Proof of location verification towards trustworthy collaborative multi-vendor robotic systems

Evan W. Wu
Toshiba-BRIL
Toshiba Europe Ltd.
Bristol, United Kingdom
wenbo.wu@toshiba-bril.com

Marius Jurt
Toshiba-BRIL
Toshiba Europe Ltd.
Bristol, United Kingdom
marius.jurt@toshiba-bril.com

Ben Holden
Toshiba-BRIL
Toshiba Europe Ltd.
Bristol, United Kingdom
ben.holden@toshiba-bril.com

Yichao Jin
Toshiba-BRIL
Toshiba Europe Ltd.
Bristol, United Kingdom
yichao.jin@toshiba-bril.com

2024 IEEE International Conference on Industrial Technology (ICIT), 25-27 Mar 2024, Bristol, UK

***Abstract*—In the context of a smart industrial manufacturing scenario, where autonomous mobile robots (AMRs) from different manufacturers operate in shared environments, it is important to establish a method for verifying the integrity of the robots. To address this issue, we propose a novel framework for verifying the completion of tasks in multi-vendor robotic systems using proof-of-location and distributed ledger technologies. This approach ensures the trustworthiness and reliability of a multi-vendor robotic system. Using distributed ledger technology (DLT), robots can independently and cryptographically verify the completion of each other's tasks. Unlike traditional solutions that require several dedicated robots to participate in the verification process simultaneously, our proposed physical verification method is more efficient and does not require a typical "mining" stage. Additionally, it can be done asynchronously without adding extra burdens or delays to other ongoing tasks. Simulation results demonstrate that our approach can efficiently and effectively identify malicious robots in a multi-vendor robotic system.**

***Index Terms*—Proof of Location, Distributed Ledger Technology, Multi-Robot System, Reputation and Trust Management**

I. Introduction

In recent years, intelligent robots [1] with powerful sensors and advanced mechanical designs have become increasingly prevalent in people's daily lives. They can be found in various environments, assisting people with repetitive and tedious tasks, such as domestic robots used for cleaning. Moreover, since they can assist humans in performing dangerous and challenging tasks in hazardous environments, they are also commonly utilized in factories and various industrial settings. However, a single intelligent robot is incapable of performing complex tasks that consist of numerous different sub-tasks [2] [3]. For example, in a warehouse scenario [4], objects are supposed to be picked, packed, labelled, and then delivered. To tackle complex tasks, a critical technology is emerging with a fleet of diverse functional robots organized to construct a fully autonomous system called a Multi-Robot System (MRS) [5].

Although a multi-robot system is capable of executing complex tasks [2], it is vulnerable to various security attacks when considering its deployment in a practical industrial scenario. Robots operating in an open access industrial environment can be physically captured, tampered with, and subsequently reintroduced into the system [8]. In this case, the attacker can easily manipulate the compromised entity to engage in fraudulent activities (i.e., intra-fraud attack), which, in a worst-case, can result in system downtime [9]. Another significant security issue is that a foreign entity (i.e., an illegitimate intruder) can access to an autonomous industrial manufacturing environment running an MRS, which means it can interfere with the actions and operations of other legitimate robots [8].

Ferrer et al. [10] proposed a potential framework for MRS based on blockchain technology. This framework introduces identities for each robot in a multi-robot system, enabling traceability and auditability of the robots' behaviors. However, due to the intrinsic properties (e.g., high resource consumption) of the blockchain system, it is impractical to deploy this system on resource-limited robots [11]. Study [12] extended the work on combining blockchain technology and multi-agent systems by presenting an approach to manage the reputation among robots. The evaluation process for task completion in their system design, nevertheless, is inefficient. This is because both the service requester and provider are required to participate in the evaluation process, and there is no guarantee of promptness in evaluating the service. Considering the inefficiency of the above systems, in this study, we focus on providing a robust and reliable multi-robot cooperation framework for practical industrial manufacturing environment, which aims to stimulate the development of future intelligent factories.

To effectively address these threats comprehensively in an industrial manufacturing environment, this study presents a proof of location-assisted (PoL) self-supervised multi-robot cooperation framework. This framework leverages Directed Acyclic Graph Distributed Ledger Technology (DAG-DLT) to record task execution data and reputation changes for each robot, ensuring non-repudiation and tamper-resistance [13]. Each robot utilizes onboard sensors, such as cameras, to perform PoL-assisted task verification.

Notably, our DLT-based PoL verification framework is novel in that it employs a physical-based location verification method, eliminating the need for conventional time-consuming processes like immediate verification, ex-

TABLE I
COMPARISON TABLE OF THE PRIOR ARTS

	Paper Published Year	Distributed Ledger Technology	Transaction Contents	Scalability	Verification		Not requiring immediate verification	No Mining process (low computational consumption)	Member reputation tracking (Incentive System)	Not requiring PoL aggregation (High efficiency)	Attack Scenarios			
					Crypto-graphical	Physical					Impersonation	Malicious Intruder	Intra-fraud	Sybil Attack
Blockchain-based PoL [6]	2018	Blockchain	Location information	low	✓	Wireless technology (short range)	✗	✗	✗	✗	✓	N/A	✓	✓
Blockchain-based zero-knowledge PoL in IoT [7]	2020	Blockchain	Digest of Location information	low	✓	Wireless technology (short range)	✗	✗	✗	✗	✓	N/A	✓	✓
Proposed approach: DLT-based PoL	2023	DAG-DLT	Task execution information	high	✓	Wireless Technology (short range) or Computer vision (proximity)	✓	✓	✓	✓	✓	✓	✓	✓

pensive mining operations, and transaction aggregation. This approach offers the dual benefits of enhancing the efficiency of multi-vendor robotic systems while ensuring the authenticity of task completion. Additional detailed comparison between the proposed DLT-based PoL and other Blockchain-based PoLs is provided in Tab. I.

