sensors

MDPI

Review

Resilient Consensus Control for Multi-Agent Systems: A Comparative Survey

Jingyao Wang [1,2,†], Xingming Deng [2,†], Jinghua Guo [2,*,†] and Zeqin Zeng [2]

[1] State Key Laboratory of Automotive Simulation and Control, Changchun 130025, China
[2] School of Aerospace Engineering, Xiamen University, Xiamen 361000, China
[*] Correspondence: guojing_0701@live.cn
[†] These authors contributed equally to this work.

Abstract: Due to the openness of communication network and the complexity of system structures, multi-agent systems are vulnerable to malicious network attacks, which can cause intense instability to these systems. This article provides a survey of state-of-the-art results of network attacks on multi-agent systems. Recent advances on three types of attacks, i.e., those on DoS attacks, spoofing attacks and Byzantine attacks, the three main network attacks, are reviewed. Their attack mechanisms are introduced, and the attack model and the resilient consensus control structure are discussed, respectively, in detail, in terms of the theoretical innovation, the critical limitations and the change of the application. Moreover, some of the existing results along this line are given in a tutorial-like fashion. In the end, some challenges and open issues are indicated to guide future development directions of the resilient consensus of multi-agent system under network attacks.

Keywords: multi-agent systems; resilient consensus; secure coordination; DoS attack; spoofing attack; Byzantine attack

check for updates

Citation: Wang, J.; Deng, X.; Guo, J.; Zeng, Z. Resilient Consensus Control for Multi-Agent Systems: A Comparative Survey. *Sensors* **2023**, *23*, 2904. https://doi.org/10.3390/s23062904

Academic Editors: Claudio Savaglio and Dawid Połap

Received: 23 November 2022
Revised: 1 March 2023
Accepted: 5 March 2023
Published: 7 March 2023

1. Introduction

An agent is an independent individual who can achieve control goals autonomously through environmental perception according to preset knowledge. Usually, an agent only has simple intelligence and basic structure. A multi-agent system (MAS) refers to a networking system composed of a number of intelligent agents who can coordinate and manage through information interaction, so as to achieve complex control objectives that cannot be reached by an agent itself [1]. The distributed consensus control of a MAS is generally to achieve synchronous behavior by constructing a fully distributed controller for each agent. Due to its potential application in broad areas, the consensus control problem has been extensively studied and a lot of significant results have been established in the literature.

In recent years, the coordination control of a MAS has become a hot research topic and has been widely applied in areas such as unmanned aerial vehicle systems, industrial internet of things and wireless sensor networks [2–7]. Its research directions mainly include consensus control, formation control and flocking/swarming behavior. As the most fundamental and important topic, consensus has been widely debated and discussed. Consensus requires that a partial state quantity or a full state quantity of agents in a MAS reach an agreement [8,9]. In the ideal case of no interference and attack, there are tremendous amounts of control strategies to enable a MAS to realize the consensus requirements and even to improve the consensus performance [10].

However, due to the openness of the communication environment and the complexity of the system structure, a MAS is very vulnerable to network attacks, which brings the risk of system instability. Fundamentally, a MAS benefits from the high efficiency of the system, but it is bound to lack a central integrated device to monitor and manage the activities of all nodes in the network. While high-intensity information exchange is required, it cannot verify the information flow in the system, making the system at risk of security problems. Therefore, it is necessary to study the resilient control structure of a MAS under fault and attack.

As for MASs, the cyber attacks that scholars have studied at present mainly include: denial of service (DoS) attacks [11], spoofing attacks [12], Byzantine attacks [13], replay attacks [14], covert attacks [15], actuator attacks [16], communication attacks [16], intelligent attacks [17], policy attacks [13] and so on. Among them, DoS and spoofing attacks are the two most typical and common network attacks in the field of MASs at present. In addition, the Byzantine attack has become an emerging and significant research topic in recent years. Thus, there are tremendous results concentrating on DoS attacks, spoofing attacks and Byzantine attacks. For this reason, this survey focuses on these three kinds of cyber attacks to illustrate the recent advances in these fields.

The motivations for the survey are twofold. Firstly, diverse control methods have been developed in the published literature throughout the last decade to explore the defense mechanisms for MASs under network attacks, which are not covered in the existing surveys [18–22]. Secondly, the related fields are mature enough to deserve a survey classifying the existing analytical approaches, the models used and the results achieved for the MASs under attacks from both systems and control perspectives. The contributions of this survey can be summarized as follows:

- It develops a comprehensive classification of resilient consensus strategies. The attack types discussed are more basic and comprehensive and can cover many special attacks developed from these three main attacks.
- It reviews an extensive set of more than 100 consensus algorithms and discerns the classes they are associated with. The attack mechanism and the corresponding security control protocol are described in terms of the formula definition and algorithm construct. The shortcomings of the control protocols are explained according to the specific parameters, so as to clearly analyze the corresponding security control framework.
- The algorithms in the same class are compared regarding their attack types, centralization, scalability and so on. This survey summarizes the main elastic control schemes corresponding to each attack as much as possible, which can be applied to a variety of actual scenarios and attack situations and provide solutions to security control problems.

The remainder of this paper is as follows. Section 2 presents the preliminary on graph theory and the consensus problem of MASs. Section 3 is dedicated to reviewing the work on DoS attacks, spoofing attacks and Byzantine attacks. Some challenging issues are raised in Section 4 to guide the future research.

2. Preliminaries and Consensus Problem for MASs

This section recalls some preliminaries about graph theory and some fundamentals on the consensus problem of MASs.

2.1. Preliminaries about Graph Theory

The information connection among agents can be modeled by a graph $\mathcal{G}(\mathcal{V},\ \mathcal{E})$, where $\mathcal{V}$ denotes the set of vertices $\{v_1,\ v_2,\ \ldots,\ v_N\}$ which represents the set of agents in the system, and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ gives the set of links which mimics the connection among agents. Given nodes i and $j \in \mathcal{V}$, i can send information to j if there exists a directed edge from i to j, which is in the form of $(j \leftarrow i)$. The adjacency matrix associated with graph $\mathcal{G}$ is denoted by $\mathcal{A} = [a_{ij}]$, where $a_{ij} = 1$ if $(j,i) \in \mathcal{E}$; 0, otherwise. $\mathcal{G}(\mathcal{V},\ \mathcal{E})$ is called an undirected graph if $\mathcal{A}$ is symmetric. The Laplacian matrix of $\mathcal{G}$ is defined by $\mathcal{L} = [l_{ij}]$, where $l_{ij} = -a_{ij}$ if $j \neq i$; $l_{ii} = \sum_{j=1}^{N} a_{ij}$ otherwise.

At time t, denote by $\mathcal{G}(t)$ the pair $(\mathcal{V},\ \mathcal{E}(t))$, where the edge set $\mathcal{E}(t)$ varies with time. If there is a random process governing the change of $\mathcal{G}(t)$, one calls the communication graphs to be randomly switching.

2.2. Consensus Problem for MASs

The consensus control problem of MASs has attracted tremendous attention from researchers in the past decades. In general, suppose that the MAS consists of N agents with first-order integrator continuous-time dynamics described by

$$\dot{x}_i(t) = u_i(t),\ i = 1,\ldots,\ N, \tag{1}$$

of which $x_i(t) \in \mathbf{R}^n$ and $u_i(t) \in \mathbf{R}^n$ denote, respectively, the state and control input of agent i at time t.

The consensus problem for agents described by (1) can be divided into the leaderless consensus problem and the leader-following consensus problem, according to the theoretical frameworks.

Definition 1. *The leaderless consensus problem is to construct a controller for a MAS given by (1) such that*

$$\lim_{t\to\infty} \|z_i(t) - z_j(t)\| = 0,\ j \in \mathcal{N}_i,\ i =\ 1,\ldots,\ N, \tag{2}$$

where $z_i(t) \in \mathbf{R}^m$ and $z_j(t) \in \mathbf{R}^m$ denote the state or output of agent i and j, respectively; $\mathcal{N}_i$ represents the neighbor set of the i-th agent.

Definition 2. *The leader-following consensus problem is to construct a controller for a MAS given by (1) such that*

$$\lim_{t\to\infty} \|z_i(t) - z_0(t)\| = 0,\ i =\ 1,\ldots,\ N, \tag{3}$$

where $z_i(t) \in \mathbf{R}^m$ and $z_0(t) \in \mathbf{R}^m$ denote the state or output of agent i and the leader, respectively.

Moreover, the first-order discrete-time MAS is composed of N agents with dynamics given by

$$\dot{x}_i(k+1) = u_i(k),\ i = 1,\ldots,\ N, \tag{4}$$

of which $x_i(k) \in \mathbf{R}^n$ and $u_i(k) \in \mathbf{R}^n$ denote, respectively, the state and control input of agent i at time point $k \in \mathbf{N}$. The above definitions can be correspondingly extended to the MAS given by (4).

Recently, the consensus problem for MAS with linearized or nonlinear dynamics have been studied in [23–25].

3. Resilient Control for MASs

This section reviews the results reported for the resilient consensus of MASs based on the limitations of the information interaction level and the constraints of the system level, respectively. Table 1 summarizes the classification of common cyber attacks of MASs. The information security problem of MASs is mainly carried out in three directions: information availability [26,27], confidentiality [28] and integrity [29]. It was gradually evolved into three specific research topics: attack detection, state observation and security control. Common network attacks mainly include denial of service attack that hinders information transmission [26,27,30,31], replay attack that repeatedly sends harmful information [32], deception attack (spoofing attack) that tampers with communication data [33], etc. From the limitations of information interaction, we focus on reviewing the following important and popular topics: the DoS attack, the spoofing attack and the Byzantine attack.

Table 1. Classification of common cyber attacks of MASs.

Limitations of information interaction level	DoS attack, Byzantine attack, spoofing attack, repay attack, police attack, communication attack
Limitations of system level	Actuator attack

3.1. DoS Attack

Network attacks can be divided into point attacks (agent dynamic behavior) and edge attacks (topology communication behavior) according to the attacked object. The former can be seen as the attacked agent being "moved out" of the topology [34], while the DoS attack belongs to the latter. That is, the control/measurement transmission channel is truncated by the attack, so that the target agent cannot obtain the signal, thereby damaging the availability of information, as shown in Figure 1. The DoS attack can be implemented by the attackers in several ways: filling buffers in a user or the kernal domain, blocking or jamming the communication among key components, and altering a routing protocol. Refs. [26,27,30,35], respectively, analyze the DoS attack in the form of centralized control and distributed control. Due to the excellent robustness of the latter, it has a broader theoretical exploration prospect than the former, but there is less relevant research at present. Researchers usually simulate the impact of the attack on the system through packet loss, serious delay or communication interruption. With the gradual progress of research, the hypothetical limitation of DoS attack model has been issued from the period known in advance [36] and gradually relaxed to the random occurrence mechanism of [30,31]. Generally speaking, the attack energy is always limited; that is, there is a period of energy accumulation time between adjacent attacks, which is called sleep time. During this period, communication can be carried out normally. If the sleep time is too short, the system will not be able to complete the transmission of control signals and the update of state values in time when the input information is lost for a long time, which may cause the irreparable loss of consensus.

