Hindawi
Computational Intelligence and Neuroscience
Volume 2022, Article ID 6732343, 26 pages
https://doi.org/10.1155/2022/6732343

Research Article

An Overview of Recent Advances of Resilient Consensus for Multiagent Systems under Attacks

Muhammad Muzamil Aslam,[1,2,3] **Zahoor Ahmed**,[4] **Liping Du**,[1] **Muhammad Zohaib Hassan**,[4] **Sajid Ali**,[3] **and Muhammad Nasir**[5]

[1]*School of Computer and Communication Engineering, University of Science and Technology, Beijing 100083, China*
[2]*Department of Electronics and Communication Engineering, University of Science and Technology China (USTC), Hefei, China*
[3]*Department of Information Sciences, University of Education Multan Campus, Lahore, Pakistan*
[4]*Department of Automation, Shanghai Jiaotong University, Shanghai 200240, China*
[5]*Department of Computer Engineering, The University of Lahore, Lahore, Pakistan*

Correspondence should be addressed to Liping Du; dlp2001@ies.ustb.edu.cn

Received 18 April 2022; Revised 26 May 2022; Accepted 31 May 2022; Published 2 August 2022

Academic Editor: Konstantinos Demertzis

Consensus control of multiagent systems (MASs) has been one of the most extensive research topics in the field of robotics and automation. The information sharing among the agents in the MASs depends upon the communication network because the interaction of agents may affect the consensus performance of the agents in a communication network. An unexpected fault and attack may occur on one agent and can propagate through the communication network into other agents. Thus, this may cause severe degradation of the whole MASs. In this paper, we first discussed MAS technologies. After that available technologies for the modeling of attacks and fundamental issues due to attacks on MAS attacks were discussed. We also introduced cooperative attack methodologies and model-based attack methodology. Objective of this article is to provide comprehensive study on recent advances in consensus control of MASs under attacks covering the published results until 2021. This survey presents different kinds of attacks, their estimation and detection, and resilient control against attacks. At the end, the survey accomplishes some potential recommendations for future direction to solve the key issues and challenges reported for secure consensus control of MASs.

1. Introduction

With advancement of communication and computer technologies, coordination control of MASs has got a lot of attention of researchers in different areas of engineering due to its broad applications in order to attain craving physical performances [1, 2]. There is speedy increment in progress of MASs because of improvement in communication, computing, and relevant technologies. MASs are also known as integration of communications, computations, physical processes, and controls which can play a key role in infrastructure [3, 4]. Cyber threats posture an actual and increasing problem, and to date, many countries struggle to counter them have lagged. However, capability to protect in contradiction of an attack or invasion must be upheld, and any country would be well served by discouraging its opponents from acting in the first place, at least when it comes to the most serious actions, namely, cyber warfare. There is vital role of cyber security in the era of technology also is biggest challenge to secure information in these days of technology. The first idea regarding cyber security in our mind is "cybercrime, cyber threat, or cyberattack"; those are increasing day by day. Several private and public sectors are taking various measures to secure such crimes, attacks, or threats.

Due to variety of applications [4], MASs have become research interesting area. Despite usefulness, MASs have a lot of security risks because of the interconnections of

various components and technologies. Since MASs are susceptible to spiteful threats and may result in the ailment of social life or loss of economic benefits. So, attack issues need considerable attention in the practical systems. In a smart transport system, an automatic controlled vehicle network can be a useful solution for an efficient and secure transport system and assists in problem-solving such as environmental protection, energy conservation, road congestion, and road accident. In contrast to the already present single-agent system, MASs are upgraded and scalable for enhancing energy efficiency and durability because they have the built-in ability for cooperative learning through the automatic decision. Recently, issues of MASs and their analysis have been well discussed in [5] but security issues of MASs have not been studied in the article and these systems are unsafe from cyberattacks and physical faults. So, we need to adjust, wait, or abandon at the time of system failure or attack [6]. MASs trust and access control issues have been highlighted. The researchers in [7, 8] highlighted MAS fault tolerant control procedure, and basic study was on reconfiguration way of topology. A very low-level attack or fault on an agent can disturb the system function and can cause damage to the system badly. Researchers have done wide research on cyber security and physical security in which detection and diagnosis, fault estimation problem, secure consensus, attack detection, and fault tolerant control were studied, and such research provides some basic methodologies and systematic suggestions for effective betterment of MASs security In Figure 1, there is framework of the intelligent transport system. Various kinds of attacks are present possible on the MASs such as man-in-middle attacks, deception attacks, cross-site scripting attacks, denial-of-service attacks, drive-by attacks, eavesdropping attacks, malware attacks, password attacks, phishing attacks, and SQL injection attacks.

In several fields of human activities, MASs have gained more attention, particularly the places where we need physical equipment, processes for control, and cooperating with the system and human, e.g., building automation networks, smart grids, and water sewerage plants. The progressing technologies, e.g., Industrial Internet or Industry 4.0 [9], are key points of MAS's importance; this idea transition will involve increasing autonomy, automation, and fulfilling fresh arrival of the production. The main motivation which is forcing the development of MASs is the conjunction of physical process and computational aptitudes, and components of the process happening in the physical surrounding are requirements. MAS scaling, e.g., large and small, is differentiated by the number of components involved [5].

These MASs are widely and geographically dispersed, heterogeneous, federated, and the critical system of life in which actuators and sensors are embedded networked for control physical world, monitoring, and sensing. There is no doubt that reserved scheduling via different own network or shared network plays a key role in the working of MAS. The selection of actuator or sensor for best performance of a specific action is an important decision, and also, proper management of actions is also important. Because of limited technology or physical constraints, there is risk of data transmission among network components, sensors, and actuators without any specific security instructions. In one point of view, interconnection of large scale of network components puts it in more complexity to save it from innate physical liabilities there. In another point of view, cyber integration generally sets up an underscore on protection and suppleness against threats and unseen from cyberspace [10, 11]. Hence, several new challenges are known to general or traditional control, software theory, and communication [12, 13].

The susceptibility of MASs in cyber parts permits attacks into the system in nonproductive and silent approach, e.g., insertion of some virus or worm in network component computerization or layers that should have medium access, could cause coordination packets distraction. In addition, there can be prohibited access of attacker to the monitoring centers and gaining decryption key in gain of normal operation [3]. It is clear that when there is no strict security protection, the attacker can either freely harm system dynamic or bring any agitation. For solution of optimization problem in selection of input or output that highlights attacks with least detect ability and maximum impact; there is a survey [14].

MAS consensus problem has been widely addressed [15, 16] with time delay. In MASs, we can found two types of delay, communication time delay (CTD) and input time delay (ITD). Here, CTD is linked between two agents interconnected time while ITD is related to data processing time. ITD may occur when controllers, actuators, or other components are linked to the network, while because of CTD, each agent may get information from a very near agent. CTD has been used in most real used applications such as computational and PWM delays in an LCL type grid-linked invertor and in controller area network bus of the distributed control network, induces delay. Here, we would like to discuss consensus problem of continuous time linear homogeneous MAS with CTD and ITD. ITD is considered multiple input time delays while CTD is single time delay. MAS consensus [14] problem has been widely studied from several studies, e.g., transportation control, coordinated defense system [17], power systems, and smart grids [18]. Consensus problem target is used to design a control law so that all agents can reach to a single point [14]. However, several present results on consensus problem were supposed as an ideal condition for investigation, e.g., secure network communication in between agents and unlimited resources network. In reality, there is presence of several impulsive issues, prime to a high security predicament and having influence on communication topology [14]. Nasty agents can grab this failing to interject communication between agents and disturb overall system stability in the multiagent network, while we can divide cyberattacks into the following cases on MASs, first is when there is an attack of nasty agent on agent and second is when nasty agent attacks to destroy the communication medium. In both cases, the communication graph is detached.

There is no high-level protection against future MAS threats or attacks. There are several types of key challenges

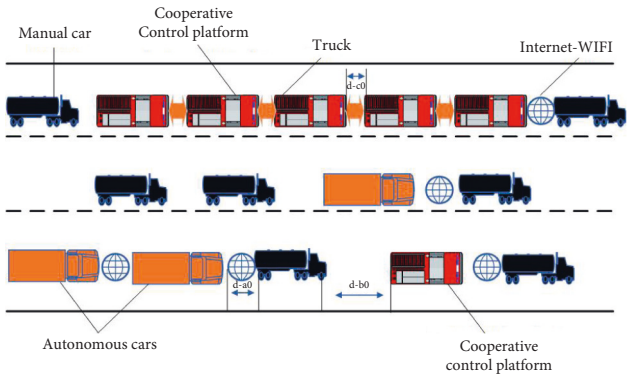

Figure 1: Intelligent transport system in coordination.

regarding MAS security, and these threats may be from the system inside such as sudden failure of the system, mobile networks security risks regarding human health, communication protocol weakness in smart grids, and limitations of physical systems. There is increasing requirement in new control system accuracy and reliability of each component. Any type of failure or fault of a system or component may lead to system performance degradation or reason for system instability or dramatic change in system operation [19].

Because communication networks consist of interacting agents which require safety and reliability to gain cooperative control and given challenges which are absent in single-agent systems such as MAS interconnection properties confuse the fault detection and identification and make worldwide and exact fault information complicated to accommodate and gain. Faults can vary both network and agent behavior suddenly. Single-agent fault can effect throughout the communication network. There may occur multiple faults at various time intervals and places. However, such challenging problems can be studied in proper form. Multiple agent composition configuration can give better termination than a single-agent system. Other than this, throughout failure of component or an agent that is not possible to adjust for the single-agent system may be effectively controlled by use of cooperation in between network connection and agents.

Inspired by the above study, practical and theoretical importance is given to review and classify some impressive MAS attacks (Figure 5) and working (Figure 6) to give a complete survey, Figure 10 describes secure and control approaches of DoS attack, and Figure 2 shows present work and key challenges required for study. Furthermore, it is of both theoretical and practical significance to present a study for safety of MASs at one platform and also to provide comprehensive survey of recent advances of resilient consensus for MAS under attacks. To see latest MAS complexity, security problems and system security are highly important. Threats can be physical, cyber, or containing both sides of MAS, and it needs a composite method for mitigation and identification of safety weaknesses. In present research, the purpose was to study weakness, challenges, mitigation schemes, attack types supposing scalability complexity of MASs, and distributive and security and safety challenges. The remainder of the paper is organized as follows: in Section 2, we studied MAS technologies; in Section 3, we studied attack modeling and methodology; in Section 4, we briefly discussed fundamental issues of MASs; in Section 5, we discussed problem formation; in Section 6, there is comprehensive study on cooperative attack methodologies; in Section 7, there is discussion on model-based attack methodology, in Section 8, deception attack detection or identification has been studied; and in Section 9, there are briefly discussed key challenges. Similarly, Figure 2 represents flowchart of paper. Table 1 explains all notations used in the manuscript.

2. MAS Supporting Technologies

Here, we study key technological improvements which are planned as well as links in between MAS and other basics which are studied to encourage technological developing chain that commanded the emergence of MASs. In several works, the concept such as smart object, embedded system, ubiquitous computing, smart environment, and sensor networks plays a key role in development of MASs. In case of time line, embedded systems are ancestors of all given knowledge appeared in the past and beginning fresh development in the field of microelectronics and replying critical problems such as remote control and automation. There is predefined functionality in embedded systems traversing across single or multiplied functions that are not easy to reprogram by the last user. The basic purpose of embedded systems was to control, design, and operate physical world process. Though, in beginning, embedded systems were closely compared to MAS or IoT, they were restricted by physical control function with the cyber space layer.

Figure 3 represents detailed general technologies supporting MASs. With the progress of technology and requirement to manage and control complicated systems, importance of the embedded system was clear and then there was an idea of the network embedded system. An important reason lacking down the availability of MAS was transition from one system to a connected system with more complexity. In view of this concept, sensor networks (SNs) strongly impact on the latest MAS. Actually, for information gathering, the SN contains a number of sensors deployed in specific place/areas. Presence of the SN eased improvements of smart objects, e.g., actuator or sensors containing microprocessor, power sources, and communication services. Thus, the SN cannot be supposed as freely unit, but as part of complicated systems. Fast development in modern computing systems containing MAS gave idea of ubiquitous computing. In addition, concept of computer system integration with daily activities enables them "unseen" for the last users. In some views, ubiquitous computing overlaps with other ideas, ambient intelligence, pervasive computing, and IoT. An important role of IoT is the establishment of capabilities for the last user to enhance present forms of everyday

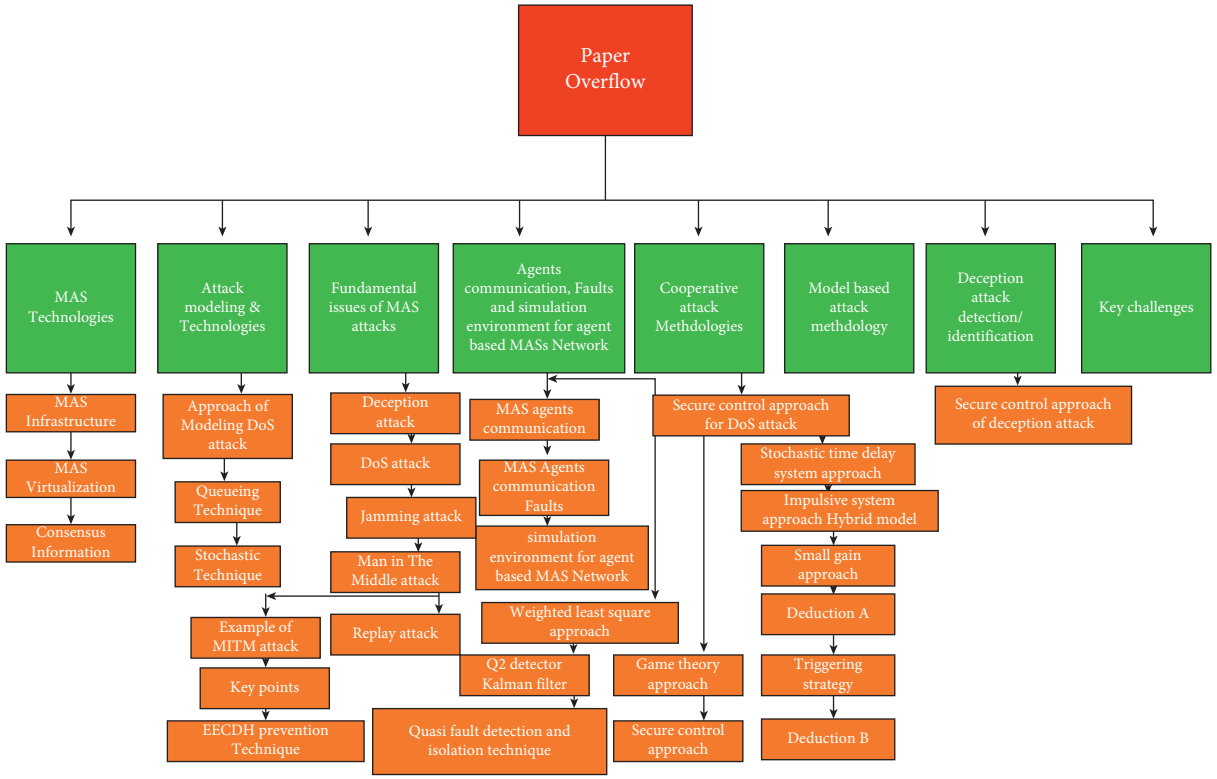

Figure 2: Paper flowchart.

Table 1: Explanation of notations.

Sr. no	Abbreviation	Explanation
1	MAS	Multiagent system
2	MASs	Multiagent systems
3	SN	Sensor network
4	IoT	Internet of Things
5	TCP	Transmission control protocol
6	IP	Internet protocol
7	NICV	Network Interface card virtualization
8	DoS	Denial-of-service
9	PC	Personal computer
10	LTI	Linear time-invariant
11	DDoS	Distributed denial of service
12	MITM	Man-in-the-middle
13	FDI	False data injection
14	PLC	Programmable logic controller
15	SCADA	Supervisory control and data acquisition
16	M2M	Machine to machine
17	SDN	Software define network
18	EECDH	Enhanced Elliptic Curve Differ-Hellman
19	WSN	Wireless sensor network
20	WLS	Weighted least square
21	LQG	Linear-quadratic-Gaussian
22	GT	Game theory

devices and improvement of private facilities by use of joined ubiquitous devices. It shows transition from the embedded system from predefined functionality to IoT and ubiquitous computing where an important need is adaptability and nimbleness. More and more improvements of computing systems run to presences of IoT and

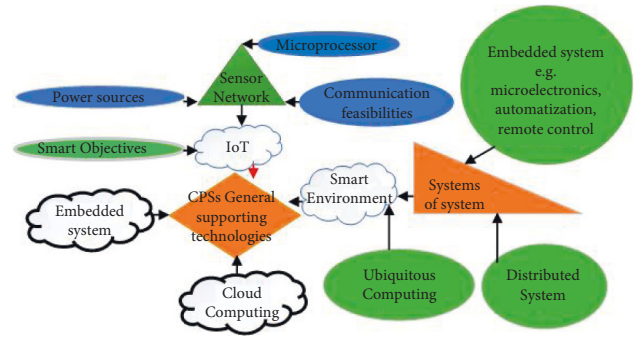

Figure 3: General technologies supporting MASs.

