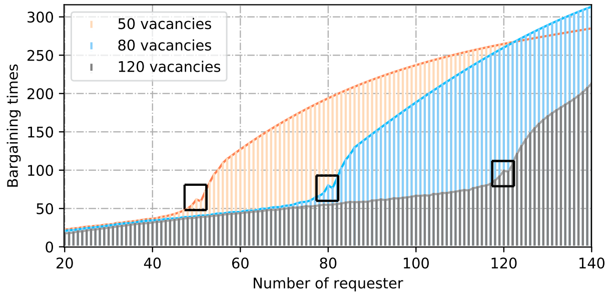


Fig. 10. Impact of requesters on bargaining times changes.

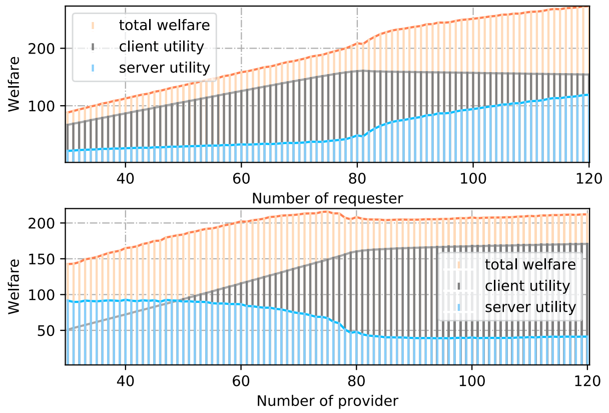


Fig. 11. Social welfare changes.

or prefer to remain single is

$$t_{\max} = 1/\epsilon(\mu \max_{i,j} \mathscr{Q}_{\xi_i^k}(\theta_j^k, \gamma_k)/S_{\gamma_k} - \upsilon \mathcal{P}_r^i S_{\gamma_k} - \nu \mathcal{P}_t^j). \tag{17}$$

Fig. 8(a) and (b) shows the bargaining time changes with different number of clients and price raising step ϵ. In Fig. 8(a), we set $\epsilon = 0.5$, and then, conducted a statistical experiment with the number of providers ranging from 30 to 150. As the number of requesters increased, the bargaining time increased as well due to more clients competing for resources. The increase in the number of requesters will raise the probability that multiple clients bid for one server (case 2), i.e., $p(\sum_i b_{i,j} > 1)$, where $\xi_i \in \mathrm{SLIST}_s, \theta_j \in \mathrm{MATLIST}_c$. Under this circumstance, the providers that received bids for multiple requesters will increase their price, which leads to higher bargain times. And then, this server will increase its unit price $b_{i,j}^{k,t}$ of data k toward requesters by ϵ. A too small price raising step ϵ will increase the bargaining times. Only after several iterations, can the provider choose the best matcher. From the figure, we can see that a larger ϵ leads to smaller variation in iteration times.

For a more comprehensive analysis, we simulate the effect of the price step and the number of requesters on the iteration times in Figs. 9 and 10. As shown in Fig. 9, when the ϵ is small, a small increase in the price raising step will greatly reduce the number of competitors. However, as the step size increases, the probability that the requesters' utility function less than 0 $[\mathcal{U}_{\xi_i}^{\mathrm{REQ}}(\theta_j, \gamma_k, p_{i,j}^k) < 0]$ will increase, thus reducing the number of iterations. When the step ϵ is large enough, the increase of ϵ will have less impact on the requester's bids. As a result, the magnitude of the reduction is smaller. For different number of clients, as stated previously, the iteration times will increase with the client increase because more clients may compete for ONE server. When the number of requesters is much smaller than the provider, the iteration times approximates linear growth. When the number of both parties is relatively close, the growth rate of bargaining times is obviously faster. As the number of requesters increases, the growth rate of iteration times will gradually slow down. The fewer the vacancies, the slower the growth rate. It is worth noting that when the number of requesters is just one more than the providers, as shown in Fig. 10, the bargaining times will be slightly smaller.

