IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 11, 2021, accepted November 4, 2021, date of publication November 15, 2021,
date of current version November 24, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3128287

Systematic Mapping Study of Security in Multi-Embedded-Agent Systems

ARTHUR BAUDET[1], OUM-EL-KHEIR AKTOUF[1], ANNABELLE MERCIER[1], AND PHILIPPE ELBAZ-VINCENT[2]

[1]LCIS, Grenoble INP, Université Grenoble Alpes, 26000 Valence, France
[2]Institut Fourier, CNRS, Université Grenoble Alpes, 38000 Grenoble, France

Corresponding author: Arthur Baudet (arthur.baudet@lcis.grenoble-inp.fr)

This work was supported by the French National Research Agency in the framework of the "Investissements d'avenir" Program under Grant ANR-15-IDEX-02.

ABSTRACT **Context:** In this paper, we study distributed and decentralized systems in which each part is modeled as an agent in a multi-agent system. Those systems provide more scalable and easier ways to control complex, distributed and interconnected systems of embedded components. We are particularly interested in methods to secure these systems. **Objectives:** This study aims to identify the main security properties studied, the parts of a multi-agent architecture that are considered most often in security studies and the technical solutions used to secure those systems. **Methods:** We conducted a systematic mapping study on research works addressing the security of multi-agent systems with embedded agents. We identified which security features were addressed, and their roles in global security architecture. **Results:** We identified 70 papers published in journals and conferences. We classified the extracted data reporting a tendency to focus on securing the availability of systems under attack by means of trust schemes, sometimes supported by cryptographic primitives. **Conclusion:** The use of cryptography appears to be limited in decentralized systems. However, solutions should be provided to overcome those limits as other solutions such as trust schemes do not protect the system from the same type of attacks.

INDEX TERMS Decentralized security, embedded system, multi-agent system, security architecture, systematic mapping study.

I. INTRODUCTION

Thanks to their high scalability, multi-agent systems are increasingly used to coordinate and organize the ever-increasing networks and systems of connected devices. Whether they are wireless sensors or autonomous vehicles, the need for security to make the users confident when using such systems with their personal data and safety is increasing.

In this context, we focus on systems that can be modeled as Multi-Embedded-Agent Systems. Such systems act as multi-agent systems with each agent embedded in a connected device. For example, they can be Wireless Sensor Networks (WSNs), Mobile Area Networks (MANETs) or Vehicular Area Networks (VANETs). We focus on these kinds of systems as they are an interesting solution to decentralized control of connected devices but have specific security needs (detailed in Section II-B). However, we are not interested in multi-agent systems hosted in a single computer that control remote devices, as in the 4.0 Industry, or in systems of mobile agents that can move from one host platform to another.

The attack surface of multi-embedded-agent systems spans from hardware to software vulnerabilities and adds new attack vectors related to their particularity: attacks can also come from corrupted or infiltrated agents taking advantage of the absence of a central authority and coordination to harm the system, hijacking the cooperation process to their own benefit. To use the multi-embedded-agent system model in critical systems such as networks of autonomous vehicles, the academic and industrial communities need to find solutions that cover the whole attack surface. As the system under study is decentralized, so should be the security solution. Otherwise, it would impose constraints (such as having a

The associate editor coordinating the review of this manuscript and approving it for publication was Vivek Kumar Sehgal.

connection to a distant server) that are impossible to satisfy in the studied system.

The main motivation for our work is to understand the current state-of-the-art in security solutions in multi-agent systems and all similar systems. A quantitative analysis of the current work in this domain will help identify possibly missing parts of a security architecture we aim to propose in future work; the results of our study will also help fellow researchers focus and contribute to less studied aspects of this domain.

Following the guidelines of [1] and [2] on how to conduct systematic mapping studies, we structured the remainder of the paper as follows: section II presents the background of our studies and related works. The research used methodology to lead this search is explained in section III. The results are detailed in section IV. Finally, we conclude and present future research directions in section V.

The data and details of each step of the systematic mapping study process and the complete list of selected papers can be found online [3].

II. BACKGROUND AND RELATED WORK

A. MULTI-EMBEDDED-AGENT SYSTEMS

We define multi-embedded-agent systems as a specific subclass of multi-agent systems.

There are many definitions of multi-agent systems because they are used in many application fields [4]–[6]. From the software engineering perspective [6]–[9], a multi-agent system represents a complex system with more than two agents, which collaborate to achieve a global behavior and reach a global result. Each agent has a level of autonomy and achieves its own goal (local result).

Generally, an agent is an intelligent entity such as ''a computer system, located in some environment, which is capable of flexible and autonomous actions in order to meet its design objectives'' [10]. In this context, autonomy relates to several concepts [11]. First, an agent is proactive, so it does not necessarily require intervention from its users or designers to adapt or change its flow of actions regarding its goals. It can deny working with other agents if their goals are not in line with its own. However, as it may also need the cooperation of other agents, it is capable of negotiating [12], convincing or being convinced [13]. Last, it is reactive and can adapt its behavior according to its environment or past experience.

In multi-agent systems and multi-embedded-agent systems, there is generally no central entity coordinating the agents. Consequently, system-level decisions are distributed among agents, thus requiring high levels of autonomy in the decision-making process, from the individual agents.

The main difference between multi-agent systems and multi-embedded-agent systems is that in the latter, the agents are embedded systems. The embedded feature adds constraints such as energy management, safety management, or other issues related to mobility, communications and integrity of the agents in a physical environment [14]. We focus in particular on multi-embedded-agent systems and distinguish them from systems of mobile agents [15] and multi-agent systems as software architectures [16].

B. SECURITY IN MULTI-EMBEDDED-AGENT SYSTEMS

Securing a multi-embedded-agent system means securing an information system by providing confidentiality, integrity and availability [17] to minimize the vulnerability of assets and resources [18] but also securing a heavily networked system that needs authentication, authorization and accounting [18] for each agent relies on communications with other agents to achieve its goals.

However, it also means addressing specific threats to multi-agent systems: agents rely on each other to achieve their goals and malicious agents can infiltrate the system to thwart it. As there is no central authority to rely on, the agents need to autonomously distinguish between malicious and trustworthy peers.

Last, since agents are embedded software, they also suffer from hardware vulnerabilities ranging from side-channel attacks to any spoofing, eavesdropping or modification of their communication that are usually performed through wireless media.

In the following, we distinguish between preventive security and security by detection. The first includes cryptography, language-level security, security policies or methodological system development to produce sound and secure systems. The second refers to intrusion detection systems, monitoring or trust models to discover and manage threats at run-time.

C. RELATED WORKS

The survey by [19] provides insight into security and challenges in multi-agent systems but focuses mainly on mobile software agents, which have different challenges from the multi-agent systems of interest in our study, where the ''host'' is not a separated entity.

Reference [20] presents extensive work on attack modeling taxonomy. Their paper focuses on open multi-agent systems of mobile agents but not on the specificities of mobility. However, the reviewed solutions make hypotheses that cannot always be satisfied in multi-embedded-agent systems; e.g., they rely on a security framework such as in JADE [21] that is not designed to include embedded constraints on agents.

Reference [22] provides thorough descriptions of general computer security, multi-agent systems and the application of security principles for multi-agent systems. However, only software multi-agent systems are considered.

In addition, though somewhat interesting, all three studies were published in 2012 and consequently do not cover most of the work conducted in the last decade.

More recent studies, [23]–[25], are also related to our work but each covers only a part of the systems we study.

Reference [23] covers more devices (agents in our case) centric systems but with a focus on hardware and physical sensor/actuator limitations.

Some applications of the works reviewed in [24] are also of interest because the studied systems rely on wireless communication before being connected to the Internet. Furthermore, Internet of Things devices are perfect candidates to create multi-embedded-agent systems as they share some embedded-agent features such as self-configuration or a strong link to their physical environment.

