Challenges and Solutions in Autonomous Driving: A Blockchain Approach

Yuntao Wang, Zhou Su, Kuan Zhang, and Abderrahim Benslimane

Abstract

The autonomous driving era is coming with tremendous potential to revolutionize transportation systems with improved safety, comfort, and intelligence on the road. Integrating connected autonomous vehicles (CAVs) and rising social networking, autonomous vehicular social networks (AVSNs) can facilitate the data dissemination in safety-critical and entertainment-related applications for autonomous driving. However, with time-varying, delay-constrained, and location-dependent characteristics in autonomous driving, it faces great challenges to incentivize CAVs to disseminate massive content in AVSNs. Meanwhile, attackers may not only disseminate fake information to confuse the network, but also pose security vulnerabilities and privacy issues for CAVs. In this article, we investigate secure and incentive content delivery in AVSNs based on the advanced blockchain. Specifically, we first present a blockchain-enabled AVSN framework to safeguard content delivery. Then, we investigate the task-based and credit-based reputation models to evaluate the trustworthiness of CAVs and RSUs, respectively. The reputation increase and task reward are explored as incentives for CAVs delivering reliable content. In addition, a novel proof of reputation consensus protocol is devised to efficiently reach consensus in blockchain-enabled AVSNs while motivating RSUs to behave honestly. Experimental results indicate that the proposed framework outperforms the existing approaches, delivering vehicular content more reliably and securely. Finally, future research directions in this emerging area are discussed.

Introduction

Intelligent transportation systems (ITSs) have been evolving rapidly over the last few decades with the rising global urbanization and industrialization. By liberating human beings from daily driving activities, autonomous vehicles have emerged as the critical component of ITSs to eliminate vehicle crashes, reduce fuel consumption, and alleviate traffic congestion [1]. Global automakers, such as Tesla, Volvo, Toyota, and Audi, have already developed prototypes of autonomous vehicles and are expected to be rolled out in 2020. Moreover, governments, including the United States, China, Germany, and France, have strongly actuated autonomous driving via policy support respecting road testing, standards, and regulations. In the research field, a number of recent works have been released to facilitate autonomous driving. The authors in [2] proposed the vehicle-to-everything (V2X)-based collaborative collision avoidance scheme for autonomous driving in overtaking scenarios. The authors in [3] developed multi-target future state prediction strategies for autonomous vehicles in real driving environments. It is predicted that the percentage of autonomous vehicles on the road will reach 75 percent by 2040, with an estimated marketing value of $7 trillion by 2050 [4].

Autonomous vehicles rely heavily on a variety of advanced sensors to precisely perceive surroundings. Due to the intrinsic limitations of on-board sensors and computing capacity, autonomous vehicles need to connect to autonomous vehicular networks (AVNs) to receive the sensed data and driving statuses from neighbors for secure autonomous driving [2]. Meanwhile, passengers on board have a strong willingness to share travel experiences, regional news, videos, and so on, with each other through social networks to make their trips more enjoyable. Compared with AVNs, autonomous vehicular social networks (AVSNs) [5], which integrate social characteristics into AVNs, can exploit the social properties among connected autonomous vehicles (CAVs) to facilitate a myriad of safety-critical and infotainment-related on-road content services. For instance, a group of proximal CAVs can form social communities based on their social features and common interests to share and exchange interested information via vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-cloud (V2C) links. By cooperatively requesting and delivering content within social communities, redundant transmissions for the same contents can be significantly mitigated, as well as the content search and dissemination for CAVs can be facilitated.

In spite of the fundamental contributions of existing works on hardware and algorithm design [2, 4], the security issues on data sharing which play a critical role in autonomous driving are rarely studied. On one hand, compared with human drivers, CAVs are more vulnerable to be compromised by attacks (e.g., GPS jamming attack, camera blinding attack) [6] and disseminate massive fake or harmful content to threaten the normal operations of nearby CAVs. Legitimate CAVs with malfunctioning sensors can also deliver incorrect information. On the other hand, to mitigate the heavy burden of communication and data processing for CAVs, roadside units (RSUs) are

Digital Object Identifier:
10.1109/MNET.001.1900504

Yuntao Wang is with Xi'an Jiaotong University; Zhou Su (corresponding author) is with Xi'an Jiaotong University and Shanghai University; Kuan Zhang is with the University of Nebraska-Lincoln; Abderrahim Benslimane is with the University of Avignon.

0890-8044/20/$25.00 © 2020 IEEE

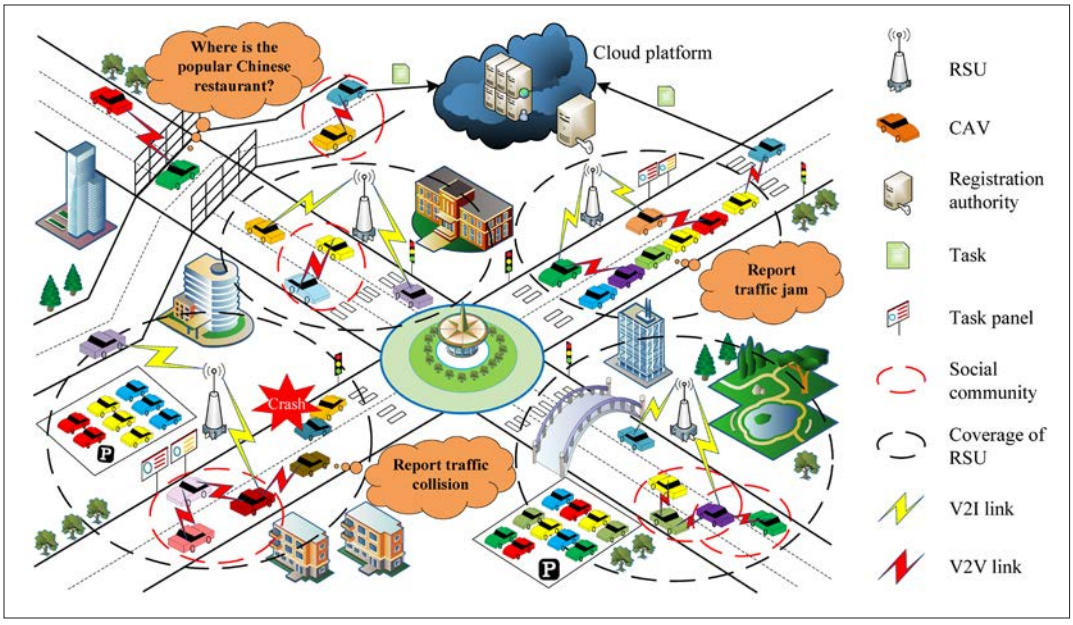

FIGURE 1. Overview of the autonomous vehicular social network and its applications.

deployed in AVSNs by executing content services at the edge of the network [1]. Since RSUs are deployed by third parties (e.g., the supermarket or parking lot) and are open accessed, they may not only provide fraudulent content services to cheat CAV users, but are vulnerable to diverse attacks such as distributed denial of service (DDoS) attacks perpetrated by malicious entities. To summarize, the challenges of secure and efficient content sharing in AVSNs are listed as follows.