Moreover, the proposed framework enables real-time tracking of trustworthiness and the verification of each robot's task completion. To validate its effectiveness, we conducted simulations by integrating the framework into an autonomous multi-vendor robotic system within a simplified industrial warehouse environment. The simulation results show that the proposed approach can efficiently and effectively identify malicious robots. The main contributions of our research work are as the following three-fold:

- **Identity and reputation management system:** The asymmetric cryptography-based identity system can promptly detect all intruders without a legitimate identity. Together with a reputation management system, the reliability and trustworthiness of each robot are trackable and auditable.
- **Task completion verification approach:** The DLT-based PoL pass-by task completion verification approach is a distributed verification process and runs in the background on each robot to verify the task completion of other entities. During verification processes, robots can detect identity impersonation and intra-fraud attacks.
- **Experimental analysis:** We verified the feasibility of the proposed framework in a industrial warehouse scenario, simulation results demonstrate that our framework can efficiently and effectively identify malicious robots in a multi-vendor robotic system.

The remaining part of this paper is organized as follows: Section II provides a detailed state-of-the-art literature review, which is followed by an overview of the proposed system and introduces the work processes in Section III. Then, in Section IV, we demonstrate the simulation results of the proposed system in two different attack scenarios. In Section V, we discuss two open issues that affect the performance of the system in the context of the batch test results. Finally, we draw the conclusion in Section VI.

II. LITERATURE REVIEW

This section provides a comprehensive literature review of state-of-the-art related works that focus on securing multi-robot systems using various technologies. We also compare the feasibility of these potential technologies by considering the challenges faced by multi-robot systems, such as resource consumption, bandwidth limitations, and identity and reputation management. Then, we will illustrate the technologies deployed in our proposed system.

Multi-robot system is an emerging technology that organizes a large number of robots to build an autonomous system that can perform tasks that a single robot cannot complete [14]. Such a system is intelligent in terms of complex task execution and team cooperation. There are numerous practical applications of an MRS ranging from agriculture (e.g., military [15], healthcare [16], logistics [17] to environment monitoring [18]. However, deploying an MRS in an industrial manufacturing environment facing various potential security threats.

Studies [8], [9], [17], [19], highlighted the current security challenges faced by an MRS from different perspectives. Bijani et al. [19] categorized security challenges (e.g., resource constraints, physical capture, fake identity, and tampering) for robotic systems based on various use cases, such as monitoring and disaster relief. On the other hand, the study [8] identified security issues existing at both the system and agent level, including threats from fake agents and services (i.e., intruders and intra-fraud), as well as threats from users to agents and agents to agents.

To prevent interference from intruders, Eduardo et al. [10] introduced an approach to encapsulate a mission's high-level objectives in an authenticated data structure known as Merkle Tree. In this way, the intruders cannot access the task information and, as a result, will not be able to disrupt the normal operation of the system. However, the proposed system design cannot guarantee that legitimate robots will perform their discovered sub-tasks honestly. Strobel et al. [20] proposed a solution that utilizes blockchain technology to manage Byzantine robots (malicious robots) and prevent Sybil attacks in a consensus decision-making scenario. Nevertheless, deploying the blockchain system on resource-limited robots is impractical due to its intrinsic properties, such

2024 IEEE International Conference on Industrial Technology (ICIT), 25-27 Mar 2024, Bristol, UK

as high resource consumption [11]. Study [21] discussed the feasibility of blockchain technology in an MRS, which focuses on four scenarios, namely security, decision-making, and behavior differentiation in a robot swarm. Compared with blockchain technology [22], DAG-based DLT [23] has strong scalability and supports high transaction throughput, which are exactly the characteristics desired by MRS [11]. Study [12] extended the work on combining blockchain technology and multi-agent systems by presenting a reputation management approach. Since both the service requester and provider are necessary for evaluating tasks completion, the promptness of service evaluation cannot be guaranteed, making it unsuitable for an industrial scenario.

To verify the authenticity of task completion, one possible solution is to witness it where it happened. Michel et al. [6] have taken a blockchain-based approach to empower network nodes to verify and store proof-of-locations (PoLs) of devices. Wei et al. [7] proposed a blockchain-based zero-knowledge PoL scheme, which enhances the protection of PoL information by encrypting it with the recipient's public key. However, both methods require timely interaction between devices during the location verification process. This requirement makes the systems less efficient or even impossible to complete location verification in areas where devices are sparsely distributed and require frequent interactions. Tab. I compares the proposed approach with the two aforementioned research works from various perspectives. Both methods can prevent several attacks (e.g., impersonation, intra-fraud, and Sybil attack). However, they perform less efficiently due to their use of blockchain technology, as it involves several time-consuming processes such as mining and transaction aggregation.

