IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 17, 2021, accepted July 5, 2021, date of publication July 9, 2021, date of current version July 22, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3096079

Leader-Following Consensus of Multiple Euler-Lagrange Systems Under Deception Attacks

LIZHANG WANG, CHUNXIA FAN, CONG XIE, AND WEI ZHOU
College of Automation and College of Artificial Intelligence, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
Corresponding author: Chunxia Fan (fancx@njupt.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61873326, and in part by the Key University Science Research Project of Jiangsu Province under Grant KYCX20_0826.

ABSTRACT In this paper, the leader-following consensus problem of a multi-Euler-Lagrange system is studied under deception attacks, where attackers can inject the false data into the data being exchanged over the communication network between two Euler-Lagrange systems. A distributed adaptive filter is proposed to compensate the unknown injection false data, where the magnitude of the false data is estimated. Meanwhile, the performance of the multiple Euler-Lagrange system consensus with the proposed filter can be guaranteed to be similar to that with the traditional controller when the communication network is not injected into false data by a malicious attacker. Furthermore, the consensus criteria of a multiple Euler-Lagrange system and the parameter design scheme of the proposed adaptive filter are achieved by using Lyapunov stability theory. Finally, a numerical example is carried out to demonstrate the effectiveness of the proposed consensus controller for a multi-Euler-Lagrange system attacked by using the false data injection.

INDEX TERMS Euler-Lagrange systems, leader-following consensus, deception attack, distributed filter.

I. INTRODUCTION

In recent years, the cooperative control of distributed network systems has been widely explored in many fields, such as the network robot systems [1], [2], distributed estimation of the wireless sensor network [3], [4], and distributed detection [5]. The cooperative control problems of distributed network systems include synchronization problems, clustering flocking problems, formation control problems, *et al*. In fact, these problems can be considered as the consensus problems, that is, each individual uses limited local information to achieve the same state or output of all individuals. Many consensus control strategies are intensively investigated under various circumstances, for example, adaptive robust control for model uncertainty or system disturbances [6], [7], distributed switching consensus for parameter jump or switching topology [1], [8], adaptive bipartite consensus for cooperation or competition between agents [6], [9], *et al*. However, the realization of the consensus control of the distributed network system depends on the security of information interaction over network communication between the agents. Therefore, it is of great significance to study the consensus problem of distributed network system when the communication channel or manipulation information is attacked, and this problem has also received some substantial research.

Recently, the security of Cyber-Physics systems has attracted much attention, where cyber attacks are concerned [10]–[13]. Generally, the cyber attacks are roughly divided into two categories: 1) the denial-of-service (Dos) attacks [14], [15] and 2) deception attacks [16], [17]. The former can destroy the system performance by preventing the timely transmission of data. The latter can be implemented by the attacker to tamper with the transmission data or inject false data, which make the control center send out wrong instructions such that the stability of the system is destroyed or executes the instructions specified by the malicious attacker. On the other hand, deception attacks are difficult to detect and prevent, so it has attracted extensive attention from many researchers.

False data injection attack has been focused on in the field of smart grid [18], [19] and wireless sensor networks [20], [21]. Next, the distributed consensus problem has been studied for a multi-agent system under deception attacks. Mustafa *et al*. [22] used the Kullback-Leibler (KL) divergence metric in [16] to design two attack detectors in order to detect various deception attacks and make the tracking

The associate editor coordinating the review of this manuscript and approving it for publication was Yilun Shang.

error of a leaderless linear distributed multi-agent system converge to zero. Considering the false data injection attacks with Bernoulli distribution in the sensor-to-controller channel, He *et al.* [17] and Wen *et al.* [23] all used distributed pulse controllers to achieve the bounded mean square consensus of multi-agent systems. Wu *et al.* [24] proposed a distributed algorithm based on event-triggered scheme to achieve the elastic consensus of a multi-agent system under deception attacks, where the damage from the malicious attacker and the consumption of computation and communication were reduced. Huang *et al.* [25] proposed a distributed adaptive filter to compensate the deception attacks from the communication channel in multi-agent systems such that the consensus of the multi-agent system was guaranteed when it was subjected to the malicious attacks and communication quantization. Zuo *et al.* [26] combined the state estimation approach with the threshold scheme to estimate the states of neighbor agents for the multi-agent system under false data injection, which ensured the mean square consensus of multi-agent systems subject to the false data injection attacks. In [22]–[26], the dynamics of agents was described as the linear motion of particles or a nonlinear dynamic satisfying the Lipschitz condition. However, the motion states of agents depend usually on the agent's dynamics. Consequently, the dynamics of agents have to be concerned when consensus of multi-agent systems are studied.

