Federated Imitation Learning: A Cross-Domain Knowledge Sharing Framework for Traffic Scheduling in 6G Ubiquitous IoT

Ao Yu, Qingkai Yang, Lihua Dou, and Mohamed Cheriet

Abstract

The ubiquitous Internet of Things (IoT) system is a key component of future 6G networks to realize a fully connected world. Extensive efforts have been made to provide on-demand traffic scheduling in IoT networks through machine learning algorithms. However, the current learning approaches are hindered by the heterogeneous information in ubiquitous IoT systems since the data are collected from different domains (e.g., space, air, ground, and ocean). To uncover the complete picture of ubiquitous IoT, this article presents a novel federated imitation learning framework for traffic prediction without compromising privacy. This framework contains a knowledge-sharing module to imitate the status of cross-domain models. After that, we design a distributed resource allocation algorithm, where the IoT devices cooperatively make association decisions using matching theory. Simulation results reveal that our proposed approach outperforms state-of-the-art federated transfer learning and achieves desirable traffic scheduling performance in a cross-domain environment.

Introduction

With the recent breakthroughs in sixth-generation (6G) communication networks, the world will witness a considerable shift in almost every aspect of our life [1, 2]. Numerous devices, such as healthcare wearables, patrol drones, and smart water quality monitoring sensors, are joining the Internet of Things (IoT) network [3]. Undoubtedly, ubiquitous IoT in the 6G era is expected to connect to anyone and anything.

In such a vast IoT network, ranging from the domains of space, air, ground, and ocean, artificial intelligence (AI) is considered the most promising paradigm to solve the traffic scheduling problem [4–6]. To allow AI algorithms to offer decision support suitable for precision traffic scheduling implementations, large amounts of heterogeneous user data collected from different sensors are necessary. For example, training a traffic prediction model requires a large database encompassing the full traffic header information, timestamp, and input data types. Another challenge of applying AI to 6G ubiquitous IoT networks is that collecting, curating, and maintaining a high-quality dataset takes considerable time, effort, and expense. It is difficult to train an efficient and practical AI model using only one data owner's data.

Recently, federated learning (FL), as an emerging decentralized AI framework, is proposed to address the above challenges by training a shared model in several participating devices [7]. FL enables extracting traffic features without moving user data out of where they reside. Instead, the distributed data collection and storage system reduces the costs of daily maintenance. Many studies have shown that models trained by FL can achieve a performance level equivalent to ones trained by centralized approaches [8–10]. Thus, FL holds significant potential for enabling traffic prediction in 6G ubiquitous IoT networks.

Nevertheless, FL also faces many critical challenges, including but not limited to data heterogeneity and training fairness. These challenges may lead to a situation where an optimal global model may not be suitable for a specific local participant. More recent research has begun to fill this gap from a transfer learning perspective [11, 12]. These approaches are generally proposed to improve target predictors' performance on target domains by transferring the knowledge contained in different but related domains. However, the difference between domains in 6G ubiquitous IoT systems is enormous. It is not possible to directly apply transfer learning technology in such a complicated environment.

In this article, we present a federated imitation learning framework to improve learning performance in ubiquitous IoT networks while guaranteeing security and user privacy. It adds a knowledge-sharing module to consult the parameters of well-trained models. Thus, the knowledge can be shared in different IoT domains via fusion. Then we delineate a decentralized scheduling approach. This approach allows global traffic scheduling across ubiquitous IoT domains that capitalize on matching theory. The distributed implementation of the traffic scheduling algorithm eliminates the need for a central entity.

Overall, the main contributions of this article can be summarized as follows:

1. Developing a knowledge-sharing module to imitate well-trained models' status in different domains, thereby realizing cross-domain knowledge sharing.

Digital Object Identifier:
10.1109/MNET.011.2100134

Ao Yu is with the Kuaishou Technology Co.;Qingkai Yang and Lihua Dou are with the Beijing Institute of Technology; Mohamed Cheriet is with the École de Technologie Supérieure.

