Department of Electrical and Electronic Engineering

Self-supervised Security in Multi-agent systems

Student: Wenbo Wu **Academic Supervisor:** Prof. Kevin Morris **Industrial Supervisor:** Marius Jurt & Ben Holden

Motivation:

Multi-robotic systems are already being deployed in logistics and warehousing scenarios to substitute humans in tedious tasks. However, developing a fully intelligent warehouse system requires the collaboration of multiple robots with different functions, which may come from different manufacturers. To ensure that heterogeneous robotic systems work as intended, security issues such as identity impersonation and malicious intruders need to be taken into account when designing such a system. [1]

Figure 1: A: Air Carrier B: Stevedore C: Parcel Carrier D: Shelf Carrier

Aim and Objectives:

- **Aim:** To develop a self-supervised heterogeneous multi-agent robotic system which can ensure each robot in the system can complete its tasks as expected.
- **Objectives:**

1. To develop a public Key Cryptography (Elliptic Curve Digital Signature Algorithm (ECDSA)) based identity system preventing impersonation attacks and malicious intruders.[2]
2. To develop a DAG-DLT based task execution ledger (Inspired by IOTA tangle) recording all the task execution records and supply a way for robots to verify the other robots' task execution records.

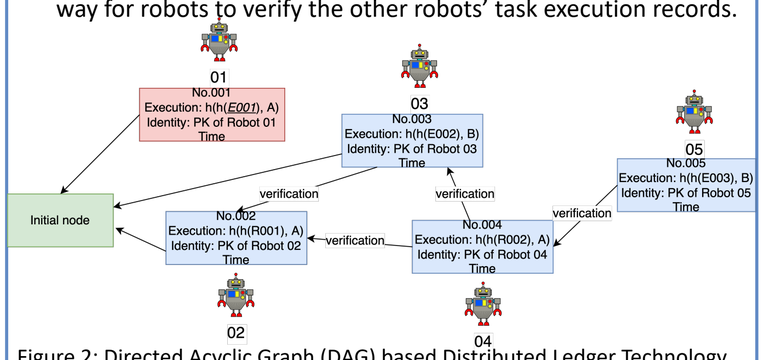

Figure 2: Directed Acyclic Graph (DAG) based Distributed Ledger Technology (DLT) Graph. **Explanation of the contents in a block:** No.002 is the index of a transaction, 'h' represents hash calculation, 'R001' the code of the object carried by Robot2 and 'R' means regular object which should be delivered to warehouse 'A' (in comparison, 'E' represents a different kind of object should be delivered to warehouse 'B'), 'PK' means public key of a robot, time will be the real time a transaction is submitted.

Attack Scenarios:

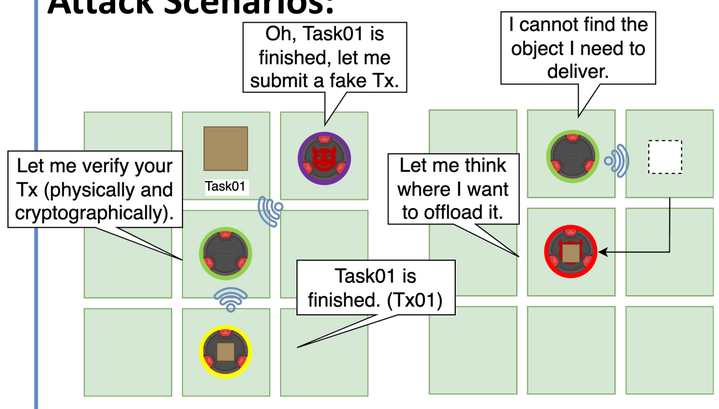

Figure 3-1: **Intra-fraud** can be defined as a legitimate robot in the system claiming to have performed a task when it did not. If a robot is physically captured, tampered with, and re-introduced into the swarm, intra-fraud may occur. [3]

Figure 3-2: **Malicious intruders** will not join the Multi-agent System but will move the objects randomly in the warehouse to disturb the task execution of the other robots.

