Scenarios for Trust Management in Swarm Robotics

Daniel Vojnar, Adela Bierska, and Barbora Buhnova
Faculty of Informatics, Masaryk University
Brno, Czech Republic
{vojnar,bierska,buhnova}@mail.muni.cz

ABSTRACT

Many terrestrial and aquatic organisms, such as ants, termites or fish, live in communities that resemble larger and more capable organisms thanks to the delicate coordination of the individuals. Humans benefit from mimicking this coordination in many technological sectors, whether it is the coordinated movement of drones, cars, or robot teaming. With the increasing autonomy and intelligence, multi-robot systems and swarm robots specifically have increasing potential to replace humans in dangerous missions, reacting collaboratively to unprecedented conditions. What if, however, one of the robots decides to sabotage such a collaborative mission? How can we support its peers in detecting an untrustworthy member? This paper identifies and classifies the scenarios of swarm-robot collaboration, which is prone to disruption by an untrustworthy member, and links them to a taxonomy of attacks, for which it highlights the importance of the trust aspect between individual robots across the scenarios. The benefits of trust are presented, discussing its capability to prevent attacks and detect malicious individuals in these types of systems.

KEYWORDS

Swarm Robotics, Trust, Scenarios, Attacks

ACM Reference Format:
Daniel Vojnar, Adela Bierska, and Barbora Buhnova. 2024. Scenarios for Trust Management in Swarm Robotics. In *2024 ACM/IEEE 6th International Workshop on Robotics Software Engineering (RoSE '24), April 15, 2024, Lisbon, Portugal.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3643663.3643967

1 INTRODUCTION

Electronic devices, vehicles and robotic systems with growing degrees of intelligence and autonomy are becoming more pervasive in our daily lives, forming entire digital ecosystems, capable of collaboration as well as competition or sabotage [1]. Multi-robot systems are evolving towards replacing humans in not only routine activities but also dangerous missions, such as in the case of underwater explorations, earthquakes, or other disasters or military operations.

A specific type of multi-robot systems designed for collaborative missions is based on so-called robot swarms [2]. Swarm robots are fairly simple (and thus better replaceable) autonomous robots that form communities to collectively accomplish a mission that they could not complete individually. These missions consist of many small tasks (e.g., collective motion, information sharing, or provisioning of an important resource) [2]. However, due to the mutual interdependence of swarm robots, the missions are susceptible to attacks, such as information manipulation, communication manipulation, or physical attacks, which can affect the overall progress of the mission and even cause casualties. [3, 4]

One of the promising solutions that has only been explored recently in the context of Social Internet of Things is based on trust management [5]. Specifically, when understanding the trustworthiness of their peers, the robots could more competently decide whether to obey a command, trust information, or continue to cooperate with the peer, based on their needs and goals. Trust management can be scaled up to the context of the entire ecosystem, where the robots collaboratively decide on the next steps, acceptance of an individual into the group or protecting themselves from an untrustworthy peer.

To support the development of trust management models for swarm robotics, the necessary prerequisite is understanding the variety of trust attacks across the multitude of collaborative scenarios that need to be covered by trust management schemes. Such an understanding is, however, currently missing.

In this paper, we bridge this gap. To this end, we collect and classify swarm robot scenarios available across scientific literature, and with the help of their common properties, we link them to possible attacks. Our main contribution is a systematic collection of scenarios, their taxonomy, and the taxonomy of attacks affecting mission success. Besides, we outline possible applications of trust techniques that could mitigate these attacks or their impact.

The paper is structured as follows. After the discussion of related work in Section 2, the main contribution is presented in Section 3 and 4, focusing on both the taxonomy of swarm-robot scenarios and attacks on the scenarios. After that, the discussion of the results is included in Section 5 and conclusion in Section 6.

2 STATE OF THE ART AND RELATED WORK

After clarifying the terminology, this section details the state of the art in swarm robotics and discusses related work on swarm-robotics scenarios and their trust attacks.

2.1 Collaboration in Robotic Systems

Multi-Robot Systems. Multi-robot systems are a type of organized system in which two or more robots collaborate to achieve a specific goal. Multi-robot systems offer numerous advantages over single-robot systems, such as improved system performance, energy efficiency, robustness, scalability, and reliability due to the

RoSE '24, April 15, 2024, Lisbon, Portugal

ACM ISBN 979-8-4007-0566-3/24/04.
https://doi.org/10.1145/3643663.3643967

collective capabilities and distributed task allocation among individual robots [6, 7]. Multi-robot systems can be classified into several categories, for example, based on the homogeneity of the individuals [8].

Swarm Robotics. The swarm-robotic approach is a multi-robotic system inspired by insect societies [9]. These systems are composed of a large number of simple robots to reach high levels of robustness, flexibility, and scalability [10]. Minor failures and anomalies are not fatal to the mission of a swarm robot system as there are many cooperating robots within the group, and each of them is, to some extent, replaceable. Therefore, particular robots are expected to be identical or at least compatible to avoid a single point of failure. Swarm coordination is decentralized and can adapt to changing problems [10, 11].

2.2 Characteristics of Swarm Robots

According to the taxonomy provided by Iocchi et al. [12], swarm robots are cooperative, aware, strongly coordinated, and they have distributed organization [9]. Each of the robots should be autonomous and capable of sensing and acting in the real environment [9].