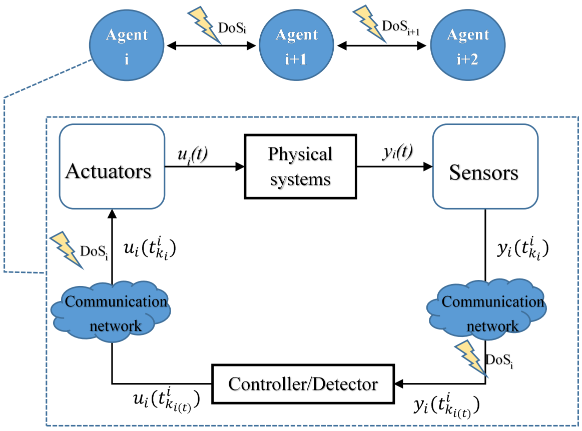

Figure 1. Multi-agent systems under DoS attack. DoS attacks may occur on the sensor–controller channel or the controller–actuator channel, affecting the transmission of system output signals and control signals, respectively. Hacker can also launch DoS attacks that can be independent of each other on different agents.

In existing studies, in order to avoid the above extreme attacks, the attack frequency F_a and attack duration T_a of DoS attacks are generally limited according to the designed control structure parameters [30–33,37,38]. Their definitions in the time period $[T_1, T_2)$ are as follows:

$$F_a(T_1,\ T_2) = \frac{N_a(T_1,\ T_2)}{T_2 - T_1}, \tag{5}$$

$$T_a(T_1,\ T_2) \leq T_0 + \frac{T_2 - T_1}{\tau_0}, \tag{6}$$

where N_a denotes the attack number in the time period $[T_1, T_2)$, $T_2 \geq T_1 \geq t_0$; $T_0 > 0$ and $\tau_0 > 1$ are scalars.

DoS attacks can paralyze the communication between agents, making the target agent unable to obtain the state information of the neighbor agents, thus, increasing the state error of the system. The trigger function of the event-triggered control mechanism is generally related to the state error, which can effectively judge the divergence of the system state error under the DoS attack, and can timely suppress the error divergence behavior. Therefore, the security control under DoS attack is mostly associated with the event-triggered mechanism [39]. While realizing flexible control, compared with periodic sampling control, it is more conducive to saving communication resources and avoiding network congestion. The event-triggered mechanism was proposed in [40,41] and then widely used in [31,42–44]. Event-triggered mechanism means that when the state deviates from the balance and exceeds the set threshold, the system stops feedback and triggers events to perform preset tasks, such as transferring information between neighbors or updating the controller. Compared with continuous-time control, an event-triggered mechanism requires additional consideration of the avoidance of Zeno behavior: that is, the situation of infinite triggering in an instant. This can be done by agreeing on the lower bound of the interval between two adjacent triggered instants [30,31] or introducing a bounded attenuation function into the event-triggered condition [44]. It can also be proved from the stability analysis that Zeno behavior does not exist [45].

According to the control structure, there are several schemes to achieve security consensus.

The simplest attack model is given in [31]; that is, the attack cycle and maximum duration are known in advance and constant, and a control scheme based on event-triggered mechanism under the leader-following topology is designed. It only allows events to be triggered during the communicable time period of the system. Under the condition that the attack parameters meet some system structural constraints, when the most serious imbalance occurs—that is, the time when the longest continuous attack ends—through the intervention of the control signal, the state quantity that deviates from the equilibrium can still be corrected, proving the feasibility of the elastic structure.

In the attack environment of random mechanism, an open-loop observer is designed in [30], as shown in Figure 2. $t^i_{k_i}$ denotes the time series updated for the controller. x_l and $\hat{x}_i$ represent the state quantity of the leader and the observed state quantity of followers, respectively. When the communication of the system is interrupted due to the attack, the observer is used to estimate the control signal and transmit it to the controller. The observer is as follows:

$$\dot{\hat{x}}_j(t) = A\hat{x}_j(t),\ t^j_{k_j} \leq t^j_{k_{j+1}}, \tag{7}$$

$$\hat{x}_j(t^j_{k_j}) = x_j(t^j_{k_j}),\ j \in \mathcal{N}_i,\ k_j \in \mathbf{N}, \tag{8}$$

where the matrix A denotes the system matrix; $\mathbf{N}$ defines the set of integers. The control protocol for the multi-agent system is given by:

$$u_i(t) = K\hat{\xi}_i(t),\ i = 1, \ldots, N, \tag{9}$$

where K is the control gain matrix, and

$$\hat{\xi}_i(t) = \sum_{j \in \mathcal{N}_i(\mathcal{G})} a_{ij}(\hat{x}_j(t) - \hat{x}_i(t)),\ i = 1, \ldots, N. \tag{10}$$

It follows from (10), that $\hat{\xi}_i(t)$ depends solely on the observed state, instead of the true state. The event-triggered condition is:

$$\|e_i(t)\| \leq \beta_i \|\hat{x}_i(t)\|,\ 0 < \beta_i < 1,\ i = 1, \ldots, N, \tag{11}$$

where $e_i(t) = \hat{x}_i(t) - x_i(t)$ denotes the observed error. When MASs suffer from DoS attacks, the control protocol proposed by [46,47] may collapse because the control signal cannot be updated as expected (e.g., set to zero). Then, the system cannot reset the e_i and gradually loses consensus. The above event-trigger strategy (11) and observer structure (7) and (8) can achieve resilient consensus under DoS attack. Setting the threshold depends on the state difference of the agent, which is the simplest form of the state-dependent triggered mechanism. The parameter β_i needs to be selected from the compromise between the performance measurement of system convergence speed and communication frequency.

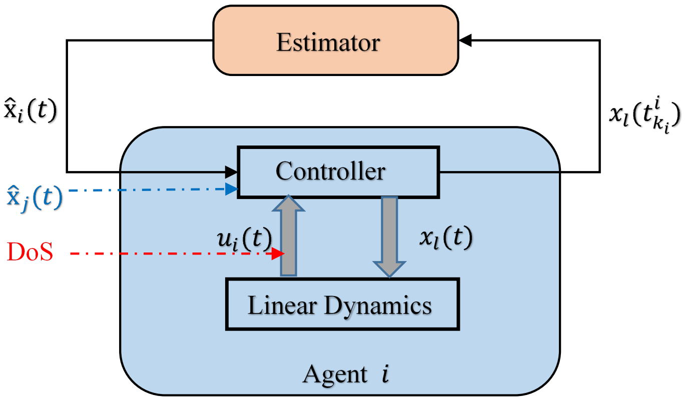

Figure 2. The event-triggered controller with an estimator under DoS attacks. $\hat{x}_j(t)$ and $\hat{x}_i(t)$ represent the estimates of agent *j* and agent *i* calculated by (7) and (8), respectively. $x_j(t^j_{k_j})$ is the state value at the triggering time $t^i_{k_i}$, where $t^i_{k_i}$ is determined by the trigger function (11). Under the influence of DoS attack, (11) can be triggered by the system, so as to update the state estimated value according to (8) and adjust the control signal on the basis of (9).

Since this estimate is designed based on the model, it means that the system can be unstable. The update process of the system can be summarized as follows: the observer calculates and estimates the state value of the neighbor according to the dynamic equation until the next triggered time $t^j_{k_j}$ comes. $\hat{x}_j(t)$ is updated to the state value passed by the neighbor at this time, and its own state value $x_i(t)$ is read and updated at the same time. The significance of signal separation is that if continuous communication cannot be achieved, it will not affect the triggering of events. When the system is attacked by DoS, the control signal will not be set to zero for a long time due to the failure to reset $e_i(t)$, thereby losing consensus [40,47].

The scheme in [40,47] can achieve exponential consensus in the two cases of leaderless and leader-following under DoS attacks, but the corresponding topology requirements are different: the former requires that the topology graph should be connected, while the latter requires that a directed spanning tree should be included. At the same time, both schemes can only be achieved when the attack frequency and duration have upper bounds. Additionally, both control schemes are not completely distributed. They use global information, namely the eigenvalues of the Laplace matrix, to design the matrix parameters of the controller, which is not conducive to the application of large-scale agent systems. The core of this scheme is to solve the problem of control interruption caused by failure to communicate by observing the state of neighbors. In addition, additional error variables $e_i^{\text{dos}} = x_i(t) - x_i(t_m)$ can be introduced into the triggering function, where t_m is the starting time of the attack, which can effectively reduce the number of unnecessary triggers of events [44].

Different from [30] and using the state measurement error $e_i(t)$ as the triggered condition, ref. [38] designs a control scheme based on the topology input triggered mechanism and gives the corresponding state observer: Given $i,\ j = i = 1, \ldots, N$, and $i \neq j$, define the state corresponding to edge (i, j) as

$$\omega_{ij}(t) \triangleq x_i(t) - x_j(t), \tag{12}$$

which satisfies

$$\dot{\omega}_{ij}(t) = A\omega_{ij}(t) + B(u_i(t) - u_j(t)), \tag{13}$$

where B is the input matrix.

After the control is triggered, the variables ω_{ij} cannot be measured until the next triggered time comes. Considering this fact, use an observer for estimation:

$$\dot{\hat{\omega}}_{ij}(t) = A\hat{\omega}_{ij}(t). \tag{14}$$

When the triggered time of the sleep time comes, assign the value directly as follows:

$$\hat{\omega}_{ij}(t^i_{ijk_i}) = \omega_{ij}(t^i_{ijk_i}). \tag{15}$$

Define topology state prediction error as:

$$\tilde{\omega}_{ij}(t) = \hat{\omega}_{ij}(t) - \omega_{ij}(t),\ t \in [t^i_{ijk_i}, t^{i+1}_{ijk_i}). \tag{16}$$

When the triggered time $t^i_{ijk_i}$ comes, the real value ω_{ij} is assigned to the estimated value $\hat{\omega}_{ij}$. Before the time $t^i_{ijk_{i+1}}$ comes, the estimated value is provided as an input to the controller for adjustment:

$$u_i(t) = -\alpha K \sum_{j \in \mathcal{N}_i} \hat{\omega}_{ij}(t), \tag{17}$$

where the scalar α denotes the coupling gain. The triggered instant and the triggering function corresponding to edge $(i,\ j)$ is

$$t^i_{ijk_{i+1}} = \inf\{t | t > t^i_{ijk_i}, f_{ij}(x_i(t), u_i(t), t) > 0 \mathrm{or} f_{ji}(x_i(t), u_i(t), t) > 0\}, \tag{18}$$

where

$$f_{ij}(x_i(t), u_i(t), t) = \| \int_{t^i_{ijk_i}}^{t} e^{A(t-s)} B u_i(s) ds \|^2 - \beta_{ij} \|B^T Q x_i(t)\|^2 \|B^T Q\|^{-2} > 0, \tag{19}$$

$$\begin{aligned} f_{ji}(x_j(t), u_j(t), t) &= \| \int_{t^j_{ijk_j}}^{t} e^{A(t-s)} B u_j(s) ds \|^2 - \beta_{ji} \|B^T Q x_j(t)\|^2 \|B^T Q\|^{-2} > 0, \\ & t \in [t^i_{ijk_i}, t^{i+1}_{ijk_i}), \end{aligned} \tag{20}$$

in which $Q \in \mathbf{R}^{n \times n}$ is a positive definite matrix.

