Edge Intelligence and Blockchain Empowered 5G Beyond for the Industrial Internet of Things

Ke Zhang, Yongxu Zhu, Sabita Maharjan, and Yan Zhang

Abstract

Edge intelligence is a key enabler for IIoT as it offers smart cloud services in close proximity to the production environment with low latency and less cost. The need for ubiquitous communication, computing, and caching resources in 5G beyond will lead to a growing demand to integrate heterogeneous resources into the edge network. Furthermore, distributed edge services can make resource transactions vulnerable to malicious nodes. Ensuring secure edge services under complex industrial networks is a big challenge. In this article, we present an edge intelligence and blockchain empowered IIoT framework, which achieves flexible and secure edge service management. Then we propose a cross-domain sharing inspired edge resource scheduling scheme and design a credit-differentiated edge transaction approval mechanism. Numerical results indicate that the proposed schemes bring significant improvement in both edge service cost and service capacities.

Introduction

The advancement of the Internet of Things (IoT) has radically changed the way factories and workplaces function, by connecting machines, people, and environments to form industrial networks while providing a great platform to develop novel applications [1]. With intensive resource requirements and strict constraints on service quality, the emerging smart industrial applications impose critical challenges on resource-constrained industrial equipment [2].

Providing mobile edge computing and edge caching capabilities together with artificial intelligence (AI) in the proximity of end users, the concept of edge intelligence has been introduced as a new paradigm to address the above challenges [3]. In edge intelligence empowered networks, edge resources are managed by AI systems for offering powerful computational processing and massive data acquisition locally at edge networks [4]. AI helps to obtain efficient resource scheduling strategies in a complex environment with heterogeneous resources and a large number of devices, while meeting the strict delay constraints and other performance requirements of industrial applications.

With the rise of beyond fifth generation (5G) techniques, terahertz communication with parallel transmission and dense spatial multiplexing pose critical challenges on constrained spectrum resources. Highly intelligent and efficient spectrum sharing is the key to the design of edge schemes. In addition, in the beyond 5G era, ubiquitous always-on connectivity for network service and applications facilitates cooperation and complementarity of various types of resources, such as computing power, caching space, and wireless spectrum, between adjacent edge networks [5]. However, mutual effects among geographically distributed heterogeneous resources make service scheduling difficult. Moreover, diverse application service demands and time-varying resource states make edge system design more complicated.

As the Industrial IoT (IIoT) paradigm significantly expands its reach, numerous connecting devices, such as the nodes recording edge service transaction data, may become vulnerable to cyber security attacks [6]. A cyber security attack is any type of offensive action that uses various methods to steal, alter, or destroy smart devices, information infrastructures, and communication networks. As these records are the key enablers for implementing edge services for industrial manufacturing and trade, it is of utmost importance to keep such data safe and to protect data privacy and integrity. Blockchain, a tamper-resistant distributed ledger of blocks storing and sharing data in a secure and consensual manner, has been introduced to tackle this challenge [7]. However, as IIoT networks consist of diverse edge services and a large number of distributed nodes, how to achieve edge resource transaction consensus in an efficient and distributed approach is still an open issue.

In this article, we propose an edge intelligence and blockchain empowered 5G beyond IIoT network for incorporating and scheduling distributed heterogeneous edge resources for industrial applications in an efficient and secure manner. We develop a cross-domain sharing enabled optimal edge resource scheduling scheme to minimize the operating cost of the edge nodes while improving service capacity. In the blockchain empowered IIoT network, to efficiently reach edge resource transaction consensus, we design a new credit-differentiated transaction approval mechanism for distributed edge nodes.

The rest of this article is organized as follows. We first present the proposed edge intelligent

Digital Object Identifier:
10.1109/MNET.001.1800526

Ke Zhang is with the University of Electronic Science and Technology of China; Yongxu Zhu is with Loughborough University; Sabita Maharjan is with Simula Metropolitan Center for Digital Engineering and University of Oslo; Yan Zhang (corresponding author) is with University of Oslo.