The Euler-Lagrange system is often used to describe the dynamical behavior of various kinds of agents, such as mobile robots, autonomous vehicles and so on. The consensus of multiple Euler-Lagrange systems can be widely applied to various field, such as space rendezvous and docking, satellite attitude adjustment and multiple manipulator coordination and so on. Consequently, there have been many contributions on the consensus of multiple Euler-Lagrange systems. In particular, Lu *et al*. considered the leader-following consensus of multiple Euler-lagrange systems with unknown dynamic leaders under a fixed topology [27]. In order to solve the problem of time-varying communication topology, He *et al*. used an adaptive distributed observer method to synthesize distributed position feedback control law [28]. In the case of actuator failure, an auxiliary controller is designed to compensate for the failure by using adaptive estimation techniques in [29]. In [30] and [2], it is considered that the Euler-lagrange system has heterogeneous, uncertain, and time-varying delays when the data of neighboring individuals are exchanged over communication networks. However, in [2], [27], [28], [29] and [30], it is not concerned that the communication networks are attacked by a malicious attacker. Actually, the Euler-Lagrange systems suffer probably deception attacks when the neighbor Euler-Lagrange system data are exchanged over the communication networks. The contributions on the security of consensus have been rarely reported as far as the authors known for multiple Euler-Lagrange systems.

Compared with faults and disturbance, deception attacks are more intelligent, such as the intermittent and random nature [17], [31]. Therefore, it is usually assumed that the deception attack follows the Bernoulli distribution, its probability and range are known. However, as a defender, it is difficult to obtain the random characteristics and boundaries of stealth attacks. As an attacker, if he wants to destroy the consensus of systems, he will inject the false data into the communication network for a while. Consequently, the consensus performance of multiple Euler-Lagrange systems depends on the estimation of attack signals if the exchanged data are injected false data.

Motivated by the above mention, it is necessary to concern the consensus of multiple Euler-Lagrange systems under deception attacks when both the characteristic and the magnitude of the attack information are unknown. The main contributions of this paper can be highlighted as follow.

1) In this paper, the consensus problem of multiple Euler-Lagrange system is studied and the leader-following consensus protocol is presented, where the leader is concerned as the root node of a graph such that a part of individuals is needed to receive the information from the leader to achieve consensus. As well as known, an Euler-Lagrange system is strongly nonlinear and strongly coupled, which increase the complexity of discussion. In [22]–[26], the agent dynamic is linear or nonlinear but Lipschitz continuous, which is relatively easy. And the results in [22]–[26] are not directly used to the consensus of multiple Euler-Lagrange systems due to the Euler-Lagrange system being strongly nonlinear and strongly coupled.
2) Deception attacks are concerned when the exchange information is transmitted over communication networks in the multiple Euler-Lagrange system. The attack signals are assumed to be unknown and bounded but their boundary being unknown. In order to eliminate the performance degradation caused by the attack signals, an adaptive distributed filter is proposed to estimate the boundary of attack signals. Compared with the attack signals studied in [16], [17] and [21], the statistical characteristic of attack signals is not needed in this paper. In [16], [17] and in [21], the attack signal follows a Gaussian distribution with known probability characteristic or a known frequency characteristic. But for a malicious attacker, the deception signals are usually sent in the form of more kinds of random signals such that the statistical characteristic of attack signals doesn't follow a certain probability.
3) An auxiliary system is designed for each following Euler-Lagrange system in order to track the desired generalized position vector, i.e., the leader's trajectory, which can track sinusoid trajectory or equilibrium point. The state vector of the auxiliary system is transmitted to the neighboring Euler-Lagrange system, that is, the exchanged information between two neighboring Euler-Lagrange system is the state vector of their respective auxiliary system. The consensus scheme is

