IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Digital Object Identifier

Security of Multi-Agent Cyber-Physical Systems: A Survey

RICHARD OWOPUTI[1], (Student Member, IEEE), and SANDIP RAY[2], (SENIOR MEMBER, IEEE)

[1]Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611 USA (e-mail: rowoputi@ufl.edu)
[2]Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611 USA (e-mail:sandip@ece.ufl.edu)

Corresponding author: Richard Owoputi (e-mail: rowoputi@ufl.edu).

This research has been supported by the National Science Foundation under Grant No. CNS-1908549.

ABSTRACT Multi-agent systems are becoming increasingly popular due to their successful implementation in several sectors. However, there are a variety of threats that might undermine the agent's security and imperil system security. As a result, security concerns should be addressed during the design of multi-agent systems. This survey reviews different models for securing multi-agent systems, which were developed based on the concepts regarding the agent's role and communications. This paper presents and categorizes the most common attacks on MASs. Then, we study and analyze numerous security strategies in the literature, classifying them as prevention, detection, and resiliency approaches based on reputation and trust. Finally, we recommend which security approach is the best countermeasure for specific types of attacks based on recent advances in the research field.

INDEX TERMS Cyber Physical System, Multi Agent Systems, Resiliency, Security

I. INTRODUCTION

THE term *multi-agent system* (MAS) is used to refer to a cyber-physical system composed of a collection of autonomous entities (or agents) that collaborate to solve a task. The term "agent" here denotes anything that perceives its environment and takes actions autonomously without direct or continuous supervision from any centralized control. The use of multiple agents (rather than a single, centralized entity) induces additional flexibility resulting from the possibility for different agents to perceive different aspects of the environment and make independent judgments while facilitating coordination and knowledge sharing [1]–[3]. Furthermore, using multiple agents induces redundancy and heterogeneity that fosters robustness against failure of individual components [4].

With the increasing advancement of Artificial Intelligence, connectivity, sensors, and robotics, the use of MASs is emerging into many critical applications, including military, space, manufacturing, electronic business, supply chain management, and many others. However, these agents move in uncertain and adversarial environments, making their activities unreliable and unsafe. It is challenging to detect malicious agents that transmit harmful communication messages. These malicious agents can lead to undesirable effects like the leakage of sensitive information or the destruction of the agents in a mission-critical scenario. It is imperative to provide security mechanisms to guarantee the tenets of security such as the confidentiality, integrity, availability, accountability, and non-repudiation of the various autonomous agents and systems that might face [5].

Over the last decade, there has been significant research on various facets of MAS security. This includes exploration and identification of various attack mechanisms on the one hand and novel techniques to mitigate such attacks on the other. Nevertheless, — and despite its great need — we did not find a comprehensive survey of the area that provides a holistic view of the challenges, progress made in the research, and limitations of the current state of the art.

The goal of this paper is to provide a comprehensive, systematic overview of the research in the security of MASs. We develop a systematic categorization of research advances in various aspects of both attacks and defenses, point out the constraints and tradeoffs within which they must operate, and state-of-the-art limitations.

The rest of the paper is organized as follows. Section II gives a tutorial overview of MASs and various categorizations developed from the perspective of security. We review the attacks on MASs in Section III. We divide the discussion

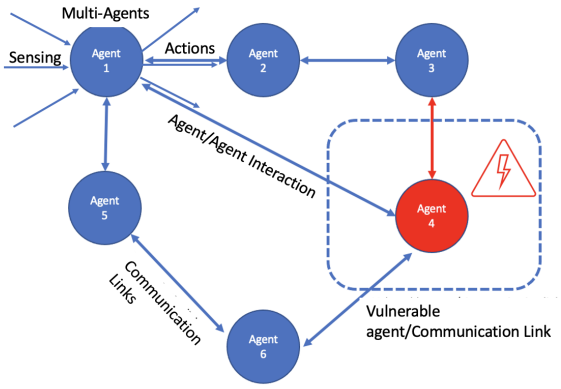

FIGURE 1: An Example MAS Containing a Vulnerable Agent

of security solutions or "defenses" into three categories: prevention (Section IV-A), detection (Section IV-B) and resiliency (Section IV-C). We conclude in Section V.

II. MULTI-AGENT SYSTEMS

Russell and Norvig [6] defines an agent as "a flexible, autonomous entity capable of perceiving the environment through the sensors connected to it." The agent senses different parameters that are used to make a decision based on the goal of the entity. This definition of agents is based on several keywords, e.g., "entities," "environment," and "parameters." Each *agent* aims to complete its assigned work while adhering to certain additional constraints, such as a deadline. To achieve this objective, the agent first senses *parameters* from the *environment*. Vested with this data, the agent can accumulate knowledge about the environment. An agent might also use the knowledge of its neighbors. This knowledge, along with the record of the previous actions taken and the goal, is fed to an extrapolation engine that decides on the agent's appropriate action.

Dorri et al. [7] discuss the features that enabled agents to solve complex tasks. These features include sociability, autonomy, and proactivity. *Sociability* is the ability of the agents to socialize with other agents. *Autonomy* allows the agents to make autonomous decisions. *Proactivity* provides agents with the ability to predict future actions using their history of past occurrences, information from other agents, and sensed parameters. In general, MASs attempt to solve complicated issues through agent collaboration. Furthermore, many MASs are deployed without centralized control, and their data is often decentralized. To strengthen MAS security, it is necessary to address the security of individual agents and the security of the interaction between the various agents. To fully comprehend agents, [8], [9] represented MASs as a graph, with the vertices of the network representing autonomous agents and the edges of the graph representing communication links between the agents.

Different previous papers have developed different ways

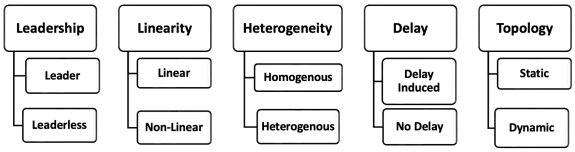

FIGURE 2: Characteristics of Multi Agent Systems

to classify MASs in terms of security features. The different classifications expose different facets of MAS designs and applications in the context of security. Here we briefly review some of these different categorizations to give a flavor of the different contexts. Nevertheless, in our own description of attacks (Section III), we eschew the classifications based on MAS features and find it convenient to develop a taxonomy of the attacks themselves.

Dorri et al. [7] consider the architectural characteristics of MASs and their role in security. They characterize MASs based on the following features.

- *Leadership.* A MAS with a leader enables "centralized decision-making" in the sense that actuation or conflict resolution is controlled by one central agent. In contrast, a leaderless MAS would operate through consensus.
- *Linearity.* In linear MAS, an agent's behavior is based on environmental characteristics that are perceived by the system. An example of this is when a robot in a multi-robot system detects a direct barrier and pauses. The agent behaviors in a nonlinear system are not exclusively reliant on the environmental characteristics that are perceived.
- *Heterogeneity.* A system is homogeneous if each agent has the same features and functionalities, heterogeneous otherwise. Heterogeneous agents have a variety of characteristics, actions, and rules. For instance, a sensor network where protocols only depend on how many sensors send any given signal is an homogeneous system
- *Delay.* The agents in the MAS might take delay into consideration when performing their tasks. In a scenario without delay, the MAS does not consider processing and communication time.
- *Topology.* The topology of a MAS can be static or dynamic. In a static topology, the position and relations of an agent remain unchanged over the lifetime of the agent. In dynamic topology, the agent's location and connections change while the agents form new communication and move from one place to another.

On the other hand, there have been efforts to create taxonomy of MASs based on security vulnerabilties. Trcek [10] defined the role of cybersecurity to be the minimization of vulnerabilities of assets and resources. The term "vulnerabilities" is generally attributed to a weakness in the system that, if discovered by an adversary, might be exploited, causing loss and damage to the system [5]. Vulnerabilities can also be defined as a secret passageway enables an adversary control in a system to perform malicious actions. Pfleeger et al.

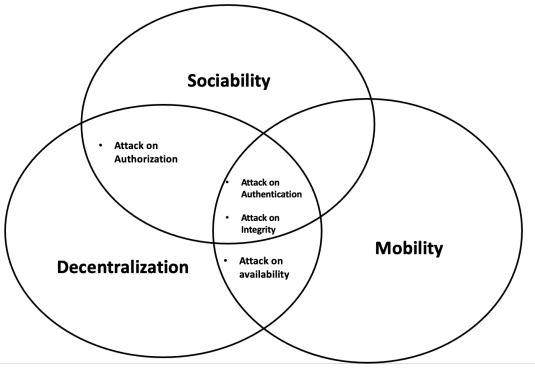

FIGURE 3: Vulnerabilities Inducing Features of Multi-Agent Systems

[11] define threats as the internal and external factors and circumstances that have the potential to cause damage to the system. An attack has been orchestrated by exploiting a vulnerability in the design. Research has shown that apparently innocuous errors or vulnerabilities on an agent can degrade the performance and even paralyze the whole MAS [12]. The following classification define MAS features that give rise to orthogonal (and complementary) vulnerabilities.

- *Sociability.* The ability of agents in the system to communicate with other agents and use this information gotten from these agents for decision-making makes the system vulnerable to malicious entities that can share falsified information or subvert the communication agents, e.g., by corrupting messages in transit. .
- *Decentralization.* The absence of a centralized controller to verify the identity of the individual agents or verifying the legitimacy of the messages in transit leaves the system vulnerable to masquerading attacks by rogue entities.
- *Mobility.* A mobile agent that has been compromised by an adversary can attack other agents indirectly by sharing compromised messages to other agents in encounters thereby disrupting the system. It can also directly attack the agent it encounters.

Finally, we can also characterize MASs based on the type of subversions. The following catetorizations adapt traditional security classifications to MASs. Fig. 2 depicts the relationship between the vulnerabilities inducing characteristics of MAS and various attacks on the system's security requirement.. We need to survey the possible attacks that have been recognized and implemented against multi-agent systems.

- *Authentication*: This guarantees that each agent is what it claims to be.
- *Authorization*: This provides assurance that the agent has legitimate right to have access to what it requires
- *Integrity*: This provides an assurance that the messages in transit have not been mutated since it was generated.
- *Availability*: The services and resources including the messages transmitted are available to the authorized agents in the system.
- *Confidentiality*: This ensures that only permitted agents have access to the resources and services, that is, only authorized agents can read the particular data.