MAS. Actually, MAS is bit far from paradigm in which functional technologies are detached from information technologies to prototype where computational and physical elements are integrated. Although IoT has no specific definition, in some cases, IoT has been described as global infrastructure containing standard protocols and communication technologies that avail facilities given by "things" to diverse applications. In another case, IoT is a general term presenting the scenario types where smart objects are deployed, enabling worldwide communication through Internet or technologies. Hence, the concept of IoT is to represent the infrastructure of the devices worldwide. The scenario where worldwide connectivity is basic need, MAS is supposed to be in the first row of such systems that can join worldwide connectivity and can be distributed among enough units. Figure 4 shows MAS infrastructure.

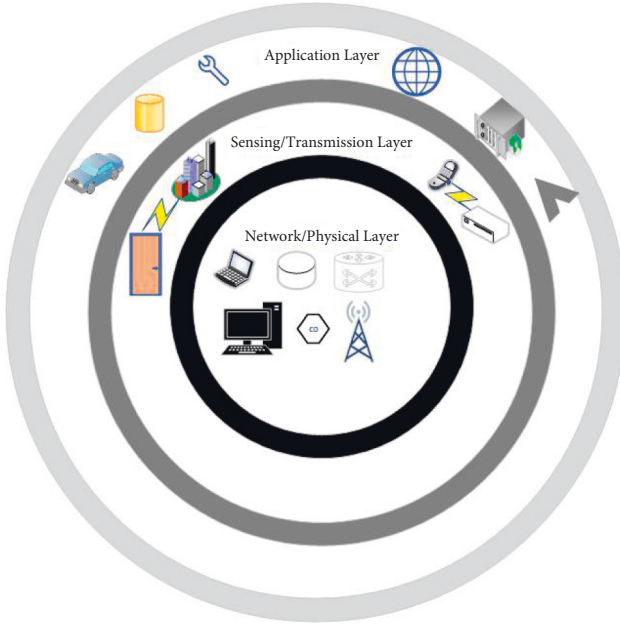

Figure 4: MAS infrastructure.

2.1. MAS Infrastructure. In development of every system, there is an important role of infrastructure, the same spread on to MAS. In general, basic element of MAS is to be considered as actuator, sensor, communication network, and controller. An important thing is that MAS can be a close-loop or open-loop system. In way of IoT, the global network has access through open loop such as Big Data and cloud computing which are addition in infrastructure of MAS. Hence, MAS may contain a huge number of heterogeneous devices containing actuators, sensors, etc. In addition, it also has roughly limitations on MAS, communication technologies, for instance, and requirement of safety protocols. We can say that such heterogeneity is the main challenge in MAS, so different kinds of devices gain care from a system. To see challenges in big and small systems, among challenges, for example, unified integrity, mobility also affects the entire system. It represents that transferring of devices may cause various problems and need to be taken in regular working of the system. Infrastructure is complicated span because it consists of both hardware and software. MAS architecture is complicated summarizing cyber and physical space. MAS architecture has been studied in [20], contains five-layer MAS infrastructure. In [14], it has been studied four-level MAS architecture. If MAS needs to be in connection with worldwide/global networks, such as Internet, TCP/IP can be the best candidate in which two last layers, physical and data, accordingly are shown by the single level. Transport, network layers, and application form other three layers part. Explained categorization of physical threats in fault estimation, detection, and tolerant of MASs has been studied in Table 2.

2.2. MAS Virtualization. In MAS, the basic purpose of virtualization is to abstract or hide complicated detail such as technical detail from above laying layers and to permit stretchy sharing resource, so that resources or working given as facilitation. So, MAS joints physical and cyber space and contains throughout process from signal to complexity of applications. There are some virtualization techniques such as network virtualization which is divided into subtypes such as router virtualization, network interface card virtualization (NICV), and link virtualization, application virtualization, and device virtualization.

Table 2: Types of fault and work on fault estimation, fault detection, and fault tolerant.

Fault type	Fault estimation	Fault detection	Fault tolerant
Actuator fault	[21]	[22]	[23, 24]
Sensor fault	[25, 26]	[27]	[28, 29]
Actuator and sensor fault	[25, 30]	[31, 32]	[19, 33, 34]

2.3. Consensus Information. Suppose a decision-making agent network with $\dot{x}_i = u_i$ attentive in accessing via local communication with nearby on $G = (V, E)$. By accessing consensus, it seems asymptotically joining to single-dimensional contract space characterized by

$$x_1 = x_2 =, \ldots = x_n. \tag{1}$$

Such contract can be represented as $x = \alpha 1$ in which $1 = (1, \ldots, 1^T)$ and $\alpha \in \mathbb{R}$ is joined decision of all agents in the group. Suppose $A = [a_{ij}]$ is adjacency matrix of G graph. Agent i set in nearby is N_i and represented as

$$N_i = \left\{ j \in V : a_{ij} \neq 0 \right\}; V = \{1, \ldots, n\}, \tag{2}$$

where i agent communicate with j agents which is neighbor of i. All set nodes and nearby agents represent E edge set of graph as $E = \left\{(i, j) \in V \times V : a_{ij} \neq 0\right\}$. $G(t) = (V, E(t))$, and a dynamic graph is that where edges set $E(t)$ and $A(t)$ adjacency matrix varying time. $N_i(t)$ nearby set in the dynamic graph of each agent is well. Such dynamic graphs are helping for explaining the mobile sensor technology network and flocks. The linear system is

$$\dot{x}_i(t) = \sum_{j \in N_i} a_{ij}\left(x_j(t) - x_i(t)\right). \tag{3}$$

It is a distributed consensus algorithm, and it follows that sum of state of all node is an invariant quantity. When applying this condition at time $t = 0$ and $t = \infty$, we get

$$\alpha = \frac{1}{n} \sum_i x_i(0), \tag{4}$$

while in another way, if there is asymptotically access of consensus, then mandatory cooperative result is equal to initial state average of all nodes. With such variance characterization, the consensus algorithm is known as average consensus algorithm and has several applications in distributed computing on networks such as sensor fusion in the sensor network.

In compact form, system dynamic can be represented as

$$\dot{x} = -Lx, \tag{5}$$

where L = graph Laplacian G and it can be defines as

$$L = D - A, \tag{6}$$

where $D = \text{diag}(d_1, \ldots, d_n)$ is degree matrix of G with zero off-diagonal elements.

L has right eigenvector of 1 linked with zero eigenvalue because of the identity $L_1 = 0$.

3. Attack Modeling and Methodology

3.1. Approach of Modeling DoS Attack. We will study two important techniques for DoS attacks modeling in MASs: one is queueing technique and also another is stochastic technique.

3.1.1. Queueing Technique. Like computers, firewalls and routers are considered networking devices, providing poor performance in supervision of DoS attacks, though trade with maximum rate because of memory resource constrains, interrupt processing, and input output processing and central processing units. However, packet loss and delay jitter are vastly affected under attack which can cause disturbance to the control system performance, e.g., mean squared error, rise and settling, and overshoot of percentage. The transmission of packet in the network control system under DoS attack is approached to smear simple techniques which are based on several input queues [35–37]. Two techniques are discussed as follows:

(1) DoS attack is launched by attackers to an endpoint from the system or PC to surrounding area nearby to endpoint. In this way, a huge number of packets are lost.

(2) DoS attack can be launched by attackers with the use of remote system to initial edged routers foremost to leisurely down network connection between controller and a remote plant.

DoS is considered as singularity that can save control signal from required time preserved. It is done by single host. It shows that control and measurement channel may be provoked individually. Hence, it can be supposed that in the process of DoS attack, it seems complicated to receive or send data. Suppose $\{m_j\}_{.j\in X_0}$ in which $m_0 > 0$, which is DoS 0/1 transition sequence; here, 0 is for "off" and 1 is for "on" situation, e.g., that time when DoS variation a transition from 0 to 1 and that time there is possibility of interruption of communication, so

$$M_j \triangleq \{m_j\} W[m_j, m_j + \rho_j]. \tag{7}$$

M_j is representing time interval of jth DoS attack. That length may be $\rho_j \in \mathrm{R}_{\geq 0}$, this is the time when there is no communication, consider $\rho_n = 0$, and here, jth DoS attack is shown as individual pulse at m_j time. An input is generated by an actuator which is based on fresh received controller data through DoS attack. Given $\rho, \varphi \in \mathrm{R}_{\geq 0}$ with $\varphi \geq \rho$, suppose that

$$\begin{aligned} &\therefore(\rho, \varphi) \triangleq \coprod_{j\in X_0} M_j \prod [\rho, \varphi], \\ &\frac{{}^{\circ}\rho\varphi \triangleq \rho\varphi}{\therefore\rho\varphi}. \end{aligned} \tag{8}$$

It represents that at each interval $[\rho, \varphi], \therefore(\rho, \varphi)$, $^{\circ}(\rho, \varphi)$ and $[\rho, \varphi]$ are representing to time instants set, when communication is permitted and stopped, respectively. Applying control signal to all $\rho \in \mathrm{R}_{\geq 0}$, it can be written as

$$\begin{aligned} w(\rho) &= \mathrm{PQ}\left(\rho_{P_{(\rho)}}\right), \\ w(\rho) &= \mathrm{PQ}\left(\rho_{P_{(\rho)}}\right). \end{aligned} \tag{9}$$

It shows that for all $\rho_j \in \mathrm{R}_{\geq 0}.P(\rho)$ modern fruitful control approach, the same to proposed techniques is used in [38]. In concluded form, we can say that there is disadvantage of this start and end of approach is not found and is most useful to post records.

3.1.2. Stochastic Technique. Generally, cyberattacks are performed when the system is weak to detect the threat and results in security defilement. In practice, such attacks are introduced by the series of actions to compare security services such as confidentiality, integrity, and availability of MAS applications such as telecommunication, military, banking, smart power grids, and transportation systems. To trace the threats and cyberattacks such as file-less malware, advance persistent threat, and zero days, CPS has become focus of interest. Other than this, a number of techniques were introduced to predict cyberattacks against MAS, in which several techniques have been developed using a stochastic approach such as Hawkes process model, Markov chain model, negative binomial distribution model, and Poisson model. In the fast-growing trend of CPS attacks, attacks are considered to be launched externally against MASs within a given amount of time and using stochastic distribution models such as Bernoulli model [38, 39] and Markov model [40]; from the LTI system, the Bernoulli model can be seen:

$$\begin{cases} Y(P+1) = B_Y(P) + \mu(P)A_W(P) + u(P), \\ F(P) = \gamma(P)H_Q(P) + h(p). \end{cases} \tag{10}$$

For the Markov model, we supposed the following:

$$\begin{cases} Y(P+1) = B_Q(P) + \mu(\delta(P+1))A_W(P) + u(P), \\ F(P) = H_Q(P) + h(P). \end{cases} \tag{11}$$

From (6), $h(p)$ = measurement noise and $u(P)$ = process noise.

These measurement noise and process noise are commonly known as independent and identically distributed. Here, with 0 mean Gaussian random vector and covariance Q, $\mu(P), \gamma(P)$ are independent identically distributed. Bernoulli is relevant to existence of DoS attack on measurement and process noises [41].

Now, see (7).

$\mu((P+1)) \in \{0,1\}$ is known as Markov controlled DoS attack sequence which stops transmitting of control signal packets to actuator in which (P) is similar to interior state of attacker [42].

4. Fundamental Issues of Multiagent Systems

Basic purpose of MAS classification is to explain overview and fundamental issues regarding cyberattacks. Some general examples of cyberattacks are distributed denial of service (DDoS), man-in-the-middle (MITM), deception attack, password attack, and malware attack. Cyberattack is an offensive action, while if there is possibility of occurring of attacks, then it is known as cyber threat, while cyber risk is interconnected with the word threat which estimates the probability of proportional loss which may occur. Figure 5 shows basic types and subtypes of security attacks.

Here, we will discuss few cyberattacks and fundamental issues discussed in latest research. Figure 6 shows working of MAS security attacks.

4.1. Deception Attack. There is hastily emerging phenomenon of use of deception technology in contemporary cyber security as a feasible means active and intelligent postbreach defense. Similar to any unruly technology it happens with fallacies. Cyber security needs to be changed from being dependent on largely detecting untrue things within a cloud of healthy activity to being focused on stopping cybercrime, which tends to tempt, phish, deceive, and trap users. Deception tactic often proves to be healthy for defense and attack. Deception technology has progressed far yonder the honeypot perception. Now a day's deception is being active in baiting and luring attackers to a deception environment. Deception, also known as malicious attacks and false data injection (FDI) attacks, is defined and studied in [9, 43–45], e.g., nominated malicious system Stuxnet which is able to be reprogrammed and running code in PLCs in SCADA system cause aberration from required conduct. In power grids, transmission system adversaries can send attack to hack remote terminal units, e.g., in substations, there are sensors [12]. For another example of such kind of attack, see study [14, 46, 47]. Deception changes cyber security by providing sole breadcrumbs and traps for industry specific environment, legacy system, IoT, and devices where low cost regularly excludes security structures. Authors in [48] considered measurement output to encounter deception attack based on Bernoulli distribution during signal transmission. To describe random property of deception attack, Bernoulli distribution has been deployed [14]. Deception attack has been used in the term of limited time boundness [14].

4.2. DoS Attack. Denial-of-service (DoS) attack denies or makes slow to the authentic users to access a resource web, e.g., emails and network. DoS attack is policies, and those are usually used for profession of communication capitals in order to forbid the measurement transmission and cause supreme possible worsening of performance of the system. The common DoS model has been studied in [49] in which DoS topographies are discussed with DoS duration and DoS frequency. Similarly, improvement in this idea has been studied for production with the output controller of dynamic feedback.

Complicated form of DoS is distributed denial of service (DDoS) [50, 51] which is also known as coordinated attack, where a huge number of cooperated machines work to achieve DoS attack [52]. However, because it can be easily created, so DDoS is easily available, has high impact and low cost of systems, consisting ability of fully detach an association [53]. It is represented that there is instability of power grids because of attacks and could give long delay jitter on network control system packets. The division of DoS attack in radio frequency identification is because of the reasons studied in [54, 55], e.g., desynchronization attack, system jamming, kill command attack, tag data modification, and random DoS attack as shown in Figure 5.

In conclusion of this DoS attack, aforementioned forms of DoS attacks are implemented for the classification of DoS attack in radio frequency identification systems as studied in [29, 54, 56]. Therefore, they could be present in many forms of MASs.

4.3. Jamming Attack. Such DoS attack refers to condition when one channel is occupied by an attacker for prevention of other node from its use which causes blocking of communication. For obtaining optimal defense mechanism for the network control system, stochastic game theory is applied [29, 57, 58]. Dynamic collaboration among attackers and sensor transmitters in the network control system was projected as the double-player stochastic game. In stochastic game, cost functions contain source cost used for conduction of attack actions, cyber-layer defense, and as possible harmed dynamic act of the network control system. Interaction effect between defender and attacker on dynamic concert of the network control system was supposed by the following cost function. Finally, a stochastic dynamic programming delinquent has been explained for gaining optimal defense mechanism.

In [59–61], security in remote state approximation of MASs has been studied. Communication between remote approximator and sensor node was taken through wireless channel that may be attacked by a jamming attacker. Best decision of process making of both attacking and communicating was discussed in case of consideration of energy constrains for both attacker and the sensor. Markov theory was used for gaining equivalent solutions, and constrained relax delinquent was designed.

For maximization of linear quadratic Gaussian used optimal jamming attack, it controls cost function while supposed energy constraints studied in [59, 60, 62]. Corresponding cost and optimal jamming agenda were consequent after studying the usage of cost function under a free attack agenda. The fresh analytically model was studied in the influence of attack jamming on broadcasting. A jamming attack for optimal energy efficient by wireless channel under jammer attacker energy constraints is studied in [63].

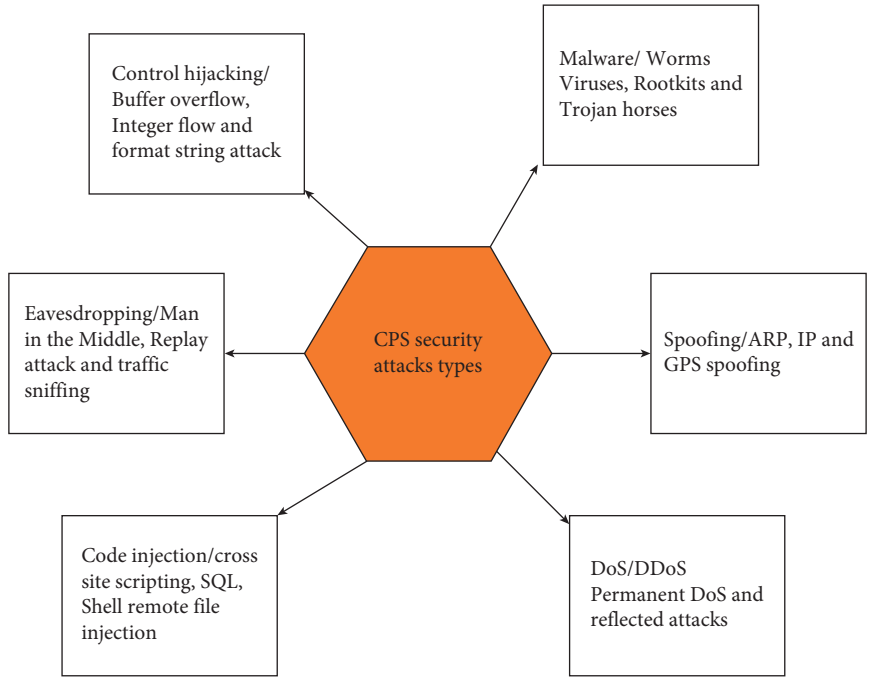

Figure 5: Types/subtypes of MAS security attacks.