When the topological edge is attacked by DoS, $\|\tilde{\omega}_{ij}(t)\|$ will break through the normal upper bound and the above triggered conditions will be met. β_{ij} is the parameter of triggering function corresponding to the edge $(i,\ j)$. Thus, the triggering threshold and the lower bound of adjacent triggered time can be flexibly set according to different edges, which reflects the distributed characteristics of event-triggered control. f_{ij} just depends on u_i and x_i, which are the state values of an agent itself. Unlike [30], which uses the neighbor's state difference as the triggered condition, ref. [38] does not require each agent to continuously broadcast its own control input and state quantity, which well maintains their own information privacy. In addition, the communication and the update of the state value can only be carried out when the state of the topological edge meets the triggering function, compared with the continuous information transmission and reception required in [30] to calculate the state observation value of the neighbor and its own real state value.

Thus, the former obviously reduces the communication cost and calculation complexity, but the corresponding parameter design is much more difficult. Moreover, compared to the general state consensus realized in [30], ref. [38] can achieve more accurate consensus results as exponential consensus.

Based on the information of the Laplace matrix eigenvalues of the communication topology, the control scheme designs the trigger parameter β_{ij} in the normal communication scenario, and then, achieves the state consensus of the system. In the case that the communication situation is under DoS attack, it can be shown that when the DoS attack frequency and the attack duration satisfy the inequality condition (related to the sleep time of DoS attack), the controller (17) can mitigate the communication anomaly caused by the DoS attack and achieve the security consensus of the system. Meanwhile, the design of parameters in both the controller (17) and the trigger function (18) relies on global information such as the non-zero minimum eigenvalue of the Laplace matrix. Thus, it is not a fully distributed control structure.

Considering the periodic DoS attack, ref. [48] models the error dynamics of the MASs as a switched time-varying delay system and proposes an event-triggered mechanism control protocol using the input time delay method, finally achieving the exponential consensus of the system. Its highlight is that, based on the existing theoretical research of time delay MASs, it converts the sampled-data term into a time delay term in the system. In addition, according to the sleep time of different DoS attacks, ref. [48] also puts forward an optimization algorithm to select the control parameters of the distributed event-triggered protocol. However, the attack is required to occur periodically. Meanwhile, the exact value of attack cycles and sleep time need to be known in advance, which makes [48] less applicable.

To sum up, for the resilient consensus problem under DoS attack, the current control scheme with high feasibility is to use the observer to simulate the evolution of normal state values during the communication paralysis period and combine the asynchronous triggered scheme to achieve consensus under the premise of limiting the attack frequency and duration. According to the accuracy and complexity of the observer and the sensitivity of the triggered mechanism, the conservatism and practicality of the corresponding consensus conclusions are different. To improve the practicability of the conclusion, the key lies in whether the attack model can fully ensure the accuracy of the prediction of the attacked object and the reduction of the actual damage.

In order to give a clear survey, we summarize the relevant work in Table 2 according to DoS type, centralized, scalability, results and references.

Table 2. Rencent Work on DoS Attacks.

Control Protocols	DoS Type	Centralized	Scalability	Results	References
Recursive Kalman fusion estimator	Stochastic	Fully	Low	Bounded mean square error	[27]
Event-triggered without observer	Deterministic	Moderate	Low	Leader-following global consensus	[31]
Event-triggered with node-based observer	Stochastic	Moderate	High	Leader-following exponential consensus	[30,40]
Event-triggered with edge-based observer	Stochastic	Moderate	High	State consensus	[38]
Event-triggered with optimization algorithm	Periodic	Moderate	Low	exponential consensus	[48]
Optimized H_∞ controller	Hidden and Stochastic	Moderate	Low	σ-error mean square stability	[47]
Distributed low-gain controller	Stochastic	Moderate	Low	Leader-following semi-global consensus	[37]
Predictor-based controller	Deterministic	Moderate	Moderate	Closed-loop stability	[49]

Ref. [47] studies the problem of fault detection and consensus control under DoS attack and proposes an attack model based on the hidden semi Markov process for the first time. It can effectively meet the conditions of stealth of attack strategy and complexity of behavior. When a DoS attack comes, the zero-order holder will maintain the amplitude of the last normal input signal. At this time, the system will change from the original uniform sampling system to the non-uniform sampling system, and the sampling period will also change. Using this property, we can define a working mode set $\phi(k)_{k\in\mathbf{N}} \in \mathcal{R} \triangleq \{1, 2, \ldots, R\}$ when the system is attacked, so that we can obtain the emission probability of the system by using a semi Markov kernel and probability density function of mode-dependent dwell time τ only through sample data:

$$\Psi(\phi(k), \eta_k^{\delta_k}) \triangleq \Pr\{\eta_k^{\delta_k} | \phi(k)\}, \tag{21}$$

where $\eta_k^{\delta_k} \in \mathcal{M}$ denotes the set of attack models observed by the system, and $\delta_k \leq \tau$ defines the running time of current mode. Let $l(\delta_k)$ be the δ_k-th observer mode, when the real attack mode is $a \in \mathcal{R}$. Through hidden Markov theory [50], a finite set of observation patterns $\hat{\mathcal{M}}_a$ can be obtained:

$$\begin{aligned} \hat{\mathcal{M}}_a &= \{0 < \Phi\{a, l(\delta_k)\} < 1;\ l(\delta_k) \in \mathcal{M};\ 1 \leq \delta_k \leq \tau\} \\ &= \{\hat{l}^1_{\delta_k}(a),\ \hat{l}^2_{\delta_k}(a), \ldots, \hat{l}^g_{\delta_k}(a)\}, \end{aligned} \tag{22}$$

where $g \triangleq |\hat{\mathcal{M}}_a|$, $\bigcup_{a=1}^{R} \hat{\mathcal{M}}_a = \mathcal{M}$ and

$$\sum_{l_{\delta_k}=\hat{l}^1_{\delta_k}(a)}^{\hat{l}^g_{\delta_k}(a)} \Phi\{a, l(\delta_k)\} = 1. \tag{23}$$

It follows from (23) that in the observation pattern set, there will always be patterns that match the real attack situation. According to the observation mode obtained by the system, the detection and control structure solely depend on the sampled data without knowing the attack statistics.

In addition, ref. [43] discusses the secure synchronization of MAS with linear dynamics under DoS attack with Markov model, but the communication resources are required to be infinite. Refs. [50,51] study the robust tracking problem when the system encounters two kinds of network attacks: communication hold and communication interruption. The switching state of the system under intermittent communication is described by the stochastic Markov process, and the control goal is achieved by using the periodic sampling control scheme based on time series. Ref. [44] discusses the situation that different topological edges of the system are attacked by different DoS at the same time: according to the number of attacked edges, it defines different limiting conditions for the attack and different triggering conditions for the controller. However, it essentially designs different schemes for all subsets of topological edges that are attacked by the same kind of DoS at the same time. Recent studies have also shown a new trend that combines DoS attacks with other system constraints such as failures, interference, saturation, etc. For example, ref. [37] combines DoS attacks with input saturation. On the premise that the system can be stabilized, it uses the small gain theory to linearize, realizing the semi-global security consensus of the system. Ref. [52] designs an observer to solve the synchronization problem of a discrete MAS when the lossy sensor with state threshold exists simultaneously with the network attack. According to whether the communication topology is directed or not, whether the leader exists or not, as well as the system order and isomorphism, the attack model will also be adjusted accordingly, and different theoretical results will be obtained: for example, ref. [10] studies the exponential consensus problem under the directed topology, and [45,53] achieve the ultimate bounded consensus under the undirected topology. Ref. [54] explores a robust output consensus scheme for heterogeneous multi-agent systems under random

DoS attacks. Refs. [55,56] design a control scheme based on self triggering, bypassing the disadvantage that event triggering requires continuous monitoring. As long as the current state value of the agent is known, the next triggering time can be calculated. In the case of maximizing the limitation of attack frequency and duration, a pulse controller with observer structure is proposed in [49] and a state reset method based on measurement error is given. In [57], considering the saturation of the system state and the gain disturbance of the control protocol caused by the network attack and communication congestion of the MAS, combined with the polling method, a robust optimal controller is given to achieve the security consensus of the MAS in the infinite time domain. Ref. [58] points out the challenges that network security brings to MAS in terms of autonomy and information interdependence. They provide a set of basic principles of network security science. The detection algorithm and mitigation algorithm of MAS for network attack are studied in [59], and a practical application example is given based on the distribution automation system. We addressed the robust secure consensus problem in [3] and the antiwindup secure control consensus issue in [35]. It is worth mentioning that the secure consensus protocols proposed in [3,35] are fully distributed secure consensus protocols without using any global information of the communication topologies.

3.2. Spoofing Attack

A MAS can be regarded as a special cyber-physical system. Its controller not only needs to obtain data from sensors, but also needs to send control information to actuators. Network attacks may occur on the channels from a sensor to a controller and from a controller to a actuator—even the controller itself may be attacked. For attackers, in addition to interrupting the information loop, tampering with the data being used for communication can also achieve destructive effects, which is a deception attack.

A spoofing attack refers to an attack in which an attacker can obtain system information and perform arbitrary operations on measurement data and control instructions. It can bypass the detection device and make the agent adopt an error value. Common false data injection (FDI) [60] attacks also fall into the scope of spoofing attacks, as well as data replay [61], data change [12] and other types of attacks. Compared with DoS attacks, deception attacks are more difficult to detect. They exist in power networks [62], smart grids [63] and other fields, which greatly threaten the integrity of data [64].

Refs. [64,65], respectively, consider the spoofing attack on the sensor–controller channel and the controller–actuator channel. Ref. [66] uses the indicator vector to model the deception attack and discusses the situation that the attack occurs on the sensor and actuator at the same time. Generally speaking, the establishment of attack model always revolves around the change of data. Similar to DoS attacks, the research of deception attacks is generally carried out in discrete-time systems, and the control methods adopted include periodic control, event-triggered control, pulse control, etc. Among them, pulse control is more commonly used because it allows discontinuous input and has the characteristics of instantaneous jump, which is very appropriate to deal with some deceptive attacks that implement state mutation.

In [67], for a Lipschitz-type nonlinear MAS under deception attack, a mean-square bounded synchronization control scheme based on distributed impulse control is proposed. Given $i = 1, \dots, N$, the Bernoulli distribution with parameter β is used to model the displacement type spoofing attack behavior on the controller–actuator channel, as shown in Figure 3.

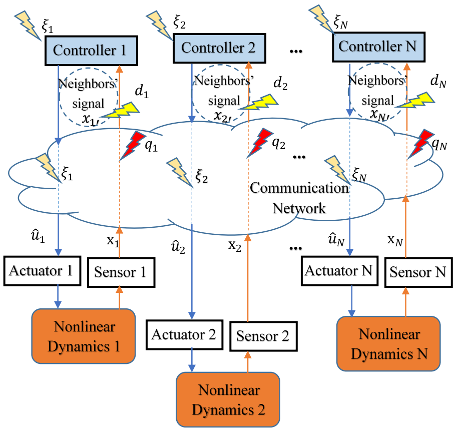

Figure 3. The deception attack in cyber-physical system. According to the secific location of the deception attack, the figure shows three different deception attacks, where ξ_i represents the deception attack on the controller itself or controller–actuator channel (tampering with the control signal u_i), q_i represents the deception attack on the sensor–controller channel (tampering with the output signal y_i), and d_i represents the deception attack on the transmission channel of the neighbor agents (tampering with the state value x_j with $j \in \mathcal{N}_i$).

