Secure and Reliable Transfer Learning Framework for 6G-enabled Internet of Vehicles

SCHOLARONE™
Manuscripts

Secure and Reliable Transfer Learning Framework for 6G-enabled Internet of Vehicles

Minrui Xu, Dinh Thai Hoang, Jiawen Kang*, Dusit Niyato, *Fellow, IEEE*, Qiang Yan, Dong In Kim, *Fellow, IEEE*

Abstract—In the coming 6G era, Internet of Vehicles (IoV) has been evolving towards 6G-enabled IoV with super-high data rate, seamless networking coverage, and ubiquitous intelligence by Artificial Intelligence (AI). Transfer Learning (TL) has great potential to empower promising 6G-enabled IoV, such as smart driving assistance, with its outstanding features including enhancing quality and quantity of training data, speeding up learning processes and reducing computing demands. Although TL had been widely adopted in wireless applications (e.g., spectrum management and caching), its reliability and security in 6G-enabled IoV were still not well investigated. For instance, malicious vehicles in source domains may transfer and share untrustworthy models (i.e., knowledge) about connection availability to target domains, thus adversely affecting the performance of learning processes. Therefore, it is important to select and also incentivize trustworthy vehicles to participate in TL. In this article, we first introduce the integration of TL and 6G-enbaled IoV and provide TL applications for 6G-enabled IoV. We then design a secure and reliable transfer learning framework by using reputation to evaluate the reliability of pre-trained models and utilizing the consortium blockchain to achieve secure and efficient decentralized reputation management. Moreover, a deep learning-based auction scheme for the TL model market is designed to motivate high-reputation vehicles to participate in model sharing. Finally, the simulation results demonstrate that the proposed framework is secure and reliable with well-design incentives for TL in 6G-enabled IoV.

Index Terms—Transfer learning, 6G, blockchain, learning-based auction, Internet of Vehicles, incentive mechanism.

I. INTRODUCTION

The unprecedented evolution of wireless communication technologies, e.g., from 4G to 5G and beyond, has paved the way for a large number of advanced vehicular network applications. Particularly, 6G technologies can provide seamless and ubiquitous communications for vehicles and infrastructures which are naturally large-scale and mobile ad-hoc [1]. Therefore, there is a strong push for future vehicle networks in 6G to meet stringent reliability and security requirements. 6G technologies are expected to bring breakthroughs as well as a comprehensive revolution for 6G-enabled Internet of Vehicles (IoV) [2]. For example, 6G can provide IoV with super-high data rates (e.g., up to 1Tb/s), very broad frequency bands (e.g., 73GHz-140GHz and 1THz-3THz), and less than 1-millisecond end-to-end latency.

Minrui Xu, Jiawen Kang, Dusit Niyato are with School of Computer Science and Engineering, Nanyang Technological University, Singapore. Dinh Thai Hoang is with School of Electrical and Data Engineering, University of Technology Sydney, Australia. Qiang Yan is with WeBank Co., Ltd., China. Dong In Kim is with the College of Information & Communication Engineering, Sungkyunkwan University, South Korea. (*Corresponding author: Jiawen Kang*)

In the near future, 6G-enabled IoV is expected to facilitate a safer, more efficient, and intelligent traffic system, which strictly requires heterogeneous communications, latency-critical applications, and scalable vehicular networks. To meet these requirements, Artificial Intelligence (AI) has been regarded as a core component to empower 6G-enabled IoV [1]. Machine Learning (ML), e.g., reinforcement learning and deep learning (DL) can be implemented to design and optimize IoV architecture and network orchestration in a cost-efficient manner. In addition, through a huge amount of data collected from entities in IoV (e.g., vehicles and infrastructures), AI solutions are able to synthesize, analyze, and provide important information for optimizing operations, thereby meeting stringent security requirements, high-mobility, and efficiency of 6G-enabled IoV. For example, AI can assist drivers by recognizing, searching, and sharing local and roadside information, e.g., traffic signs and adaptive speed signs [3]. This smart driving assistance thus can significantly improve driving safety, reduce fuel consumption, and traffic management efficiency in 6G-enabled IoV.

Although being considered an integral component of 6G, current ML approaches have been facing challenges for practical implementation in IoV, high mobility, dynamics, and heterogeneity. In particular, the deployment of AI in 6G-enabled IoV is constrained by dynamic wireless environments, lack of labeled data, long training process, and limited capacity and resources of vehicles. Fortunately, Transfer Learning (TL) [4] has been recently introduced with many applications in wireless networks, e.g., spectrum management and signal recognition. TL can develop intelligent solutions to maximize data extraction efficiency from the same or similar domains, thereby remarkably enhancing AI solutions for IoV [5]. As a result, the development of TL for future 6G-enabled IoV is expected to significantly speed up the learning process and reduce computing costs, thus meeting the extremely high requirements of 6G-enabled IoV.

