International Core Journal of Engineering Volume 10 Issue 5, 2024
ISSN: 2414-1895 DOI: 10.6919/ICJE.202405_10(5).0019

A Review on Consensus of Nonlinear Multi-Agent Systems under Cyber Attacks

Qiushi Wang[1], Hongwei Ren[2]

[1] School of Information and Communication Engineering, Jilin Institute of Chemical Technology, Jilin 132022, China

[2] Guangdong University of Petrochemical Technology, School of Automation, Maoming 525000, China

Abstract

With the wide application of multi-agent systems (MASs) in industrial, manufacturing and military industries, their security has become a key factor in the development of the society, and the threat of cyber-attacks on system security is becoming more and more prominent. This paper summarizes the current state of research on the consistency of nonlinear multi-intelligent body systems based on cyber-attacks. First, the current research status of several cyber-attacks is described. Subsequently, the current research progress of nonlinear multi-intelligent body system consistency under cyber-attacks is introduced from the perspectives of system dynamics modeling, consistency research and control protocols. Finally, the main challenges facing the research on consistency of nonlinear multi-intelligent body systems under cyber-attacks are outlooked.

Keywords

Cyber Attacks; Nonlinear Multi-Intelligent Systems; Consensus.

1. Introduction

In today's era of rapid technological development, Multi-Agent Systems (MASs) have become an integral part of many fields. A multi-agent system is an ensemble of multiple collaborating and interacting intelligences that work together in a system to achieve a common goal. This system model can be applied in various domains such as unmanned systems, Internet of Things, intelligent transport systems, social networks, etc. In these areas, the performance and stability of multi-intelligent body systems are directly related to the effective operation of the system, so research on multi-intelligent body systems is becoming increasingly important.

However, as networks continue to expand, cybersecurity issues are becoming increasingly serious. The proliferation of cyberattacks poses a serious threat to the operation of multi-intelligence systems, and in May 2017, a major ransomware attack known as WannaCry hit the world. The attack quickly spread to hundreds of thousands of computers around the world by infecting vulnerabilities in the Windows operating system. The attackers used encryption to lock users' files and then blackmailed victims into paying a ransom to unlock them. The attack resulted in the compromise of computer systems across the globe in a wide range of industries, including healthcare organisations, banks and transport systems. As well as paying a hefty ransom, victims are facing huge financial losses to repair systems and recover data. Healthcare organisations, in particular, have experienced the loss of case records and patient data due to the inability to access them properly, which has had a direct impact on healthcare services. In 2013 and 2014, Yahoo Inc. suffered two major data breaches in which attackers stole users' personal information. The attacks compromised the personal information of a large number of users, leaving many people vulnerable to identity theft and phishing attacks. In

ISSN: 2414-1895 DOI: 10.6919/ICJE.202405_10(5).0019

addition to the immediate impact on individual users, this caused long-term damage to Yahoo Inc.'s reputation and user trust.

Therefore, how to defend against cyber attacks has become a hot research topic in recent years. In this context, this paper will review the existing research from the following aspects. Introducing several common network attacks and their effects, and introducing several control protocols under typical attacks. By comprehensively exploring the existing research, we aim to provide valuable knowledge to both academia and industry, and promote further development in the field of multi-intelligent body systems.

2. Cyber Attack in Multi-Intelligent Systems

2.1 State of the Art Research on Denial-of-Service Attacks (DoS Attacks)

DoS attack is one in which the attacker uses various means to prevent the target system from providing normal services in order to achieve the goal of crippling or destroying the system. This type of attack exposes the vulnerability of network systems and reflects the continuous development and improvement of hacking techniques. Over the past few decades, DoS attacks has gone through several stages of evolution. Early attacks focused on consuming network bandwidth by sending large numbers of packets or requests that overloaded the target system and prevented it from functioning properly. As network defence technologies have improved, attacks have evolved to include distributed denial of service (DDoS) attacks, application layer attacks and more. This makes it increasingly difficult to defend against DoS attacks. In [1], event-triggered security cooperation control for linear multi-agent systems under DoS attacks is investigated. They considered time-series based DoS attacks that can occur intermittently with unknown attack strategies. The consensus problem for non-linear multi-agent systems under attack and communication delays is addressed in the literature [2]. Attacking agents can strategically send messages with false values or conspire with other attacking agents to disrupt the normal operation of the system. The distributed consensus control problem for multi-agent systems under DoS attacks is studied in the literature [3]. In contrast to the existing results, the attacker in this paper compromises each channel independently instead of performing the same DoS attack on all channels. Impulse consensus for nonlinear MASs under DoS attack in a leader-follower framework is studied in the literature [4]. Sufficient conditions for the impulsive interval and impulsive attack ratio for which the system can continue to operate are provided, assuming that the system can recover from a DoS attack. Distributed event-triggered security consensus control for multi-agent systems subject to DoS attacks and controller gain variations is discussed in the literature [5]. The paper assumes that information about DoS attacks can be detected, such as the attack period and the duration of successive attacks. The observability of networked control systems under DoS attacks is studied in the literature [6]. It is shown how DoS attacks destroy the observability of networked control systems. Cooperative control of nonlinear multi-agent systems under DoS attacks has been studied in the literature [7], which investigated leader-follower security consensus for second-order multi-agent systems with nonlinear dynamics and event-triggered control strategies under DoS attacks. A consensus security control scheme in the presence of DoS attacks based on an event-triggered mechanism is proposed in the literature [8]. In contrast to the scenario where the attack knocks out all channels simultaneously, the DoS attack discussed in this paper is intermittent, leading to independent failures of multiple transmission channels. The event-triggered consensus problem for second-order nonlinear multi-intelligent body systems under DoS attacks, which prevent communication networks from providing normal services, has been studied in the literature [9]. Considering the general class of DoS attacks of limited duration, novel distributed event-triggered consensus protocols accompanied by first-order holdout are employed to ensure globally bounded consensus convergence under directed network topologies. An event-triggered cluster consensus scheme for heterogeneous nonlinear second-order multi-agent systems subject to intermittent DoS attacks, actuator failures, and integral quadratic constraints is proposed in the literature [10] for a directed communication topology containing a directed spanning

ISSN: 2414-1895 DOI: 10.6919/ICJE.202405_10(5).0019

tree. An event-triggered adaptive fault-tolerant fixed-control scheme for cluster consensus in the face of simultaneous network attacks and actuator failures is designed based on localised communication.