0890-8044/21/$25.00 © 2021 IEEE

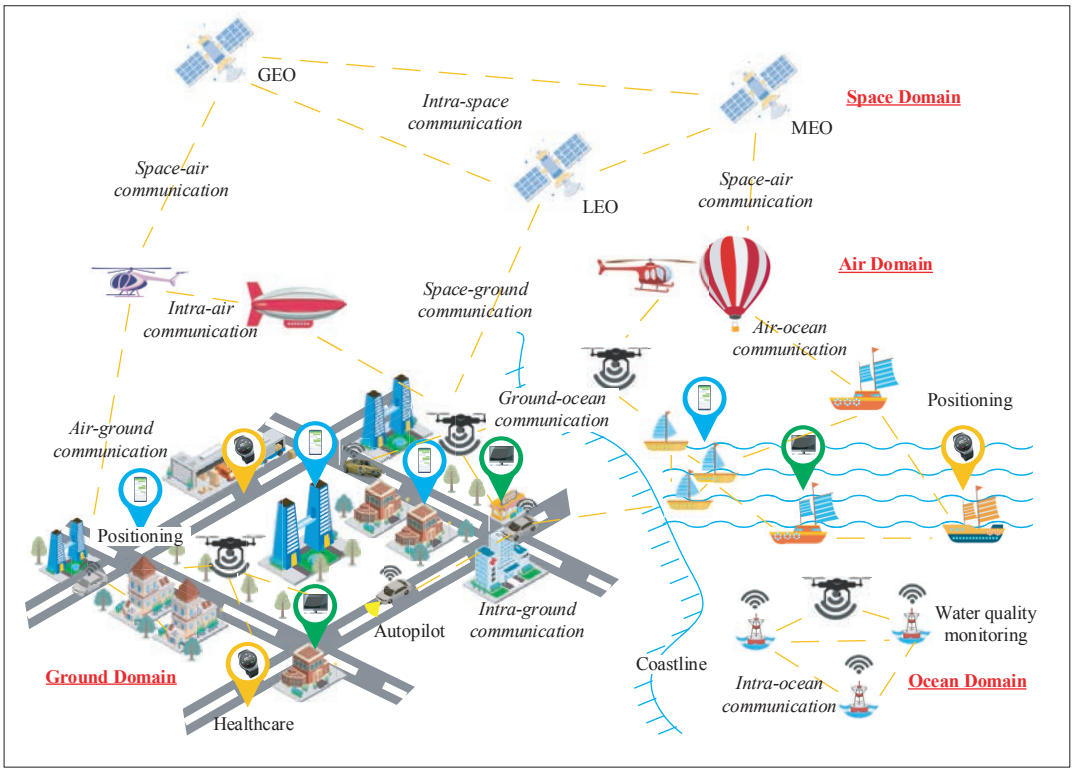

FIGURE 1. The ubiquitous IoT system architecture in the 6G era.

2. Elaborating a distributed scheduling approach based on matching theory, where the traffic can be scheduled via an IoT devices preference list.
3. We explore how federated imitation learning may provide a solution for future traffic scheduling in 6G ubiquitous IoT systems, and highlight the challenges and future directions.

The rest of this article is organized as follows. We first introduce the structure of ubiquitous IoT networks and present the motivations and challenges of FL deployment. Next, the knowledge-sharing framework is presented for cross-domain traffic prediction. We then propose a matching-based scheduling approach to allocate resources in a heterogeneous environment effectively. Simulation results are then shown. Further discussion of the future directions is provided. Finally, we conclude the article in the final section.

FL in Ubiquitous IoT Networks: Motivations and Challenges

This section introduces a novel paradigm for 6G ubiquitous IoT, and presents the motivations and core challenges of large-scale deployment of FL in 6G scenarios.

System Architecture

As depicted in Fig. 1, the ubiquitous IoT system comprises four main domains: space, air, ground, and ocean. These four domains can work as large-scale integrated networks or independent segments. This system allows traffic scheduling among peer IoT devices in an ad hoc manner. For example, in Fig. 2, space and air nodes only need to update the parameters of the global model with local datasets, and to send the training results to the cloud, which aggregates the global model. This training process is repeated until the performance of the local model can satisfy the customized needs of users. Furthermore, diverse connection methods, including interconnections and intraconnections, help deal with the heterogeneous IoT networks.

1. Space domain: A space network consists of several satellites and their supporting infrastructures, such as ground stations and operation control platforms. The satellites, according to their altitude, are indifferent orbits with different functions. At an altitude of 35,786 km, geostationary Earth orbit (GEO) has the broadest coverage and the most prolonged transmission delay. Medium Earth orbit (MEO) appears at an altitude of 3000 km to provide navigation services (e.g., American's GPS and China's Beidou). Low Earth orbit (LEO) has the lowest orbit, only 200–3000 km. The LEO constellations could provide detection and communication services with less delay, but require complicated ground control systems. By integrating different satellites into the system, different orbits' advantages will make up for each other's shortcomings and provide ubiquitous coverage services.
2. Air domain: In the air segment, high and low altitude platforms (HAPs and LAPs) are usually used to complement the ground network. At an altitude of 0.3–30 km, HAPs and LAPs mainly consist of several aircraft, such as unmanned aerial vehicles (UAVs), helicopters, and balloons. The flying aircraft can provide edge caching and task offloading services for ground or ocean users. In this work, the UAVs are employed as the cloud parameter servers. Compared to ground nodes, air infrastructures have broad coverage, low cost, and flexible movement.