However, due to the utilization of knowledge from different sources, which might be untrusted, to improve learning efficiency, the reliability and security of TL are the main concerns for its deployment. Thus, in this article, we introduce a novel framework that provides secure and reliable services for deploying TL in future 6G-enabled IoV. Specifically, we introduce the concept of reputation as a metric to evaluate the reliability and trustworthiness of pre-trained models built and owned by vehicles, and thus design a reputation-based trainer selection scheme for FL. To achieve secure and efficient decentralized reputation management, consortium blockchain is leveraged for reputation management. Finally, to motivate

Fig. 1: Tradition machine learning vs. Transfer Learning for 6G-enabled IoV in Space-Air-Ground Integrated Networks.

high-reputation vehicles participating in TL model transferring, a deep learning-based auction (DLA) scheme is designed to incentivize trustworthy vehicles.

The main contributions of this article are summarized as follows:

- We first introduce TL, 6G, and IoV together with their integration which envisions a blueprint for future intelligent transportation systems. To enable efficient TL deployment, we design a novel model trading market for 6G-enabled IoV. The proposed model trading can effectively improve the quality of ML in TL environments by encouraging good source model owners to participate and contribute.
- We employ reputation as a reliable metric to select trustworthy pre-trained models for reliable TL. We then design a distributed reputation calculation and management scheme by utilizing blockchain technology to regulate the reputation in a decentralized and secure manner. With the proposed metric and scheme, TL can be performed in IoV systems in a more secure and reliable way.
- To achieve dynamic and reliable model trading, we propose the DLA scheme considering the reputation of model sellers and bids of model buyers. This scheme is effective to maximize revenue for sellers, i.e., source model owners, while guaranteeing individual rationality and incentive compatibility for buyers, i.e., target model owners. Simulation results show that the proposed TL framework can assure secure and reliable services as well as well-incentives for vehicles.

II. FUNDAMENTALS OF TRANSFER LEARNING

A. Overview

Transfer learning has recently been introduced as a highly effective machine learning solution that can address many existing problems of traditional ML methods [4]. TL can effectively extract valuable knowledge from learning tasks in source domains to improve the learning performance in similar target domains. For example, in Fig. 1, we provide an example of using traditional ML and TL for 6G-enable IoV in Space-Air-Ground Integrated Networks (SAGIN) [6], which

aim to provide ubiquitous connectivity by utilizing ground, air, and space vehicles and infrastructures. In SAGIN, ML was adopted for optimal path choosing for satellite networks to improve the driving navigation and safety of vehicles. However, collecting data from SAGIN for ML model training is intricate and unbalanced. In details, data from the safe domain, e.g., with rare accident events, is rich while data from the risky domain, e.g., with frequent accident events, is scarce, leading to unsatisfactory driving performance of ML models in risky tasks, such as car crashes. Thus, the development of TL is expected to provide many benefits over traditional ML techniques. For example, by leveraging valuable knowledge from similar environments or applications, TL can overcome the lack of labeled data in specific tasks. Additionally, the shared knowledge, along with knowledge collected and extracted from previous experiences, can also be utilized to reduce computation workloads required for model training as well as to speed up slow learning processes of traditional ML techniques. Furthermore, the knowledge from other sources can be transferred in the form of weights, such as learning rate and random seed. As a result, TL does not incur much communication overhead, and data privacy is also protected. With such outstanding benefits, TL has been considered to be an indispensable part of future wireless networks [5].

B. Basic Concepts

- *Domain:* A domain is defined by a feature space and a marginal probability distribution. The marginal probability distribution is the probability distribution of different types of signal in the dataset.
- *Task:* Given a domain, a task can be defined by a label space (e.g., a set of all driving decisions) and a predictive function. By training with datasets of the source and the target domains, the predictive function can predict labels for given data samples.

Based on the domain and task, TL can be defined as follow: given a source domain with a corresponding source task and a target domain with a corresponding target task, the goal of TL is to learn the target predictive function by leveraging the knowledge gained from the source domain and the source

task. In TL, either the source domain and the target domain are different or the tasks of both domains are different. Take autonomous driving as an example, this means that, either the image features of the set of source driving experience and the set of target driving experience are different (i.e., driving under different scenarios), or the marginal distributions of the two sets are diverse. Therefore, TL can be applied in various applications in 6G-enabled IoV.