2.2 State of the Art Research on False Data Injection Attacks (FDI Attacks)

FDI attack is an attacker's attempt to introduce false information into the system by manipulating or forging the transmission data in the sensor and actuator channels, thus affecting the system's control process and leading to degradation of the system's performance. This attack typically occurs in scenarios such as control systems, smart grids, IoT and big data applications, and poses a threat to system stability and reliability. FDI attacks are a common form of threat to smart grids. Three different supervised learning techniques have been analysed in the literature [11], each used in conjunction with three different feature selection techniques. Their research contributes to the exploration of strategies to improve the detection, mitigation and recovery of FDI attacks by applying machine learning methods. In the literature [12], a control scheme is proposed that aims to detect and mitigate FDI attacks in networked control systems. The scheme also addresses the challenges posed by measurement and process noise, highlighting the importance of achieving integrated cybersecurity in networked control systems. A new approach to FDI attack detection using autoencoders (AEs) has been introduced in the literature [13], demonstrating the potential of deep learning techniques to protect Industrial Internet of Things (IIoT) systems from critical security threats such as FDI. A comprehensive review of cybersecurity in smart microgrids is presented in the literature [14]. They highlight the importance of addressing the issue of FDI attacks, which disrupt the integrity of data in the network/communication network, as a particularly challenging threat to smart microgrids. FDI attacks against programmable logic controllers (PLCs), an important component of industrial control systems (ICS) in smart grids and smart city systems, have been studied in the literature [15]. The study highlights the potential vulnerability of ICS components to FDI attacks. An attack-resistant distributed cooperative control algorithm based on hidden layers has been proposed in the literature [16] to address the secondary control problem of island microgrids under FDI attacks. Compared to existing attack-resistant distributed control methods, the proposed controller can mitigate the adverse effects of FDI attacks on actuators, sensors and control system communication links by a sufficiently large α and is robust to state-dependent FDI attacks. A recovery controller with discrete-time FDI and Denial of Service (DoS) attacks has been proposed in the literature for DC microgrids [17]. Based on the stability analysis method for hybrid systems, sufficient conditions for selecting the control parameters under DoS attacks with the average delay of FDI attacks and normal communication rate are provided in literature [18]. In this paper, a distributed data-driven intrusion detection method is proposed to detect the presence of sparse hidden FDI attacks in multi-area interconnected power systems. The proposed distributed intrusion detection method avoids the overfitting problem that is common when implementing machine learning algorithms in large-scale systems. In these studies, FDI attacks have attracted considerable attention due to their ability to disrupt the normal operation of the network without being detected. An attack design scheme based on a nonlinear physical constraint model, which is theoretically capable of generating stealthy FDI attacks, has been proposed in the literature [19].FDI attacks represent a class of cyber-attacks that can maliciously alter a large amount of otherwise protected data, which may not be easily detected by existing operational practices, thus degrading the predictive performance of the power system with catastrophic consequences. A novel data-driven FDI attack detection mechanism has been proposed in the literature [20] to automatically detect intrusions and thus improve the reliability and resilience of energy forecasting systems.

2.3 State of the Art Research on Replay Attack

Replay attack is an attack that takes valid communication packets that have been intercepted and retransmits them to the target system. Replay attack does not require any specific information about the system model; it uses channel intrusion, eavesdropping and other means to obtain a certain period of time between the sender and receiver of the communication data, and then at another moment captures the data being re-sent to the receiver. This attack is usually implemented using network

ISSN: 2414-1895 DOI: 10.6919/ICJE.202405_10(5).0019

sniffing, man-in-the-middle attacks and other technical means. First, an in-depth study of the application of security controls to counter replay attacks has been carried out in the literature [21]. By examining the key issues of control, communication and computation, a number of solutions are provided for the overall security of networked systems. The concern in the literature [23] is the sequential detection of replay attacks. They proposed a method for sequential monitoring of replay attacks, which improves the system's ability to combat replay attacks by detecting and identifying attacks in real time. For networked control systems, literature [23] proposed an optimal periodic watermarking scheme to improve the detection efficiency of replay attacks in networked systems. The study highlighted the importance of inserting watermarks at the right time. Furthermore, literature [24] presents a random coding detection scheme in the face of replay attacks, which enhances network security by introducing the concept of random coding to improve the robustness of the system against replay attacks. In the field of networked control systems, literature [25] provides an in-depth analysis of the performance of networked control systems under replay attacks, highlighting the importance of building resilient networked control systems to effectively counter network attacks. Finally, a replay attack detection method based on stochastic game theory has been proposed in literature [26]. By introducing game theory, they provide a more sophisticated and comprehensive perspective to counter the threat of replay attacks that may occur in the system.

Taken together, the studies in the above literature on different types of cyber-attacks provide different methods and theoretical foundations for defending against their effects. From control algorithms to game theory, these studies provide important theoretical support and practical guidance for building more secure and robust network systems. Future research should further deepen the understanding of cyber-attacks and improve existing countermeasures to ensure the security and reliability of network systems.