Trustworthiness of CAVs and RSUs: CAVs might not be capable of distinguishing reliable content from massive fake ones to make appropriate decisions. The trustworthiness of CAVs and RSUs in content transmission should be assessed.

Incentive for CAVs: CAV users usually lack enthusiasm to share content if without sufficient compensation. Due to the self-driving features of CAVs and a tremendous volume of vehicular contents, traditional incentive methods in vehicular networks are either incompatible or inefficient for AVSNs.

Security of Content Delivery: In AVSNs, adversaries may not only tamper with and forge content, but also conduct diverse attacks to threaten CAVs' security and privacy. The risk of attacks on legitimate CAVs may reduce the effect of incentives in content delivery.

In this article, we exploit the promising blockchain technique to assist secure and incentive content sharing in AVSNs. Specifically, we first present the framework of blockchain-enabled AVSNs in content transmission. Based on the immutable ledgers, cryptocurrency, and asymmetric encryption in the blockchain, the security of content transactions and reputation values can be guaranteed, as well as CAVs' identity privacy. Then, based on the social features and user behaviors, two reputation assessment models are established for both CAVs and RSUs to motivate their legitimate behaviors and improve content reliability. In addition, with the implementation of Boneh-Lynn-Shacham (BLS) multi-signature [7], we devise a proof of reputation (PoR) consensus protocol to efficiently deploy the blockchain network into AVSNs consisting of RSUs and resource-limited CAVs. Simulation experiments are carried out to evaluate the proposed framework. Finally, we point out several open research directions and the outlook of AVSNs from efficiency, incentive, and security perspectives.

The remainder of this article is organized as follows. The background of AVSNs and blockchain is introduced in the next section. Several challenges for content delivery in AVSNs are then summarized. Following that, a framework for blockchain-enabled AVSNs is developed. Then, we draw important directions for future studies and close our work with conclusions.

Blockchain and Autonomous Vehicular Social Networks

Autonomous Vehicular Social Networks

As the scale of AVNs increases rapidly, massive content generated by CAVs leads to heavy network overhead. AVSNs can facilitate content delivery for a variety of on-road services and applications by incorporating social factors into AVNs [5]. In general, CAV users in proximity with shared interests can be interested in similar information. For instance, CAV users with the same destination may intend to share similar traffic situations. When they travel in an urban district, they may tend to obtain the same local information, for example, weather conditions and popular restaurants. As shown in Fig. 1, by exploiting social relationships among CAV users such as establishing social communities, CAVs can cooperatively request, deliver, and exchange content to mitigate network congestion arising from the redundant transmissions for the same contents. In addition, through interest matching and friend discovery, the process of searching and disseminating content can be accelerated in AVSNs.

Compared with mobile social networks (MSNs) [8], since CAVs move at high speed

To strengthen the reliability of content delivery in AVSNs, social reputation is essential to determine the trustworthiness of content sender and service provider. In this way, CAV users can evaluate the social reputation of others and only receive content from nodes with high trustworthiness.

around a city, the communication duration and contact frequency in AVSNs are quite short. With high mobility, network topologies in AVSNs are highly dynamic, and social relationships among CAV users are very weak. Compared with vehicular social networks (VSNs) [8], when a CAV travels on the road, a huge body of heavy computations are required to execute various driving tasks in real time. For instance, the data volume to download a 3D high-precision map with the centimeter-level is 3-4 GB/km [4]. These differences show the complexity of content dissemination in AVSNs in relation to MSNs and VSNs.

With the massive content volume and time-varying, delay-constrained, and location-dependent features for autonomous driving applications, edge computing [4] has emerged as a promising solution by exploring roadside infrastructures such as RSUs to offer high bandwidth, low latency, and improved connectivity for vehicular content services. However, the open-access and selfish features of RSUs introduce severe security vulnerabilities in content delivery for CAVs. To strengthen the reliability of content delivery in AVSNs, social reputation is essential to determine the trustworthiness of content sender and service provider [5]. In this way, CAV users can evaluate the social reputation of others and only receive content from nodes with high trustworthiness. In addition, a reputation increase can become a reward for CAVs or RSUs with good behavior in disseminating reliable contents or content services.

Blockchain in Vehicular Content Delivery

As the number of CAVs is expected to grow geometrically in the next few decades, the cost of centralized content management for massive scattered CAVs may be unaffordable [9]. In addition, the centralized network structure may suffer from data tampering attacks and privacy leakage once the central server is hacked. Fortunately, blockchain has provided a decentralized solution to tackle the above issues. Blockchain is a distributed public ledger containing a growing sequence of hash-chained blocks, which adopts consensus operation for distributed storage and can immutably record data in decentralized networks without reliance on trusted central entities [10]. Different from traditional centralized approaches, data is recorded as blocks and shared over the entire blockchain network. This special data structure provides better robustness to prevent a single point failure and is featured with traceability, non-repudiation, and non-tampering [11]. Compared with permissionless blockchain networks, only authorized nodes (e.g., vehicles and RSUs) can join in the permissioned blockchain-based vehicular networks after registration, which can protect the network against external adversaries.

Currently, various blockchain systems have been proposed and leveraged to ensure data security and prevent attacks in content sharing services. However, it occupies extremely stringent computing and storage resources for nodes to run traditional proof-of-work (PoW) algorithms to reach consensus in the blockchain network [9], where the resources of vehicles are generally insufficient. To efficiently implement the blockchain among resource-limited vehicles and stimulate the honest behavior of consensus nodes, a feasible option is exploiting social reputation as the stake of RSU nodes for consensus node election, block building, and ledger management in an energy-efficient manner [11]. In blockchain-enabled vehicular networks, content transactions among vehicles are verified and forwarded by nearby peer nodes. Then, each consensus node runs the consensus protocol to make an agreement on the transactions to be stored in blockchain. Finally, after reaching consensus, the newly generated block which contains a set of valid transactions is linearly appended to the blockchain.

