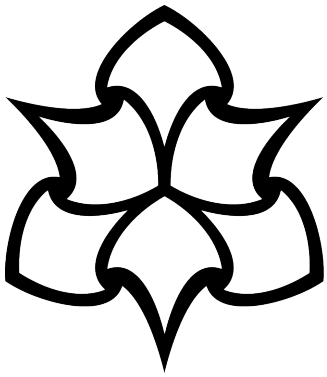

Manchester Metropolitan University

Li, J and Wu, J and Li, J and Bashir, AK and Piran, MJ and Anjum, A (2021) Blockchain-Based Trust Edge Knowledge Inference of Multi-Robot Systems for Collaborative Tasks. IEEE Communications Magazine, 59 (7). pp. 94-100. ISSN 0163-6804

Downloaded from: https://e-space.mmu.ac.uk/628376/

Version: Accepted Version

Publisher: IEEE

DOI: https://doi.org/10.1109/MCOM.001.2000419

Please cite the published version

https://e-space.mmu.ac.uk

Blockchain-based Trust Edge Knowledge Inference of Multi-robot Systems for Collaborative Tasks

Jianan Li, Jun Wu, Jianhua Li, Ali Kashif Bashir, Md. Jalil Piran, and Ashiq Anjum

***Abstract*—The collaborative inference helps robots to complete large tasks with mutual collaboration in edge-assisted multi-robot systems. It is challenging to provide the trusted edge collaborative inference in the presence of malicious nodes. In this article, we propose a blockchain-based collaborative edge knowledge inference (BCEI) framework for edge-assisted multi-robot systems. First, we formulate the inference process at the edge as the collaborative knowledge graph construction and sharing model. Second, to guarantee the trust of knowledge sharing, an efficient knowledge-based blockchain consensus method is presented. Finally, we conduct a case study on the emergency rescue application to evaluate the proposed framework. The experiment results demonstrate the efficiency of the proposed framework in terms of latency and accuracy.**

***Index Terms*—Multi-robot system; Blockchain; Edge inference; Knowledge graph.**

I. Introduction

MULTI-ROBOT systems require cooperation among a group of robots for complex tasks. Such coordination needs the cloud infrastructure, which provides sufficient computing resources for emerging robotic applications [1], [2]. The cloud and robots are not colocated and cloud-enabled computation may result in high-latency, which is intolerable to the multi-robot systems [3]. Mobile edge computing (MEC) pushes the computing resources near robots to effectively reduce the latency [4]. In multi-robot systems, robots need to conduct knowledge sharing-based collaborative inference to complete large and complex tasks [5]. The knowledge sharing-based collaborative inference avoids the limited and inconsistent knowledge of robots during operations, where the knowledge indicates the models and descriptions about robot operation [6]. However, recent knowledge sharing is available for cloud infrastructure but not for edge-assisted systems.

There are security threats to the collaborative inference in edge-assisted multi-robot systems. An attacker can misuse, alter, or destroy the knowledge of the system to further affect the actions of robots [7]. Therefore, it is critical to construct a secure environment for knowledge sharing-based collaborative inference in the presence of untrusted and malicious robots. There are research works to improve the security of multi-robot systems. For example, K. Saulnier et al. in [8] proposed a model to predict the probability of security in multi-robot systems, but they did not provide defense approaches. R. Wehbe and R. K. Williams in [9] proposed a graph topology-based strategy that allows multiple mobile robots to move together in the presence of malicious robots. However, their approach did not consider complex actions in collaborative tasks. Briefly, existing approaches focused on securing the collaboration for a specific action but ignored the knowledge-sharing in varying environments. Besides, existing approaches achieve consensus among robots without ensuring traceability and integrity. The aforementioned centralized trust solutions are not suitable for distributed edge-assisted multi-robot systems. Therefore, we raise three requirements to ensure the trust of the knowledge sharing-based collaborative inference process, including 1) a decentralized inference framework, 2) traceability and integrity of knowledge, and 3) trust in the presence of malicious nodes.

The blockchain provides a trust solution for multi-party communication and traces transactions in a decentralized environment. The blockchain has proven effective in ensuring integrity and privacy. Therefore, blockchain is suitable to solve the trust issue of collaborative inference in edge-assisted multi-robot systems. We are the first to introduce the blockchain into collaborative inference among robots. Besides, existing consensus mechanisms such as proof-of-work (PoW) in the blockchain suffer from low throughput and high resource consumption problems [10]. Therefore, an efficient and adaptable consensus process is necessary for edge-assisted multi-robot systems with restrained resources.