C. Social Welfare

Fig. 11 shows the social welfare changes versus the number of requesters/providers. We first evaluate the utility curve with the number of requesters (the number of providers is set to 80). When the number of requesters is less than the number of providers, both the client's and server's utility increase with the number of requesters. Since the requester chooses to match the node with the highest client's utility, it grows faster than the requester's utility. When the number of requesters is greater that of providers, the utility of the requester will drop slightly. (The reason for this phenomenon will be described later.)

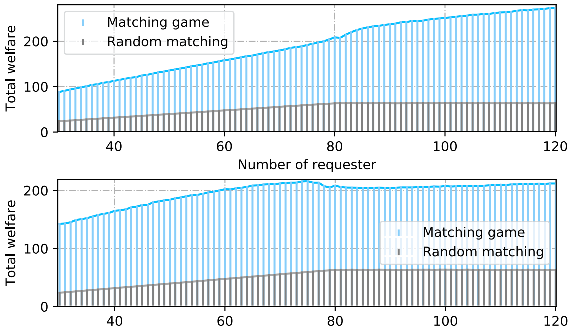


Fig. 12. Total welfare of different match scheme.

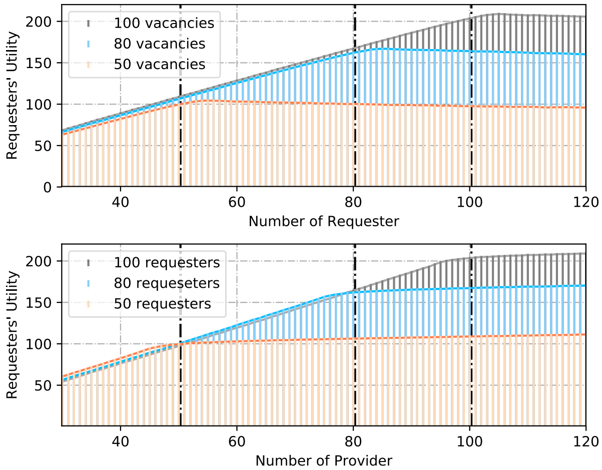


Fig. 13. Requesters' utility changes.

For the server, the utility will increase with the requester, because when the number of requesters increases, there may be more clients competing for the same provider, which results in the price increment and leads to the server's welfare growth.

To highlight the superiority of the matching method, we compared our matching method with random matching. Fig. 12 depicts the comparison of total social welfare with different number of participants. At the beginning, the total utility was proportionate to the number of requesters/providers. But when the ratio of the supply and demand reached 1, the total utility remained unchanged.

Fig. 13 illustrates the requesters' utility versus the number of requesters/providers. We simulated the case of several different vacancies. *Vacancy* indicates the maximum number of clients that can be matched. 50 vacancies indicated that there were 50 suppliers, and the maximum number of positions the supplier may provide is 1 or 25 suppliers with two positions, i.e., $\sum_j q_j^k = 50$. Note that not all nodes had the same quota. It is observed that the requesters' utility was proportionate to the quantity of requesters. As the number of requesters increased, the total utility increased as more requesters were matched to providers with positive utilities. However, but when the quantity of clients was greater than that of vacancies, the utility of all requesters decreased slowly, which is attributed to the fact that multiple demanders requested for a small number of resources, i.e., supply fell short of the demand. In each iteration, several clients may compete to match with one provider, and in such a situation, suppliers will increase their transaction price. In other words, competition between requesters reduces overall utility. It also clearly indicates that the changes in the utility is related to the providers' vacancies available. Similarly, there was a positive correlation between total requesters' welfare and the number of providers. But once the number of providers reached 50 (/80/100), the growth rate of welfare slowed down slightly. At the stage where the number of providers was greater than that of the requesters, the requesters had more choices, they can match the nodes that benefit themselves even more.

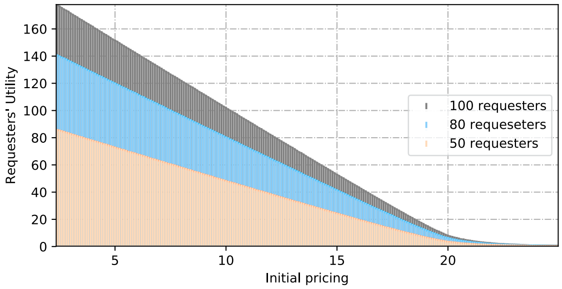


Fig. 14. Impact of initial pricing on system performance.