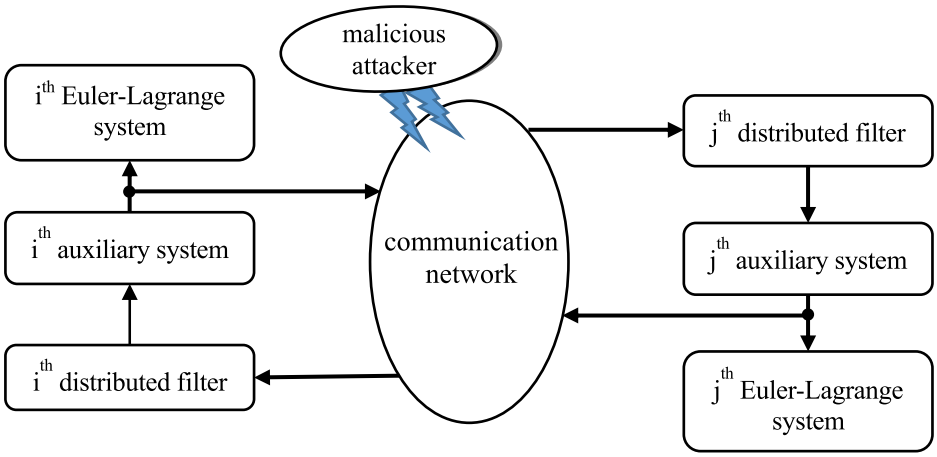

FIGURE 1. Consensus scheme.

shown in Fig. 1, where the communication between i^{th} Euler-Lagrange system and j^{th} system of its neighboring individuals is attacked by a malicious attacker.

The rest of this paper is arranged as follows: introduce some preliminaries and the problem formulation in Section II. A distributed filter is presented and a consensus protocol is achieved in Section III. Some numerical examples are given in Section IV and conclusions are drawn in Section V.

Notations: R^n is the n-dimensional vector space. $||.||$ denote the 2-norm of vectors or matrices. $diag\{\ldots\}$ and $blkdiag\{\ldots\}$ represent diagonal matrix and block diagonal matrix respectively. $\otimes$ means the Kronecker product of a matric. $A > 0$ means that A is a positive matric with an appropriate dimension. $\lambda_{\min}(A)$ is the minimum eigenvalue of A.

II. PRELIMINARIES AND PROBLEM FORMULATION

A. MULTIPLE EULER-LAGRANGE DYNAMICS MODEL

Consider a multi-agent system composed of N Euler-Lagrange systems which can be described as the following

$$M_i(q_i)\ddot{q}_i + C_i(q_i, \dot{q}_i)\dot{q}_i + G_i(q_i) = \tau_i, \quad i = 1, 2, \ldots, N \quad (1)$$

where $q_i, \dot{q}_i, \ddot{q}_i \in R^n$ are the generalized position, velocity and acceleration vectors of ith Euler-Lagrange system respectively. $M_i(q_i) \in R^{n\times n}$ is the symmetric positive-definite inertia matric, $C_i(q_i, \dot{q}_i)\dot{q}_i \in R^n$ is the Coriolis and centripetal forces vector, $G_i(q_i) \in R^n$ is the gravitational vector. $\tau_i \in R^n$ is the control input.

The system (1) has the following properties.

Property 1: The matrix $\dot{M}_i(q_i) - 2C_i(q_i, \dot{q}_i)$ is skew-symmetric.

Property 2: For any $x, y \in R^n$, the system (1) can be linearly parameterized as

$$M_i(q_i)x + C_i(q_i, \dot{q}_i)y + G_i(q_i) = Y_i(q_i, \dot{q}_i, x, y)\theta_i$$

where $Y_i(q_i, \dot{q}_i, x, y) \in R^{n\times m}$ is the regressor matrix and $\theta_i \in R^m$ is an unknown but constant parameter vector.