In this paper, we propose a blockchain-based collaborative edge inference (BCEI) framework for edge-assisted multi-robot systems. The main contribution of this work includes the following.

- The inference process at the edge is formulated as collaborative knowledge graph construction among robots, which is efficient for knowledge sharing.
- The blockchain is utilized to provide a decentralized approach to maintain traceable and integral knowledge among robots, which is suitable for knowledge sharing for complex tasks in varying environments.
- An efficient knowledge-based blockchain consensus method is presented to guarantee the trust in the presence of malicious nodes.

We provide a trusted, decentralized, and efficient approach for collaborative inference among robots. Besides, our work can be extended to other edge-assisted scenarios, such as the smart logistics industry and emergency rescue in disasters.

The rest of this paper is organized as follows. First, we propose the collaborative inference framework for multi-robot

Jianan Li, Jun Wu (corresponding author), and Jianhua Li are with Shanghai Jiao Tong University and the Shanghai Key Laboratory of Integrated Administration Technologies for Information Security; A. K. Bashir is with Department of Computing and Mathematics, Manchester Metropolitan University, Manchester M15 6BH, U.K, and School of Electrical Engineering and Computer Science, National University of Science and Technology(NUST), Islamabad, Pakistan; Md. Jalil Piran is with Computer Engineering Department Sejong University, Seoul, South Korea; Ashiq Anjum is with Department of Informatics, University of Leicester, UK.

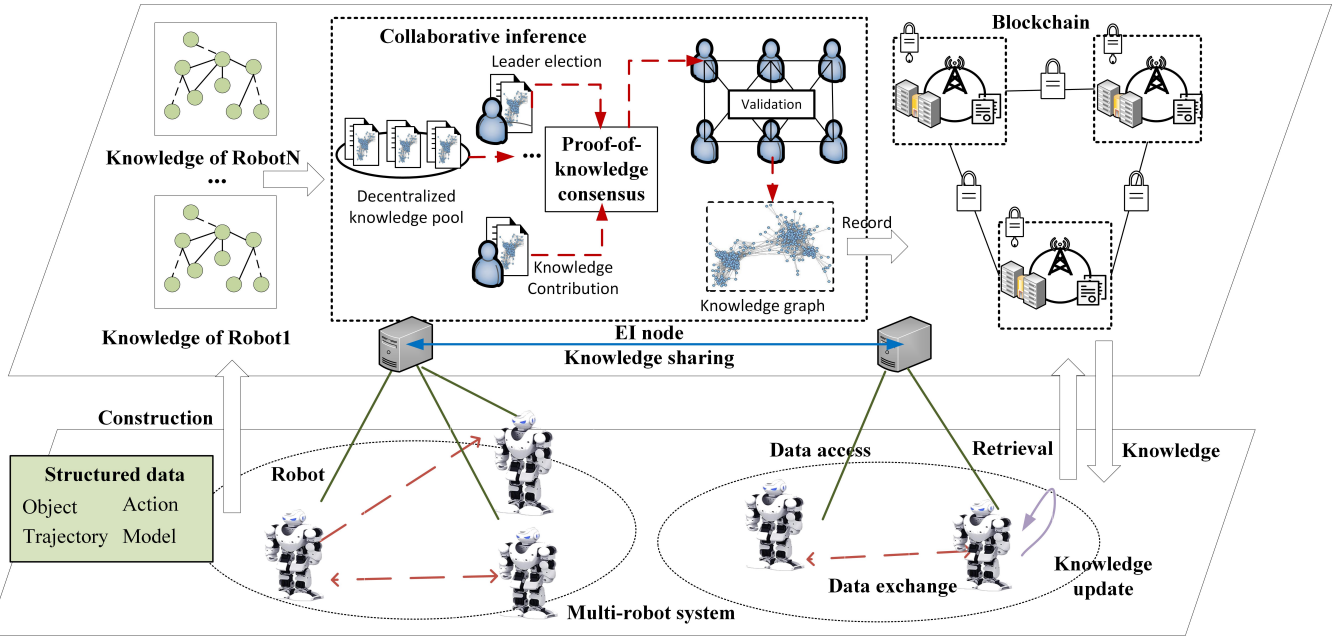

Fig. 1. Blockchain-based collaborative edge inference.

systems. Then, we propose the knowledge-based blockchain consensus. Next, we discuss application scenarios and use emergency rescue as a case study. We conduct experimental evaluations to illustrate the efficient performance. Finally, we conclude the work and discuss future issues.