 0890-8044/19/$25.00 © 2019 IEEE

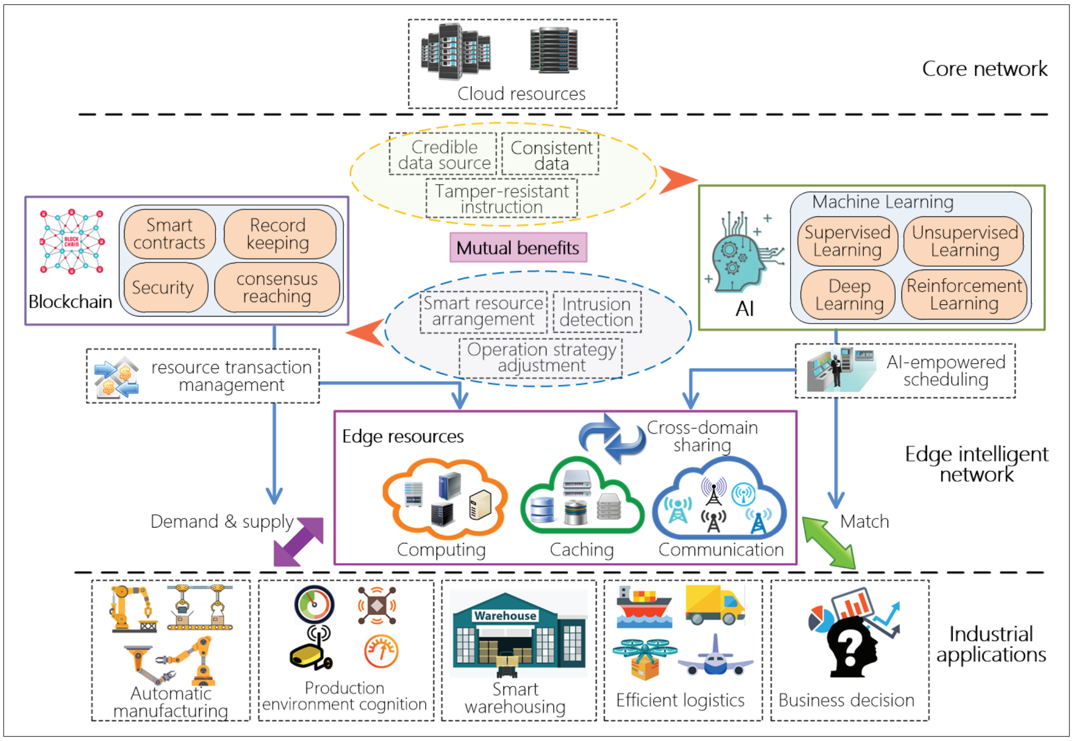

FIGURE 1. Framework of intelligent and secure edge network for 5G beyond IIoT.

and secure IIoT network. In the following section, we design a cross-domain sharing enabled edge resource scheduling scheme. Next, we develop a credit-differentiated transaction approval mechanism. Then we evaluate the performance of our proposed schemes through numerical results. Conclusions and future work are presented in the final section.

Edge Intelligence and Blockchain Empowered 5G Beyond IIoT Networks

Figure 1 shows the framework of our proposed intelligent and secure 5G beyond IIoT networks, which leverages edge intelligence and blockchain in edge service scheduling and resource transaction management. The framework consists of three planes. The industrial application plane, which is at the bottom of the framework, illustrates typical applications with intensive edge resource requirements. With the aid of edge resources distributively deployed in close proximity to the production site, warehouse, logistics road, and manager office, these applications can be executed such that their performance requirements can be met. In order to efficiently schedule heterogeneous edge resources while offering a secure and trustworthy digital platform for edge service transactions, we deploy blockchain and AI modules in the edge intelligent network plane. The core network plane located at the top of the framework is a fundamental part of the IIoT network, seamlessly integrating IIoT and remote cloud. This plane consists of high-performance computing servers and large-capacity storage space. When edge resources are not adequate for serving the industrial applications, the servers in the core network can provide auxiliary service, especially for delay-tolerant applications.

Edge Intelligence for 5G Beyond IIoT

By integrating environment cognition, data analytics, machine-to-machine communication, and robotic automation, IIoT holds great potential to enhance manufacturing efficiency and to enable powerful industrial applications [8]. These applications have intensive resource demands and low latency constraints. For instance, in automatic manufacturing, to make robotics operate efficiently, high-performance computing and communication resources are required for real-time sensory data processing and low-latency control signaling, respectively. In addition, the implementation of smart warehousing demands caching resource to store a large scale of warehousing information. It is a critical challenge to perform these powerful applications on resource constrained industrial devices.

In 5G beyond, both infrastructure and devices will be connected ubiquitously and reliably with the help of seamless communication coverage. This brings high agility in resource deployment and facilitates pushing service to the proximity of end subscribers. By offloading tasks directly to edge servers, the resource burden of the devices can be alleviated, while application processing latency is reduced.

To meet diverse resource demands and different performance requirements of the generated applications, edge resources need to be efficiently managed. Edge intelligence, which enables edge serving nodes with distributed AI capability, is a promising paradigm for resource scheduling. By integrating AI function into edge networks, edge intelligent servers have full insight of working environments in terms of the resource correlation between heterogeneous types and the feasibility of cooperation with adjacent nodes. In addition, accurate prediction of resource states and application demands can be obtained with the help of

AI algorithms in the edge, which contributes to improving resource scheduling efficiency. Moreover, as edge services typically utilize resources approximate to subscribers, edge resource scheduling does not need to know the information of the entire IIoT network. Transmitting locally learned serving information directly to distributed AI processing entities in such an edge intelligence approach is more efficient than obtaining resource scheduling strategies from remote central AI nodes. Thus, inspired by edge intelligence, diverse servers at the edge intelligent network plane can recognize serving context, understand industrial application demands, incorporate heterogeneous resources, and offer flexible communication, computing, and caching services in an efficient manner.