When the attack succeeds, replace the control input signal u_i with an error signal ψ_i:

$$u_i(t) = c\sum_{k=1}^{\infty}(-\sum_{j=1}^{N} l_{ij}x_j(t) - d_i(x_i(t) - x_l(t)))\delta(t - t_k), \tag{24}$$

$$\hat{u}_i(t) = \sum_{k=1}^{\infty}[\beta_i(t)\psi_i(t) + (1 - \beta_i(t))u_i(t)]\delta(t - t_k), \tag{25}$$

where $\text{Prob}\{\beta_i(t) = 1\} = \bar{\beta}$; $\text{Prob}\{\beta_i(t) = 0\} = 1 - \bar{\beta}$; δ denotes the Dirac pulse; d_i is the corresponding element value of the i-th degree matrix; c is the coupling strength, and it is assumed that β_i is independent and the attack signal is bounded: $\|\psi(t_k)\|^2 \leq \psi$.

For the MASs with the following nonlinear dynamics:

$$\dot{x}_i(t) = Ax_i(t) + Bf(x_i(t) + \hat{u}_i(t)),\ i = 1, \ldots, N, \tag{26}$$

$$\dot{x}_l(t) = Ax_l(t) + Bf(x_l(t)), \tag{27}$$

where x_i is the state of the i-th follower, x_l is the state of the leader and $f(\cdot)$ is a Lipschitz type nonlinear function.

The protocol defines a parameter μ, which corresponds to the Laplace matrix, degree matrix, coupling strength and attack strength. By limiting the value range of μ, the communication topology can be appropriately designed according to the attack situation. At the same time, when μ satisfies the linear matrix inequality condition of the pulse interval parameter h_2—that is, when the pulse interval as well as the topological coupling coefficient match the strength of the deception attack and the attack probability—the control protocols (24) and (25) can successfully defend the deception attack and the followers (26) track the leader (27) in the mean square sense. The selection of coupling strength c and pulse interval parameter h_2 are related to the global information of communication topology, so the control protocol is not completely distributed. In addition, the system dynamics contains random variables about deception attack as β_i. Thus, it can only realize the target of bounded synchronous tracking in the mean square sense. Compared with the case of no attack, $\bar{\beta}$ increases the upper bound of the synchronization error and narrows the pulse spacing, which also puts forward corresponding requirements for c. That is why $\bar{\beta}$ is always restricted.

Compared with [67], ref. [68] studies the overlay spoofing attack on the sensor–controller channel, as shown in Figure 3. The attack causes the normal state value to be superimposed with the error value $q_i(t)$:

$$u_i(t) = \sum_{k=1}^{\infty}[c\sum_{j=1}^{N}[-l_{ij}x_j(t) + \beta_{ij}q_i(t)] - cd_i(t)[x_i(t) - x_l(t)]]\delta(t - t_k). \tag{28}$$

Ref. [68] also achieves mean square bounded synchronization, but only the size of the upper bound of the error is affected by $\bar{\beta}$. Regardless of the attack mode, the synchronization performance is mainly affected by the coupling strength, degree matrix, attack probability and pulse spacing. In particular, the first two terms play a decisive role in reducing synchronization error when the probability of each side being attacked is the same.

Most of the above research fail to effectively eliminate the impact of spoofing attacks on MASs, resulting in the boundedness of their final consensus. As for that, ref. [69] proposes a distributed filter with adaptive compensator as follows:

$$\begin{cases} \dot{\psi}_i(t) = E\psi_i(t) + \hat{\varepsilon}_i(t) \\ \hat{\varepsilon}_i(t) = -\hat{\varepsilon}_i(t) + \varepsilon^a_{q,i}(t) + \rho_{a,i}(t) \\ \rho_{a,ij}(t) = -\frac{F_i^T\hat{\varepsilon}_i(t)\hat{\delta}^2_{a,ij}(t)}{\|F_i^T\hat{\varepsilon}_i(t)\|\hat{\delta}_{a,ij}(t)+\vartheta_{ij}(t)} \end{cases} \tag{29}$$

where $\psi_i(t)$ and $\hat{\varepsilon}_i(t)$ are the states of the observer and filter, respectively. $\varepsilon^a_{q,i}(t)$ is the relative observation, and $\rho_{a,i}(t) = \sum_{j\in N_i} a_{ij}\rho_{a,ij}(t)$ is the compensation term. $\hat{\delta}_{a,ij}(t) = -\lambda\sigma_{ij}(t)\hat{\delta}_{a,ij}(t) + \lambda\|F_i^T\hat{\varepsilon}_i(t)\|$, $\sigma_{ij}(t)$ is a bounded signal. $\hat{\delta}_{a,ij}(t)$ is the estimate of the spoofing attack signal.

Under the function of the filter, the system can compensate the offset of consensus error variables caused by spoofing attacks and achieve accurate consensus result without error. The distributed controller only uses the local information of the agent itself and does not need to use the random characteristic and upper bound of the attack signal, which is more conducive to distributed applications. However, the design complexity of the controller is related to the dimension of the system state, which makes it extremely difficult to design its control parameters for complex systems.

The assumption that the attack is bounded and obeys Bernoulli distribution made in [67,68] is very conservative. It also stipulates that the error values received by the attacked agents are the same and will not vary as the topology changes, resulting in low practicability of the conclusion. Ref. [70] studies the substitution spoofing attack on the transmission channel of the neighbor node, as shown in Figure 3. It only borrows the concept of the "F-local" to limit the maximum number of simultaneous attacks:

$$\mid \{j \in \mathcal{N}_i(k) : (j, i) \in \mathcal{E}_A(k)\} \mid \leq F,\ F \in \mathrm{R}, \tag{30}$$

where $\mathcal{E}_A(k)$ is the topological edge set that is attacked at time point k. Let $\mathcal{E}_T(k)$ be the trust edge set that is known to not be attacked:

$$x^i_j(k) = d^i_j(k),\ j \in \mathcal{N}_i,\ (j, i) \in \mathcal{E}_A(k), \tag{31}$$

$$x^i_j(k) \equiv x_j(k),\ j \in \mathcal{N}_i,\ (j, i) \in \mathcal{E}_T(k), \tag{32}$$

where $x^i_j(k)$ denotes the information received by node i through the edge (j, i) at time point k, and $d^i_j(k)$ represents the error value.

It can be proved that as long as the agent has a trust entry edge, all of its state values will always fall under a trust state value on the interval. Suppose that $H(k)$ and $h(k)$, respectively, represent the largest and minimum state values. When the deception attack occurs on the entry edge of agent i, one has $x_{ij} \notin [h(k), H(k)]$. If x_{ij} is used to update the controller, the agent i may output an abnormal state value, which can lead to the extension of adjustment time, or even system instability. Then, one can design a weighted average sub-sequence reduction algorithm with trust edge set based on [71], so as to complete the screening of problematic state values. The algorithm can be summarized as the following: when there is no trust edge, from the sequence of state values sorted according to size obtained at each time, taking its own state value as the boundary, the first F and the last F state values are screened out; However, if there are trust edges, only the trust values will be sorted and directly used for updating, and other state values will not be processed:

$$x_i(k+1) = x_i(k) + c \sum_{j \in \mathcal{R}_i(k)} a_{ij}(k)(x_j^i(k) - x_i(k)),\ i = 1, \ldots, N, \tag{33}$$

where $\mathcal{R}_i(k)$ is the set of state values for updating after screening. If updated according to the above method, $x_i(k+1) \in [h(k), H(k)]$ will always be satisfied and extreme deviation due to attack will not occur. When there is no trust edge set in the system, if the topology has $2F+1$ robustness [71], the system can achieve elastic consensus under F-local deception attacks. Compared with [67,68], (32) does not introduce random variables of spoofing attacks, so it can achieve more accurate consensus. When the system topology is time-varying $\mathcal{G}(k) = (\mathcal{V}, \mathcal{E}(k))$, the robustness condition needs to be satisfied in a sufficiently long continuous time series to ensure that each node is sufficient to screen the sequence and broadcast the state values accurately. When the system has a trust edge set, the situation is similar, except that the condition of robustness should be consistent with the trust edge set: that is, it should have $2F+1$ generalized robustness with respect to $\mathcal{E}_T$ [70]. In order to further improve the practicability of the conclusion, ref. [70] also considers the situation that the topology does not meet the robustness. If the topology $\mathcal{G}(k) = (\mathcal{V}, \mathcal{E}(k))$ has a spanning tree in a sufficiently long continuous time—that is, the consensus topology has a spanning tree—it can also achieve elastic consensus in a time-varying topology. Further, when $\mathcal{G}_T(k) = (\mathcal{V}, \mathcal{E}_T(k))$ contains a spanning tree, the goal can also be achieved. When the F-local hypothesis is no longer satisfied—that is, when the number of attacks is uncertain—as long as $\mathcal{G}_T(k) = (\mathcal{V}, \mathcal{E}_T(k))$ has a spanning tree and the root node only has a trust entry edge, consensus can also be achieved.

Since spoofing attacks involve the operation of communication data, they are generally more difficult to deal with than DoS attacks that truncate channels. On the one hand, according to the constraint conditions of the attack, the transmission frequency of the control signal and the coupling strength of the communication topology can be designed, and the distributed pulse control can be used to achieve the certain state synchronization. However, the restrictions on the attack situation are generally strong and conservative; On the other hand, a filtering algorithm can be designed to exclude data values suspected of tampering. After this, a secure state update can be carried out, but the corresponding topology needs to be specially constructed. At the same time, since the algorithm can only screen out problematic extreme values, it may be difficult to deal with more complex attacks.

In addition, there are also methods performing security control through state observation [72]. Ref. [60] establishes an observer based on the Kalman filter and realizes the system mean square consensus under the influence of Gaussian white noise and FDI attack. Different from the former, while observing, it also proposes a threshold comparison scheme to decide whether to use the observed value as the input of the next time step, as shown in Figure 4:

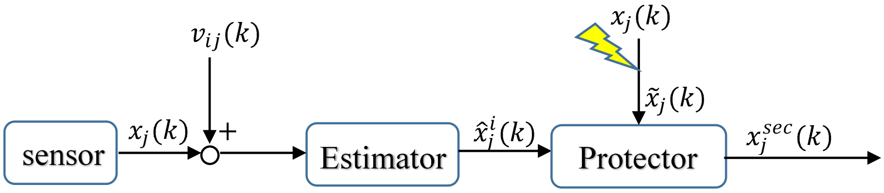

Figure 4. The schematic diagram of the screening mechanism. $x_j(k)$ represents the state value of agent j obtained by the sensor, and $v_{ij}(k)$ is the sensor noise in agent i. $\hat{x}_j^i(k)$ is the state value estimated by agent i, and $\tilde{x}_j(k)$ is the state value that may be tampered by the deception attack. Through the screening mechanism of the protector, the system can finally obtain the secure state value $x_j^{sec}(k)$.

When the difference between the actual value of the state $\tilde{x}_j(k)$ and the observed value $\hat{x}_j^i(k)$ does not meet the preset threshold, observation will be enabled for control. That is,

$$x_i(k+1) = x_i(k) - \epsilon \sum_{j=0}^{N} ll_{ij}(k)[\theta_{ij}(k)\tilde{x}_j(k) + (1-\theta_{ij}(k))\hat{x}_j^i(k))] + \omega_i(k), \tag{34}$$

$$\theta_{ij}(k) = \begin{cases} 1, \text{ if} \|\tilde{x}_j(k) - \hat{x}_j^i(k)\| \le \phi(k) \\ 0, \text{ otherwise.} \end{cases} \tag{35}$$

However, the observer embedded in each agent contains the information of system dynamics structure and communication topology. The control structure is thus not completely distributed.