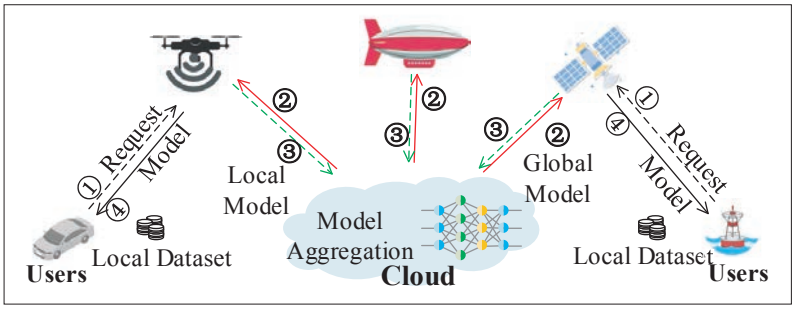

FIGURE 2. An example scenario of a federated learning framework for a 6G ubiquitous IoT system. ①: Users send their request to nodes in air or space domain; ②: cloud delivers the global model to the selected air or space nodes; ③: air or space nodes iteratively train the global model with a local dataset and send back a local model for aggregation. Repeat ②③; then the trained model is delivered to users.

3. Ground domain: For the ground network, the cellular network is now evolving to 6G networks to support heterogeneous IoT services, including indoor positioning, vehicular communications, and health monitoring. The services provided by IoT devices would generate traffic to computing and scheduling. The ground network can provide high-speed data transmission. However, the coverage of ground infrastructures in remote and rural areas is inadequate, and IoT devices usually have limited energy and computing capabilities.
4. Ocean domain: The ocean communication networks would be integrated into the ubiquitous IoT system in the future. Ships near the coastline can directly access the ground networks. For ships that go farther from the coast, aircraft and satellites can provide global Internet access. Nevertheless, accessing from space and air usually has high latency and limited data rate. Moreover, UAV-assisted buoy relay is also used in water quality monitoring and marine creature protection.

In conclusion, the ubiquitous IoT system is a complex integrated network that coordinates among space, air, ground, and ocean segments. It has the largest-ever coverage scale, and helps to manage and coordinate heterogeneous IoT devices. Managing a system at this scale requires the assistance of AI techniques. AI-based approaches can precisely extract and learn high-level traffic features such as burst traffic in hotspot areas and hybrid traffic in cross-domain areas. Meanwhile, AI takes much less time than humans to make decisions.

Motivations and Challenges

From a service perspective, traffic scheduling in heterogeneous IoT networks should be implemented in different domains in a data-sharing manner. Unfortunately, user datasets are not always available because sharing user data poses technical challenges related to privacy protection and legal issues.

FL addresses this challenge by training a shared global model with several decentralized participants. In an FL setting, the private source data does not need to be retrieved from the database, and the training process is realized only by updating the model parameters and gradients. Specifically, local models send the gradient to cloud parameter servers. After aggregation, the learning task is performed, an the updated model parameters and gradients are sent back to local models with service requests.

Moreover, to gain knowledge from the well-trained model, federated transfer learning is proposed to improve learners' performance on target domains. Through the FL paradigm and knowledge transfer, federated transfer learning can build personalized models by collating data from different participants without leaking privacy data.

Up to now, lots of efforts have been made to use federated transfer learning to learn cross-domain knowledge. However, in a heterogeneous IoT system, the difference between domains might be enormous. In this case, the data are collected from completely different domains (e.g., air to ground) with various sensors (e.g., UAV-based or vehicle-based). It is hard to adopt the transfer learning approach directly. Therefore, in this article, a knowledge-sharing module is designed to imitate the knowledge shared by models from other domains.

Knowledge-Sharing Framework

This section introduces the details of the proposed knowledge-sharing framework, including a federated imitation learning architecture and a knowledge-sharing module.

Federated Imitation Learning Architecture

The framework of federated imitation learning is performed in ubiquitous IoT networks. There are local participants, cloud parameter servers, and local datasets. Local participants need to learn knowledge from local datasets, and the cloud parameter servers share well-trained knowledge collected from other domains. Inspired by the Fuzzy theory [13], the knowledge-sharing module can transfer parameters to cloud parameter servers, which contain necessary heterogeneous local traffic features. The details of the knowledge-sharing module are illustrated in the next subsection.