C. Classification of Transfer Learning

Based on the similarity between domains and tasks as well as the availability of labeled data, TL can be classified into:

- *Inductive TL*: The source and target domains are the same, but the source and target tasks are different. For inductive TL, the target data should be labeled. Depending on the availability of labeled data at the source domain, inductive TL can be further classified into *self-taught learning* and *multi-task learning*. In *self-taught learning*, the source data is not labeled, and they cannot be used for training the target predictive function. Instead, they can be leveraged to reduce the feature space in the target domain. In contrast, labeled source data is available in *multi-task learning*. Thus, the source model's weights and parameters can be transferred to the target model.
- *Transductive TL*: The source and target domains are different, but the source and target tasks are the same. For transductive TL, labeled target data is not required, while the source data must be labeled. Since the two tasks are the same and the source model is trained with labeled data, the source model's weights and parameters can be transferred to the target model to overcome the lack of labeled data at the target domain.
- *Unsupervised TL*: The target and source tasks are different and there is no labeled data in both domains. For unsupervised TL, the knowledge gained from the unsupervised learning process at the source task can be transferred to serve as the initial point for learning the target task, thereby improving the learning performance of the target task.

The choice among these three TL classifications is determined by the availability of training data in learning problems. When labeled data is available in target domains, Inductive TL can be utilized to accelerate the learning process of TL. If labeled data is unavailable in target domains but available in source domains, Transductive TL is effective to be leveraged to enhance quality and quantity of data in target domains. Finally, when labeled data is unavailable in both source and target domains, Unsupervised TL can be used to transfer the knowledge between source and target domains.

D. Strategies of Deep Transfer Learning

Imitating the brain structure of creatures, DL uses a multi-layered architecture called Deep Neural Networks (DNN). DNN is trained to perform specific tasks such as classification, clustering, or regression. With the training data, DNN updates its knowledge, which is represented by its parameters. Using the knowledge acquired during its learning phase, DNN executes the learned task. A trained DL model can be regarded as knowledge obtained from training data, including its architecture and parameters. Therefore, DL provides an effective way to transfer knowledge from one domain to another one, namely, Deep Transfer Learning (DTL) [4]. There are three typical strategies used in DTL:

- *Off-the-shelf pre-trained models*: DL model training is a data-hungry and time-consuming work. Fortunately, such an inefficient training process is relieved by directly leveraging pre-trained models, which are trained from neighboring domains, for target tasks. For example, in traffic sign classification tasks, some pre-trained models, such as VGG, GoogLeNet, and ResNet50, can be easily obtained from common DL libraries.
- *Pre-trained models as feature extractors*: Extracting features is an important procedure in ML algorithms, which directly affects decision-making for these algorithms. In DL, DNN can automatically learn the features extraction from the training data. Therefore, knowledge from the source domain is embedded in this new representation, which improves the learning process in the target domain.
- *Fine-tuning pre-trained models*: Instead of leveraging all parameters of pre-trained models directly, certain parts or a whole pre-trained source model can be continuously fine-tuned with target data to further improve the performance of the TL model further. The fine-tuned of pre-trained models can be performed in Weight Initialized and Selective Fine-tuning.

However, the best strategy selection for DTL is not straightforward, which should consider multiple factors including the size of target data and similarity between the source and target domains. For example, when target labeled data is large, Weight Initialization is an effective solution since overfitting is not a considerable concern. In contrast, when target data is small, we can use a pre-trained model as a feature extractor. Moreover, if source and target data are similar, we can use the whole pre-trained model. Otherwise, it is better to transfer only some general features from the first few layers of DNN.

E. Potential Applications of TL in 6G-enabled IoV

1) Mobile Extended Reality: Mobile Extended Reality (XR) refers to various technologies, such as augmented, mixed, and virtual reality employed to digitally enhance vehicular environments and human interactions in real-time. The rapid development of 6G networking technologies and wearable devices is paving the way for XR. However, this also brings forth several challenges. Particularly, drivers' demands for more high-quality and personalized experiences have been rapidly increasing in 6G-enabled IoV. For example, a federated learning algorithm in [7] was used to proactively determine vehicles' orientations and mobility to minimize breaks in presence that can detach the XR users from their virtual world. However, conventional ML techniques might not be effective as they may require a lot of data and training time. By utilizing TL, data collected from vehicles' individual interactions can be collected to train a generalized ML model, and then the model

TABLE I: Potential Applications of Transfer Learning in 6G-enabled IoV

6G-enabled IoV Applications	Typical Services	TL Strategies	TL Advantages
Mobile Extended Reality	Minimizing breaks in presence of XR users [7]	Fine-tuning pre-trained models	Enhancing quality of experiences, reducing computing demands
Mobile Digital Twins	Mitigating unreliability in long-distance communication [8]	Pre-trained models as feature extractors	Improving driving safety, protecting drivers' privacy
UAV-assisted Autonomous Driving	Providing ultra-high reliability and connectivity [9]	Off-the-shelf pre-trained models	Addressing lack of labeled data, speeding up learning processes

is transferred to other nodes (e.g., vehicles) for fine-tuning, thereby enhancing the quality of experiences and reducing computing demands simultaneously.