3. Research on Security Consensus of Nonlinear Multi-agent Systems

3.1 Consensus Studies

Consensus, from the point of view of control theory, means that the state variables of the various intelligences eventually reach consistency under the action of certain control protocols and controllers. These states can be position, speed, etc. State consistency means that the states of multiple intelligences in a system can converge or remain consistent. This consistency can be achieved by coordinating individual decisions or communications, and is the basis for agents to work together. The study of coherence in multi-agent systems focuses not only on the stability and performance of the system as a whole, but also on the interaction and synergy between individuals. Research methods in this area include control theory, optimisation algorithms, distributed algorithms, etc. to achieve consensus of states and behaviors in multi-agent systems. There are also several different forms of studying consistency in different multi-agent systems in the existing literature.

In multi-agent systems without leader [27], appropriate control protocols are usually introduced to make the states of agents in the system converge eventually. This method is widely applicable to both directed connected graphs and undirected connected graphs. The specific description is as follows $\lim_{t\to\infty}\left\|x_i(t)-x_j(t)\right\|=0,\forall i,j=1,\ldots,N.$ Where $x_i(t)$ represents the state of the agent i.

In multi-agent systems with leader [28], the final state of other agents is consistent with that of the leader under the guidance of the control protocol. This consensus control mechanism effectively ensures that the states of the agents in the system are synchronized, so that they tend to the same motion state. In this framework, the leader plays a guiding and regulating role, ensuring that the state of all agents in the system evolves towards a consistent goal through appropriate control strategies. The specific description is as follows $\lim_{t\to\infty}\left\|x_i(t)-x_0(t)\right\|=0,\forall i=1,\ldots,N.$ Where $x_0(t)$ represents the state of the leader.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202405_10(5).0019

The exponential consensus mentioned in reference [29] refers to the situation where the convergence rate of the leader and the following consensus errors in the system is similar to an exponential function. The specific description is as follows $\|x_i(t)-x_0(t)\| \le \theta \|x_i(t_0)-x_0(t_0))\| e^{-\varepsilon(t-t_0)}.\forall i=1,\ldots,N.$ Where θ is constant, ε is the decay rate.

3.2 Nonlinear Multi-agent System Dynamics Model

Nowadays, as multi-agents play an increasingly important role in various fields, the research on the consistency of multi-agent systems is only increasing. Compared with traditional linear systems, the modeling of nonlinear multi-agent systems is more close to the real situation and can more accurately capture the complex dynamic behavior of the system. A typical nonlinear system is proposed in reference [30] as follows:

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

Where $f(x_i(t))$ is the internal nonlinear function of the agent i. In practice, the system is more susceptible to external environment and other interference. A heterogeneous nonlinear second-order multi-agent system with actuator faults and integral quadratic constraints is proposed in reference [10].

$$\begin{cases} \dot{x}_i(t) = v_i(t), & i = 1,\ldots,N \\ \dot{v}_i(t) = f_{n_i}(t, x_i(t), v_i(t)) + u_i^F(t) + \sum_{k=1}^{p_i} B_{ik} w_{ik}(t) & n_i = 1,2,\ldots,s \\ \xi_{ik}(t) = H_{ik} v_i(t) + G_{ik} u_i^F(t), & k = 1,2,\ldots,p_i \end{cases} \tag{2}$$

Where $x_i(t), v_i(t)$ and $u_i^F(t)$ represents position status, speed status and fault input signal respectively. $w_{ik}(t)$ and $\xi_{ik}(t)$ are respectively the output and input of the integral quadratic constraint. $f_{n_i}(t, x_i(t), v_i(t))$ represents the nonlinear dynamics of the agent itself and is a differentiable nonlinear bounded function. B_{ik}, H_{ik} and G_{ik} are parametric matrices with appropriate dimensions.

For systems with nonlinear parts and uncertain interference, nonlinear and uncertain terms were transformed respectively in [31] and [32]. In most literatures, equivalent transformation was carried out using existing mathematical theories, but the actual situation was often more complicated, so the transformation process was not completely equivalent. And the system modeling in practical engineering is not exactly the same, how to establish the equivalent mathematical model of engineering system and the mathematical equivalent transformation of nonlinear and external interference is also the future focus of research.

3.3 Nonlinear Multi-agent System Control Protocol

3.2.1 Event-triggered Control

The core of event-triggered control is to decide when to update control based on the change in system state. The basic principle involves the design of trigger conditions and the construction of an event generator. In nonlinear multi-agent systems, the principle of event-triggered control has a more significant advantage because it can flexibly adjust the control frequency according to the specific dynamic characteristics of the system, thus reducing the computational and communication burden. The design of the trigger conditions includes the monitoring of the system state and system faults.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202405_10(5).0019

For example, in the literature [33], an event-triggered strategy using a predictive observer is proposed to solve the failure of event triggering control under DoS attacks. Specific description is as follows:

$$t_{k+1}^{i} = inf\left\{ t > t_k^i \mid e_i^T(t)\Omega e_i(t) \geq \theta \left\| \sum_{j=1}^{N} a_{ij}(\delta_i(t) - \delta_j(t)) \right\|_{\Omega}^{2} \right\} \tag{3}$$

Where $e_i(t)$ represents the error between the agent's estimated state and the predicted state, $\delta_i(t)$ represents the error between the agent's predicted state and the actual state. Ω is a positive definite matrix and θ is a normal number. This event- triggered control is a static event-triggered control. In [34], a dynamic event triggering control is designed by introducing a dynamic variable, which plays an important role in excluding Zeno's behavior. When the dynamic variable is 0, the event-triggered mechanism becomes a static event triggering control. Trigger conditions can also be designed by defining the threshold of error or the rate of system state change. For example, in [35], a threshold event-triggered mechanism is designed to detect and determine whether to update the impulsive control input. This flexibility enables the event-triggered control to be adjusted only when the system needs it, effectively reducing the control frequency and saving the communication resources of the system. The construction of event generator is a key component of event-triggered control. The accuracy and stability of trigger control can be ensured by designing the event generator properly. Common generators include cycle trigger, threshold trigger, and so on. In nonlinear multi-agent systems, it is very important to select the appropriate event generator to adapt to the system dynamic characteristics and task requirements.