In addition, we also evaluated the requesters' utility versus the initial pricing. As shown in Fig. 14, with initial price increase, the users utility decreased because they had to pay more. If the utility of a node was negative, the node preferred to be unmatched, which brought about an unsatisfied client. The requesters' utility first decreased near linearly with increasing initial price, and the amplitude of utility decrement decreased with the boosting price. The reasons behind such phenomena are lower individual returns and lower matching rate. When the unit price is high enough, a significant amount of *buyers* would prefer to remain *single*. This induces the total utility to drop to almost zero. It is remarkable that our simulation was set in a one-to-one situation (there were as many vacancies as there were requesters).

D. Matching Rate

The matching rate is a significant performance index of any matching system. It is directly proportional to the total number of matched information holders that can raise their benefits by offering information. Before each transaction is completed, *sellers* will price the messages that they are going to share. Fig. 15 illustrates the relation between initial pricing and the number of unsatisfied users for various requester quantities. The system performed with nearly 100% matching rate when the initial price was less than 14 vehicle coins per unit. Intuitively, as the initial price grows, the number of unsatisfied users increase. From Fig. 15, we can observe that when the initial price was higher, the curve will show significant fluctuations. At each inflection point, there were more vehicles just at the critical point of matching. If the initial price was less than the point, more requesters preferred to match with a server; otherwise, they remained single. The position of the wave inflection point was also related to the definition of the utility function. If the

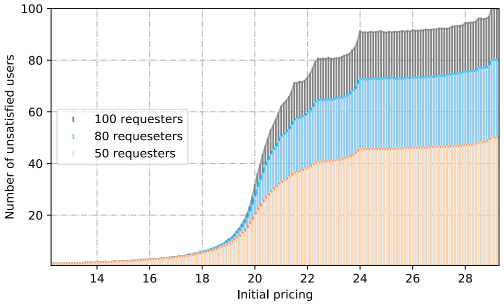


Fig. 15. Impact of initial pricing on matching rate.

proportion of the price, i.e., υ, is reduced, the entire curve will stretch to the right.

E. System Security Analysis

The blockchain-based content trading system can defend against many traditional security attacks.

1) Hypocritical Message Release: We embed an RES in information trading, i.e., publishing false messages can damage the reputation of the node. The client node will not request content from a node with a low reputation value, thereby, suppressing the revenue of the malicious node.

2) Single Point of Failure: The OBUs can trade data in a P2P manner without a third party, and the system will not be damaged by one node failure.

3) Privacy Leakage: Since all accounts are pseudonymous by multiple wallet addresses, the account security can be ensured. At the same time, during trading, the participants only submit their bid prices to the auctioneer without private information, which protects identity privacy.

4) False Transaction: All transaction records are publicly audited and authenticated. Only the node-approved transaction records can be packed into a block, and then, stored in the blockchain.

F. Application Scenario

In IoV, there are two main applications of content sharing: safety-related and nonsafety-related information. The demands for information transmission in each scenario are different. On one hand, the drivers can share safety-related information, such as traffic accident and sudden braking. Here, the client is more concerned with the reliability of the information than the delay in transmission. In this case, the requester can increase the weight of reputation. On the other hand, when passengers require for nonsafety-related information, such as video about live broadcast or music, the client may pay less attention to the information reliability. The users can adjust the relative weight of reputation and delay for different demands. Our secure content-sharing scheme is more suitable for highway scenes, where the relative position of vehicles is relatively fixed. In the case of a rapid change in vehicle topology, the members of the underlying blockchain would change dramatically, which makes the accounting more complicated.

For example, the vehicles on the highway may request for traffic conditions on different road sections. However, some nodes may want traffic situation of road section A, but it only has that of road section B. This node will send an Interest that contains its desire to meet the needs. This Interest will be spread within the group. If the request is not satisfied, the data that it holds, along with its requests, will be sent to the header. After that, the RSU will collect the requests and data content, and then, does matching for both sides. Then, the requester will request for information about traffic situation of road section A to the matcher and pay for the content. Finally, the data sharing is completed.