III. ATTACKS ON MULTI-AGENT SYSTEMS

Fig. 4 shows a taxonomy of various attacks on MASs. We classify an attack according to its impact on the victim, effect on communication (which we call "Attack Operation"), origin, victim, and frequency. Our taxonomy can be viewed as a complete black-box classification of MAS attacks. It is black-box in the sense that we deliberately eschew the mechanism of the attack and focus on categorizing attacks based on the features of its manifestation that can be used by an external observer to describe the attack. It is complete in the sense that the external effect on any attack can be described with the features specified in the taxonomy. Furthermore, combining these five characteristics ensures encapsulation and precision in the resulting attack space required for a comprehensive evaluation. We analyze the usefulness of our resilient technique by listing numerous example attacks as a combination of the five identifying criteria. In the description below, we use this taxonomy to systematically explore research on MAS attacks.

A. ATTACK OPERATION

Disclosure attacks

A disclosure attack is an attack on confidentiality, i.e., the attacker accesses confidential information from agents. An obvious way to achieve this is by intercepting sensitive messages in transit. An adversary can also gain authorized access to the agent's data, such as the state and the internal code of the agents. Provenance attacks such as disclosing a mobile agent's itinerary information to an adversary are other attacks that the agents should be cautious about. Other, more sophisticated disclosure attacks are probing attacks, where the adversary probes the victim's private database of confidential information. One specific type of probing attack is the ontology attack, which works as follows. An ontology is generally defined as "a formal, explicit specification of a shared conceptualization" [13]. Ontologies are widely used by agents in MASs for sending queries; this is achieved via a semi-open ontology-based system. Obviously, all agents must have the same understanding of the ideas communicated in the messages to interpret them consistently. The adversary can subvert this process and actively probe the agents by accessing the victim agent's private local knowledge (e.g., decision rules and policies) and injecting facts into the agent's knowledge base, asking queries, and evaluating results. Other probing attacks have also been explored in recent research [14]–[16]. In particular, Bijani et al. [14] demonstrated four probing attacks on MASs controlled by electronic institutions: explicit query, implicit query, injection, and indirect query attacks. These attacks utilize Lightweight Coordination Calculus interaction models. They developed

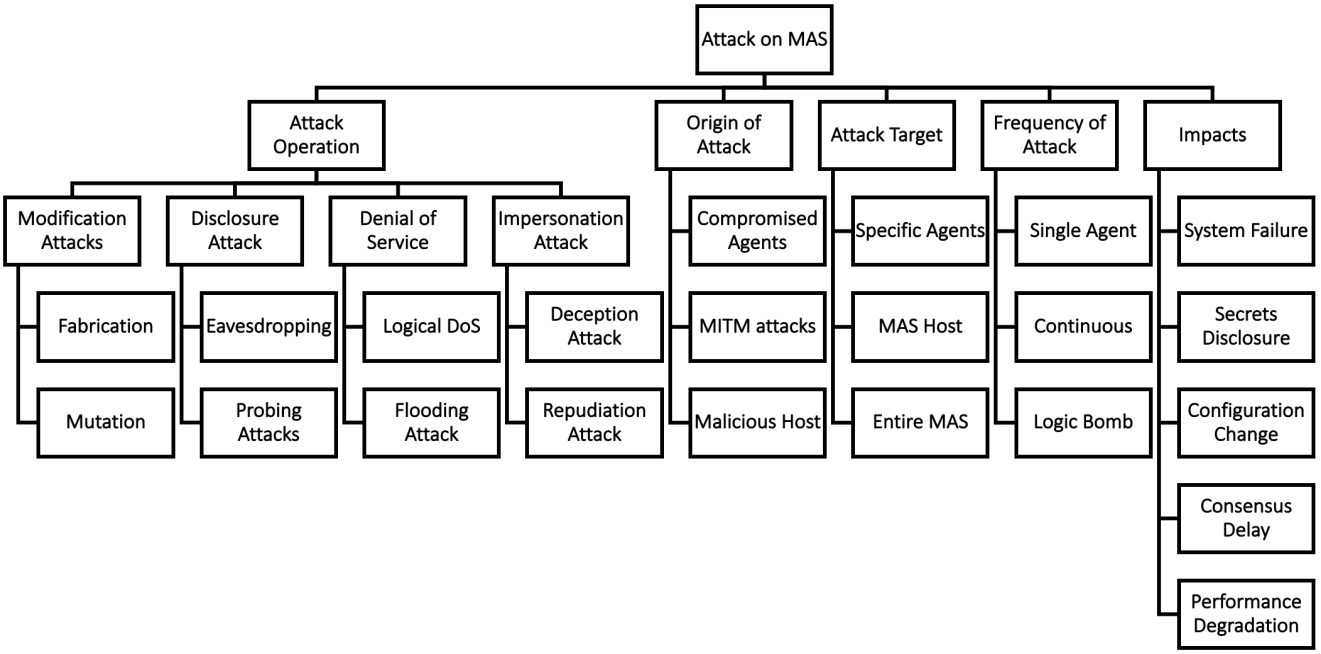

FIGURE 4: A Taxonomy of MAS Attacks

a secrecy analysis framework for the interaction models to detect probing attacks. .

Mutation Attacks

A key expectation from an integrated system is that information is not tampered with [17]. A *mutation attack* on a MAS occurs when this expectation is undermined, possibly (though not exclusively) by a malevolent agent. Mutation attacks are classified into *altering* and *injection* attacks. In an altering attack, the adversary modifies the agents' interaction, resulting in an alteration of the information transfer process. For instance, Rehak et al. [18] show an altering attack where a malicious agent can exploit vulnerabilities in the system by performing a buffer overflow. The adversary can also alter the agent code, data and configuration, and the event logging of the multi-agent system. Yue *et al*. [19] present a type of mutation attack in which two or more malicious agents surround a sender agent and collude to mutate the sent messages. Bijani et al. [20] present another type of mutation attack in which the adversary infuses forged information into the system to cause a malicious outcome or infer confidential information. This attack could be implemented via *message injection* attack or *knowledge injection*. In message injection, malicious messages are introduced to control the victim agent's interaction with other agents; knowledge injection entails the introduction of false information into the victim agent's knowledge base to affect its decisions.

Denial of Service

In a denial-of-service (DoS) attack on MASs, the attacker attempts to prevent the system from providing the intended services to its legitimate users. DoS attacks may target wasting other agents' resources [21], delaying the service [22], making real users forsake the system [23], or ruining the system's reputation [24]. A malicious agent may attack just one agent or a group of agents. A distributed DoS (DDoS) attack involves collaboration by more than one attacking entity. Persis et al. [25] established a general DoS attack model that imposes limits on the frequency and duration of attacks. Traynor *et al.* [26] divided Denial of Service (DoS) attacks into two classes: *flooding* and *logical* attacks. Flooding occurs when a malicious sends a high number of messages to one or more agents in a bid to overwhelm the agent or connections between agents, The adversary can do this by consuming the agent or network resources such as the communication bandwidth. Logical DoS uses more sophisticated methods to exploit the system. For instance, the adversary can create falsified interaction models to make the agents in the multi-agent system perform useless tasks or remain in infinite loops.

Impersonation

In an impersonation attack, an adversary produces a large number of anonymous agents, possibly with the goal of misusing the resources and changing the system configuration of the victim agent. Impersonation attacks are generally categorized as deception or repudiation. In a deception attack, the adversary can send deceptive messages to other

agents [27]. Lifeng Ma et al. [28] proposed a deception attack where the attack signals are injected by the adversary into the measurement data during the process of information transmitted via the communication network. In repudiation attacks, the adversary can create fake agents (together with fake interaction) for impersonation [29]. Once done, the adversary can use these fake agents to increase their trust value, e.g., by making the fake agents falsely certify their veracity. Eventually, the increased trust value would cause the benign agents to believe in the reliability of a malicious agent. The malicious agents then perform some interactions and then repudiate the existence of those interactions, thereby defaming the system.

B. ORIGIN OF ATTACK

The attack origin is the vulnerability point through which the adversaries can gain unauthorized access to the MAS application. Unauthorized access can be accomplished by compromising one or more agents or implementing a man-in-the-middle attack. Mustafa and Modares [30] demonstrated that an attack on a compromised agent could have a negative impact on intact agents that are reachable from it. They presented a mathematical framework for the analysis of this attack. Their study emphasizes the importance of developing unique resilient control mechanisms to offset the impacts of the attacker and establish an invulnerable consensus. Yang *et al.* [31] also described various attacks based on MITM to disrupt the formation control process of multi-agent systems. They analyzed potential formation control security issues on a multi-robot system. The experimental findings of the paper revealed that the MITM-based attacks may readily disrupt the formation motions of a multi-robot system and that several designed MITM attacks can even cause irreparable loss. There has also been work on MAS compromises through malicious or compromised hosts [32]. For instance, the host might include local access control mechanisms to prevent agents from reading and manipulating information belonging to other agents. It would also incorporate resource management, which would provide equitable resource allocation to agents running on the host, preventing a single agent (or a collection of agents) from using too many resources and preventing other agents from functioning optimally.

C. TARGET, FREQUENCY, AND IMPACT

The adversaries can target a single agent as seen in [30] or the entire fleet of agents in the MAS. The attackers can also target the system's host or the middleware controlling the MAS. The attack can be continuous within a time limit or orchestrated at intervals during the MAS operation. An external event, such as time, location, or the arrival of a certain agent, triggers an event-triggered attack, also known as a logic bomb [33]. Finally, the impact of the attack can include degradation of the performance [34], leakage of sensitive information (e.g., through eavesdropping or probing attack [13] [20]), a change in the configuration of the data, agent or the entire MAS system leading to the system not behaving in the intended manner [18]. The attack can lead to an increase in the time it would take for the agents to reach a consensus which would lead to undesirable effects, including a complete system failure [35].

FIGURE 5: MAS Defense Taxonomy

IV. MAS DEFENSE STRATEGIES

Security assurance for MASs has been a very active research topic integrating a variety of architecture, design, and validation techniques. In this paper, we categorize defenses into three basic classes as shown in Fig. 5. By prevention strategies we mean the use of design solutions to eliminate the possibility specific classes of attacks, while resiliency strategies entail monitoring for specific attack classes after deployment and performing mitigations.