In addition, other researches on event-triggered control have proposed a new two-layer event-triggered sliding mode control class [36], which is specially used to achieve finite-time robust consensus in nonlinear disturbed multi-agent systems. Notably, this approach is considered to be comparable in algorithmic complexity to traditional single-layer event-triggered sliding mode control. Further developing on this topic, the input delay edge in the event-triggered consensus scenario of multi-agent systems is deeply studied in [37]. Important contributions have been made to their research, including the elaboration of a parametric setting procedure, the accurate calculation of input delay edges, the derivation of more general conditions for building event trigger functions to exclude Zeno behavior, the application of self-triggering control schemes to avoid continuous measurements, and the solution of unmeasurable state problems with observer-based control schemes. The event-triggered consensus tracking of higher-order stochastic nonlinear multi-agent systems is studied in literature [38]. In addition, the effectiveness of the proposed event-triggered control scheme is verified by numerical examples. Literature [39] extends consensus to FR actional-order multi-agent systems by triggering control of sampled data events, and proposes a distributed control protocol to ensure the consensus of fractional-order multi-agent systems. In another study, reference [40] focuses on the consensus tracking problem of continuously switched stochastic nonlinear multi-agent systems, using an event-triggered control strategy. Their work involves a new protocol design framework and the effectiveness of the proposed event-triggered control scheme is tested by numerical examples. In [41], an observer-based event-triggered control method is proposed for linear multi-agent systems with unmeasurable states to solve the distributed optimal coordination problem. The issue of event-triggered tracking control for second-order multi-agent systems with system nonlinearity is investigated in literature [42] using the distributed sliding mode control method. By employing distributed events to trigger the sliding mode controller, the system state can converge to the integral sliding mode surface within a finite time period. A collaborative control design for heterogeneous multi-agent systems is proposed in literature [43], utilizing an event-triggered approach. This design scheme is implemented on both linear heterogeneous multi-agent systems and uncertain Euler-Lagrange multi-agent systems, yielding significantly improved results compared to existing approaches. Extending the research to predetermined performance control, reference [44] discusses

ISSN: 2414-1895 DOI: 10.6919/ICJE.202405_10(5).0019

the problem of simultaneous state triggering and controller output triggering in multi-agent systems. The backstepping technique is successfully employed to construct a virtual control signal based on the original system state in the event-triggering control design. In a recent contribution, [45] examines a multi-agent system with input constraints and proposes a centralized dynamic time-interval event triggering strategy along with an appropriately designed minimum interevent time. This triggering strategy simplifies the evaluation process of system stability and Zeno behavior by introducing scaling ideas into the algorithm.

3.2.2 Adaptive Control

Adaptive control is a method that dynamically adjusts control parameters in real time based on the system's dynamic characteristics, with the objective of effectively dealing with system dynamics and external disturbances. This approach continuously monitors system performance and automatically adapts the control strategy to ensure stability and optimal performance in an uncertain environment. The fundamental principle of adaptive control involves model reference and parameter adjustment. The model reference method generates a control signal by comparing the error between the actual system output and the desired output from a reference model. Parameter adjustment entails real-time identification of system dynamic characteristics and correction of parameters to adapt to changes in the system. A basic distributed adaptive control protocol is designed in [46], which is described as follows:

$$u_i(t) = K[\sum_{j=0, j\neq i}^{N} a_{ij}(x_i(t) - x_j(t)) + b_i(x_i(t) - x_0(t))] \tag{4}$$

Where $x_0(t)$ is the state of leader, $x_i(t)$ and $x_j(t)$ is the state of follower. a_{ij} represents the network topology, b_i represents the connection state between the leader and the follower, K is the control gain.

In addition, other studies on adaptive control have made contributions to this field by solving the fixed-time tracking problem of uncertain nonlinear systems in [48]. Their method involves expressing parametric adaptive methods as nonlinear differential equations, which is different from traditional adaptive design methods. On the basis of this topic, reference [49] extends their research to the problem of adaptive fuzzy tracking control for strict feedback nonlinear systems with time-varying input delay and all-state constraints. By using fuzzy logic systems to approximate unknown nonlinear functions, they propose a novel adaptive fuzzy backstepping control strategy to ensure the semi-global final uniform boundedness of closed loop nonlinear systems. A novel control design based on cooperative control theory was introduced in [50] for controlling a single-jointed robotic arm driven by pneumatic artificial muscles (PAMs) in the opposing biceps/triceps position. In a real PAM drive system, uncertainty is the inherent characteristic of its parameters, so an adaptive cooperative control algorithm is proposed for PAM-driven robot arms that are perturbed by parameters. In [51], a fuzzy adaptive two-position trigger control is studied for uncertain nonlinear systems with actuator faults and dead-time constraints. Based on the improved fuzzy logic system (FLSs), a fuzzy adaptive compensation control is established to solve these problems. Literature [52] extends the research scope to a class of adaptive practical fixed time control strategies for nonlinear systems with strict feedback. A novel adaptive practical fixed time controller is constructed by using backward step algorithm, finite time Lyapunov stability theory and fuzzy logic control. In [53], the finite-time adaptive fuzzy preset performance control for non-strict feedback nonlinear systems is considered. A finite-time adaptive output feedback controller is constructed by integrating pre-set performance control and command filter technology into backstep recursive design, and the stability of closed loop system is strictly proved. For uncertain nonlinear systems with input lag, a fuzzy adaptive event-triggered finite time constraint control method is proposed in [54]. This innovative approach aims to