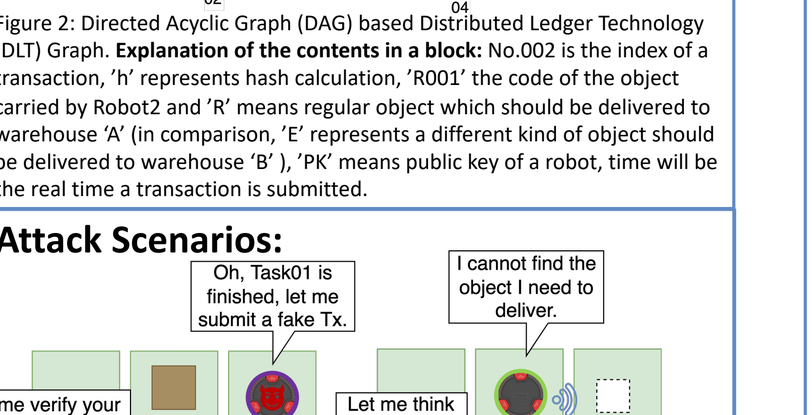

Figure 3-3: **Identity impersonation** is defined as the attempt by some malicious robots to use the identity of a legitimate robot and the public key to perform actions that disrupt the normal execution of tasks and submit the corresponding transactions. [3]

Figure 3-4: **Sybil Attacks** is another way to reduce the efficiency of a robotic system by submitting a large number of fake transactions without performing a task since the legitimate robots in a system need to verify if the transactions in the DLT graph are valid or not.

System Overview:

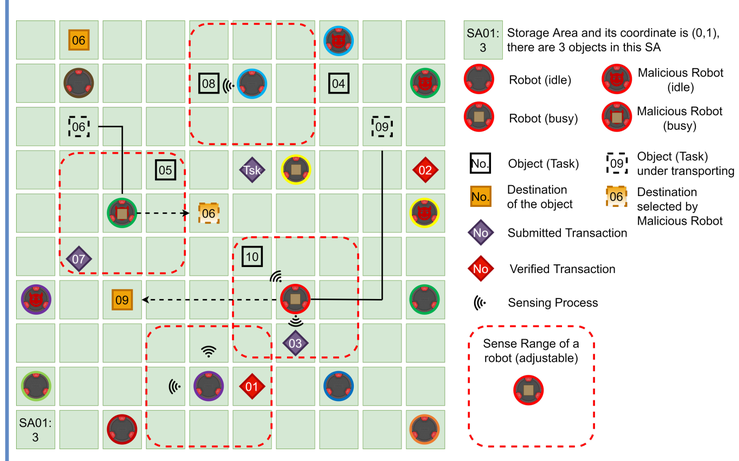

Figure 4: System overview with comments

Main Process:

1. Warehouse Initialization
2. Storage Areas Initialization
3. DLT Graph Initialization (Genesis)
4. Swarm Controller Initialization
5. Robots Initialization
6. Task Manager Initialization
7. Objects & Tasks Generation

Background Processes (Deamon):

- Local DLT Graph Synchronization
- Transaction Verification (Signature & Physically): Prevent intra-fraud
- Intruder Detection

Thread 1:
Single Robot Task Execution
Thread 2:
Single Robot Task Execution
Thread 3:
Single Robot Task Execution
Thread 4:
Single Robot Task Execution
...

Single Robot Task Execution: (a single thread)

1. Task Acquisition
2. Object Accessing
3. Task Executing
4. Object Delivery
5. Transaction Generation
6. Signature Generation
7. Transaction Submission

Simulation and Results:

Configuration:
Scenario: Intra-fraud
Size of Warehouse: 5*5
Number of legitimate robots: 5
Sensing radius: 2
Number of Malicious robots: 5
Number of tasks: 100

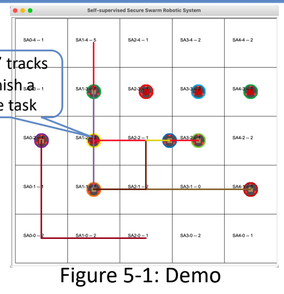

Figure 5-1: Demo

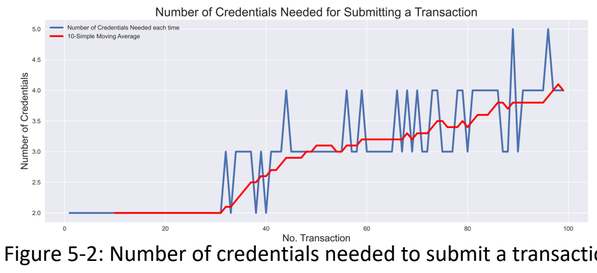

Figure 5-2: Number of credentials needed to submit a transaction

Tips: Transactions need to be verified.