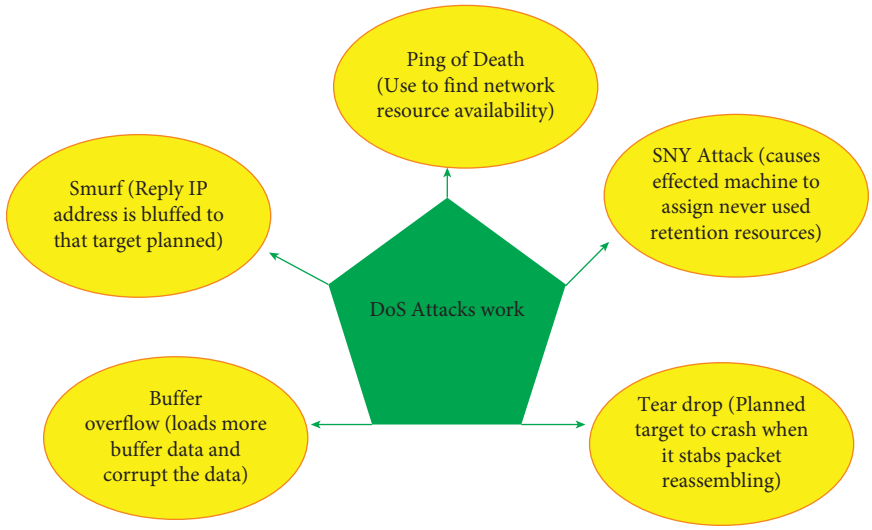

Figure 6: Working of DoS attacks.

These attacks forced by power constrained pulse width-modulated jammers are supposed to be moderately recognized, which is jammer period and unchanging inferior destined and jammers asleep periods are identified. Controller synthesis problem that is an event based for network control systems and strong event triggered communication scheme was studied in [27]. In conclusion, piecewise Lyapunov function is applied to guarantee exponential stability of the system.

4.4. Man-in-the-Middle (MITM) Attack. Generally name "man in the middle" is derived from a game scenario known as basketball, where two players aim to throw a ball to each other, and one of them tries to clutch it [64]. MITM is well-known computer security attack, which gives a great challenge to security professional. Actually, it hits real data flowing between confidentiality, endpoint, and integrity of the data. For analyzing and categorizing the MITM scope, researchers should read [65] survey.

Basically, MITM takes benefit of authentication protocol weakness used by communication networks. Usually, the third party is responsible for authentication that issues certificates because the system of certificate production becomes another way of solid weakness. MITM attacks permits unauthorized parties to snoop data by backdoor.

4.4.1. Example of MITM Attack. About in 2015 [66], it was known that Lenovo machines are available with already installed adware known as superfish which injects adds on browser such as Internet Explorer and Google Chrome. Superfish installs a compiled certificate into Windows certificate database. It leaves all secure stock layer (SSL) certificates given by Hypertext transfer protocol secure (HTTPS) that are linked with personal certificates. Such situation may provide an access to hackers to receive sensitive information such as bank account information, transactions, or user lifestyle..

Internet of Things (IoT) is progressing from smart home to smart cities and making our lives dependent. With the passage of time, billions of M2M will be interconnect with each other, and the big problem is to manage such a big problem for network administrator. Intensive-security methods, classical computing method as antivirus, and encryption are not directly installed software. With network infrastructure, it is compulsory to make IoT devices more secure.

Opposite to the traditional security network, software define network (SDN) [63] gives several new features, as centralized control and network programmer, which skilled the owner to manage network automatic in a dynamic and flexible way. We can see that IoT future [67] is SDN dependent. Open floe channels security issues of IoT, e.g., MITM, are studied in [68].

Distributed methodology for agent network permission targeted for execution of the distributed algorithm to control MITM attack is studied in [69, 70] which intends steering algorithm result towards erratic values of risky configurations. An example of MITM attack is shown in Figure 7.

Figure 7(a) shows victims without attackers, and Figure 7(b) shows victims with attacker, contenting message between A and B without notice.

4.4.2. Key Points. There are following key points of MITM:

(1) MITM permits hackers to intercept confidential data.

(2) MITM is session hijacking type.

(3) MITM permits hackers to insert malicious data and sites in form misty from genuine data.

(4) MITM exploits real-time nature of data transfer and communication to go hidden.

(5) MITM contains hackers inserting themselves as proxies or relays in an ongoing data transfer or appropriate conversation.

Researchers can study the following literature for their research interest of MITM attack [71–73].

4.4.3. EECDH Prevention Technique. Enhanced Elliptic Curve Differ-Hellman (EECDH) prevention technique for MITM attack is well studied in current research [45] which improves the security level. Keep secure MITM attack where communication carrier clears themselves before cooperating their keys, to use Differ-Hellman key exchange for communal verification, so that during cloud sharing, data privacy sustained.

4.5. Replay Attack. Such kind of deception attack happened when adversary succeed in recording some of the transmission data, e.g., in MAS, sensing data are injected [74, 75]. This form of attack is supposed to happen in two ways, e.g., in 1st way of Figure 7 recording data of attacker from system and injecting the same data in the system, and another way is attack could be outside carrying that subject to physical systems represented in Figure 8 [76]. Likewise, an attacker formed communication connection in between two last points to enclosure observed messages in various areas in globe generally present in WSN [77]. In designing, such attack could be assumed as changeable delays with unidentified data on variable rates and upper bounds. Applying time-delay system concept jointly by optimization methods acceptable max upper bound can be premeditated [3].

There is no requirement of system information in such form of attack, containing information on designed estimator and controllers; for detection, this activity makes it complicated. Adopting counters and time-stamp in the transmitted data is solution opposite to such attack. Two phases, first and second of replay attack, has been shown in 8.

There is not enough research that studies controlling of MASs subject to replay attacks, e.g., recording vista control variation direct to replay attack is discussed in [78], which gives an explicit and simple connection in between computing, attacking horizons, and infinite-horizon cost. Then, asymptotic exponential stability of the system is ensured by availing enough condition set; see one more example study [74, 79]. Feasibility terms of replay attack and countermeasure suggestions those enhance the possibility of detection by supposing control performance are discussed in [80]. And integrity attack on the control system is countermeasured and analyzed proficient of showing these attacks were not assumed. For further example of such attack, we can see [79, 81, 82].

5. Agents Communication, Faults, and Simulation Environment for Agent-Based MAS Network

In this section, we will study MAS agent communication, faults, and simulation environment.

5.1. MAS Agent Communication. We know that MAS contains self-directed agent group which works in cooperation with each other through other communication medium to gain considered goals, and find number of usage in different areas such as physics, biology, mathematics, social science, and computer engineering.

Since 1962 [83], agent's communication has been studied. Mainly used communication approaches are message passing, speech act, and blackboard. In message passing, agents directly message each other as shown in Figure 9(a). There is use of broadcast or point to point agent

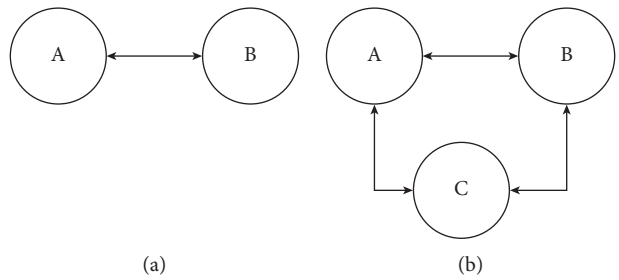

Figure 7: Victim with and without attack.

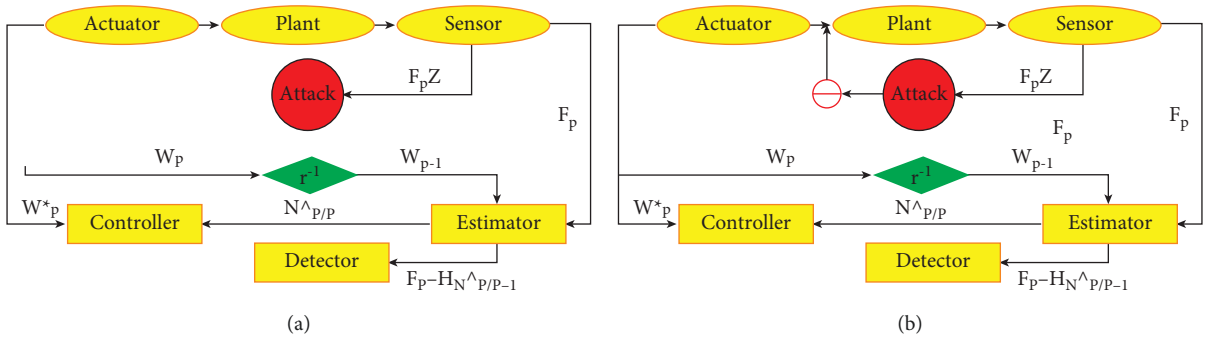

Figure 8: First and second phase of replay attack.

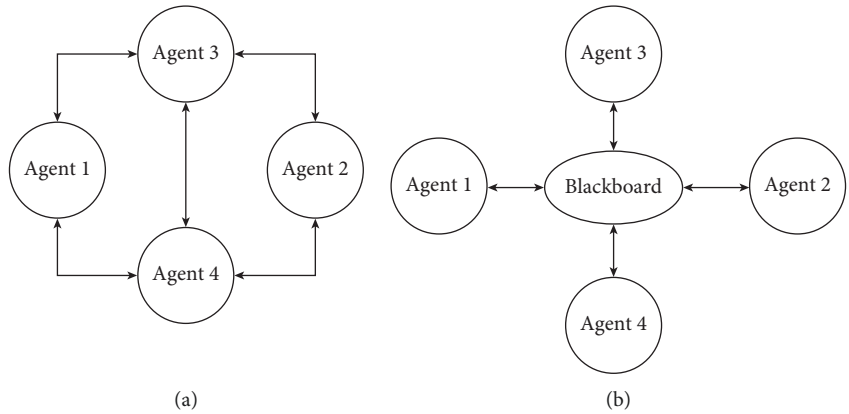

Figure 9: An overview on communication approaches in MAS.

communication to communicate with other agents. In the broadcast communication, one agent sends message to all nearby agents while in former agent one can directly talk to another agent in case of other agent address information.

In speech act, researchers in [84] studied that some sentences or utterance verbs are act as speech acts that vary physical environment such as in general environment if general person uses sentence that "I now make you man and wife" such kind of sentence have impact on physical environment by introducing new condition and rule. Agent action can be as a speaker, which produces utterance to vary listener belief [84, 85].

In blackboard communication, agents share data with each other in collaboration by use of central repository known as blackboard, Figure 9(b). In this, data of each agent are stored in blackboard which are accessible and readable by other agents. Blackboard uses control information for controlling agent's access. It is important for message semantics that need to confirm communicating agents with each other who have the same understanding of exchanged data. Sometimes in heterogeneous agents, it can be a challenging task.

5.2. MAS Agent Communication Faults. Basically, for MAS, two kinds of faults are considered known as network fault and agent fault. Network fault occurs in the communication network and may disturb communication performance while agent fault that can occur in internal components of actuators, agents, and sensors. There are

three types of classification of agent's faults, sensors faults, agents fault, and actuator fault which may affect agent dynamic.

5.3. Simulation Environment for Agent-Based MAS Network. Here, we are studying various evaluations and modeling methods used for metrics performance that differ depends upon task and MAS application of the considered agent-based system in comparison with state of the art. There are three basic evaluation methods, MATLAB, Java agent development framework, and GAMA.

Using MATLAB, we study MAS performance, especially with mathematical complex environment. In addition, it is adjustable to Java agent development framework for more work on MAS performance.

Java agent development framework is mostly used among simulators in MAS. Its admiration stalks from following properties. It benefits from third-party libraries and also is Java based. It is also written on foundation of intelligent physical agent's standard. For designing MAS, it has graphical interface. It supports simulation distributed systems, is open source, and can link to Matlab, and also it skins complexity of MAS.

Third, GAMA is simulation and modeling platform for agent-based system development. There are some advantages of GAMA such as it supports widely level MAS that contains a huge number of agents, it is useful for simulation purpose of any kind of MAS application, and it supports intuitive agent-based language such as GAML.

Studied simulation methods are specifically for MAS, while because of large-level usage, specific evaluation methods are used for system analyzing in particular application and can be deployed for agent-based system simulation performance to see issues in that application.

This is an important method which is usually used in the deception attack in sensor networks which contains the hypothesis test with predefined probabilities of binary hypothesis [86, 87]. Cooperative spectrum sensing performance limit is evaluated subject to Byzantine attacks; however, false data affect the fusion center, because of that output of wrong sensor increased [88, 89]. On binary hypothesis, a similar ratio detector is considered to manage with already determined fixed error for security of smart grid in sensor network data [20, 87, 90], energy frame work that is deep learning based, and block chain based is well studied in [20, 89]. A detector based on progressed similar has been studied in [91–93] and supposed for unobservable and observable circumstances in the SCADA system. An example of such methods has been applied in [94]. Important hypothesis applied is that all node transmitted packets are arbitrary; by this way, probability of next packet will not affect in verdict a packet to be nasty. In conclusion, there can be several forms of attacks those can affect single or several packets. For calculation of trust values, it is to be considered that node is transferring "X" packets; here, j packets are supposed to be normal. Observation of $x(X) = j$ distribution is studied by given binomial distribution:

$$K(x(X) = j|K) = \binom{X}{j} K^j (1-k)^{X-j}. \tag{12}$$

Here, K shows that i^{th} packet probability is normal k(K) = no. of normal packets this model intends to guess the probability of $K(W_{X+1} = 1|x(X) = j)$ and result out either the $X + 1$ packet is in normal form. With the use of Bayesian theorem, the following probability distribution is calculated:

$$\begin{aligned}&(K)\left(W_{X+1} = \frac{1}{x(X)}, = j\right)\\ &= K\left(W_{X+1} = 1x(X) = j\right)K(x(N) = j.\end{aligned} \tag{13}$$

Here, we can apply marginal probability distribution:

$$\begin{aligned}k(x(X) = j) &= \int_0^1 k(x(X) = p|k)g(k).vk,\\ K\left(W_{X+1} = 1, x(X) = j\right) &= \int_0^1 K(x(X) = j|k)g(k)k.vk.\end{aligned} \tag{14}$$

There are no data for k; now, it is considered that it can be found by uniform prior distribution $g(k) = 1$; here, $k \in [0, 1]$. Hence, we can rewrite above equations (12)–(14) as

$$\begin{aligned}K\left(W_{X+1} = 1, x(X) = j\right) &= \frac{\int_0^1 K(x(X) = j|k)g(k)k.vk}{\int_0^1 k(x(X) = p|k)g(k).vk},\\ &= \frac{p+1}{X+2}.\end{aligned} \tag{15}$$

In resultant from equation (15), both of normal packets number j and X which is whole packets can be found in WSN, after the collection of traffic information. By applying suitable threshold, we can find malicious node. Some numerical results of such malicious nodes has been studied in [92, 95]. With the use of this model, we can find malicious node.

5.4. Weighted Least Square (WLS) Approach. It is an effectual consistent attack detection method for dimension data. Mostly, it is applied in power systems and smart grids [96–99]. By comparison of predefined threshold and constructed measurement residual, we carried out a bad resultant.

Suppose

$$r = MY + c. \tag{16}$$

Here, $M = [m_{\text{ab}}]_{i*j}$ is known as measurement Jacobian matrix with full column rank, when $j > x$, m and r are considered states vector and measurement, respectively, and c is system noise effecting. Estimated delinquent is used to solve the m^* of variable m, which is better for measurement of meter r w.r.t equation (10). Estimated measurement r^* and observed measurement have a difference that is defined

as $z = r - r^* = r - MY^*$. WLS problem is to find an estimate m^* which slow the index performance $D(Y^*)$, which can be found by the given formula:

$$\min_{y*} D(Y^*) \coloneqq (r - MY^*)^Z U(r - MY^*). \tag{17}$$

In this weight matrix, $U \coloneqq \sum -1$.

To simulate 1st order optimal situation, $D(Y^*)$ is studied in [43]:

$$y^*\left(M^Z UM \coloneqq Cr\right), \tag{18}$$

where "C" is pseudoinverse of M and $CM = 1$.