Last, the WSN studied in [25] is also an excellent example of possible application of multi-embedded-agent systems. Except for the base, the sensors fit most of the feature of embedded agents: resource limitations, large-scale deployment, wireless communication, strong link to their environment and even the need to aggregate information can be modeled as cooperation.

Using a more formal approach to literature study in the form of a systematic mapping study [26], our paper intends to review the work done on all systems that could be modeled as multi-embedded-agent systems. Our work focuses on the security properties, the technological solutions and the studied security architecture parts. Other related works such as [22], [25] are either too specific in their applications or too old to satisfy our needs.

III. RESEARCH METHODOLOGY

Reference [1] defines systematic mapping studies as studies that "are designed to provide a wide overview of a research area, to establish if research evidence exists on a topic and provides an indication of the quantity of the evidence." A systematic mapping study is broader than a systematic literature study [26] in its search and data extraction stage and aims to summarize the results. However, the methodology used remains the same as a systematic literature study, so we followed the guidelines provided by [1], [2], [26] to perform our study. An overview of the search process flow we followed is given in Fig. 1.

A. RESEARCH QUESTIONS

The goal of this mapping study is to determine security practices in multi-embedded-agent systems to propose a generic security architecture. We aim to cover as many security needs as necessary with a focus on the least covered needs. This leads to the following research questions (RQs):

- **RQ1** What are the main security properties studied in multi-embedded-agent systems?
- **RQ2** What are the specific technical solutions for securing multi-embedded-agent systems?
- **RQ3** Which parts of a global security architecture for multi-embedded-agent systems are studied?

B. SEARCH STRATEGY

As suggested in [27], we describe our search strategy by answering the following questions:

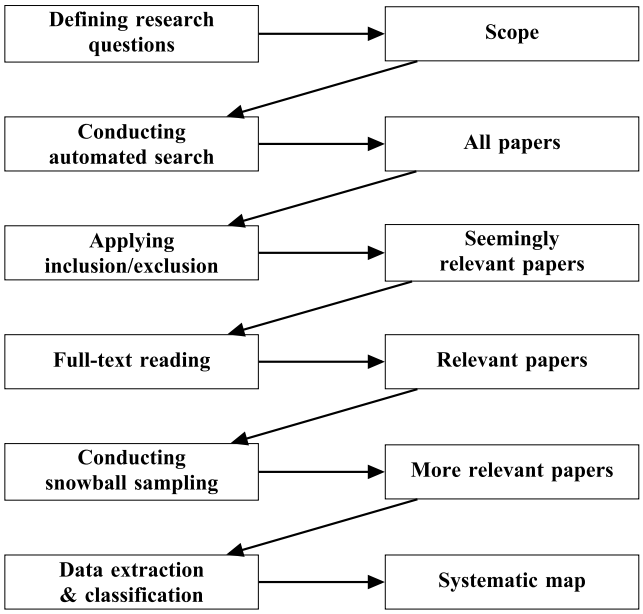

FIGURE 1. Search process flow.

- **Which?** We followed a two-step search strategy: an automated search followed by a backward snowballing once the relevant papers from the automated search were identified. We first gathered all the results of the main venues for our field of research and applied two filtering processes (from inclusion/exclusion criteria and then full-text reading). Then, we applied one iteration of snowball sampling to the references of the included papers.
- **Where?** We used electronic databases from the four main venues in our research field: [28]–[31].
- **What?** We aimed to provide an overview of the efforts made to secure multi-embedded-agent systems from a security architecture point of view. We hence derived our search string from those two main topics: "multi-agent system" and "embedded agent" from "embedded multi-agent system" and "authentication," "authorization," "confidentiality" and "integrity" from "security architecture." This resulted in the following search string:

```
("multi-agent system" OR "embedded
multi-agent system" OR "embedded
agent") AND ("security architecture"
OR "authentication" OR
"authorization" OR "confidentiality"
OR "integrity")
```

  We limited ourselves to eight Boolean operators as it was the limit for one of the search engines we used and remained purposely broad on the terms not to bias the results on a specific part of a security architecture.
- **When?** The study included works from 2010-01-01 to the date of the search, 2020-08-27. As cybersecurity has evolved substantially in recent decades, we kept only the most recent works.

C. STUDY SELECTION

We applied the following criteria:

Inclusion:

- Papers that propose a security solution for multi-embedded-agent systems;
- Papers that propose a security solution for a multi-agent system with no hypothesis on the type of agents (that may as well be embedded);
- Papers that propose a security solution for a system that can be modeled as a multi-embedded-agent system (see Section II for examples of such systems).

Moreover, we included papers referring to systems not characterized as multi-agent systems by the authors but that we could model as multi-embedded-agent systems. Examples of such systems are as follows:

- Robot communities;
- Wireless Sensor Networks;
- Mobile Ad Hoc Networks;
- Vehicular Area Networks;
- Some Internet of Things setups;
- Some Cyber-physical systems setups.

The exclusion criteria were as follows:

- Secondary or tertiary studies;
- Papers not available in English;
- Papers not available in full text;
- Papers not subjected to peer reviews.

We also excluded papers referring to multi-agent systems as software architectures with all their components running on a single machine with a process per agent. Examples of such systems are as follows:

- Cloud-enabled computing (centralized, has no constraints on energy, computation power. . .);
- Mobile agents (as they are purely software agents);
- Multi-agent systems using the Web (communications are done through web technologies with very few limitations);
- Multi-agent systems studied from an automation point of view.

We also found a considerable number of papers presenting trust schemes or enhancements of trust schemes for multi-agent systems. We only included papers proposing trust schemes (and not an enhancement of one) for the specific case of multi-embedded-agent systems or related cases.

Last, we kept ''borderline'' papers, papers that satisfied almost but not all our inclusion criteria. Our goal was first, to keep them to the full-text reading stage to be sure not to dismiss them too early and second, to add them to the included papers as starting points for the snowball sampling process.

D. DATA EXTRACTION

We extracted the relevant data to our search from the papers using the form presented in Table 1.

For the *security property* field, we listed which elements of the CIA and AAA models (see below) were taken into account in the studies. To this end, we did not try to deduce more than what the authors were presenting but only checked if keywords or related wording were present in the papers.

TABLE 1. Data extraction form.

General data	
Id	A unique identifier used to refer to the paper
DOI	The DOI or ISSN or URL of the paper
Publication date	The date of publication
Title	The title of the paper
Authors	The list of authors of the paper
Study specific data	
Application field	The system modeled as multi-embedded-agent systems
Architecture part	The part of a security architecture the authors focus on
Security property	The security properties the authors focus on
Threat	The threat model or attacks considered by the contribution of the paper
Technology	The technical solutions used in the contribution of the paper

Although not directly related to the research questions, we added the Application field and Threat classification to better understand extracted data.

AAA model, from network security:

- Authentication
- Authorization
- Accounting/Non-repudiation

CIA model, from information security:

- Confidentiality
- Integrity
- Availability

Furthermore, we differentiated the confidentiality and integrity of data in transit between agents, referred to as ''communication confidentiality'' and ''communication integrity'') and data at rest, data stores and accessible by specific agents, referred to as ''data confidentiality'' and ''data integrity.''

E. ANALYSIS AND CLASSIFICATION

Except for the *application field*, the classification criteria are not exclusive. A paper can propose a solution to secure two or more security properties using two or more technical solutions and contributing to two or more parts of the security architecture. This means that the exact numbers shown on the different graphs should be used with care.

As we will explain in Section IV, we determined during the backward snowball sampling that there were many papers that we could qualify as multi-agent due to their characteristics (decentralized systems, autonomous subsystems. . .) but that were not characterized as such by their authors. Therefore, we decided to quantify the impact of those papers in our research. This is why we introduced the field *application field* in our extraction form.