A. PREVENTION STRATEGIES

A number of prevention mechanisms have been proposed to protect multi-agents against adversaries. In the description below, we categorize the strategies based on the key security feature used in the prevention, e.g., cryuptography, authentication, or acess control restriction.

Encryption and Cryptography

Cryptography is one of the most popular and widely used security mechanisms, with a history dating back to the history of written language itself. The approach is to develop methods for encrypting information into ciphers to protect it from illegal users. Modern cryptography includes mathematical methods for protecting digital information, systems, and distributed computing from hostile actions. Encryption of sensitive data and authentication is the first and most effective step toward countering MITM attacks, unauthorized access to agents, provenance attacks, and agent log modification.

Among cryptographic protections in MASs, Kapitonov *et al.* [36] describes how to organize a communication system

between agents in a peer-to-peer network using the decentralized Ethereum Blockchain technology and smart contracts. Each agent of the network owns a shared distributed database, which consists of a chain of information blocks in which each current block relates to the previous block using a unique cryptographic identifier. Adding a new block to the database is impossible without the agreement between all the agents. The disadvantages of this method, as the authors indicate, are due to the limitations of blockchain, which include disruptions and discredits generated by the principle of the blockchain network, the legal status of this network has not been completely worked out as the technology has to be regulated according to the law of the various states. Blockchain technology is also in its crude state and needs much more work to be done. Costa *et al.* [37] introduces a message-oriented middleware that improves communication efficiency and adds a new component called the certification authority service to the typical multi-agent system architecture. This component is responsible for generating certificates that agents in the platform can use to ensure their identity and communicate messages safely in the FIPA (Foundation for Intelligent Physical Agents architecture) [38] for multi-agent systems. The author describes the limitations of the approaches. The approach has three potential points of failure that need to be addressed by future research. The failure points include the RabbitMQ broker failure, Master node failure, and CA certification service failure. The proposed approach does not include a form of protection for the agent's decision process regarding the choice to trust the sender of a given message.

Horvat *et al.* [39] proposes an extension to the existing TFTP that is required for use in embedded systems of low computation power such as multi-agent system called STFTP. STFTP is a more secure version in the form of added authentication and established confidentiality for use in the multi-agent system platform. The added security comes from Digest Access Authentication combined with the SHA-1 hash function, as compared to the previous MD5 scheme, which was proved cryptographically unsafe.

Voronova and Zhilenkov [40] proposed a method for increasing the cryptographic stability of communication channels between agents in a multi-agent system to ensure information security. This is accomplished using an encryption process based on dynamic chaos systems, as well as synchronization. The author proposed that the essential security and privacy of communication channels between agents can be enforced using chaotic circuits capable of producing chaotic fluctuations from audio frequencies to the optical range and used as sources of chaotic carriers in a variety of applications such as broadband communications, signal masking, chaotic modulation, spectrum expansion, radars, and cryptography for high-entropy information sources.

A downside common to the above approaches is that they do not shield the agents from the influence of programs operating on network nodes. Because of the presence of a large number of malicious programs that can illegally alter the operation of agents and modify sensitive information that agents operate with. This problem remains largely unaddressed. This prompted a rise in resilience study, which would be described in Section IV-C. Another issue with employing symmetric encryption techniques in an open multi-agent system is the necessity for a distinct secret key for each pair (or group) of agents exchanging secret keys, which might cause scalability issues for numerous agents. For example, in a MAS set up with a high number of agents, it appears impossible to allocate and keep a distinct encryption key for each pair of agents. According to Bijani et al., [14], This issue can be solved by combining symmetric encryption with public-key cryptography schemes, which as used in some other papers. Wong & Sycara [41] proposed a security infrastructure to address the RETSINA framework's security and trust [42] which is a reusable multi-agent infrastructure and provides solutions for secure communication, the integrity of system-level services (such as naming and matchmaking services), and accountability. To achieve agent communication security, they coupled unique agent IDs and the Secure Socket Layer (SSL) protocol beneath their agent communication layer.

Other cryptographic techniques for preventing attacks against MAS have been explored [43], [44], [45], [46], [47]. Besides encryption, certificate-based security approaches such as SSL [48], digital signature [49], and integrity checking [50] have also been used in preventing interaction modification attacks.

Authentication

Authentication is the process of recognizing an agent's identity in the MAS by associating an incoming request with a set of identifying credentials. Since a request may originate on a remote host and may traverse several machines and network channels that are secured in different ways (and are not equally trusted) implies that it is non-trivial to authenticate the original source of communication in a distributed system.

Sabir et al. [51] developed an authentication scheme that uses JSON Web Token (JWT) to secure the communication between the agents by ensuring the integrity of the exchanged messages. JWT is a compact, URL-safe means of representing claims to be transferred between two parties. An authentication agent is responsible for the generation of JWT for the different agents who want to communicate with other agents.

Chatterjee *et al.* [52] proposed a timestamp-based mutual authentication protocol to enhance security during communication in monitoring systems like multi-agent systems. The scheme is based on Elliptic Curve Diffie–Hellman (ECDH) in wireless sensor network, which gives authentication and confidentiality. The proposed protocol is suitable for multi-agent systems as it requires less bandwidth and has a low storage requirement for the user side hence low computation costs. There are other papers that proposed the use of the Elliptic Curve Cryptosystem (ECC) for authentication. [53], [54], [55], [56].

In vehicular communications, Zhang *et al.* [57] proposed RAISE, a unique RSU-assisted message authentication scheme in which Roadside Units are in charge of evaluating the authenticity of messages transmitted from cars and informing them of the results. The proposed RAISE system has numerous advantages due to its lower processing and computational overhead. RAISE also uses the k-anonymity technique to safeguard the privacy of the cars. Hao *et al.* [58] also developed a way for authenticating VANETs using roadside units in which roadside unit (RSU) acts as the key distributor for the group of vehicles. This leads to another problem in which the RSUs can be compromised. The authors created a secure key distribution strategy that can prevent us from acting irrationally. The protocol ensures that compromised RSUs and hostile vehicles can be tracked. Aside from these, there has been research on other authentication schemes suitable for MASs [59], [60], and [61].

Access Control Mechanisms

Access control is the way of safeguarding the MAS by restraining what resources can be accessed or the entity accessing the resources. Role-based access control supports centralized security management, simplifies authorization management of MAS, and protects the integrity of information. Access control using security policy is common in MASs. Agents usually stipulate their policies for revealing information and information collection processes from other agents. If an agent's policy for disclosing information matches another agent's policy for information collection, the information is transmitted between the agents. Various middleware systems have been developed over the years to ensure access control policies in MASs. These architectures include JADE-S [62] which is a decentralized and inflexible access control scheme, SeMoA [63] which is centralized but also inflexible, and AgentScape [64] which uses role-based access control methods and can be customized.

Bijani *et al.* [14] identified the significant challenges of access control-based security methods: they are usually low-level middleware and only control access to low-level objects. This is challenging as this method finds it difficult to detect high-level violations such as impersonation and probing attacks. To solve the issue of end-to-end security interoperability, Tan and Poslad [65] presented a policy-based architecture for dynamic security reconfiguration in open and heterogeneous systems. This architecture detects and investigates policy disputes and the need for security reconfiguration, then resolves them at the meta-level without modifying the implementation of essential techniques. Paruchuri *et al.* [66] introduced a randomized policy to reduce the predictability of an agent's action using a decision-theoretic model based on the Multi-agent Constrained Markov Decision Problem (MCMDP). They also developed an algorithm called the Rolling Down Optimization that effectively generates new access control policies through linear programming.

B. DETECTION STRATEGIES

Preventing all types of assaults is not always practicable or viable in a MAS platform. As a result, as the second line of defense, the design and implementation of effective detection and reaction systems against potential assaults are critical. The earlier an assault is identified, the less influence it has on the victim agents. Detection strategies can be subdivided into two classes according to the method used: *behavior-based* and *knowledge-based*. Behavior-based detection methods "learn" normal behavior and communication patterns among agents and then detect intrusions by analyzing differences from expected or normal traffic. On the other hand, knowledge-based detection strategies use the knowledge pertaining to specific attacks.

Anomaly Detection

Anomaly detection refers to the problem of discovering patterns in data that do not conform to expected behavior. In various application fields, these nonconforming patterns are referred to as anomalies, outliers, discordant observations, exceptions, aberrations, surprises, oddities, or contaminants [2]. Anomaly detection is used in a broad range of applications, including credit card [67], insurance [68], and healthcare fraud detection [69], intrusion detection for cybersecurity [70], defect detection in safety-critical systems, and military surveillance for enemy operations [71].

Mateos and García [72] created an architecture for anomaly detection in MASs. This architecture is made up of several agents, each of which is modeled as a virtual digital shell of each asset in the manufacturing line. These agents gather information generated by the asset. There is also a central agent, such as a middle-ware. This central agent consists of a learning algorithm that detects abnormal behavior among other agents. Anomaly detection then constitutes the following tasks.

- Collecting, analyzing, and processing vast amounts of data in real-time under the supervision of intelligent agents; and
- Applying learning algorithms such as machine learning models (predictive models) in the multi-agent system to predict the normal state of the MAS.

Anomaly detection techniques in open MASs use a diversity of methods, including classification, clustering, or statistical analysis techniques. The anomaly detection algorithm assists the MAS system in differentiating aberrant activity from normal behaviors. Following are three main aspects of the predictive models used in detecting abnormality.

- *Feature selection* allows the machine learning model makes sense of the data provided.
- *Learning parameters* are parameters that algorithms employ to manage various learning aspects such as model size, the maximum number of iterations in the learning data, and regularization type.
- *Probability* of the presence of an anomaly is calculated and compared against a predefined threshold to infer an

TABLE 1: Defence strategies

	Prevention
Encryption and Certificate	[14], [36]–[50]
Authentication	[51]–[61]
Access Control	[14], [62]–[66]
	Detection
Behavior-based (Anomaly Detection)	[2], [67]–[79]
Knowledge-based (Point-based Approaches)	[80]–[87]
	Resiliency
Trust and Reputation	[88]–[100]
Game-Theoretical Approach	[101]–[116]
Stochastic Approach	[85], [87], [117]–[134]

anomaly.