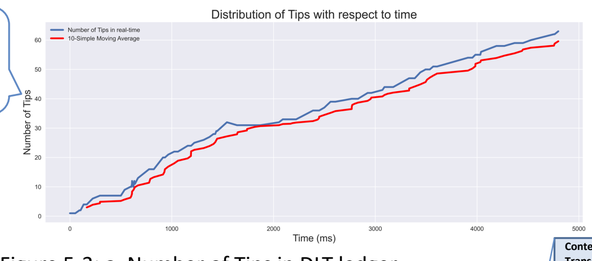

Figure 5-3: a. Number of Tips in DLT ledger

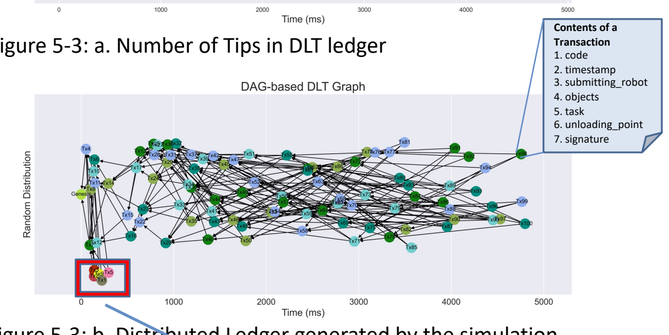

Figure 5-3: b. Distributed Ledger generated by the simulation

Detected Malicious Robots Identity of robot | location | detected time (s)

MRobot0	f5a4ea755124bf649d23a74e7270f7b0eb09d2513f4e58f1f15511c9d20a554c	(4, 2)	0.21
MRobot1	086a9d2ff9d3e95213785408270bdeeaf82ecab36785ce0da92a4645cd52003b	(0, 2)	0.25
MRobot2	a0aa90e493250480e49fcc101020e322834294b26933663f897784de097312fe	(1, 2)	0.51
MRobot3	b6edc2a0d6967509172d665413a7593e13cd242d5ed83bc3cd50e09da06cbb8f	(1, 3)	0.58
MRobot4	d08af755a1ffc587e1f420595e16e814bb2ae63425d71cadc105c404925ee688	(3, 1)	0.59

Figure 5-4: Detected malicious robots and their corresponding location, detected time

Performance Analysis (Batch test - 10):

Scenario: Simulation without Attacks

Configuration:

- 5*5 warehouse size
- 1 sensing & communication range
- 200 number of tasks
- Number of robots: [5,10]
- Conclusion: With the task number fixed, the time elapsed to finish all the tasks will decrease with the robot number increasing. Therefore, the communication amount will decrease as well.

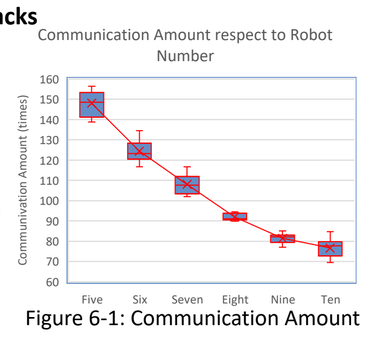

Figure 6-1: Communication Amount

Configuration:

- 5 robots
- Number of tasks: [100,1000]
- The rest configs are same as the above simulation.
- Conclusion: With other parameters fixed, the amount of communication increases linearly with the number of tasks increasing. The metric is inspired by [4].