We also added a *threat* field to give more context on the analysis of our results on security properties.

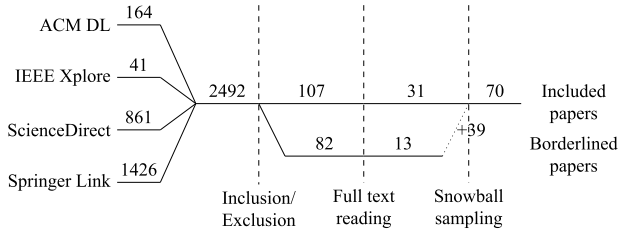

FIGURE 2. Evolution of the number of papers through the selection process.

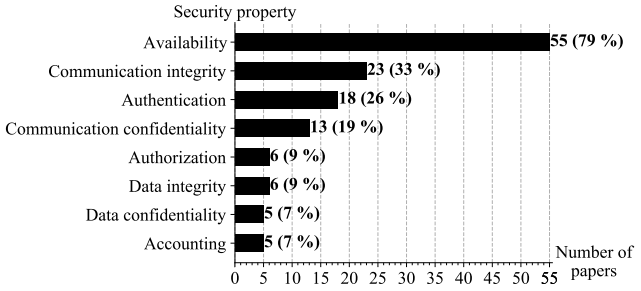

FIGURE 3. Number of papers studying each security property (details can be found in Table 4).

F. VALIDITY EVALUATION

Concerning the work in [32], the main threat to validity and especially to reproducibility is the subjectivity of the interpretations of the extracted data. Only the classification concerning the security properties was considered in the preparation stage as we had no hypothetical values range for the other data extraction fields.

This leads us to a second threat, the misclassification of primary studies, that can arise when all the classes cannot be considered at the beginning of the study. To mitigate it, we did several iterations of the classification process to refine our classification scheme each time.

Last, a threat to validity specific to our study is a broader than expected application field of multi-agent system solutions. The results of the snowball sampling will be discussed in more detail in Section IV but we found during the snowball sampling stage numerous papers in several fields of research, such as WSNs or MANETs, using multi-agent solutions or at least with the same features as multi-agent systems without naming them multi-agents. Therefore, for more detailed results on multi-agent systems, those research fields should also be included by using the keywords MANET or WSN in the initial search. The present study was not sized to include them; doing so would have added more than five thousand papers to the initial search results, but some of the works are represented as a result of the snowball sampling search.

IV. RESULTS

As illustrated in Fig. 2, from the 2492 papers obtained in initial search on the four main editor search tools, we selected 31 using inclusion and exclusion criteria and then added 39 from a backward snowball sampling on the included and borderline papers for a total of 70 resulting papers. The detailed dataset including the list of the 70 papers with their corresponding ID can be found online [3] and a list of the selected papers is given in Table 3.

The unexpectedly high number of added papers during snowball sampling for such a study must be put in perspective. First, snowball sampling was performed from the references of the included papers and the borderline papers. Sixteen of the added papers were found from references in borderline papers. Moreover, most of the added documents would not have been found during the initial search because they did not include the multi-agent system keyword but proposed a system that we could model as a multi-agent system, e.g., a MANET with autonomous nodes.

A. STUDIED SECURITY PROPERTIES (RQ1)

For each selected paper, we identified the security properties targeted by the proposed solution and represented obtained results in Fig. 3. As the solutions did not always target one unique security property, the sum of the numbers on the lines does not correspond to the number of papers. Nevertheless, we can see that most, $\frac{55}{70} \approx 79\%$, of the proposed solutions in the selected papers had the objective of preserving the availability of the system under attack. The second and one-third most studied properties were the integrity of the communications and the authentication, but less than a third of the solutions considered them.

Such a prominent interest in system availability can be explained by one of the specificities of multi-agent systems, namely the need for inter-agent cooperation. Even if every information system requires confidentiality on a certain level, and every distributed system requires preserving integrity of the intra-system communications, multi-agent systems can be particularly vulnerable to malicious systems acting as agents and trying to disrupt their operation. Following this reasoning, we were surprised that authentication was not more studied but we were able to determine an explanation in several papers, including [33]–[35]. Indeed, authentication relies heavily on cryptography and, as we will present in Section IV-B, the use of cryptography in multi-embedded-agent systems can be challenging and has limited results.

To better understand our results, we compared the security properties with the threats presented in the papers. The resulting graph is shown in Fig. 4. This graph shows that, even if availability is the most encountered as the main priority, attacks related to communication between agents are studied in half of the cases so communication integrity is more relevant than the results in Fig. 3 show. Details about the attacks are shown in Fig. 5 and Table 6. We classified the attacks according to the used means and the achieved goals. Most of the works studied internal attacks, so attacks from one or more malicious agents. Very few attack models were described but we presumed that the attackers had total control over the network since the communications were done over

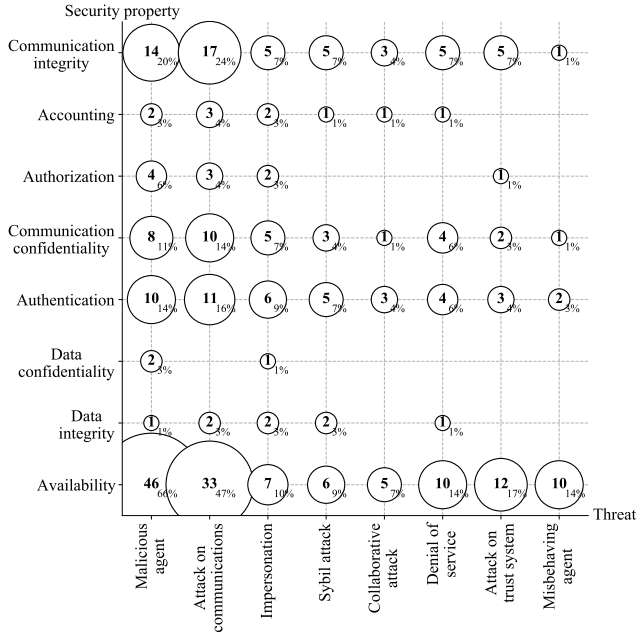

FIGURE 4. Distribution of accounted threats depending on the targeted security properties.

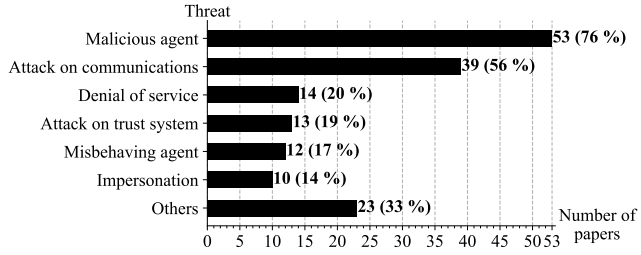

FIGURE 5. Threat consideration in the selected papers (details can be found in Table 6).

wireless technologies. Thus, the communications were the first part of the system to be attacked. Even though they could be considered as attacks on the communications, we differentiated denial of service attacks as they do not target specific security properties except availability, whereas attacks on the message content relate to availability and communication integrity. Last, we differentiate malicious and misbehaving agents as the latter implies that the attacker will only abuse the organization, by unnecessarily requiring help or refusing to help other agents for example, while not tampering or intercepting message content. This distinction allows us to understand that even if the attacks are coming from inside, they rarely happen at the organization level. Only 17% of the papers studied this threat.