II. Background

A. Blockchain

Blockchain is a kind of distributed ledger utilizing encryption technology to protect data security [11]. In a blockchain, the participating nodes record and package transactions in a block. The consensus mechanism is the core component of the blockchain to ensure trust among multiple entities without a third party. All participating nodes achieve the consensus and elect a leader to broadcast the block to the entire chain. Every node holds a ledger and maintains the blockchain for the security and integrity of transactions. The blockchain avoids single point failure and centralized corruption and ensures transparency and traceability of transactions. Besides, the mechanism of the blockchain incentives participants with benefits and improves the activity of the whole network. Due to its ability to achieve collaborative trust among multiple entities, blockchain is a key technology to ensure trust for many fields, including finance, industry, and transportation systems.

B. Knowledge Graph

With the explosive growth of content-based information, the knowledge graph is becoming a significant technology to promote inference capability [12]. The knowledge graph builds a database by modeling semantic entities and attributes, and indicates potential relations between them. Recently, several knowledge graphs, including the Google Knowledge Graph and DBpedia, have been successfully integrated with artificial intelligence (AI) and greatly promoted the performance of learning models. The integration of knowledge graph and AI provides a fast and convenient knowledge-based inference approach, such as smart question answering and social network recommendation systems [14].

III. Blockchain-based Collaborative Edge Inference

A. Overview

We present the BCEI framework for multi-robot systems, as illustrated in Fig. 1. We formulate the collaborative inference at the edge as the collaborative knowledge graph construction and sharing model. It is assumed that most nodes in the system are honest. The PoK consensus of blockchain is achieved by the collaborative construction of knowledge graphs. The framework consists of two parts. 1) Robots provide raw data on their action, model, target object, physical attributes, and trajectories. Besides, robots execute tasks according to received knowledge from the edge. 2) Edge-inference (EI) nodes are responsible for collaborative inference. The EI nodes generate individual knowledge and achieve PoK consensus in the process of collaborative knowledge graph construction. The EI nodes are responsible for maintaining the blockchain and get a payment from the blockchain-based collaborative inference process.

The BCEI includes four functions. 1) Knowledge construction: the collaborative inference at the edge is formulated as collaborative knowledge graph construction among nodes. 2) Knowledge storing: there is no central web-enabled knowledge database in the system, and the knowledge is stored in the distributed database at the edge. 3) Knowledge sharing: the knowledge sharing and aggregation process is recorded in the blockchain, which guarantees security and traceability. 4) Knowledge incentive: the PoK consensus in the blockchain is related to the knowledge contribution, which incentives participants.

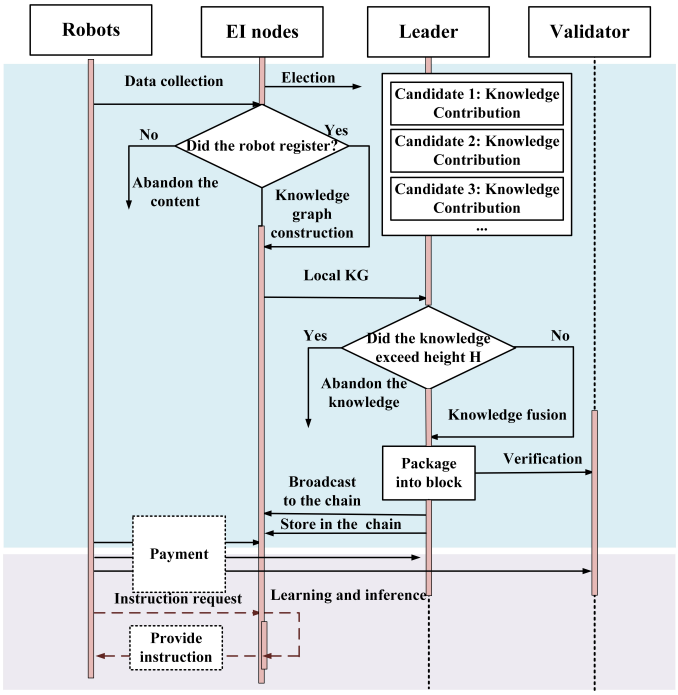

Fig. 2. Knowledge construction in blockchain-based collaborative edge inference.

To execute a complex task, robots communicate with others through the implemented edge interfaces via Wi-Fi/5G/LAN. The robot is registered with an ID. The edge node generates its private key and public key. The robot collects data about the actions, target objects, physical attributes, and trajectories, and submits the data to the edge. Figure 2 presents the collaborative inference process. The complex task is published into the blockchain when the task starts. After receiving the selected task, the EI nodes construct a knowledge graph together and achieve the PoK consensus. The constructed knowledge graph is returned to robots for task execution. The task requester has the copyright of the knowledge, which means that only authorized roles can read and modify the knowledge graph. Knowledge can be provided for similar tasks in different environments. The task publication and graph retrieval are recorded in the chain for further audit.