Different from transfer learning, the knowledge-sharing module can fuse heterogeneous knowledge in several different domains, imitating the uncertainty concept judgment and reasoning thinking mode of the human brain. Weights of knowledge-sharing modules are computed using fuzzy logic dealing with various parameters. It senses the load and data concentration, and adjusts the proportion of different model parameters accordingly.

In addition to using local datasets for training, it can also perform knowledge-sharing to obtain well-trained parameters from cloud parameter servers with service requests. As illustrated in Fig. 3, the overall framework of federated imitation learning is explained.

In the proposed framework, the main goal is to predict traffic in target areas and learn to model high-level heterogeneous traffic features, and capture commonalities from the local time-series datasets. Thus, we adopt variational long short-term memory (LSTM) as our baseline model, which has forward and backward hidden layers to learn the temporally contextual information and can be trained by a backpropagation through time (BPTT) algorithm. Federated imitation learn-

ing can be performed either online or offline. Note that knowledge-sharing and model training are simultaneous, while federated imitation learning is performed online.

Knowledge-Sharing Module

To fuse heterogeneous knowledge in different domains, a knowledge-sharing module is incorporated into the framework. Inspired by the Fuzzy theory, the knowledge-sharing module offers the local model the ability to build cognitive connections among different domains. Specifically, it can form the probability distributions of different features and map them to high or low scores. Referring to the probability distributions, the knowledge-sharing module can reduce the uncertainties. Moreover, to capture the commonalities of cross-domain features, the knowledge-sharing module modifies the local features' probabilities referring to the global sharing parameters.

In the local model, we use front layers as feature extractors to learn the local datasets. The knowledge-sharing module is a feed-forward layer behind the front layers. Thus, the knowledge-sharing module states can be calculated depending on the current output state of the front layer and the global sharing parameters from cloud parameter servers. This structure enables IoT devices to learn a global shared model while keeping the local datasets inside the devices. Furthermore, it is not necessary to upload raw datasets to the cloud servers. Only the model parameters and gradients are shared in the cloud parameter servers.

Note that the global sharing parameters in the cloud are only used as a guide for local models. The global sharing parameters in cloud servers are updated with a cautious strategy, which means it will not make serious mistakes. Still, these parameters might not be optimal for each local model. Therefore, every local model must train its knowledge-sharing module based on the global sharing parameters received from the cloud.

Overall, the knowledge-sharing module can speed up the local training and increase the cross-domain traffic prediction accuracy. In the learning of local models, the local parameters and global sharing parameters are trained. In some cases, it can adjust the proportion of local parameters and global sharing parameters in the process of backpropagation. For instance, the local feature extraction might be frozen, and only the knowledge-sharing module is trained.

Matching-Theory-Based Decentralized Scheduling Approach

In this section, a decentralized traffic scheduling approach is proposed for ubiquitous IoT systems in which the preference list and distributed matching algorithm are presented.

Preference List

In 6G ubiquitous IoT systems, tasks prefer to be assigned to the devices that best minimize the processing cost and enjoy the available resources considering IoT devices' limited energy and computing capability. With that objective, the preference list of each device is proposed as a reference for node selection.

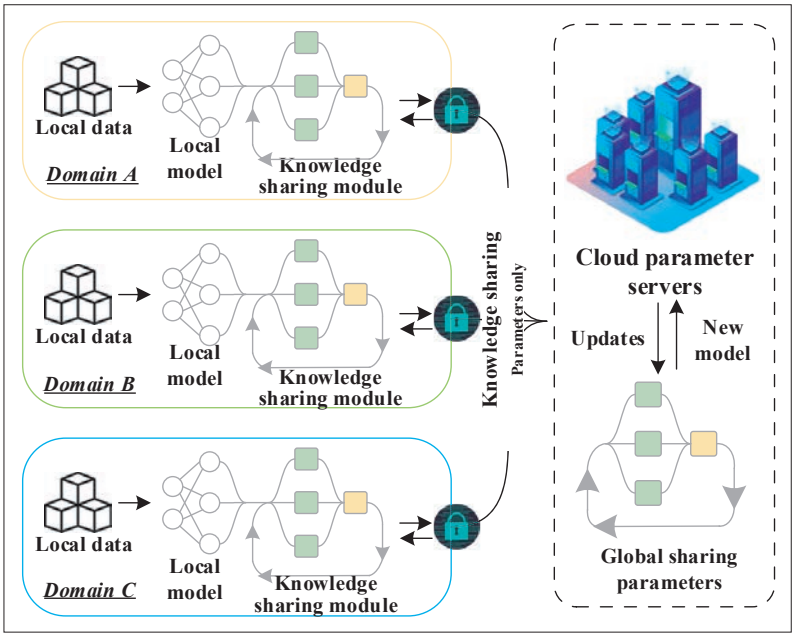

FIGURE 3. Schematic of the federated imitation learning framework.