Servin and Kudenko [73] shows how a group of agents coordinate their actions to reach the common goal of anomaly detection. Decision agents learn how to understand action signals supplied by sensor agents without any previously assigned interpretations or logic throughout this process. These action signals integrate the partial information gathered by sensor agents and are utilized by decision agents to reconstruct the global state of the environment. The technique was then used to recognize abnormal activities when the multi-agent system was introduced to DoS attacks. The main advantage of this learning approach is that the machine learning model does not need to be trained with prior information from the DoS data. However, the limitation of this approach is that it requires a large amount of data and high computational resources. Replay attack detection in a multi-agent system using stability analysis and loss effective watermarking

Anomaly detection has also been successfully applied to multi-robot systems (MRS), which constitute an essential class of MASs. One such approach is an online data-driven anomaly detection approach (ODDAD) proposed by Khalastchi *et al.* [74], in which the anomaly is detected in real-time using the current input data. The occurrence of a fault in the system was detected in three steps. The input was initially filtered to reduce noise. Dimension reduction was applied by splitting the data into sets of correlated attributes. Finally, the Mahalanobis Distance calculation was applied to each set-in order to return the probability of a data instance being an outlier. If the likelihood falls above a calculated threshold, an anomaly is detected.

Goh *et al.* [75] proposed using an LSTM-RNN to forecast a data sequence for anomaly detection in cyber-physical systems. Because anomalies or cyber-attacks usually happen over time, correlating time-series data information over time provides a way to recognize anomalies. The LSTM-RNN is used as a predictor to model normal behavior. The Cumulative Sum technique then identifies abnormal behavior with a meager false positive rate. This strategy is essential in real-world CPS applications where abnormal behavior is uncommon. The limitation of this paper is that only a small amount of data gotten from one aspect of the system was used for training or validating the data set due to limited resources and infrastructures.

Khazraei *et al.* [76] proposed a method for detecting replay attacks in a MAS by analyzing the stability of the system and using loss-effective watermarking techniques. Each agent is assigned a local estimator and an anomaly detector. An adversary detection method is then proposed based on a watermarked control strategy, in which watermarking signal is shared among the agents within the network. However, sharing watermarked signals through the network reduces the performance.

Boddupalli et al. [77], [78] proposed an anomaly technique based on machine learning that can be used in conjunction with several cooperative autonomous vehicle applications to identify and mitigate communication attacks. The primary concept is to create models that can learn normal behavior associated with benign V2X communication and detect unusual behavior to detect possibly harmful communication. This approach was applied to applications such as Platooning, Cooperative adaptive cruise control, Smart Intersection detection, and Dynamic cooperative route management. However, the framework only considers attacks from a single communication channel.

Additional information on machine learning-based anomaly detection in MAS was presented by Kim et al. [79] . Their survey analyzes attack-detection methods based on ML approaches and threats that harm the CPS. The physical system, the network, and the application layer were abstracted from the complicated CPS structure in their hierarchical CPS model. They also provided examples of attack implementations and cyber-physical attacks for each

CPS tier. Additionally, they offered a variety of ML-based approaches for detecting cyber-physical attacks, such as anomaly detection, which took into account the hierarchical CPS model to identify and handle attacks that target different layers.

Knowledge-based Approaches

Knowledge-based approaches for intrusion detection, — also sometimes referred to as misuse detection, — look for runtime indicators that match a given pattern of misbehavior. The advantage of this approach over behavioral-based techniques is low false positive rates. However, the drawback of this approach is the need for an up-to-date database of each attack vector. Consequently, the approach is ineffective against zero-day attacks.

Huang et al. [80] proposed a real-time detection scheme against false data injection attacks in smart grid networks. The authors built an analytical model to configure the detection system for performance assurance based on the fundamental detection criteria using the adaptive CUMSUM algorithm. The approach could detect false data attacks when the post-change probability density function is unknown.

Varshovi et al. [81] proposed a fuzzy IDS based on a DoS attack to address the uncertainty problem in distinguishing between normal and malicious network traffic. In more than 5 million test sessions, the system had a detection rate of 99.9 ZZXCC. 1%, with only roughly 1600 false alarms against DoS flooding attacks that used a limited set of features. Lima et al. [82] developed a defense approach for supervisory control systems that detects intrusions and prevents damage induced by man-in-the-middle cyber-attacks in sensor and control communication channels. They developed a deterministic model of systems subjected to the sensor and actuator channel attacks, as well as a defense method for detecting intrusions and protecting the system from damage caused by man-in-the-middle attacks on communication network channels in CPS. Vuong et al. [83] developed a method based on decision trees for constructing simple detection criteria, which they tested against DoS and command injection attacks. They discovered that adding physical input elements to cyber-physical systems can significantly reduce false positive rates and improve overall intrusion detection accuracy. Besides these, there have been several other approaches to knowledge-based intrusion detection system [84], [135], [86], [87].

C. RESILIENCY STRATEGIES

A significant requirement of multi-agent systems is resiliency, i.e., the capacity to supply services consistently despite bugs, failures, attacks, and subversions. Incorporating resilience into MASs is an active field of research with a large volume of work. Our focus in this section is confined to resiliency against security attacks.

Reputation and Trust

There has been significant research on models of trust and confidence for building resilient MAS against adversarial attacks. Lee and See [88] define trustworthiness as the attitude that an agent will help achieve an individual's goals in a situation characterized by uncertainty and vulnerability. Since conventional network security techniques such as encryption, firewall, and access control cannot predict agent behavior from a trust standpoint, trust concerns have grown in popularity. In various applications, the term "trustworthiness of an agent" has been used to signify a variety of notions, including (but not limited to the following: (1) the agent precisely executes the coordinator's directions; (2) the agent accurately communicates its status (e.g., position, velocity, etc.); or (3) the agent is not malicious.

Das and Islam [89] defined a reputation trust model as a model that collects, distributes, and aggregates feedback about participants' past behavior. These models assist agents in deciding who to trust, encourage trustworthy conduct, and discourage involvement by dishonest agents. The reputation trust model was divided into two categories based on how the evaluator agents evaluate the information process.

- Direct experience model/Local Trust Models in which the reputation and trust values are based on direct encounters and observations (firsthand value)
- Global reputation/Trust models in which the agents combine information about the reputation of the target agent from all other agents interacting with the target agent.

Although global reputation models converge to a better decision than the direct experience model, they are more complex and more challenging to manage than the natural experience models. The global reputation model also fails when the adversaries change their behavior strategically to benefit them. The high workload demand of the global reputation problem is also an issue that needs to be tackled.

Das and Islam proposed a technique called Secured Trust. This dynamic trust computation technique can identify unexpected strategic changes in malicious behavior and has the added function of balancing workload among service providers in the multi-agent system. This approach employed a unique policy of using an exponential averaging process to decrease storage costs in computing agent trust. However, this is counter-intuitive as it adds additional workload to the system. The limitation of the method was that it did not consider how to transmit trust data securely. However, this can be addressed by combining the proposed approach with other security issues like cryptography.

Zhang et al. [90] proposed a method called SFtrust, which uses two trust metrics, one for service trust and one for feedback trust. Even with variable feedback, this technique can fully use all the agents' service capabilities. One limitation of this approach is the lengthy computational time. Another limitation is the inability of the static weighted average of the local feedback trust to incorporate the evaluating agent's

cumulative experience appropriately.

Hu et al. [91] proposed a robust feedback credibility global trust model called FCtrust that distinguishes between offering feedback and delivering services. This approach assesses the reliability of any recommender who provides feedback using transaction density and similarity measures. However, this approach still must deal with the limitation of the inability to find a way to transmit trust data securely. Coordination may be utilized for autonomous and mobile MASs, such as those found in ground transportation systems or unmanned aerial vehicles, to provide higher safety over human-operated agents, to increase system efficiency, or both. When the MAS comprises both trustworthy and untrusted agents, the MAS must provide safe and efficient coordination.

A critical application domain of multi-agent cooperation is multi-vehicle platooning, which employs artificial intelligence to examine platoon members and assess their level of trustworthiness to avoid attacks that might result in accidents. Hu *et al.* [92] proposed a technique called REPLACE for creating a trust-based Platoon service. In REPLACE, users may assess the conduct of lead drivers, and the data can then be used to advise others on whether to join a platoon with that leader. An iterative filtering technique is used to cope with false feedback from user automobiles. One limitation of this approach is that the attack primarily aims to provide unjustified trust in the leader vehicle, but other attacks apply to the platooning application. These methodologies, however, examine individual vehicles in isolation and do not consider vehicle communication and cooperation. Another limitation is that the proposed methodologies do not consider scenarios in which the Platooning scheme is attacked by multiple adversaries simultaneously.

Cheng *et al.* [93] addressed these issues by building a universal framework based on a logical characterization of trust that enables systematic quantification of trust in individual agents. To assess an agent's trustworthiness, the proposed includes short-term and long-term behavioral histories. The framework helps select coordinating rules that accomplish the required trade-off between safety and efficiency based on quantifiable trust values. The proposed framework was successfully applied in three multi-agent platforms, such as the Cooperative adaptive cruise control (CACC), Autonomous intersection management (AIM), and the Reinforcement Learning Traffic light control system, to demonstrate its feasibility and applicability. The limitation of this approach, particularly in the CACC application, is that it considers a centralized authority that maintains the trust distribution and reputation ratings. The centralized system presents a single point of failure on the network.

Ensuring secure and trusted communications within Vehicular Adhoc Networks (VANETs) is another exciting application area. Several works have described the trust solutions in VANETS, a subset of multi-agent systems. Dotzer et al. [94] proposed a VANET reputation framework called VARS, which is an entirely distributed approach based on reputation. Peers can develop opinions about a message based on the aggregated opinions of other nodes and direct interactions with the sender. What sets this approach from other methods is the fact that the approach gives more importance to the views coming from the closest agents to the reported events. The limitation of the approach is the added overhead in the message transmitted by aggregating other nodes' opinions.