VII. Conclusion

In this article, we tackled the VNDN data sharing problem, which broadly addresses the reputation management, information security, and the data supply and demand matching. We built a double-layer blockchain trading system for the VNDN local area information transmission. To achieve a wider range of data sharing, RSUs act as data aggregators for supply and demand collection. After that, a one-to-many matching game model was built. To prevent malicious nodes from spreading fake messages, we designed a reasonable RES that was embedded in the matching model. In our future work, besides taking the client demand and server supply into account, we will extend our one-to-many assignment game to matching with externalities, and further, explore the data sharing issue to facilitate the content retrieval with a combined matching problem.

References

[1] L. Yao, A. Chen, J. Deng, J. Wang, and G. Wu, “A cooperative caching scheme based on mobility prediction in vehicular content centric networks,” *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 5435–5444, Jun. 2018.

[2] C. Chen, J. Hu, T. Qiu, M. Atiquzzaman, and Z. Ren, “CVCG: Cooperative V2V-aided transmission scheme based on coalitional game for popular content distribution in vehicular ad-hoc networks,” *IEEE Trans. Mobile Comput.*, vol. 18, no. 12, pp. 2811–2828, Dec. 2019.

[3] T. Qiu, X. Wang, C. Chen, M. Atiquzzaman, and L. Liu, “TMED: A spider web-like transmission mechanism for emergency data in vehicular ad hoc networks,” *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8682–8694, Sep. 2018.

[4] Z. Yan, S. Zeadally, and Y. Park, “A novel vehicular information network architecture based on named data networking (NDN),” *IEEE Internet Things J.*, vol. 1, no. 6, pp. 525–532, Dec. 2014.

[5] S. H. Ahmed, S. H. Bouk, M. A. Yaqub, D. Kim, H. Song, and J. Lloret, “CODIE: Controlled data and interest evaluation in vehicular named data networks,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 6, pp. 3954–3963, Jun. 2016.

[6] Y. Hui, Q. Zheng, O. Lu, and K. Li, “A query privacy-enhanced and secure search scheme over encrypted data in cloud computing,” *J. Comput. Syst. Sci.*, vol. 90, no. 1, pp. 14–27, 2017.

[7] S. Meng, L. Qi, Q. Li, W. Lin, X. Xu, and S. Wan, “Privacy-preserving and sparsity-aware location-based prediction method for collaborative recommender systems,” *Future Gener. Comput. Syst.*, vol. 96, no. 1, pp. 324–335, 2019.

[8] H. Dai, Z. Zheng, and Y. Zhang, “Blockchain for Internet of Things: A survey,” *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.

[9] J. Huang, L. Kong, G. Chen, M. Wu, X. Liu, and P. Zeng, “Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism,” *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3680–3689, Jun. 2019.

[10] T. Jiang, H. Fang, and H. Wang, “Blockchain-based internet of vehicles: Distributed network architecture and performance analysis,” *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4640–4649, Jun. 2019, doi: 10.1109/JIOT.2018.2874398.

[11] X. Zhang and X. Chen, "Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network," *IEEE Access*, vol. 7, no. 1, pp. 58241–58254, 2019.

[12] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3548–3558, Jun. 2019.

[13] P. Basu, N. Khan, and T. D. C. Little, "A mobility based metric for clustering in mobile ad hoc networks," in *Proc. 21st Int. Conf. Distrib. Comput. Syst. Workshops*, Mesa, AZ, USA, 2001, pp. 413–418.

[14] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of Bitcoin," *IEEE Commun. Surv. Tuts.*, vol. 20, no. 4, pp. 3416–3452, 4Q 2018.

[15] J. Kang *et al.*, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019.

[16] Q. Yang and H. Wang, "Toward trustworthy vehicular social networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 42–47, Aug. 2015.

[17] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.

[18] S. Bayat, R. H. Y. Louie, Z. Han, B. Vucetic, and Y. Li, "Distributed user association and femtocell allocation in heterogeneous wireless networks," *IEEE Trans. Commun.*, vol. 62, no. 8, pp. 3027–3043, Aug. 2014.