ISSN: 2414-1895 DOI: 10.6919/ICJE.202405_10(5).0019

effectively utilize limited communication resources to mitigate the impact of input lag on the performance and convergence time of the control system. In [55], the adaptive neural decentralized tracking control problem for a class of output-constrained switched connected nonlinear systems with unknown similar feedback lag control inputs is considered. Numerical simulation results show the effectiveness of the adaptive decentralized control scheme. Finally, the fault-tolerant consensus control problem of general nonlinear multi-agent systems under actuator fault, interference and fault network is solved in [56]. Based on a neural network observer and adaptive control strategy, they design a fault-tolerant consensus control scheme that ensures a bounded consensus for closed loop multi-agent systems with interference and fault networks and actuator faults.

3.2.3 Impulsive Control

Impulsive control is a discrete control method, the essence of which is that the state of the system experiences a sudden change at a discrete time point, which is usually triggered by the impulse signal. The form of pulse can be rectangular impulsive, exponential impulsive, etc. Different forms of pulse will lead to different responses of the system. The basic principle of pulse control includes pulse generation, application and influence. The generation of pulse involves the design and generation method of impulsive signal, and the application of impulsive is realized by coupling the impulsive signal with the dynamic equation of the system. The pulse affects the evolution of the system by changing the state of the system, so as to achieve the predetermined control goal. A distributed event-triggered impulsive protocol was designed in reference [57], in which each agent receives information from neighboring agents and performs impulsive control only when its own trigger function exceeds a given tolerance, which is described as follows:

$$u_i(t) = \sum_{k=1}^{\infty} (-(x_i(t) - x_j(t))\delta(t - t_k^i)) \tag{5}$$

Where $x_i(t)$ and $x_j(t)$ is the state of the agent i and the agent j. t_k^i is impulsive instant. $\delta(t)$ is Dirac function.

In addition, in other researches on impulsive control, the consensus problem of nonlinear multi-agent systems is deeply studied in literature [58], which adopts impulsive-based protocol and event-based asynchronous sampling data. They established sufficient conditions regarding system parameters and event-based sampling schemes to ensure consensus. Literature [59] focuses on the dynamic consensus protocol of a class of nonlinear saturated multi-agent systems, which makes the traditional low-gain feedback method no longer applicable. Their work introduces alternative approaches for input-saturated scenarios. Reference [60] studies the adaptive consensus problem of multi-agent nonlinear systems, with special attention to odd-impulsive control sequences. The proposed pulse control protocol with odd impulsive sequence is more efficient and flexible than the existing fixed pulse consensus method for multi-agent systems. Reference [61] discusses the consensus problem of nonlinear multi-agent systems with fuzzy modeling uncertainty through the state-constrained mixed pulse protocol. They replace the uncertainty of multi-agent systems with fuzzy logic systems and propose a judgment strategy that only includes relative information with neighbors. Literature [62] studies the consensus control scheme of nonlinear multi-agent systems subject to random disturbance, and adopts an effective variable pulse consensus method to eliminate the limitation of fixed pulse time, so as to be more reliable and flexible in practical applications. In [63], the problem of pulse dichotomous consensus for second-order multi-agent systems without relative velocity information is studied. Using topological graph theory, they designed a distributed impulsive control strategy. On the other hand, some studies have considered the consensus problem of multi-agent systems caused by edge event-triggered strategies and state-constrained impulsive control. Regarding the trigger control of edge events, its rules are proposed in [64], and the trigger time of edge events is made into pulse time to avoid Zeno behavior. In [65], the leader-following consensus problem under pulse

ISSN: 2414-1895 DOI: 10.6919/ICJE.202405_10(5).0019

control for nonlinear multi-agent systems with interval time-varying delay is studied. By utilizing the stability theory of pulsed systems and algebraic graph theory, they deduced sufficient conditions to ensure a multi-agent system leader-follow consensus. Literature [66] studies how to achieve the state consensus of the whole system by dynamically adding some new agent groups to the original multi-agent system. They use impulsive control theory and Lyapunov stability theory to analyze the conditions, so that the whole multi-agent system with dynamic addition characteristics can achieve state consensus. Reference [67] aims to propose a self-triggered consensus control scheme for nonlinear multi-agent systems with sensor saturation. The controller is designed to be updated only in discrete time, thus enabling the system to be modeled as a hybrid system with pulse dynamics.

4. Summary

In this paper, the influence of network attacks on the consistency of nonlinear multi-agents is deeply studied, and the current research progress in related fields is reviewed. Firstly, we discuss various kinds of network attacks, including DoS attack, fake data injection attack and replay attack, and make clear the mechanism of these attacks to destroy the consistency of multi-agent system. Secondly, by combing the basic knowledge of nonlinear multi-agent system, the basic knowledge of system mathematical model and control protocol is introduced, which lays a foundation for the subsequent research.

Despite the remarkable progress in existing research, there are still a series of problems that need to be solved in the face of increasingly complex forms of cyber attacks and nonlinear multi-agent systems. First of all, the hidden and difficult to detect nature of attacks is still a problem that needs to be solved. Future research could explore the use of advanced techniques such as deep learning to improve the accuracy and real-time of attack detection. Secondly, with the continuous expansion of the application field of multi-agent systems, the complexity of the system is also increasing, so the need to further develop the robustness enhancement technology to ensure that the system can maintain consistency under attack. Finally, interdisciplinary research should be strengthened to integrate knowledge in fields such as control theory, communication technology and network security to promote the further development of this research field.

In general, although there are some limitations, this review provides useful implications for future research and hopes to promote the further development of the academic community in the field of cyber attack and nonlinear multi-agent consistency.