5.5. Q^2 Detector Kalman Filters. Here, we used characteristics of Kalman filter residual instead of WLS, to make it feasible for good or bad data:

$$\begin{aligned} Q_{p+1} &= B_{Q_p} + A_{b_p} + u_p, \\ F_p &= H_{Q_p} + h_p. \end{aligned} \tag{19}$$

In this, $b_p \in R^k, Q_p \in R^k$ and $F_p \in R^j$ are the control input, state variable, and system measurements, respectively; $h_p \approx \nabla(0, R)$and $u_p \in R^k$ are measurement noise and process noise, respectively. We can calculate $Q^*_{p/p}$ with the use of given Kalman filter:

$$\begin{aligned} \mathcal{M}^*_{0|-1} &= N^*_0, \\ K_{0|-1} &= \varepsilon, \\ Q^*_{p+1} &= B_{Q_p} + A_{b_p}, \\ K_{p+1|p} &= BK_p B^Z + S, \\ P_p &= K_{p|p-1} H^Z + R\Big)^{-1}, \\ Q^*_p &= K_{p|p-1} + P_p\left(F_p - HQ^*_{p|p-1}\right), \\ K_p &= K_{p|p-1} - P_p HK_{p|p-1}. \end{aligned} \tag{20}$$

It has been known that Kalman filter exists in $F_i - HQ^*_{i|i-1}$ for equation (19), with LQG controller, and Kalman filter is Gaussian independent identically distributed [22]. Suppose

$$e_p \coloneqq \sum_{i=p-\mathrm{T}+1}^{p} \left(F_i - \mathrm{C}Q^*_{i|i-1}\right)^Z \sigma^{-1}\left(F_{i-}\mathrm{C}Q^*_{i|i-1}\right). \tag{21}$$

Here, e_p = has an Q^2 distribution among jT independent degree in normal operation which shows the lower probability of greater e_p. T is window size. Here,

$$e_p \overset{<M_0}{>_{M_1}} \rho. \tag{22}$$

where M_0 represents null hypothesis, M_1 represents under attack hypothesis, ρ represents threshold discussed in [100, 101] used for the SCADA system, and the same results have been shown in [102]. Q^2 detector with cosine has been explained in [95, 103, 104] for the detection of false data injection attacks which affects smart grid. An algorithm is discussed for the detection of deception attack in an application which could be remote state application, smart sensors used for data receiving [105]. Second application of such kind has been studied for the detection of bias injection attacks for stochastic rectilinear dynamical scheme [12, 106–109]. Multiclass support vector machine was discussed for building an intrusion detection model.

5.6. Quasi Fault Detection and Isolation Techniques (FDI). FDI is famous and widely used in the networked control system. It identifies the fault presence, location, and fault type because it contains the monitoring system. This technique is helpful in detection of exterior attack in MASs. Attacks were supposed as unidentified inputs which effects both of states and measurements [110–113]. Using graph theory, undetectable attacks were characterized and also with the use of distributed and centralized monitor have been planned for the detection of distinguishing attacks. Based on geometric approach, a fault detection method has been implemented for detection of cyberattacks and fault in power systems or networks [114, 115]. The common system was applied for the detection of deception attacks and sensor actuator [44, 114]. Likewise, a model diagnosis system and free-fall detection were studied for designing cyberattack detector for the distribution system of water [26]. For detection and differentiation of both cyberattacks and fault, an intelligent generalized predictive controller was intended [25, 116]. Cyberattack can be targeted by recognized weakness in the system, which is weak point of FDI, different from losers commonly arbitrary or random. For designing the required robust system, this technique needs cautious investigation in order. In conclusion, it is important because of highly study, which lot of research has been done on for detection of cyber security in power systems, e.g., [117–120].

5.6.1. Argument. Bayesian detection with binary hypothesis has been broadly studied and pragmatic in sensor network data fusion [23, 121,122]. In meaning of state approximation, there is need of system noise in a stochastic framework for the attack detection method, because it allows a probabilistic state approximation [64, 123]. Hence, there is need to smear mean and variance for state disruption distribution shown as freely variables. Providing of confident state approximation is important in many present applications, e.g., system guidance and navigation, target tracking, and attack [64, 123]. In short, modeling the state distributions in some sets supposed to be unidentified, but limited noises are more suitable. Therefore, $\aleph^2$ is mostly useful based on holding discrepancies in approximation conduct which forecast by a model. Resultant unidentified but limited sounds are suboptimal, and attack detection feasibility is reduced.

6. Cooperative Attack Methodologies

Comparing to other kinds of attacks, e.g., DoS attack and replay attack, we got no much more interaction of researchers. This is because of phenomenon that fixed on controlling of MASs. Both defending and detection against DoS attacks in a state approximation delinquent were

studied in [124, 125]. Data of sensor are transferred to the estimator by a packet, falling communication network. Already defined Kalman filtering [126, 127] for approximation of state for the untrustworthy communication system is pragmatic in this network. First of all, hypothesis testing detection problem is articulated, while supposing already known knowledge of network statics. Secondly, there were considered two preventing policies with the use of secure coding packet slant for recompensing the absence data, and another is improved on transmission power up gradation to control the blocking upshot of attack.

In [126, 127], game theory approach has been studied, e.g., collaboration between attacker and sensor is designed as zero sum stochastic game, which finger to DoS attack in remote state approximation. Presence of Nash equilibrium was primarily studied for such kind of game, and later on the best policies were planned for fixing sensor transmission power. For calculation of asymptotic performance of remote approximator, planned form game is applied in [128, 129].

For nonlinear chaotic systems, sliding mode control with actuator fault and decentralized sliding mode for heterogeneous MASs problem of fault tolerant control considering both DoS and network fault is discussed in [25, 131]. It is to be supposed that network fault contains of deterioration, signal attenuation, and perturbations of couplings those are in nonlinear form. Reimbursement of perturbed couplings and faulted were gained to apply a strategy which is known as slide mode planned strategy; by way of unidentified constraints of approximation, then the mathematical analysis method and Lyapunov stability theory were applied to assurance the asymptotic management of the nonlinear confused system. We see another example of approximation of delinquent in MASs exposed to DoS attack studied in [7, 130–132].

6.1. Secure Control Approaches for DoS Attack. For controlling MASs exposed to DoS attack, many researchers worked; those are shown in Figure 10.

6.1.1. Stochastic Time-Delay System Approach. Here, DoS is designed as stochastic process with signal delay. Deception and DoS attacks are supposed to be freely stirring and designed as Bernoulli distributed white sequences in [12, 131]. Suppose the discrete time stochastic system with measurements and noise effecting the system, as

$$\begin{cases} Q_{P+1} = \left(B_0 + \prod_{i=1}^{z} \tau_{a,p} B_a \right) Q_P + \mathrm{BW}_P \Big), \\ F_P = \left(H_0 + \prod_{a=1}^{r} \tau_{i,P} H_a \right) Q_P. \end{cases} \tag{23}$$

Here, $F_P \in R^{x_f}$ is measurement of sensor and $Q_{P+1} \in R^{x_m}$ is state vector, and $W_P \in R^{x_w}$ is input of controller. $B_a\,(a = 0, 1, \ldots, z)$, A and $H_a\,(a = 0, 1, 2, \ldots, l)$ are with appropriate dimension and constant matrices. $\tau_{a,p} \in R\,(a = 1, 2, \ldots, z)$ and $\tau^*_{a,p} \in R\,(a = 0, 1, 2, \ldots, l)$ are multiplicative noises with unity variance and zero means, and jointly uncorrelated with P and a, z and l those are positive integer, A rank is considered to be x_w, and to study this kind of problem, we see the given model of attack:

$$F^{\varphi}_{P_r} = \left(\mu^{\widetilde{=}\varphi}_{p_r} + \partial^{\varphi}_{P_r} h^{\varphi}_{P_r} \right) + \left(1 - \mu^{\varphi}_{P_r} \right) F^{\varphi}_{P_{r-1}}, \tag{24}$$

where $F^{\varphi}_{P_r}$ = data received by controller and $h^{\varphi}_{P_r} \in R^{x_f}$ = stands for attackers injected signals as in (23):

$$h^{\varphi}_{P_r} = -F^{\widetilde{=}\varphi}_{P_r} + {}^{\varphi}_{p_r}, \tag{25}$$

where ${}^{\varphi}_{p_r}$ is freely fixed signal which satisfies

$$\begin{aligned} \left\| \delta^{\varphi}_{P_r} \right\| &\le \mathrm{epsilon}_2, \\ \mathrm{Prob}\left\{ \mu_{P_r} = 0 \right\} &= 1 - \widehat{\mu}, \\ \mathrm{Prob}\left\{ \mu_{P_r} = 1 \right\} &= \widehat{\mu}, \\ \mathrm{Prob}\left\{ \partial_{P_r} = 0 \right\} &= 1 - \widehat{\partial}, \\ \mathrm{Prob}\left\{ \partial_{P_r} = 1 \right\} &= \widehat{\partial}. \end{aligned} \tag{26}$$

μ_{P_r} and ∂_{P_r} = white sequences Bernoulli distributed with 0 and 1 value. Probability is given in (26). In (26),$\dot{\partial} \in [(0, 1)]$and $\partial \in (0, 1)$ are identified constants. Some enough states are gained to confirm the security needs of the system in which we gained some enough conditions.

6.1.2. Impulsive System Approach Hybrid Model. Here, we showed a system that is beneath DoS attack showed by the impulsive system. Resilient control techniques and resources aware are designed with malicious DoS attack studied in [133–135]. Specifically, an event-based control scheme which is output that is output based was pragmatic to control to get the communication strategy and control in lass of nonlinear feedback systems which is provoked by exogenous troubles.

Suppose

$$p: \begin{cases} \widehat{Q}_K = g_K (Q_K, W, U), \\ F = f_r (Q_K), \end{cases} \tag{27}$$

where p = plant. Here, $U \in R^{x_u}$ = uproar input, $F^* \in R^{x_f}$ = state vector, $W \in R^{x_W}$ = control input, and$F \in R^{x_f}$ output of plant:

$$E: \begin{cases} \widehat{Q}_q = g_q \left(Q_q, \widehat{F} \right), \\ W = f_K \left(Q_q, \widehat{F} \right). \end{cases} \tag{28}$$

In this, $Y_c \in R^{x_q}$ = controller state, $F^* \in R^{x_f}$ = fresh gained measured output, and $W \in R^{x_w}$ = controller output; resultant output is $r = e(Q)$ in which $r \in R^{x_r}$ and $Q = (Q_k, Q_q)$. Here, attack is DoS and interval of attack is represented by $\{M_x\}_{x \in X} \in I_{\mathrm{Dos}}$; at this time period, there is no communication between controller and sensor since attack. DoS attack collection time is given as

$$\varnothing \triangleq \sum_{x \in X} M_x. \tag{29}$$

To apply framework, hybrid model F^* updating can be

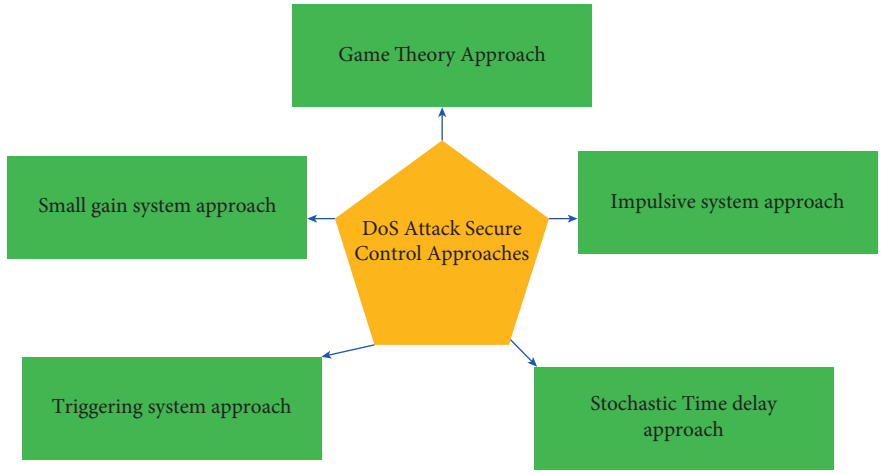

Figure 10: Secure control approaches of DoS attack.

$$\widehat{F*} = \begin{cases} F, \text{ When } \rho_b \nexists \varnothing, \\ \widehat{F}, \text{When } \rho_b \exists \varnothing. \end{cases} \tag{30}$$

Transmission error $c \triangleq F^* - f$ can be

$$c^+ = \begin{cases} F, \text{ When } \rho_b \nexists \varnothing, \\ \widehat{F}, \text{When } \rho_b \exists \varnothing. \end{cases}$$

$$\rho_{\text{miet}} = \begin{cases} \dfrac{1}{L_r}\left(\dfrac{r(1-\gamma)}{2(0/0)((x/l)-1)+1+0}\right), \gamma > L, \\ \dfrac{1}{L}\dfrac{1-\gamma}{1+\gamma}, \gamma = L, \\ \dfrac{1}{L_r}\arctan h\left(\dfrac{z(1-\gamma)}{2(\gamma/\gamma+1)((\aleph/L)+1+\gamma)}\right), \gamma < L. \end{cases} \tag{31}$$

Equation (31) represents maximum allowed transmission interval limited ρ_{miet} that is characterized, where $z = |(\gamma/L)^2 - 1|, L \geq 0$ is fixed, $\gamma \in (0,1)$ shows present information in local area at a mechanism known as event triggered mechanism, and we obtained γ as

$$\langle \nabla h(Q), g(g,c,u) \leq -\sigma(\|Q\|) - \sigma(\|F\|) - M^2(Q,W) - \epsilon_1(U(c)) + \sigma^2 U^2(c) + \vartheta^2 \|U^2\| \rangle. \tag{32}$$

This condition explanation is well studied in [135]. At the end, to suppose DoS attack in normal form, these DoS attacks are banned in form of duration and frequency.

6.1.3. Small Gain Approach. Distribution system stabilization problem exposed to DoS frequency characterization, DoS attack, and preserved stability duration is studied in [135]. To preserve communication resources, a hybrid communication technique is also supposed. By using of hybrid transmission technique, zero behavior can be saved and load communication can be compact efficiently. e.g., a large-scale system contains X interacting subsystem is supposed with given model:

$$\aleph_a^*(\varphi) = B_a Q_a(\varphi) + A_a Q_a(\varphi) + \coprod_{b \in X_a} M_{\text{ab}} Q_b(\varphi). \tag{33}$$

In this, B_a, A_a and M_{ab} are with suitable breadth. $Q_a(\varphi)$ and $W_a(\varphi), \varphi \in R_{>0}$ are control and state input of the subsystem. Input control applied to "a" subsystem is

$$W_a(\varphi) = P_a Q_a \varphi_P^i + \coprod_{b \in X_i} L_{\text{ab}} Q_b \varphi_p^b, \tag{34}$$

where L_{ab} = controller coupling gain.

Suppose $\{m_x\} x \in X_0, m_0 \geq 0$ representing off/on DoS transmission, e.g., DoS displays time instant transmission from 0 to 1. Hence,

$$M_x \triangleq \{m_x\} \cup [m_x, m_x + \rho_x]. \tag{35}$$

Equation (35) shows x^{th} DoS time instant. ρ_x is length on which there is DoS attack on the network; suppose

$$\therefore(\rho,\varphi) \triangleq \sum_{x \in X_0} M_x \sum(\rho,\varphi). \tag{36}$$

This is subclass of (ρ, φ), and also there is DoS attack on the network.

(1) Hypothesis A. Equation (36) is supposed to be constant in DoS frequency, in this $\tau \in R_{>0}$ and $\rho_O \in R_{>0}$, as

$$x(\rho,\varphi) \leq \tau + \frac{\varphi - \rho}{\rho_O}. \tag{37}$$

(2) Hypothesis B. $p \in R_{\geq 0}$ and $Z \in R_{>1}$ are present as constant in DoS duration:

$$|\therefore(\rho,\varphi)| \leq p + \frac{\rho - \varphi}{Z}. \tag{38}$$

(3) Hypothesis C. When there is no DoS attack, an intersampling interval ∇ is present, e.g.,

$$\left\|c_a(\varphi)P\right\| \le \in_a \left\|Q_a(\varphi)\right\|. \tag{39}$$

$\in_a$ is appropriate design constraint.

6.1.4. Deduction A. Equation (33) is representing the distributed system, and equation (34) is for control input, so for this distributed system and control input communication of a plant controller on collective network with Hypothesis C, and sampling ∇ interval. For any DoS attack, the large-scale system is asymptotically constant. Hypothesis A and B with freely τ and p and ρ_O and Z are as follows:

$$\begin{aligned} &\frac{1}{Z} + \frac{\nabla_*}{\rho_O} < \frac{\tau_1}{\tau_1 + \tau_2}, \\ &\left\|\mathscr{L}_1(P)\right\| + \left\|\mathscr{L}_2(P)\right\| \le \mathscr{L}. \end{aligned} \tag{40}$$

And its subsets are discussed, and second deduction detail is discussed in [136].