Blockchain for 5G Beyond IIoT

In edge intelligence empowered IIoT networks, resource-hungry industrial applications can be offloaded to or aided by edge servers for better performance and lower latency. In the serving process, some sensitive information, such as product parameters and business decisions, may be passed to the edge servers for processing. A protection mechanism is required to minimize the risk of sending data to fake or untrusted edge nodes [9]. Furthermore, during the service, resource transactions are performed between subscriber devices and edge service providers. In order to guarantee the authenticity and fairness of transactions, key information about the transaction, such as resource type, quantity, and price, must be recorded. In addition, applications always need to be accomplished with the aid of heterogeneous resources at multiple edge nodes. For instance, a computing task offloading first uses communication resources for file transfer and then utilizes computing resources for processing. Thus, there is a correlation between transactions in an edge service process. An efficient and automatic arrangement of consecutive edge resource transactions is therefore necessary.

As 5G beyond technique brings enhanced communication capacity as well as ubiquitous edge services, a large scale of diverse resource transactions can be performed all cross the networks. Traditional central control approaches are usually prone to high overhead and delay for transferring volumes of information across geography. Moreover, in edge intelligence empowered IIoT, the implementation of automatic edge service relies on a reliable and tamper-resistant transaction management mechanism. However, a central control node may be vulnerable to malicious attacks. Thus, designing efficient, flexible, and secure transaction management for 5G beyond IIoT emerges as a critical challenge.

To address the challenge while meeting the above requirements, we incorporate blockchain into the IIoT networks. Blockchain, which is a key technology in the 5G beyond era, acts as a tamper-resistant distributed ledger sharing and storing data among a large amount of nodes, and helps keep the security and privacy of the IIoT edge network ecosystem [10]. Specifically, the distributed ledger technology is of particular relevance to the distributed topology of IIoT networks, which can contribute to accelerating transactions and thus to reducing settlement time. In addition, through recording edge service transactions on a large amount of edge nodes, blockchain answers the challenge of single point of failure and data tampering. Moreover, there is no intermediary or third party participating in the edge serving process, and subscribers and service providers can transact and verify ledgers independently, which reduces cost and improves transaction flexibility. Besides transaction data, edge servers' availability, reliability, and credibility can also be recorded in blockchains. These records help subscribers find trustworthy edge servers. For implementing consecutive resource transactions in the blockchain-enabled task execution process, smart contract, which contains a set of agreed rules indicating the cooperation serving steps of edge nodes, can be utilized.

Edge Intelligent and Secure 5G Beyond IIoT Networks

Edge intelligence and blockchain both carry benefits to the IIoT network, and seamlessly integrating the two brings extra advantages. When paired with blockchains, AI of edge intelligence is able to operate securely and efficiently. In the process of AI empowered edge resource scheduling, a large amount of system information is used for strategy training. Aided by blockchain, the credibility of the information sources can be verified, which helps in preventing data forgery. Moreover, in distributing AI-enabled scheduling instructions to edge servers, tamper-resistant delivery can be achieved in a blockchain-based approach. As AI implementation always requires intensive computing and caching resources, the learning process may be divided and executed on multiple distributed edge nodes. Blockchain technology can ensure the consistency of the decomposed tasks and the pieces of learning data. Furthermore, in the decentralized IIoT network, economic incentives built on blockchains (e.g., bitcoin) can be utilized to motivate distributed edge nodes to participate in AI execution.

On the other side, due to its powerful analysis and prediction capabilities, AI makes blockchain operation scalable and efficient. Utilizing AI algorithms, characteristics of the edge nodes can be learned, and edge resources can be efficiently allocated to take transaction-proof works and to store blockchain data. In addition, based on accurate prediction of IIoT network state changes, the implementation strategies of blockchain on the edge nodes can be flexibly adjusted. Moreover, aided by AI technique, intrusion issues against blockchains can be detected, which further helps improve IIoT network security [11].

Edge Intelligence and Cross-Domain Sharing Enabled Resource Scheduling

Inspired by the edge intelligence of the proposed 5G beyond IIoT networks, in this section, we present a new resource scheduling scheme in a cross-domain sharing approach.

Cross-Domain Sharing of Edge Resources

5G beyond technique promises advantages in providing ubiquitous edge resources for industrial applications all over IIoT networks. However, due to the diversity and time-varying features of application demands as well as non-uniform distribution of edge serving capacities in spatio-temporal dimensions, resource arrangement that strictly and directly follows application demands in terms of resource types and amounts is inefficient and even impractical in certain resource-poor scenarios.

To address the problem, we design a new cross-domain edge resource sharing strategy. Here the cross-domain encompasses crossing between diverse resource types and different IIoT networks. Specifically, we leverage the AI module of the proposed 5G beyond IIoT network to learn the characteristics of application demands and edge resource states, and further exploit the mutual effects and complementary relationships between heterogeneous resources in different networks. By integrating these relations into the design of edge resource arrangement, possible service degradation due to the lack of certain resources can be made up by employing other resources in the current or adjacent networks so that the edge service demands can be met.

For instance, in a smart warehouse, a large amount of warehousing data needs to be stored in caching servers. Using computing resources for data compression, the size of data is reduced. Consequently, the strain on caching resources is alleviated through exploiting computing capabilities.