Multi-robot systems have promising applications in various business scenarios, such as warehousing, healthcare, and environmental monitoring. Ensuring that nodes in the system can reliably perform the assigned tasks is challenging. In addition, the working environments are often highly dynamic in many scenarios. Therefore, it is desirable to establish an efficient method for tracking the reliability of each robot in the system. In this paper, we propose a cooperation framework for multi-robot system in an industrial manufacturing environment. The framework utilizes proof-of-location and distributed ledger technologies to enhance the system's performance. The detailed system design will be illustrated in Section III.

III. System Overview

In this section, we will focus on the structure of our proposed system, called Proof-of-Location Assisted Self-Supervised Multi-Robot System (PoL-SMRS), as depicted in Figure 1. We will also discuss how the robots within the system supervise each other to ensure the trustworthiness of each entity.

A. Identity Management

One of the obstacles to transfer MRS from academia to industry is the issue of authentication of the identity of robots

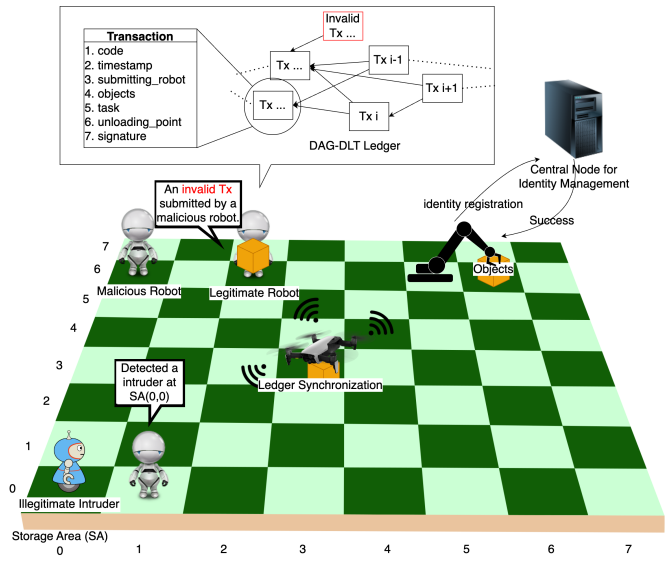

Fig. 1. Proof of Location-assisted Self-supervised Multi-Agent Robotic System Overview

[19]. Given the large number of robots performing tasks in full autonomy requiring extensive data sharing and task collaboration, we need to ensure that each robot in the MRS is reliable and their behaviours are traceable. It is desirable for an individual robot in a MRS to determine whether the other robots are legitimate entities before interacting with them. Technology such as asymmetric cryptography [24] can provide identity authentication and integrity verification to robots in a MRS.

To introduce the concept of identity in a MRS, we firstly need to determine how to define the unique identity of a robot. In asymmetric cryptography algorithms such as elliptic curve digital signature algorithm (ECDSA) and Rivest Shamir Adleman (RSA) [24], a device generates a pair of keys: a public key and a private key. The public key is generally publicly available and poses no impact on system security. The private key will be stored locally and, if compromised, will cause unpredictable security risks. Therefore, using the public key, which is already publicly available, as the robot's identity ensures that the identity is unique within the MRS and allows secure interaction with other robots. All the robots that join the system have access to task list as well as the member list. The system will firstly initialize a distributed ledger containing the Genesis node. Each member who successfully registers their identity synchronizes the ledger's content with the central server.

The PoL-SMRS is compatible with homogeneous or heterogeneous MRSs, so any devices wanting to join the system can generate a public-private key pair locally and register with the identity management system using the public key. After successful registration, the robot is given a certain initial reputation value (e.g., 100) in the incentive system and recorded in the central server. Reputation values give an indication of how