Robots can interact via sensing (i.e., observing or being aware of another robot) or via communication (i.e., exchanging messages) [10]. Both sensing and communication are local, and one cannot expect that robots will have access to some global information [11]. However, both organization and communication can be centralized (entirely or partially) if appropriate [13]. Robots within a swarm are homogeneous; occasionally, some individuals can have some specializations, e.g., sensor modules with larger sensor equipment. Overall, their abilities are limited, and we expect that individuals cannot solve the task alone [9]. Therefore, robots within a swarm have to cooperate to accomplish a given mission. As they are not centrally organized, they need to self-organize themselves based on their actual environment and interactions with each other [11, 12]. This collaboration depends on coordination protocol which should be shared and followed by robots to evaluate signals and behavior of each other correctly [12].

2.3 Trust Management in Swarm Robotics

Numerous studies have looked at the utilization of swarm robots or overall multi-robot systems, however scarce attention has been given to the critical matter of establishing trust among these robotic entities [14–16] and its implications in various scenarios [2, 17, 18].

Yang and Parasuraman in [19] dealt with the creation of an agent trust model for heterogeneous multi-robot cooperation. This model is based on Relative Needs Entropy, which is used to determine the degree of trust between individual robots, robot and group of robots and groups based on their needs. Their procedure was simulated on search and rescue scenarios. Yet, the work does not provide insight into the multitude of trust scenarios and their attacks.

Blockchain is now a widely-discussed approach towards assuring trust between robots. For instance, Mallikarachchi et al. [20] present a way to connect Robotic Operating system with Ethereum blockchain using Smart contracts technology. This approach, while exhibiting notable advantages of trustable shared truth and history management, faces certain limitations connected to the current version of Ethereum in terms of the system scalability along with a slow contract deployment rate and fewer transactions per second.

Li et al. [21] circumvented some of the blockchain limitations [22] by creating the Blockchain-based collaborative edge interface framework, enabling secure knowledge sharing among bots, avoiding knowledge pollution, and detecting malicious nodes. Yet, all these approaches are currently very scarce and do not yet cover the variety of trust-attack scenarios that one could encounter in swarm robotics.

2.4 Overview of Scenarios in Swarm Robotics

In our work, we intend to collect swarm robotics scenarios that would be as complete as possible, so that the possible trust attacks could be identified. At the moment, there are already works collecting and describing a few possible scenarios, but not with the intention to cover all possible scenarios in sufficient detail to identify possible trust applications.

Specifically, Şahin [23], Khaldi [24], and Tan [25] provided categories for swarm robot tasks divided by their environment and requirements. They are a valid overall introduction to swarm robotics and cover their possible applications in the real world. However, they are not suited to support trust-attack scenarios classification as they focus more on the mission's target than on robots' behavior and communication.

A taxonomy based on different types of collective behavior was provided by Brambilla [15], and later, this taxonomy was extended by others [17, 26, 27]. These papers are a significant signpost in the topic of swarm robotics and are a good base for our collection. They are more focused on taxonomy and generalization of scenarios, whereas we need more detailed granularity to cover all possible situations that could be affected by applying the trust techniques.

Besides, Higgins [3] laid out various challenges to the security of robotic swarms, focusing on their potential deployment in public and commercial settings, which became a useful input for our taxonomy of attacks, which is based on specific, simple scenarios identified as part of our work.

3 SCENARIOS IN SWARM ROBOTICS

This section discusses the process of scenario collection, together with the presentation of resulting scenarios and their classification.

3.1 Methodology

3.1.1 Search Process. To identify relevant papers associated with the scope of this scenario collection, we performed a search in Google Scholar, Scopus, Springer, ACM Digital Library, and IEEE Xplore academic databases. We first run the following search query to retrieve relevant studies from the libraries:

- swarm AND (robotics OR robots) AND (task OR mission OR cooperation OR scenario OR challenge OR attack OR sabotage OR vulnerability)

After that, we filtered the studies with respect to their correspondence with the query (considering their titles and abstracts) and then filtered the relevant results according to the inclusion and exclusion criteria.

Table 1: Resource Centered Scenarios Overview

ID	Scenario	Task	References
R1	Collaborative manipulation	Robots shall collaborate to manipulate objects in the environment.	[2, 27–29]
R2	Object clustering	Robots shall collect objects in the environment to previously unspecified places.	[29]
R3	Sorting	Robots shall sort objects by their features.	[2]
R4	Object assembling	Robots shall physically link objects together to build a structure.	[29]
R5	Foraging	Robots shall search for objects and return them to the specified base.	[2, 27]
R6	Consuming	Robots shall search for objects in the environment and process them. The process is similar to foraging, but robots do not carry the item to the base but perform work in place.	[30]
R7	Charging in the nest	Robots shall recharge their batteries on a limited number of chargers during missions.	[2]
R8	Information spreading	Robots shall spread information within the system. That means robots shall coordinate to propagate information to all individuals within the system.	[31]
R9	Object tracking	Robots shall observe and follow a moving object.	[32]

3.1.2 Inclusion/Exclusion Criteria. The inclusion criteria that have been defined to provide systematic guidelines to include papers during the filtering phase are:

IC1. The paper discusses the swarm robotics.
IC2. The paper explicitly describes one or more scenarios to an efficient extent (one or more norm-pages).
IC3. The described scenarios include inter-robot communication or cooperation within the swarm.

The exclusion criteria that have been defined to provide systematic guidelines to exclude papers during the filtering phase are as follows:

EC1. Papers in languages other than English.
EC2. Papers with up to 3 pages.
EC3. Gray literature (e.g., editorials and keynotes).

3.1.3 Search Results. From the results, 36 papers met our inclusion criteria, and from those, 17 were excluded by exclusion criteria. From the remaining 19 papers, we extracted scenarios with as much granularity as possible.