Another example is energy resources for computing or caching server functions. Since the operation of an edge server consumes energy, there is a strong correlation between energy supply and edge service capabilities. To some extent, energy can be taken as a special type of edge resource. Due to the constrained power quota for an industrial region and the limited capacity of remote grid transmission, it is impossible for an edge network to have unlimited power supply for a certain period of time. For an area without a sustainable energy source, utilizing communication resources to offload tasks to adjacent areas with sufficient power supply can cope with the fluctuation of power consumption.

Moreover, in intelligent logistic applications, an autonomous truck relies on roadside edge services to provide traffic information processing while obtaining real-time driving instructions along with its running. However, due to the non-uniform distribution of computing resources, the truck may not get stable edge services. With cross-domain sharing in place, more spectrum can be allocated to the network lacking computing resources so that the truck can obtain better communication capability, which helps offload tasks to more powerful computing servers in far networks. Thus, stable computing services can be obtained at the cost of communication resources.

Edge Resource Scheduling for 5G Beyond IIoT

Inspired by this cross-domain sharing strategy, we propose a smart edge resources scheduling scheme, which minimizes the edge service cost in an AI driven approach.

Figure 2 shows the proposed resource scheduling model for IIoT networks. There are N edge networks geographically distributed in an area. Each network is equipped with an edge computing server, a caching server, and a base station.

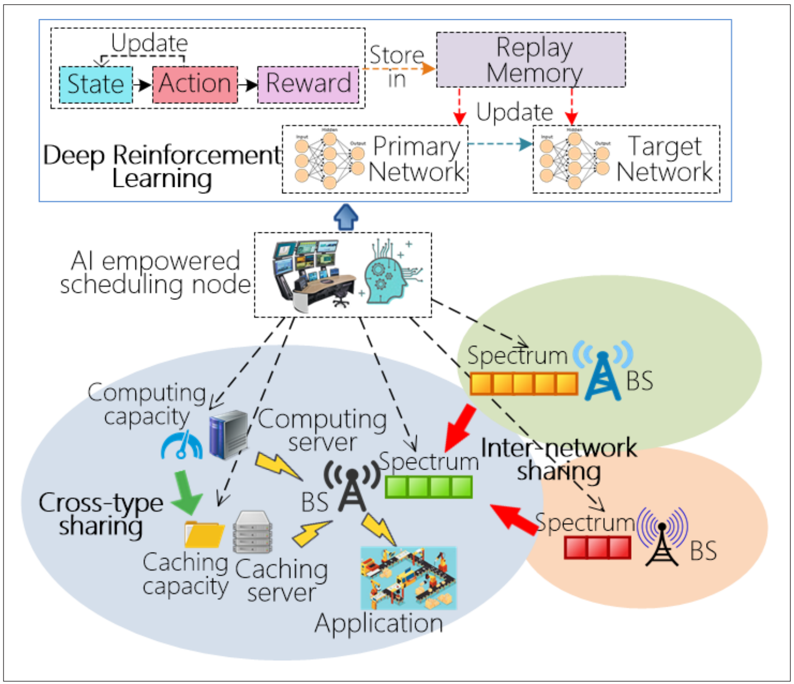

FIGURE 2. Cross-domain sharing empowered edge resource scheduling for 5G beyond IIoT networks.

The edge resources of network n are described in the form of a tuple: computing capacity C_n, caching space S_n, and the amount of spectrum B_n. An AI empowered resource scheduling node is responsible for managing these heterogeneous edge resources. The scheduling node gathers resource states and industrial application demands from servers and base stations, and then generates scheduling instructions. Both information and instructions are transmitted through wired or dedicated wireless control channels. In these networks, M types of industrial applications are generated and served with the edge resources. An application can either demand a computing task to be offloaded to an edge computing server or obtain information from a caching server. A type of application is identified with three components and can be presented as $\{c_m, s_m, t_m^{\max}\}$, where c_m and s_m are the required computing and caching resources for processing and storing the task of application m, respectively. $t_m^{\max}$ is the time constraint, that is, the end-to-end time between task generation and completion.

With ultra-densely deployed communication infrastructures in 5G beyond networks, the spectrum becomes scarce, and multiplexing plays a vital role in spectrum management. In the proposed IIoT edge networks, we exploit the multiplexing relationship between the spectrum resources of adjacent networks. If the spectrum consumption of network n' is reduced by amount $\Delta b_{n,n'}$, the communication capacity of network n will increase by $f_{n,n'}$. Besides spectrum sharing among adjacent networks, local edge resource sharing across different types is also considered. In particular, we use $g_{m,n}$ to denote the reduction of type m application's caching demand caused by data size compression with the consumption of computing resources in network n.