Tajeddine et al. [95] proposed a trust-based privacy-preserving model for VANETS. The methodology is unique in maintaining accurate reputation-based trust while protecting privacy. The vehicles are arranged into groups, each with a reputation value. Each group's reputation improves if the average of its members' opinions is consistent with the road condition. The limitation of this approach is that the vehicles are hardly resilient against colluding vehicles in the same group. Many trust and reputation approaches also suffer badly from their total resource consumption. To combat this problem, a subjective logic-based technique is presented for modifying reliability information in data exchanged by the MAS [37]. Subjective logic is a branch of probabilistic logic that explicitly considers cognitive uncertainty and source trust. The paper's method provides a trade-off between security, generality, and resource usage. The technique is shown to cope with heterogeneous agents, isolate faulty agents, and show little resource management.Other research work that discussed the role of reputation and trust in securing MAS includes [96], [97], [98], [99], [100].

Game Theory

Game theory is a mathematical model for understanding conflict and cooperation among rational, intelligent decision-makers [101]. The idea is to model interactions between different parties as games, such that a "win" in the game corresponds to achieving some specific goal for the cooperative artifacts being modeled. The game can either be static or dynamic. Various MAS security can be naturally modeled through game theory [102], [103], [104], [105], [106], [107], [108], [109], [110].

Farhadi et al. [111] explored a dynamic network with strategic agents that discreetly monitor their security state and are exclusively concerned with increasing their utility. The author posed a mechanism design issue for a network manager whose goal is to dynamically allocate his limited security resources across the network to maximize overall network security over time. The authors took advantage of the dynamic correlation between the security states of the agents to generate a set of inference signals for all agents over time. They outlined a dynamic incentive mechanism that maintains the agents' incentive compatibility and individual rationality and delivers a socially efficient conclusion using the proposed inference signals.

Farhadi et al. [112] proposed an incomplete information two-player game platform that models the interaction between the service providers and various clients, which could be agents in our case. The game is analyzed using perfect Bayesian Nash equilibrium (PBNE) under different situations. This helps prevent malicious activities of the attacker

clients leading to the provision of quality services to the benign client.

La et al. [113] studied the application of game-theoretic concepts to the idea of honeypots in IoT and cyber-physical systems. They considered a game-theoretic model of deception involving an attacker and a defender. The game model tries to answer fundamental problems such as how the defender should react to various observations made by the attacker and if deception benefits the attacker and the defender. The authors devised a Bayesian game of incomplete information to reflect the defender's poor awareness of impending attacks.

In the presence of replay attacks, Miao et al. [114] created a zero-sum, finite horizon, non-stationary stochastic game to minimize the worst-case control and detection costs. The game also obtains an optimal control policy for switching between control-cost optimal (but non-secure) and secure (but cost-suboptimal) controllers. The authors demonstrated that the system's optimal strategy exists and presented a suboptimal algorithm for calculating the system's strategy using a combination of robust game approaches and a stationary stochastic game algorithm with a finite horizon. This approach can also be extended to other cyber-physical systems to find the optimal policy.

In the military settings, Anwar et al. [115] introduced a novel method for cyber-deception that protects critical nodes while also trapping the adversary. This is done by formulating a stochastic game to study the interactions between the administrator of the system and the other clients or agents. In this game, the defender's goal is to stop the attacker early in the cyber-attack chain and prevent more dangerous scenarios from materializing. The limitation of this approach is the cost, as the game is computationally expensive for each player, and this cost grows with the network size.

Çeker et al. [116] provided a game theoretic approach in preventing DoS attacks.They presented a deception-based protection system that uses game theory to describe the defender-attacker interaction. They created a new defense architecture that proactively uses deception to aid in the development of effective responses to adversary attacks that are unconventional, coordinated, and complicated. They also used a new quantification method for the cost variables to generate Bayesian equilibrium solutions for this model and assess the complementary strategies of the participants. The limitation of this paper is that it only considered a one-period game between the game players due to simplicity, as this would not be the case in a real-life scenario.

Stochastic Resiliency

MASs operating in a real-world environment are subject to noise, interference, and obstructions that can severely affect the agents' communication quality. There is a need to develop various model-based resilient control algorithms that enable the team of autonomous agents to accomplish their formation tasks even in the presence of different adversaries. The *stochastic resiliency* technique, also called *probabilistic resiliency*, deals with adversarial attacks and probabilistic communication constraints.

A fundamental problem for stochastic resiliency is consensus, which entails information exchange so that the group of agents can agree on a specific quantity of interest [87]. Shang [117] explored the consensus problem for MASs over directed networks with state constraints. The authors developed the robust state constrained consensus in the presence of rogue agents who may have been compromised.

Yual et al. [118] proposed a method of establishing robust consensus in multi-hop communication in a scenario where some nodes are malicious and try to prevent consensus by sending false information. Using the proposed Mean Subsequence Reduced (MW-MSR) algorithm, they investigated robust asymptotic (approximate) consensus under the malicious scenario. Normal nodes will filter out the extreme values created by malicious multi-hop neighbors. The MW-MSR method not only improves the robustness of the network but also speeds up the convergence in consensus forming even in adversarial environments.

There has been significant research on the resiliency of MASs against DoS attacks. Lu and Yang [119] proposed such a resiliency scheme and demonstrated that despite the DoS assault, the proposed distributed state-feedback and observer-based controller achieves consensus. The primary concept is to ignore the information gained from the attacked channels to reach a safe consensus. The limitation of this approach is that the consensus approach may be triggered even without the presence of a DoS attack. Cetinkaya et al. [120] proposed a stochastic communication strategy for multi-agent consensus under Jamming attacks. In this protocol, agents seek to communicate information with their neighbors at uniformly distributed random time instants. Agent communication attempt timings are randomized in this protocol, and the attacker is unaware of them until after the agents have made their attempts. They show that when the suggested communication protocol is paired with a stochastic ternary control rule, agents may attain consensus regardless of the number of attacks using probabilistic analysis. The limitation of this paper is that the MAS system utilizing the approach might take a longer time to reach consensus compared to the base approach, but that is a realistic trade-off for resiliency. Other papers that explored how the multi-agent system can still reach consensus even when the system is attacked include [121], [122], [123], [124].

A common control strategy against DoS attacks is event-triggered control. It determines when and how often data samplings, transmissions, and security control mechanisms should be done depending on well-defined events rather than predetermined times. Cheng et al. [125] proposed a distributed event-triggered consensus of a generally linear multi-agent system subjected to periodic denial-of-service (DoS) jamming attacks. In this paper, DoS attacks are carried out by sending out pulse-width modulated (PWM) jamming signals. A distributed event-triggered mechanism was developed to mitigate the attack, and a resilient event-triggered coordina-

tion protocol was constructed, enabling the MAS to reach exponential consensus. Persis et al. [126] investigated event-resilient control techniques for linear systems operating in a DoS environment. The suggested control strategy's resiliency stems from its capacity to adjust the sample rate in response to the state of the process and the existence of DoS attacks.

Ma et al. [127] The authors proposed a resilient wireless cyber-physical management system that is resilient against both physical and wireless interference. Their solution incorporates a holistic controller that generates actuation signals to physical plants and reconfigure the Wireless sensor-actuator networks to retain the desired control performance while conserving wireless resources. Under ideal network settings, the controller considers the worst-case evolution of the plant's Lyapunov function. The authors simulated the process using real-world data, and the simulation's outcome demonstrated that their holistic controller could maintain secure physical operation despite considerable wireless interference and sensor disturbances

Fang et al. [128] described how stochastic systems could use two-way coding to protect linear time-invariant (LTI) feedback control systems against injection attacks. The two-way transformation known as two-way coding, which operates in a feedback loop, takes the signals in the forward path and the feedback path and outputs a new signal to the forward path and a second new signal that continues in the feedback path. The two-way coding can distort the attacker's viewpoint of the control system; it has been shown that this distorted vision on the attacker's side makes it easier to detect attacks or limit the attacker's options.

Pole-dynamics attacks are typical covert cyber-physical attacks based on system theory that tampers with control-related information in communication networks. To counter PDA, Kim et al. [129] suggested a real-time resilient CPS framework. The proposed architecture is a holistic approach needed to detect, isolate, and recover from the PDA in real-time. We incorporate the PDA detection technique on SDN switches, and the proposed detection algorithm distinguishes the PDA from other anomalies, such as disruptions and transient behaviors. The PDA attacker should be removed from the network to limit further damage. A unique data transmission line is needed for sensor measurement because of the attacker's isolation. After restoring the transmission line, the computing system receives the accurate sensor reading and restores the physical system to its initial condition.

Another extensible innovative cybersecurity architecture for ICS is proposed by Paridari et al. [130]. The framework comprises two components: an attack detection module that uses data analytics to identify threats and a resilient control policy that keeps the physical system secure during and after an attack. The architecture ensures that attacks such as man-in-the-middle and DoS attacks cannot destabilize the system. This resiliency technique is accomplished by safeguarding a few carefully chosen sensors. To do this, the supervisory controller generates a correction vector signal , sent to the local controllers to correct the attacked signals. As a result, the controller is reconfigured.

Other control-oriented resiliency techniques against attacks against various cyber-attacks were described in a survey by Kim et al. [131]. The authors thoroughly analyzed how cyber-physical attacks affect CPS, such as Multi-agent systems, due to the disruption of the controlled networks and how to construct CPS that is resilient to such attacks. The survey characterized CPS as a hierarchical networked control system with physical, network, and application layers. One limitation of the survey was that it only focuses on attacks that can disrupt the physical dynamics of the Multi-agent system.

Cetinkaya et a. [85] describes another event-controlled stochastic resiliency strategy in which the authors explored control of linear dynamical systems in networks subject to random packet losses and malicious attacks. The authors demonstrated that the proposed probabilistic characterization could handle independent and dependent loss instances by using a tail probability inequality for the sum of processes representing random packet losses and malicious attacks. Other event-controlled resilient mechanisms have explored resiliency against jamming attacks and random packet losses, which also explores resiliency for the system against denial of service attacks [132], [133], [134].