Challenges of Content Delivery Over AVSNs

With the expanding number of CAVs and the increasing demands for secure and reliable on-road content services, new challenges such as reliability, incentive, and security arise in content delivery over AVSNs.

Trustworthiness of CAVs and RSUs

Malicious CAVs may deliver dishonest, meaningless, and even harmful content to interfere with others' driving activities. For example, a malicious CAV may disseminate forged traffic accidents to keep the road clear for itself. Besides, malicious RSUs may cheat CAVs by offering fake content services. Currently, reputation models are suggested as an effective approach to identify malicious nodes in vehicular networks [5]. However, owing to the large scale of AVSNs, it is unrealistic to calculate and update the trustworthiness of all CAVs and RSUs in a centralized manner. How to distributedly evaluate the trustworthiness of CAVs and RSUs in AVSNs and select trustworthy CAVs to deliver reliable content becomes an issue of significance.

Incentive for CAVs

Since it takes both computing and energy resources for resource-limited CAVs to share and exchange content, rational and selfish CAVs will not contribute their content if without enough incentives. A potential risk of privacy leakage may further discourage CAV's enthusiasm in content dissemination. Moreover, due to the high velocity of CAVs and a huge body of content in autonomous driving, traditional incentive methods in MSNs and VSNs do not work well in AVSNs [8]. How to motivate CAVs with resource constraints to collect, verify, and forward reliable content to accelerate the content dissemination in the ever-changing AVSNs is a nontrivial issue.

Security of Content Delivery

Compared with human driving mode, CAVs are controlled by self-driving programs and are more vulnerable to be attacked or hijacked by attackers via various attacks [6]. Additionally, due to the dependence on a trusted central node such as the cloud platform, potential security issues (e.g.,

single point of failure, privacy disclosure) could arise in centralized AVSNs [9]. Recently, blockchain offers a decentralized solution to eliminate reliance on central nodes and safeguard content sharing process [10]. However, due to the high mobility and resource-constrained nature of CAVs and potential risks of misbehaving consensus nodes, it is still an open and vital issue to efficiently implement a lightweight blockchain in AVSNs to secure content disseminating.

Framework of Blockchain-Enabled AVSNs

Blockchain-enabled AVSNs integrate the decentralized blockchain technology with AVSNs, which can simultaneously satisfy the requirements of reliable, secure, and incentive content disseminating in the autonomous driving context. In this section, we present a novel framework for content delivery in blockchain-enabled AVSNs, as shown in Fig. 2.

Network Architecture

RSUs: A group of RSUs $\mathcal{J}$ are strategically deployed alongside the road to provide V2I connections when CAVs pass through their coverage areas. Each RSU is managed by its operator, and the communication coverage of RSU $j \in \mathcal{J}$ is defined as a circle with radius of Z_j.

CAVs: CAVs can perform as distributed sensor hubs on the road to collect data by in-vehicle sensors or smart devices (e.g., iPad, iPhone, and so on), and publish them to other data consumers. In addition, CAVs are equipped with onboard unit (OBU) devices to support both V2V and V2I communications [2]. Each CAV $i \in \mathcal{I}$ can request the desired content by sending a task request for task $u \in \mathcal{U}$ with its desired requirements to the specific RSU. For instance, if CAV i wants to know the traffic conditions in a specific area in the coverage of RSU j to guide its trip to the destination, it can post a rewarding mission on RSU j for the desired information.

Social Communities: A social community is composed of a group of proximity CAVs with common social characteristics [5]. Let $\mathcal{S}$ denote the set of social groups in AVSNs, and l_s be the number of CAVs in social group $s \in \mathcal{S}$. CAVs within a social community can communicate with each other and cooperatively request the same contents to reduce network congestion as well as the cost for obtaining desired contents. Based on the social graph $\mathcal{G}$ of CAV users, each CAV i calculates the social scores of nearby CAVs and invites the top ϱ CAVs with highest social scores to construct social communities. Let $S_{i,i'}$ be the social score between CAV i and CAV i' , which can be computed as $S_{j,j'} = sim_{i,i'} \times mf_{i,i'}$. Here, $sim_{i,i'}$ is the social similarity [12] between two CAV users' social interest profiles, and $mf_{i,i'}$ is the number of mutual social friends between CAV i and CAV i'in $\mathcal{G}$.

Permissioned Blockchain Network: In the permissioned blockchain context, only authorized individuals can participate in the decentralized network. There are two types of nodes in the network, that is, consensus nodes and ordinary nodes. Consensus nodes can participate in the consensus process for global ledger management, while ordinary nodes only relay, exchange and accept ledgers [11]. Each block contains two parts: the block header and the block body. The block header mainly contains the hash of the previous block, the hash of the current block, and the timestamp. The block body stores all valid transactions during each consensus interval [10]. In blockchain-enabled AVSNs, RSUs perform as the full nodes which store the full ledgers (i.e., all the blocks), while CAVs act as the lightweight nodes which only store the metadata (i.e., the block header) of blocks due to the limitation of computation and storage capacities [9].