Assume that the leader's signal is generated by an exosystem whose dynamic is described by the following

$$\dot{q}_0 = Sq_0 \quad (2)$$

where $q_0 \in R^n$ is a generalized position vector of the leader, $S \in R^{n\times n}$ is the constant system matrix of the leader.

B. GRAPH THEORY

The network communication topology between multiple Euler-Lagrange systems is represented by a weighted directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$. Each Euler-Lagrange system is regarded as a node, the set of nodes is $\mathcal{V} = \{i | i = 1, 2, \ldots, N\}$, and the leader is defined as the 0^{th} node. The set of directed edges is $\mathcal{E} = \{(i, j) | i \in \mathcal{V}, j \in \mathcal{V}, i \neq j\}$, where the edge $(j, i) \in \mathcal{E}$ indicates that the i^{th} node can receive information from the j^{th} node. The adjacency matrix is $\mathcal{A} = [a_{ij}] \in R^{N\times N}$, where $a_{ij} > 0$ if and only if $(j, i) \in \mathcal{E}$, otherwise $a_{ij} = 0$. Definition $\mathcal{N}_i = \{j | (j, i) \in \mathcal{E}\}$ represents the neighbor set of the i^{th} node. Define the Laplacian matrix of graph $\mathcal{G}$ as $\mathcal{L} = D - \mathcal{A}$, where the diagonal matrix $D = diag\{d_1, d_2, \ldots, d_N\} \in R^{N\times N}$, $d_i = \sum_{j\in\mathcal{N}_i} a_{ij}$.

The following assumptions are necessary to design the consensus protocol.

Assumption 1: The network communication topology $\mathcal{G}$ consists of a directed spanning tree with the node 0 as its root.

Assumption 2: The real part of all eigenvalues of the leader system matrix S is zero.

Firstly, recall the adaptive consensus controller in [32].

$$\tau_i = -K_i s_i + Y_i(q_i, \dot{q}_i, \dot{q}_{ri}, \ddot{q}_{ri})\hat{\theta}_i \quad (3)$$

$$\dot{\hat{\theta}}_i = -\Lambda_i^{-1} Y_i^T(q_i, \dot{q}_i, \dot{q}_{ri}, \ddot{q}_{ri}) s_i \quad (4)$$

$$\dot{q}_{ri} = S\eta_i - \alpha(q_i - \eta_i) \quad (5)$$

$$\dot{\eta}_i = S\eta_i + \mu \sum_{j\in\mathcal{N}_i} a_{ij}(\eta_j - \eta_i) \quad (6)$$

where $s_i = \dot{q}_i - \dot{q}_{ri}$, $\eta_i \in R^n$, $\eta_0 = q_0$ and $\mu > 0$. K_i is the control gain, Λ_i represents a symmetric positive matrix. $\hat{\theta}_i$ is the adaptive estimation of the system parameters θ_i. η_i

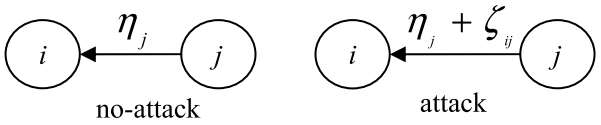

FIGURE 2. Communication signal transmission.

indicates the estimation of the leader's state q_0 of the ith Euler-Lagrange system.

Remark 1: The followers can't synchronize the leader's states if they only obtain the leader's system matrix S because the leader is oscillatory according to Assumption 2. For two autonomous oscillatory systems, the condition of synchronizing them is that both their initial values and their system matrix have to be same. Therefore, a distributed observer (6) must be equipped to estimate the online states of the leader. So, under adaptive parameter control law (3) - (5) and distributed observer (6), the positon and velocity consensus of multiple Euler-Lagrange systems can be realized.