After receiving the traffic prediction results from the federated imitation learning framework, the algorithm first visits the devices on which the predicted traffic can be scheduled. The selection of destination devices is based on three factors: the prediction errors, the remaining resources, and the transmission delay. The prediction error quantifies the deviations of the actual traffic arrival time from the predicted results. The resources in IoT networks include application resources (i.e., CPU and memory) and transport resources (i.e., bandwidths and hop of each candidate path). The transmission delay is used to find devices as close as possible to provide on-demand services.

Then the algorithm compares the three factors of these alternative devices. If the device on top of the list has enough resources to serve the task, it is recorded on the list. Otherwise, this device is removed from the list, and the next device is visited.

Distributed Matching Algorithm

The distributed matching algorithm adopts matching theory, a mathematical framework in economics, to make intelligent scheduling decisions. The traffic scheduling problem is formulated as a one-to-many device matching problem. Our solution aims to find an optimal matching pair between devices to carry the predicted tasks and maximize resource allocation efficiency on IoT systems.

During resource allocation, each device is permitted to collect the devices they are interested in according to the preference list. The devices do not need to know the preferences of other devices. Instead, the devices only make decisions based on the local data they have collected. Thus, a matching -theory-based approach can be implemented in a distributed manner without a centralized controller. This approach's effectiveness and correctness have been proved by some recent research [14, 15].

For the matching algorithm, the detailed steps are listed as follows:

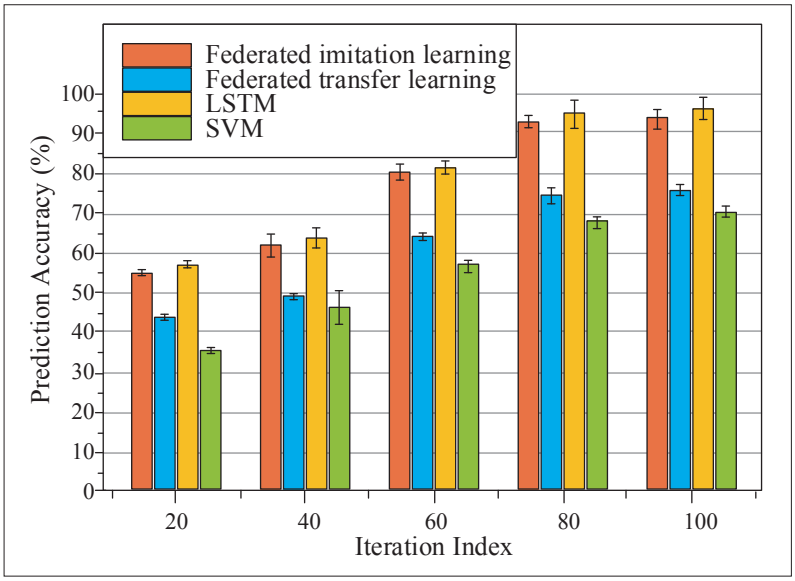

FIGURE 4. Comparison between the prediction accuracy of the proposed federated imitation learning and that of the federated transfer learning, LSTM, and SVM.

Step 1: The algorithm loops through the preference list and then selects the most preferred destination devices.

Step 2: Then the algorithm contacts the device by sending it a message and waits for the response.

Step 3: If the device's answer is No, place the device at the end of the preference list, and the algorithm moves to check the next device on the list.

Step 4: Otherwise, if the device accepts to host the tasks, the loop breaks, and the matching between the source and destination devices is successful.

Note that the whole algorithm is repeated after a certain period before the update of the preference lists.

A Case Study

This section presents a case study to illustrate the benefits of the proposed federated imitation learning framework and matching-theory-based scheduling approach.

Experimental Setup

Considering the ubiquitous IoT network's largest ever geographical scale, in this article, a simplified network structure is constructed as the considered topology. This topology consists of 2 GEOs, 8 MEOs, 32 LEOs, 600 UAVs, 10,000 ground nodes, and 2000 ocean nodes. The routing design of each domain follows different policies. The air and ground links have the largest bandwidth and lower delay, while space and ocean links have higher delay but lower bandwidth. Traffic is transported from one source device to one or many destination devices independent and identically distributed (i.i.d.). They employ the UAVs as the cloud parameter servers, while the ground and ocean nodes are the devices with local datasets. The values of the main parameters in the considered topology are given in Table 1. This article simulates the experiments in Tensorflow (Python 2.7/3.5). A multi-core workstation with 16 2.10 GHz Intel Xeon® CPU E5-2620 v4 cores, 2 NVIDIA TITAN XP GPU cores, and 64 GB RAM is deployed to accelerate the learning process.