Acknowledgments

This research was funded in part by National Natural Science Foundation of China under Grant 62273109, in part by the Guangdong Basic and Applied Basic Research Foundation under Grant 2023A1515010168, Grant 2019A1515010830, in part by the Key Special Foundation for General Universities in Guangdong Province under Grant 2022ZDZX1018, and in part by the Maoming Science and Technology Plan Foundation under Grant 2022S043.

References

[1] Feng, Zhi and G. Hu . "Distributed secure average consensus for linear multi-agent systems under DoS attacks." 2017 American Control Conference (ACC) IEEE, 2017: 2261-2266.

[2] Yiming, Wu and Xiongxiong He. "Secure consensus control for multiagent systems with attacks and communication delays," IEEE/CAA Journal of Automatica Sinica, 2017, 4(1): 136-142.

[3] An-Yang, Yang and Guang-Hong. "Distributed consensus control for multi-agent systems under denial-of-service." Information Sciences: An International Journal 439-440(2018):95-107.

[4] Yiting Wang and Wangli He. "Impulsive Consensus of Leader-following Nonlinear Multi-agent Systems Under DoS Attacks", IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society, 2019, 6274-6279.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202405_10(5).0019

[5] Lijuan Zhang, Jinliang Liu and Jinde Cao ."Resilient event-triggered consensus control for nonlinear muti-agent systems with DoS attacks."Journal of the Franklin Institute, 2019, 356(13):7071-7090.

[6] Liu, Chenxi, et al. "Observability Analysis of Networked Control Systems Under DoS Attacks." IECON 2023-49th Annual Conference of the IEEE Industrial Electronics Society. IEEE, 2023: 1-6.

[7] Tao Dong and Yanlin Gong; "Leader-following Secure Consensus for Second-order Multi-agent Systems with Nonlinear Dynamics and Event-triggered Control Strategy Under DoS Attack", Neurocomputing, 2020,416(21):95-102.

[8] Yang Yang, Yanfei Li and Dong Yue. "Event-trigger-based Consensus Secure Control of Linear Multi-agent System Under DoS Attacks Over Multiple Transmission Channels", Science China Information Sciences, 2020,63(150208).

[9] Yu Shang, ChengLin Liu and KeCai Cao; "Event-triggered Consensus Control of Second-order Nonlinear Multi-agent Systems Under Denial-of-service Attacks", Transactions of the Institute of Measurement and Control, 2021;43(10):2272-2281.

[10] XiangGui Guo; PeiMing Liu; JianLiang Wang; Choon Ki Ahn; "Event-Triggered Adaptive Fault-Tolerant Pinning Control for Cluster Consensus of Heterogeneous Nonlinear Multi-Agent Systems Under Aperiodic DoS Attacks", IEEE Transactions on Network Science and Engineering, 2021, 8 (2) :1941-1956.

[11] J. Sakhnini, H. Karimipour and A. Dehghantanha, "Smart Grid Cyber Attacks Detection Using Supervised Learning and Heuristic Feature Selection," 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 2019; 108-112.

[12] Arman Sargolzaei; Kasra Yazdani; Alireza Abbaspour; Carl D. Crane III; Warren E. Dixon; "Detection and Mitigation of False Data Injection Attacks in Networked Control Systems", IEEE Transactions on Industrial Informatics, 2019, 16(6): 4281-4292.

[13] Mariam M. N. Aboelwafa; Karim G. Seddik; Mohamed Hamdy Eldeframwy; Yasser Gadallah; Mikael Gidlund; "A Machine-Learning-Based Technique for False Data Injection Attacks Detection in Industrial IoT", IEEE Internet of Things Journal, 2020, 7(9): 8462-8471.

[14] Farzam Nejabatkhah; Yun Wei Li; Hao Liang; Rouzbeh Reza Ahrabi; "Cyber-Security of Smart Microgrids: A Survey",Energies, 2020, 14(1): 27.

[15] Serkan Gönen; H. Hüseyin Sayan; Ercan Nurcan Yilmaz; Furkan Üstünsoy; Gökçe Karacayilmaz; "False Data Injection Attacks and The Insider Threat in Smart Systems", Computers & Security, 2020, 97: 101955.

[16] Yulin Chen; Donglian Qi; Hangning Dong; Chaoyong Li; Zhenming Li; Jianliang Zhang; "A FDI Attack-Resilient Distributed Secondary Control Strategy for Islanded Microgrids", IEEE Transactions on Smart Grid, 2020, 12(3): 1929-1938.

[17] Xiao-Kang Liu; Changyun Wen; Qianwen Xu; Yan-Wu Wang; "Resilient Control and Analysis for DC Microgrid System Under DoS and Impulsive FDI Attacks", IEEE Transactions on Smart Grid, 2021, 12(5): 3742-3754.

[18] Jiayu Shi; Shichao Liu; Bo Chen; Li Yu; "Distributed Data-Driven Intrusion Detection for Sparse Stealthy FDI Attacks in Smart Grids", IEEE Transactions on Circuits and Systems II: Express Briefs, 2020, 68(3): 993-997.

[19] Nam N. Tran; Hemanshu R. Pota; Quang N. Tran; Jiankun Hu; "Designing Constraint-Based False Data-Injection Attacks Against The Unbalanced Distribution Smart Grids", IEEE Internet of Things Journal, 2021, 8(11): 9422-9435.

[20] A. Ahmadi; Mojtaba Nabipour; Saman Taheri; B. Mohammadi-ivatloo; V. Vahidinasab "A New False Data Injection Attack Detection Model for Cyberattack Resilient Energy Forecasting",IEEE Transactions on Industrial Informatics, 2022, 19(1): 371-381.