B. TECHNICAL SOLUTIONS FOR SECURING MULTI-EMBEDDED-AGENT SYSTEMS (RQ2)

As shown in Fig. 6, 37% of the papers use cryptographic schemes to secure their system under attack and 64% of the papers propose the use of trust schemes. These trust schemes allow agents to detect malicious and misbehaving

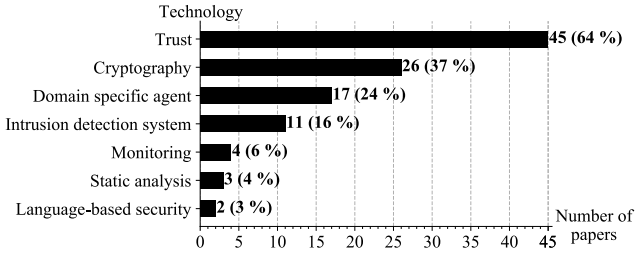

FIGURE 6. Number of papers using each technical solution (details can be found in Table 2).

agents and to exclude them from the system. They can be seen as a decentralized intrusion detection system and should not be confused with works aiming at increasing the trust from the user to the computer system: the trust is computed by each agent regarding the other agents. The scarce use of cryptography in securing multi-embedded-agent systems, which is paramount to secure almost any computer systems, may be explained by the fact that, according to [33]–[35], cryptography suffers from two drawbacks when used in this context: (i) it does not protect the system from internal attacks (from malicious agents for example) and (ii) it requires a central third-party entity to manage the cryptographic keys. Last, the features arising from the use of cryptography (e.g., confidentiality, integrity, or authentication) are not specifically needed in multi-embedded-agent systems, so authors may assume that they were addressed earlier in the design of these systems.

As trust schemes are a large domain, we only focused on trust schemes specifically targeting multi-agent systems, but many other works also applies in this context. As shown in Fig. 4 they are essentially used to protect, at least the availability of the system: they aim to exclude any agent not behaving as expected by their peers. This also means that less effective or faulty agents can also be excluded even if they are not malevolent.

In Table 2, we can see that papers 2, 10, 17, 27, 30, 33, 34, 37, 38, 45, 50, 51, 52, 56, and 65 rely on cryptographic primitives to enhance their trust schemes (e.g., for authorization or identification). In a context where an attacker has total control over the communication media, it seems unrealistic to rely on exchanged messages to compute the trust of other agents as any message could have been tampered with. Moreover, non-authenticated agents could also deny their implication in malevolent acts or change their identity to clean their slate.

Last, we can see that a quarter of the solutions rely on new agents deployed specifically, the domain-specific agents, rather than adapting the applicative agents, the agents fulfilling the system tasks, to carry the security solutions. Examples of such domain-specific agents include agents storing a Blockchain to decrease the cost in energy or computation to run a Blockchain for the application, or agents logging the communications to detect intruders, being responsible for a specific task in a new security scheme such as storing keys or

TABLE 2. Details on the number of papers using each technical solution.

Technology	Paper id
Trust	0, 2, 3, 5, 9, 10, 12–18, 20, 22, 23, 25, 27–30, 32–38, 40–45, 47, 50–53, 55–58, 63, 65
Cryptography	2, 4, 6, 7, 10, 11, 17, 21, 27, 30, 31, 33, 34, 37–39, 45, 50–52, 54, 56, 60, 64, 65, 68
Domain specific agent	1–3, 6, 7, 9, 24, 30, 39, 42, 46, 47, 50, 54, 60, 61, 64
Intrusion detection system	26, 48, 49, 51, 59, 61, 62, 66–69
Monitoring	1, 5, 24, 46
Static analysis	0, 8, 54
Language-based security	8, 19

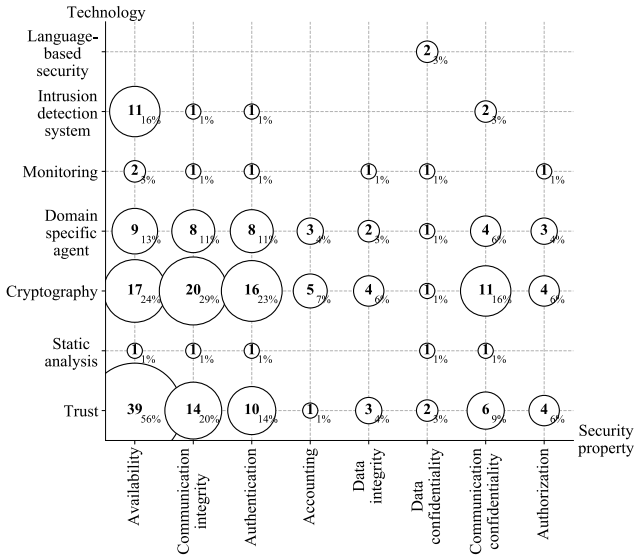

FIGURE 7. Distribution of technical solutions depending on the targeted security properties.

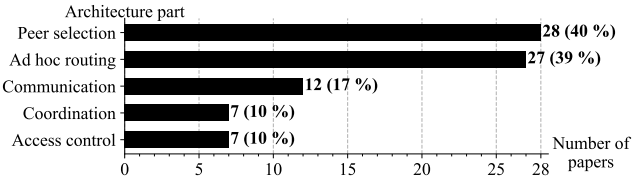

FIGURE 8. Number of papers studying each part of a multi-agent architecture (details can be found in Table 5).

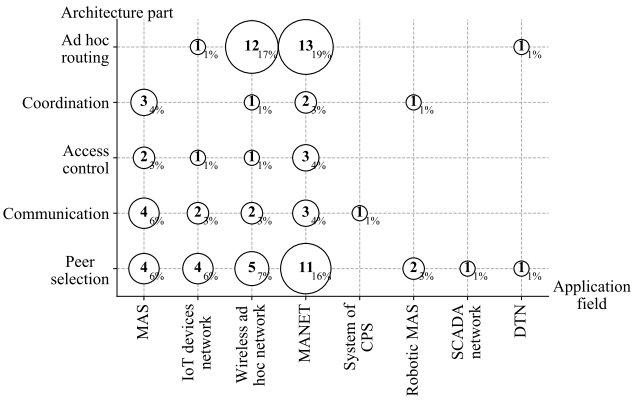

FIGURE 9. Distribution of secured multi-agent architecture parts depending on the type of system, which the multi-agent system is deployed on. (*MAS: Multi-Agent System, IoT: Internet of Things, MANET: Mobile Ad hoc NETwork, CPS: Cyber-Physical System, SCADA: Supervisory Control And Data Acquisition, DTN: Delay Tolerant Network*).

access rules. While the use of specific agents helps decrease the weight of the security solutions on the applicative system, they may be problematic to use in certain conditions as new security agents should be deployed to replace failing ones as long as the system is running. Consequently, specific agents could prove to be more costly than simply deploying more capable applicative agents.

C. STUDIED ARCHITECTURE PARTS (RQ3)

To avoid redundancy with RQ2, we focused on classifying the studied security architecture parts on the multi-agent specificities. We collected the part of the multi-embedded-agent system architecture that was secured in each paper. Similarly as for RQ1, the need for cooperation between agents seems to be the main motivation. In particular, how to choose the right agent for cooperation or to route messages. In this specific case, peer selection and ad hoc routing are mutually exclusive, even if the second one can be seen as a subcategory of the first one. We distinguished them first because of the number of their occurrences and second because, as we can see in Fig. 9, the study of ad hoc routing is mainly done in wireless and mobile ad hoc networks. Those two application fields are the most predominant, but they are not the only fields with multi-agent solutions. See Figure 10 and Table 7 for the distribution of application fields in our study.

None of the papers investigated hardware security. This was no surprise as the field of hardware security is comprehensive and not specific to multi-agent systems, wireless networks, sensor networks or mobile area networks. Nonetheless, it should not be forgotten that any software security solution relies on the underlying hardware security, so, to ultimately secure a multi-embedded-agent system, suitable solutions from hardware security works should also be studied.

Overall, we can see that the papers focus on choosing the suitable agents to cooperate with rather than on how they would do so. Similarly as before, this can be explained as giving a choice to the agents to find the most suitable peers to work with is a specificity of multi-agent systems while wireless communication, coordination and access control also exist in other fields.