Parameters	Values
Data arrival rate (Mb/s)	Random in [2, 10]
Simulation time (min)	120
Simulation area (km^2)	10 × 10
UAV coverage	100 nodes or 1 km^2
UAV propulsion power (W)	100
Computation capacity (GHz)	Uniform in [1.8, 2.4]
CPU cycles	8
Satellite users	Random in [100, 500]
Carrier frequency (GHz)	2.4
Bandwidth of channel (kHz)	128 ×15 kHz
Single-hop delay (ms)	Uniform in [10, 80]

TABLE 1. Simulation setup.

For the local datasets, the packet header information was collected every 5 min from three university data centers deployed in Beijing in January 2021. All the datasets were temporally coded, randomly sampled, and divided into training, validation, and test datasets at a ratio of 6:3:1. The local dataset is a collection of input-output pairs. The input is a column input vector including timestamp, arrival time, processing time, source and destination ports, and IP addresses of source and destination. The output is the traffic arrival time. As for the federated imitation learning structure, we set the mini-batch size to 120 and the initial learning rate to 0.005. LSTM consists of 5 input layer units, 6 hidden layers, and 1024 hidden units in each local model. The proposed knowledge-sharing module contains a feed-forward layer with 512 hidden units. The prediction accuracy was calculated by the root mean square error (RMSE), and the prediction window size is 12.

Result Analysis

As depicted in Fig. 4, the performance of the proposed federated imitation learning model with that of federated transfer learning, LSTM, and support vector machine (SVM) was compared with an identical simulation configuration. Among these comparison algorithms, federated imitation learning and federated transfer learning are federated models. Besides that, LSTM and SVM are popular traffic prediction models. In all experiments, we adopted the same datasets. The prediction task was 5 min ahead of traffic prediction. From the results, the prediction accuracy of federated imitation learning is higher than those of federated transfer learning and SVM but very close to that of LSTM. This is because the core technique of federated imitation learning to prediction is the LSTM structure. Furthermore, FL can protect data privacy by keeping the training dataset locally. That the federated imitation learning model performs better than federated transfer learning is within our expectations because the transfer learning technology cannot perform well in a large-scale heterogeneous environment.

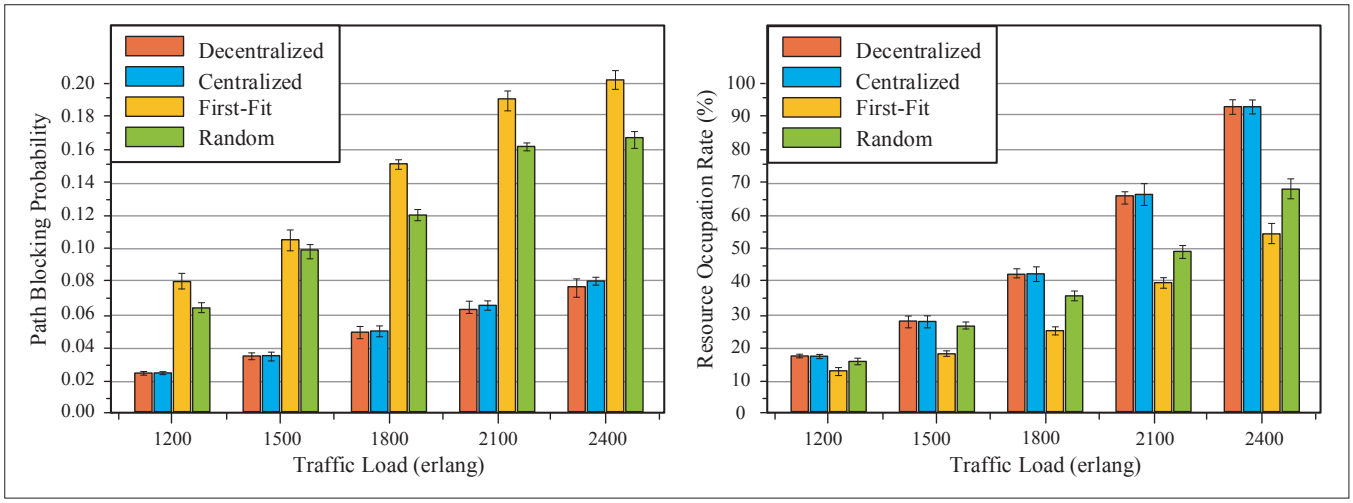

FIGURE 5. a), b): Path-blocking probability and resource occupation rates of decentralized, centralized, first-fit, and random traffic scheduling algorithms.