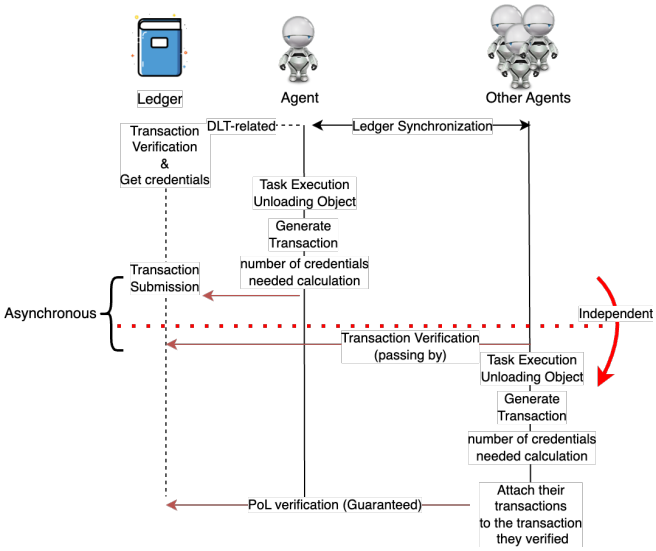

Fig. 2. Conceptual work process of PoL-SMRS

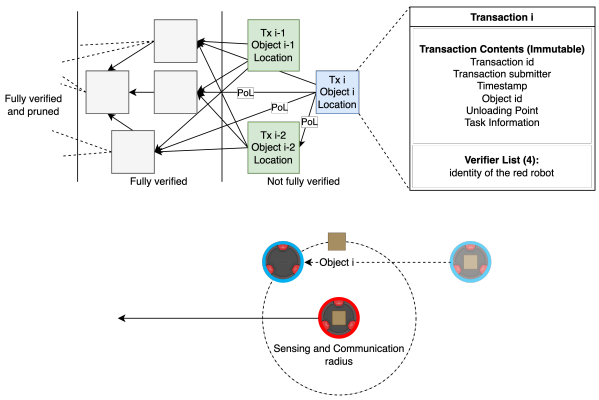

Fig. 3. Visualization of the work process of a regular robot in the PoL-SMRS

reliable a robot is, which is necessary to track the reliability of members in an open access environment. A robot needs to spend a certain amount of reputation value when acquiring a task, and partial of the reputation value (e.g., 80%) will be returned when the task has been performed and verified as valid. The remaining part will be rewarded to verifiers equally.

Each robot is equipped with several sensors (e.g., cameras) to detect intruders. Intruders are defined as nodes that are not registered in the identity system. The detection process can be specified by the user, for example through pre-trained computer vision models to find nodes that are not a member of the system.

B. Work Process of PoL-SMRS

Each robot, after successfully joining the PoL-SMRS system, performs its tasks according to the process depicted in Fig. 2. The solid line in the middle of Fig. 2 represents the primary work steps of a robot, the dashed line on the left shows the background processes of a robot, and the solid line on the right side demonstrate the work processes of other robots in the system.

1) Task Acquisition: The robot first calculates the nearest object that needs to be transported based on its current location, the source location of objects in the task list and the task allocation algorithm. Then it obtains the corresponding task from the task management system. The robot's identity will be added to the relevant task execution record, so it can perform the task.

2) Task Execution and PoL-assisted Pass-by Verification: During the task execution period, the robot moves according to the shortest distance to the destination. As it moves, the robot filters out any transactions submitted whose unloading locations are within the robot's current sensory range (namely, tip selection) and performs PoL-assisted proximity verification (e.g., the red robot depicted in Fig. 3). Transaction verification includes two steps: transaction integrity is verified via the signature of transactions, and the location of objects is verified via onboard sensors (e.g., camera). The PoLs, which include images and timestamps, are stored locally by verifiers. The PoLs generated during the verification process are used for auditing when required. Each transaction is verified a certain number of times (e.g., 4) by different peer robots. The number of verifications can be set by the user according to the deployment scenario and required level of security.

In a highly dynamic environment, an object may need to be transported frequently within a warehouse. To ensure that an object is verified for a specific times before it is transported again, we have added a verification priority feature to PoL-SMRS. The time at which an object is re-transported will directly impact the verification priority of the current task corresponding to that object. If a transaction verified by a robot is valid, the robot will receive the credential corresponding to that transaction. The robot can attach its transaction to the transactions it verified using the credential.

The robot will report an error to the central server if there is a mismatch between the actual location of the object and the unloading point recorded in the transaction or if the signature is invalid. At the same time, the robot broadcasts the identity of the submitter of the corresponding transaction to the entire system to locate the illegitimate robot in time.

3) Object Delivery and Transaction Generation: As soon as a robot delivers the object to the destination, the robot generates a transaction at the unloading point to record information about the task executed (e.g., the blue robot and the zoomed transaction contents in Fig. 3). The robot then digitally signs the task execution-related information with its private key and adds the generated signature to the transaction. The digital signature ensures the integrity of the transaction and its non-repudiation.

4) Credential Calculation and Transaction Submission: When a robot submits a transaction, it first needs to calculate how many credentials it needs by using the dynamic credential formula listed in Formula 1, namely, how many transaction nodes it needs to attach its transaction to. The robot which

does not have sufficient credentials to submit a transaction needs to keep moving and perform proximity verification to the transactions submitted within its sensory range to obtain sufficient credentials. The transactions in the ledger that need to be verified are called tips.

The number of credentials required for a robot to submit a transaction is proportional to the number of tips in the ledger and the number of credentials stored by the robot. Users can personalise the *Divisor* and *Base* in the Formula 1 depending on the timeliness of the transaction verification they require. The smaller the Divisor, the timelier the transaction is verified. Suppose the robot successfully submits the transaction to the distributed ledger and is verified by all four different peer robots as valid. In that case, the robot will receive partial of the reputation value (e.g., 80%) it spent on the task acquisition. The remaining part of the reputation value (e.g., 20%) will be rewarded to the verifiers equally.

$$Credential_{needed} = \frac{Tips_{realtime} + Credentials_{local}}{Divisor} + Base \quad (1)$$

C. Attack Scenarios and Solutions

We will illustrate four categories of attacks in a intelligent warehouse systems and how the PoL-SMRS can prevent them.