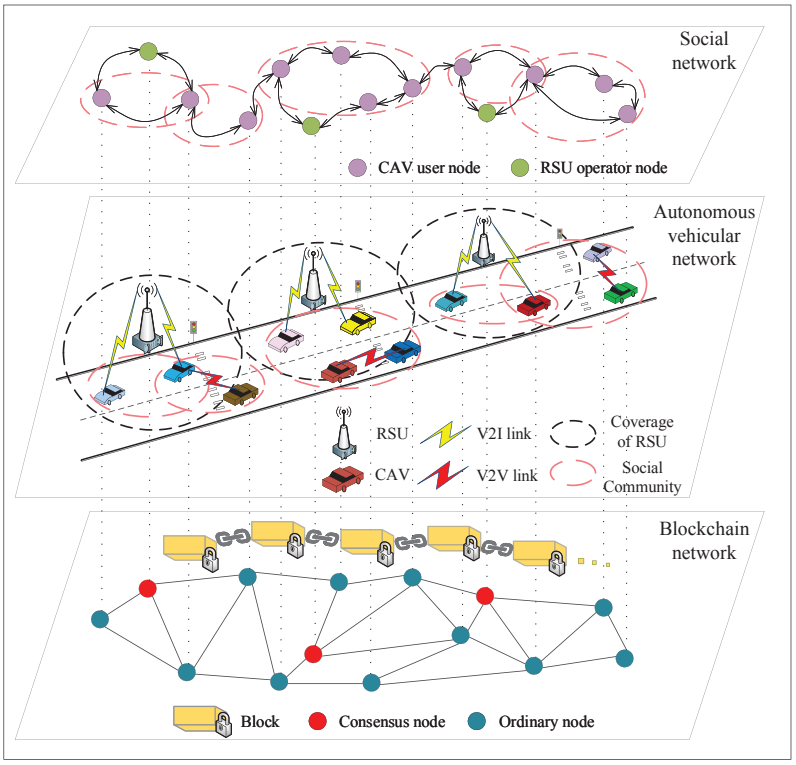

FIGURE 2. Network architecture of blockchain-enabled AVSNs.

Vehicular Content Delivery

As shown in Fig. 3, there are three kinds of CAVs in the delivery process of task data, that is, requester r in social community s, worker m in worker group $\mathcal{M}$, and witness w in witness group $\mathcal{W}$. Requesters within a social community can cooperatively publish a task for the desired content with individual requirements (i.e., the reputation threshold θ, the number of required witnesses k, and the time to live TTL). A worker can hunt the published tasks and collect the task data (i.e., content $c \in \mathcal{C}$). Witnesses are responsible for verifying the collected task data.

First, the social community s posts a rewarding mission u on a specific RSU j with the multi-signature of all its members. Each RSU maintains a task panel recording the statuses of tasks requested in its coverage. After receiving task u, RSU j checks the attached signature and adds the task into its task panel. Each task has three statuses, that is, $status_u = \{-1, 0, 1\}$, where -1 means task u can be hunted, 0 means task u is in process, while 1 means task u has been completed. CAVs in the coverage of RSU j with reputation value greater than θ can be the worker of task u by sending a request to RSU j based on the first come first serve principle. To motivate CAVs to participate

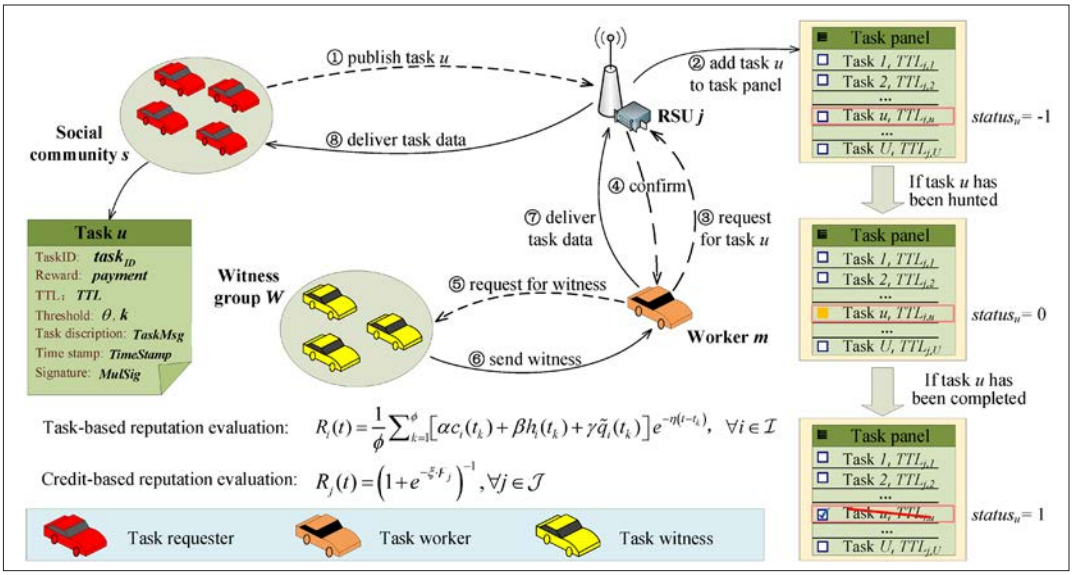

FIGURE 3. Process of content delivery in blockchain-enabled AVSNs.

in the witness process, worker m can invite nearby CAVs whose reputation value is larger than θ as witnesses by rewarding a small number of task coins. Each nearby CAV w, who agrees on the task data and sends back its signature to worker m, becomes the witness of the task. After receiving more than k agreements from k different witnesses, worker m delivers the content to RSU j attached with the multi-signature of k witnesses to earn the reward in task u. Then, RSU j checks whether the requirements in task u are satisfied, determines the quality of task completion q_u, and delivers the collected content to social community s. Finally, the content c is delivered to all the members in the social community s and the cost for obtaining the content can be divided and shared evenly among them.

Reputation Evaluation

Task-Based Reputation: The task-based reputation model is presented to evaluate the trustworthiness of CAV users for accomplishing tasks. The following dimensions are used to evaluate the reputation of CAVs: cooperativeness, honesty, and quality of task completion. The cooperativeness of CAV i, that is, $c_i(t)$, is defined as the weighted sum of the numbers of tasks worked and witnessed by CAV i during time slot t. The honesty of CAV i, that is, $h_i(t)$, is defined as the difference between the numbers of tasks worked and canceled by CAV i during time slot t. The records for working and witnessing the specific tasks are stored in the transaction data in blockchain. For each task u, $q_u \in [0, 1]$ denotes the quality of task completion quantized by RSUs, where 1 means the highest quality while 0 means the opposite. The normalized quality of task completion, that is, $\tilde{q}_i(t)$, is derived by averaging the quality of tasks completed by CAV i during time slot t. As shown in Fig. 3, based on these three dimensions, the reputation value R_i of CAV i can be obtained. Here, α, β, γ are normalization factors; ϕ is the number of time slots till current time slot t; $e^{(.)}$ is the exponential decay function indicating that the latest interactions are more important than previous ones; η is the positive time decay factor.