Remark 2: Compared with the general leader-following consensus protocol in [33], the reference torque $\dot{q}_{ri}$ is generated by the leader's speed information and the neighbor's position information, while an auxiliary system (6) is introduced to observe the leader's information in [32]. The exchange information is the state vector of each auxiliary system. There are two advantages of introducing the auxiliary system (6). The multiple Euler-Lagrange system can track an equilibrium point but also a sinusoid trajectory on the one hand; on the other hand, the leader's position and speed information are not needed to be transmitted to the following Euler-Lagrange system, which is in conformity with the principle of bird swarming and the other biological cluster.

C. DECEPTION ATTACK

The states of the distributed observer (6) are transmitted over the communication network in a multiple Euler-Lagrange system such that they are vulnerable to cyber attacks. Here, a deception attack is concerned, as shown in Fig. 2, that is, the exchanged states η_j from Euler-Lagrange system j to system i are injected into the false data ζ_{ij}. Then the ith Euler-Lagrange system receives the information from its neighbor (jth) can be described as

$$\eta_{ij}^{a}(t) = \eta_j(t) + \zeta_{ij}(t) \tag{7}$$

where attack signal $\zeta_{ij}(t)$ is assumed to satisfy $\|\zeta_{ij}(t)\| \leq \bar{\zeta}_{ij}$, where $\bar{\zeta}_{ij}$ is an unknown positive constant.

Remark 3: The attack signal ζ_{ij} in (7) satisfies the bounded limitation $\|\zeta_{ij}(t)\| \leq \bar{\zeta}_{ij}$, it means that the magnitude of the attack signal is limited. Such assumption is reasonable because the system will be equipped with anomaly detectors to check anomalies in the actual network communication process. For malicious attackers, if they want to bypass the detector and not be detected, the magnitude of the attack signal has to be some constraint. On the other hand, considering the limited energy of the injected attack signal, it is reasonable that the attack signal is limited. In [17], the magnitude of the deception attack is assumed to be known. However, attack signals are often stealth and difficult to be discovered, so the magnitude of the attack signal is difficult to be obtained. Consequently, the assumption that the attack signal is bounded and the magnitude is unknown is more consistent with reality.

Remark 4: The attack model (7) may seem to be the introduction of disturbance signals, but there is still a big difference. Generally, a disturbance occurs at the Euler-Lagrange system and doesn't at the communication networks so that this disturbance only acts on the disturbed individual and doesn't on its neighbor. On the other hand, the disturbance in communication networks usually follows certain probability distribution which can be estimated according to the known communication parameter. However, the deception attack signals are often injected into communication networks by a malicious attacker, which is often difficult to be found. So a new estimator is needed to prevent the performance degradation from the deception attack.

Remark 5: The attack signal is only assumed to be bounded and its boundary being unknown in (7), which is different form the attack signal in [16], [17] and [21]. In [16], [17] and [21], the attack signal follows a probability distribution with known statistical characteristic or known frequency, which is difficult to be obtained for a defender. Consequently, the assumption of deception attack signal is more reasonable than those in [16], [17] and [21].

D. PROBLEM FORMULATION

From the above discussion on the multiple Euler-Lagrange systems, considering the communication networks subjected attacks is more realistic and more significant when one studies the leader-following consensus of the multiple Euler-Lagrange system.

The objective of this paper is to design a consensus scheme such that the multiple Euler-Lagrange systems (1) achieve generalized positon and velocity consensus when the communication network are injected false data as the form of (7), that is

$$\lim_{t\to\infty}(q_i - q_0) = 0, \quad \lim_{t\to\infty}(\dot{q}_i - \dot{q}_0) = 0, \quad \forall i \in \mathcal{V}$$