In order to minimize the operating costs of the IIoT edge networks while meeting the service demands of industrial applications, the problem of optimal edge resource scheduling can be formulated as

$$\min U = \sum_{n \in \mathcal{N}} \sum_{m \in \mathcal{M}} X_{m,n}$$
$$\text{s.t.} \quad t_m \le t_m^{\max},$$
$$\sum_{m \in \mathcal{M}} (c_m + \Delta c_{m,n}) \le C_n$$
$$\sum_{m \in \mathcal{M}} (s_m - g_{m,n}) \le S_n$$
$$\sum_{m \in \mathcal{M}} b_m \le B_n + \sum_{n' \in \mathcal{N}} (f_{n,n'} - \Delta b_{n',n}) \quad (1)$$

where $X_{m,n}$ is the cost of resource consumption for network n serving application type m. The first constraint indicates that the execution time of an application task should be under its delay tolerance. The last three constraints ensure that the shared and allocated heterogeneous resources are within the available computing resources, storage capacities of a server, and the communication capacity of each base station, respectively. It is noteworthy that Eq. 1 can be extended to further take into account the security issue. For instance, a confidential task needs computing resources to encrypt the information, or it may need the edge cache to implement close-range data delivery, avoiding interception during long-distance transmission. Thus, security issues can be mapped to the demands for edge resources, which are reflected in both the objective function and constraints of the problem.

Deep Reinforcement Learning Approach for Optimal Resource Scheduling

In Eq. 1, the relation between $\Delta f_{m,n}$ and $\Delta b_{m,n}$ is nonlinear and complex. Furthermore, in large-scale IIoT networks, the competition between multiple users from different networks using constrained edge resources makes it challenging to solve the resource scheduling optimization problem. To derive the optimal cross-domain sharing empowered edge resource scheduling in Eq. 1, we turn to deep reinforcement learning (DRL) technology, which is an attractive approach to solve the complicated problem. In IIoT networks, an AI empowered resource scheduling node gathers industrial application demands and resource states, while running the DRL algorithm on an agent and drawing the optimal scheduling strategies. Three main elements of the DRL algorithm, namely state, action, and award, are described below.

State: The state consists of the service demands of diverse applications in different networks, and the available capacity of heterogeneous resources of each edge node.

Action: The action is defined as edge resource scheduling strategies, which allocate heterogeneous edge resources for various types of industrial applications generated in different networks.

Reward: As a reward function needs to be related to the objective of Eq. 1, we set the reward as the operating costs of the edge nodes. The learning aims to minimize this reward.

The DRL process operates in time steps. At each step, following the ε-greedy policy, the agent of the primary network exploits the currently learned best action with probability 1 – ε to maximize rewards greedily, or explores the environment to find better actions with probability ε. It maps current state to a selected action, receives a reward, and makes a state transition to the next state. The experience tuples of this agent, which consist of the current state, the selected action, reward, and next state, are stored in replay memory.

The target network can be taken as an old version of the primary network, and it updates its parameters according to those of the primary network at regular intervals. A batch of randomly selected experience data from the replay memory is used to calculate the difference between the action-values of primary and target networks. The parameters of the primary network are updated in a stochastic gradient approach. The learning process continues until convergence of the parameters is achieved.

Transaction Approval for Blockchain Empowered 5G Beyond IIoT

Following the optimal resource scheduling strategies obtained in the previous section, edge services are implemented, which bring resource transactions between edge servers and subscriber devices. In the proposed edge intelligent and secure IIoT networks, edge serving transactions can be safely recorded in blockchains. However, before records are written to blockchains, the network needs to achieve consensus. In this section, we focus on the consensus process, and present a new credit-differentiated transaction approval mechanism.

Edge Service Transaction Approval in 5G Beyond IIoT

To provide efficient and fair edge services, accurate and tamper-resistant resource transaction records are indeed required [12]. Although blockchain technology offers a promising paradigm to ensure secure and traceable transactions across different fields, its traditional transaction consensus acquisition approach, such as proof of work, cannot be applied directly into 5G beyond IIoT networks due to the following issues.

First, a massive number of edge nodes exist in the IIoT network, and some of them have limited computing capability, caching space, and power supply. They may not be able to execute highly intensive calculations to validate transactions and achieve consensus. In addition, to preserve privacy, the edge service nodes usually hide their real identity. It is difficult to prove the truth of edge service transactions without revealing nodes' identities. Furthermore, as execution of a consensus algorithm requires computation resources, being rational edge nodes, they lack the motivation to join in the approval mechanisms [13]. Thus, the path to transaction consensus under IIoT environments has emerged as a critical challenge.

To address this challenge, we utilize the idea of consortium blockchain, and choose the nodes with powerful computing and caching capabilities, such as edge computing servers, base stations, and smart grid aggregators, to undertake transaction verification [14]. For securing privacy of the edge nodes, an anonymous message forwarding approach is adopted in their interactions. Furthermore, we leverage a credit network approach to guarantee reliability of the anonymous announcements while incentivizing edge nodes to join the approval process [15]. Each approval node has a credit account, which reflects the reputation record of the node in the transaction approval process. By evaluating the accounts, whether a node is honest or malicious can easily be determined. Once consensus of a transaction ledger is reached, credit coin reward is paid to the approval nodes' accounts, which motivates the nodes to announce true transactions. However, the traditional credit-based transaction approval approach ignores the difference in nodes' awareness of transaction issues, which leads to an inefficient consensus achieving process.

Credit-Differentiated Transaction Approval Mechanism

Unlike previous credit-based works, we design a new credit-differentiated transaction approval mechanism that incorporates the difference of transaction confirmation degree among various nodes into the consensus acquisition process, and improves the accuracy and efficiency of transaction verification. Figure 3 shows the overview of the proposed mechanism.