3.1.4 Scenario Clustering. After selecting all the scenarios, we clustered them into six groups according to the common activity, goal or type that accompanies all the tasks in the group:

- Resource Centered Scenarios Overview
- Collective Movement Scenarios Overview
- Swarm Maintenance Scenarios Overview
- Spatial Orientation Scenarios Overview
- Information Sharing Types
- Decision Making Types

The results are presented in Tables 1, 2, 3, 4, 5, 6, giving the id and name of the scenario, description of the scenario task and linking the papers used for scenario extraction.

3.2 Overview of Scenarios

This section describes four scenario groups and two types/forms groups. Scenario groups in Tables 1, 2, 3, 4 are clustered by the main target of the tasks, and the types groups in Tables 5, 6 by the format of the task.

Table 2: Collective Movement Scenarios Overview

ID	Scenario	Task	References
M1	Spatial organization	Robots shall split positions within the environment and reorganize.	[27]
M2	Aggregation	Robots shall reduce the distance between them and gather in a certain place.	[27–29]
M3	Dispersion	Robots shall occupy the largest possible area without losing connectivity.	[27]
M4	Grazing	Robots shall explore the environment in such a way as to traverse the largest amount of space, similar to lawn mowing.	[30]
M5	Flocking	Robots shall move together to a target location.	[2, 27]
M6	Cooperative hole/obstacle avoidance	Robots shall avoid an object in the environment cooperatively, which means the swarm could decide to assemble into a structure and overcome the object instead of bypassing it.	[29]
M7	Object collision avoidance	Robots shall adjust their movements to avoid a collision with an object.	[2]
M8	Robot collision avoidance	A robot shall adjust its movement to avoid a collision with another robot.	[2]
M9	Pattern formation	Robots shall restructure themselves to a repetitive pattern. An example in nature is honeybee nests.	[27–29]
M10	Self-assembly	Robots shall physically connect and form a single organism.	[27–29]
M11	Robot soccer	Robots shall cooperate together to play a game and defeat the enemy team. In robot soccer, the two robot teams, where robots have different skills and capabilities, are "playing" soccer. Robot soccer is a competitive scenario that can be transferred to military defense operations.	[29]

Table 3: Swarm Maintenance Scenarios Overview

ID	Scenario	Task	References
S1	Deployment	Robots shall deploy themselves to the environment without any central coordination.	[2]
S2	Flock centering	Robots shall localize the center of their swarm and, that way, create a target location for individuals in a flocking scenario.	[2]
S3	Time synchronization	Robots shall synchronize their clocks to unify their time and movement.	[32]
S4	Velocity matching	Robots shall match their velocity to prevent collisions.	[2]
S5	Information sharing	Robots shall share information with an individual or a group. In contrast to information spreading, this task focuses on the ability to pass a piece of information to others, not to coordinated propagation through the whole community.	[2, 33]
S6	Decision making	Robots shall evaluate known information and select a uniform procedure.	[2, 27, 28, 34]

Resource Centered Scenarios. During the mission, robots manipulate many resources and objects that are significant for success. It can be, for example, physical objects meant to be collected or destroyed, but also resources such as information that has to be spread through the whole environment or charging stations, which has to be reasonably shared between robots. Resource-centered scenarios are listed in table 1.

Collective Movement Scenarios. The swarm is a distributed system with many individuals who must cooperate so their movement can be effective and meaningful. Possible scenarios of the movement of individuals and the group as a whole are listed in table 2.

Swarm Maintenance Scenarios. Some scenarios do not directly aim at the mission accomplishment but serve more as preparation and maintenance of the functioning and synchronized state of the swarm. Collected maintenance scenarios are listed in table 3. Information sharing and decision making have multiple variations, which are described in Tables 5 and 6.

Table 4: Spatial Orientation Scenarios Overview

ID	Scenario	Task	References
O1	Mapping	Robots shall create a map of the environment.	[27, 29]
O2	Navigation	Robots shall guide an individual or a group through the environment.	[2]
O3	Localization	Robots shall identify the position of the swarm without external reference, global position state.	[27, 29]
O4	Beacon navigating	Robots shall serve as beacons, which means they send information about closeness to the target/other beacon.	[2]
O5	Distance measuring	Robots shall measure distance based on the intensity of signals retrieved from sensors.	[2]

Table 5: Information Sharing Types

ID	Type	Description	References
I1	Direct communication	The robots communicate directly, often by transferring data to the signal.	[2]
I2	Communication through the environment	The robots indirectly communicate via the environment as a medium (pheromones, marking the environment), also called stigmergy.	[2]
I3	Communication via sensors	Robots send and retrieve signals, e.g., light or sound, using sensors.	[2]
I4	Using shared memory	All robots within the swarm have access to a shared source of information that they can read and possibly update.	[2]
I5	Part of the robots knows some global information and propagates it to the rest	Only selected robots have access to a shared source of information and pass it on to the rest of the swarm.	[2]
I6	Broadcasting of a table with information	Each of the robots has its own table with information, broadcasts it periodically to others, and updates it based on tables from nearby robots.	[33]
I7	Leaving information about actions previously done	Robots leave marks in the environment to inform others about their activity and progress.	[2]
I8	Leaving pheromones and waiting for help	Robots leave information in the environment about a need for help and wait near the found resource or problem.	[2]
I9	Sending pulses showing direction to the target	After finding a resource, the robot informs others by sending a signal in the direction of the found resource.	[2]

Spatial Orientation Scenarios. The swarm may not previously know the environment of the mission. Therefore, it is crucial to be able to explore the surroundings and also be able to share this information with other robots and possibly help them orient themselves. Table 4 contains collected scenarios in the spatial orientation of individuals and the whole swarm.

Information Sharing and Decision Making Types. Decision-making and information sharing may have many forms, which can be linked to different kinds of attacks. Therefore, we assigned ID to their types described in Table 5 for information sharing and Table 6 for making decisions.