V. CONCLUSION

This systematic mapping study covered 70 papers selected from 2500 over 4 different editor databases and aimed at identifying and classifying the needs of security in multi-embedded-agent systems and the provided solutions to meet those needs.

We discussed the benefits and limitations of the most commonly used solutions, applying trust schemes to distinguish between malevolent and trustworthy agents to cooperate with. That type of solutions protect the system against malicious

TABLE 3. List of included papers.

ID	Title	Authors	Publication date	DOI
0	An adaptive and Socially-Compliant Trust Management System for virtual communities	Reda Yaich and Olivier Boissier and Philippe Jaillon	2012-03-30	10.1145/2245276.2232112
1	New Security Approach for IoT Communication Systems	Boudhir Anouar Abdelhakim	2018-10-11	10.1145/3286606.3286779
2	Cluster-based secure communication mechanism in wireless ad hoc networks	M.-H. Guo and H.-T. Liaw and D.-J. Deng and H.-C. Chao	2010-12-01	10.1049/iet-ifs.2009.0120
3	Dynamic Role-Based Access Control with Trust-Satisfaction and Reputation for Multi-agent System	Jae Wook Woo and Myung Jin Hwang and Chun Gyeong Lee and Hee Yong Youn	2010-06-07	10.1109/WAINA.2010.63
4	Authentication and load balancing scheme based on JSON Token For Multi-Agent Systems	Badr Eddine Sabir and Mohamed Youssfi and Omar Bouattane and Hakim Allali	2019-02-23	10.1016/j.procs.2019.01.029
5	An intelligent based healthcare security monitoring schemes for detection of node replication attack in wireless sensor networks	S. Anitha and P. Jayanthi and V. Chandrasekaran	2020-07-25	10.1016/j.measurement.2020.108272
6	Attribute-based authentication for multi-agent systems with dynamic groups	Qi Zhang and Yi Mu and Minjie Zhang	2010-06-12	10.1016/j.comcom.2010.06.009
7	Bubbles of Trust: A decentralized blockchain-based authentication system for IoT	Mohamed Tahar Hammi and Badis Hammi and Patrick Bellot and Ahmed Serhrouchni	2018-06-30	10.1016/j.cose.2018.06.004
8	Secure information sharing in social agent interactions using information flow analysis	Shahriar Bijani and David Robertson and David Aspinall	2018-02-03	10.1016/j.engappai.2018.01.002
9	CRiBAC: Community-centric role interaction based access control model	Youna Jung and James B.D. Joshi	2012-02-13	10.1016/j.cose.2012.02.002
10	Impact of trust model on on-demand multi-path routing in mobile ad hoc networks	Hui Xia and Zhiping Jia and Lei Ju and Xin Li and Edwin H.-M. Sha	2012-09-22	10.1016/j.comcom.2012.09.002
11	The open blockchain-aided multi-agent symbiotic cyber–physical systems	Rafał Skowroński	2018-09-13	10.1016/j.future.2018.11.044
12	Trust management for secure cognitive radio vehicular ad hoc networks	Ying He and F. Richard Yu and Zhexiong Wei and Victor Leung	2018-11-22	10.1016/j.adhoc.2018.11.006
13	A cognitive chronometry strategy associated with a revised cloud model to deal with the dishonest recommendations attacks in wireless sensor networks	Farah Khedim and Nabila Labraoui and Ado Adamou Abba Ari	2018-09-06	10.1016/j.jnca.2018.09.001
14	Towards multiple-mix-attack detection via consensus-based trust management in IoT networks	Zuchao Ma and Liang Liu and Weizhi Meng	2020-05-24	10.1016/j.cose.2020.101898
15	An efficient and versatile approach to trust and reputation using hierarchical Bayesian modelling	W.T. Luke Teacy and Michael Luck and Alex Rogers and Nicholas R. Jennings	2012-09-07	10.1016/j.artint.2012.09.001
16	A new evidential trust model for open distributed systems	Liming Jiang and Jian Xu and Kun Zhang and Hong Zhang	2011-09-29	10.1016/j.eswa.2011.09.077
17	Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain	Iván García-Magariño and Raquel Lacuesta and Muttukrishnan Rajarajan and Jaime Lloret	2018-11-27	10.1016/j.adhoc.2018.11.010
18	Trust prediction and trust-based source routing in mobile ad hoc networks	Hui Xia and Zhiping Jia and Xin Li and Lei Ju and Edwin H.-M. Sha	2012-02-25	10.1016/j.adhoc.2012.02.009
19	Probing Attacks on Multi-Agent Systems Using Electronic Institutions	Shahriar Bijani and David Robertson and David Aspinall	2012-01-01	10.1007/978-3-642-29113-5_4
20	Dynamic Trust Management Framework for Robotic Multi-Agent Systems	Igor Zikratov and Oleg Maslennikov and Ilya Lebedev and Aleksandr Ometov and Sergey Andreev	2016-09-28	10.1007/978-3-319-46301-8_28
21	A Decentralised Approach to Task Allocation Using Blockchain	Tulio L. Basegio and Regio A. Michelin and Avelino F. Zorzo and Rafael H. Bordini	2017-05-09	10.1007/978-3-319-91899-0_5
22	A Trust-Based Approach for Detecting Compromised Nodes in SCADA Systems	Francesco Buccafurri and Gianluca Lax and Domenico Rosaci and Antonello Comi	2013-09-20	10.1007/978-3-642-40776-5_20
23	Lightweight trusted routing for wireless sensor networks	Laurent Vercouter and Jean-Paul Jamont	2012-05-24	10.1007/s13748-012-0017-7
24	A Security Response Approach Based on the Deployment of Mobile Agents	Roberto Magán-Carrión and Pedro García-Teodoro and José Camacho	2013-05-24	10.1007/978-3-642-38073-0_16
25	ARMAN: Agent-based Reputation for Mobile Ad hoc Networks	Guy Guemkam and Djamel Khadraoui and Benjamin Gâteau and Zahia Guessoum	2013-05-24	10.1007/978-3-642-38073-0_11
26	Security Computing for the Resiliency of Protecting from Internal Attacks in Distributed Wireless Sensor Networks	Xu Huang and Dharmendra Sharma and Muhammad Ahmed	2012-09-07	10.1007/978-3-642-33078-0_2