As the nodes belong to various edge service types and are located in different areas, they may have diverse awareness of an edge service transaction. For instance, when a task is offloaded from an industrial application node to an edge computing server, a base station, which transmits the task files and computation results, can prove this computing service very definitely. Adjacent base stations that provide auxiliary information for the service may act as auxiliary witnesses. However, other wireless access points or edge servers unrelated to this service cannot recognize and approve this resource transaction.

In the light of the above observations, we bring different awareness of edge services into the transaction approval mechanism. Specifically, the amount of credit coins spent for a node issuing an announcement is proportional to the degree of its awareness about the edge resource transaction.

The main steps of the transaction approval mechanism are as follows. At first, the approval node with the largest number of credit coins initializes a transaction verification process, and posts the verification request. The other approval nodes that are aware of this transaction respond to the verification request and pay the awareness degree related credit coins for their approval announcements. Then the initiator node counts the credit coins attached to the received announcement. If coin number has reached a given threshold, a block recording this transaction is added to existing blockchains.

All the nodes participating in the approval process receive credit coin rewards, which are proportional to and higher than the coins they spent in the response process. To guard the credit accounts of the approval nodes from being tampered with, the accounts are also recorded in the blockchains.

The proposed transaction approval mechanism is expected to provide a guarantee of secure and reliable transactions among edge servers and subscribers. The main advantages of this design in terms of efficiency and security are as follows.

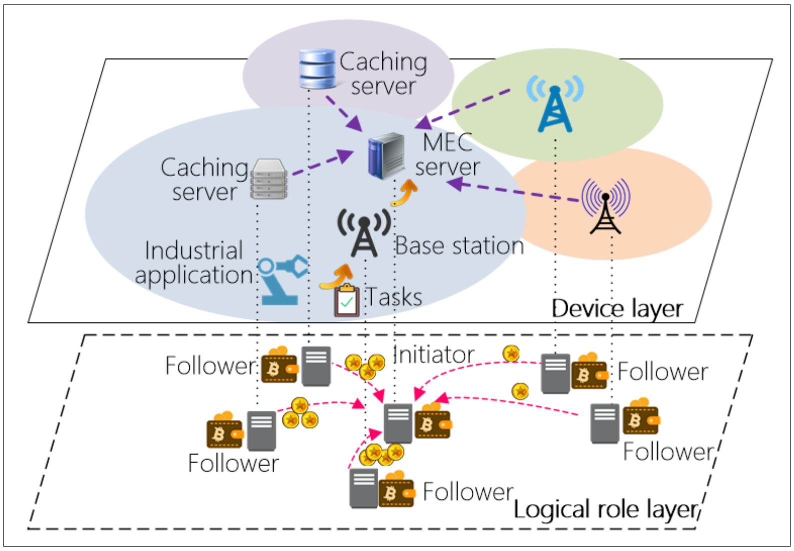

FIGURE 3. Credit-differentiated transaction approval mechanism.

Efficient and Privacy-Protected Approval Process: The approval reaches consensus based on the received credit coins attached to announcements, but not the number of participating edge nodes. An approval process can be implemented with a few highly credible nodes and low transmission overhead,which helps in improving the approval efficiency. In addition, the mechanism never needs to authenticate edge nodes' real identification, hence protecting their privacy.

Reliable and Tamper-Resistant Transaction Recording: Enabled by blockchain, the resource transactions are recorded and synchronized in a decentralized manner among a large number of IIoT edge nodes, which maintains the reliability and tamper resistance of the records simultaneously.

Incentive-Driven and Credit-Differentiated Announcement: Driven by the credit coin reward, edge nodes actively participate in the approval process. In addition, as the reward is related to the spent credit coins in the announcement, the nodes will dynamically adjust the amount of investment coins that reflects their confirmation degree of the transaction events.

Numerical Results

In this section, we evaluate the performance of the proposed DRL empowered optimal resource scheduling scheme. We consider five base stations. Each base station is equipped with a computing server and a caching server, whose computing and caching capacities are randomly taken from the range (15, 25) GHz and (1, 10) GB, respectively. Ten types of industrial application tasks are generated in this environment with delay constraints randomly distributed in (0.1, 2) s.

Figure 4 compares the service costs of the edge networks with different resource scheduling schemes. The scheme without any resource sharing has the highest cost. As this scheme allocates edge resources to applications strictly according to their requirements, it cannot obtain more flexible and economical scheduling solutions. In contrast, when implementing

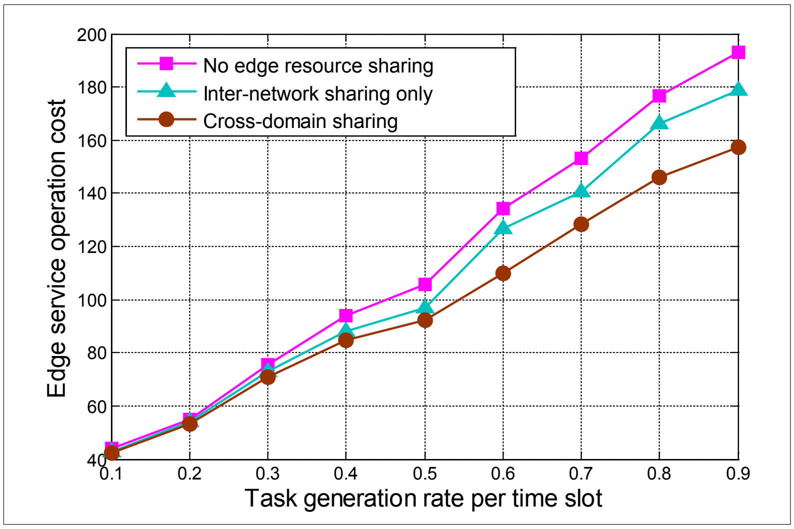

FIGURE 4. Edge service costs with different resource scheduling schemes.