1) Identity Impersonation and Repudiation: In the PoL-SMRS, each robot must use a unique identity to join the system. Since the identity system is based on asymmetric cryptography algorithms, any robot can access the identity information and the public key of other robots. All the transactions in a DLT Ledger are digitally signed, which means that a malicious robot cannot impersonate a legitimate robot.

For example, suppose a malicious robot (fake agent) observes that a legitimate robot has successfully delivered an item to the corresponding destination. In this case, a malicious robot can use the observed information to submit fake transactions to the distributed ledger to increase its reputation value. Since each transaction has a signature generated using the private key, the fake transaction can be easily verified and exposed by legitimate robots. Therefore, asymmetric cryptography-based identity systems can inherently prevent identity impersonation attacks. In contrast, if a robot signs a transaction using its private key and denies that it submitted the transaction, we can verify it using its public key due to the non-repudiation feature of digital signatures [25].

2) Sybil Attack: Sybil attack is a kind of attack that exists in DLT, which can severely impact the efficiency of the network [20]. An attacker can subvert the distributed ledger by creating many virtual robot identities (i.e., fake agents) and registering them to the identity management system. In this way, the attacker can submit lots of fake transactions using the fake identities without performing the tasks. Since the legitimate robots in a MRS need to verify all the transactions recorded in the distributed ledger, their efficiency will be affected by the verification processes as lots of the transactions are invalid.

To prevent the Sybil attack, we integrated a reputation-based incentive system into PoL-SMRS. Each robot needs to be registered using a valid unique identifier (hardware based) for identity. All the robots will have an initial reputation value (e.g., 100) after joining the system successfully. A robot must spend a certain reputation value to obtain a task. Since each robot has an fixed initial reputation value, a robot cannot obtain an unlimited number of tasks and not perform them.

3) Illegitimate Intruder: Each robot participating in task executions must have a legitimate identity. Otherwise, it will be considered as an illegitimate intruder. Since autonomous MRS requires a large number of robots with different functions to work together in an open-access environment, it is essential to verify the identity of each robot. Suppose a robot already in the warehouse does not have a legitimate identity. It can move around the warehouse and deliver items to a wrong storage area. In this case, the task execution by legitimate robots will be affected. If an illegitimate intruder were to carry out a large number of random item movements, this would severely impact the efficiency of the MRS and eventually lead to complete downtime.

We developed an intruder detection function for robots in a MRS to prevent this attack. All the robots in the warehouse without a legitimate identity registered in the central node will be regarded as intruders. If a robot detects an intruder, it will immediately report the information (e.g., identity and location of the malicious robot) to the central server.

4) Intra-fraud: Intra-fraud is another attack that can severely affect the efficiency of the MRS. An attacker could physically capture, manipulate, and re-introduce a legitimate robot into the warehouse, in which case an intra-fraud attack would occur. As the robot has a legitimate identity registered to the central node, it could obtain tasks from the task list and partially execute them (e.g., randomly unloading objects into a storage area in the middle of a delivery). It can generate a transaction with the unloading point being the target destination to complete the attack.

As we propose a physical (and cryptographical) task execution verification approach, the successive robots will sense the actual location of the shipment and compare it with the information in the ledger and task list. If the information does not match, the verifier will report to central server an alert with the object's location and the transaction submitter's identity. The central server then uses the verification results of multiple robots to make a judgement and intercept the manipulated robot in time.

IV. Performance Evaluation

To verify the feasibility of our proposed approach, we developed PoL-assisted self-supervised multi-robot system to simulate MRS in a smart warehouse scenario.

Fig. 4 was captured during the simulation running. We set different colours for different robots in a grid warehouse.

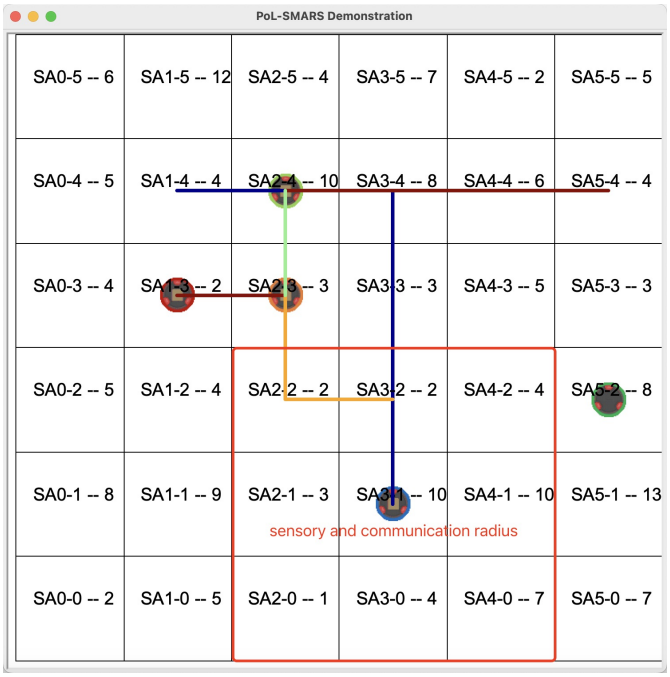

Fig. 4. Simulation of PoL-SMRS in a warehouse (6*6) scenario with 5 robots. The number of objects in each storage area (SA) is shown in cells.