[19] S. Bayat, Y. Li, L. Song, and Z. Han, "Matching theory: Applications in wireless communications," *IEEE Signal Process. Mag.*, vol. 33, no. 6, pp. 103–122, Nov. 2016.

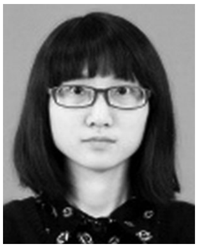
[20] S. Von and H. David, *CRC Standard Curves and Surfaces With Mathematica*. Boca Raton, FL, USA: CRC Press, 2006.

[21] D. Gusfield and R. W. Irving, *The Stable Marriage Problem: Structure and Algorithms*. Cambridge, MA, USA: MIT Press, 1989.

Chen Chen (M'09–SM'18) received the B.Eng., M.Sc., and Ph.D. degrees in electrical engineering and computer science (EECS) from Xidian University, Xi'an, China, in 2000, 2006, and 2008, respectively.

He is currently an Associate Professor with the Department of Telecommunication, Xidian University. He is also the Director with the Xi'an Key Laboratory of Mobile Edge Computing and Security, and the Director with the Intelligent Transportation Research Laboratory, Xidian University. He was a Visiting Professor with the Department of EECS, University of Tennessee, and of Computer Science with the University of California. He has authored/coauthored two books, more than 80 scientific papers in international journals and conference proceedings. He has contributed to the development of five copyrighted software systems and invented 50 patents.

Dr. Chen is a Senior Member of the China Computer Federation and a Member of the ACM and Chinese Institute of Electronics. He serves as the General Chair, Program Committee Chair, Workshop Chair, or Technical Program Committee Member for a number of conferences.



Cong Wang received the B.Eng. degree in electronic and information engineering from Chongqing Jiaotong University, Chongqing, China, in 2016. Since 2016, she has been working toward the master's degree with Xidian University, Xi'an, China.

Her research interests include wireless communication, computer engineering, traffic information, and control engineering.

Tie Qiu (M'12–SM'16) received the Ph.D. degree in computer science from the Dalian University of Technology, Dalian, China, in 2012.

He is currently a Full Professor with the School of Computer Science and Technology, Tianjin University, Tianjin, China. Prior to this position, he was an Assistant Professor in 2008 and an Associate Professor in 2013 with the School of Software, Dalian University of Technology. He was a Visiting Professor with the Electrical and Computer Engineering Department, Iowa State University, Ames, IA, USA (2014–2015). He has authored/coauthored nine books, more than 150 scientific papers in international journals and conference proceedings, such as IEEE/ACM TRANSACTIONS ON NETWORKING, IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, IEEE COMMUNICATIONS MAGAZINE, etc. There are 12 papers listed as ESI highly cited papers. He has contributed to the development of three copyrighted software systems and invented 14 patents.

Dr. Qiu serves as an Associate Editor for the IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, an Area Editor for the *Ad Hoc Networks* (Elsevier), an Associate Editor for the IEEE ACCESS JOURNAL and *Computers and Electrical Engineering* (Elsevier), and a Guest Editor for *Future Generation Computer Systems*. He serves as a General Chair, Program Chair, Workshop Chair, Publicity Chair, Publication Chair, or Technical Program Committee Member for a number of international conferences. He is a Senior Member of the China Computer Federation and a Senior Member of the Association for Computer Machinery.

Ning Lv received the B.Eng. degree in electrical engineering and automation from Xi'an Jiaotong University, Xi'an, China, in 2000, and the M.Sc. degree in circuit and system engineering in 2004 from Xidian University, Xi'an, where he is currently working toward the doctoral degree in pattern recognition and intelligent system.

Qingqi Pei (SM'15) received the B.S., M.S., and Ph.D. degrees in computer science and cryptography from Xidian University, Xi'an, China, in 1998, 2005, and 2008, respectively.

He is currently a Professor and a Member with the State Key Laboratory of Integrated Services Networks. His research interests include cognitive network, data security, and physical layer security.

Dr. Pei is also a Professional Member of the Association for Computing Machinery and a Senior Member of the Chinese Institute of Electronics and the China Computer Federation.