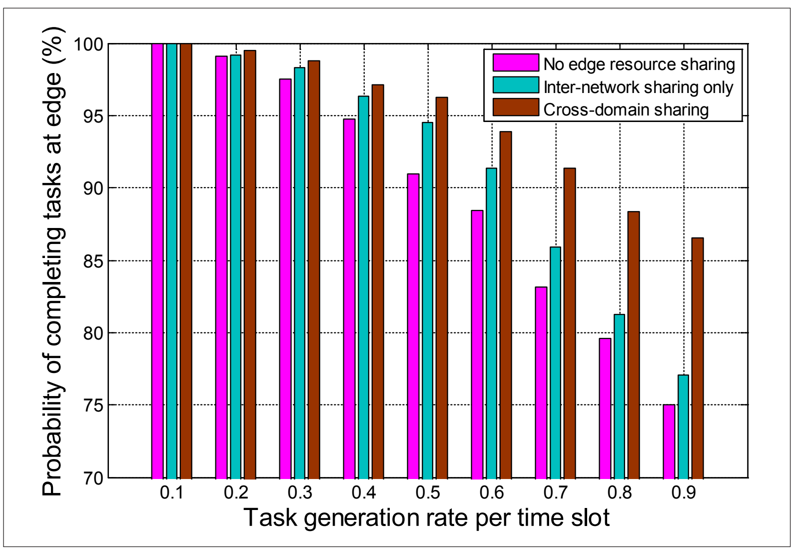

FIGURE 5. Probability of completing tasks at edge networks with different scheduling schemes.

an inter-network sharing scheme, aided by communication resource sharing between adjacent networks, an application node may obtain more bandwidth for better transmission quality to offload its task to edge servers in other networks with lower operating costs. Thus, the system service cost can be reduced. Furthermore, in our proposed cross-domain sharing scheme, besides the inter-network sharing of communication resources, the cross-domain sharing among computing and caching resources is incorporated into resource scheduling, which enables a flexible and cost-effective edge serving approach through heterogeneous resource complementarity, and further reduces the system cost.

Figure 5 presents the probability of tasks that can be completed at edge networks without the aid of cloud resource in core networks. It is clear that our proposed cross-domain sharing scheme yields the highest probability compared to other schemes, especially with high task generation rate. As the number of generated tasks increases, more resource demands are placed on edge servers. If the edge network cannot meet the demands, some of the tasks are offloaded to the remote cloud. In our proposed scheme, both inter-network and cross-domain sharing strategies help to address edge resource shortage at a local network or of a special type through flexible resource scheduling. In this way, the service capacity of the edge IIoT networks is improved. Thus, the probability of completing tasks at the edge under specified delay constraints can be enhanced significantly.

Conclusion and Future Work

In this article, we present an edge intelligent and secure 5G beyond framework for IIoT networks. By leveraging the newly proposed cross-domain sharing strategy and DRL technique, we develop an efficient edge resource scheduling scheme. To secure edge service transaction of the IIoT network, we design a new credit-differentiated transaction approval mechanism. Numerical results indicate that our proposed schemes greatly reduce the edge service costs and improve the service capacity.

Despite promising recent work in the area of edge intelligence empowered IIoT networks, there are still some fundamental questions that are largely unexplored. For instance, as learning is a process that evolves step by step using early knowledge for later understanding, a dynamically changing environment seriously impairs the learning performance. An efficient AI processing mechanism that copes with highly dynamic 5G beyond networks needs to be further investigated. Moreover, diverse blockchain technologies may exist in the networks, which may have different ledger types, contract rules, and consensus mechanisms. The way to interoperate and integrate them in securing edge transactions is also an interesting topic.

Acknowledgment

This research is partially supported by fundamental research funds for the central universities, China, under Grant No. 2672018ZYGX2018J001, the Xi'an Key Laboratory of Mobile Edge Computing and Security, under Grant No. 201805052-ZD3CG36, the key research and development plan of Shaanxi province, under Grant No. 2017ZDCXL-GY-05-01, the Science and Technology Program of Sichuan Province, under Grant No. 2019YFH0007, and the European Unions Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No. 824019,

References

[1] Z. Zhou *et al.*, "Energy-Efficient Industrial Internet of UAVs for Power Line Inspection in Smart Grid," *IEEE Trans. Industrial Informatics*, vol. 14, no. 6, Jan. 2018, pp. 2705–14.