TABLE II
CONFIGURATION OF THE SIMULATIONS

Parameters	Values
Size of the Warehouse	6*6 (cells)
Number of Robots	5 (Regular) 2 (Malicious)
Number of Tasks	200
Sensory and Communication Radius	1 (Chebyshev Distance)
Movement Velocity	20 (cells/sec)
Verification Times for a Transaction	4
Parameters of Dynamic Credential Calculation Formula	10 (Divisor) 2 (Base)
Batch Test	10 (runs)

Each cell represents a storage area. The tasks for robots are transporting objects from one storage area to another one, and the tasks are randomly generated. The movements of a robot from the source to the destination of an object follow the Manhattan distance, as the coloured lines in Fig. 4. The communication and sensory radius of a robot is defined as Chebyshev distance, as the red square depicted in Fig. 4.

In the remainder, we analysed how the system performs in different scenarios by demonstrating the simulation results in two attack scenarios (malicious robots and intruders). The configurations for the two simulation scenarios are the same, which can be found in Tab. II.

A. Malicious Robots (Intra-fraud)

In an intra-fraud scenario, the tampered malicious robot will not deliver the object to the specified location as per the task information, but will indicate in the submitted transaction that it has successfully completed the task. Such attacks can lead to chaos in the warehouse. The PoL-SMRS provide a task completion verification approach to supervise each robot and track their reliability via a reputation-based incentive system.

Fig. 5 depicts the number of tips in the ledger during the simulation. From the figure we can see that the number of tips in the ledger stabilises in a certain interval and is dependent on the parameter settings of the dynamic credential calculation formula. The number of credential required for the robot to submit each transaction is recorded in Fig. 6.

The distributed ledger generated from the simulation is shown in Fig. 7. The DAG-DLT ledger was generated with the coloured transaction nodes. The colour of the nodes in the ledger (in Fig. 7) matches the colour of the robots (in Fig. 4). Each node in the ledger represents a transaction, and the edges represent the attachment relationships between nodes.

In the intra-fraud attack scenario, malicious robots can participate in task execution and submit fake transactions. The fake transactions are shown in the left-bottom corner in Fig. 7. All these transactions were orphaned after a specific times (e.g., 4) of failed verification, and no other transaction was attached to them. Also, the central server will block the corresponding submitters from accessing the task and member lists. Part of the robot's time was wasted trying to verify these fake transactions, so the transaction density was slightly lower in this period than in other parts. Tab. III shows two malicious robots detected in one simulation run, and the simulation run time (200-tasks period) is 16.33 seconds.

TABLE III
DETECTED MALICIOUS ROBOTS

Reference	Identity	Location	Time (s)
MRobot0	32fa748c878...ed0562c98980d	(5, 1)	3.09
MRobot1	856bd3f3147...72ddba933e8e	(3, 1)	3.38

TABLE IV
DETECTED INTRUDERS

Reference	Identity	Location	Time (s)
Intruder0	75b3d5d5c...413cbe826ddfde66	(1, 3)	0.06
Intruder1	f1913548b...75e0da395d14af6	(4, 2)	0.06

B. Intruders

The intruders are defined as the robots without valid identities. These robots can move in the warehouse and randomly place objects in different storage areas to disturb the normal execution of the system. In PoL-SMRS, we assume that the intruders have different appearance compared to legitimate robots. Therefore, the intruders can be easily identified by the onboard cameras of legitimate robots. Tab. IV shows the location and time of the intruders being detected in one simulation run, and the simulation run time (200-tasks period) is 15.77 seconds. The simulation results of the illegitimate intruder scenario are similar to the intra-fraud scenario, we will not show the duplicated figures here.

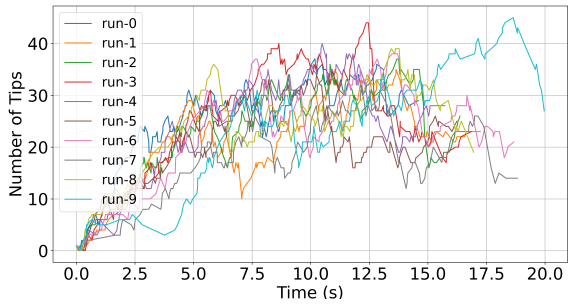

Fig. 5. Number of tips with respect to Time in Intra-fraud Scenario

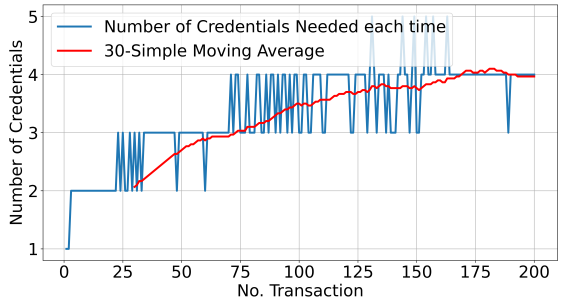

Fig. 6. Number of Credentials Needed for each transaction in Intra-fraud Scenario