V. SUMMARY AND CONCLUSION

We presented a comprehensive high-level discussion on various methodologies needed to secure the MAS. We comprehensively reviewed recent developments in the physical safety and cyber-security of MASs. We discussed various MAS characteristics (e.g., sociability, mobility, and decentralization) and their influence on vulnerabilities. We provided an extensive survey of the spectrum of attacks on MASs and various prevention, detection, and resiliency strategies. Despite significant research on the security of open MAS, many security vulnerabilities remain. A viable solution must account for various challenges, including limitations in computational resources and real-time requirements for the solutions. We believe that the overview of potential threats and security techniques in MASs will pave the way for a comprehensive understanding of the state of the art in the research area and facilitate future research.

REFERENCES

[1] Rohallah Benaboud and Toufik Marir. Flexibility measurement model of multi-agent systems. Multiagent and Grid Systems, 16(3):309–341, 2020.

[2] Varun Chandola, Arindam Banerjee, and Vipin Kumar. Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3):1–58, 2009.

[3] Shiyong Wang, Jiafu Wan, Daqiang Zhang, Di Li, and Chunhua Zhang. Towards smart factory for industry 4.0: A self-organized multi-agent system with big data based feedback and coordination. Computer Networks, 101:158–168, 2016.

[4] Michael J. Wooldridge. An introduction to multiagent systems. John Wiley, 2012.

[5] Rodolfo Carneiro Cavalcante, Ig Ibert Bittencourt, Alan Pedro da Silva, Marlos Silva, Evandro Costa, and Robério Santos. A survey of security in multi-agent systems. Expert Systems with Applications, 39(5):4835–4846, 2012.

[6] Stuart Russell and Peter Norvig. A modern, agent-oriented approach to introductory artificial intelligence. ACM SIGART Bulletin, 6(2):24–26, 1995.

[7] Ali Dorri, Salil S. Kanhere, and Raja Jurdak. Multi-agent systems: A survey. IEEE Access, 6:28573–28593, 2018.

[8] Russell Merris. Laplacian matrices of graphs: A survey. Linear Algebra and its Applications, 197-198:143–176, 1994.

[9] Michel Rigo. Advanced graph theory and combinatorics. John Wiley & Sons, 2016.

[10] Denis Trcek. Managing information systems security and privacy. Springer Science & Business Media, 2006.

[11] Charles P. Pfleeger, Shari Lawrence Pfleeger, and Jonathan Margulies. Security in computing. Pearson India Education Services, 2018.

[12] Dan Zhang, Gang Feng, Yang Shi, and Dipti Srinivasan. Physical safety and cyber security analysis of multi-agent systems: A survey of recent advances. IEEE/CAA Journal of Automatica Sinica, 8(2):319–333, 2021.

[13] Amir Mohamed Talib, Rodziah Atan, Rusli Abdullah, and Masrah Azrifah Azmi Murad. Security framework of cloud data storage based on multi agent system architecture - a pilot study. 2012 International Conference on Information Retrieval & Knowledge Management, 2012.

[14] Shahriar Bijani, David Robertson, and David Aspinall. Probing attacks on multi-agent systems using electronic institutions. Declarative Agent Languages and Technologies IX, page 33–50, 2012.

[15] Vitor Graveto, Luís Rosa, Tiago Cruz, and Paulo Simões. A stealth monitoring mechanism for cyber-physical systems. International Journal of Critical Infrastructure Protection, 24:126–143, 2019.

[16] Gyujin Na and Yongsoon Eun. A multiplicative coordinated stealthy attack and its detection for cyber physical systems. In 2018 IEEE Conference on Control Technology and Applications (CCTA), pages 1698–1703. IEEE, 2018.

[17] C. Mitchell. Security for mobility. Electronics & Communication Engineering Journal, 14(5):178–178, 2002.

[18] Martin Rehák, Michal Pechoucek, Martin Grill, Jan Stiborek, Karel Barto, and Pavel Celeda. Adaptive multiagent system for network traffic monitoring. IEEE Intelligent Systems, 24(3):16–25, 2009.

[19] Ji Y Yue X, Qiu X and Zhang C. P2p attack taxonomy and relationship analysis. 2009 P2P attack taxonomy and relationship analysis, 2009.

[20] Shahriar Bijani and David Robertson. A review of attacks and security approaches in open multi-agent systems. Artificial Intelligence Review, 42(4):607–636, 2012.

[21] Hoang Lan Nguyen and Uyen Trang Nguyen. Study of different types of attacks on multicast in mobile ad hoc networks. In International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06), pages 149–149, 2006.

[22] Zihao Cheng, Dong Yue, Songlin Hu, Hui Ge, and Lei Chen. Distributed event-triggered consensus of multi-agent systems under periodic dos jamming attacks. Neurocomputing, 400:458–466, 2020.

[23] Trung Dong Huynh, Nicholas R Jennings, and Nigel R Shadbolt. An integrated trust and reputation model for open multi-agent systems. Autonomous Agents and Multi-Agent Systems, 13(2):119–154, 2006.

[24] Esther M Amullen, Sachin Shetty, and Lee H Keel. Model-based resilient control for a multi-agent system against denial of service attacks. In 2016 World Automation Congress (WAC), pages 1–6. IEEE, 2016.

[25] Claudio De Persis and Pietro Tesi. Input-to-state stabilizing control under denial-of-service. IEEE Transactions on Automatic Control, 60(11):2930–2944, 2015.

[26] Patrick Traynor, Patrick McDaniel, and Thomas La Porta. Future directions and challenges. Security for Telecommunications Networks, page 157–162, 2008.

[27] Dong Wang, Zidong Wang, Bo Shen, Fuad E. Alsaadi, and Tasawar Hayat. Recent advances on filtering and control for cyber-physical systems under security and resource constraints. Journal of the Franklin Institute, 353(11):2451–2466, 2016.

[28] Lifeng Ma, Zidong Wang, and Yuan Yuan. Consensus control for nonlinear multi-agent systems subject to deception attacks. 2016 22nd International Conference on Automation and Computing (ICAC), 2016.

[29] André Teixeira, Daniel Pérez, Henrik Sandberg, and Karl Henrik Johansson. Attack models and scenarios for networked control systems. Proceedings of the 1st international conference on High Confidence Networked Systems - HiCoNS '12, 2012.

[30] Aquib Mustafa and Hamidreza Modares. Attack analysis for discrete-time distributed multi-agent systems. 2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton), 2019.

[31] Yue Yang, Yang Xiao, and Tieshan Li. Attacks on formation control for multiagent systems. IEEE Transactions on Cybernetics, page 1–13, 2021.

[32] G Annie Sujitha. A software agent framework to overcome malicious host threats and uncontrolled agent clones. International Journal of Advanced Information Technology, 2(2):13–27, 2012.

[33] M.S. Greenberg, L.C. Byington, and D.G. Harper. Mobile agents and security. IEEE Communications Magazine, 36(7):76–85, 1998.

[34] Farid Sharifi, Youmin Zhang, and Amir G. Aghdam. A distributed deployment strategy for multi-agent systems subject to health degradation and communication delays. Journal of Intelligent & Robotic Systems, 73(1-4):623–633, 2013.

[35] Yu Wenwu, Wei Ren, Ming Cao, and Guanrong Chen. Delay-induced consensus and quasi-consensus in multi-agent systems. Distributed Cooperative Control of Multi-agent Systems, page 214–228, 2016.

[36] Aleksandr Kapitonov, Sergey Lonshakov, Aleksandr Krupenkin, and Ivan Berman. Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of uavs. 2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS), 2017.

[37] Davide Costa, Daniel Garrido, and Daniel Silva. Efficient secure communication for distributed multi-agent systems. Proceedings of the 13th International Conference on Agents and Artificial Intelligence, 2021.

[38] Fabio Bellifemine, Agostino Poggi, and Giovanni Rimassa. Developing multi-agent systems with a fipa-compliant agent framework. Software: Practice and Experience, 31(2):103–128, 2001.

[39] G. HORVAT, D. ZAGAR, and G. MARTINOVIC. Stftp: Secure tftp protocol for embedded multi-agent systems communication. Advances in Electrical and Computer Engineering, 13(2):23–32, 2013.

[40] Anna V. Voronova and Anton A. Zhilenkov. Cryptographic strength of encryption in a multi-agent system. 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), 2021.

[41] H. Chi Wong and Katia Sycara. Adding security and trust to multiagent systems. Applied Artificial Intelligence, 14(9):927–941, 2000.

[42] Katia Sycara, Joseph A. Giampapa, Brent Langley, and Massimo Paolucci. The retsina mas, a case study. Software Engineering for Large-Scale Multi-Agent Systems, page 232–250, 2003.

[43] Dhuha Dheyaa Khudhur and Muayad Sadik Croock. Developed security and privacy algorithms for cyber physical system. International Journal of Electrical & Computer Engineering (2088-8708), 11(6), 2021.

[44] Michael Kirkpatrick, Elisa Bertino, and Frederick T Sheldon. Restricted authentication and encryption for cyber-physical systems. In DHS CPS Workshop Restricted Authentication and Encryption for Cyber-physical Systems, 2009.

[45] Kandasamy Muniasamy, Seshadhri Srinivasan, Juri Vain, and M Sethumadhavan. Formal methods based security for cloud-based manufacturing cyber physical system. IFAC-PapersOnLine, 52(13):1198–1203, 2019.

[46] Youngjin Kim, Vladimir Kolesnikov, and Marina Thottan. Resilient end-to-end message protection for cyber-physical system communications. IEEE Transactions on Smart Grid, 9(4):2478–2487, 2016.

[47] Young-Jin Kim, Vladimir Kolesnikov, and Marina Thottan. Resilient end-to-end message protection for large-scale cyber-physical system communications. In 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), pages 193–198. IEEE, 2012.

[48] Joshua Davies. Implementing SSL/TLS using cryptography and PKI. John Wiley and Sons, 2011.

[49] Rossilawati Sulaiman, Dharmendra Sharma, Wanli Ma, and Dat Tran. A multi-agent security architecture. 2009 Third International Conference on Network and System Security, 2009.

[50] Kamil Piętak, Adam Woś, Aleksander Byrski, and Marek Kisiel-Dorohinicki. Functional integrity of multi-agent computational system supported by component-based implementation. Holonic and Multi-Agent Systems for Manufacturing, page 82–91, 2009.