Information sharing can take many forms and implementations. They differ in the use of signal types (e.g. data, light, sound), in mediation using different media (e.g. environment, shared memory) or in the application of algorithms (e.g. broadcasting).

Decision Making is usually concerned with the flow of decision making, the number of options, what is being decided (e.g. allocation members, tasks), the information available to individual robots, or who is involved in the decision. For example, if we look at the amount of manpower available to the swarm, the robots may be deciding what is the optimal distribution of manpower for maximum efficiency or whether it is even sensible to perform the mission in such numbers.

Table 6: Decision Making Types

ID	Type	Description	References
D1	Consensus	The robots agreed on the result of several possibilities.	[27]
D2	Decision made by small group or leader	The intelligence of the swarm is not strictly distributed. Only a selected individual or group makes decisions for the whole swarm.	[34]
D3	Allocation of members among sources	The robots distribute among the individual sources for future work.	[34]
D4	Recruitment of mission members	The swarm searches for and accepts new members needed for the mission accomplishion.	[34]
D5	Task allocation	The robots allocate the tasks each one will be executing.	[27, 28]
D6	Exploitation vs. exploration	The swarm has to decide whether the gathered information is enough to make a decision or whether it is necessary to continue exploring the environment.	[34]
D7	Maximizing the net energy (collected resources / time searching)	While searching for resources, robots must decide how many robots to search and how much to collect, and when to stop searching.	[2]

4 SCENARIO ATTACKS

This section describes categories of issues occurring in swarm robot scenarios, summarized in Figure 1. We also briefly outline how the concept of trust between robots can help us address these vulnerabilities and reduce the risk of mission failure.

4.1 Methodology

Our next step was searching each of the collected scenarios individually to find possible attack vectors and investigate trust applications to avoid them.

This process revealed to us that the coverage of this area by existing literature is very sparse and close to non-existing, so we used the help of the description of the scenarios to predict what vulnerabilities could take place, although some of them were not explicitly discussed in literature. To this end, for each scenario, we considered the negation of the task as a possible attack. We also targeted shared information and its security attributes, which are accountability, traceability, confidentiality, and integrity [35]. The next source of inspiration was studies of insider attacks [36] as the robots in the swarm have the role of an insider. In combination with attacks found in papers, we assigned at least seven different attacks for each scenario in Section 3.2. As the last step, we clustered the attacks into a taxonomy in the Figure 1.

According to the possible issues occurring in the scenarios, we have created these eight clusters:

- Information Manipulation or Ignoring
- Manipulation with Communication Channels
- False Performance Promises
- Authority misusing
- Physical attacks
- Attacks on Internal Intelligence
- Decision making attacks

Some of the scenarios mentioned above are subtasks of the other discussed ones. This fact leads to a transitive transfer of susceptibility to attacks from one scenario to another. Therefore, we decided

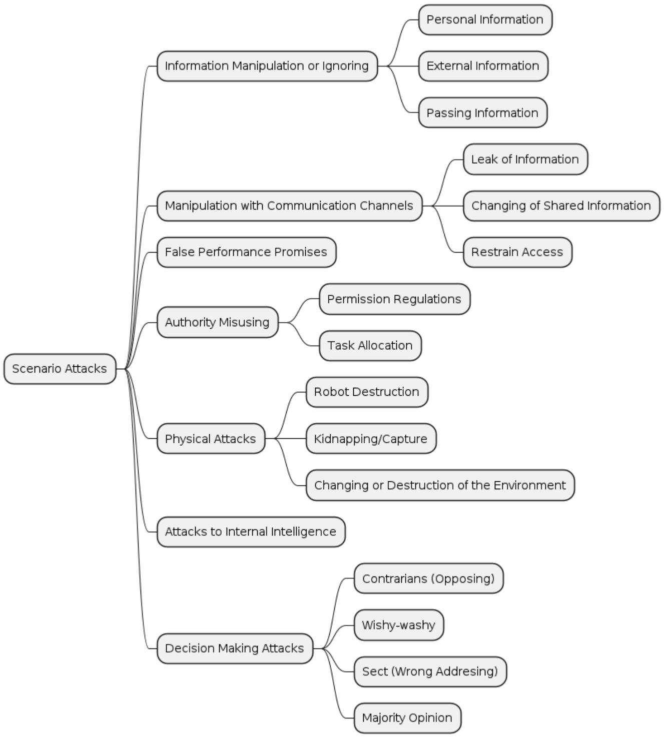

Figure 1: Proposed taxonomy of attacks.

to always list all possible attack-vulnerable scenarios, including the transitive ones.

The groups are described in the next sections.

4.2 Information Manipulation or Ignoring

Any modification of information and its dissemination, lying about its status or the status of other objects, robots, or ignoring instructions, which is an issue related to all scenarios, altogether causes significant problems in evaluating the next steps during the mission [31]. We have classified these actions according to the type of erroneous information from the perspective of the individual into three sections:

4.2.1 Individual Information. The robot is passing information about itself that others cannot validate, like misleading sensor data, its future motion, or information about its charged battery. Spoofing [37] in general is also misleading with individual information. If sensors are the target, it is called sensor spoofing [38], where the attacker manipulates the distances between robots and affects the instructions to the other members of the swarm.

Scenarios related to this problem: R1, R2, R3, R4, R5, R6, R7, R8, R9, M1, M2, M3, M4, M5, M6, M7, M8, M9, M10, M11, S1, S2, S3, S4, S5 (I3, I7), S6 (D3, D4, D5, D6, D7), O4, O5

Trust Solution. Each individual can be assigned a trust score managed by a centralized or decentralized reputation model [39], which is updated based on the interactions and experience of the robots, and help other robots to decide on the trustworthiness of the individual and its information.