[21] Mo, Yilin, and Bruno Sinopoli. "Secure control against replay attacks." 2009 47th annual Allerton conference on communication, control, and computing (Allerton). IEEE, 2009: 911-918.

[22] Naha, Arunava, et al. "Sequential detection of replay attacks." IEEE Transactions on Automatic Control, 2022, 68(3): 1941-1948.

[23] Fang, Chongrong, et al. "Optimal periodic watermarking schedule for replay attack detection in cyber–physical systems." Automatica, 2020, 112: 108698.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202405_10(5).0019

[24] Ye, Dan, Tian-Yu Zhang, and Ge Guo. "Stochastic coding detection scheme in cyber-physical systems against replay attack." Information Sciences, 2019, 481: 432-444.

[25] Zhu, Minghui, and Sonia Martinez. "On the performance analysis of resilient networked control systems under replay attacks." IEEE Transactions on Automatic Control, 2013, 59(3): 804-808.

[26] Miao, Fei, Miroslav Pajic, and George J. Pappas. "Stochastic game approach for replay attack detection." 52nd IEEE conference on decision and control. IEEE, 2013: 1854-1859.

[27] Lei Chen, Zhongshen Li. A review of multi-intelligent body system consistency. Automation Expo, 2018, 35(2):74-78.

[28] Tan, Xuegang, Jinde Cao, and Xaodi Li. "Consensus of leader-following multiagent systems: A distributed event-triggered impulsive control strategy." IEEE Transactions on Cybernetics, 2018, 49(3): 792-801.

[29] Wang, Yiting, and Wangli He. "Impulsive consensus of leader-following nonlinear multi-agent systems under DoS attacks," IECON 2019-45th Annual Conference of the IEEE Industrial Electronics Society. IEEE, 2019, 1: 6274-6279.

[30] Tang, Wenyan, et al. "Consensus of nonlinear multi–agent systems with distributed event–triggered impulsive control." Journal of Vibration and Control, 2022, 28(7-8): 882-891.

[31] Liu, Yang, and Yingmin Jia. "Event-triggered consensus control for uncertain multi-agent systems with external disturbance." International Journal of Systems Science, 2019, 50(1): 130-140.

[32] Qi, Yiwen, et al. "Event-triggered and guaranteed cost finite-time H∞ control for uncertain switched linear systems." Optimal Control Applications and Methods, 2018, 39(4): 1337-1353.

[33] Sun, Yuan-Cheng, and Guang-Hong Yang. "Event-triggered distributed state estimation for multiagent systems under DoS attacks." IEEE Transactions on Cybernetics, 2020, 52(7): 6901-6910.

[34] D. Liu and G. -H. Yang, "A Dynamic Event-Triggered Control Approach to Leader-Following Consensus for Linear Multiagent Systems." IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2021, 51(10) : 6271-6279.

[35] K. Zhang and E. Braverman"Event-Triggered Impulsive Control for Nonlinear Systems With Actuation Delays." IEEE Transactions on Automatic Control, 2023, 68(1) : 540-547.

[36] Leimin Wang; Ming-Feng Ge; Zhigang Zeng; Junhao Hu; "Finite-time Robust Consensus of Nonlinear Disturbed Multiagent Systems Via Two-layer Event-triggered Control."Information Sciences, 2018, 466: 270-283.

[37] Nankun Mu; Yonghui Wu; Xiaofeng Liao; Tingwen Huang "Input Time Delay Margin In Event-Triggered Consensus Of Multiagent Systems" IEEE transactions on cybernetics, 2018, 49(5): 1849-1858.

[38] Wencheng Zou; Choon Ki Ahn; Zhengrong Xiang "Event-Triggered Consensus Tracking Control of Stochastic Nonlinear Multiagent Systems" IEEE Systems Journal, 2019, 13(4): 4051-4059.

[39] Yiwen Chen; Guoguang Wen; Zhaoxia Peng; Ahmed Rahmani "Consensus of Fractional-order Multiagent System Via Sampled-data Event-triggered Control" Journal of the Franklin Institute, 2019, 356(17): 10241-10259.

[40] Wencheng Zou; Peng Shi; Zhengrong Xiang; Yan Shi"Consensus Tracking Control Of Switched Stochastic Nonlinear Multiagent Systems Via Event-Triggered Strategy" IEEE Transactions on Neural Networks and Learning Systems, 2019, 31(3): 1036-1045.

[41] Zhenhong Li; Zizhen Wu; Zhongkui Li; Zhengtao Ding "Distributed Optimal Coordination for Heterogeneous Linear Multiagent Systems With Event-Triggered Mechanisms" IEEE Transactions on Automatic Control, 2019, 65(4): 1763-1770.

[42] Deyin Yao; Hongyi Li; Renquan Lu; Yang Shi "Distributed Sliding-Mode Tracking Control Of Second-Order Nonlinear Multiagent Systems: An Event-Triggered Approach" IEEE Transactions on Cybernetics, 2020, 50(9): 3892-3902.

[43] Yi Dong; Zongli Lin "An Event-Triggered Observer and Its Applications in Cooperative Control of Multiagent Systems" IEEE Transactions on Automatic Control, 2021, 67(7): 3647-3654.

[44] Lili Zhang; Weiwei Che; Chao Deng; Zhengguang Wu "Prescribed Performance Control for Multiagent Systems Via Fuzzy Adaptive Event-Triggered Strategy" IEEE Transactions on Fuzzy Systems, 2022, 30(12): 5078-5090.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202405_10(5).0019

[45] Zhang, Kai, et al. "Consensus of Input Constrained Multi-Agent Systems by Dynamic Time-Varying Event-Triggered Strategy With a Designable Minimal Inter-Event Time." IEEE Transactions on Circuits and Systems II: Express Briefs, 2023.