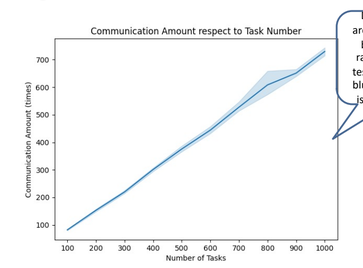

Figure 6-2: Communication Amount

Configuration:

- Configuration: The same as the second simulation configs.
- Conclusion: With other parameters fixed, the time needed to finish all the tasks increases with the number of tasks increasing.

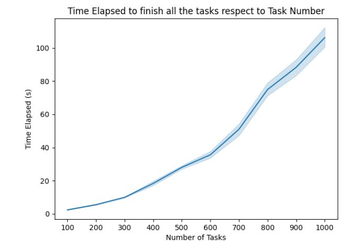

Figure 6-3: Time elapsed to finish all the tasks

Scenario: Malicious Intruder

Configuration:

- 5*5 warehouse size
- 1 sensing & communication range
- 5 legitimate robots
- 100 tasks
- 5 malicious intruders
- Time elapsed to finish all the tasks: around 3.5s
- Conclusion: With 5 times of simulations, the times of the malicious intruders being detected are distributed approximately in range (0, 0.14). The reference of the robots denotes the order the robots being detected.

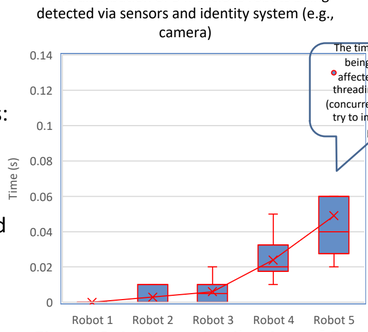

Figure 6-4: Time distribution of 5 malicious robots being detected

Scenario: Intra-fraud

Configuration:

- 5*5 warehouse size
- 2 sensing & communication range
- 5 legitimate robots
- 100 tasks
- 5 illegitimate robots
- Time elapsed to finish all the tasks: around 4.74s
- Conclusion: With 5 times of simulations, the times of the malicious robots being detected are distributed approximately in range (0.1, 0.9).

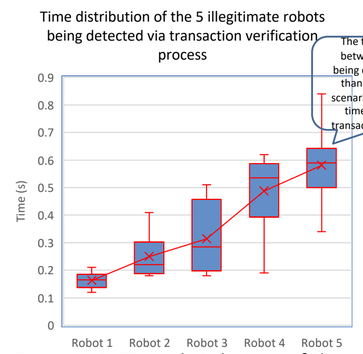

Figure 6-5: Time distribution of the 5 illegitimate robots being detected

Conclusion:

The self-supervised multi-agent system can ensure that all the heterogeneous robots in a warehouse scenario complete their tasks as expected. The proposed system can prevent four kinds of potential threats:

- Malicious intruder (Identity system)
- Identity impersonation (Identity system)
- Intra-fraud (Physical and cryptographic verification processes)
- Sybil attacks (Incentive system)

According to the performance analysis above, our system can locate all the malicious robots in a short period of time without consuming too much extra resources (e.g., communication amount, energy).

Future Directions:

- Distributed Task Management System: task creation, task sensing
- Distributed Identity System (web of trust)
- Smart Contract & Consensus mechanisms: DLT Graph Synchronization, Transaction verification (Byzantine fault)
- Incentive System optimization: Prevent Sybil Attacks with credits (reputation or currency) of robots
- Multi-processing or ROS based simulation
- Reaction to Malicious robots (e.g., expel from warehouse)

University of BRISTOL TOSHIBA

[1]. Wen, J., He, L. and Zhu, F., 2018. Swarm robotics control and communications: Imminent challenges for next generation smart logistics. *IEEE Communications Magazine*, *56*(7), pp.102-107.
[2]. Castelló Ferrer, Eduardo. "The blockchain: a new framework for robotic swarm systems." *Proceedings of the future technologies conference*. Springer, Cham, 2018.
[3]. Bijani, S. and Robertson, D., 2014. A review of attacks and security approaches in open multi-agent systems. *Artificial Intelligence Review*, *42*(4), pp.607-636.
[4]. Ferrer, Eduardo Castelló, et al. "Secure and secret cooperation in robot swarms." *Science Robotics* 6.56 (2021): eabf1538.