6.1.5. Triggering Strategy. Equation (33) is representing the distributed system and equation (34) is for control input, so for this distributed system and control input communication of a plant controller on collective network with Hypothesis C, and sampling ∇ interval. For any DoS attack, the large-scale system is asymptotically constant. Hypothesis A and B with freely τ and p and ρ_O and Z are as follows:

$$\frac{1}{Z} + \frac{\nabla_*}{\rho_O} < \frac{\tau_1}{\tau_1 + \tau_2}. \tag{41}$$

We supposed a plant jammer-operator, in which communication between plant and operator is effected by jammer studied in [137]. For reduction of the system communication system, an event triggered time order was assumed. Suppose $W \in R^j$ and $Q \in R^x$ be input and state vector, respectively. Given system is to be supposed

$$\begin{aligned} \aleph^*(\varphi) &= B_Q(\varphi) + A_W(\varphi), \\ w(\varphi) &= PQ(\varphi_P), \quad \forall_\varphi \in \left[\varphi_P, \varphi_{P+1}\right], \end{aligned} \tag{42}$$

where B, A, and P, are proper dimensions matrices, and $\{\varphi_P\}_{p\ge1}$ = triggering time sequence. Now, suppose $c(\varphi) = Q(\varphi_P) - Q(\varphi)$, For all $\in \left\lfloor \varphi_{P,}\varphi_{P+1} \right\rfloor$, system is stable, if function $W(Q) = Q^Z K_P$ connected with $\lfloor E \rfloor > 1$ is supposed the control $W(\varphi)$ which at time Z_P updated, to see given triggering law

$$\left|c(\varphi_P)\right|^2 = \in \frac{\lfloor E \rfloor - 1}{\lfloor \mathrm{KAP} \rfloor.^2} \left|Q(\varphi_K)\right|^2, \quad P \ge 1. \tag{43}$$

This law time sequence is

$$\varphi_{p,x} = \left\{\varphi_1 \text{ satisfying above equation } \varphi_1 \in \left\langle (x-1)Z,\ (x-1)Z + Z_0^1 \right\rangle\right\} \cup \{xZ\}. \tag{44}$$

Here, equation (42) is with asymptomatically stable, and equation (44) is triggering law.

6.1.6. Deduction B. See equations (42) and (44) if assumed conditions mollifies. It is studied in [137]:

$$\begin{aligned} &\frac{(1-\in)Z_1^0(|E|) - 1}{2} > |K| \log(\mu), \\ &\mu \coloneqq \exp\left(\left(Z - Z_0^1\right)\alpha(B + \mathrm{AP})\right) \\ &\quad + \frac{\mathrm{AP}}{\alpha(A + \mathrm{AP})} * \left(\left|\frac{\mathrm{AK}}{B} + 1\right|\right)\left\{1 - \exp\left(\left(Z - Z_0^1|A|\right)\right) * \left(1 - \exp\left(\left(Z - Z_0^1\right)\alpha(B + \mathrm{AP})\right)\right), \alpha(B + AP) < 0. \end{aligned} \tag{45}$$

Control strategy for the linear and nonlinear system with the use of the triggered method subjected to DoS attacks depends on study of ISS-Lyapunov function has been described in [138–140]. Maximum %age of time loosing response data deprived of the foremost system is instability was characterized and an event-based controller for that presence of minimum inside sampling time is definite has been supposed.

6.2. Game Theory (GT) Approach. GT deals with planned collaboration in between several named players and decision makes [107, 140, 141]. Each player preference order in between many options is increased in an impartial purpose for player, and all players try to optimize own impartial function. It depends on the alternate of another player in any nontrivial game, and this process of optimization depends on the selection of second players [142]. For applications of game theory in the network, we can study the literature

[143–145]. For getting secure control in a lot of research studies, this method was pragmatic. Disadvantage which is because of DoS attack is designed as Markov process depends on the game among defending strategies and attack [145]. Using Lyapunov theory, four theorems were derived for assurance of the stability of system. For handling computation complexity of optimal strategies for both players, a Nash Q-learning algorithm is studied [144]. Sensor data are transmitted through a large number of channels remotely, making them vulnerable to malicious attacks. There is need to select one channel to sensor in between these paths with less probability to attack with data transmitting data. It is also decided by attackers that which channel is suitable for attack, e.g., [119]. From literature review, we can find some more examples of applying such kind of approach [142, 146].

CoFence Mechanism is assumed for DoS defense attack that endorsed "domain help domain" cooperative network between the NFV-based domain network. Furthermore, there is a dynamic resource allocation characterization for game, and we establish a game model to get incentive-compatible, effective, reciprocal, and fair resource allocation method to work on Nash equilibrium [147]. In [148], the authors supposed conflict between attacker and defender and designed a game theory framework for collective security detection.

6.3. Secure Control Approach. For the event triggering system or discrete time system, stochastic time-delay approach can be applied subject to arbitrary DoS attack. The system is designed using Markov process and Bernoulli process with identified statically information to govern the freely present DoS attack. In an event triggered system, impulsive system approach can be applied and is powerful in network control systems as studied in [135]. To reduce the communication in between system part triggering strategy is enough, since signal sent only specific condition of triggering is despoiled, that will minimize burden of communication.

Need of throughout information of the system is one limitation in game theory. With imperfect and incomplete information, game theory application is a developing field in network privacy and security. In addition, there is need of agents for correct estimation of security game limitations. For security measures and attack prevention, observation capabilities avail required basis [80, 149].

7. Model-Based Attack Methodology

There are two possible forms of occurrence of deception attacks: one is that targeted attacks which defined states are effected and random attacks where arbitrary measurements are defined [48]. In view of control engineering, it is designed as stochastic process [48, 150]. We supposed the following system for best understanding of this idea:

$$\begin{cases} Q(P+1) = B_Q(P) + A_W(P), \\ F^*(P) = H_Q(P), \\ F(P) = F^*(P) + \mu(P)h(P). \end{cases} \tag{46}$$

$W(P) \in R^{x_w}, Q(P) \in R^{x_n}$ and $F(P) \in R^{x_b}, F^*(P) \in R^{x_b}$ are the control input, states, received signal, and measured output, respectively, and $\mu(P)$ is Bernoulli distributed with deception occurrence possibility with values one and zero; so,

$$\begin{cases} \text{Prob}\{\mu(P) = 1\} = \mu^*, \\ \text{Prob}\{\mu(P) = 0\} = 1 - \mu^*. \end{cases} \tag{47}$$

Description of deception attack is

$$h(P) = -F^* + \tau(P). \tag{48}$$

(1) Note. It is considered that data transferred by attackers mean injected fault data could be subtracted into two steps according to representation of equation (48)

$-F^* =$ for cancellation of original signal, and $\tau(P)$ is supposed to be freely limited energy signal as characterized in [150]:

$$\coprod_{P=0}^{\infty} \tau^Z(P)\tau \le \tau^{-2}. \tag{49}$$

For the time varying class system, variance-constrained distributed problem direct to several divisions of noises, unidentified but limited turbulences, there is also study of deception over sensor network [151]. Present measurement at each node is gathered from both of neighbors and single sensors. There is insertion of deception signals into right signals of input used for controlling W_P and output measurements $F_{a,p}$ during data transmission process shown in Figure 11. An article for designing of deception attack is studied in which nasty signals are inserted by the adversary into both measurement and control data during information communication process via network communication. Following signals effect signals.

8. Deception Attack Detection or Identification

It is conscious issue of deception attack estimation for prevention of any detection mechanism since attack form, the main target of affecting stability of the system. Bias injection issue hitting Kalman filter in the system containing chi-square detector is studied [152]. It proved that worst situation problem quadratically constrained can be reduced as quadratic program permits to gain criterion that is useful for selection of sensors for safe and condition on number of sensors need to keep the attack effect with encoded threshold.

Centralized security problem for stochastic system linear time-invariant with multidate-sensors fusion subject to deception attack is studied in [6]. Data transferred on each sensor by adversaries as extra signal which makes feasible boundary situations such as [25, 150]. For formulation individual rate discrete time systems, there was use of lifting technique. Using stochastic analysis techniques, enough conditions were gained for gaining already determined original system security level. For effecting uniform quantization, deception attack was supposed in distributive

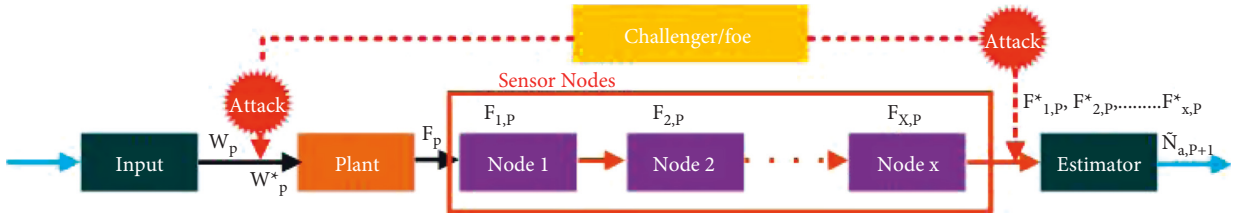

Figure 11: Deception attack schematic.

recursive filtering problem of stochastic system discrete time-delayed [6, 83, 153]. We supposed the following system for showing its working:

$$\begin{aligned} Q(P+1) = &\left(B_0(P) + \prod_{r=1}^{Z} \epsilon_Z(P) B_r(P) \right) Q(P) \\ &+ \left(B_0^{\varnothing}(P) + \prod_{r=1}^{Z} \epsilon_r(P) B_r^{\varnothing}(P) \right) Q(P+\rho) \\ &+ A(P) \in (P). \end{aligned} \tag{50}$$

With sensors "x" studied as

$$\begin{aligned} \widehat{F}_a(P) &= \left(H_0(P) + \widehat{\epsilon}_a(P) H_a(P)\right) Q(P) + O(P) h_a(P), \\ a &= 1, 2, 3, \ldots, x. \end{aligned} \tag{51}$$

$Q(P)$ state that directly cannot be observed. $\widehat{F}_a(P)$ is sensor "a" output without quantization. $\widehat{\epsilon}_a(P)$ and $h_a(P)$ are white distortions with zero means and conversance unity, collectively uncorrelated "P" and a, $\widehat{\epsilon}_a(P) \in R$, and $\epsilon_Z(P) \in R$ ($Z = 1, 2, 3, \ldots, z$) are multiplicative noises with unity variance and zero means, and jointly correlated in P. ρ and z are positive integers. $B_r(P), B_r^o(P)$ and $H_a(P)$ are identified fixed matrices with well-suited dimensions. In equations (48)–(50), the same dimension effect is studied. Upper limitation for error filtering covariance has been studied in [31].

For modeling of distributed state estimator, event triggered scheme is applied to the wireless sensor network for false data injection attack [31, 154]. Each sensor estimate is checked if it attacked at all-time step before transmission of data to nearby sensor, and it may stop in case of attacked. Using event triggered scheme, an optimal estimator gain is supposed to reduce mean square estimation fault covariance, and modeled distributed estimator stability is certain with enough condition of driving. Already the discussed Bayesian method was pragmatic for both estimation and detection of states for MASs subject to turn attack signal and wrong measurements [154, 155].

Kalman filter which ensures a safe state estimation algorithm for the stochastic dynamic system was studied in [156–158]. Adversary caused freely subset of sensors is to be supposed in this problem, and an upper limit on sensors effected by attacks was designed to uphold an adequate state approximation fault. Insecure estimation situation is studied for the control system of network direct to fault data insertion attack containing a $\aleph^2$ detector. In addition, a precise algorithm was used, and defense of rare communication channels instead of defending all is studied. Nonlinear stochastic discrete time-delay filtering problem in systems pretentious by arbitrary deception attack and arbitrary sensor saturation were studied in [159]. Suppose the system

$$\begin{aligned} Q(P+1) = &B_Q(P) + B_{\varnothing} \aleph(P - \varnothing(P)) + \mathrm{Ag}(Q(P)) \\ &+ A_{\varnothing} g_{\varnothing}(Q(P - \varnothing(P))) + O_{\epsilon}(P). \end{aligned} \tag{52}$$

$Q(P) \in R^{x_n}$ = state vector $\in (P) \in R$ = zero mean Gaussian, and $B, B_{\varnothing}, A, A_{\varnothing}$, and O are identified constant matrices with suitable dimensions. The following condition is satisfied by nonlinear functions g and $g_{\varnothing}$:

$$\begin{aligned} &[g(Q) - P_1 Q].^Z [g(Q) - P_2 Q] \le 0, \\ &[g_{\varnothing}(Q) - Z_1 Q]^Z [g_{\varnothing}(Q) - Z_2 Q] \le 0. \end{aligned} \tag{53}$$

In this, P_1, P_2, Z_1, and Z_2 are appropriate dimensions real matrices. $P_1 = P_1 - P_2$ and $Z = Z_1 - Z_2$ are positive symmetric definite matrices. Given filter designed is supposed in this system:

$$\widehat{Q}(P+1) = Y\widehat{Q}(P) + X_f(P). \tag{54}$$

To ensure the required security level in the filtering system, an enough condition is derived with stochastic analysis technique. For filter obtaining, inequality linear matrix with constraints of nonlinear is resolved.

8.1. Secure Control Approaches of Deception Attack. Deception attack affected discrete time stochastic nonlinear system problem of security control with quadratic cost criterion is studied in [160]. Both actuating and measurement signals were directed to deception as in Figure 11:

$$W(P) = \widehat{W}(P) + \partial(P) \in (P). \tag{55}$$

In Figure 12, B1 and B2 are supposed to be attacker, in system false data system, e.g., $\in (P) = -\widehat{W}(P) + \mathscr{L}_1(P)$ and $h(P) = -\widehat{F}(P) + \mathscr{L}_2(P)$.,

$$W(P) = \widehat{W}(P) + \partial(P) \in (P), \tag{56}$$

$$F(P) = \widehat{F}(P) + L(P) h(P). \tag{57}$$

where $W(P)$ = actuator input, $\widehat{W}(P)$ = controller outputs directed to attacks, $F(P)$ = controller gained signal, $\widehat{F}(P)$ = sensor measurement directed to attacks, $\epsilon(P)$ and $h(P)$ = transmitted signals by attacker, and $\partial(P)$ and $\gamma(P)$ = Bernoulli distributed mutually independent with stochastic variable one and zero, with following probabilities:

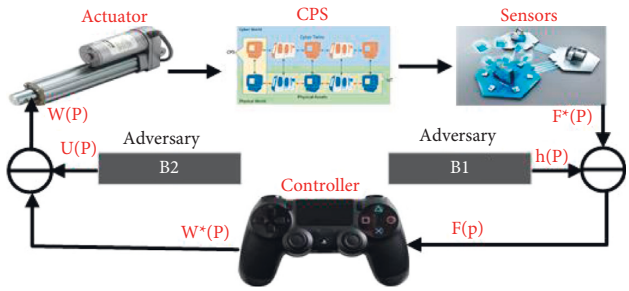

Figure 12: Deception attack schematic.

$$\begin{aligned}
&\text{Prob}\{\partial(P) = 1\} = \widehat{\partial},\\
&\text{Prob}\{\partial(P) = 0\} = 1 - \widehat{\partial},\\
&\text{Prob}\{L(P) = 1\} = \widehat{L},\\
&\text{Prob}\{L(P) = 0\} = 1 - \widehat{L}.
\end{aligned} \tag{58}$$

In Figure 8, B1 and B2 are supposed to be attacker, in system false data system, e.g., $\in (P) = -\widehat{W}(P) + \mathscr{L}_1(P)$ and $h(P) = -\widehat{F}(P) + \mathscr{L}_2(P)$.

Structuring a dynamic output field or controller feedback is the basic purpose of this delinquent, e.g., given security in possibility is attained while gaining higher limited of the already choose quadratic cost function. Hence, to derive some enough situations by matrix discriminations form in input-to-state framework stability in possibility stochastic analysis approach was pragmatic. To apply matrix inverse lemma controller obtained upper bound.

In [161, 159], there is study of the secure network predictive control system and an architecture for secure and dependent automotive MASs, integrating data message digest algorithm, encryption standard algorithm, predictive control recursive network method, and time-stamp strategy. Predictive control recursive networks rely on time delays, which is pragmatic to ensure the performance of the system, especially when a deception attack influences it.It will accomodate the consequences of attacks and network flaws such as package disorder, package dropout, and time-varying delay.

We studied consensus control and consensus management problem in [162]. There was latest definition of quasi-consensus given for describing the consensus performance with constraints on each agent to keep within few ellipsoidal regions at all-time instant, which based on given topology. In addition, measured result is available for controller from both nearby and individual agents. For gaining quasi-consensus, enough situations are gained with the use of recursive matrix for required control system inequalities.

A resilient control system [139, 163] has been supposed for network control systems effected by false data injections attacks, so that using measurement data and control input they could not be find. Attack of zero variable on plant state variable is not identified during attack, and it seems after result of attack. Hence, a strong Gaussian controller which is linear quadratic is supposed so that there is online updating of Kalman filter from data transferred by an active version of comprehensive prospect ratio detector with the capability to speedy improve of behavior after attack [164].