III. MAIN RESULTS

In this section, to achieve the leader-following consensus of multiple Euler-Lagrange systems (1) and leader (2), a distributed observer of the ith Euler-Lagrange system with a filter equipped an adaptive attack compensator is proposed, which is given as follow

$$\dot{\eta}_i(t) = S\eta_i(t) + \hat{g}_i(t) \tag{8}$$

$$\dot{\hat{g}}_i(t) = -\hat{g}_i(t) + \sum_{j\in\mathcal{N}_i} a_{ij}(\eta_{ij}^{a}(t) - \eta_i(t)) + v_i(t) \tag{9}$$

where η_i, $\hat{g}_i$ denote the states of the consensus observer (8) and filter (9) of the ith Euler-Lagrange system respectively, $v_i(t) = \sum_{j\in\mathcal{N}_i} a_{ij}v_{ij}(t)$ is a novel adaptive attack compensator, which is used to adaptively offset the impact of attack,

designed as

$$v_{ij}(t) = -\frac{P_i^T \hat{g}_i(t)\hat{\zeta}_{ij}(t)}{||\hat{g}_i^T(t)P_i|| + \sigma_{ij}(t)} \tag{10}$$

where $\hat{\zeta}_{ij}(t)$ is an estimation of the upper bound of the attack, and it is given in the following form

$$\dot{\hat{\zeta}}_{ij}(t) = -\kappa\sigma_{ij}(t)\hat{\zeta}_{ij}(t) + \kappa||\hat{g}_i^T(t)P_i|| \tag{11}$$

where $\kappa > 0, P = blkdiag\{P_1, P_2, \ldots, P_N\}, P_i \in R^{n\times n}$ is a positive matrix to be determined later. $\sigma_{ij}(t)$ is any positive definite continuous and bounded function, satisfying

$$\lim_{t\to\infty}\int_{t_0}^{t}\sigma_{ij}(\tau)d\tau \le \bar{\sigma}_{ij} \le \infty, \quad i = 1, 2, \ldots, N,\ j \in \mathcal{N}_i \tag{12}$$

where the function $\sigma_{ij}(t)$ can be chosen as an exponential decay function $\beta e^{-\gamma t}$ ($\beta > 0$, $\gamma > 0$), which implies $\lim_{t\to\infty}\beta e^{-\gamma t} = 0$.

Remark 6: The distributed filter (9) - (11) can directly and adaptively compensate for the attack, which is simpler and more convenient. And the multiple Euler-Lagrange systems can be guaranteed to be consensus and stability regardless of whether the attack is injected or not. It does not need to be equipped with an additional attack detector to detect attacks as in [10], [20]. In [24], an event-triggered mechanism is introduced to reduce the impact of malicious attack. But if the malicious attack occurs when the event generator is not triggered, the agent will receive the deception signals such that the consensus performance may be reduced.

Let consensus observer error be $\tilde{\eta}_i = \eta_i - \eta_0$, where $\eta_0 = q_0$. According to (2) and (8), one can obtain

$$\dot{\tilde{\eta}}_i = S\tilde{\eta}_i + \hat{g}_i. \tag{13}$$

Defining $\tilde{\eta} = [\tilde{\eta}_1^T, \tilde{\eta}_2^T, \ldots, \tilde{\eta}_N^T]^T$, $\hat{g} = [\hat{g}_1^T, \hat{g}_2^T, \ldots, \hat{g}_N^T]^T$, $v = [v_1^T, v_2^T, \ldots, v_N^T]^T$, $\zeta = [\zeta_1^T, \zeta_2^T, \ldots, \zeta_N^T]^T$. Then (13) and (9) can be rewritten in the vector forms as follows

$$\dot{\tilde{\eta}} = (I_N \otimes S)\tilde{\eta} + \hat{g} \tag{14}$$

$$\dot{\hat{g}} = -\hat{g} + (-\mathcal{H} \otimes I_n)\tilde{\eta} + v + \zeta \tag{15}$$

where $\mathcal{H} = \mathcal{L} + diag(a_{10}, a_{20}, \ldots, a_{N0})$, $\zeta_i = \sum_{j\in\mathcal{N}_i} a_{ij}\zeta_{ij}$.

Let the attack's upper bound estimation error be $\tilde{\zeta}_{ij} = \bar{\zeta}_{ij} - \hat{\zeta}_{ij}$, and the dynamic is

$$\dot{\tilde{\zeta}}_{ij} = -\kappa\sigma_{ij}(t)\tilde{\zeta}_{ij} + \kappa||\hat{g}_i^T P_i|| + \kappa\sigma_{ij}(t)\bar{\zeta}_{ij} \tag{16}$$

The main result is described in the following theorem.