Ref. [73] studies the detection and identification of physical faults and FDI attacks and designs an exception handling mechanism with independent detector and cooperative detector through a H_∞ multi-objective optimization method. The former is used to judge whether faults and attacks exist, and the latter is used to distinguish the two kinds of anomalies. At the same time, it puts forward the concept of intermediary centrality, which well describes the possibility of different topological edges being attacked so that detection resources can be reasonably allocated. Then, sensitivity and accuracy can be improved. However, there is a compromise between the accuracy and the robustness of the system to disturbances.

Ref. [74] obtains the necessary and sufficient conditions for the system under FDI attack to lose security consensus, according to which the prediction error can be set to an arbitrary value by bypassing the detection mechanism. Ref. [75] constructs a distributed filter against spoofing attacks by using a network composed of sensors of itself and of neighbors. Starting from the characteristic that both belong to opposite side attacks, ref. [76] studies the discrete-time stochastic system under DOS attack and deception attack and achieves consensus through event-triggered control. Ref. [77] gives a detection structure based on a neural network to judge whether the system is attacked by FDI. Ref. [78] proposes the concept of "competitive interaction" to design a flexible and cooperative control mechanism to achieve consensus under FDI attacks.

In order to give a clear survey, we summarize the recent work in Table 3 according to methodologies, attack location, spoofing attack type, centralized, scalability and references.

Table 3. Recent Work on Spoofing Attacks.

Methodologies	Attack Location	Spoofing Attack Type	Centralized	Scalability	References
Impulse control	Sensor–controller channel	Bernouli distributed FDI	Moderate	High	[64,66,68]
Impulse control	Controller–actuator channel	Bernouli distributed FDI	Moderate	High	[65–67]
Secure control	Neighbor information channel	F-local type	Moderate	High	[70,71,73]
Distributed filter with adaptive compensator	Neighbor information channel	Stochastic and bounded	Fully distributed	Low	[69]
Kalman filter based estimator	Information channel	Conditional probability FDI	Moderate	Low	[60]
Neural network based observer	Information channel	White noise based FDI	Moderate	Moderate	[77]
Event-trigger output feedback controller	Neighbor information channel	Bernouli distributed FDI	Moderate	High	[76]

3.3. Byzantine Attack

Imagine a group of unmanned aerial vehicles (UAVs). If the attacker knows several UAVs in the group in advance and continuously sends wrong navigation data to nearby aircraft groups through them, it is obvious that this will cause the group to deviate from the pre-orientation as a whole. It can even cause the group to crash due to the lack of coordination between the air frames. We call these UAVs that continuously launch attacks "abnormal agents". We call the problem that the system must achieve consensus to a variety of state variables in this environment "elastic consensus".

Abnormal agents are generally divided into two types: fault agents and malicious agents. The former is caused by changes in the environment, without human subjective factors, and may cause abnormal updates of the agent's state; The latter is a malicious agent designed by human beings to damage the testability of the system, which may block the operation of the system.

Byzantine attacks describe the attack situation when there are malicious agents in the agent network. Specifically, a malicious agent is an agent that satisfies one of the following three conditions:

1. The state value will not be updated as set.
2. Do not transmit its real state value to at least one outgoing neighbor.
3. The state values transmitted to different outgoing neighbors at the same time are inconsistent.

The focus of their attacks is to send malicious state values to normal agents to make the system disordered. That is, the agent group mistakenly regards the malicious agent as the leader of the system, so that the system state value is guided to a harmful range, as shown in Figure 5. The malicious state value refers to a value that does not conform to the change direction of the normal state value of the system. The key to the problem is to screen out the malicious state value or shield its impact to the maximum extent.

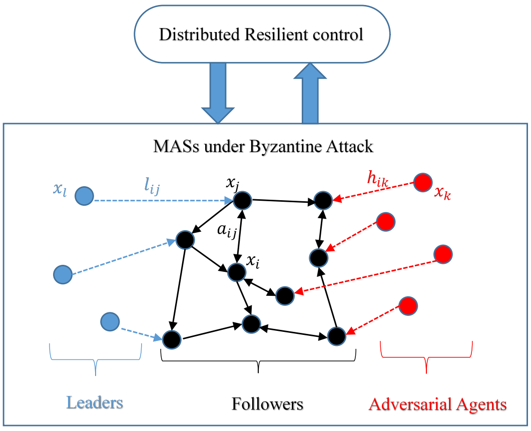

Figure 5. The diagram of a Byzantine attack. When the communication topology of agent i meets certain conditions, each follower x_i can not only directly receive the data of neighbor agent x_j ($a_{ij} \neq 0$), but also directly receive data from leaders x_l ($l_{ij} \neq 0$) and adversarial agents x_k ($h_{ik} \neq 0$). It is worth noting that the abnormal state information sent by x_k may lead the system to an unexpected direction or even cause the system to crash.

Different from the error state value of the above substitution type spoofing attack, the malicious state value of the Byzantine attack is sent by an agent that originally exists in the system topology, while the former is sent by an external attacker. In terms of detection and security control, there will be differences between the two.

To achieve security consensus under the Byzantine attack, there are three main solutions: scheme one is to detect and screen malicious agents in advance, scheme two is to set up trusted decision-making agents, and scheme three is to propose an elastic control structure to maintain the system state or output within a tolerable range. Among them, scheme one is based on the robust structure of the graph, while scheme two generally sets up "trust nodes" to relax the robustness conditions of the graph. The two principles are similar. If the research object of scheme three is a heterogeneous system, it needs to use adaptive control structure or output feedback control structure to adjust under the premise of considering sensor error. The introduction of the concept of topology robustness gradually extends the deployment conditions of attack coping strategies to the communication structure, which can be achieved by modifying on the original topology [79] or constructing a special k-cycle graph [80].

Most of the existing research refers to the mean subsequence reduction (MSR) algorithm under the branch of distributed fault-tolerant control algorithm in the computer field to screen out the state values. However, it can only screen out the state variables with extreme values and has no ability to detect abnormal state values. In order to ensure that the screened state sequence still retains enough state quantity to maintain normal operation, the MSR algorithm generally needs to be applied in combination with graph robustness theory. At the same time, the concept of "F-total" and "F-local" should be used to limit the maximum number of malicious agents in the system [71]. In fact, the F-local type Byzantine model can be transformed into the above F-local type deception attack model as long as the outgoing edge of the Byzantine node is regarded as suffering from a substitution type deception attack. Otherwise, it is not true.

In the absence of external input, the final state value of the consensus achieved by this method always falls in a convex hull composed of the initial state value of the normal agents [81]; this final value will be affected by the behavior of the malicious agent. For the leadership system, the ideal situation is to track the leader's state reference value by followers while shielding the impact of attacks. However, since the reference value may not fall into the above convex hull, further improvement is required.

Ref. [82] uses the modified sliding window MSR algorithm to solve the problem of elastic inclusion control in multi-leader systems and successfully makes followers track leaders whose state values are outside the convex hull. The parameter F in the algorithm is the corresponding parameter F in the F-local model to limit the maximum number of malicious agents. The time window loosens the robustness requirements of the topology map and no longer requires robustness to be maintained at every time step. It can be proved that, under the condition that graph $\mathcal{G}(T)$ has strong $(T, t_0, 2F+1)$ robustness to the leader set $\mathcal{L}$, the system can track the leader state values outside the upper convex hull. This is because the robustness of the topology ensures that there is at least one state value of a normal leader in the filtered state value sequence. Since the design of MSR algorithm needs to obtain the maximum number F of malicious agents in advance, the control protocol is not completely distributed. At the same time, the controller puts forward robustness requirements for communication topology, which makes the controller unsuitable for large-scale MASs.

In the context of the security consensus of MAS on network attacks, in [83] for Byzantine attacks, two improved schemes based on MSR algorithm which relax the strict restrictions of the algorithm on network topology, improve the convergence speed of the system and solve the compatibility problem with clock synchronization are proposed.

Ref. [82] proposes using the sliding window approach to transform the elastic consensus problem in the continuous domain into the discrete domain, making it possible to further improve the scheme through the event-triggered mechanism [84]. The main difficulty in applying event-triggered control to MSR is the processing of the difference between the current state value and the last passed state value. Ref. [84] regards the difference of the above state variables as non-attenuated noise and uses it as the basis for triggering. They give two control schemes to achieve elastic consensus of the system. However, the consensus still has bounded error. At each discrete time, the state value of the agent will be updated. Whether to broadcast it will be decided according to whether the triggered conditions are met: save the last broadcast value as an auxiliary state value; compare it with the updated state value; and trigger if the difference is greater than the threshold value. The author used the modified MSR algorithm and event-triggered mechanism to achieve consensus with bounded error, under the condition that the robustness of relevant topology is satisfied.

Under the event-triggered mechanism, the system cannot achieve accurate consensus and must leave an upper bound of error c that grows exponentially with the number of normal agents. One can set the triggering parameter c_0 by 0 to achieve error free consensus, but the number of triggers will increase. When $t \to \infty$, the event-triggered mechanism will lose its effect due to attenuation. The final conclusion is almost the same as that in [82]. Consider reducing the conservatism of the conclusion by adjusting the update structure. Since the update structure reduces unnecessary state updates, under the same error c, the number of system triggers will be less, but the convergence speed will be slower. In short, the accuracy of event-triggered mechanism and consensus cannot be reconciled well in the context of MSR algorithm. Compared with periodic sampling control, event triggering reduces the number of information exchanges. However, due to the existence of triggering parameters, there is always an error in the consensus state value. At the same time, for the threshold-triggered mechanism, it is also necessary to consider the balance between the convergence performance and the communication frequency caused by the threshold value. Ref. [85] proposes a sliding-mode control method, which only makes periodic judgment when the state is measurable, does not need continuous triggering condition detection and has better economic benefits, which also belongs to a feasible improvement direction.

Ref. [86] focuses on the observation of the state rather than screening. They achieve the uniform ultimate boundedness of the system ouput. In consideration of malicious agent attacks and bounded sensor errors, it designs an observer so that the outputs of all followers in a heterogeneous system converge successfully to a dynamic convex hull composed of the outputs of complex leaders.