Credit-Based Reputation: The credit-based reputation model is presented to evaluate the trustworthiness of RSU operators in the consensus process of blockchain. As shown in Fig. 3, the reputation value R_j of RSU j lies within (0, 1), and is calculated based on its credit score F_j in blockchain. Here, ζ is the adjustment coefficient; F_j is associated with RSU j's behaviors. Honest behaviors can gradually increase the credit score, while malicious behaviors can destroy the credit score rapidly [11]. The credit score of RSU j consists of two parts, namely, the positive part F_j^P and the negative part F_j^N. Furthermore, a punishment factor is introduced to punish RSUs' misbehaviors and prevent malicious RSUs from recovering quickly even if they behave legitimately in next time slots. F_j^P is positively related to the number of times that RSU j becomes a consensus node and the corresponding occurrence time for being a consensus node. Meanwhile, RSUs can conduct various kinds of misbehaviors (e.g., invalid block generation, transaction forgery). F_j^N is negatively related to the number of misbehaviors of RSU j, the punishment value of each misbehavior type, and the corresponding occurrence time of each misbehavior. Here, the credit score of each RSU in $\mathcal{J}$ is initialized by $F_j^0 = 0$ such that $R_j(0) = 0.5$, and updated during each consensus interval based on its positive and negative behavior records traced in the immutable blockchain.

PoR Consensus Protocol

To efficiently achieve consensus in permissioned blockchain-enabled AVSNs, the PoR consensus protocol is devised and presented in Fig. 4.

Phase 1: System Initialization and Entity Registration: The registration authority (RA) serves as an authorized agent which is responsible for entity registration and key management in the network. RA selects a bilinear pairing, hash functions, and its private key for system initialization, and broadcasts the system parameters to the network.

CAVs and RSUs become authorized nodes in the blockchain network after registration with RA through binding their true identities, for example, the unique vehicle identification number (VIN) of

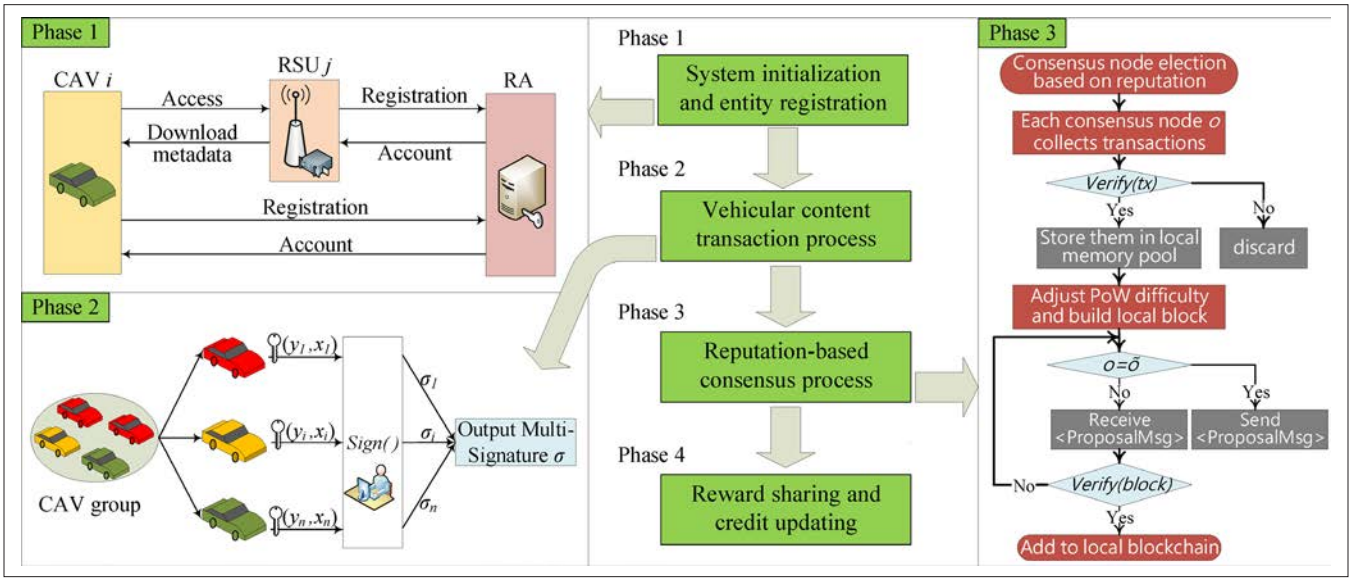

FIGURE 4. Illustration of PoR consensus protocol.

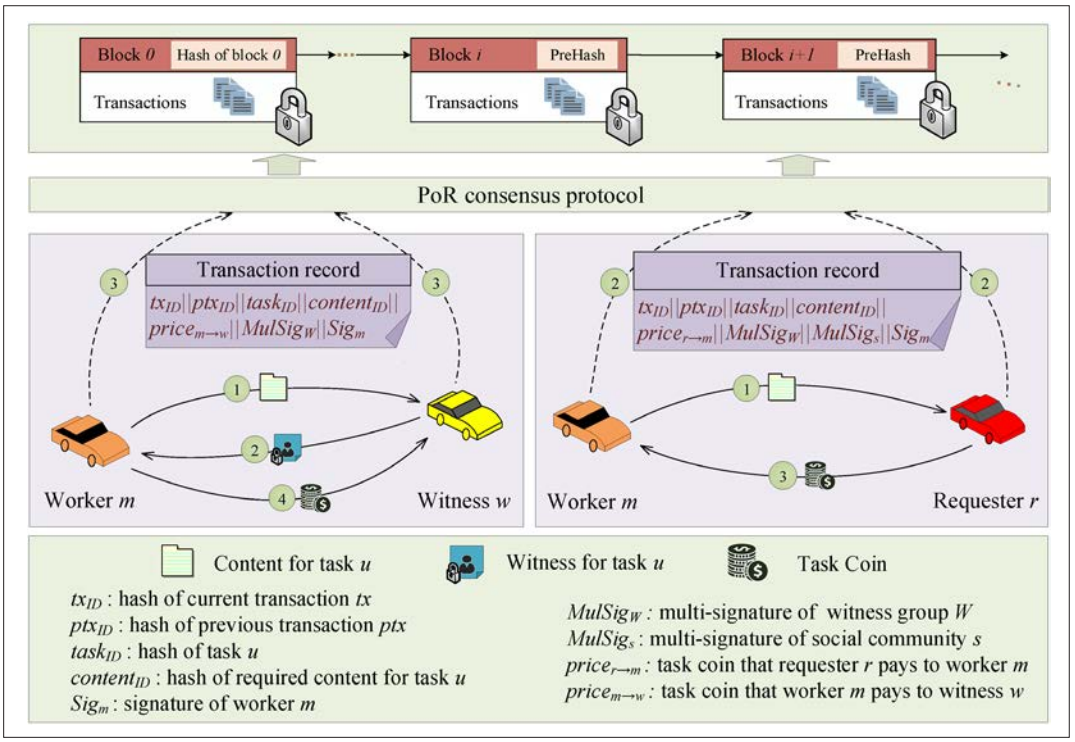

FIGURE 5. Process of content transactions in decentralized permissioned blockchain.