[46] H. Tang, Y. -J. Wu and X. -Z. Jin, "Robust Adaptive Leader-following Control of a Class of Multi-agent Systems" 2020 Chinese Control And Decision Conference (CCDC). IEEE, 2020: 2967-2972.

[47] Yong-ming Li; Xiao Min; Shaocheng Tong "Adaptive Fuzzy Inverse Optimal Control for Uncertain Strict-Feedback Nonlinear Systems"IEEE Transactions on Fuzzy Systems, 2019, 28(10): 2363-2374.

[48] Fang Wang and Guanyu Lai"Fixed-time Control Design for Nonlinear Uncertain Systems Via Adaptive Method" Systems & Control Letters, 2020, 140: 104704.

[49] Tong Wang; Ju Wu; Yujia Wang; Min Ma "Adaptive Fuzzy Tracking Control for A Class of Strict-Feedback Nonlinear Systems With Time-Varying Input Delay and Full State Constraints" IEEE Transactions on Fuzzy Systems, 2019, 28(12): 3432-3441.

[50] Humaidi Amjad J., et al. "A new adaptive synergetic control design for single link robot arm actuated by pneumatic muscles." Entropy, 2020, 22(7): 723.

[51] Zhang Chunliang, et al. "Fuzzy adaptive two-bit-triggered control for a class of uncertain nonlinear systems with actuator failures and dead-zone constraint." IEEE Transactions on Cybernetics, 2020, 51(1): 210-221.

[52] Chen Ming, Huanqing Wang and Xiaoping Liu. "Adaptive fuzzy practical fixed-time tracking control of nonlinear systems." IEEE Transactions on Fuzzy Systems, 2019, 29(3): 664-673.

[53] Cui, Guozeng, Jinpeng Yu, and Peng Shi. "Observer-based finite-time adaptive fuzzy control with prescribed performance for nonstrict-feedback nonlinear systems." IEEE Transactions on Fuzzy Systems, 2020, 30(3): 767-778.

[54] Wang Jianhui, et al. "Fuzzy adaptive event-triggered finite-time constraint control for output-feedback uncertain nonlinear systems." Fuzzy Sets and Systems, 2022, 443: 236-257.

[55] Zhao Yanwei, et al. "Adaptive neural decentralised control for switched interconnected nonlinear systems with backlash-like hysteresis and output constraints." International Journal of Systems Science, 2022, 53(7): 1545-1561.

[56] Xiaozheng Jin; Shaoyu Lu and Jiguo Yu "Adaptive NN-Based Consensus for A Class of Nonlinear Multiagent Systems With Actuator Faults and Faulty Networks", IEEE Transactions on Neural Networks and Learning Systems, 2021, 33(8): 3474-3486.

[57] Tang Wenyan, et al. "Consensus of nonlinear multi–agent systems with distributed event–triggered impulsive control." Journal of Vibration and Control, 2022, 28(7-8): 882-891.

[58] Han, Yiyan, Chuandong Li, and Zhigang Zeng. "Asynchronous event-based sampling data for impulsive protocol on consensus of non-linear multi-agent systems." Neural Networks, 2019, 115: 90-99.

[59] Xiaolu Liu; Duxin Chen; Zhiwei Liu; Yan-Wu Wang "Distributed Leaderless Impulsive Consensus of Non-linear Multi-agent Systems with Input Saturation" Nonlinear Analysis: Hybrid Systems, 2020, 36: 100855.

[60] Tiedong Ma; Tiantian Yu; Jiangshuai Huang; Xinsong Yang; Zhenyu Gu; "Adaptive Odd Impulsive Consensus of Multi-agent Systems Via Comparison System Method" Nonlinear Analysis: Hybrid Systems, 2020, 35: 100824.

[61] Le You; Chuandong Li; Yiyan Han "Consensus of Nonlinear Multi-agent Systems with Fuzzy Modelling Uncertainties Via State-constraint Hybrid Impulsive Protocols" International Journal of Machine Learning and Cybernetics, 2020, 11(12): 2653-2664.

[62] Jing Xiao; Xiaoxuan Guo; Yubin Feng; Haibo Bao; Ning Wu; "Leader-Following Consensus of Stochastic Perturbed Multi-Agent Systems Via Variable Impulsive Control and Comparison System Method" IEEE Access, 2020, 8: 113183-113191.

[63] Zhen Li; Wenqing Wang; Yongqing Fan; Hongbo Kang "Impulsive Bipartite Consensus of Second-order Multi-agent Systems Without Relative Velocity Information" Communications in Nonlinear Science and Numerical Simulation, 2020, 80: 104987.

[64] Le You; Chuandong Li; Xiaoyu Zhang; Zhilong He "Edge Event-triggered Control and State-constraint Impulsive Consensus for Nonlinear Multi-agent Systems" AIMS Mathematics, 2020, 5(5): 4151-4167.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202405_10(5).0019

[65] M. Syed Ali; R. Agalya; Zeynep Orman; Sabri Arik "Leader-Following Consensus of Non-linear Multi-agent Systems with Interval Time-Varying Delay Via Impulsive Control" Neural Processing Letters, 2021, 53: 69-83.

[66] Xiang Hu; Zufan Zhang; Chuandong Li "Consensus of Multi-agent Systems with Dynamic Join Characteristics Under Impulsive Control" Frontiers of Information Technology & Electronic Engineering, 2021, 22(1): 120-133.

[67] Duxin Chen; Xiaolu Liu; Wenwu Yu; Lei Zhu; Qipeng Tang "Neural-Network Based Adaptive Self-Triggered Consensus of Nonlinear Multi-Agent Systems With Sensor Saturation" IEEE Transactions on Network Science and Engineering, 2021, 8(2): 1531-1541.