The threat model includes two aspects. 1) Malicious robots. Some compromised robots submit incorrect or harmful inputs to the edge. 2) Malicious EI nodes. Some malicious EI nodes tend to spread false knowledge in the network.

B. BCEI Components

We design a BCEI architecture, which consists of the following components.

- Permissioned blockchain. The permissioned blockchain maintains secure connections among participants. Only identified nodes can participate in block generation and verification. The permissioned blockchain solves the malicious robot pollution problem and protects the privacy of data.
- Proof-of-knowledge consensus. We propose the PoK consensus for collaborative inference to guarantee the security of knowledge construction and reduce traffic load and computational overhead. The PoK consensus of BCEI is reached by committee nodes in the knowledge construction process. The committee nodes first construct individual knowledge graphs according to the knowledge of a robot. Then the committee leader is responsible for knowledge fusion.
- The hybrid blockchain. The chain is composed of a main permissioned blockchain and several light blockchains. The light blockchains are deployed in a specific local region and are responsible for the collaborative inference of the multi-robot system. Meanwhile, the constructed semantic knowledge graphs are recorded in the main permissioned blockchain and utilized for analogous tasks in different environments.

C. Analysis of BCEI

We analyze the BCEI from efficiency, scalability, and security perspectives.

- Efficiency. The BCEI establishes a secure collaborative inference architecture for multi-robot systems. The decentralized knowledge database is utilized for specific collaborative tasks. The decentralized knowledge database can be shared for similar tasks. Thus, the knowledge from one group of robots can be shared with another group of robots for similar tasks in different environments, which improves system efficiency.
- Scalability. The BCEI consists of a main blockchain and several light blockchains. The hybrid blockchain architecture improves scalability when the knowledge graphs are massive.
- Security. 1) Single points failure: the BCEI avoids power concentration and single point failure by applying blockchain. 2) DDoS attack: participants make a deposit to the chain before submitting a graph, which prevents malicious participants from executing DDoS attacks by repeatedly submitting the same graphs. 3) Injection attack: intentionally submitting harmful information from a malicious robot contradicts the knowledge submitted by other robots. This Injection attack can be detected by the system immediately. Besides, the knowledge graph database is constructed by multiple participants. The leader is only responsible for knowledge fusion and broadcasting, which hardens spreading malicious knowledge in the chain. 4) 51% attack: the PoK consensus elects the leader according to the knowledge contribution, which prevents 51% attacks. The knowledge contribution is related to the popularity of submitted graphs. The popularity of a knowledge graph about a specific task in a region is difficult to predict. The nodes that tend to spread false knowledge reduce the contribution and are at risk of being judged as malicious nodes.

IV. Blockchain Architecture

We introduce the blockchain to BCEI and propose the PoK consensus for collaborative inference. The collaborative

inference is modeled as the consensus process. There are three roles in the blockchain:

- The miner nodes are responsible for knowledge graph construction. After task publication, the miner nodes collaborate in knowledge graph construction. To encourage the nodes to maintain the blockchain, the participants receive a reward according to their contributions. When the nodes complete the task, the task requesters pay for the task to maintain the stable operation of the blockchain.
- The committee leader is selected according to the knowledge contribution during the collaborative inference process. The committee leader receives more reward than miner nodes.
- The validators are selected to guarantee the quality of submitted knowledge graphs. They are also responsible for the validation of the information in the generated block. The validators also receive a reward for the validation process.

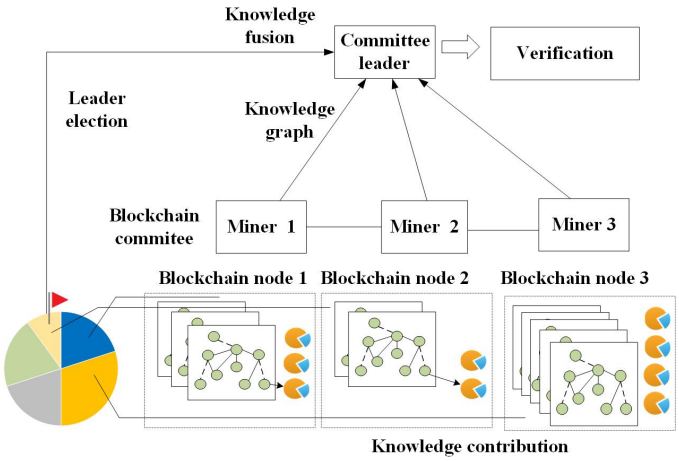

Fig. 3. Proof-of-knowledge consensus in BCEI.