4.2.2 External Information. The robot informs about its observation of its surroundings, which concerns other robots or objects in the environment and their attributes, like weight or size. In this scenario, the robot also serves as the information source but describes facts verifiable by the others.

Scenarios related to this problem: R1, R2, R3, R4, R5, R6, R9, M5, M6, M7, M11, S5 (I4, I5, I6, I8, I9), S6 (D1, D2, D3, D6, D7), O1, O2, O3, O4, O5

Trust Solution. Each interaction can be paired with a validation of the action, which can be used to feed the update of the trust score of the robot who shared it.

4.2.3 Passing the Information. Passing the information means the robot receives information from other sources (robot or server) and passes it to the next one. This scenario is the only one where the robot is not the source of the information but only a mediator, which does not mean it cannot modify it.

Scenarios related to this problem: R1, R2, R3, R4, R5, R6, R7, R8, R9, M1, M2, M3, M4, M5, M6, M9, M10, M11, S2, S3, S4, S5 (I1, I2, I5), S6 (D1), O1, O2, O3, O4, O5

Trust Solution. Information passing could be propagated via established trusted peer groups [5], which would enable information sharing only to trusted robots (i.e. friends) and access to peer opinion in case of doubt.

4.3 Manipulation with Communication Channels

Communication and information exchange is crucial for the mission's success. Pieces of information can be manipulated as described in Section 4.2. This category focuses on the weaknesses of passing and storing of data, while the content of messages is put aside here. Overall, even a leak of the position and size of the swarm may be dangerous, as during foraging, mapping, and localization, a leak of found resources' position and features can cause their loss.

4.3.1 Leak of Information. A leak of information is a kind of insider attack when a robot misuses its privileges and shares secret information with unauthorized entities. This may lead to resource theft or better-targeted attacks.

Scenarios related to this problem: R2, R5, R8, R9, M2, M3, M11, S5 (I4), O3

Trust Solution. A lower level of trust in a potentially malicious robot should lead to its lower trust score within the ecosystem and in effect its lower privileges and, therefore, less information provided to them. In case of a sudden loss of trust in an individual, we can change the position of the swarm or resources to make their knowledge irrelevant.

4.3.2 Changing of Shared Information. Many AI algorithms work with shared sources of information, which individuals update to find a solution together as a group without repeating mistakes and searching. This shared information source can be a single point of failure when malicious robots change recorded data, and therefore, the rest of the group works with false information.

Scenarios related to this problem: R2, R5, R7, R9, M2, S2, S5 (I4, I5), O1, O3, O4, O5

Trust Solution. Robots with low trust scores could only have read-only access to the information. Individual robots can consider accepting information updates based on their author's trust score. In such a case, it is crucial that the trust scores are managed by a reputation model [39] that is tailored to the context of swarm robotics.

4.3.3 *Restrain Access.*

The work of the swarm robots is based on distributed communication and sharing of information. Therefore, interference with communication and signals can be a real threat to the mission. Malicious robots can, for example, prevent signal transmission by overloading the communication channel with a high amount of irrelevant messages.

Scenarios related to this problem: R1, R2, R3, R4, R5, R6, R7, R8, R9, M1, M2, M3, M4, M5, M6, M8, M9, M10, M11, S1, S2, S3, S4, S5 (I1, I3, I4, I5, I6, I9), S6 (D1, D2, D3, D4, D5, D6, D7), O1, O2, O3, O4, O5

Trust Solution. Well-designed trust solution could support the isolation of misbehaving robots from the environment, or deny their access to communication channels.

4.4 False Performance Promises

Many missions are time-critical. These missions may be sabotaged by individuals promising task completion within a time that is not realistic (even because the individual has no intention of completing the task). When the group does not question the behavior of the malicious individual, they will wait for an unnecessarily long time, even with some timeout set up. Repeatedly broken promises may lead to critical time loss and mission failure.

Scenarios related to this problem: R2, R5, R6, R7, R9, M4, O1, O2

Trust Solution. Variable trust rates between individuals can support proper labor division where the most time-critical tasks are assigned to the most trusted individuals. Timeout for waiting for task completion may also vary based on the trust rate.

4.5 Authority Misusage

In swarm systems whose intelligence is not strictly distributed and uses any kind of hierarchy or leadership, problems may arise when malicious robots obtain leader roles. They can manipulate other robots to do unwanted things, and it is harder to detect and eliminate them because leaders usually have access to more information and can give out orders without explanation.

4.5.1 *Permission Regulations.*

In the role of authority in the swarm with a hierarchy of rights, a malicious robot may have permission to change the rights of other robots. This way, they could, for example, deny other robots access to some information or resources.

Scenarios related to this problem: S6 (D2)

Trust Solution. Untrusted robots could be excluded from superior roles and prevented from manipulating the rights of other robots. Alternatively, the decisions by borderline-trust-score robots could undergo supervision or check by another trusted robot to make sure the decision is not discrimination against another individual.

4.5.2 *Task Allocation.*

Leaders often give orders to subordinates to simplify and speed up the process of decision-making and choosing the next steps in the missions. Malicious leaders can force other robots to unwanted and destructive actions, which can abort the whole mission. When a malicious robot gains a leadership role, it can hijack the whole swarm and manipulate it towards its individual goals.

Scenarios related to this problem: S6 (D2, D5)

Trust Solution. A malicious leader can be evaluated as untrusted based on the given orders and other actions in a process where its subordinates can provide evidence and a superior can perform the evaluation. After evaluating a leader as untrusted, various actions can be taken to ensure ecosystem safety (replacing it in its role, double checking its actions, isolating it from the ecosystem).