2) Mobile Digital Twins: Digital twins utilize the digital monitoring of physical vehicles to achieve real-time and accurate operations for 6G-enabled IoV. With the availability of a massive amount of data, ML is an essential solution for digital twins to leverage such data to enable various cutting-edge vehicular applications. For instance, a federated learning-empowered digital twin wireless network was introduced in [8] to mitigate the unreliability in long-distance communication between vehicles and infrastructures. However, due to strict requirements of driver-privacy protection and data sharing, the ML-based driving virtual assistants usually do not have sufficient data for timely traffic analysis and monitoring. To solve this problem, TL can be used to leverage knowledge from similar experiences (i.e., source domain) to each vehicle (i.e., target domain) aiming to improve the ML-based personal driving assistant's performance for driving safety.

3) UAV-assisted Autonomous Driving: Despite its rapid development, autonomous driving is still facing challenges in 6G-enabled IoV. Particularly, Unmanned aerial vehicles (UAV)-assisted automated driving systems are network-dependent, i.e., they require continuous communication to function properly. In this context, ML can provide these systems with ultra-high reliability and connectivity [1]. TL can be applied into these systems which are impeded by lack of labeled data, to enhance the performance of the conventional ML techniques. Specifically, there are many factors affecting vision-based data, e.g., weather conditions and broken infrastructures. These variances are not always presented in a dataset collected for a specific area. Therefore, knowledge about these variances can be transferred from a more comprehensive dataset of different areas to improve the target models' robustness if such events occur. For example, to optimize the performance of the autonomous driving systems under environments with different objectives, uncertainties, and dynamics, a TL-based framework was developed in [9] for enhancing scalability and reliability for joint radar and data communication systems. In conclusion, TL can empower vehicles to learn quickly an optimal policy when they travel to new environments.

Finally, the summary of these aforementioned potential applications is provided in Table. I.

III. CHALLENGES OF IMPLEMENTING TRANSFER LEARNING IN 6G-ENABLED IOV

A. Technical Challenges of TL Algorithms

1) Determine the Source Task: TL requires in-depth and task-specific analysis in domains of source and target tasks to determine whether these tasks are similar. For example, to perform similar resource management tasks in IoV, the source task can be chosen based on physical distance from source to target vehicles [4]. The reason is that surrounding vehicular networks of source and target tasks are similar, and hence their experiences are likely to be related. Alternatively, TL can transfer knowledge of the same vehicular task (e.g., pedestrian detection task) to different driving environments. However, 6G-enabled IoV typically has very wide coverage [1], leading to a large number of choices for source domains for TL applications. Moreover, several 6G-enabled IoV services, e.g., satellite communications, are specific to certain areas and groups of vehicles. If source and target domains are not correlated, the use of TL in 6G-enabled IoV even makes target models perform worse than just training with only target data.

2) Determine What to Transfer: Following the choice of the source task, the domain knowledge needs to be transferred to target tasks. Determining what to transfer is important for TL to enable vehicular networks to cover a wide range of scenarios. However, in some scenarios, e.g., car crashes which are rare, obtaining the labeled data for TL training in the real world is intractable and even impossible. As such, transductive TL is typically used to transfer some related knowledge to handle the tasks in such scenarios. For instance, in emergency rescue tasks, the rescue vehicles can be trained to save life in simulation systems and then be dispatched in real-world [1]. To further reduce fine-tuning time, some TL approaches to transfer the entire source model, while others transfer only the first few layers of DNN. However, this question depends on IoV scenarios that affect the fine-tuning time of TL.

B. Reliability and Security of TL

1) Decentralized Environment: Most of the aforementioned TL model sharing schemes are centralized, i.e., the transfer of knowledge is governed by a single entity, e.g., a network operator. However, in 6G-enabled IoV with a massive scale of interconnected vehicles and infrastrutures [1], decentralized TL model sharing is a more promising approach. Particularly, valuable knowledge can be obtained from external or third-party sources such as neighboring networks, controlled by different operators, or vehicles. However, for such decentralized approaches, security and privacy challenges become a primary concern, e.g., attackers, eavesdroppers, and malicious vehicles. For example, a model used for accident prevention in 6G-enabled IoV should have a higher degree of accuracy than that of an ordinary vehicular networks because a single false negative event (e.g., failed to predict a potential accident) could have very serious consequences. In recent years, blockchain, which can enhance decentralized network's

security and privacy, has been successfully applied in various wireless applications. Thus, utilizing blockchain for decentralized TL is a attractive research direction. For instance, the authors in [10] proposed a blockchain-based framework for DTL. By using blockchain and smart contracts, the proposed framework allows vehicles to securely and reliably share their models, data, and resources. Moreover, smart contracts facilitate automatic payment processes, which paves the way for crowdsourcing-enabled TL.