There are three types of transactions in the PoK blockchain: task publication (PubT), knowledge graph construction (ConT), and knowledge retrieval (RevT). The PoK process is a process including knowledge extraction, knowledge fusion, and knowledge processing, as shown in Fig. 2.

A. Task Publication (PubT)

The task publication indicates the inference goal of the participants. It is recorded in the chain for further audit. The task publication transaction contains the following content: [Timestamp, Robot list, Task description, Block height, Reward, Signature]. The robot list indicates the knowledge resources of this task. The task description includes the ontologies of the multi-robot system's task. The block height H specifies the time limit for the knowledge graph submitted by the participating nodes. If the time for a node to submit the result exceeds the height, this proof is considered invalid. The robot list indicates the knowledge resources of this task, while the task description includes the ontologies of the multi-robot system's task. The participating nodes receive a reward according to their contributions.

B. Knowledge Graph Construction (ConT)

Each participant builds an individual knowledge graph of a robot and submits it to the committee leader. The knowledge graph construction includes knowledge extraction, knowledge graph embedding, and knowledge fusion. The collected data are described as a triple (h, r, t), where h is the head entity, t is the tail entity, and r represents the relation between the two entities. The participating nodes extract the entities and generate the knowledge graph according to the ontologies of robots. Knowledge graph embedding is performed to translate the entities and relations to a low-dimensional semantic vector that is efficient for analysis in the learning model. PTransE learning model is considered for collaborative inference. The node submits the graph to the leader under the block height H for knowledge confusion. The submitted graph follows the transaction format such as [Timestamp, RDF triples, Hash of subgraph, Signature].

The committee leader is responsible for knowledge fusion and block generation. The election of the leader is according to the knowledge contribution of participants, as illustrated in Fig. 3. The knowledge contribution refers to the contribution degree accumulated by a participant during knowledge graph construction. It considers the popularity and scale of the uploaded knowledge graphs. The popularity of one uploaded knowledge graph is estimated by its retrieval frequency across the whole network. The scale of the knowledge graph is estimated according to the entities and relations in the knowledge graph. The quality of the knowledge is represented by the triple confidence, which indicates the reliability of knowledge in the triple [14]. Inspired by the path-constraint resource allocation algorithm over networks (PCRA), we consider resource allocation to measure the reliability of knowledge. A triple with higher confidence means the knowledge in the triple is more reliable. Participants with more knowledge contributions have a higher possibility to be elected as a committee leader. For any given entity e_i in sub-graph G_i, the leader is responsible for finding an entity e_j in sub-graph G_j in another individual knowledge sub-graph that refers to the same entity as e_i. The constructed graph has the form [Timestamp, RDF triples, Hash of graph, Signature]. The committee leader broadcasts the generated block to the validators for approval.

The validators are selected randomly among the committee members. The validators audit the knowledge contribution and check the content of the block after receiving the constructed graph. After validation of the block, the knowledge graph is recorded in the blockchain. Only verified knowledge graphs are recorded and broadcast in the blockchain. The generated block is in the form [Timestamp, Signature, Hash head of the block, Hash of knowledge graph].

C. Knowledge Retrieval (RevT)

The knowledge retrieval process includes knowledge requests and sharing, which is recorded as a transaction in the blockchain in the form [Timestamp, Requester ID, Ontologies, Provider ID, Hash of data log, Hash head]. The requester first sends the request for specific knowledge to the main blockchain. The main blockchain nodes retrieve from the

database according to the ontologies about the task and obtain the requested knowledge graph. Then the request is forwarded to the task publisher. The knowledge graph is accessible after permission is obtained from the task publisher.

V. Application Scenario and Case Study

A. Application Scenario

Emergency rescue faces the following challenges. Gaps and narrow spaces are difficult to explore by human emergency responders, which greatly hindered rescue missions. Besides, the communication infrastructure may be destroyed during the disaster. The robots controlled via cloud communication infrastructure failed to respond quickly [1]. The requirements of the emergency rescue are three-fold, including efficient and accurate operation, low-latency communication, and operation in an unknown environment. The proposed BCEI can satisfy the requirements and aid with the rescue tasks. Therefore, the emergency rescue case is considered as a typical application scenario of the BCEI.