TABLE 3. *(Continued.)* **List of included papers.**

27	Mobility Aware Clustering Scheme with Bayesian-Evidence Trust Management for Public Key Infrastructure in Ad Hoc Networks	V. S. Janani and M. S. K. Manikandan	2017-12-13	10.1007/s11277-017-5107-1
28	Trust Model Based on D-S Evidence Theory in Wireless Sensor Networks	Kai Yang and Shuguang Liu and Junwei Shen	2014-11-02	10.1007/978-3-662-46981-1_28
29	An Energy Aware Approach to Trust Management Systems for Embedded Multi-Agent Systems	Arthur Darroux and Jean-Paul Jamont and Oum-El-Kheir Aktouf and Annabelle Mercier	2019-09-10	10.1007/978-3-030-30856-8_9
30	A Cognitive Trust Model for Access Control Framework in MANET	Soumya Maity and Soumya K. Ghosh	2012-12-19	10.1007/978-3-642-35130-3_6
31	FairAccess: a new Blockchain-based access control framework for the Internet of Things	Aafaf Ouaddah and Anas Abou Elkalam and Abdellah Ait Ouahman	2017-02-19	10.1002/sec.1748
32	Trust-based on-demand multipath routing in mobile ad hoc networks	X. Li and Z. Jia and P. Zhang and R. Zhang and H. Wang	2010-12-01	10.1049/iet-ifs.2009.0140
33	Building a Trust-Aware dynamic routing solution for Wireless Sensor Networks	Hongmei Deng and Yi Yang and Guang Jin and Roger Xu and Weisong Shi	2010-12-10	10.1109/GLOCOMW.2010.5700197
34	A Trust Management System for Securing Data Plane of Ad-Hoc Networks	Shuaishuai Tan and Xiaoping Li and Qingkuan Dong	2015-09-27	10.1109/TVT.2015.2495325
35	Dempster-Shafer evidence theory based trust management strategy against cooperative black hole attacks and gray hole attacks in MANETs	Bo Yang and Ryo Yamamoto and Yoshiaki Tanaka	2014-02-19	10.1109/ICACT.2014.6779177
36	Providing trust in wireless sensor networks using a bio-inspired technique	Félix Gómez Mármol and Gregorio Martínez Pérez	2010-02-18	10.1007/s11235-010-9281-7
37	Design And Implementation Of a Trust-Aware Routing Protocol For Large WSNs	Theodore Zahariadis and Leligou Helen and Trakadas Panagiotis and Karkazis Panagiotis	2010-07-01	10.5121/ijnsa.2010.2304
38	Trust Evaluation Based on Node's Characteristics and Neighbouring Nodes' Recommendations for WSN	Shaik Sahil Babu and Arnab Raha and Mrinal Kanti Naskar	2014-08-19	10.4236/wsn.2014.68016
39	Multi-Agent System Protecting from Attacking with Elliptic Curve Cryptography	Xu Huang and Pritam Gajkumar Shah and Dharmendra Sharma	2010-01-12	10.1007/978-3-642-14616-9_11
40	A Distributed Trust Management Mechanism for the Internet of Things Using a Multi-Service Approach	Carolina Veronica Lezama Mendoza and João Henrique Kleinschmidt	2018-09-12	10.1007/s11277-018-5942-8
41	Trust and Reputation Mechanisms for Multi-agent Robotic Systems	Igor A. Zikratov and Ilya S. Lebedev and Andrei V. Gurtov	2014-08-29	10.1007/978-3-319-10353-2_10
42	Trust-Based Cluster Head Selection Algorithm for Mobile Ad Hoc Networks	Raihana Ferdous and Vallipuram Muthukkumarasamy and Elankayer Sithirasenan	2011-11-18	10.1109/TrustCom.2011.76
43	Security Enhancements for Mobile Ad Hoc Networks With Trust Management Using Uncertain Reasoning	Zhexiong Wei and Helen Tang and F. Richard Yu and Maoyu Wang and Peter Mason	2014-04-01	10.1109/TVT.2014.2313865
44	Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks	Rutvij H. Jhaveri and Narendra M. Patel	2016-05-11	10.1002/dac.3148
45	RIPsec – Using reputation-based multilayer security to protect MANETs	T.H. Lacey and R.F. Mills and B.E. Mullins and R.A. Raines and M.E. Oxley and S.K. Rogers	2011-09-28	10.1016/j.cose.2011.09.005
46	A security architecture based on immune agents for MANET	Xia Ye and Junshan Li	2010-02-17	10.1109/ICWCSC.2010.5415918
47	ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks	Wenjia Li and Houbing Song	2015-11-12	10.1109/TITS.2015.2494017
48	Distributed Deployment of Anomaly Detection Scheme in Resource-Limited IoT Devices	Qun Du and Yunkai Wei and Yuming Mao	2019-09-19	10.1109/ICCT46805.2019.8947005
49	A lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology	Hichem Sedjelmaci and Sidi Mohammed Senouci and Mohamad Al-Bahri	2016-06-14	10.1109/ICC.2016.7510811
50	Trust-Based Intrusion Detection and Clustering Approach for Wireless Body Area Networks	Dinesh Kumar Anguraj and S. Smys	2019-01-01	10.1007/s11277-018-6005-x
51	Towards Blockchained Challenge-Based Collaborative Intrusion Detection	Wenjuan Li and Yu Wang and Jin Li and Man Ho Au	2019-08-14	10.1007/978-3-030-29729-9_7
52	A Novel Trust-Aware Geographical Routing Scheme for Wireless Sensor Networks	Theodore Zahariadis and Panagiotis Trakadas and Helen C. Leligou and Sotiris Maniatis and Panagiotis Karkazis	2012-05-15	10.1007/s11277-012-0613-7
53	A trust-based multipath routing framework for Mobile Ad hoc NETworks	Xin Li and Zhiping Jia and Peng Zhang and Haiyang Wang	2010-09-09	10.1109/FSKD.2010.5569349
54	DIPLOMA: Distributed Policy Enforcement Architecture for MANETs	Mansoor Alicherry and Angelos D. Keromytis	2010-11-15	10.1109/NSS.2010.27
55	Cross layer approach to detect malicious node in MANET	Vidya N. Patil and Sandeep A. Thorat	2013-06-06	10.1109/ICCCNT.2013.6726582

TABLE 3. ***(Continued.)*** **List of included papers.**

56	AMD: Audit-Based Misbehavior Detection in Wireless Ad Hoc Networks	Yu Zhang and Author image of Loukas Lazos and Loukas Lazos and William Kozma	2012-12-21	10.1109/TMC.2012.257
57	Reputed Packet Delivery Using Efficient Audit Misbehaviour Detection and Monitoring Method in Mobile Ad Hoc Networks	A. Vijayakumar and K. Selvamani and Arya Pradeep kumar	2015-05-22	10.1016/j.procs.2015.04.124
58	Trust management and adversary detection for delay tolerant networks	Erman Ayday and Hanseung Lee and Faramarz Fekri	2011-01-06	10.1109/MILCOM.2010.5680245
59	Misbehavior nodes detection and isolation for MANETs OLSR protocol	Ahmed M. Abdalla and Imane A. Saroit and Amira Kotb and Ali H Afsari	2011-02-22	10.1016/j.procs.2010.12.020
60	PROVISIONING OF EFFICIENT AUTHENTICATION TECHNIQUE FOR IMPLEMENTING IN LARGE SCALE NETWORKS (PEAT)	S Lingeshwari	2014-12-17	10.20894/IJMSR.117.006.001.006
61	Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks	Uzma Khan and Shikha Agrawal and Sanjay Silakari	2015-04-23	10.1016/j.procs.2015.01.006
62	Power aware malicious nodes detection for securing MANETs against packet forwarding misbehavior attack	Deepika Kukreja and S. K. Dhurandher and B. V. R. Reddy	2017-04-27	10.1007/s12652-017-0496-2
63	Trust-based neighbor selection using activation function for secure routing in wireless sensor networks	Osama AlFarraj and Ahmad AlZubi and Amr Tolba	2018-06-04	10.1007/s12652-018-0885-1
64	BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks	Rongxing Lu and Xiaodong Lin and Haojin Zhu and Xiaohui Liang and Xuemin Shen	2011-03-17	10.1109/TPDS.2011.95
65	Towards a reputation-based routing protocol to contrast black-holes in a delay tolerant network	Gianluca Dini and Angelica Lo Duca	2012-03-24	10.1016/j.adhoc.2012.03.003
66	A Context Adaptive Intrusion Detection System for MANET	Bo-Chao Cheng and Ryh-Yuh Tseng	2010-06-20	10.1016/j.comcom.2010.06.015
67	Swarm based Intrusion Detection and Defense Technique for Malicious Attacks in Mobile Ad Hoc Networks	G. Indirani and K. Selvakumar	2012-07-01	10.5120/7915-9258
68	Algorithms for a distributed IDS in MANETs	P.M. Mafra and J.S. Fraga and A.O. Santin	2013-07-08	10.1016/j.jcss.2013.06.011
69	An intrusion detection & adaptive response mechanism for MANETs	Adnan Nadeem and Michael P. Howarth	2013-09-07	10.1016/j.adhoc.2013.08.017

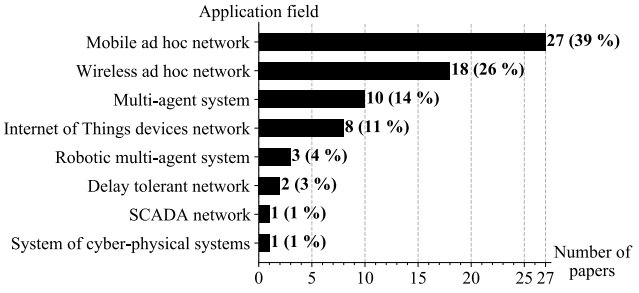

FIGURE 10. **Choices of application fields for multi-agent solutions (details can be found in Table 7).**

agents trying to attack its availability, which seems to be the most studied security property in multi-embedded-agent systems. Nonetheless, protecting the confidentiality and integrity of the transmitted information in the system requires the use of cryptographic primitives in a context in which no central authority can distribute certificates to new agents connecting to the system during runtime for example.