Figures 5a and 5b compare the path-blocking probability and resource occupation rate, respectively, with the traffic load for decentralized, centralized, first-fit, and random scheduling algorithms. The centralized algorithm is the same as the decentralized algorithm but needs a centralized controller. The path-blocking probability values for the decentralized algorithm and the centralized algorithm were smaller than the first-fit and random algorithms when the traffic load is low. The path-blocking probability values of the first-fit and random algorithms were unacceptable when traffic was dense. It also illustrates that our distributed algorithm outperforms the first-fit and random algorithms in resource occupation rate. The distributed algorithm also performs slightly better than the centralized algorithm when the traffic load becomes large. Because the distributed algorithm does not need a controller to determine the resource allocation, the decision process is quick. To this end, we can conclude that our solution achieves satisfying performance in large-scale heterogeneous IoT networks.

Future Directions

Based on the proposed framework, possible research directions can be conducted in the following aspects.

Learning Algorithm Design: The 6G IoT system is a ubiquitous network. There are so many devices with different functions that thus generate enormous heterogeneous traffic types. This makes it hard for an engineer to choose a suitable learning model. Moreover, the neural network architecture is deeply concerned with the targeted issues, which are usually not scalable. Furthermore, considering the multi-dimensional input data, the problem of how to design an effective and scalable learning architecture remains unsolved.

Framework Deployment: When we try to deploy the ubiquitous IoT system, the transmission delay is a serious problem. For instance, the ultra-large network scale makes it tough to access remote nodes (e.g., GEO or cross-ocean devices). Moreover, the computation cost required for each parameter update exceeds IoT devices' capacity because the distributed approach often means increased communication cost.

Multi-Dimensional Resources Integration: The wide-area network coverage of IoT and massive device connections enriches the total amount of network resources. It adds new resource forms, forming a network where wireless, spectrum, processing, storage, and other multi-level heterogeneous resources coexist. Resources at different levels in the network have different forms, and even the deployment of some resources is isolated from each other. Most of the existing resource scheduling strategies are designed in the same dimension and cannot be applied to new scenarios with multiple layers of complex resources. Therefore, achieving flexible resource scheduling and coordination among multi-layer resource scenarios has become a challenge faced by the current industrial Internet.

Network Centralized Control: Different communication protocols such as industrial communication protocols, general protocols, and wireless protocols have different regulatory processing requirements. Existing networks can only implement service control for a single access protocol, resulting in the isolation of diverse control functions in the same scenario, making it challenging to achieve efficient control integration. In the network, the function configuration is rigid, and the operation is complicated. It is challenging to complete open and unified control and function integration of multiple systems. Therefore, achieving effective control integration for heterogeneous systems has become an urgent challenge in IoT.

Conclusion

This work has proposed a cross-domain knowledge-sharing framework for efficient traffic scheduling in 6G ubiquitous IoT networks. The main components of our solution are:

1. The federated imitation learning model with a novel knowledge-sharing module to fuse the heterogeneous traffic features
2. The matching theory-based scheduling algorithm that helps schedule traffic to the appropriate devices with an IoT device preference list

By integrated the federated learning model into a distributed algorithm, the cross-domain knowledge-sharing framework can effectively allocate

the heterogeneous IoT resources without compromising user privacy.