For a heterogeneous system with leaders and attackers:

$$\left\{ \begin{array}{c} \dot{x}_i = A_i x_i + B_i u_i, \\ y_i = C_i x_i \end{array} \right., i \in \mathcal{F}, \left\{ \begin{array}{c} \dot{x}_l = S x_l, \\ y_l = R x_l \end{array} \right., l \in \bar{\mathcal{L}}, \left\{ \begin{array}{c} \dot{x}_k = f_k(x_k), \\ y_k = C_k x_k \end{array} \right., k \in \bar{\mathcal{A}}, \tag{36}$$

where $\mathcal{F}$, $\bar{\mathcal{L}}$, $\bar{\mathcal{A}}$ are respectively a collection of followers, leaders and attackers. The controller is

$$u_i = K_i \bar{x}_i + H_i \bar{z}_i - H_i \hat{d}_i, \tag{37}$$

$$\dot{\bar{z}}_i = F_i \bar{z}_i + G_i \bar{e}_{yi}, \tag{38}$$

where $\bar{e}_{yi} = \sum_{j \in \mathcal{F}} a_{ij}(\bar{y}_j - \bar{y}_i) + \sum_{l \in \bar{\mathcal{L}}} a_{il}(y_l - \bar{y}_i) + \sum_{k \in \bar{\mathcal{A}}} a_{ik}(y_k - \bar{y}_i)$. $\bar{x}_i = x_i + \delta_i$ is the measurable state value considering the sensor error δ_i, $\bar{z}_i$ is the corresponding state compensation value, and $\hat{d}_i$ is the compensation signal given by the observer. Matrices K_i, H_i, F_i and G_i are control gains to be designed. By establishing a judgment mechanism to set a_{ij} or a_{ik} to zero, malicious output signals outside the preset range can be effectively excluded from the update calculation. For malicious values within the range, good fault-tolerant control can be achieved through real-time compensation of $\hat{d}_i$. Based on the internal model principle and output-feedback control, the following observer scheme can obtain the compensation signal $\hat{d}_i$:

$$\dot{\hat{x}}_i = A_i \hat{x}_i + B_i K_i \hat{x}_i + B_i H_i \hat{z}_i + B_i H_i \omega_i, \tag{39}$$

$$\dot{\hat{z}}_i = F_i \hat{z}_i + G_i \hat{e}_{yi}, \tag{40}$$

$$\dot{\hat{\delta}}_i = -(A_i + B_i K_i)\theta_i - B_i H_i \omega_i, \tag{41}$$

$$\dot{\hat{d}}_i = F_i \hat{d}_i - G_i C_i \hat{\delta}_i, \tag{42}$$

where $\theta_i = \bar{x}_i - \hat{x}_i - \hat{\delta}_i, \omega_i = \bar{z}_i - \hat{z}_i - \hat{d}_i, \hat{y}_i = C_i \hat{x}_i, \hat{e}_{yi} = \sum_{j \in \mathcal{F}} a_{ij}(\hat{y}_j - \hat{y}_i) + \sum_{l \in \mathcal{L}} a_{il}(y_l - \hat{y}_i)$.

The introduction of term $B_i H_i \omega_i$ in Equation (39) makes the real-time feedback adjustment of the observer more flexible, Since ω_i is only related to $\bar{e}_{yi}$, this term can change dramatically with the change of sensor error and attacker's behavior. $\hat{d}_i$ is mainly affected by ω_i and θ_i. The former can be considered as an elastic index to measure the propagation of error $\bar{e}_{yi}$ in the communication network, while the latter can reflect the observation accuracy of state variables and sensor errors. The introduction of the above parameters makes it have better compensation effects than the traditional observer [87].

One can get the closed-loop error equation of the system by defining $\vec{x}_i = \left[\hat{x}_i^T, \hat{z}_i^T\right]^T$ and combining the augmented output regulation equation. Then, by proving the stability of the error system, it can be proved that the output feedback control protocol can make the followers' output values converge to a dynamic convex hull composed of the leader's output value. In addition, the design of the parameters requires the spectral information of the adjacency matrix, so the protocol is not fully distributed.

At present, there are two main coping strategies for Byzantine attacks: identify malicious agents and move out of the topology [88,89] or design an elastic control structure to maintain the system feature quantity within a tolerable range in the presence of malicious nodes. Ref. [82,84] belong to the latter because the MSR algorithm does not have a detection function. In addition, since the state values are directly screened out, it is equivalent to malicious nodes being invisibly moved out of the topology, which will adversely affect the overall connectivity of the network. For small-scale network topology, the scheme of repairing by real-time compensation is more ideal.

Refs. [90,91] try to improve the algorithm by embedding an input observer. However, this method needs to know the total number of agents attacked and global information such as topology in advance. Ref. [92] breaks through the above limitations and gives a fully distributed observer based on local information for isomorphic systems. The breakthrough of the research still lies in proposing more efficient detection schemes, writing more intelligent screening algorithms and designing more versatile distributed observers.

In addition, refs. [93,94] study the high-order discrete- and continuous-time systems under attack, respectively, by using the robustness of topology. Ref. [95] adopts a robust control scheme based on game theory to achieve elastic consensus. Refs. [96,97] select the weighted MSR algorithm to complete the tracking control of any reference value. Ref. [98] then discusses the security consensus of Byzantine attacks through trusted nodes and also considers setting up decision nodes to avoid malicious values while making specific quantities that tend to be leaders outside the convex hull. Ref. [99] studies the left reversibility of the structure by using the concept of topology node separation, which makes it possible to design communication topology and then realize accurate attack detection. Ref. [90] regards a linear network with abnormal agents as a linear system with sparse actuator anomalies and observes the state with a decoder. Ref. [100] explains the observability of the state of the problem system by using the orthogonal complement matrix, successfully distinguishing the fault agent from the malicious agent, and applying the switched gradient descent algorithm to reduce the computational complexity of the traditional state observation method.

In order to give a clear survey, we summarize the above work in Table 4 according to methodologies, Byzantine attack type, centralized, scalability and references.

Table 4. Recent Work on Byzantine Attacks.

Methodologies	Byzantine Attack Type	Centralized	Scalability	References
MSR algorithm extensions	False data injection	Moderate	High	[85,90–92]
Set up trusted decision-making agents	False data injection	Moderate	Moderate	[88,89]
Elastic control	False data injection	Moderate	Moderate	[82,84,86]

3.4. Relevant Application Scenarios

In some fields closely related to MASs, the above resilient control algorithms are gradually deployed. For example, in the field of intelligent transportation systems, ref. [101] develops a distributed control strategy based on event-triggered mechanism to deal with deception attacks on the sensor–controller channel and achieves the stability of the vehicle platoon system. Ref. [102] designs a resilient controller composed of observers using sliding mode and adaptive estimation theory, focusing on the detection of the vehicle platoon system under DoS attack. In the field of smart grid, ref. [103] establishes a distributed observer structure based on the principle of consensus control, so as to detect FDI attacks in Distributed Generation Units and isolate infected information channels in DC microgrids. Ref. [104] explores the security control of modern power generation systems under DoS attack and proposes an adaptive resilient control protocol based on event-triggered communication scheme. It applies Lyapunov–Krasovskii functional theory to prove the exponential stability of the smart grid system. More relevant studies can be found in [105]. In the field of sensor networks, ref. [106] discusses the H_∞ observation problem under the two-channel FDI attacks. It constructs a distributed observation model against the attack on the basis of the sensor's own information and neighbors' information. In the field of multi-robot systems, ref. [107] provides a distributed switching control protocol based on the consensus control theory for DoS attacks and deception attacks. On the one hand, it gives a coordination-free consensus protocol to adjust the weight of each robot under deception attack. On the other hand, based on the control theory of the leader-following system, it converts the robot compromised by DoS attack into a sub-robot following the specific leader.

Remark 1. *It is worth mentioning that all the works reviewed in this survey are gathered in a systematic way: first connecting keywords such as DoS attacks and Byzantine attacks on Google* *scholar. Then, the reference list of the relevant articles were obtained, followed by narrowing and refining the searching results by year, authors and, finally, source type.*

4. Conclusions and Future Directions

In conclusion, we have provided a survey regarding some recent developments on resilient consensus control of MASs. To sum up, for the security consensus of MAS under network attack, there are two main solutions: designing elastic control structure or anomaly observer. It involves a wide range of research fields, such as adaptive control, feedback control, robust control for controller design, stochastic process theory and probability statistics knowledge for attack modeling, and H_∞-control theory and optimization methods for system optimization. Some screening algorithms and judgment algorithms in the computer field can even be applied. The main thinking directions for different cyber attacks can be summarized as the following: for DoS attacks with communication interruption, the key is how to intervene in the control of MASs during the period of network paralysis, so that it will not have irreparable consensus deviation. For example, building a tighter topology or a more accurate state observer is a good method. Since deception attacks that tamper information involve data operations, we can choose from schemes such as detecting and moving out of topology or constructing observers and compensators to compensate the error value in real time; For the Byzantine attack that implements induced confusion, it is necessary to design a better malicious agent screening algorithm or repair scheme.

However, the survey is by no means complete. Note that there are still many interesting and yet critical issues concerning MASs under cyber attacks that deserve further study, even though a variety of efficient tools have been successfully developed to solve various challenging problems in this active research field. Some interesting yet important future research issues are provided as follows.

1. Since the effectiveness of network attacks is often accompanied by the appearance of physical faults, an interesting problem is to study network security issues together with fault detection, removal and isolation or integrating other abnormal work issues to improve the practicability of the conclusions, such as saturation problems, measurement noise, communication delay, quantization errors and parameter uncertainty. Especially when complex situations such as mismatched disturbances and multiple time delays are involved, some of the elastic control structures obtained for specific models need to be converted into data-driven ones. Otherwise, it is difficult to play its role. When the detection mechanism confuses faults and attacks, the system may crash. Therefore, the screening methods of the two also belong to the feasible scope of discussion.
2. In the consideration of improving the existing research, another interesting topic is to optimize the control structure, improve the attack stochastic model, achieve more accurate consensus conclusions, relax the theoretical assumptions of the original system and improve the performance of the trigger structure. The further relaxation of the assumptions on the topology network and communication environment is beneficial to the compatibility of the elastic control technology.
3. In the case of actual application, an elastic control scheme need to be designed and modified based on the site situation, so as to boost the feasibility of the excellent theory. For example, in reality, the event-triggered mechanism is often less reliable than the periodic sampling control within the allowable range of communication costs due to noise interference, data clutter, processor performance, sensor sensing abnormalities caused by external factors and actuator failures. Compared with information systems, the control parameter requirements applied to industrial systems are often more stringent because of their high risks.