B. Case Study

The emergency rescue scenario is illustrated in Fig. 4. We investigate how BCEI could provide a knowledge sharing-based collaborative inference approach and assist multi-robots systems as follows. We assume that Robot A and Robot B are identified in the rescue task R_y, and Robot C is identified in the rescue task R_x that happens before R_y. The task of Robot A and Robot B is composed of three steps:

1. Simultaneous localization and mapping. Robot A retrieves the keywords "mapping" and "earthquake" in the knowledge base at the edge. Then Robot A downloads the related knowledge from rescue task R_x provided by Robot C.

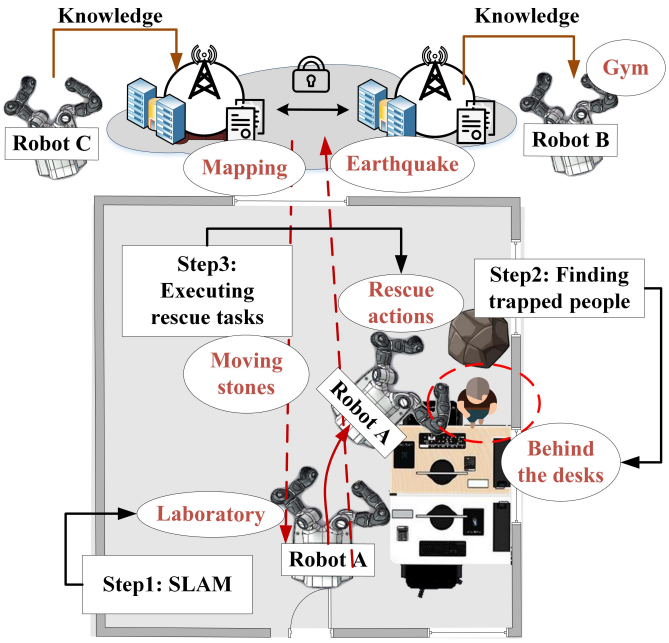

Fig. 4. Emergency rescue task utilizing collaborative inference: (a) simultaneous localization and mapping; (b) finding trapped people; (c) executing rescue tasks.

Robot A explores the environment according to the mapping knowledge from other robots and learns that the environmental location of the task is a "laboratory".

2. Finding trapped people. Robot A explores the laboratory and infers the location of trapped people. The possible location of trapped people can be estimated according to a semantic similarity to a location from a similar task, such as R_x. Robot A infers that the possible locations of trapped persons are "under chairs" or "behind desks".

3. Executing rescue tasks. Robot A executes the rescue actions after finding the trapped people: moving broken chairs; raising the alarm; recording the state of trapped people; removing trapped people from gaps. The action models are recorded in the knowledge graph of Robot A and submitted to the edge node. Robot B in another location can download the models and knowledge, and execute the mapping and rescue tasks in the "gym".

The construction and retrieval process is recorded in the blockchain. The blockchain operates as a "Rescue Recorder" that includes a "Rescue Knowledge Recorder" and "Rescue Data Recorder". The Rescue Knowledge Recorder is utilized for knowledge sharing, and the Rescue Data Recorder is utilized for rescue analysis.

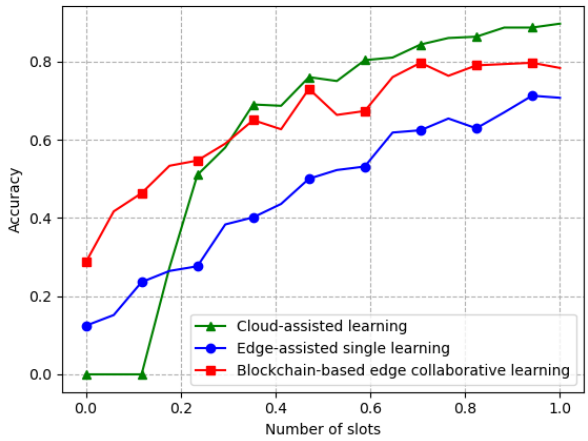

Fig. 5. Accuracy of BCEI, cloud-assisted robots, and a single edge-assisted robot.

VI. Simulation and Experiments

This section discusses the simulation and experimental results of BCEI. A real experiment is established with the Raspberry Pi 3 Model B (denoted Rasp3+) installed with a micro SD card via Power over Ethernet (PoE). The Rasp3+ has been previously used as a robots essential processor component [15].