2) Model Quality Evaluation: TL is still vulnerable to adversarial attacks for data owners (e.g., vehicles) in 6G-enabled IoV can intentionally or unintentionally mislead the source model during TL processes. For instance, in the poisoning attack, an attacker sends a malicious source model to manipulate the parameters of the source model, resulting in the failure of the model transfer [4]. Furthermore, dynamic vehicular networking environments may lead to some unintentional adverse behaviors of source model owners. In addition, data owners may unintentionally update poor-quality models due to high-speed mobility or energy constraints, thereby degrading the learning performance. Thus, TL should be able to evaluate the quality of transferred models accurately to avoid such intentionally or unintentionally unreliable model sharing.

3) Efficient Incentive Mechanism for Model Sharing: TL can improve the effectiveness of current ML algorithms by transferring the knowledge of the source domain to the target domain. However, to motivate high-quality source model trainers to share their models, an efficient incentive mechanism for a model sharing market is also needed. In this market, source model trainers (e.g., vehicles) as sellers spend their data and computing resources to improve the inference ability of pre-trained models in source domains. On the other hand, model buyers in the market are the receivers, whose goals are obtaining the utility-maximized and reliable target models to perform their local tasks (e.g., traffic sign recognition tasks). Naturally, participants in the TL market are self-interested and attempt to maximize their utilities. Model sellers intend to maximize their revenue from model trading, while model buyers aim to receive the best models for local tasks. Without proper pricing and allocation mechanisms, trustworthy model sellers may be reluctant to share their models with potential buyers. Moreover, in 6G-enabled IoV which requires ultra-high reliable and ultra-low latency services [1], incentive schemes are required to perform decisions in real-time under dynamic network environments. As a result, the incentive scheme designed for the TL market to meet these stringing requirements has still not well investigated.

IV. A SECURE AND RELIABLE FRAMEWORK OF TRANSFER LEARNING FOR 6G-ENABLED IOV

In this section, we propose a secure and reliable TL framework for 6G-enabled IoV to address the aforementioned problems. In particular, this framework includes three phases, i.e., blockchain-empowered decentralized model sharing, reputation for model quality evaluation, and learning-based auction for model trading. Thus, the proposed TL framework for 6G-enabled IoV can offer decentralized and real-time services.

A. Blockchain Empowered TL Model Trading Markets

We consider pre-trained model sharing as model trading between source and target domains in a TL model trading market. To achieve secure pre-trained model trading, a consortium blockchain named "TL blockchain" is established on edge servers (e.g., RoadSide Units, RSU) acting as miners to run smart contracts for model information sharing and model trading of the pre-trained models [11]. Specifically,

- *Model Information Sharing Smart Contract*: Each model owner (e.g., a vehicle) first finalizes a training task (e.g., traffic sign recognition) in the source domain. The model owners generate metadata of their pre-trained models including pseudonyms of owners, model descriptions of the pre-trained models (e.g., training task, accuracy, model size, model usage, trading requirement, timestamp, and digital signature for information verification), and biding prices. The model owners then run the model information sharing smart contract to automatically upload the metadata to the TL blockchain miners, thus running a consensus algorithm, e.g., delegated proof-of-stake, to finish block verification and synchronization. After that, the pre-trained models can be recorded on the TL blockchain for model trading (as illustrated in Steps 1 and 2 in Fig. 2).

- *Model Trading Smart Contract*: Model buyers (e.g., vehicles) in the target domain obtain the latest block data from the TL blockchain. According to buyers' training tasks, e.g., pedestrian recognition, buyers search the metadata on the block data and pick out potential model sellers (i.e., model owners in the source domain). Buyers also retrieve the reputation values of model sellers from the TL blockchain to filter malicious sellers with low reputations. Here, we utilize reputation value as a metric to indicate the reliability of model owners, and the reputation reflects the quality of pre-trained models of model owners (more details about reputation are given in Section IV-B). Model buyers and sellers perform a learning-based auction scheme for model pricing and trading according to bidding prices and the reputation of the sellers (Section IV-C). Then, model buyers obtain pre-trained models (i.e., knowledge) from the matched sellers and begin to fine-tune their target models. If the training performance of a target task is good enough, e.g., accuracy higher than a given threshold, the buyer will treat this trading record as a positive event and generate a good reputation rating (Steps 3, 4 and 5 in Fig. 2) [12]. After that, a model trading smart contract will be executed to upload the reputation and trading records to miners in TL blockchain for block verification and recording (Step 6 in Fig. 2).