Actuator attacks and sensor attacks for controller of MASs were proposed in [74, 164–166], and a progressive adaptive strong control scheme is discussed for adversarial mitigating attack in the cyber physical system. Nussbaum function with speedy progressive rate and estimation mechanism is adaptive bound. The double-step back step method was applied to mitigate effects of actuator attack and sensor attacks, and to apply exponentially decaying barrier Lyapunov function, a variable state was controlled.

A feasible control delinquent of MASs data-driven direct to actuator attack class is studied in [166], an unidentified nonstop time linear physical system containing outside instabilities was supposed, and input control signal sent via network layers is supposed to be vulnerable to cyberattacks. For eradicating actuator attack effect, nearby optimal performance and stability of MASs can be gained by data-based adaptive essential sliding-mode control approach. Use of abnormal monitor detection mechanism contains detector threshold information, frequency characteristics, and attack structure for a set of frequency constrained actuator, and sensor attack can be studied in [166]. Explained categorization of cyber threats in cyberattack detection of MASs and secure consensus of MASs has been studied in Table 3.

Table 3: Categorization of cyber threats in cyberattacks, detection, and consensus of MASs.

Attack types	Work on cyberattack detection of MASs	Secure consensus of MASs
Actuator fault	[7, 54,167]	[90]
Sensor fault	[168, 169]	[27]
Actuator and sensor fault	[30, 169]	[31, 170]

Table 4: MAS challenges.

Sr. number	Challenges	Research work on MAS challenges
1	Security	[155, 172]
2	Learning	[173, 174]
3	Fault detection	[21, 33, 34, 175]
4	Localization	[176, 177]
5	Task allocation	[178–180]
6	Organization	[176, 177, 181]
7	Formation	[138, 182]
8	Connectivity	[167, 175, 183, 184]
9	Consensus	[167, 175, 183, 184]
10	Control ability	[175, 185, 186]
11	Synchronization	[175, 186]

9. Key Challenges

Report [82] tells us clearly that there is no high-level security against upcoming attacks or threats. In addition, an open integrated ecosystem idea for cooperation of security issues was studied. Though, in security system, there should be collaboration of stalk holders, it will have advantage form face threat understanding.

Table 5: Summary of different strategies for MAS.

Application	Goal	Architecture	DRL algorithm	Q function estimator	Reference
Maximum power point tracking (MPPT) control	To solve MPPT problem of photovoltaic system in practical condition	Photovoltaic system microgrid base	Deep deterministic policy gradients algorithm	Deep neural network (DNN)	[153]
Secondary control/ frequency regulation	With enough load, restoring stability	Hybrid distributed power system as separated small grid	Actor-critic based algorithm	Neural network (NN)	[175]
Bus voltage stability	Designing DC-DC control converter	DC microgrid	Q network/deep Q network	NN	[166]

Table 6: Comparison of different methodologies of system security.

Benefits	Drawbacks	Methodology
Resiliency to GPS spoofing attack. Speedy and correct finding of anomaly in gained data.	Require a mathematical model of system because there may be complication without any mathematical model when applying to system	Luenberger observer and artificial neural network (ANN) [172]
Resiliency to GPS spoofing attack	Susceptible to unforeseen attack. Costly against abrupt attack has low accuracy	Machine learning-based algorithm [39]
Resiliency to GPS spoofing and expected attacks	Susceptible against suspicions and system disturbances, model accuracy dependent complicated to apply on nonlinear system	Model-based detection algorithm [148]
Low computation load. Resiliency to GPS spoof attack	Susceptible to GPS spoofing attack	Communication [62, 65]
Secure conventional disturbances in between communication connections		

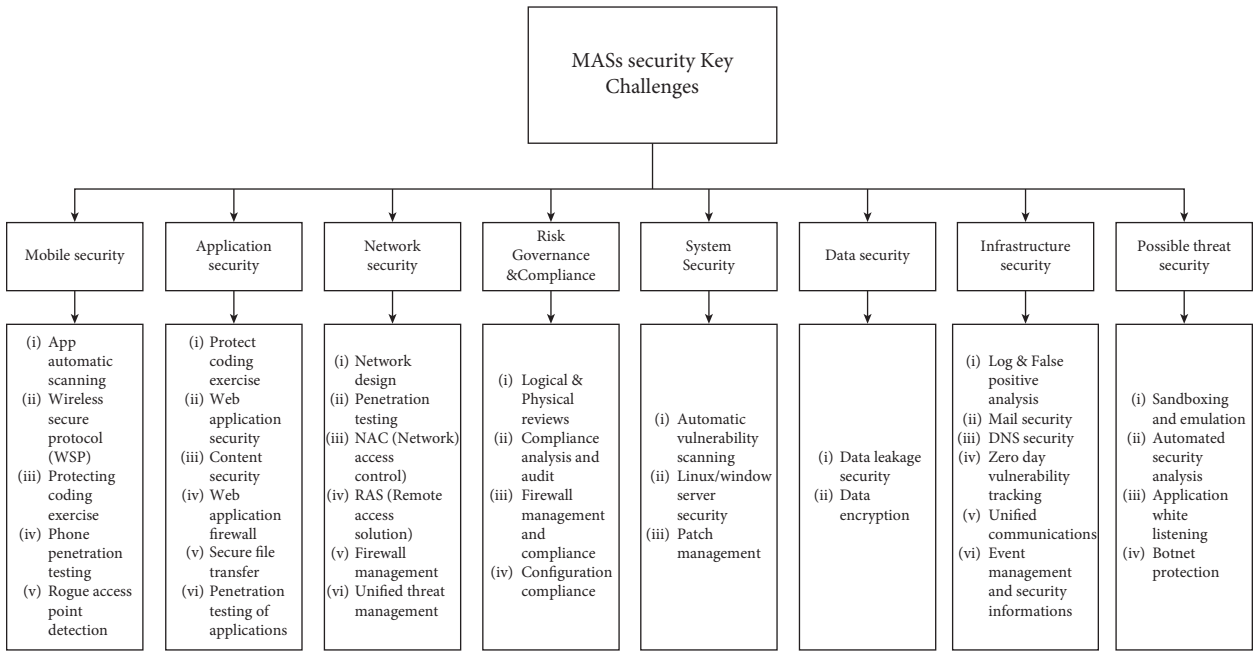

Figure 13: Overall MAS security challenges.

Key challenge for MASs is that there should be no system outside attack, but also from inside, e.g., a worker who is not interested to learn more about the board system. Designing of protective filter based on results of attack measurement for getting high security is one of the key challenges. To see present filtering technologies, those are not sufficient for security assurance, since it is complicated for defenders to get an idea about the time and trick of cyberattack. The Kalman filter method is not enough for MASs, and it is difficult to gain attacker in statically characterization of signal transmitted [107, 171]. In research studies, interest control problem and filtering in concern of security are getting more and attention, e.g., [79] in which there assurance of security against integrity attacks with the use of minimax optimization advancement [167].

With the deficiency of federal reliable power, agent identity verification and creating trust between agents are a big challenge. We can call it decentralization.

Basically, agents use knowledge or information which they get or need from decision-making process environment or another nearby agents. It makes an agent susceptible against malicious entries which may share false data to have effect on agent decision.

Highly important problem is needed to differentiate an accidental failure from an attack. The resulting sign from these accidental situations has chance of similarity, but reaction should not be the same. Fault is repairable. MASs should have capability to defend itself against attacks. Understanding of operations in MASs may be interrupted by malicious attack. A lot of attack stories have been presented in Table 1 of [78].

For MASs, integrity is an important requirement. There is need to pay attention toward sensor networks as well as to data integrity and superstructure. There is also not much more methodology in progressing of secure MAS, so there are several patented results, which may base on possibly exposed approaches.

For designing of applications, we need to see both quality of service and security assurance. For practical applications, considering of multiple attacks is an important point that we can face simultaneously. Present planning of security against several forms of attacks is insufficient for industrialization. In addition, security need and resource constraints as energy limitation and communication bandwidth in practically required to be supposed simultaneously.

Mobile devices are considered threats carrying because these are using several services and external networks. With the progressing of smart wearable mobile applications, loT of challenges presents in progressive of these applications' security measures, as there can be risk of human health and life.

For smart grids, basic challenges are communication protocol weakness, heterogeneity of protocols, and technology and limitation of physical systems. Table 4 represents research work on MAS challenges. Table 5 shows summary of different strategies for MAS while Table 6 represents comparison of different methodologies of system security. General security needs in MASs are integrity (which gives surety that since generation, there is no modification in message), authentication (that is sure that each agent is the one claim to be), confidentiality (which gives surety that only allowed agents are able to read specific data), availability, and authorization. Figure 13 represents overall security challenges in MASs.

10. Conclusion and Future Directions

MASs are virtually all around. They can be retrieved and switched remotely, such topographies make susceptible to cyberattacks. There is physical environment process on virtualization and cyber space as a key role for notion plays a central role in MAS. This article explained high-level inclusive discussion regarding various features of MASs that will aid new researchers to cover basic idea of MASs, key challenges in progressing MAS attack, e.g., system failure, virtualization and mobility, and MAS performance methods. First, we studied various attack types in MASs; second, we discussed threats with consistent subtypes and then their possible detection methodologies. After that we give detailed study of MAS attacks and their detection methodologies. Furthermore, an important work of this paper is subjected on several MAS aspects regarding security issues and key challenges. This article will play an important role for researchers to get maximum knowledge about MAS attacks and also to serve as an insightful and overall resources on MASs for researchers.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors hereby confirm that there are no conflicts of interest.

Acknowledgments

This work was supported by the National Key RD Program of China (the major project no. 2020YFB1807900) of China.

References

[1] X. Ge, Q.-L. Han, and Z. Wang, "A threshold-parameter-dependent approach to designing distributed event-triggered H_{∞} consensus filters over sensor networks," *IEEE Transactions on Cybernetics*, vol. 49, no. 4, pp. 1148–1159, 2019.

[2] B. Liu, H.-T. Zhang, H. Meng, D. Fu, and H. Su, "Scanning-chain formation control for multiple unmanned surface vessels to pass through water channels," *IEEE Transactions on Cybernetics*, vol. 52, no. 3, pp. 1850–1861, 2022.

[3] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, 2018.

[4] V. Belenko, V. Chernenko, V. Krundyshev, and M. Kalinin, "Data-driven failure analysis for the cyber physical infrastructures," in *Proceedings of the 2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*, pp. 1–5, IEEE, Taipei, Taiwan, May 2019.

[5] M. Wolf and D. Serpanos, "Safety and security in cyber-physical systems and internet-of-things systems," *Proceedings of the IEEE*, vol. 106, no. 1, pp. 9–20, 2018.

[6] D.-B. Pan, G. Zhang, S. Jiang, Y. Zhang, and B.-Y. Cui, "Delay-independent traffic flux control for a discrete-time lattice hydrodynamic model with time-delay," *Physica A: Statistical Mechanics and Its Applications*, vol. 563, p. 125440, Article ID 125440, 2021.

[7] B. Chen, L. Yu, D. W. C. Ho, and W.-A. Zhang, "Networked Fusion Estimation under Denial-of-Service Attacks," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 3835–3840, 2017.

[8] M. Nasir, M. Muzamil Aslam, and Z. Ahmed, "Stabilization of an Arbitrary Order Transfer Function with Time Delay H2 Controller," 2021, https://www.researchgate.net/publication/357620374_Stabilization_of_an_arbitrary_order_transfer_function_with_time_delay_H2_Controller.

[9] B. Mrugalska and M. K. Wyrwicka, "Towards lean production in industry 4.0," *Procedia Engineering*, vol. 182, pp. 466–473, 2017.

[10] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2016.

[11] M. Muzamil Aslam, J. Zhang, B. Qureshi, and Z. Ahmed, "Beyond6g-consensus traffic management in crn, applications, architecture and key challenges," in *Proceedings of the 2021 IEEE 11th International Conference on Electronics Information and Emergency Communication (ICEIEC)*, pp. 182–185, IEEE, Beijing, China, June 2021.

[12] Z. Ahmed, M. M. Khan, M. A. Saeed, and W. Zhang, "Consensus control of multi-agent systems with input and communication delay: a frequency domain perspective," *ISA Transactions*, vol. 101, pp. 69–77, 2020.

[13] C. H. Ho, S. C. Chan, Y. Hou, and Y. Hou, "A robust statistical approach to distributed power system state estimation with bad data," *IEEE Transactions on Smart Grid*, vol. 11, no. 1, pp. 517–527, 2020.

[14] M. M. Aslam, L. Du, Z. Ahmed, H. Azeem, and M. Ikram, "Consensus performance of traffic management system for cognitive radio network: an agent control approach," in *Communications in Computer and Information Science,* vol. 1138, pp. 138–145, Springer, 2019.

[15] B. Ning, Q.-L. Han, Z. Zuo, J. Jin, and J. Zheng, "Collective behaviors of mobile robots beyond the nearest neighbor rules with switching topology," *IEEE Transactions on Cybernetics*, vol. 48, no. 5, pp. 1577–1590, 2018.

[16] B. Ning, Q.-L. Han, and L. Ding, "Distributed finite-time secondary frequency and voltage control for islanded microgrids with communication delays and switching topologies," *IEEE Transactions on Cybernetics*, vol. 51, no. 8, pp. 3988–3999, 2021.

[17] A. Khan, F. Aftab, and Z. Zhang, "Self-organization based clustering scheme for fanets using glowworm swarm optimization," *Physical Communication*, vol. 36, p. 100769, Article ID 100769, 2019.

[18] A. Khan, F. Aftab, and Z. Zhang, "Bicsf: bio-inspired clustering scheme for fanets," *IEEE Access*, vol. 7, pp. 31446–31456, 2019.

[19] H. Yang, Q.-L. Han, X. Ge et al., "Fault-tolerant cooperative control of multiagent systems: a survey of trends and methodologies," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 4–17, 2020.

[20] B. Kailkhura, Y. S. Han, S. Brahma, and P. K. Varshney, "Distributed bayesian detection in the presence of byzantine data," *IEEE Transactions on Signal Processing*, vol. 63, no. 19, pp. 5250–5263, 2015.

[21] X.-Z. Jin, W.-W. Che, Z.-G. Wu, and Z. Zhao, "Adaptive consensus and circuital implementation of a class of faulty multiagent systems," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 1, pp. 226–237, 2022.

[22] S. Pal, B. Sikdar, and J. Chow, "Detecting data integrity attacks on scada systems using limited pmus," in *Proceedings of the 2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 545–550, IEEE, Sydney, NSW, Australia, November 2016.

[23] A. Stief, J. R. Ottewill, J. Baranowski, and M. Orkisz, "A pca and two-stage bayesian sensor fusion approach for diagnosing electrical and mechanical faults in induction motors," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 12, pp. 9510–9520, 2019.

[24] L. Zhao and G.-H. Yang, "Adaptive sliding mode fault tolerant control for nonlinearly chaotic systems against dos attack and network faults," *Journal of the Franklin Institute*, vol. 354, no. 15, pp. 6520–6535, 2017.

[25] A. A. Yaseen and M. Bayart, "Cyber-attack detection with fault accommodation based on intelligent generalized predictive control," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 2601–2608, 2017.

[26] Steve Starrett, *World Environmental and Water Resources congress 2009*, American Society of Civil Engineers, Kansas City, p. 6664, 2009.

[27] S. Hu, H. Xiao, and C. Yi, "A novel detrended fluctuation analysis method for gear fault diagnosis based on variational mode decomposition," *Shock and Vibration*, vol. 2018, pp. 1–11, 2018.

[28] C. Liu, B. Jiang, R. J. Patton, and K. Zhang, "Decentralized output sliding-mode fault-tolerant control for heterogeneous multiagent systems," *IEEE Transactions on Cybernetics*, vol. 50, no. 12, pp. 4934–4945, 2020.

[29] L. Zhao and G.-H. Yang, "Adaptive fault-tolerant control for nonlinear multi-agent systems with dos attacks," *Information Sciences*, vol. 526, pp. 39–53, 2020.

[30] H. Wang, Y. Kang, L. Yao, H. Wang, and Z. Gao, "Fault Diagnosis and Fault Tolerant Control for T-S Fuzzy Stochastic Distribution Systems Subject to Sensor and Actuator Faults," *IEEE Transactions on Fuzzy Systems*, vol. 29, no. 11, pp. 3561–3569, 2021.

[31] A. Atta Yaseen and M. Bayart, "Cyber-attack detection in the networked control system with faulty plant," in *Proceedings of the 2017 25th Mediterranean Conference on Control and Automation (MED)*, pp. 980–985, IEEE, Valletta, Malta, July 2017.

[32] K. Michail, K. M. Deliparaschos, S. G. Tzafestas, and A. C. Zolotas, "Ai-based actuator/sensor fault detection with low computational cost for industrial applications," *IEEE Transactions on Control Systems Technology*, vol. 24, no. 1, pp. 293–301, 2016.