In the simulation, a classification task is considered as an example of a typical sub-task in robots tasks, such as location determination, object detection, and object recognition. The performance of three approaches is compared: cloud-assisted learning approach, edge-assisted single learning approach, and BCEI. The cloud-assisted learning approach refers to centralized inference with a large distance between robots

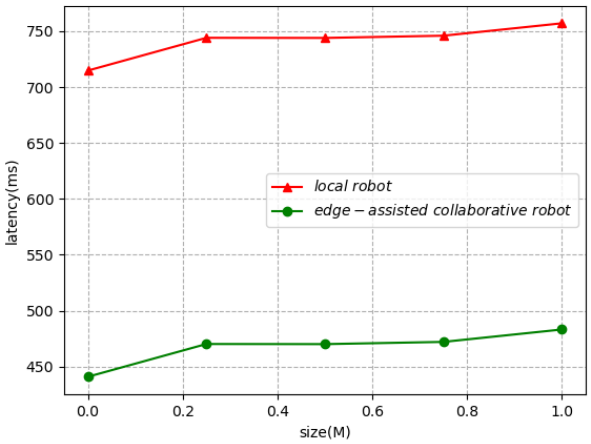

Fig. 6. Latency of local robots and an edge-assisted collaborative robot.

and the cloud. The edge-assisted single learning approach refers to decentralized inference at the edge without knowledge sharing. Figure 5 presents the accuracy of the above three approaches. We can observe that the response latency of the edge-assisted single learning approach and BCEI is smaller than that of the cloud-assisted approach. This is because the edge decreases the communication distance in the task. Besides, the performance of BCEI is much better than that of the edge-assisted single learning approach, which indicates the advantage of collaborative inference at the edge.

We consider an image-recognition task for the Rasp3+ in the experiments. The edge-computing environment and robots are established with Rasp3+s that communicate with each other via LAN. Figure 6 shows the performance of a local robot and an edge-assisted collaborative robot. The latency is composed of the transmission latency and computing latency of the task. The experimental results show that the edge-assisted collaborative robot can execute the task quicker. The latency increases with the increasing transmission knowledge size. The reason is that the local robot executes the image-recognition task without assistance from other robots. But the edge-assisted collaborative robot has the pre-trained knowledge that is stored at the distributed knowledge base on the Rasp3+. The computational complexity of the inference algorithm is $O(MNK)$, where M is the number of submitted knowledge graph at the time interval T_{i-1}, N is the number of triples in knowledge graphs, and K is the number of relation paths of a specific triple. In a specific time interval, the number of submitted knowledge graph and relation paths is usually far lower than the scale of a knowledge graph. Therefore, the computational complexity is tolerable. Besides, the knowledge contribution is calculated according to the state at the last time interval. This eliminates the computation time of leader selection in the consensus process.

VII. Challenges and Future Works

The edge-assisted multi-robot systems are foreseen to be applicable for wide applications. We discuss the various challenges of utilizing the proposed framework and future works in the following.

- Due to the limited resources of robots, the resource allocation models need further investigations such as efficient communication, computing, and caching strategies.
- To satisfy the real-time requirements of edge-assisted multi-robot systems, it is in-demand but challenging to optimize the blockchain architecture and block generation mechanism.
- The privacy-preserving methods for the knowledge protection need to be further studied in the face of various privacy disclosure problems at the edge.

VIII. Conclusion

In this paper, we proposed a BCEI framework in edge-assisted multi-robot systems to provide the trusted edge collaborative inference in an insecure environment. We formulated the inference process at the edge as collaborative knowledge graph construction and sharing model among robots. The efficient PoK blockchain consensus method was proposed for ensuring the trust of knowledge sharing, avoiding knowledge pollution, and detecting malicious nodes. Then a case study on the emergency rescue scenario was discussed. The evaluation results demonstrated that the proposed system improves efficiency and accuracy. Finally, we outlined future research directions and challenges including resource allocation, blockchain optimization, and privacy-preserving methods for the edge-assisted multi-robot systems.

Acknowledgment

This work is supported by National Natural Science Foundation of China (Grant No. 61972255).