4.6 Physical Attacks

Many attacks are based on inter-robot communication and information sharing and manipulation. In robotics, we also have to think about the hardware and surroundings of the robots, which significantly affect their mission. It is impossible to isolate working robots from physical threats without limiting their capabilities, but with the use of trust, we can try to isolate potential attackers from the working environment and, that way, protect it and the swarm.

4.6.1 *Robot Destruction.*

Usually, the most extreme type of attack is the physical destruction of an individual or even a whole group of robots. A malicious robot can attack their colleague at any time, during any type of mission. Some attacks can be stealthy or can cause more harm, for example, by leading the group to some kind of trap.

Scenarios related to this problem: R1, R2, R3, R4, R5, R6, R7, R8, R9, M1, M2, M3, M4, M5, M6, M7, M8, M9, M10, M11, S1, S2, S3, S4, S5 (I1, I3, I4, I5, I6, I8, I9), S6 (D1, D2, D3, D4, D5, D6, D7), O1, O2, O3, O4, O5

Trust Solution. In an ideal situation, a potential attacker would not be accepted into the ecosystem of robots or would be detected and isolated. In case the untrusted robot is inside the swarm, the rest of the robots could still keep affecting its trust score via reporting on their interactions with it, so that protective action can be taken once a suspicious comes about an intent to cause damage.

4.6.2 *Kidnapping/Capture.*

Being kidnapped is a problem for the single robot and the whole group as capabilities are reduced, information may leak, or even the kidnapped robot can be misused. Robots can be kidnapped when other robots lead them to dangerous or hostile areas or simply carry them away. Without trust measurement between robots, an individual connects and goes with anyone from their group. Therefore, a single malicious robot may convince many others to leave their mission and willfully fall into enemy hands.

Scenarios related to this problem: R1, R2, R3, R4, R5, R6, R7, R8, R9, M1, M2, M3, M4, M5, M6, M7, M8, M9, M10, M11, S1, S2, S3, S4, S5 (I1, I3, I4, I5, I6, I8, I9), S6 (D1, D2, D3, D4, D5, D6, D7), O1, O2, O3, O4, O5

Trust Solution. If the robots were capable of distrusting others, they would be more durable against kidnapping. It is true that distrust cannot always prevent an involuntary physical displacement, but at least it can lead to excluding the misbehaving robot from the group. In the best case, the robot capable of kidnapping would not even be accepted into the swarm.

4.6.3 *Changing or Destruction of the Environment.* Missions of swarm robots usually include interaction with their surroundings, either during a movement, or the goal itself can include searching the environment. Changing or destroying the environment may make orientation in space more difficult or even lead to the complete failure of the mission.

Scenarios related to this problem: R1, R2, R3, R4, R5, R6, R7, R9, S5 (I7, I8), S6 (D6, D7), O1, O2, O3, O4, O5

Trust Solution. Similarly to previous types of physical attacks, the elimination of the potential attacker before they cause any harm can prevent unwanted destruction of the environment. The untrusted robot may be more properly observed by the rest and prevented from approaching mission-critical items.

4.7 Attacks on Internal Intelligence

Swarm robots usually use distributed intelligence to accomplish the mission, but each individual within the swarm has its inner intelligence mechanism, too. These mechanisms can have variable complexity, and if known to the enemy, they can attack specifically to the mechanism’s weaknesses. There are many intelligence mechanisms, especially machine learning models, with specific types of possible weaknesses that can exploited by malicious robots. This category covers all of them, as their more detailed taxonomy is not relevant to our taxonomy of attacks. Feeding false information to the robot’s learning model may lead to unreasonable behavior. Some more complex attacks may cause bias against some opinions or individuals. Targeted changes in learning data can also make the victim overlook some kind of information or behavior.

Scenarios related to this problem: R1, R2, R3, R4, R5, R6, R7, R8, R9, M1, M2, M3, M4, M5, M6, M7, M8, M9, M10, M11, S1, S2, S3, S4, S5 (I1, I2, I3, I4, I5, I6, I7, I8, I9), S6 (D1, D2, D3, D4, D5, D6, D7), O1, O2, O3, O4, O5

Trust Solution. The data used for learning may be observed and weighted by the author’s trust score. In case of distrust, the robot can ignore the data or have it verified. Designers of the robot can also consider more rigid models and regularly check robot’s bias.

4.8 Decision Making Attacks

Attacks on the robot’s decision-making can impact the outcome of the process or delay reaching an agreement with the rest of the swarm. It is essential to prioritize the decision-making process to avoid this significant shortcoming.

4.8.1 *Contrarians (Opposing).* This means always opposing the majority of the group, which leads to the slowing down of the decision process [40].

Scenarios related to this problem: R1, R2, R5, R6, R7, R8, R9, M1, M2, M3, M4, M5, M6, M9, M10, M11, S1, S2, S3, S4, S6 (D1), O1, O2, O3, O5

Trust Solution. Create a trust decay system where team members who consistently dissent without contributing positively see their trust scores gradually diminish over time. However, team members can regain their reputation through sustained constructive contributions.

4.8.2 *Wishy-Washy.* Another type of slowing down the decision, but in this case the robot is constantly changing his opinion. This behavior can escalate to a deadlock [40].

Scenarios related to this problem: R1, R2, R5, R6, R7, R8, R9, M1, M2, M3, M4, M5, M6, M9, M10, M11, S1, S2, S3, S4, S6 (D1), O1, O2, O3, O5

Trust Solution. Design collaborative stability evaluation and peer-based assessment, which allows other robots or entities in the system to provide input on the trustable stability of a given robot.