[2] K. Wang *et al.*, "Green Industrial Internet of Things Architecture: An Energy-Efficient Perspective," *IEEE Commun. Mag.*, vol. 54, no. 12, Dec. 2016, pp. 48–54.

[3] M. Du *et al.*, "Differential Privacy Preserving of Training Model In Wireless Big Data With Edge Computing," *IEEE Trans. Big Data*, accepted.

[4] S. Bazrafkan and P. M. Corcoran, "Pushing the AI Envelope: Merging Deep Networks to Accelerate Edge Artificial Intelligence in Consumer Electronics Devices and Systems," *IEEE Consumer Electronics Mag.*, vol. 7, no. 2, Feb. 2018, pp. 55–61.

[5] Y. Zhu *et al.*, "Content Placement in Cache-Enabled Sub-6 Ghz and Millimeter-Wave Multi-Antenna Dense Small Cell Networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 5, Feb. 2018, pp. 2843–56.

[6] C. Xu, K. Wang and M. Guo, "Intelligent Resource Management in Blockchain Based Cloud Data Centers," *IEEE Cloud Computing*, vol. 4, no. 6, Nov. 2017, pp. 50–59.
[7] J. Kang *et al.*, "Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks," *IEEE Internet of Things*, vol. 6, no. 3, June 2019, pp. 4660–70.
[8] K. Wang *et al.*, "Green Energy Scheduling for Demand Side Management in the Smart Grid," *IEEE Trans. Green Commun. and Networking*, vol. 2, no. 2, Jan. 2018, pp. 596–611.
[9] C. Xu *et al.*, "Making Big Data Open in Edges: A Resource-Efficient Blockchain-Based Approach," *IEEE Trans. Parallel and Distributed Systems*, vol. 30, no. 4, Apr. 2019, pp. 870–82.
[10] H. Liu, Y. Zhang and T. Yang, "Blockchain Enabled Security in Electric Vehicles Cloud and Edge Computing," *IEEE Network*, vol. 32, no. 3, May/June 2018, pp. 78–83.
[11] M. Signorini *et al.*, "BAD: Blockchain Anomaly Detection," arXiv:1807.03833, July, 2018.
[12] J. Kang *et al.*, "Enabling Localized Peer-to-Peer Electricity Trading Among Plug-In Hybrid Electric Vehicles Using Consortium Blockchains," *IEEE Trans. Industrial Informatics*, vol. 13, no. 6, Dec. 2017, pp. 3154–64.
[13] Z. Zhou *et al.*, "Blockchain and Computational Intelligence Inspired Incentive-Compatible Demand Response in Internet of Electric Vehicles," *IEEE Trans. Emerging Topics in Computational Intelligence*, vol. 3, no. 3, June 2019, pp. 205–16.
[14] Z. Li *et al.*, "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things," *IEEE Trans. Industrial Informatics*, vol. 14, no. 8, Aug. 2018, pp. 3690–3700.
[15] A. Kate, "Introduction to Credit Networks: Security, Privacy, and Applications," *Proc. ACM SIGSAC Conf. Computer and Commun. Security*, Oct. 2016, pp. 1859–60.

Biographies

Ke Zhang (zhangke@uestc.edu.cn) received his Ph.D. degree from the University of Electronic Science and Technology of China in 2017. He is currently a lecturer in the School of Information and Communication Engineering, University of Electronic Science and Technology of China. His research interests include scheduling of mobile edge computing, design and optimization of next-generation wireless networks, and the Internet of Things.

Yongxu Zhu [S'16, M'19] (y.zhu4@lboro.ac.uk) received her M.S. degree from Beijing University of Posts and Telecommunications, China, and Dublin City University, Ireland, in 2012 and 2013, respectively, and her Ph.D. degree in electrical engineering from University College London, United Kingdom, in 2017. She is a research associate with Loughborough University, United Kingdom. Her research interests include UAV communications, wireless edge caching, millimeter-wave communications, heterogeneous cellular networks, and physical-layer security. She is currently a research associate at the Wolfson School of Mechanical, Electrical and Manufacturing Engineering, Loughborough University.

Sabita Maharjan [M'09] (sabita@simula.no) received her Ph.D. degree in networks and distributed systems from University of Oslo and Simula Research Laboratory, Norway, in 2013. She is currently a senior research scientist at the Simula Metropolitan Center for Digital Engineering, Norway, and an associate professor (adjunct position) at University of Oslo. Her current research interests include vehicular networks and 5G, network security and resilience, smart grid communications, the Internet of Things, machine-to-machine communication, software defined wireless networking, and advanced vehicle safety.

Yan Zhang [SM'10] (yanzhang@ieee.org) is a full professor in the Department of Informatics, University of Oslo. He is an Editor of several IEEE journals, including *IEEE Communications Magazine*, *IEEE Network*, *IEEE Transactions on Green Communications and Networking*, *IEEE Communications Surveys & Tutorials*, and *IEEE Internet of Things*. His current research interests include next generation wireless networks leading to 5G beyond and cyber physical systems. He is an IEEE VTS Distinguished Lecturer and a Fellow of IET. He received the 2018 "Highly Cited Researcher" (top 1 percent by citations) award from Clarivate Analytics.