Our paper showed that studies on this topic are very limited in the context of multi-embedded-agent systems. Therefore, this could be a challenging and relevant topic for future work on multi-embedded-agent systems security.

APPENDIX A
LIST OF INCLUDED PAPERS

See Table 3.

TABLE 4. **Details on the number of papers studying each security property.**

Security property	Paper id
Availability	0, 7, 9, 10, 12–16, 18, 20–38, 40, 41, 43, 44, 46–53, 55–59, 61–69
Communication integrity	1, 2, 4, 7, 10–12, 18, 27, 33, 34, 37–39, 45, 50, 52, 54, 56, 60, 64, 65, 68
Authentication	1, 2, 4, 6, 7, 10, 11, 27, 30, 33, 42, 45, 52, 54, 56, 64, 65, 68
Authorization	5, 6, 9, 31, 33, 50
Data integrity	3, 5, 7, 17, 21, 31
Communication confidentiality	4, 6, 10, 12, 39, 45, 52, 54, 56, 60, 65, 67, 68
Data confidentiality	3, 5, 8, 19, 31
Accounting	2, 4, 6, 7, 11

TABLE 5. **Details on the part of a multi-embedded-agent security architecture studied for each paper.**

Architecture part	Paper id
Peer selection	0, 5, 10, 13, 15, 16, 20, 22, 24, 25, 29, 36, 40–42, 46–51, 55, 58–61, 66, 68
Ad hoc routing	2, 10, 14, 18, 23, 26–28, 32–35, 37, 38, 43, 44, 52–54, 56, 57, 62–65, 67, 69
Communication	1, 2, 4, 6–8, 11, 12, 39, 45, 52, 54
Coordination	8, 9, 17, 19, 21, 54, 60
Access control	3, 6, 9, 27, 30, 31, 54

APPENDIX B
CHOICES OF APPLICATION FIELDS FOR MULTI-AGENT SOLUTIONS

See Figure 10.

TABLE 6. Details on threat consideration in the selected papers.

Threat	Paper id
Malicious agent	0, 3, 6, 9–16, 18–20, 22–24, 26–30, 32–38, 40–53, 55–61, 63, 67, 69
Attack on communications	6, 7, 10, 14, 17, 18, 20, 24, 26, 28, 32–35, 37–39, 43–47, 50, 52, 53, 56–65, 67–69
Message replaying	2, 7, 14, 20, 26, 37, 38, 59–64, 68, 69
Denial of service	11, 12, 14, 16, 17, 26, 28, 29, 45, 46, 54, 64, 67, 69
Attack on trust system	13, 15, 16, 25, 27, 37, 40, 45, 47, 50–52, 58
Misbehaving agent	13, 15, 22, 24, 36, 42, 45, 46, 48, 49, 55, 57
Impersonation	5–7, 23, 27, 45, 52, 56, 59, 67
Sybil attack	7, 10, 17, 26–28, 45, 68
Collaborative attack	10, 11, 35, 58, 62, 64
Information leakage	8, 17, 19, 67
Probing	6, 19
Disinformation	17, 41
Chosen ciphertext attack	6

We differentiate malicious and misbehaving agents as a malicious agent will use a composition of a wide range of attacks to harm the system whereas a misbehaving agent will only try to abuse the cooperation with others agents. Misbehaving agent behavior will range from selfishness in refusing to complete a given task to downright abuse by requiring other agents to complete their tasks for them.
The attacks from the Attack on trust system category are the ones specifically targeting trust management systems, e.g., white washing or bad mouthing attacks.

TABLE 7. Details on the choices of application field for multi-agent solutions.

Application field	Paper id
Mobile ad hoc network	10, 12, 17, 18, 24, 25, 27, 30, 32, 35, 42–47, 53–55, 57, 59, 61, 62, 66–69
Wireless ad hoc network	2, 3, 5, 13, 23, 26, 28, 33, 34, 36–38, 50, 52, 56, 60, 63, 64
Multi-agent system	0, 4, 6, 8, 9, 15, 16, 19, 29, 39
Internet of Things devices network	1, 7, 14, 31, 40, 48, 49, 51
Robotic multi-agent system	20, 21, 41
Delay tolerant network	58, 65
SCADA network	22
System of cyber-physical systems	11

APPENDIX C
DETAILS ON THE GRAPHS OF THE FIGURES 3, 5, 8, AND 10

See Tables 4–7.