4.8.3 *Sect.* A group of robots that does not change its opinion in any circumstance, i.e. does not take into account whether the situation evolves or not. Ignoring environmental information is related to Section 4.2 [40].

Scenarios related to this problem: R1, R2, R5, R6, R7, R8, R9, M1, M2, M3, M4, M5, M6, M9, M10, M11, S1, S2, S3, S4, S6 (D1), O1, O2, O3, O5

Trust Solution. Trust scores extended by new dynamic metrics could be influenced by the ability of robots to adapt their behavior in response to new information or changes in the environment.

4.8.4 *Majority Opinion.* Enables the owner of the group majority to influence the result according to his needs. The process is similar to the blockchain 51% problem.

Scenarios related to this problem: R1, R2, R5, R6, R7, R8, R9, M1, M2, M3, M4, M5, M6, M9, M10, M11, S1, S2, S3, S4, S6 (D1), O1, O2, O3, O5

Trust Solution. Introduce a distributed trust score system that assesses each owner’s historical contributions, reliability, and decision outcomes. Scores dynamically adjust based on quality and alignment.

5 DISCUSSION

While there is extensive research on swarm robotics, a comprehensive overview of its scenarios together with attacks on them that could be addressed with trust management approaches, is so far missing. These topics cannot be neglected as we cannot expect all robots within the swarm to be well-behaved, with no intention to disrupt the mission. Our proposed attack taxonomy and possible trust solutions may be only an initial systematic attempt in this direction, but still providing an important stepping stone towards the trust management research in swarm robotics, which may lead to more reliable usability of swarm robotics in the real world.

The collected swarm robotics scenarios and attack taxonomy can serve as a base for the following research on attack prevention using trust. We only gave initial hints towards possible trust solutions of attacks in Section 4. These can now be extended and deepened by proposing more concrete solutions and methods. The application of trust techniques may affect the original scenarios; therefore, they should be adapted to their usage. Finally, the whole construct may be applied to some concrete system or mission.

6 CONCLUSION

In this paper, we collected swarm robotics scenarios and attacks from current research and proposed a taxonomy of both, which can serve as a stepping stone for future research in trust management in swarm robotics. For each category, we suggested the possible application of trust management to prevent the attack or reduce its consequences. These trust applications are our proposal for future research directions, which should lead to more detailed and concrete methods.

ACKNOWLEDGMENTS

The work was supported by Grant Agency of Masaryk University (GAMU), Interdisciplinary Research Projects sub-programme, project "Forensic Support for Building Trust in Smart Software Ecosystems" (no. MUNI/G/1142/2022).

REFERENCES

[1] Rafael Capilla, Emilia Cioroaica, Barbora Buhnova, and Jan Bosch. On autonomous dynamic software ecosystems. *IEEE Transactions on Engineering Management*, 69(6):3633–3647, 2022.

[2] Levent Bayındır. A review of swarm robotics tasks. *Neurocomputing*, 172:292–321, 2016.

[3] Fiona Higgins, Allan Tomlinson, and Keith M Martin. Threats to the swarm: Security considerations for swarm robotics. *International Journal on Advances in Security*, 2(2&3), 2009.

[4] Yogesh Kumar Sharma and Ashish Bagla. Security challenges for swarm robotics. *SECURITY CHALLENGES*, 2(1):45–48, 2009.

[5] Subhash Sagar, Adnan Mahmood, Quan Z Sheng, Jitander Kumar Pabani, and Wei Emma Zhang. Understanding the trustworthiness management in the social internet of things: A survey. *arXiv preprint arXiv:2202.03624*, 2022.

[6] Zhi Yan, Nicolas Jouandeau, and Arab Ali Cherif. A survey and analysis of multi-robot coordination. *International Journal of Advanced Robotic Systems*, 10(12):399, 2013.

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

[8] Rachael N Darmanin and Marvin K Bugeja. A review on multi-robot systems categorised by application domain. In *2017 25th mediterranean conference on control and automation (MED)*, pages 701–706. IEEE, 2017.

[9] Iñaki Navarro and Fernando Matía. An introduction to swarm robotics. *Isrn robotics*, 2013:1–10, 2013.

[10] Levent Bayindir and Erol Şahin. A review of studies in swarm robotics. *Turkish Journal of Electrical Engineering and Computer Sciences*, 15(2):115–147, 2007.

[11] Marco Dorigo, Mauro Birattari, and Manuele Brambilla. Swarm robotics. *Scholarpedia*, 9(1):1463, 2014.

[12] Markus Hannebauer, Jan Wendler, Enrico Pagello, Luca Iocchi, Daniele Nardi, and Massimiliano Salerno. Reactivity and deliberation: a survey on multi-robot systems. In *Balancing Reactivity and Social Deliberation in Multi-Agent Systems: From RoboCup to Real-World Applications*, pages 9–32. Springer, 2001.

[13] Jan Carlo Barca and Y Ahmet Sekercioglu. Swarm robotics reviewed. *Robotica*, 31(3):345–359, 2013.

[14] Ahmad Reza Cheraghi, Sahdia Shahzad, and Kalman Graffi. Past, present, and future of swarm robotics. In *Intelligent Systems and Applications: Proceedings of the 2021 Intelligent Systems Conference (IntelliSys) Volume 3*, pages 190–233. Springer, 2022.

[15] Manuele Brambilla, Eliseo Ferrante, Mauro Birattari, and Marco Dorigo. Swarm robotics: a review from the swarm engineering perspective. *Swarm Intelligence*, 7:1–41, 2013.

[16] Yara Rizk, Mariette Awad, and Edward W Tunstel. Cooperative heterogeneous multi-robot systems: A survey. *ACM Computing Surveys (CSUR)*, 52(2):1–31, 2019.