each CAV and the business license of each RSU. Then, each authorized node $q \in \mathcal{Q}$ gets its account including its public/private key pair $\{y_q, x_q\}$, certificate Cer_q, and wallet address w_q. Here, the private key should be secretly kept by the node itself, while the public key is publicly known in the network. The certificate is issued to uniquely identify a node, while the wallet address is used to send or receive coins in the blockchain. RA maintains a certificate repository that stores all registered entities and the corresponding identities. In the coverage of RSU j, CAVs can access to RSU j via authentication and download the blockchain data.

Phase 2: Vehicular Content Transaction Process: As shown in Fig. 5, all content transactions among workers, witnesses and requesters are forwarded to the blockchain network and verified by the consensus nodes. Note that all requesters in the social community s sign the same content request (i.e., task u), and all witnesses in the witness group $\mathcal{W}$ sign the same task data (i.e., content c). To ease the communication and storage cost of multiple signatures in blockchain, we employ the BLS multi-signature for transaction generation and verification by aggregating all the signatures in a CAV group. Compared with other digital signature schemes, BLS signatures are far shorter in the signature size [7], for example, digital signature standard (DSS) is 320 bit long while BLS signature is only 160 bit long.

The security of the BLS multi-signature scheme relies on the standard computational co-Dif-

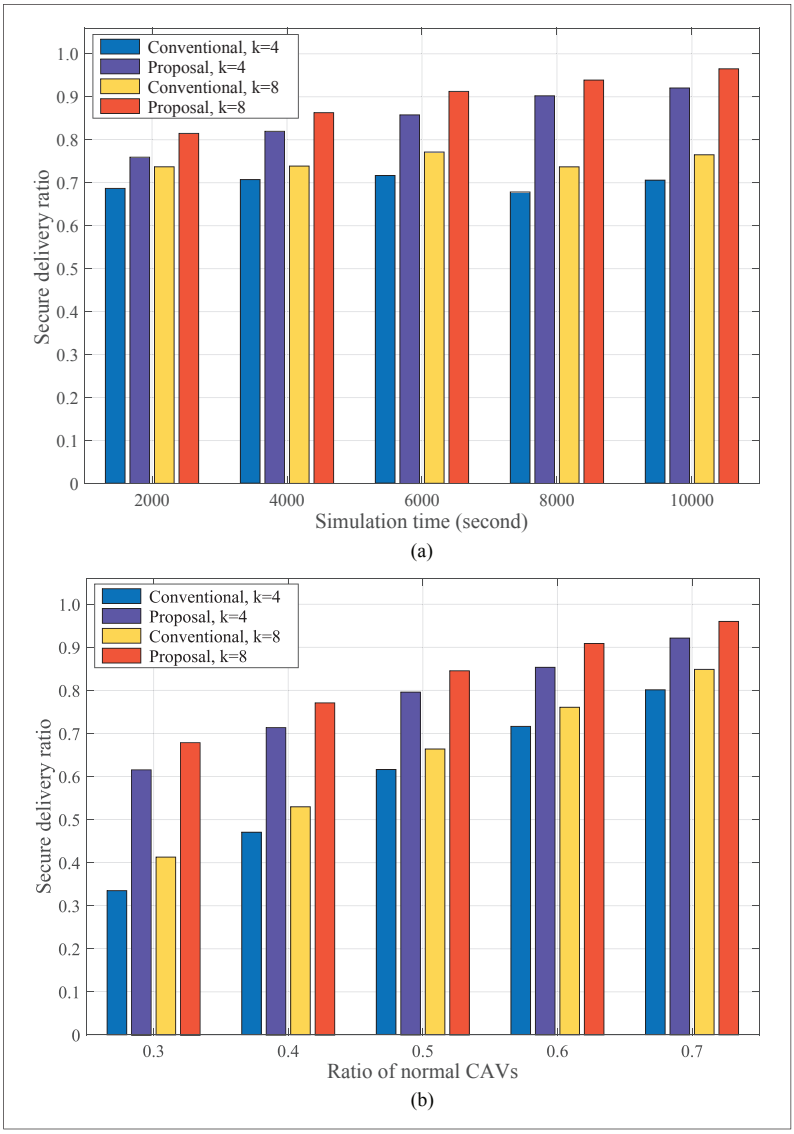

FIGURE 6. a) Secure delivery ratio with different simulation time; b) Secure delivery ratio with different ratios of normal CAVs.

fie-Hellman (co-CDH) assumption [7]. Let n be the number of CAVs in the group. Each member i in the CAV group signs the message Msg and generates its signature σ_i by using its private key and the public keys of other CAVs in the group. Next, a designated secretary is elected in the CAV group to compute the aggregated public key apk by using all the public keys of CAVs in the group. By aggregating all the signatures of CAVs in the group on the same message, the BLS multi-signature σ is generated by the designated secretary. Given (Msg, apk, σ), each verifier can verify the generated BLS multi-signature independently.

Phase 3: Reputation-Based Consensus Process: In the consensus process, each authorized RSU can vote for a consensus node in the blockchain network for ledger management. The voting weight of each RSU is determined by its stake, that is, reputation value. The top O delegates, that is, RSUs, by voting are selected and recorded in the consensus node list (CNL). All valid transactions tx are ordered by their timestamps, packaged into a Merkle tree, and put into a local block by each consensus node. Each consensus node o in CNL competes with each other to solve a PoW puzzle with a certain difficulty which is inversely proportional to its reputation value [10]. The fastest consensus node $\tilde{o}$ that solves its PoW puzzle broadcasts its block proposal *ProposalMsg* to the whole network which contains the solution of PoW puzzle, newly built block, current block height, and hash of the previous block *PreHash*. Other consensus nodes apply a hash validation-comparison function and the longest-chain rule to verify whether they accept this new block. If the verification passes, each consensus node appends the newly generated block to its local blockchain. Each CAV synchronizes the metadata of the latest global blockchain. Note that the higher reputation of RSU, the higher probability to solve its PoW puzzle in less time. Thus, our PoR mechanism can decrease resource consumption of honest RSUs while increasing the cost of attacks conducted by malicious RSUs. In addition, since only trustworthy RSUs with high reputation can be elected as consensus nodes, potential security issues arising from the malicious consensus nodes can be alleviated.