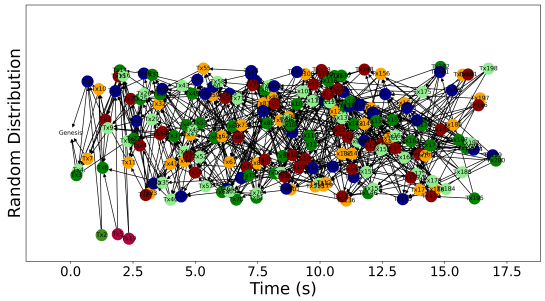

Fig. 7. DLT Graph with respect to Time in Intra-fraud Scenario

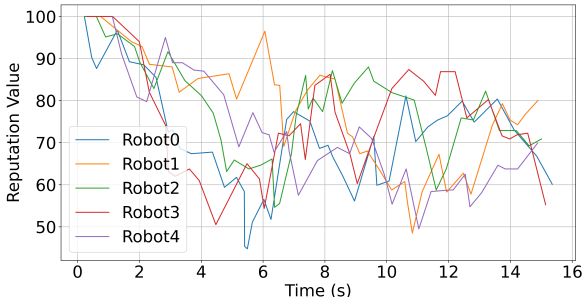

Fig. 8. Reputation Trends of each robot in Intra-fraud Scenario

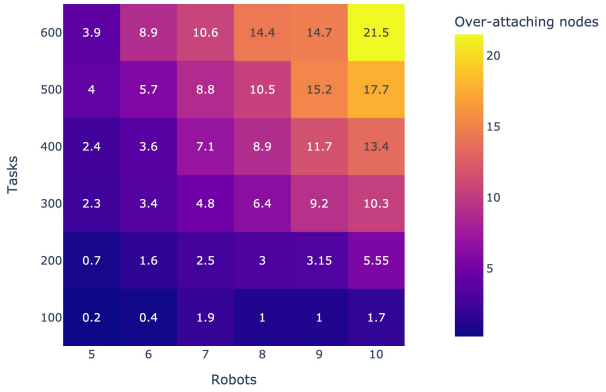

Fig. 9. Number of Over-attaching nodes with respect to Number of robots and tasks

V. Discussion

In a Low-power mesh network, the robots in the PoL-SMRS system implement a fully connected network via relays. However, this connection may not be completely reliable. When the task execution environment is large enough, individual robots can become disconnected from the group and thus unable to synchronize data with other robots for a while. As a result, a single transaction may be verified more times than the specified number of verifications, namely, over-attaching problems. In addition, different robots may disagree on the verification of the same transaction, namely, the Byzantine fault problem. We will discuss these two issues separately in the remaining part of this section.

A. Over-attaching Problem

To test the severity of the over-attaching problem in a low-power mesh network, we conducted batch tests (ten runs for each configuration) to verify the system's performance in two dimensions. Fig. 9 is a heatmap of the growth of over-attaching nodes, which shows a linear growth as the number of tasks grows or as the number of robots grows (the other parameters are the same in Tab. II). However, when increasing both the number of tasks and the number of robots, the growth of over-attaching points tends to increase almost exponentially (values on the diagonal in the graph). For future work, we consider leveraging a consensus mechanism to eliminate the over-attaching nodes problem to improve the system's performance.

B. Byzantine Fault Problem

A single transaction node verified by multiple robots may get different verification results. In a detailed explanation, half of the verifiers consider a transaction valid, while the other half consider it invalid. A disagreement problem will be raised, the so-called Byzantine fault. An additional auditing strategy is needed to resolve this disagreement. In this project,

2024 IEEE International Conference on Industrial Technology (ICIT), 25-27 Mar 2024, Bristol, UK

we mainly use central server as coordinators to validate transactions and record Byzantine robots to expel them from the warehouse in case of disagreements. The problem could also be eliminated with a consensus mechanism [20].

VI. Conclusion

In this paper, we propose the PoL-SMRS system to address potential security issues in future intelligent warehousing. PoL-SMRS is designed to prevent intruders, identity impersonation, intra-fraud, and Sybil attacks in MRS. The system primarily uses DLT to record task completion information of robots (in the form of transactions) and requires other robots to verify it. Using a physical-based PoL pass-by verification approach to verify transactions physically and cryptographically incurs a negligible resource overhead. In addition, we design a robot identity management system based on asymmetric cryptographic algorithms and a message integrity verification method. This system ensures the authenticity and reliability of robot identities within the system. Simulation results show that our proposed MRS framework and method can promptly detect illegitimate or malicious robots. In future work, we need to investigate how to eliminate the problem of over-attaching nodes and the Byzantine fault through various consensus mechanisms. Furthermore, as the central server manages the current incentive system, other potential threats can easily arise in the event of single-point (e.g., central server) failure. Smart contracts could be a potential solution to this problem. Finally, we will also exploring the applicability of the multi-robot cooperation framework to other industrial domains, such as electric vehicle (EV) parking and charging validation.

References

[1] W. He, Z. Li, and C. P. Chen, "A survey of human-centered intelligent robots: issues and challenges," *IEEE/CAA Journal of Automatica Sinica*, vol. 4, no. 4, pp. 602–609, 2017.