B. Decentralized Reputation Management

Similar to [12], reputation is introduced to measure the trustworthiness and reliability of model sellers according to their historical behaviors. By the reputation, model buyers can select reliable and trusted model buyers with high-quality pre-trained models, thus avoiding the effects of low-quality
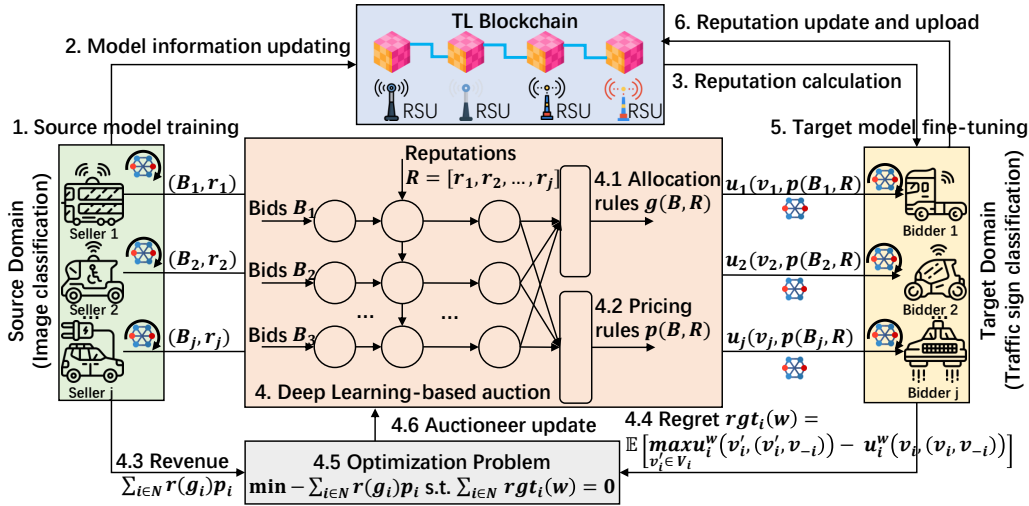
Fig. 2: A secure and reliable TL framework for 6G-enabled IoV including three main phases, i.e., blockchain-empowered decentralized model sharing, reputation for model quality evaluation, and learning-based auction for model trading.

models on target task training. Moreover, since reputation plays a significant role for TL, to remove the potential risks of centralized reputation calculation and management, we design a decentralized reputation calculation and management scheme utilizing advantages of TL and blockchain technologies.

- *Decentralized reputation calculation:* For each traded pre-trained model from a seller, it will generate a performance rating of the pre-trained model using in the target tasks by model quality evaluation methods, e.g., sharply values [13]. If the pre-trained model leads to good performance on the target tasks, e.g., high accuracy, the model buyer treats this trading interaction with the model seller as a positive event, otherwise, the interaction is a negative event. Then, the direct reputation of buyer i for seller j is denoted as the ratio of the number of positive interaction events to the total number of interaction events in a time window. To achieve accurate and objective reputation calculation, we should consider both direct reputation and an overall recommended reputation from its friends, who have cooperated with the buyer before, for the same seller. Here, the overall recommended reputation is expressed by the weighted sum of the trustworthiness weights of buyers for their friends and the corresponding recommended reputation of the friend to the same seller. Both the trustworthiness weight and reputation value are in the range of [0, 1]. Moreover, the referenced reputation values from strangers are the average reputation value of a stranger to the seller. Finally, the integrated reputation value r_{ij} of buyer i to seller j is the weighted sum of the direct reputation, the recommended reputation, and the referenced reputation values.
- *Blockchain-based reputation management:* To achieve secure and decentralized reputation management, after model training, the model buyers upload their integrated reputation values with the corresponding digital signatures as "transactions" to the miners of the TL blockchain. With the help of an efficient consensus algorithm, the

verified reputation data is stored in the TL blockchain for immutable, transparent, and reliable management. These reputation values will be recommended to and referenced by other model buyers.

C. Deep Learning-based Auction Scheme for TL Model Trading

To develop an efficient incentive mechanism, auction theory is regarded as a promising tool to maximize the income of model sellers while ensuring the bidder's desired characteristics, such as individual rationality and incentive compatibility [14]. However, traditional auction schemes cannot be applied to real-time optimal trading and pricing scenarios. We, therefore, develop a Deep Learning-based auction (DLA) scheme to make the allocating and pricing decisions for model sharing when demands of vehicles frequently change over time. Particularly, an auctioneer parameterized by neural networks first performs monotone transformations of input buyers' values, as well as the reputation of sellers. Based on the real-time reputations of sellers, the auctioneer then calculates the allocation rules, i.e., winning probabilities of bidders, and conditional payment rules for the TL model market. Lastly, the auctioneer is trained w.r.t. the loss function so that it can adjust the weights to optimize the expected outcome of this market.