Phase 4: Reward Sharing and Credit Updating: After reaching consensus, the fastest consensus node $\tilde{o}$ is rewarded with a certain amount of task coins, that is, the transaction fee charged in each content transaction. Then, the system updates the credit scores of all consensus nodes based on their recorded behaviors in the blockchain.

Security Analysis

Dependability of Content Delivery: We use the following metric to evaluate the dependability of content delivery. **Secure delivery ratio:** the proportion of successfully delivered true and secure content to the total delivered content in the network. Malicious CAVs may not only forge content data or inject viruses in the delivered content, but also collude to lie and give fake witnesses. In Fig. 6, we compare the proposed framework with the conventional approach [13], which represents a group of cryptography-based literatures, in terms of secure delivery ratio. In the conventional approach, the task requester only accepts content witnessed by a threshold number of vehicles, while the reputation of vehicles is not considered.

In our simulation, the coverages of RSU and CAV are 600m and 200m, respectively. The vehicle density and average vehicle velocity are 60 vehicles/km and 45km/h, respectively. The task is generated by each CAV per second. The TTL of the task follows a uniform distribution varied from 2 to 25s. The reputation threshold is set as 0.6. In Fig. 6a, the ratio of malicious CAVs is set as 0.4. In Fig. 6b, the simulation time is set as 6000s. From the results in Fig. 6, the proposed framework can obtain a higher secure delivery ratio than the conventional approach because only trustworthy CAVs with high reputation can deliver task data and give witnesses in the proposed framework to combat collision attack. Additionally, when the number of required witnesses k grows, both of two schemes can acquire a higher secure delivery ratio since more required witnesses indicate higher cost in delivering content and fewer CAVs will give evidence if the task data is fake.

Integrity and Authentication of Content: The use of collision-resistant hash functions and asymmetric encryption in blockchain ensures the integrity and authentication of content as follows: the sender signs the hash digest of content with its private key, and the receiver verifies the correctness of the signature and checks the hash value of the received content.

Prevention of Forgery: Adversaries may forge transactions and tamper reputation values for profit. On one hand, if an adversary attempts to tamper one of the blocks, he/she needs to recalculate the PoW puzzles of the modified block and all the blocks after this block. Therefore, the transactions stored in each block are nearly unforgeable. On the other hand, the reputation values of nodes are calculated based on the immutable behavior records in blockchain, and cannot be tampered with by adversaries.

Conditional Anonymity: By dynamically changing pseudonyms (i.e., public keys) in different transactions, the anonymity and unlinkability of CAVs can be achieved to hide their true identities. In addition, when disputes arise, RA can reveal the true identity of any adversary to achieve conditional anonymity to prevent anonymous entities from launching attacks without being punished.

In summary, the proposed framework can improve reliability, security, and incentive for content dissemination in AVSNs by integrating with the permissioned blockchain technique.

Future Research Directions

AVSN is a new research topic, and many challenges remain to be addressed. To achieve a flexible, effective, and safe framework for AVSNs, we discuss several open research directions including but not limited to the following.

Quality of Experience (QoE) Support in AVSNs

A tremendous amount of vehicular content is expected to be produced, processed, delivered, and consumed in the upcoming autonomous driving landscape. The growing data traffic and stringent demands for different vehicular content applications pose significant challenges to QoE support in AVSNs [1]. For instance, traffic-related information requires short latency and high reliability, while social entertainment data is delay-tolerant but price-sensitive. Software-defined network (SDN)-based AVSNs offer a potential solution to facilitate flexible network management and optimize vehicular content management in a centralized and programmable manner by decoupling the data plane and control plane [14]. For example, SDN devices such as CAVs can collaborate with each other to get the complete content based on instructions provided by SDN controllers, for example, RSUs or other edge equipment. However, how to implement the control plane to improve QoE in AVSNs becomes an issue to be investigated.

Scalable and Lightweight Blockchain for AVSNs

Due to the ever-increasing number of CAVs and content applications, existing blockchain technology faces bottlenecks in throughput, capacity, isolation, and scalability to improve the quality of content services in AVSNs. One plausible solution is blockchain sharding [15] which splits the whole network into multiple shards, and each shard processes a disjoint set of transactions in parallel. With sharding technology, the throughput of blockchain can increase linearly as more nodes join the system. A main problem in sharding blockchain-based AVSNs is the processing of cross-shard transactions, where efficient inter-shard consensus protocols need to be developed with the integration of CAVs' mobility management. Other promising approaches such as blockchainless directed acyclic graph, sidechain, and lightning network are purposed in recent works to improve the scalability of blockchain [15]. However, these approaches are still under-developed and how to design lightweight and scalable blockchain networks for large-scale AVSNs remains an issue of significance.

Other promising approaches such as blockchainless directed acyclic graph, sidechain, and lightning network are purposed in recent works to improve the scalability of blockchain. However, these approaches are still under-developed and how to design lightweight and scalable blockchain networks for large-scale AVSNs remains an issue of significance.

Security Aware AVSNs

Compared to traditional vehicles driven by humans, the sensor-rich and V2X-enabled CAVs may easily leak out personal privacy and threaten nearby vehicles' security once hijacked [6]. A possible solution is using the blockchain technique to meet the security requirements in decentralized AVSNs. However, such security provisioning operations may degrade the network efficiency in AVSNs [9]. For instance, consensus operation, a crucial process to guarantee the security of blockchain networks, may bring significant delay during content distribution. Accordingly, how to secure content distribution with delivery efficiency is a critical issue in AVSNs, especially for delay-sensitive applications.