[51] Badr Eddine Sabir, Mohamed Youssfi, Omar Bouattane, and Hakim Allali. Authentication and load balancing scheme based on json token for multi-agent systems. Procedia computer science, 148:562–570, 2019.

[52] Kakali Chatterjee, Asok De, and Daya Gupta. A secure and efficient authentication protocol in wireless sensor network. Wireless Personal Communications, 81(1):17–37, 2015.

[53] Ali Zakerolhosseini and Morteza Nikooghadam. Secure transmission of mobile agent in dynamic distributed environments. Wireless Personal Communications, 70(2):641–656, 2013.

[54] Morteza Nikooghadam, Farshad Safaei, and Ali Zakerolhosseini. An efficient key management scheme for mobile agents in distributed networks. In 2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010), pages 32–37. IEEE, 2010.

[55] Haya Hasan, Tasneem Salah, Dina Shehada, M Jamal Zemerly, Chan Yeob Yeun, Mahmoud Al-Qutayri, and Yousof Al-Hammadi. Secure lightweight ecc-based protocol for multi-agent iot systems. In 2017 IEEE 13th international conference on wireless and mobile computing, networking and communications (WiMob), pages 1–8. IEEE, 2017.

[56] Yousra Berguig, Jalal Laassiri, and Sanae Hanaoui. Anonymous and lightweight secure authentication protocol for mobile agent system. Journal of Information Security and Applications, 63:103007, 2021.

[57] Chenxi Zhang, Xiaodong Lin, Rongxing Lu, Pin-Han Ho, and Xuemin Shen. An efficient message authentication scheme for vehicular communications. IEEE Transactions on Vehicular Technology, 57(6):3357–3368, 2008.

[58] Yong Hao, Yu Cheng, Chi Zhou, and Wei Song. A distributed key management framework with cooperative message authentication in vanets. IEEE Journal on Selected Areas in Communications, 29(3):616–629, 2011.

[59] Xiaonan Liu, Zhiyi Fang, and Lijun Shi. Securing vehicular ad hoc networks. In 2007 2nd International Conference on Pervasive Computing and Applications, pages 424–429, 2007.

[60] Xiaodong Lin, Chenxi Zhang, Xiaoting Sun, Pin-Han Ho, and Xuemin Sherman Shen. Performance enhancement for secure vehicular communications. In IEEE GLOBECOM 2007 - IEEE Global Telecommunications Conference, pages 480–485, 2007.

[61] Wenlong Shen, Lu Liu, Xianghui Cao, Yong Hao, and Yu Cheng. Cooperative message authentication in vehicular cyber-physical systems. IEEE Transactions on Emerging Topics in Computing, 1(1):84–97, 2013.

[62] Salvatore Vitabile, Vincenzo Conti, Carmelo Militello, and Filippo Sorbello. An extended jade-s based framework for developing secure multi-agent systems. Computer Standards & amp; Interfaces, 31(5):913–930, 2009.

[63] Youna Jung, Minsoo Kim, Amirreza Masoumzadeh, and James B. Joshi. A survey of security issue in multi-agent systems. Artificial Intelligence Review, 37(3):239–260, 2011.

[64] N.J.E. Wijngaards, B.J. Overeinder, M. van Steen, and F.M.T. Brazier. Supporting internet-scale multi-agent systems. Data & amp; Knowledge Engineering, 41(2-3):229–245, 2002.

[65] J TAN and S POSLAD. Dynamic security reconfiguration for the semantic web. Engineering Applications of Artificial Intelligence, 17(7):783–797, 2004.

[66] Praveen Paruchuri, Jonathan P. Pearce, Janusz Marecki, Milind Tambe, Fernando Ordóñez, and Sarit Kraus. Coordinating randomized policies for increasing security of agent systems. Information Technology and Management, 10(1):67–79, 2009.

[67] Swati Gupta, Meenu, Sanjay Patel, Surender Kumar, and Goldi Chauhan. Anomaly detection in credit card transactions using machine learning. International Journal of Innovative Research in Computer Science & amp; Technology, 8(3), 2020.

[68] Basma Moharram. Multi-dimensional approaches to anomaly detection: A study of insurance claims*. Rutgers Studies in Accounting Analytics: Audit Analytics in the Financial Industry, page 111–144, 2019.

[69] Aryya Gangopadhyay and Song Chen. Health care fraud detection with community detection algorithms. 2016 IEEE International Conference on Smart Computing (SMARTCOMP), 2016.

[70] Benot Morel. Anomaly based intrusion detection and artificial intelligence. Intrusion Detection Systems, 2011.

[71] Tom Brotherton and Tom Johnson. Anomaly detection for advanced military aircraft using neural networks. In 2001 IEEE Aerospace Conference Proceedings (Cat. No. 01TH8542), volume 6, pages 3113–3123. IEEE, 2001.

[72] Nuria Mateos García. Multi-agent system for anomaly detection in industry 4.0 using machine learning techniques. ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal, 8(4):33–40, 2019.

[73] Arturo Servin and Daniel Kudenko. Multi-agent reinforcement learning for intrusion detection: A case study and evaluation. In German Conference on Multiagent System Technologies, pages 159–170. Springer, 2008.

[74] Eliahu Khalastchi, Meir Kalech, and Lior Rokach. A hybrid approach for fault detection in autonomous physical agents. Technical report, BEN-GURION UNIV OF THE NEGEV BEERSHEBA (ISRAEL), 2014.

[75] Jonathan Goh, Sridhar Adepu, Marcus Tan, and Zi Shan Lee. Anomaly detection in cyber physical systems using recurrent neural networks. 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), 2017.

[76] Amir Khazraei, Hamed Kebriaei, and Farzad Rajaei Salmasi. Replay attack detection in a multi agent system using stability analysis and loss effective watermarking. 2017 American Control Conference (ACC), 2017.

[77] Srivalli Boddupalli and Sandip Ray. Redem: Real-time detection and mitigation of communication attacks in connected autonomous vehicle applications. In IFIP International Internet of Things Conference, pages 105–122. Springer, 2019.

[78] Srivalli Boddupalli, Akash Someshwar Rao, and Sandip Ray. Resilient cooperative adaptive cruise control for autonomous vehicles using machine learning. IEEE Transactions on Intelligent Transportation Systems, 2022.

[79] Sangjun Kim and Kyung-Joon Park. A survey on machine-learning based security design for cyber-physical systems. Applied Sciences, 11(12):5458, 2021.

[80] Yi Huang, Jin Tang, Yu Cheng, Husheng Li, Kristy A. Campbell, and Zhu Han. Real-time detection of false data injection in smart grid networks: An adaptive cusum method and analysis. IEEE Systems Journal, 10(2):532–543, 2016.

[81] Ali Varshovi, Maryam Rostamipour, and Babak Sadeghiyan. A fuzzy intrusion detection system based on categorization of attacks. In 2014 6th Conference on Information and Knowledge Technology (IKT), pages 50–55, 2014.

[82] Públio M. Lima, Marcos V.S. Alves, Lilian K. Carvalho, and Marcos V. Moreira. Security against network attacks in supervisory control systems. IFAC-PapersOnLine, 50(1):12333–12338, 2017. 20th IFAC World Congress.

[83] Tuan Phan Vuong, George Loukas, Diane Gan, and Anatolij Bezemskij. Decision tree-based detection of denial of service and command injection attacks on robotic vehicles. In 2015 IEEE International Workshop on Information Forensics and Security (WIFS), pages 1–6, 2015.

[84] Hichem Sedjelmaci and Sidi Mohammed Senouci. A new intrusion detection framework for vehicular networks. In 2014 IEEE International Conference on Communications (ICC), pages 538–543, 2014.

[85] Ahmet Cetinkaya, Hideaki Ishii, and Tomohisa Hayakawa. Networked control under random and malicious packet losses. IEEE Transactions on Automatic Control, 62(5):2434–2449, 2017.

[86] Tongxiang Li, Bo Chen, Li Yu, and Wen-An Zhang. Active security control approach against dos attacks in cyber-physical systems. IEEE Transactions on Automatic Control, 66(9):4303–4310, 2021.

[87] Hongchun Qu, Libiao Lei, Xiaoming Tang, and Ping Wang. A lightweight intrusion detection method based on fuzzy clustering algorithm for wireless sensor networks. Advances in Fuzzy Systems, 2018, 2018.

[88] John D. Lee and Katrina A. See. Trust in automation: Designing for appropriate reliance. Human Factors: The Journal of the Human Factors and Ergonomics Society, 46(1):50–80, 2004.

[89] Anupam Das and Mohammad Mahfuzul Islam. Securedtrust: A dynamic trust computation model for secured communication in multiagent systems. IEEE Transactions on Dependable and Secure Computing, 9(2):261–274, 2012.

[90] Yunchang Zhang, Shanshan Chen, and Geng Yang. Sftrust: A double trust metric based trust model in unstructured p2p system. 2009 IEEE International Symposium on Parallel & amp; Distributed Processing, 2009.

[91] Jianli Hu, Quanyuan Wu, and Bin Zhou. Fctrust: A robust and efficient feedback credibility-based distributed p2p trust model. 2008 The 9th International Conference for Young Computer Scientists, 2008.

[92] Hao Hu, Rongxing Lu, Zonghua Zhang, and Jun Shao. Replace: A reliable trust-based platoon service recommendation scheme in vanet. IEEE Transactions on Vehicular Technology, 66(2):1786–1797, 2017.

[93] Mingxi Cheng, Chenzhong Yin, Junyao Zhang, Shahin Nazarian, Jyotirmoy Deshmukh, and Paul Bogdan. A general trust framework for multi-agent systems. In Proceedings of the 20th International Conference on Autonomous Agents and MultiAgent Systems, pages 332–340, 2021.

[94] Florian Dotzer, Lars Fischer, and Przemyslaw Magiera. Vars: A vehicle ad-hoc network reputation system. In Sixth IEEE International Sympo-

sium on a World of Wireless Mobile and Multimedia Networks, pages 454–456. IEEE, 2005.

[95] Ayman Tajeddine, Ayman Kayssi, and Ali Chehab. A privacy-preserving trust model for vanets. 2010 10th IEEE International Conference on Computer and Information Technology, 2010.