In DLA, the auctioneer knows the value distribution of bidders but not their actual valuation. The auctioneer inputs sellers' reputations and bidders' bids, and then outputs the pricing rules and the allocation rules (Steps 4.1 and 4.2 in Fig. 2). The buyer with its valuation obtains its utility computed as valuation minus price. An auction is dominant strategy incentive compatible (DSIC) [15], if each buyer maximizes its utility by reporting truthfully regardless of its counterparts report. When each buyer receives a non-zero utility at the end of the auction, it is (ex-post) individually rational. The DSIC auction requires each buyer to report truthfully, and so the revenue on the valuation profile should be accurate. The DSIC

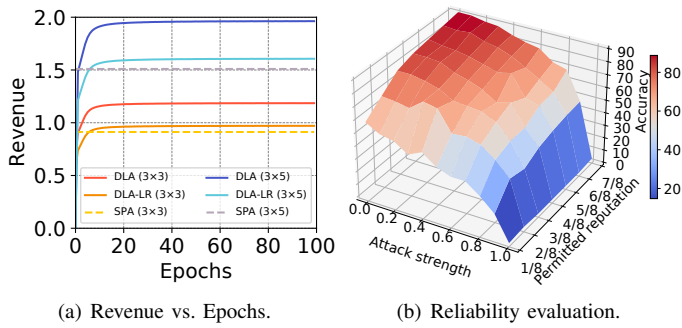(a) Revenue vs. Epochs.   (b) Reliability evaluation.

Fig. 3: Security and reliability evaluation of the proposed TL framework and DLA scheme, where the attack strength is the ratio of falsified labels of a training dataset of the sellers and the permitted reputation is the required reputation to allow sellers to participate.

auction that maximizes its revenue is considered as the optimal DSIC auction design.

To obtain a satisfactory solution for DSIC auction, DLA schemes are widely adopted. DLA utilizes multi-layer neural networks to encode auction mechanisms. In order to handle sequentially inputted bids for multiple items in the TL model Market, neural networks are used to process the current state and output the temporal results. In detail, reputations downloaded from the TL blockchain are input in the hidden layer. Thus, the proposed auction scheme is more reliable. Then, the temporal results are input to the softmax layer for allocation rules and the sigmoid layer for pricing rules. The goal of the DLA scheme is to find a solution to minimize the negative, expected revenue (Step 4.3 in Fig. 2), while satisfying incentive compatibility. Our primary goal is to ensure that the selected auction satisfies the requirement for incentive compatibility in the learning problem. Our method for measuring incentive compatibility is to calculate an ex-post regret for every bidder. Bidder is likely to regret their decision ex-post (Step 4.4 in Fig. 2). In this context, the learning problem is to minimize the expected loss, i.e., the expected negated revenue s.t. sum ex-post regret for all bidders equals zero (Step 4.5 in Fig. 2). Using the augmented Lagrangian method, we solve the constrained training problem over the space of neural autoworker parameters. Adding a quadratic penalty term for violating constraints, the Lagrangian function is defined for the optimization problem. Therefore, the DLA scheme can make secure and reliable optimal allocation and pricing decisions for the TL model market in real-time, hence preventing malicious vehicles from adversely affecting the performance of TL in 6G-enabled IoV.

D. Simulation Results

Simulations are used to illustrate the effectiveness of our DL-based auction scheme. The proposed auction scheme is implemented with the same parameters in [15]. TL model markets are simulated with different numbers of participants to analyze the performance of the DLA scheme. Here, TL model markets consist of 3 buyers and 3 sellers (3×3) and 3 buyers and 5 sellers (3×5). Figure 4 shows the simulation results for

evaluation of the proposed secure and reliable TL framework. As shown in Fig. 3(a), the DLA scheme converges quickly to the solution. The model sellers with low reputation, i.e., DLA-LR, receive less revenue in model trading. However, the revenue of DLA schemes with different numbers of sellers is much higher than that of the second-price auction (SPA) [14]. This proves the effectiveness of the proposed scheme whether the number of sellers is equal to three or five. Moreover, Fig. 3(b) shows the change of TL model accuracy affected by malicious sellers' attack strength and the permitted reputation of the TL market. We can observe that the increasing attack strength decreases the accuracy of target models. The higher reputation threshold of being sellers brings larger accuracy because fewer malicious models from low-reputation sellers are transferred to the buyers in the target domain. Fig. 3(b) also illustrates that the reputation scheme can ensure reliable and secure TL by removing unreliable or malicious source model trainers.