[2] A. Farinelli, E. Zanotto, E. Pagello *et al.*, "Advanced approaches for multi-robot coordination in logistic scenarios," *Robotics and Autonomous Systems*, vol. 90, pp. 34–44, 2017.

[3] L. Iocchi, D. Nardi, M. Piaggio, and A. Sgorbissa, "Distributed coordination in heterogeneous multi-robot systems," *Autonomous robots*, vol. 15, pp. 155–168, 2003.

[4] D. B. Poudel, "Coordinating hundreds of cooperative, autonomous robots in a warehouse," *Jan*, vol. 27, no. 1-13, p. 26, 2013. [Online]. Available: https://www.academia.edu/download/30491528/seminarpaper.pdf

[5] A. Gautam and S. Mohan, "A review of research in multi-robot systems," in *2012 IEEE 7th international conference on industrial and information systems (ICIIS)*. IEEE, 2012, pp. 1–5.

[6] M. Amoretti, G. Brambilla, F. Medioli, and F. Zanichelli, "Blockchain-based proof of location," in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*. IEEE, 2018, pp. 146–153.

[7] W. Wu, E. Liu, X. Gong, and R. Wang, "Blockchain based zero-knowledge proof of location in iot," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE, 2020, pp. 1–7.

[8] F. Higgins, A. Tomlinson, and K. M. Martin, "Threats to the swarm: Security considerations for swarm robotics," *International Journal on Advances in Security*, vol. 2, no. 2&3, 2009.

[9] Y. Hedin and E. Moradian, "Security in multi-agent systems," *Procedia Computer Science*, vol. 60, pp. 1604–1612, 2015.

[10] E. C. Ferrer, T. Hardjono, A. Pentland, and M. Dorigo, "Secure and secret cooperation in robot swarms," *Science Robotics*, vol. 6, no. 56, p. eabf1538, 2021.

[11] J. P. Queralta, F. Keramat, S. Salimi, L. Fu, X. Yu, and T. Westerlund, "Blockchain and emerging distributed ledger technologies for decentralized multi-robot systems," *Current Robotics Reports*, vol. 4, no. 3, pp. 43–54, 2023.

[12] D. Calvaresi, V. Mattioli, A. Dubovitskaya, A. F. Dragoni, and M. Schumacher, "Reputation management in multi-agent systems using permissioned blockchain technology," in *2018 IEEE/WIC/ACM international conference on web intelligence (WI)*. IEEE, 2018, pp. 719–725.

[13] X. Liu, B. Farahani, and F. Firouzi, "Distributed ledger technology," *Intelligent Internet of Things: From Device to Fog and Cloud*, pp. 393–431, 2020.

[14] A. Dorri, S. S. Kanhere, and R. Jurdak, "Multi-agent systems: A survey," *Ieee Access*, vol. 6, pp. 28 573–28 593, 2018.

[15] T. Chung, "Offensive swarm-enabled tactics (offset)," *DARPA Tactical Technology Office Proposers Day, Arlington, VA, Accessed January*, vol. 30, 2017. [Online]. Available: https://apps.dtic.mil/sti/pdfs/AD1125864.pdf

[16] S. Kumar, A. Nayyar, and A. Paul, *Swarm intelligence and evolutionary algorithms in healthcare and drug development*. CRC Press, 2019.

[17] 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, pp. 102–107, 2018.

[18] A. Jeradi, M. M. Raeissi, A. Farinelli, N. Brooks, P. Scerri *et al.*, "Focused exploration for cooperative robotic watercraft." in *AIRO@ AI* IA*, 2015, pp. 83–93. [Online]. Available: http://profs.scienze.univr.it/~farinelli/pubs/jeradi-CEUR-15.pdf

[19] S. Bijani and D. Robertson, "A review of attacks and security approaches in open multi-agent systems," *Artificial Intelligence Review*, vol. 42, pp. 607–636, 2014.

[20] V. Strobel, E. Castelló Ferrer, and M. Dorigo, "Managing byzantine robots via blockchain technology in a swarm robotics collective decision making scenario," in *2018 International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2018)*, 2018. [Online]. Available: http://hdl.handle.net/1721.1/115883

[21] E. Castelló Ferrer, "The blockchain: a new framework for robotic swarm systems," in *Proceedings of the Future Technologies Conference (FTC) 2018: Volume 2*. Springer, 2019, pp. 1037–1058.

[22] Q. Zhu, S. W. Loke, R. Trujillo-Rasua, F. Jiang, and Y. Xiang, "Applications of distributed ledger technologies to the internet of things: A survey," *ACM computing surveys (CSUR)*, vol. 52, no. 6, pp. 1–34, 2019.

[23] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: A survey," *IEEE internet of things journal*, vol. 6, no. 5, pp. 8076–8094, 2019.

[24] N. J. G. Saho and E. C. Ezin, "Survey on asymmetric cryptographic algorithms in embedded systems," *IJISRT*, vol. 5, pp. 544–554, 2020. [Online]. Available: https://ijisrt.com/assets/upload/files/IJISRT20DEC110.pdf

[25] W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao, and G. Wang, "Digital signature scheme for information non-repudiation in blockchain: a state of the art review," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, pp. 1–15, 2020.