[17] Pollyanna G Faria Dias, Mateus C Silva, Geraldo P Rocha Filho, Patricia A Vargas, Luciano P Cota, and Gustavo Pessin. Swarm robotics: A perspective on the latest reviewed concepts and applications. *Sensors*, 21(6):2062, 2021.

[18] Cindy Calderón-Arce, Juan Carlos Brenes-Torres, and Rebeca Solis-Ortega. Swarm robotics: Simulators, platforms and applications review. *Computation*, 10(6):80, 2022.

[19] Qin Yang and Ramviyas Parasuraman. How can robots trust each other for better cooperation? a relative needs entropy based robot-robot trust assessment model. In *2021 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pages 2656–2663. IEEE, 2021.

[20] Sanjaya Mallikarachchi, Can Dai, Oshani Seneviratne, and Isuru Godage. Managing collaborative tasks within heterogeneous robotic swarms using swarm contracts. In *2022 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, pages 48–55. IEEE, 2022.

[21] Jianan Li, Jun Wu, Jianhua Li, Ali Kashif Bashir, Md Jalil Piran, and Ashiq Anjum. Blockchain-based trust edge knowledge inference of multi-robot systems for collaborative tasks. *IEEE Communications Magazine*, 59(7):94–100, 2021.

[22] Muhammad Salek Ali, Massimo Vecchio, Miguel Pincheira, Koustabh Dolui, Fabio Antonelli, and Mubashir Husain Rehmani. Applications of blockchains in the internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 21(2):1676–1717, 2018.

[23] Erol Şahin. Swarm robotics: From sources of inspiration to domains of application. In *International workshop on swarm robotics*, pages 10–20. Springer, 2004.

[24] Belkacem Khaldi and Foudil Cherif. An overview of swarm robotics: Swarm intelligence applied to multi-robotics. *International Journal of Computer Applications*, 126(2), 2015.

[25] Ying Tan and Zhong-yang Zheng. Research advance in swarm robotics. *Defence Technology*, 9(1):18–39, 2013.

[26] Melanie Schranz, Martina Umlauft, Micha Sende, and Wilfried Elmenreich. Swarm robotic behaviors and current applications. *Frontiers in Robotics and AI*, page 36, 2020.

[27] Nadia Nedjah and Luneque Silva Junior. Review of methodologies and tasks in swarm robotics towards standardization. *Swarm and Evolutionary Computation*, 50:100565, 2019.

[28] Yogeswaran Mohan and SG Ponnambalam. An extensive review of research in swarm robotics. In *2009 world congress on nature & biologically inspired computing (nabic)*, pages 140–145. IEEE, 2009.

[29] Aleksis Liekna, Janis Grundspenkis, et al. Towards practical application of swarm robotics: overview of swarm tasks. *Engineering for rural development*, 13:271–277, 2014.

[30] Tucker Balch. Communication, diversity and learning: Cornerstones of swarm behavior. In *International workshop on swarm robotics*, pages 21–30. Springer, 2004.

[31] Eduardo Castelló Ferrer, Thomas Hardjono, Alex Pentland, and Marco Dorigo. Secure and secret cooperation in robot swarms. *Science Robotics*, 6(56):eabf1538, 2021.

[32] Yara Khaluf, Emi Mathews, and Franz J Rammig. Self-organized cooperation in swarm robotics. In *2011 14th IEEE International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing Workshops*, pages 217–226. IEEE, 2011.

[33] Frederick Ducatelle, Gianni A Di Caro, Carlo Pinciroli, Francesco Mondada, and Luca Gambardella. Communication assisted navigation in robotic swarms: self-organization and cooperation. In *2011 IEEE/RSJ International Conference on Intelligent Robots and Systems*, pages 4981–4988. IEEE, 2011.

[34] Christian Blum and Daniel Merkle. *Swarm intelligence: introduction and applications*. Springer Science & Business Media, 2008.

[35] Nazila Gol Mohammadi, Sachar Paulus, Mohamed Bishr, Andreas Metzger, Holger Koennecke, Sandro Hartenstein, and Klaus Pohl. An analysis of software quality attributes and their contribution to trustworthiness. In *CLOSER*, pages 542–552, 2013.

[36] Salvatore J Stolfo, Steven M Bellovin, Shlomo Hershkop, Angelos D Keromytis, Sara Sinclair, and Sean W Smith. *Insider attack and cyber security: beyond the hacker*, volume 39. Springer Science & Business Media, 2008.

[37] Xinyu Huang, Yunzhe Tian, Yifei He, Endong Tong, Wenjia Niu, Chenyang Li, Jiqiang Liu, and Liang Chang. Exposing spoofing attack on flocking-based unmanned aerial vehicle cluster: A threat to swarm intelligence. *Security and Communication Networks*, 2020:1–15, 2020.

[38] Yingao Yao, Pritam Dash, and Karthik Pattabiraman. Poster: May the swarm be with you: Sensor spoofing attacks against drone swarms. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pages 3511–3513, 2022.

[39] Barbora Buhnova. Trust management in the Internet of Everything. In *European Conference on Software Architecture. ECSA 2022 Tracks and Workshops.*, pages 123–137. Springer, 2023. Preprint at http://arxiv.org/abs/2212.14688.

[40] Francesco Canciani, Mohamed S Talamali, James AR Marshall, Thomas Bose, and Andreagiovanni Reina. Keep calm and vote on: Swarm resiliency in collective decision making. In *Proceedings of workshop resilient robot teams of the 2019 ieee international conference on robotics and automation (ICRA 2019)*, volume 4, 2019.