Funding: This work was supported in part by the National Natural Science Foundation of China through Grant No. 61803319, 61903278, in part by the Foundation of State Key Laboratory of Automotive Simulation and Control under Grant No. 20210207, in part by the State Key Laboratory of Automotive Safety and Energy under Grant No. KFY2206, and in part by the Major Science and ATechnology Projects of Xiamen of China under Grant No. 3502Z20201015.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: The authors also would like to thank anonymous reviewers who gave valuable suggestion that has helped to improve the quality of the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Li, Y.; Xu, F.; Xie, G.Q. Review of the development and application of multi-agent technology. *Comput. Eng. Appl.* **2018**, *54*, 13–21.
2. Mou, Z.; Liu, B. Design of a heterogeneous multi-platform sensor management and intelligent control system. *J. Command. Control* **2019**, *5*, 221–227.
3. Wang J.; Deng, X.; Guo, J.; Luo, Y.; Li, K. A fully distributed anti-windup control protocol for intelligent-connected electric vehicles platooning with switching topologies and input saturation. *IEEE/ASME Trans. Mechatron.* **2022**. [CrossRef]
4. Guo, J.; Li, L.; Wang, J.; Li, K. Cyber-physical system-based path tracking control of autonomous vehicles under cyber-attacks. *IEEE Trans. Ind. Inf.* **2022**. [CrossRef]
5. Fortino, G.; Russo, W.; Savaglio, C. Agent-oriented Modeling and Simulation of IoT Networks. In Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS), Gdansk, Poland, 11–14 September 2016; pp. 1449–1452.
6. Mascardi, V.; Weyns, D. Engineering Multi-agent Systems Anno 2025. In Proceedings of the 6th International Workshop on Engineering Multi-Agent Systems (EMAS), Stockholm, Sweden, 14–15 July 2018; pp. 3–16.
7. Kampik, T.; Amaral, C.J.; Hubner, J.F. Developer Operations and Engineering Multi-agent Systems. In Proceedings of the 9th International Workshop on Engineering Multi-Agent Systems (EMAS), Virtual Event, 3–4 May 2021; pp. 175–186.
8. Li, Y.; Tang, C.; Peeta, S.; Wang, Y. Nonlinear consensus-based connected vehicle platoon control incorporating car-following interactions and heterogeneous time delays. *IEEE Trans. Intell. Transp. Syst.* **2019**, *20*, 2209–2219. [CrossRef]
9. Shen, Y.; Wang, X.; Han, S.; Chen, L.; Wang, F. Agent-based technology in intelligent vehicles and drivin: State-of-the-art and prospect. *J. Command. Control* **2019**, *5*, 87–98.
10. Pasqualetti, F.; Bicchi, A.; Bullo, F. Consensus computation in unreliable networks: A system theoretic approach. *IEEE Trans. Intell. Transp. Syst.* **2012**, *57*, 90–104. [CrossRef]
11. Zhang, T.; Li, Z. Resilient Network-level Design of Leader-follower Multi-agent Systems Against DoS Attacks. In Proceedings of the 39th Chinese Control Conference (CCC), Shenyang, China, 27–29 July 2020; pp. 5122–5127.
12. Ma, L.F.; Wang, Z.D.; Yuan, Y. Consensus Control for Nonlinear Multi-Agent Systems Subject to Deception Attacks. In Proceedings of the 22nd International Conference on Automation & Computing (ICAC), University of Essex, Colchester, UK, 7–8 September 2016; pp. 21–26.
13. Su, L.L.; Vaidya, N. Multi-Agent Optimization in the Presence of Byzantine Adversaries: Fundamental Limits. In Proceedings of the American Control Conference (ACC), Boston, MA, USA, 6–8 July 2016; pp. 7183–7188.
14. Franze, G.; Tedesco, F.; Famularo, D. Resilience Against Replay Attacks: A Distributed Model Predictive Control Scheme for Networked Multi-Agent Systems. *IEEE/CAA J. Autom. Sin.* **2021**, *8*, 628–640. [CrossRef]
15. Sizkouhi, A.; Rahimifard, M.; Selmic, R. Covert Attack and Detection Through Deep Neural Network on Vision-Based Navigation Systems of Multi-Agent Autonomous Vehicles. In Proceedings of the 2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Prague, Czech Republic, 9–12 October 2022; pp. 2583–2590.
16. Wang, S.; Zheng, S.; Zhao, C.; Jian, H.; Li, H. Formation control of nonlinear multi-agent systems with actuator and communication attacks,. In Proceedings of the 40th Chinese Control Conference (CCC), Shanghai, China, 26–28 July 2021; pp. 2286–2291.
17. Ahmadzadeh, M.; Ahmadi, M.; Babahaji, M.; Sharifi, I. Resilient Consensus in Double-Integrator Systems with Switching Networks Facing Smart Attacks. In Proceedings of the 7th International Conference on Robotics and Mechatronics (ICRoM), Sharif Univ Technol, Tehran, Iran, 20–21 November 2019; pp. 451–456.
18. Gulzar, M.M.; Rizvi, S.T.H.; Javed, M.Y.; Munir, U.; Asif, H. Multi-agent cooperative control consensus: A comparative review. *Electronics* **2018**, *7*, 22. [CrossRef]
19. Shi, P.; Yan, B. A survey on intelligent control for multi-agent systems. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *51*, 161–176. [CrossRef]
20. Duo, W.; Zhou, M.C.; Abusorrah, A. A survey of cyber attacks on cyber physical systems: Recent advantages and challenges. *IEEE/CAA J. Autom. Sin.* **2022**, *9*, 784–801. [CrossRef]
21. Wu, J.; Peng, C.; Yang, H.; Wang, Y. Recent advances in event-triggered security of networked systems: A survey. *Int. J. Syst. Sci.* **2022**, *53*, 2624–2643. [CrossRef]

22. Ding, L.; Yan, G. A survey of the security issues and defense mechanisms of multi-agent systems. *CAAI Trans. Intell. Syst.* **2020**, *15* 425–434.
23. Wang, J.; Wen, G.; Duan, Z. Distributed anti-windup consensus control of heterogeneous multi-agent systems over Markovian randomly switching topologies. *IEEE Trans. Autom. Control* **2022** , *67*, 6310–6317. [CrossRef]
24. Wang, J.; Guo, J.; Luo, Y.; Li, K.; Zheng, H. Design of switching controller for connected vehicles platooning with intermittent communication via mode-dependent average dwell-time approach. *IEEE Internet Things J.* **2023**, *10*, 2708–2719. [CrossRef]
25. Wang, J.; Duan, Z. A performance region-based approach to the H_∞ leader-following consensus of nonlinear multiagent systems. *Int. J. Robust Nonlinear Control* **2021** , *31(6)*, 2168–2185. [CrossRef]
26. Persis, C.D.; Tesi, P. Resilient control under denial-of-service. In Proceedings of the 19th IFAC Congress, Cape Town, South Africa, 24–29 August 2014; pp. 134–139.
27. Chen, B.; Ho, D.W.C.; Zhang, W.A.; Yu, L. Distributed dimensionality reduction fusion estimation for cyber-physical systems under DoS attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 455–468. [CrossRef]
28. Ruan, M.; Gao, H.; Wang, Y. Secure and privacy-preserving consensus. *IEEE Trans. Autom. Control* **2019**, *64*, 4035–4049. [CrossRef]
29. Cardenas, A.A.; Amin, S.; Sastry, S. Secure control: Towards survivable cyber-physical systems. In Proceedings of the 28th International Conference on Distributed Computing Systems Workshops, Washington, DC, USA, 17–20 June 2008; pp. 495–500.
30. Feng, Z.; Hu, G. Secure cooperative event-triggered control of linear multiagent systems under DoS attacks. *IEEE Trans. Control. Technol.* **2020**, *28*, 741–752. [CrossRef]
31. Xu, Y.; Fang, M.; Shi, P.; Wu, Z.G. Event-based secure consensus of mutiagent systems against DoS attacks. *IEEE Trans. Cybern.* **2020**, *50*, 3468–3476. [CrossRef]
32. Lee, P.; Clark, A.; Bushnell, L.; Poovendran, R. A passivity framework for modeling and mitigating wormhole attacks on networked control systems. *IEEE Trans. Autom. Control* **2014**, *59*, 3224–3237. [CrossRef]
33. Ding, D.; Wang, Z.; Han, Q.; Wei, G. Security control for discrete-time stochastic nonlinear systems subject to deception attacks. *IEEE Trans. Syst. Man Cybern.-Syst.* **2018**, *48*, 779–789. [CrossRef]
34. Shames, I.; Teixeira, A.M.H.; Sandberg, H.; Johansson, K.H. Distributed fault detection for interconnected second-order systems. *Automatica* **2011**, *47*, 2757–2764. [CrossRef]
35. Wang J.; Li, Y.; Duan, Z.; Zeng, J. A fully distributed robust secure consensus protocol for linear multi-agent systems. *IEEE Trans. Circuits Syst. II Express Briefs* **2022**, *69*, 3264–3268. [CrossRef]
36. Foroush, H.S.; Martinez, S. On event-triggered control of linear systems under periodic denial-of-service jamming attacks. In Proceedings of the IEEE 51st Annual Conference on Decision and Control, Maui, HI, USA, 10–13 December 2012; pp. 2551–2556.
37. Du, S.; Yan, Q.; Gao, Y.; Wang, C. Secure consensus of multiagent systems with input saturation and DoS attacks. In Proceedings of the 39th Chinese Control Conference (CCC), Shenyang, China, 27–29 July 2020; pp. 4807–4812.
38. Xu, Y.; Fang, M.; Wu, Z.G.; Pan, Y.J.; Chadli, M.; Huang, T. Input-based event-triggering consensus of multiagent systems under denial-of-service attacks. *IEEE Trans. Syst. Man Cybern.-Syst.* **2020**, *50*, 1455–1464. [CrossRef]
39. Zhang, K.; Wang, D.; Lv, Y. Review of distributed event-trigger control in multi-agent system. *J. Nanjing Univ. Inf. Sci. Technol. (Nat. Sci. Ed.)* **2020**, *12*, 540–548.
40. Dimarogonas, D.V.; Frazzoli, E.; Johansson, K.H. Distributed event-triggered control for multi-agent systems. *Trans. Autom. Control* **2012**, *57*, 1291–1297. [CrossRef]
41. Tabuada, P. Event-triggered real-time scheduling of stabilizing control tasks. *IEEE Trans. Autom. Control* **2007**, *52*, 1680–1685. [CrossRef]
42. Gao, L.; Deng, S.; Ren, W. Differentially private consensus with an event-triggered mechanism. *IEEE Trans. Control. Netw. Syst.* **2019**, *6*, 60–71. [CrossRef]
43. Feng, Z.; Wen, G.; Hu, G. Distributed secure coordinated control for multiagent systems under strategic attacks. *IEEE Trans. Cybern.* **2017**, *47*, 1273–1284. [CrossRef]
44. Yang, Y.; Li, Y.; Yue, D. Event-trigger-based consensus secure control of linear multi-agent systems under DoS attacks over multiple transmission channels. *Sci. China-Inf. Sci.* **2020**, *63*, 150208. [CrossRef]
45. Yi, X.; Liu, K.; Dimarogonas, D.V.; Johansson, K.H. Dynamic event-triggered and self-triggered control for multi-agent systems. *IEEE Trans. Autom. Control* **2019**, *64*, 3300–3307. [CrossRef]
46. Cheng, T.; Kan, Z.; Klotz, J. Event-Triggered Control of Multiagent Systems for Fixed and Time-Varying Network Topologies. *IEEE Trans. Autom. Control* **2017**, *62*, 5365–5371. [CrossRef]
47. Wu, Z.; Xu, Y.; Lu, R.; Wu, Y.; Huang, T. Event-triggered control for consensus of multiagent systems With fixed/switching topologies. *IEEE Trans. Syst. Man Cybern.-Syst.* **2018**, *48*, 1736–1746. [CrossRef]
48. Cheng, Z.; Yue, D.; Hu, S.; Ge, H.; Chen, L., Distributed event-triggered consensus of multi-agent systems under periodic DoS jamming attacks. *Neurocomputing* **2020**, *400*, 458–466. [CrossRef]
49. Feng, S.; Tesi, P. Resilient control under denial-of-service: Robust design. *Automatica* **2017**, *79*, 42–51. [CrossRef]
50. Cai, B.; Zhang, L.; Shi, Y. Control synthesis of hidden semi-Markov uncertain fuzzy systems via observations of hidden modes. *IEEE Trans. Cybern.* **2020**, *50*, 3709–3718. [CrossRef] [PubMed]
51. Feng, Z.; Hu, G.; Wen, G. Distributed consensus tracking for multi-agent systems under two types of attacks. *Int. J. Robust Nonlinear Control* **2016**, *26*, 896–918. [CrossRef]