[33] W. Zou, C. K. Ahn, and Z. Xiang, "Fuzzy-approximation-based distributed fault-tolerant consensus for heterogeneous switched nonlinear multiagent systems," *IEEE Transactions on Fuzzy Systems*, vol. 29, no. 10, pp. 2916–2925, 2020.

[34] C. Deng and C. Wen, "Distributed resilient observer-based fault-tolerant control for heterogeneous multiagent systems under actuator faults and dos attacks," *IEEE Transactions on Control of Network Systems*, vol. 7, no. 3, pp. 1308–1318, 2020.

[35] Y. Shoukry and P. Tabuada, "Event-triggered state observers for sparse sensor noise/attacks," *IEEE Transactions on Automatic Control*, vol. 61, no. 8, pp. 2079–2091, 2016.

[36] F.-F. Wang and Q. H. Liu, "A Bernoulli-Gaussian Binary Inversion Method for High-Frequency Electromagnetic Imaging of Metallic Reflectors," *IEEE Transactions on Antennas and Propagation*, vol. 68, no. 4, pp. 3184–3193, 2020.

[37] T. Sui, Y. Mo, D. Marelli, X. Sun, and M. Fu, "The vulnerability of cyber-physical system under stealthy attacks," *IEEE Transactions on Automatic Control*, vol. 66, no. 2, pp. 637–650, 2021.

[38] K. Granström, M. Fatemi, and L. Svensson, "Poisson multi-Bernoulli mixture conjugate prior for multiple extended target filtering," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 56, no. 1, pp. 208–225, 2020.

[39] B. Xu, J. Shi, M. Lu, J. Cong, L. Wang, and B. Nener, "An automated cell tracking approach with multi-Bernoulli filtering and ant colony labor division," *IEEE/ACM*

Transactions on Computational Biology and Bioinformatics, vol. 18, no. 5, pp. 1850–1863, 2021.

[40] S. Amin, G. A. Schwartz, and S. Shankar Sastry, "Security of interdependent and identical networked control systems," *Automatica*, vol. 49, no. 1, pp. 186–192, 2013.

[41] A. Mishra, R. Singh Chowhan, and A. Mathur, "Sniffer detection and load balancing using aglets in a cluster of heterogeneous distributed system environment," in *Proceedings of the 2016 IEEE 7th Power India International Conference (PIICON)*, pp. 1–6, IEEE, Bikaner, India, November 2016.

[42] G. K. Befekadu, V. Gupta, and P. J. Antsaklis, "Risk-sensitive control under Markov modulated denial-of-service (dos) attack strategies," *IEEE Transactions on Automatic Control*, vol. 60, no. 12, pp. 3299–3304, 2015.

[43] P. C. Evans and M. Annunziata, "Industrial Internet: Pushing the Boundaries," *General Electric Reports*, pp. 488–508, 2012.

[44] J. Yan, F. Guo, and C. Wen, "False data injection against state estimation in power systems with multiple cooperative attackers," *ISA Transactions*, vol. 101, pp. 225–233, 2020.

[45] M. Tian, Z. Dong, and X. Wang, "Analysis of false data injection attacks in power systems: a dynamic bayesian game-theoretic approach," *ISA Transactions*, vol. 115, pp. 108–123, 2021.

[46] S. Xiao, Q.-L. Han, X. Ge, and Y. Zhang, "Secure distributed finite-time filtering for positive systems over sensor networks under deception attacks," *IEEE Transactions on Cybernetics*, vol. 50, no. 3, pp. 1220–1229, 2020.

[47] T. Zou, A. S. Bretas, C. Ruben, S. C. Dhulipala, and N. Bretas, "Smart grids cyber-physical security: parameter correction model against unbalanced false data injection attacks," *Electric Power Systems Research*, vol. 187, p. 106490, Article ID 106490, 2020.

[48] J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, and Z. Fan, "Sparse malicious false data injection attacks and defense mechanisms in smart grids," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 5, pp. 1–12, 2015.

[49] C. De Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Transactions on Automatic Control*, vol. 60, no. 11, pp. 2930–2944, 2015.

[50] K.-L. Miao, J.-W. Zhu, and W.-A. Zhang, "Distributed guaranteed cost control of networked interconnected systems under denial-of-service attacks: a switched system approach," in *Proceedings of the 2018 33rd Youth Academic Annual Conference of Chinese Association of Automation (YAC)*, pp. 911–915, IEEE, Nanjing, China, May 2018.

[51] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (sdn) and distributed denial of service (ddos) attacks in cloud computing environments: a survey, some research issues, and challenges," *IEEE communications surveys & tutorials*, vol. 18, no. 1, pp. 602–622, 2016.

[52] O. A. Wahab, J. Bentahar, H. Otrok, and A. Mourad, "Optimal load distribution for the detection of vm-based ddos attacks in the cloud," *IEEE transactions on services computing*, vol. 13, no. 1, pp. 114–129, 2020.

[53] Y. Ali, Y. Xia, L. Ma, and A. Hammad, "Secure design for cloud control system against distributed denial of service attack," *Control Theory and Technology*, vol. 16, no. 1, pp. 14–24, 2018.

[54] J. H. Sarker and A. M. Nahhas, "Mobile rfid system in the presence of denial-of-service attacking signals," *IEEE Transactions on Automation Science and Engineering*, vol. 14, no. 2, pp. 955–967, 2017.

[55] D. Kshirsagar and S. Kumar, "An Efficient Feature Reduction Method for the Detection of Dos Attack," *ICT Express*, vol. 7, no. 3, pp. 371–375, 2021.

[56] M. Long, C.-H. Wu, and J. Y. Hung, "Denial of service attacks on network-based control systems: impact and mitigation," *IEEE Transactions on Industrial Informatics*, vol. 1, no. 2, pp. 85–96, 2005.

[57] S. Liu, P. X. Liu, and A. El Saddik, "A stochastic game approach to the security issue of networked control systems under jamming attacks," *Journal of the Franklin Institute*, vol. 351, no. 9, pp. 4570–4583, 2014.

[58] M. Zhang, J. Chen, S. He, L. Yang, X. Gong, and J. Zhang, "Privacy-preserving database assisted spectrum access for industrial internet of things: a distributed learning approach," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 8, pp. 7094–7103, 2020.

[59] L. Peng, L. Shi, X. Cao, and C. Sun, "Optimal attack energy allocation against remote state estimation," *IEEE Transactions on Automatic Control*, vol. 63, no. 7, pp. 2199–2205, 2018.

[60] R. Gan, Y. Xiao, J. Shao, and J. Qin, "An Analysis on Optimal Attack Schedule Based on Channel Hopping Scheme in Cyber-Physical Systems," *IEEE transactions on cybernetics*, vol. 51, no. 2, pp. 994–1003, 2021.

[61] J. Qin, M. Li, L. Shi, and X. Yu, "Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks," *IEEE Transactions on Automatic Control*, vol. 63, no. 6, pp. 1648–1663, 2018.

[62] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal dos attack scheduling in wireless networked control system," *IEEE Transactions on Control Systems Technology*, vol. 24, no. 3, pp. 843–852, 2016.

[63] A. Benslimane and H. Nguyen-Minh, "Jamming attack model and detection method for beacons under multi-channel operation in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 7, pp. 6475–6488, 2017.

[64] Y. Pan, Z. Zheng, and D. Fu, "Bayesian-based water leakage detection with a novel multisensor fusion method in a deep manned submersible," *Applied Ocean Research*, vol. 106, p. 102459, Article ID 102459, 2021.

[65] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.

[66] I. Paul, "Lenovo preinstalls man-in-the-middle adware that hijacks," *Superfish may make it trivial for attackers to spoof any HTTPS website*, 2015.

[67] Di Wu, D. I Arkhipov, E. Asmare, Z. Qin, and J. A. McCann, "Ubiflow: mobility management in urban-scale software defined iot," in *Proceedings of the 2015 IEEE Conference on Computer Communications (INFOCOM)*, pp. 208–216, IEEE, Hong Kong, China, April 2015.

[68] C. Li, Z. Qin, E. Novak, and Q. Li, "Securing SDN Infrastructure of IoT-Fog Networks From MitM Attacks," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1156–1164, 2017.

[69] G. Oliva, S. Cioaba, and C. N. Hadjicostis, "Distributed calculation of edge-disjoint spanning trees for robustifying distributed algorithms against man-in-the-middle attacks," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 4, pp. 1646–1656, 2018.

[70] J. Huang, D. W. C. Ho, F. Li, W. Yang, and Y. Tang, "Secure remote state estimation against linear man-in-the-middle attacks using watermarking," *Automatica*, vol. 121, p. 109182, Article ID 109182, 2020.

[71] Y. Mirsky, N. Kalbo, Y. Elovici, and A. Shabtai, "Vesper: using echo analysis to detect man-in-the-middle attacks in LANs," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1638–1653, 2019.

[72] A. Esfahani, G. Mantas, J. Ribeiro et al., "An efficient web authentication mechanism preventing man-in-the-middle attacks in industry 4.0 supply chain," *IEEE Access*, vol. 7, pp. 58981–58989, 2019.

[73] A. A. M Mazharul Amin and M S Mahamud, "An alternative approach of mitigating arp based man-in-the-middle attack using client site bash script," in *Proceedings of the 2019 6th International Conference on Electrical and Electronics Engineering (ICEEE)*, pp. 112–115, IEEE, Istanbul, Turkey, April 2019.

[74] M. Zhu and S. Martinez, "On the performance analysis of resilient networked control systems under replay attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 3, pp. 804–808, 2014.

[75] Y. Mo and B. Sinopoli, "Secure estimation in the presence of integrity attacks," *IEEE Transactions on Automatic Control*, vol. 60, no. 4, pp. 1145–1151, 2015.

[76] H. Tan, B. Shen, Y. Liu, A. Alsaedi, and B. Ahmad, "Event-triggered multi-rate fusion estimation for uncertain system with stochastic nonlinearities and colored measurement noises," *Information Fusion*, vol. 36, pp. 313–320, 2017.

[77] R. Merco, Z. Abdollahi Biron, and P. Pisu, "Replay attack detection in a platoon of connected vehicles with cooperative adaptive cruise control," in *Proceedings of the 2018 Annual American Control Conference (ACC)*, pp. 5582–5587, IEEE, Milwaukee, WI, USA, June 2018.

[78] S. Garg, K. Kaur, G. Kaddoum, K. K. R Choo, and R. C. Kwang, "Toward secure and provable authentication for internet of things: realizing industry 4.0," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4598–4606, 2020.

[79] M. A. Quddus, O. Shahvari, M. Marufuzzaman, J. M. Usher, and R. Jaradat, "A collaborative energy sharing optimization model among electric vehicle charging stations, commercial buildings, and power grid," *Applied Energy*, vol. 229, pp. 841–857, 2018.

[80] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys*, vol. 45, no. 3, pp. 1–39, 2013.

[81] Y. Mo and S. Bruno, "Secure control against replay attacks," in *Proceedings of the 2009 47th annual Allerton conference on communication, control, and computing (Allerton)*, pp. 911–918, IEEE, Monticello, IL, USA, October 2009.

[82] B. Tang, L. D. Alvergue, and G. Gu, "Secure networked control systems against replay attacks without injecting authentication noise," in *Proceedings of the 2015 American Control Conference (ACC)*, pp. 6028–6033, IEEE, Chicago, IL, USA, July 2015.

[83] B. J. Austin, V. Heine, and L. J. Sham, "General theory of pseudopotentials," *Physical Review*, vol. 127, no. 1, pp. 276–282, 1962.

[84] R. Kibble, "Speech acts, commitment and multi-agent communication," *Computational & Mathematical Organization Theory*, vol. 12, no. 2-3, pp. 127–145, 2006.

[85] M. Colombetti and M. Verdicchio, "An analysis of agent speech acts as institutional actions," in *Proceedings of the first international joint conference on Autonomous agents and multiagent systems: Part 3*, pp. 1157–1164, DBLP, Bologna, Italy, 2002.

[86] D. Ding, Z. Wang, G. Wei, and F. E. Alsaadi, "Event-based security control for discrete-time stochastic systems," *IET Control Theory & Applications*, vol. 10, no. 15, pp. 1808–1815, 2016.

[87] S. Amin, X. Litrico, S. Sastry, and A. M. Bayen, "Cyber Security of Water SCADA Systems-Part I: Analysis and Experimentation of Stealthy Deception Attacks," *IEEE Transactions on Control Systems Technology*, vol. 21, no. 5, pp. 1963–1970, 2013.

[88] G. Falco, C. Caldera, and H. Shrobe, "Iiot cybersecurity risk modeling for scada systems," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4486–4495, 2018.

[89] S. Adepu and A. Mathur, "Distributed attack detection in a water treatment plant: method and case study," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 1, pp. 86–99, 2021.

[90] G. Wen, X. Zhai, Z. Peng, and A. Rahmani, "Fault-tolerant secure consensus tracking of delayed nonlinear multi-agent systems with deception attacks and uncertain parameters via impulsive control," *Communications in Nonlinear Science and Numerical Simulation*, vol. 82, p. 105043, Article ID 105043, 2020.

[91] E. Drayer and T. Routtenberg, "Detection of false data injection attacks in smart grids based on graph signal processing," *IEEE Systems Journal*, vol. 14, no. 2, pp. 1886–1896, 2020.

[92] S. Li, K. Xue, D. S. L. Wei, H. Yue, N. Yu, and P. Hong, "Secgrid: a secure and efficient sgx-enabled smart grid system with rich functionalities," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1318–1330, 2020.

[93] M. Muzamil Aslam, M. Nauman Irshad, and A. Z. E. E. M. Hassan, "Cost effective & energy efficient intelligent smart home system based on iot," *Afyon Kocatepe Üniversitesi Uluslararası Mühendislik Teknolojileri ve Uygulamalı Bilimler Dergisi*, vol. 3, no. 1, pp. 10–20.

[94] M. A. Ferrag and L. Maglaras, "Deepcoin: a novel deep learning and blockchain-based energy exchange framework for smart grids," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1285–1297, 2020.

[95] Y. Dong, N. Gupta, and N. Chopra, "False data injection attacks in bilateral teleoperation systems," *IEEE Transactions on Control Systems Technology*, vol. 28, no. 3, pp. 1168–1176, 2020.

[96] D. Ye and T.-Y. Zhang, "Summation detector for false data-injection attack in cyber-physical systems," *IEEE Transactions on Cybernetics*, vol. 50, no. 6, pp. 2338–2345, 2020.

[97] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2218–2234, 2020.

[98] W. Meng, W. Li, C. Su, J. Zhou, and R. Lu, "Enhancing trust management for wireless intrusion detection via traffic sampling in the era of big data," *IEEE Access*, vol. 6, pp. 7234–7243, 2018.

[99] S. Aoufi, A. Derhab, and M. Guerroumi, "Survey of false data injection in smart power grid: attacks, countermeasures and challenges," *Journal of Information Security and Applications*, vol. 54, p. 102518, Article ID 102518, 2020.

[100] G. Yadav and K. Paul, "Assessment of scada system vulnerabilities," in *Proceedings of the 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, pp. 1737–1744, IEEE, Zaragoza, Spain, September 2019.

[101] Ş. Dalgaç, F. Karadağ, M. Bakır, O. Akgöl, E. Ünal, and M. Karaaslan, "Chiral metamaterial-based sensor applications to determine quality of car lubrication oil," *Transactions of the Institute of Measurement and Control*, vol. 43, no. 7, pp. 1640–1649, 2021.

[102] Y. Mo and B. Sinopoli, "On the performance degradation of cyber-physical systems under stealthy integrity attacks," *IEEE Transactions on Automatic Control*, vol. 61, no. 9, pp. 2618–2624, 2016.

[103] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Processing Letters*, vol. 22, no. 10, pp. 1652–1656, 2015.

[104] A. Karatepe, O. Akgöl Yadgar, and I. Abdulkarim, "A monopole microwave-assisted electrochemical sensor for the detection of liquid chemicals," *Digest Journal of Nanomaterials & Biostructures (DJNB)*, vol. 16, no. 3, 2021.

[105] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, "Optimal linear cyber-attack on remote state estimation," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 4–13, 2017.

[106] Z. Ahmed, M. A. Saeed, A. Jenabzadeh, and Z. Weidong, "Frequency domain analysis of resilient consensus in multi-agent systems subject to an integrity attack," *ISA Transactions*, vol. 111, pp. 156–170, 2021.

[107] M. M. Aslam, L. Du, X. Zhang, Y. Chen, Z. Ahmed, and B. Qureshi, "Sixth generation (6g) cognitive radio network (crn) application, requirements, security issues, and key challenges," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–18, 2021.

[108] S. Keele, "Guidelines for Performing Systematic Literature Reviews in Software Engineering," *EBSE*, vol. 259, 2007.

[109] M. M. Aslam, L. Du, Z. Ahmed, M. N. Irshad, and H. Azeem, "A deep learning-based power control and consensus performance of spectrum sharing in the cr network," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–16, 2021.

[110] L. Cheng, Ke Tian, D. Yao, L. Sha, and R. A. Beyah, "Checking Is Believing: Event-Aware Program Anomaly Detection in Cyber-Physical Systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 973pp. 353–1441, USA, 2019.