References

[1] G. Hu, W. P. Tay and Y. Wen, "Cloud robotics: architecture, challenges and applications," *IEEE Network*, vol. 26, no. 3, 2012, pp. 21-28.
[2] J. Wen, L. He and F. Zhu, "Swarm Robotics Control and Communications: Imminent Challenges for Next Generation Smart Logistics," *IEEE Communications Magazine*, vol. 56, no. 7, 2018, pp. 102-107.
[3] X. Lin, et al., "Making Knowledge Tradable in Edge-AI Enabled IoT: A Consortium Blockchain-Based Efficient and Incentive Approach," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, 2019, pp. 6367-6378.
[4] Q. Zhang et al., "Response Delay Optimization in Mobile Edge Computing Enabled UAV Swarm," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 3, 2020, pp. 3280-3295.
[5] A. K. Bozcuolu et al., "The Exchange of Knowledge Using Cloud Robotics," *IEEE Robotics and Automation Letters*, vol. 3, 2018, no. 1072-1079.
[6] Moritz Tenorth;Michael Beetz, "KnowRob: A knowledge processing infrastructure for cognition-enabled robots," *The International Journal of Robotics Research*, vol. 32, no. 5, 2013, pp. 566-590.
[7] W. Han et al., "Quantitative Assessment of Wireless Connected Intelligent Robot Swarms Network Security Situation," *IEEE Access*, vol. 7, 2019, pp. 134293-134300.
[8] K. Saulnier et al., "Resilient Flocking for Mobile Robot Teams," *IEEE Robotics and Automation Letters*, vol. 2, no. 2, 2017, pp. 1039-1046.
[9] R. Wehbe and R. K. Williams, "A Deep Learning Approach for Probabilistic Security in Multi-Robot Teams," *IEEE Robotics and Automation Letters*, vol. 4, no. 4, 2019, pp. 4262-4269.
[10] M. S. Ali et al., "Applications of Blockchains in the Internet of Things: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, 2019, pp. 1676-1717.

[11] J. Huang et al., "Towards Secure Industrial IoT: Blockchain System with Credit-Based Consensus Mechanism, *IEEE Transactions on Industrial Informatics (TII)*, vol. 15, No. 6, 2019, pp. 3680-3689.
[12] B. van Luijt and M. Verhagen, "Bringing Semantic Knowledge Graph Technology to Your Data," *IEEE Software*, vol. 37, no. 2, 2020, pp. 89-94, March-April.
[13] S. Bhatt et al., "Knowledge Graph Semantic Enhancement of Input Data for Improving AI," *IEEE Internet Computing*, vol. 24, no. 2, 2020, pp. 66-72.
[14] Xie, R.et al., "Does William Shakespeare REALLY Write Hamlet? Knowledge Representation Learning With Confidence", *Proceedings of the AAAI Conference on Artificial Intelligence*, vol.32, no.1, 2018.
[15] C. Irvene et al., "HoneyBot: A Honeypot for Robotic Systems," *Proceedings of the IEEE*, vol. 106, no. 1, 2018, pp. 61-70.

Jianan Li received the B.S. degree from School of Electronic Information Engineering in Beijing Jiao Tong University, Beijing, China, in 2017. Now, she is a Ph.D. candidate at the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University.

Jun Wu (junwuhn@sjtu.edu.cn) received his Ph.D. degree in information and telecommunication studies from Waseda University, Japan, in 2011. He was a visiting researcher at Muroran Institute of Technology, Japan, from January 2019 to February 2019. He is currently a professor in the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University.

Jianhua Li received his B.S., M.S., and Ph.D. degrees from Shanghai Jiao Tong University in 1986, 1991, and 1998, respectively. He is currently a professor in the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University. He got the Second Prize of the National Technology Progress Award of China.

Ali Kashif Bashir is a Senior Lecturer/Associate Professor and Course Leader of BSc (H) Computer Forensics and Security at the Department of Computing and Mathematics, Manchester Metropolitan University, United Kingdom. He received his Ph.D. in computer science and engineering from Korea University South Korea. He is serving as the Editor-in-chief of the IEEE FUTURE DIRECTIONS NEWSLETTER. He is also serving as area editor of KSII Transactions on Internet and Information Systems; associate editor of IEEE Internet of Things Magazine, IEEE Access, IET Quantum Computing, Journal of Plant Disease and Protection.

Md. Jalil Piran received the Ph.D. degree in electronics and radio engineering from Kyung Hee University, South Korea, in 2016. He was a Post-Doctoral Research Fellow in resource management and quality of experience in 5G cellular networks and the Internet of Things (IoT) with the Networking Laboratory, KyungHee University. He is currently an Assistant Professor with the Department of Computer Science and Engineering, Sejong University, Seoul, South Korea.

Ashiq Anjum is a professor of distributed systems at the University of Leicester, UK. Previously, he was a professor of distributed systems and director of the Data Science Research Centre at the University of Derby, UK. His research interests are in data intensive distributed systems and high performance analytics platforms for continuous processing of streaming data. He has been consistently securing grants from different funding agencies for investigating high performance analytics systems for producing intelligence and evidence for engineering, aerospace, medical and security applications.