52. Feng, Z.; Hu, G. Distributed tracking control for multi-agent systems under two types of attacks. In Proceedings of the 19th IFAC World Congress, Cape Town, South Africa, 24–29 August 2014; pp. 1–6.
53. Ding, D.; Wang, Z.; Ho, D.W.C.; Wei, G. Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks. *IEEE Trans. Cybern.* **2017**, *47*, 1936–1947. [CrossRef] [PubMed]
54. Garcia, E.; Cao, Y.; Casbeer, D.W. Decentralized event-triggered consensus with general linear dynamics. *Automatica* **2014**, *50*, 2633–2640. [CrossRef]
55. Xu, W.; Ho, D.W.C.; Zhong, J.; Chen, B. Event/self-triggered control for leader-following consensus over unreliable network with DoS attacks. *IEEE Trans. Neural Netw. Learn. Syst.* **2019**, *30*, 3137–3149. [CrossRef] [PubMed]
56. Senejohnny, D.; Tesi, P.; De Persis, C. Self-triggered coordination over a shared network under denial-of-service. In Proceedings of the 54th IEEE Conference on Decision and Control, Osaka, Japan, 15–18 December 2015; pp. 3469–3474.
57. Shi, M. Research on Network Security and Optimization of Control System Based on Game Theory. Master's Thesis, Yanshan University, Qinhuangdao, China, 2019.
58. Singh, M.P. Cyber security as an application domain for multiagent systems. In Proceedings of the 14th International Conference on Autonomous Agents and Multiagent Systems (AAMAS), Istanbul, Turkey, 4 May 2015.
59. Choi, I.S.; Hong, J.; Kim, T.W. Multi-agent based cyber attack detection and mitigation for distribution automation system. *IEEE Access* **2020**, *8*, 183495–183504. [CrossRef]
60. Zuo, Z.; Cao, X.; Wang, Y. Security control of multi-agent systems under false data injection attacks. *Neurocomputing* **2020**, *404*, 240–246. [CrossRef]
61. Pang, Z.; Liu, G. Design and implementation of secure networked predictive control systems under deception attacks. *IEEE Trans. Control. Technol.* **2012**, *20*, 1334–1342. [CrossRef]
62. Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst.* **2011**, *14*, 1–33. [CrossRef]
63. Deng, R.; Liang, H. False data injection attacks with limited susceptance information and new countermeasures in smart grid. *IEEE Trans. Ind. Inform.* **2019**, *15*, 1619–1628. [CrossRef]
64. Wu, S.; Guo, Z.; Shi, D.; Johansson, K.H.; Shi, L. Optimal innovation-based deception attack on remote state estimation. In Proceedings of the 2017 American Control Conference, Seattle, WA, USA, 24–26 May 2017; pp. 3017–3022.
65. Li, H.; Wu, Y.; Chen, M. Adaptive fault-tolerant tracking control for discrete-time multiagent systems via reinforcement learning algorithm. *IEEE Trans. Cybern.* **2021**, *51*, 1163–1174. [CrossRef] [PubMed]
66. Mustafa, A.; Modares, H. Attack analysis and resilient control design for discrete-time distributed multi-agent systems. *IEEE Robot. Autom. Lett.* **2020**, *5*, 369–376. [CrossRef]
67. He, W.; Mo, Z.; Han, Q.; Qian, F. Secure impulsive synchronization in Lipschitz-type multi-agent systems subject to deception attacks. *IEEE-CAA J. Autom. Sin.* **2020**, *7*, 1326–1334. [CrossRef]
68. He, W.; Gao, X.; Zhong, W.; Qian, F. Secure impulsive synchronization control of multi-agent systems under deception attacks. *Inf. Sci.* **2018**, *459*, 354–368. [CrossRef]
69. Huang, X.; Dong, J. Reliable Leader-to-Follower Formation Control of Multiagent Systems Under Communication Quantization and Attacks. *IEEE Trans. Syst. Man Cybern.-Syst.* **2020**, *50*, 89–99. [CrossRef]
70. Fu, W.; Qin, J.; Shi, Y.; Zheng, W.X.; Kang, Y. Resilient consensus of discrete-time complex cyber-physical networks under deception attacks. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4868–4877. [CrossRef]
71. LeBlanc, H.J.; Zhang, H.; Koutsoukos, X.; Sundaram S. Resilient asymptotic consensus in robust networks. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 766–781. [CrossRef]
72. Li, Y.; Shi, L.; Chen, T. Detection against linear deception attacks on multi-sensor remote state estimation. *IEEE Trans. Control. Netw. Syst.* **2018**, *5*, 846–856. [CrossRef]
73. Li, Y.; Fang, H.; Chen, J. Anomaly detection and identification for multiagent systems subjected to physical faults and cyberattacks. *IEEE Trans. Ind. Electron.* **2020**, *67*, 9724–9733. [CrossRef]
74. Hu, L.; Wang, Z.; Han, Q.; Liu X. State estimation under false data injection attacks: Security analysis and system protection. *Automatica* **2018**, *87*, 176–183. [CrossRef]
75. Ding, D.; Wang, Z.; Ho, D.W.C.; Wei, G. Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks. *Automatica* **2017**, *78*, 231–240. [CrossRef]
76. Ding, D.; Wang, Z.; Wei, G.; Alsaadi, F.E. Event-based security control for discrete-time stochastic systems. *IET Control Theory Appl.* **2016**, *10*, 1808–1815. [CrossRef]
77. Sargolzaei, A.; Yazdani, K.; Abbaspour, A.; Crane, C.D.; Dixon, W.E. Detection and mitigation of false data injection attacks in networked control systems. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4281–4292. [CrossRef]
78. Gusrialdi, A.; Qu, Z.; Simaan, M.A. Competitive interaction design of cooperative systems against attacks. *IEEE Trans. Autom. Control* **2018**, *63*, 3159–3166. [CrossRef]
79. Zhang, H.; Sundaram, S. Robustness of information diffusion algorithms to locally bounded adversaries. In Proceedings of the 2012 American Control Conference, Montreal, QC, Canada, 27–29 June 2012; pp. 5855–5861.
80. Usevitch, J.; Panagou, D. r-Robustness and (r,s)-Robustness of Circulant Graphs. In Proceedings of the 2017 IEEE 56th Annual Conference on Decision and Control, Melbourne, Australia, 12–15 December 2017.

81. Dibaji, S.M.; Ishii, H.; Tempo, R. Resilient randomized quantized consensus. *IEEE Trans. Autom. Control* **2018**, *63* , 2508–2522. [CrossRef]
82. Usevitch, J.; Panagou, D. Resilient leader-follower consensus to arbitrary reference values in time-varying graphs. *IEEE Trans. Autom. Control* **2020**, *65*, 1755–1762. [CrossRef]
83. Yan, H. Research on Distributed Security Mechanism of Multi-Agent System. Master′s Thesis, Hangzhou Dianzi University, Hangzhou, China, 2019.
84. Wang, Y.; Ishii, H. Resilient consensus through event-based communication. *IEEE Trans. Control Netw. Syst.* **2020**, *7*, 471–482. [CrossRef]
85. Behera, A.K.; Bandyopadhyay, B.; Yu, X. Periodic event-triggered sliding mode control. *Automatica* **2018**, *96*, 61–72. [CrossRef]
86. Zuo, S.; Lewis, F.L.; Davoudi, A. Resilient output containment of heterogeneous cooperative and adversarial multigroup systems. *IEEE Trans. Autom. Control* **2020**, *65*, 3104–3111. [CrossRef]
87. Hamidreza, M.; Rohollah, M.; Lewis, F.L.; Ali, D. Static output-feedback synchronisation of multi-agent systems: A secure and unified approach. *IET Control Theory Appl.* **2018**, *12*, 1095–1106.
88. Pasqualetti, F.; Doerfler, F.; Bullo, F. Attack detection and identification in cyber-physical systems. *IEEE Trans. Autom. Control* **2013**, *58*, 2715–2729. [CrossRef]
89. Sundaram, S.; Hadjicostis, C.N. Distributed function calculation via linear iterative strategies in the presence of malicious agents. *IEEE Trans. Autom. Control* **2011**, *56*, 1495–1508. [CrossRef]
90. Fawzi, H.; Tabuada, P.; Diggavi, S. Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Trans. Autom. Control* **2014**, *59*, 1454–1467. [CrossRef]
91. Dibaji, S.M.; Ishii, H. Resilient consensus of double-integrator multi-agent systems. In Proceedings of the 2014 American Control Conference, Portland, OR, USA, 4–6 June 2014; pp. 5139–5144.
92. Xie, C.; Yang, G. Decentralized adaptive fault-tolerant control for large-scale systems with external disturbances and actuator faults. *Automatica* **2017**, *85*, 83–90. [CrossRef]
93. Dibaji, S.M.; Ishii, H. Resilient consensus of second-order agent networks: Asynchronous update rules with delays. *Automatica* **2017**, *81*, 123–132. [CrossRef]
94. LeBlanc, H.J.; Koutsoukos, X. Resilient first-order consensus and weakly stable, higher order synchronization of continuous-time networked multiagent systems. *IEEE Trans. Control Netw. Syst.* **2018**, *5*, 1219–1231. [CrossRef]
95. Vamvoudakis, K.G.; Hespanha, J.P. Game-theory-based consensus learning of double-integrator agents in the presence of worst-case adversaries. *J. Optim. Theory Appl.* **2018**, *177*, 222–253. [CrossRef]
96. Usevitch, J.; Panagou, D. Resilient leader-follower consensus to arbitrary reference values. In Proceedings of the 2018 Annual American Control Conference, Milwaukee, WI, USA, 27–29 June 2018; pp. 1292–1298.
97. Abbas, W.; Vorobeychik, Y.; Koutsoukos, X. Resilient consensus protocol in the presence of trusted nodes. In Proceedings of the 2014 7th International Symposium on Resilient Control Systems, Denver, CO, USA, 19–21 August 2014.
98. Abbas, W.; Laszka, A.; Koutsoukos, X. Improving network connectivity and robustness using trusted nodes with application to resilient consensus. *IEEE Trans. Control Netw. Syst.* **2018**, *5* , 2036–2048. [CrossRef]
99. Weerakkody, S.; Liu, X.; Son, S.H.; Sinopoli, B. A graph-theoretic characterization of perfect attackability for secure design of distributed control systems. *IEEE Trans. Control Netw. Syst.* **2017**, *4*, 60–70. [CrossRef]
100. Lu, A.; Yang, G. Secure state estimation for multiagent systems with faulty and malicious agents. *IEEE Trans. Autom. Control* **2020**, *65*, 3471–3485. [CrossRef]
101. Bansal, K.; Mukhija, P. Event-triggered control of vehicle platoon under deception attacks. *Proc. Inst. Mech. Eng. Part D J. Automob. Eng.* **2022**, *236*, 1401–1413. [CrossRef]
102. Biron, Z.; Dey, S.; Pisu, P. Real-Time Detection and Estimation of Denial of Service Attack in Connected Vehicle Systems. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 3893–3902. [CrossRef]
103. Gallo, A.; Turan, M.; Nahata, P.; Boem, F.; Parisini, T.; Ferrari-Trecate, G. Distributed Cyber-Attack Detection in the Secondary Control of DC Microgrids. In Proceedings of the European Control Conference (ECC), Limassol, Cyprus, 12–15 June 2018; pp. 351–356.
104. Lu, K.; Zeng, G.; Luo, X.; Weng, J.; Zhang, Y.; Li, M. An Adaptive Resilient Load Frequency Controller for Smart Grids With DoS Attacks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 4689–4699. [CrossRef]
105. Huseinovic, A.; Mrdovic, S.; Bicakci, K.; Uludag, S. A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid. *IEEE Access* **2020**, *8*, 177447–177470. [CrossRef]
106. Song, H.; Shi, P.; Zhang, W.; Lim, C.; Yu, L. Distributed H_∞ Estimation in Sensor Networks With Two-Channel Stochastic Attacks. *IEEE Trans. Cybern.* **2020**, *50*, 465–475. [CrossRef] [PubMed]
107. Lee, S.; Min, B. Distributed Control of Multi-Robot Systems in the Presence of Deception and Denial of Service Attacks. *arXiv* **2021**, arXiv:2102.00098.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.