[111] Y. I. Abdulkarim, Ş. Dalgaç, F. O. Alkurt et al., "Utilization of a triple hexagonal split ring resonator (srr) based metamaterial sensor for the improved detection of fuel adulteration," *Journal of Materials Science: Materials in Electronics*, vol. 32, no. 19, pp. 24258–24272, 2021.

[112] S. Dalgac, V. Akdogan, S. Kiris et al., "Investigation of methanol contaminated local spirit using metamaterial based transmission line sensor," *Measurement*, vol. 178, p. 109360, Article ID 109360, 2021.

[113] M. Nasir, M. F. Hayat, A. Jamal, and Z. Ahmed, "Frequency domain consensus control analysis of the networked multi-agent system with controller area network bus-induced delay," *Journal of Vibration and Control*, p. 107754632110224, Article ID 107754632110224, 2021.

[114] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[115] J. Miloševič, T. Tanaka, H. Sandberg, and K. H. Johansson, "Analysis and mitigation of bias injection attacks against a kalman filter," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 8393–8398, 2017.

[116] W.-J. He, H.-T. Zhang, Z. Chen et al., "Temperature control for nano-scale films by spatially-separated atomic layer deposition based on generalized predictive control," *IEEE Transactions on Nanotechnology*, vol. 14, no. 6, pp. 1094–1103, 2015.

[117] X. Li and K. W. Hedman, "Enhancing power system cyber-security with systematic two-stage detection strategy," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 1549–1561, 2020.

[118] B. Li, Y. Chen, S. Huang, R. Yao, Y. Xia, and S. Mei, "Graphical evolutionary game model of virus-based intrusion to power system for long-term cyber-security risk evaluation," *IEEE Access*, vol. 7, pp. 178605–178617, 2019.

[119] F. Li, R. Xie, B. Yang et al., "Detection and identification of cyber and physical attacks on distribution power grids with pvs: an online high-dimensional data-driven approach," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 10, no. 1, pp. 1282–1291, 2022.

[120] Y. Zhang, V. V. G. Krishnan, J. Pi et al., "Cyber physical security analytics for transactive energy systems," *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 931–941, 2020.

[121] B. Kailkhura, Y. S. Han, S. Brahma, and P. K. Varshney, "Asymptotic analysis of distributed bayesian detection with byzantine data," *IEEE Signal Processing Letters*, vol. 22, no. 5, pp. 608–612, 2015.

[122] A. D'Addabbo, A. Refice, G. Pasquariello, F. P. Lovergine, D. Capolongo, and S. Manfreda, "A bayesian network for flood detection combining sar imagery and ancillary data," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 54, no. 6, pp. 3612–3625, 2016.

[123] H. Wang, J. Ruan, B. Zhou et al., "Dynamic data injection attack detection of cyber physical power systems with uncertainties," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 10, pp. 5505–5518, 2019.

[124] H. Zhang, Y. Qi, H. Zhou, J. Zhang, and J. Sun, "Testing and defending methods against dos attack in state estimation," *Asian Journal of Control*, vol. 19, no. 4, pp. 1295–1305, 2017.

[125] T. Hirakawa, K. Ogura, B. Bahadur Bista, and T. Takata, "A Defense Method against Distributed Slow http dos attack," in *Proceedings of the 2016 19th international conference on network-based information systems (NBiS)*, pp. 152–158, IEEE, Ostrava, Czech Republic, September 2016.

[126] B. Sinopoli, L. Schenato, M. Franceschetti, K. Poolla, M. I. Jordan, and S. S. Sastry, "Kalman filtering with intermittent observations," *IEEE Transactions on Automatic Control*, vol. 49, no. 9, pp. 1453–1464, 2004.

[127] J. Shi, G. Qi, Y. Li, and A. Sheng, "Stochastic convergence analysis of cubature kalman filter with intermittent observations," *Journal of Systems Engineering and Electronics*, vol. 29, no. 4, pp. 823–833, 2018.

[128] Y. Wu, Y. Li, and L. Shi, "A game-theoretic approach to remote state estimation in presence of a dos attacker," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 2595–2600, 2017.

[129] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, "A game-theoretic approach to fake-acknowledgment attack on cyber-physical systems," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 3, no. 1, pp. 1–11, 2017.

[130] B. Chen, D. W. C. Ho, W.-A. Zhang, and L. Yu, "Distributed dimensionality reduction fusion estimation for cyber-physical systems under dos attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 2, pp. 455–468, 2019.

[131] C. Yang, W. Yang, and H. Shi, "Dos attack in centralised sensor network against state estimation," *IET Control Theory & Applications*, vol. 12, no. 9, pp. 1244–1253, 2018.

[132] D. He, C. Chen, S. Chan, and J. Bu, "Dicode: dos-resistant and distributed code dissemination in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 5, pp. 1946–1956, 2012.

[133] Y. Xu, M. Fang, Z.-G. Wu, Y. J. Pan, Y.-J. Chadli, and T. Huang, "Input-based event-triggering consensus of multiagent systems under denial-of-service attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 4, pp. 1455–1464, 2020.

[134] V. S. Dolk, P. Tesi, C. De Persis, and W. P. M. H. Heemels, "Output-based event-triggered control systems under denial-of-service attacks," in *Proceedings of the 2015 54th IEEE Conference on Decision and Control (CDC)*, pp. 4824–4829, IEEE, Osaka, Japan, December 2015.

[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*, vol. 4, no. 1, pp. 93–105, 2017.

[136] S. Feng, P. Tesi, and C. De Persis, "Towards stabilization of distributed systems under denial-of-service," in *Proceedings of the 2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, pp. 5360–5365, IEEE, Melbourne, VIC, Australia, December 2017.

[137] H. Shisheh Foroush and S. Martinez, "On event-triggered control of linear systems under periodic denial-of-service jamming attacks," in *Proceedings of the 2012 IEEE 51st IEEE Conference on Decision and Control (CDC)*, pp. 2551–2556, IEEE, Maui, HI, USA, December 2012.

[138] S. Su, Z. Lin, and A. Garcia, "Distributed synchronization control of multiagent systems with unknown nonlinearities," *IEEE Transactions on Cybernetics*, vol. 46, no. 1, pp. 325–338, 2016.

[139] L. Ding, Q.-L. Han, B. Ning, and D. Yue, "Distributed resilient finite-time secondary control for heterogeneous battery energy storage systems under denial-of-service attacks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 7, pp. 4909–4919, 2020.

[140] E. Mousavinejad, X. Ge, Q.-L. Han, F. Yang, and L. Vlacic, "Resilient tracking control of networked control systems under cyber attacks," *IEEE Transactions on Cybernetics*, vol. 51, no. 4, pp. 2107–2119, 2021.

[141] D. Smirnov and A. Golkar, "Design optimization using game theory," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 2, pp. 1302–1312, 2021.

[142] Q. Zhu and Tamer Basar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 46–65, 2015.

[143] A. Riahi Sfar, Y. Challal, P. Moyal, and E. Natalizio, "A game theoretic approach for privacy preserving model in iot-based transportation," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 12, pp. 4405–4414, 2019.

[144] J. Zhang, Y. Zhu, and Z. Chen, "Evolutionary game dynamics of multiagent systems on multiple community networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 11, pp. 4513–4529, 2020.

[145] S. Guan, J. Wang, H. Yao, C. Jiang, Z. Han, and Y. Ren, "Colonel blotto games in network systems: models, strategies, and applications," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 637–649, 2020.

[146] N. Hou, Z. Wang, D. W. C. Ho, and H. Dong, "Robust partial-nodes-based state estimation for complex networks under deception attacks," *IEEE Transactions on Cybernetics*, vol. 50, no. 6, pp. 2793–2802, 2020.

[147] B. Rashidi, C. Fung, and E. Bertino, "A collaborative ddos defence framework using network function virtualization," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 10, pp. 2483–2497, 2017.

[148] K. Wang and M. Du, "Game-theory-based Active Defense for Intrusion Detection in Cyber-Physical Embedded Systems," *ACM Transactions on Embedded Computing Systems*, vol. 16, no. 1, pp. 1–21, 2016.

[149] Y. He, H. Li, X. Cheng, Y. Liu, C. Yang, and L. Sun, "A blockchain based truthful incentive mechanism for distributed p2p applications," *IEEE Access*, vol. 6, pp. 27324–27335, 2018.

[150] D. Ding, Z. Wang, Q.-L. Han, and G. Wei, "Security control for discrete-time stochastic nonlinear systems subject to deception attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 5, pp. 779–789, 2018.

[151] L. Ma, Z. Wang, Q.-L. Han, and H.-K. Lam, "Variance-constrained distributed filtering for time-varying systems with multiplicative noises and deception attacks over sensor networks," *IEEE Sensors Journal*, vol. 17, no. 7, pp. 2279–2288, 2017.

[152] E. Mousavinejad, F. Yang, Q.-L. Han, and L. Vlacic, "A novel cyber attack detection method in networked control systems," *IEEE Transactions on Cybernetics*, vol. 48, no. 11, pp. 3254–3264, 2018.

[153] X. You, S. Dian, R. Guo, and S. Li, "Exponential stability analysis for discrete-time quaternion-valued neural networks with leakage delay and discrete time-varying delays," *Neurocomputing*, vol. 430, pp. 71–81, 2021.

[154] H. Zhang, X. Zhou, Z. Wang, and H. Yan, "Maneuvering target tracking with event-based mixture kalman filter in mobile sensor networks," *IEEE Transactions on Cybernetics*, vol. 50, no. 10, pp. 4346–4357, 2020.

[155] X. Wang, M. Maghami, and G. Sukthankar, "Leveraging network properties for trust evaluation in multi-agent systems," in *Proceedings of the 2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology*, vol. 2, pp. 288–295, IEEE, Lyon, France, August 2011.

[156] T. Shinohara, T. Namerikawa, and Z. Qu, "Resilient reinforcement in secure state estimation against sensor attacks with a priori information," *IEEE Transactions on Automatic Control*, vol. 64, no. 12, pp. 5024–5038, 2019.

[157] Y. Yuan, H. Yuan, L. Guo, H. Yang, and S. Sun, "Resilient control of networked control system under dos attacks: a unified game approach," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 5, pp. 1786–1794, 2016.

[158] S. Mishra, Y. Shoukry, N. Karamchandani, S. N. Diggavi, and P. Tabuada, "Secure state estimation against sensor attacks in the presence of noise," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 49–59, 2016.

[159] V. A. Kumar, D. Das, and I. E. E. E. Senior Member, "Data Sequence Signal Manipulation in Multipath Tcp: The Vulnerability, Attack and its Detection," *Computers & Security*, vol. 103, Article ID 102180, 2021.

[160] S. Q. Ali Shah, F. Z. Khan, and M. Ahmad, "The Impact and Mitigation of Icmp Based Economic Denial of Sustainability Attack in Cloud Computing Environment Using Software Defined Network," *Computer Networks*, vol. 187, Article ID 107825, 2021.

[161] Z.-H. Pang and G.-P. Liu, "Design and implementation of secure networked predictive control systems under

deception attacks," *IEEE Transactions on Control Systems Technology*, vol. 20, no. 5, pp. 1334–1342, 2011.

[162] L. Ma, Z. Wang, and Y. Yuan, "Consensus control for nonlinear multi-agent systems subject to deception attacks," in *Proceedings of the 2016 22nd International Conference on Automation and Computing (ICAC)*, pp. 21–26, IEEE, Colchester, UK, September 2016.

[163] Y. Pang, H. Xia, and M. J. Grimble, "Resilient nonlinear control for attacked cyber-physical systems," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 6, pp. 2129–2138, 2020.

[164] T. Rhouma, K. Chabir, and M. N. Abdelkrim, "Resilient control for networked control systems subject to cyber/physical attacks," *International Journal of Automation and Computing*, vol. 15, no. 3, pp. 345–354, 2018.

[165] G. Franzè, F. Tedesco, and W. Lucia, "Resilient control for cyber-physical systems subject to replay attacks," *IEEE Control Systems Letters*, vol. 3, no. 4, pp. 984–989, 2019.

[166] A. Abbaspour, A. Sargolzaei, and K. Yen, "A neural network based resilient control design for distributed power systems under faults and attacks," in *Proceedings of the 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe)*, pp. 1–6, IEEE, Palermo, Italy, June 2018.

[167] Q.-K. Li, H. Lin, Xi Tan, and S. Du, "H consensus for multiagent-based supply chain systems under switching topology and uncertain demands," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 12, pp. 4905–4918, 2018.

[168] L. E. Venghi, F. Aguilera, P. Martin de la Barrera, C. Hernán, and C. H. De Angelo, "Detection and isolation of current-sensor and open-switch faults in electric traction drives," *IEEE Latin America Transactions*, vol. 19, no. 8, pp. 1335–1346, 2021.

[169] P. S. Kumar, L. Xie, M. S. M. Halick, and V. Vaiyapuri, "Stator end-winding thermal and magnetic sensor arrays for online stator inter-turn fault detection," *IEEE Sensors Journal*, vol. 21, no. 4, pp. 5312–5321, 2021.

[170] D. Zhang, G. Feng, Y. Shi, and D. Srinivasan, "Physical safety and cyber security analysis of multi-agent systems: a survey of recent advances," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 2, pp. 319–333, 2021.

[171] J. Jasper and S. R Isaac, "A Secure Routing Scheme to Mitigate Attack in Wireless Adhoc Sensor Network," *Computers & Security*, vol. 102, Article ID 102197, 2021.

[172] A. Abbaspour, A. Sargolzaei, P. Forouzannezhad, K. K. Yen, and A. I. Sarwat, "Resilient control design for load frequency control system under false data injection attacks," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 9, pp. 7951–7962, 2020.

[173] T. Liang, Y. Lin, L. Shi, J. Li, Y. Zhang, and Y. Qian, "Distributed vehicle tracking in wireless sensor network: a fully decentralized multiagent reinforcement learning approach," *IEEE Sensors Letters*, vol. 5, pp. 1–4, 2020.

[174] Y. Hou, Y.-S. Ong, J. Tang, and Y. Zeng, "Evolutionary multiagent transfer learning with model-based opponent behavior prediction," *IEEE transactions on systems, man, and cybernetics: Systems*, vol. 51, no. 10, pp. 5962–5976, 2021.

[175] W. Meng, P. X. Liu, Q. Yang, and Y. Sun, "Distributed synchronization control of nonaffine multiagent systems with guaranteed performance," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 31, no. 5, pp. 1571–1580, 2020.

[176] B. Horling and V. Lesser, "A survey of multi-agent organizational paradigms," *The Knowledge Engineering Review*, vol. 19, no. 4, pp. 281–316, 2004.

[177] T. T. Nguyen, S. Nahavandi, and S. Nahavandi, "Deep reinforcement learning for multiagent systems: a review of challenges, solutions, and applications," *IEEE Transactions on Cybernetics*, vol. 50, no. 9, pp. 3826–3839, 2020.

[178] C. Yu, M. Zhang, F. Ren, and G. Tan, "Multiagent learning of coordination in loosely coupled multiagent systems," *IEEE Transactions on Cybernetics*, vol. 45, no. 12, pp. 2853–2867, 2015.

[179] L. Busoniu, R. Babuska, and B. De Schutter, "A comprehensive survey of multiagent reinforcement learning," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 38, no. 2, pp. 156–172, 2008.

[180] X.-F. Xie and J. Liu, "Multiagent optimization system for solving the traveling salesman problem (tsp)," *IEEE Transactions on Systems, Man, and Cybernetics - Part B: Cybernetics: A Publication of the IEEE Systems, Man, and Cybernetics Society*, vol. 39, no. 2, pp. 489–502, 2009.

[181] J. Shi, J. Wan, H. Yan, and H. Suo, "A survey of cyber-physical systems," in *Proceedings of the 2011 international conference on wireless communications and signal processing (WCSP)*, pp. 1–6, IEEE, Nanjing, China, November 2011.

[182] H. Zhang, J. H. Park, D. Yue, and X. Xie, "Finite-horizon optimal consensus control for unknown multiagent state-delay systems," *IEEE Transactions on Cybernetics*, vol. 50, no. 2, pp. 402–413, 2018.

[183] L. Hao, X. Zhan, J. Wu, T. Han, and H. Yan, "Bipartite finite time and fixed time output consensus of heterogeneous multiagent systems under state feedback control," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 6, pp. 2067–2071, 2020.

[184] S. Xu, J. Cao, Q. Liu, and L. Rutkowski, "Optimal control on finite-time consensus of the leader-following stochastic multiagent system with heuristic method," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 6, pp. 3617–3628, 2021.

[185] D. Li, S. S. Ge, and T. H. Lee, "Fixed-time-synchronized consensus control of multiagent systems," *IEEE Transactions on Control of Network Systems*, vol. 8, no. 1, pp. 89–98, 2021.

[186] M. S. Mahmoud and B. J. Karaki, "Output-synchronization of discrete-time multiagent systems: a cooperative event-triggered dissipative approach," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 1, pp. 114–125, 2020.