[96] Davide Calvaresi, Valerio Mattioli, Alevtina Dubovitskaya, Aldo Franco Dragoni, and Michael Schumacher. Reputation management in multi-agent systems using permissioned blockchain technology. In 2018 IEEE/WIC/ACM international conference on web intelligence (WI), pages 719–725. IEEE, 2018.

[97] Rabiya Khalid, Omaji Samuel, Nadeem Javaid, Abdulaziz Aldegheishem, Muhammad Shafiq, and Nabil Alrajeh. A secure trust method for multi-agent system in smart grids using blockchain. IEEE Access, 9:59848–59859, 2021.

[98] Jana Jost and Benedikt Mättig. Trust and reputation in heterogeneous multi-agent system for production processes based on the market economy. In 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), volume 1, pages 1321–1324. IEEE, 2020.

[99] Trung Dong Huynh. Trust and reputation in open multi-agent systems. PhD thesis, University of Southampton, 2006.

[100] Michael Sievers, Azad M Madni, Parisa Pouya, and Robert Minnichelli. Trust and reputation in multi-agent resilient systems. In 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC), pages 741–747. IEEE, 2019.

[101] S Rasoul Etesami and Tamer Başar. Dynamic games in cyber-physical security: An overview. Dynamic Games and Applications, 9(4):884–913, 2019.

[102] Afrand Agah and Sajal K Das. Preventing dos attacks in wireless sensor networks: A repeated game theory approach. Int. J. Netw. Secur., 5(2):145–153, 2007.

[103] Karel Durkota, Viliam Lisỳ, Branislav Bošanskỳ, and Christopher Kiekintveld. Optimal network security hardening using attack graph games. In Twenty-Fourth International Joint Conference on Artificial Intelligence, 2015.

[104] Thomas E Carroll and Daniel Grosu. A game theoretic investigation of deception in network security. Security and Communication Networks, 4(10):1162–1172, 2011.

[105] Charles A Kamhoua. Game theoretic modeling of cyber deception in the internet of battlefield things. In 2018 56th Annual Allerton Conference on Communication, Control, and Computing (Allerton), pages 862–862. IEEE, 2018.

[106] Mohammad Rasouli, Erik Miehling, and Demosthenis Teneketzis. A supervisory control approach to dynamic cyber-security. In International Conference on Decision and Game Theory for Security, pages 99–117. Springer, 2014.

[107] Charles A Kamhoua, Niki Pissinou, and Kia Makki. Game theoretic modeling and evolution of trust in autonomous multi-hop networks: Application to network security and privacy. In 2011 IEEE International Conference on Communications (ICC), pages 1–6. IEEE, 2011.

[108] Yuzhe Li, Ling Shi, Peng Cheng, Jiming Chen, and Daniel E Quevedo. Jamming attack on cyber-physical systems: A game-theoretic approach. In 2013 IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, pages 252–257. IEEE, 2013.

[109] Mbazingwa E Mkiramweni, Chungang Yang, Jiandong Li, and Zhu Han. Game-theoretic approaches for wireless communications with unmanned aerial vehicles. IEEE Wireless Communications, 25(6):104–112, 2018.

[110] Jianguo Sun, Wenshan Wang, Qingan Da, Liang Kou, Guodong Zhao, Liguo Zhang, and Qilong Han. An intrusion detection based on bayesian game theory for uav network. In 11th EAI International Conference on Mobile Multimedia Communications, page 56. European Alliance for Innovation (EAI), 2018.

[111] Farzaneh Farhadi, Hamidreza Tavafoghi, Demosthenis Teneketzis, and Jamal Golestani. A dynamic incentive mechanism for security in networks of interdependent agents. In International Conference on Game Theory for Networks, pages 86–96. Springer, 2017.

[112] Sadegh Farhang, Mohammad Hossein Manshaei, Milad Nasr Esfahani, and Quanyan Zhu. A dynamic bayesian security game framework for strategic defense mechanism design. In International conference on decision and game theory for security, pages 319–328. Springer, 2014.

[113] Quang Duy La, Tony QS Quek, and Jemin Lee. A game theoretic model for enabling honeypots in iot networks. In 2016 IEEE International Conference on Communications (ICC), pages 1–6. IEEE, 2016.

[114] Fei Miao, Miroslav Pajic, and George J. Pappas. Stochastic game approach for replay attack detection. In 52nd IEEE Conference on Decision and Control, pages 1854–1859, 2013.

[115] Ahmed H Anwar, Charles Kamhoua, and Nandi Leslie. A game-theoretic framework for dynamic cyber deception in internet of battlefield things. In Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, pages 522–526, 2019.

[116] Hayreddin Çeker, Jun Zhuang, Shambhu Upadhyaya, Quang Duy La, and Boon-Hee Soong. Deception-based game theoretical approach to mitigate dos attacks. In International conference on decision and game theory for security, pages 18–38. Springer, 2016.

[117] Yilun Shang. Resilient consensus in multi-agent systems with state constraints. Automatica, 122:109288, 2020.

[118] Liwei Yuan and Hideaki Ishii. Resilient consensus with multi-hop communication. In 2021 60th IEEE Conference on Decision and Control (CDC), pages 2696–2701. IEEE, 2021.

[119] An-Yang Lu and Guang-Hong Yang. Distributed consensus control for multi-agent systems under denial-of-service. Information Sciences, 439-440:95–107, 2018.

[120] Ahmet Cetinkaya, Kaito Kikuchi, Tomohisa Hayakawa, and Hideaki Ishii. Randomized transmission protocols for protection against jamming attacks in multi-agent consensus. Automatica, 117:108960, 2020.

[121] James Usevitch and Dimitra Panagou. Resilient finite-time consensus: a discontinuous systems perspective. In 2020 American Control Conference (ACC), pages 3285–3290. IEEE, 2020.

[122] James Usevitch and Dimitra Panagou. Resilient leader-follower consensus to arbitrary reference values in time-varying graphs. IEEE Transactions on Automatic Control, 65(4):1755–1762, 2019.

[123] Heath J LeBlanc, Haotian Zhang, Shreyas Sundaram, and Xenofon Koutsoukos. Resilient continuous-time consensus in fractional robust networks. In 2013 American Control Conference, pages 1237–1242. IEEE, 2013.

[124] Yilun Shang. Consensus of hybrid multi-agent systems with malicious nodes. IEEE Transactions on Circuits and Systems II: Express Briefs, 67(4):685–689, 2019.

[125] Zihao Cheng, Dong Yue, Songlin Hu, Hui Ge, and Lei Chen. Distributed event-triggered consensus of multi-agent systems under periodic dos jamming attacks. Neurocomputing, 400:458–466, 2020.

[126] Claudio De Persis and Pietro Tesi. Resilient control under denial-of-service. IFAC proceedings Volumes, 47(3):134–139, 2014.

[127] Yehan Ma, Dolvara Gunatilaka, Bo Li, Humberto Gonzalez, and Chenyang Lu. Holistic cyber-physical management for dependable wireless control systems. ACM Transactions on Cyber-Physical Systems, 3(1):1–25, 2018.

[128] Song Fang, Karl Henrik Johansson, Mikael Skoglund, Henrik Sandberg, and Hideaki Ishii. Two-way coding in control systems under injection attacks: from attack detection to attack correction. In Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems, pages 141–150, 2019.

[129] Sangjun Kim, Yongsoon Eun, and Kyung-Joon Park. Stealthy sensor attack detection and real-time performance recovery for resilient cps. IEEE Transactions on Industrial Informatics, 17(11):7412–7422, 2021.

[130] Kaveh Paridari, Niamh O'Mahony, Alie El-Din Mady, Rohan Chabukswar, Menouer Boubekeur, and Henrik Sandberg. A framework for attack-resilient industrial control systems: Attack detection and controller reconfiguration. Proceedings of the IEEE, 106(1):113–128, 2017.

[131] Sangjun Kim, Kyung-Joon Park, and Chenyang Lu. A survey on network security for cyber–physical systems: From threats to resilient design. IEEE Communications Surveys and Tutorials, 24(3):1534–1573, 2022.

[132] Hamed Shisheh Foroush and Sonia Martínez. On triggering control of single-input linear systems under pulse-width modulated dos signals. SIAM Journal on Control and Optimization, 54(6):3084–3105, 2016.

[133] Ahmet Cetinkaya, Hideaki Ishii, and Tomohisa Hayakawa. Event-triggered output feedback control resilient against jamming attacks and random packet losses. IFAC-PapersOnLine, 48(22):270–275, 2015.

[134] Shan Liu, Shanbin Li, and Bugong Xu. Event-triggered resilient control for cyber-physical system under denial-of-service attacks. International Journal of Control, 93(8):1907–1919, 2020.

[135] V. S. Dolk, P. Tesi, C. De Persis, and W. P. M. H. Heemels. Event-triggered control systems under denial-of-service attacks. IEEE Transactions on Control of Network Systems, 4(1):93–105, 2017.

RICHARD OWOPUTI received his B.S. degree in Electrical Engineering from the Federal University of Technology, Akure, Nigeria, in 2017 and the M.S. degree in Electrical engineering from the University of Florida, Gainesville, Florida, in 2021. He is pursuing a Ph.D. in Electrical engineering at the University of Florida, Gainesville, Florida, USA. He is also a Research Assistant in the Rising Laboratory, University of Florida, Gainesville. He works in the domain of connected autonomous vehicles, including fleet management. His research interest includes the investigation of the security vulnerabilities in multi-agent coordination and developing resiliency solutions to defend the coordination scheme against a spectrum of adversaries.

SANDIP RAY (SM'13) is an Endowed IoT Term Professor at the Department of Electrical and Computer Engineering, University of Florida at Gainesville, Florida, USA. His research involves developing correct, dependable, secure, and trustworthy computing through cooperation of specification, synthesis, architecture and validation technologies. He focuses on next generation computing applications, including Internet-of-Things applications, autonomous automotive systems, smart homes, intelligent implants, etc. Before joining University of Florida, Dr. Ray was a Senior Principal Engineer at NXP Semiconductors, and prior to that, a Research Scientist at Intel Strategic CAD Labs. In addition to Intel and NXP, his research found applications in AMD, IBM, Galois, Microsoft, and Rockwell Collins. He has a PhD from University of Texas at Austin and is a Senior Member of IEEE.