REFERENCES

[1] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," School Comput. Sci. Math. Keele Univ. Dept. Comput. Sci. Univ. Durham, Keele, U.K., Tech. Rep. EBSE-2007-01, 2007. [Online]. Available: http://jnoll.nfshost.com/cit816-spring-19/topics/slrs/Kitchenham_2007%_Guidelines.pdf
[2] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Inf. Softw. Technol.*, vol. 64, pp. 1–18, Aug. 2015.
[3] A. Baudet, O.-E.-K. Aktouf, A. Mercier, and P. Elbaz-Vincent. (2021). *Systematic Mapping Study of Security in Multi-Embedded-Agent Systems Dataset*. [Online]. Available: https://zenodo.org/record/4590885
[4] P. Leitao, V. Marik, and P. Vrba, "Past, present, and future of industrial agent applications," *IEEE Trans. Ind. Informat.*, vol. 9, no. 4, pp. 2360–2372, Nov. 2013.
[5] J. P. Müller and K. Fischer, *Application Impact of Multi-agent Systems and Technologies: A Survey*. Berlin, Germany: Springer, 2014, pp. 27–53.
[6] J.-P. Jamont and M. Occello, "Meeting the challenges of decentralised embedded applications using multi-agent systems," *Int. J. Agent-Oriented Softw. Eng.*, vol. 5, no. 1, pp. 22–68, 2015.
[7] M. S. Greenberg, J. C. Byington, and D. G. Harper, "Mobile agents and security," *IEEE Commun. Mag.*, vol. 36, no. 7, pp. 76–85, Jul. 1998.
[8] M. N. Huhns and L. M. Stephens, "Multiagent systems and societies of agents," *Multiagent Syst., Modern Approach Distrib. Artif. Intell.*, vol. 1, no. 42, pp. 79–114, 1999.
[9] M. Wooldridge and N. R. Jennings, "Intelligent agents: Theory and practice," *Knowl. Eng. Rev.*, vol. 10, no. 2, pp. 115–152, 1995.
[10] N. R. Jennings, K. Sycara, and M. Wooldridge, "A roadmap of agent research and development," *Auto. Agents Multi-Agent Syst.*, vol. 1, pp. 7–38, Jan. 1998.
[11] C. Carabelea, O. Boissier, and A. Florea, "Autonomy in multi-agent systems: A classification attempt," in *Agents and Computational Autonomy*, vol. 2969. Berlin, Germany: Springer, 2003, pp. 103–113.
[12] D. Calvaresi, K. Appoggetti, L. Lustrissimi, M. Marinoni, P. Sernani, A. F. Dragoni, and M. Schumacher, "Multi-agent systems' negotiation protocols for cyber-physical systems: Results from a systematic literature review," in *Proc. 10th Int. Conf. Agents Artif. Intell.*, 2018, pp. 224–235.
[13] J. Dix, S. O. Hansson, G. Kern-Isberner, and G. R. Simari, "Belief change and argumentation in multi-agent scenarios," *Ann. Math. Artif. Intell.*, vol. 78, nos. 3–4, pp. 177–179, Dec. 2016.
[14] C. Barnier, O.-E.-K. Aktouf, A. Mercier, and J.-P. Jamont, "Toward an embedded multi-agent system methodology and positioning on testing," in *Proc. IEEE Int. Symp. Softw. Rel. Eng. Workshops (ISSREW)*, Oct. 2017, pp. 239–244.
[15] H. Idrissi, "Anonymous ECC-authentication and intrusion detection based on execution tracing for mobile agent security," *Wireless Pers. Commun.*, vol. 94, no. 3, pp. 1799–1824, Jun. 2017.
[16] O. Boissier, R. H. Bordini, J. F. Hübner, and A. Ricci, "Dimensions in programming multi-agent systems," *Knowl. Eng. Rev.*, vol. 34, p. e2, 2019.
[17] C. P. Pfleeger and S. L. Pfleeger, *Security in Computing*, 4th ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2006. [Online]. Available: https://www.pearson.com/us/higher-education/product/Pfleeger-Security-i%n-Computing-4th-Edition/9780132390774.html
[18] D. Trcek, *Managing Information Systems Security and Privacy*, no. 1. Berlin, Germany: Springer, 2006. [Online]. Available: https://www.springer.com/gp/book/9783540281030
[19] S. V. Nagaraj, "Securing multi-agent systems: A survey," in *Advances in Computing and Information Technology*, vol. 176. Berlin, Germany: Springer, 2012, pp. 23–30.
[20] S. Bijani and D. Robertson, "A review of attacks and security approaches in open multi-agent systems," *Artif. Intell. Rev.*, vol. 42, no. 4, pp. 607–636, Dec. 2014.
[21] F. Bellifemine, A. Poggi, and G. Rimassa, "Developing multi-agent systems with JADE," in *Intelligent Agents VII Agent Theories Architectures and Languages*, vol. 1986. Berlin, Germany: Springer, 2001, pp. 89–103.
[22] R. C. Cavalcante, I. I. Bittencourt, A. P. da Silva, M. Silva, E. Costa, and R. Santos, "A survey of security in multi-agent systems," *Expert Syst. Appl.*, vol. 39, no. 5, pp. 4835–4846, 2012.
[23] W. U. Guangyu, J. Sun, and J. Chen, "A survey on the security of cyber-physical systems," *Control Theory Technol.*, vol. 14, no. 1, pp. 2–10, 2016.
[24] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, "Internet of Things: Evolution and technologies from a security perspective," *Sustain. Cities Soc.*, vol. 54, Mar. 2020, Art. no. 101728.
[25] D. E. Boubiche, S. Athmani, S. Boubiche, and H. Toral-Cruz, "Cybersecurity issues in wireless sensor networks: Current challenges and solutions," *Wireless Pers. Commun.*, vol. 16, no. 6, pp. 1–37, 2020.
[26] J. Biolchini, P. G. Mian, A. C. C. Natali, and G. H. Travassos, "Systematic review in software engineering," COPPE UFRJ, Rio de Janeiro, Brazil, Tech. Rep. RT-ES 679/05, 2005. [Online]. Available: https://www.cos.ufrj.br/uploadfile/es67905.pdf
[27] H. Zhang, M. A. Babar, and P. Tell, "Identifying relevant studies in software engineering," *Inf. Softw. Technol.*, vol. 53, pp. 625–637, Jun. 2011.
[28] ACM. (2020). *ACM Digital Library Advanced Search Tool*. [Online]. Available: https://dl.acm.org/search/advanced
[29] IEEE. (2020). *IEEE Xplore Advanced Search Tool*. [Online]. Available: https://ieeexplore.ieee.org/search/advanced
[30] Springer Nature. (2020). *Springer Search Tool*. [Online]. Available: https://link.springer.com/search
[31] Elsevier B.V. (2020). *Sciencedirect Advanced Search Tool*. [Online]. Available: https://www.sciencedirect.com/search

[32] X. Zhou, Y. Jin, H. Zhang, S. Li, and X. Huang, "A map of threats to validity of systematic literature reviews in software engineering," in *Proc. 23rd Asia–Pacific Softw. Eng. Conf. (APSEC)*, 2016, pp. 153–160.
[33] R. H. Jhaveri and N. M. Patel, "Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks," *Int. J. Commun. Syst.*, vol. 30, no. 7, p. e3148, May 2017.
[34] X. Li, Z. Jia, P. Zhang, R. Zhang, and H. Wang, "Trust-based on-demand multipath routing in mobile ad hoc networks," *IET Inf. Secur.*, vol. 4, no. 4, pp. 212–232, 2010.
[35] V. N. Patil and S. A. Thorat, "Cross layer approach to detect malicious node in MANET," in *Proc. 4th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2013, pp. 1–6.

ARTHUR BAUDET received the B.S. and Engineering degrees in computer science and networks from the Esisar Engineering School, Grenoble INP, Valence, France, in 2017 and 2019, respectively. He is currently pursuing the Ph.D. degree in computer science with Université Grenoble Alpes.

He is also working with the LCIS, Grenoble INP, Université Grenoble Alpes. His current research interest includes security issues in distributed decentralized systems, such as multi-agent systems, with a focus on systems of embedded devices.

OUM-EL-KHEIR AKTOUF received the master's and Ph.D. degrees in computer science from the Grenoble Institute of Technology, in 1993 and 1997, respectively.

After a two-year of postdoctoral position, she has been an Associate Professor with the Esisar Engineering School and the LCIS, Grenoble INP, Université Grenoble Alpes, since 1999. She was also a Visiting Professor on sabbatical leave at the Department of Computer Engineering, San José State University, CA, USA, for the period 2014–15. Her teaching activities include operating systems, real time systems, distributed computing and computing systems dependability. She has supervised or co-supervised almost 15 Ph.D. candidates, postdoctoral researchers, and research and development engineers. She has taken part as the principal investigator or a scientific contributor on 12 funded research projects and contracts. Her research interests include dependability, safety and security of embedded and interconnected applications and systems (sensor-based applications and multi-embedded agent systems) using runtime tests, diagnosis, and monitoring approaches.

ANNABELLE MERCIER received the master's degree in computer science with University Nice Sophia Antipolis on the theme of contractualization of component-based software and nonfunctional properties, and the Ph.D. degree from the School of Mines of St Étienne.

During her thesis in information retrieval domain at the St Étienne School of Mines, she participated at international information retrieval campaigns (TREC, CLEF) to test her approach on several benchmarks. Since 2007, she has been an Associate Professor with the Université Grenoble Alpes and a Researcher with the LCIS. She also studied services composition. Her teaching activities include web programming and administrative data processing. She has supervised or co-supervised three Ph.D. candidates, postdoctoral researchers, and research and development engineers. Her main research interest includes the detection of collective products provided by autonomous systems.

PHILIPPE ELBAZ-VINCENT was a Marie Curie Fellow of the EU and has held visiting research positions at IHES, France, EPFL, Switzerland, MPI für Mathematik, Bonn, Germany, and the Hausdorff Research Institute for Mathematics, Bonn, from 1998 to 1999. He is currently a Professor of mathematics with the Université Grenoble Alpes, France, where he has been leading the Cybersecurity Institute, since 2018. He has supervised approximately 30 alumni (Ph.D., postdoctoral scholars, and research and development engineers) and has been the (co)head or partners of more than 20 funded research projects, most often involving industrial partners. His research interests include number theory, cryptography, code obfuscations, and information theory.