References

[1] S. Dang *et al.*, "What Should 6G Be?," *Nature Electronics*, vol. 3, no. 1, Jan. 2020, pp. 20–29.
[2] G. Wang *et al.*, "SFC-Based Service Provisioning for Reconfigurable Space-Air-Ground Integrated Networks," *IEEE JSAC*, vol. 38, no. 7, 2020, pp. 1478–89.
[3] T. Yang, J. Chen, and N. Zhang, "AI-Empowered Maritime Internet of Things: A Parallel-Network-Driven Approach," *IEEE Network*, vol.34, no. 5, Sept./Oct. 2020, pp. 54–59.
[4] D. Kwon *et al.*, "Multiagent DDPG-Based Deep Learning for Smart Ocean Federated Learning IoT Networks," *IEEE IoT J.*, vol. 7, no. 10, 2020, pp. 9895–9903.
[5] M. Al-Garadi *et al.*, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," *IEEE Commun. Surveys & Tutorials*, vol. 22, no. 3, 2020, pp. 1646–85.
[6] C. Pradhan *et al.*, "Computation Offloading for IoT in C-RAN: Optimization and Deep Learning," *IEEE Trans. Commun.*, vol. 68, no. 7, 2020, pp. 4565–79.
[7] Y. Zhan *et al.*, "A Learning-Based Incentive Mechanism for Federated Learning," *IEEE IoT J.*, vol. 7, no. 7, 2020, pp. 6360–68.
[8] S. Rahman *et al.*, "Internet of Things intrusion Detection: Centralized, On-Device, or Federated Learning?," *IEEE Network*, vol. 34, no. 6, Nov./Dec. 2020, pp. 310–17.
[9] L. Khan *et al.*, "Federated Learning for Edge Networks: Resource Optimization and Incentive Mechanism," *IEEE Commun. Mag.*, vol. 58, no. 10, Oct. 2020, pp. 88–93.
[10] S. Zhang *et al.*, "Air-Ground Integrated Vehicular Network Slicing with Content Pushing and Caching," *IEEE JSAC*, vol. 36, no. 9, 2018, pp. 2114–27.
[11] H. Lin *et al.*, "Towards Secure Data Fusion in Industrial IoT Using Transfer Learning," *IEEE Trans. Industr. Inform.*, vol. 17, no. 10, 2021, pp. 7114–22.
[12] Y. Fan *et al.*, "IoTDefender: A Federated Transfer Learning Intrusion Detection Framework for 5G IoT," *Proc. IEEE 14th Int'l. Conf. Big Data Science and Engineering*, 2020, pp. 88–95.
[13] T. Hößler *et al.*, "Stable Matching for Wireless URLLC in Multi-Cellular, Multi-User Systems," *IEEE Trans. Commun.*, vol. 68, no. 8, 2020, pp. 5228–41.
[14] C. Su *et al.*, "UAV-Assisted Wireless Charging for Energy-Constrained IoT Devices Using Dynamic Matching," *IEEE IoT J.*, vol. 7, no. 6, 2020, pp. 4789–4800.
[15] R. Fantacci and B. Picano, "A Matching Game with Discard Policy for Virtual Machines Placement in Hybrid Cloud-Edge Architecture for Industrial IoT Systems," *IEEE Trans. Industr. Inform.*, vol. 16, no. 11, 2020, pp. 7046–55.

Biographies

Ao Yu (yuaobupt@gmail.com) received his Ph.D. degree in information and communication engineering from Beijing University of Posts and Telecommunications (BUPT), China, in 2021. From 2020 to 2021, he was a research intern in the Systems Engineering Department at the University of Quebec — École de technologie supérieure (ÉTS), Montreal, Canada. He is currently a research scientist at Kuaishou Technology Co., Ltd., Beijing, China. His main research interests include deep learning, IoT networks, optical and wireless networks, and AIOps.

Qingkai Yang (qingkai.yang@bit.edu.cn) received his first Ph.D. degree from Beijing Institute of Technology, China, and his second one from the University of Groningen, the Netherlands, in 2018. He is currently an associate professor with the School of Automation, Beijing Institute of Technology. His research interest is in cooperative control of multi-agent systems and autonomous agents.

Lihua Dou (doulihua@bit.edu.cn) received her B.S., M.S., and Ph.D. degrees in control theory and control engineering from Beijing Institute of Technology in 1979, 1987, and 2001, respectively. She is currently a professor of Control Science and Engineering with Beijing Institute of Technology. Her current research interests include command and control, pattern recognition, and ad hoc networks.

Mohamed Cheriet (mohamed.cheriet@etsmtl.ca) received his M.Sc. and Ph.D. degrees in computer science from the University of Pierre & Marie Curie (Paris VI) in 1985 and 1988, respectively. Since 1992, he has been a professor in the Systems Engineering Department at the University of Quebec — École de Technologie Supérieure (ÉTS), and was appointed as a full professor there in 1998. He is the founder and director of Synchromedia Laboratory for multimedia communication in telepresence applications. He is an expert in computational intelligence, pattern recognition, mathematical modeling for image processing, cognitive and machine learning approaches, and perception. In addition, he has extensive experience in cloud computing and network virtualization, and softwarization. He has published more than 450 technical papers in the field. He serves on the Editorial Boards of several renowned journals and international conferences. As Tier 1 Canada Research Chair on Sustainable and Smart Eco-Cloud, he leads the first smart-university campus in Canada, created as a hub for innovation and productivity at Montreal. He is the General Director of the FRQNT Strategic Cluster on the operationalization of sustainability development, CIRODD (2019–2026). He is a 2016 Fellow of the International Association of Pattern Recognition (IAPR), a 2017 Fellow of the Canadian Academy of Engineering (CAE), a 2018 Fellow of the Engineering Institute of Canada (EIC), and a 2019 Fellow of Engineers Canada (EC).