Conclusion

In this article, we have investigated content delivery in AVSNs based on blockchain. As a hot topic of AVSNs, data sharing services can be efficiently realized by employing blockchain techniques. Specifically, we have proposed a blockchain-enabled framework in AVSNs for secure and incentive vehicular content delivery. A reputation model is devised to evaluate the trustworthiness of CAVs and RSUs while motivating participants to behave honestly. In addition, we have developed a PoR consensus protocol to efficiently achieve consensus among RSUs and resource-limited CAVs in the blockchain. Experiment results have shown the efficiency of the proposed framework. Finally, several open research directions are discussed. We hope this article sheds more light on the incentive and security for content delivery in AVSNs, where more innovative and pioneering research in this emerging area will be seen in the future.

Acknowledgment

This work is supported in part by NSFC (nos. U1808207, 91746114); the 111 Project; and the Project of the Shanghai Municipal Science and Technology Commission, 18510761000.

References

[1] S. Liu *et al.*, "Edge Computing for Autonomous Driving: Opportunities and Challenges," *Proc. IEEE*, vol. 107, no. 8, Aug. 2019, pp. 1697–1716.

[2] R. Deng, B. Di, and L. Song, "Cooperative Collision Avoidance for Overtaking Maneuvers in Cellular V2X-Based Autonomous Driving," *IEEE Trans. Vehicular Technology*, vol. 68, no. 5, May 2019, pp. 4434–46.

[3] L. Du *et al.*, "Adaptive Visual Interaction Based Multi-Target Future State Prediction for Autonomous Driving Vehicles," *IEEE Trans. Vehicular Technology*, vol. 68, no. 5, May 2019, pp. 4249–61.

[4] Z. Su, Y. Hui, and T. H. Luan, "Distributed Task Allocation to Enable Collaborative Autonomous Driving with Network Softwarization," *IEEE JSAC*, vol. 36, no. 10, Oct. 2018, pp. 2175–89.

[5] S. W. Loke, "Cooperative Automated Vehicles: A Review of Opportunities and Challenges in Socially Intelligent Vehicles Beyond Networking," *IEEE Trans. Intelligent Vehicles*, vol. 4, no. 4, Dec. 2019, pp. 509–18.

[6] R. Xing *et al.*, "Trust-Evaluation-Based Intrusion Detection and Reinforcement Learning in Autonomous Driving," *IEEE Network*, vol. 33, no. 5, Sept.-Oct. 2019, pp. 54–60.

[7] H. C. A. van Tilborg and S. Jajodia, "Encyclopedia of Cryptography and Security," *Springer Science & Business Media*, 2014.

[8] X. Wang *et al.*, "Privacy-Preserving Content Dissemination for Vehicular Social Networks: Challenges and Solutions," *IEEE Commun. Surveys & Tutorials*, vol. 21, no. 2, Secon d Quarter 2019, pp. 1314–45.

[9] Y. Liu *et al.*, "LightChain: A Lightweight Blockchain System for Industrial Internet of Things," *IEEE Trans. Industrial Informatics*, vol. 15, no. 6, June 2019, pp. 3571–81.

[10] J. Huang *et al.*, "Towards Secure Industrial IoT: Blockchain System with Credit-Based Consensus Mechanism," *IEEE Trans. Industrial Informatics*, vol. 15, no. 6, June 2019, pp. 3680–89.

[11] Y. Wang, Z. Su, and N. Zhang, "BSIS: Blockchain-Based Secure Incentive Scheme for Energy Delivery in Vehicular Energy Network," *IEEE Trans. Industrial Informatics*, vol. 15, no. 6, June 2019, pp. 3620–31.

[12] S. Ding *et al.*, "A Novel Trust Model based Overlapping Community Detection Algorithm for Social Networks," *IEEE Trans. Knowledge and Data Engineering*, doi: 10.1109/TKDE.2019.2914201. 2019.

[13] L. Chen, S. Ng, and G. Wang, "Threshold Anonymous Announcement in VANETs," *IEEE JSAC*, vol. 29, no. 3, Mar. 2011, pp. 605–15.

[14] S. Garg *et al.*, "MobQoS: Mobility-Aware and QoS-Driven SDN Framework for Autonomous Vehicles," *IEEE Wireless Commun.*, vol. 26, no. 4, Aug. 2019, pp. 12–20.

[15] J. Xie *et al.*, "A Survey on the Scalability of Blockchain Systems," *IEEE Network*, vol. 33, no. 5, Sept.-Oct. 2019, pp. 166–73.

Biographies

YUNTAO WANG is working on his Ph.D. degree at the school of Cyber Science and Engineering of Xi'an Jiaotong University, Xi'an, P. R. China. His research interests include security and privacy in wireless network architecture and vehicular networks.

ZHOU SU (zhousu@ieee.org) received the Ph.D. degree from Waseda University, Tokyo, Japan, in 2003. He is an associate editor of *IET Communications*, and an associate editor of *IEICE Trans on Communications*. He is the Chair of the Multimedia Services and Applications over Emerging Networks Interest Group (MENIG) of the IEEE Communications Society, the Multimedia Communications Technical Committee. He received the best paper award at IEEE CyberSciTech2017, WiCon2016, CHINACOM2008, and the Funai Information Technology Award for Young Researchers in 2009.

KUAN ZHANG has been an assistant professor in the Department of Electrical and Computer Engineering, University of Nebraska-Lincoln, USA, since September 2017. He received the B.Sc. degree in communication engineering and the M.Sc. degree in computer applied technology from Northeastern University, China, in 2009 and 2011, respectively. He received the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Canada, in 2016. He was also a postdoctoral fellow with the Broadband Communications Research (BBCR) group, Department of Electrical and Computer Engineering, University of Waterloo, Canada, from 2016-2017. His research interests include security and privacy for mobile social networks, ehealthcare systems, cloud/edge computing and cyber physical systems.

ABDERRAHIM BENSLIMANE has been a full professor of computer science at Avignon University/France since 2001. He is the Chair of the ComSoc Technical Committee on Communication and Information Security. He is the EiC of *Inderscience Int. J. of Multimedia Intelligence and Security* (IJMIS), area editor for Security for the *IEEE IoT Journal*, area editor of *Wiley Security and Privacy*, and an editorial member of *IEEE Wireless Communication Magazine*, *Elsevier Ad Hoc Journal*, *IEEE Systems and Wireless Networks*. He is founder and serves as General-Chair of the IEEE WiMob since 2005 and of iCOST and MoWNet international conference since 2011. He was a board committee member, Vice-Chair of Student activities of the IEEE France section/Region 8; he was the Publication Vice-Chair and Conference Vice-Chair of the ComSoc TC for Communication and Information Security.