V. CONCLUSIONS AND OPEN ISSUES

In this article, we propose a secure and reliable transfer learning framework for 6G-enabled IoV with blockchain empowered model trading market. In the model trading market, we first introduce reputation as the metric to evaluate the reliability of model sellers in the source domain. With the help of reputation, we then design the machine learning-based auction scheme considering sellers' reputations to achieve optimal DSIC auction in model trading pricing for reliable model trading in TL. The simulation results show that the proposed framework and scheme can provide secure and reliable transfer learning services with well-design incentives for 6G-enabled IoV.

There are several possible directions that are worth being studied: 1) Since vehicles in 6G networks have limited power and resources. It still remains to be an open issue on how to design light-weight and resource-efficient TL algorithms for large-scale deployment on these vehicles by combining advanced machine learning techniques, such as sparse representation in neural networks, and pruning algorithms to dwindle TL models. 2) Since model quality valuation methods directly affect the reputation calculation, there is one more open issue on how to design more accurate and efficient model quality valuation methods for 6G-enable IoV to improve the accuracy and objectivity of reputation calculation, thus enhancing the detection performance of unreliable model sellers. 3) It is also an open issue on how to improve the scalability of consortium blockchain for efficient reputation management in TL-based 6G-enabled IoV. Sharding and cross-chain technologies are promising solutions to establish scalable and efficient blockchain systems for 6G-enabled IoV. 4) Considering the high overhead of a large number of vehicles that may join in the transfer learning for 6G-enabled IoV, efficient schemes for optimizing the number of training model in target domains are worth investigating to balance the learning performance and resource cost.

References

[1] B. Ji, X. Zhang, S. Mumtaz, C. Han, C. Li, H. Wen, and D. Wang, "Survey on the internet of vehicles: Network architectures and applications," *IEEE Communications Standards Magazine*, vol. 4, no. 1, pp. 34–41, Mar. 2020.

[2] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Network*, vol. 34, no. 3, pp. 134–142, May/June 2020.

[3] X. Zhou, W. Liang, J. She, Z. Yan, and K. I.-K. Wang, "Two-layer federated learning with heterogeneous model aggregation for 6G supported Internet of Vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 5308–5317, June 2021.

[4] Q. Yang, Y. Zhang, W. Dai, and S. J. Pan, *Transfer learning*. Cambridge University Press, 2020.

[5] C. T. Nguyen, N. Van Huynh, N. H. Chu, Y. M. Saputra, D. T. Hoang, D. N. Nguyen, Q.-V. Pham, D. Niyato, E. Dutkiewicz, and W.-J. Hwang, "Transfer learning for future wireless networks: A comprehensive survey," *arXiv preprint arXiv:2102.07572*, 2021.

[6] N. Kato, Z. M. Fadlullah, F. Tang, B. Mao, S. Tani, A. Okamura, and J. Liu, "Optimizing space-air-ground integrated networks by artificial intelligence," *IEEE Wireless Communications*, vol. 26, no. 4, pp. 140–147, Aug. 2019.

[7] M. Chen, O. Semiari, W. Saad, X. Liu, and C. Yin, "Federated echo state learning for minimizing breaks in presence in wireless virtual reality networks," *IEEE Transactions on Wireless Communications*, vol. 19, no. 1, pp. 177–191, Jan. 2020.

[8] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Low-latency federated learning and blockchain for edge association in digital twin empowered 6G networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 5098–5107, July 2021.

[9] N. Q. Hieu, D. T. Hoang, D. Niyato, P. Wang, D. I. Kim, and C. Yuen, "Transferable deep reinforcement learning framework for autonomous vehicles with joint radar-data communications," *arXiv preprint arXiv:2105.13670*, 2021.

[10] A. ul Haque, M. S. Ghani, and T. Mahmood, "Decentralized transfer learning using blockchain & IPFS for deep learning," in *International Conference on Information Networking (ICOIN)*, pp. 170–177, Jan. 2020.

[11] H. Lin, J. Hu, X. Wang, M. F. Alhamid, and M. J. Piran, "Toward secure data fusion in industrial IoT using transfer learning," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 10, pp. 7114–7122, Oct. 2021.

[12] J. Kang, Z. Xiong, D. Niyato, S. Xie, and J. Zhang, "Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10700–10714, Dec. 2019.

[13] M. R. Parvez and K.-W. Chang, "Evaluating the values of sources in transfer learning," in *Proceedings of the 2021 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies*, (Online), pp. 5084–5116, Association for Computational Linguistics, June 2021.

[14] D. Niyato, N. C. Luong, P. Wang, and Z. Han, *Auction Theory for Computer Networks*. Cambridge University Press, 2020.

[15] P. Dütting, Z. Feng, H. Narasimhan, D. Parkes, and S. S. Ravindranath, "Optimal auctions through deep learning," in *International Conference on Machine Learning*, pp. 1706–1715, PMLR, May 2019.