Theorem 1: Suppose that Assumptions 1 and 2 hold. If there exists symmetric matrics $P > 0$ and $Q > 0$ to make the following LMI holds:

$$\begin{bmatrix} \left((I_N \otimes S)^T Q + Q(I_N \otimes S)\right) & Q & (\mathcal{H} \otimes I_n)^T P \\ * & -\frac{1}{a_1}I & 0 \\ * & * & -a_2 I \end{bmatrix} < 0$$

$$\frac{1}{2a_1}I + \frac{a_2}{2}I - P < 0 \tag{17}$$

where $a_1 > 0, a_2 > 0$. Thus, the generalized position and velocity consensus of the multiple Euler-Lagrange system (1) with leader (2) are achieved by using the adaptive parameter control laws (3) - (5) and distributed observer (8) - (11) when deception attack (7) occurred over the communication channel.

Proof: Consider the following Lyapunov function for (14) – (16)

$$V_1(t) = \frac{1}{2}\tilde{\eta}^T Q\tilde{\eta} + \frac{1}{2}\hat{g}^T P\hat{g} + \frac{1}{2\kappa}\sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\tilde{\zeta}_{ij}^2 \tag{18}$$

Taking the derivative of (18), one can obtain

$$\begin{aligned}
&\dot{V}_1(t) \\
&= \frac{1}{2}\dot{\tilde{\eta}}^T Q\tilde{\eta} + \frac{1}{2}\tilde{\eta}^T Q\dot{\tilde{\eta}} + \dot{\hat{g}}^T P\hat{g} + \frac{1}{\kappa}\sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\tilde{\zeta}_{ij}\dot{\tilde{\zeta}}_{ij} \\
&= \frac{1}{2}\left((I_N \otimes S)\tilde{\eta} + \hat{g}\right)^{\mathrm{T}} Q\tilde{\eta} + \frac{1}{2}\tilde{\eta}^T Q\left((I_N \otimes S)\tilde{\eta} + \hat{g}\right) \\
&\quad + \left(-\hat{g} + (-\mathcal{H} \otimes I_n)\tilde{\eta} + v + \zeta\right)^{\mathrm{T}} P\hat{g} + \frac{1}{\kappa}\sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\tilde{\zeta}_{ij}\dot{\tilde{\zeta}}_{ij} \\
&= \frac{1}{2}\dot{\tilde{\eta}}^T\left((I_N \otimes S)^T Q + Q(I_N \otimes S)\right)\tilde{\eta} + \hat{g}^T Q\tilde{\eta} - \hat{g}^T P\hat{g} \\
&\quad - \tilde{\eta}^T(\mathcal{H} \otimes I_n)^T P\hat{g} + \hat{g}^T Pv + \hat{g}^T P\zeta + \frac{1}{\kappa}\sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\tilde{\zeta}_{ij}\dot{\tilde{\zeta}}_{ij}
\end{aligned}$$

According to the following inequality

$$2\alpha^{\mathrm{T}}\beta \le \frac{1}{\eta_{\alpha\beta}}\alpha^{\mathrm{T}}\alpha + \eta_{\alpha\beta}\beta^T\beta \quad \forall\eta_{\alpha\beta} > 0,$$

the second term and the fourth term in time derivative of $V_1(t)$ can be transformed into the following

$$\begin{aligned}
\hat{g}^T Q\tilde{\eta} \le{}& \frac{1}{2a_1}\hat{g}^T\hat{g} + \frac{a_1}{2}\tilde{\eta}^T QQ\tilde{\eta} \\
&- \tilde{\eta}^T(\mathcal{H} \otimes I_n)^T P\hat{g} \le \frac{1}{2a_2}\tilde{\eta}^T(\mathcal{H} \otimes I_n)^T \\
&\times PP(\mathcal{H} \otimes I_n)\tilde{\eta} + \frac{a_2}{2}\hat{g}^T\hat{g}
\end{aligned}$$

thus, the time derivative of $V_1(t)$ can be written as follow

$$\begin{aligned}
\dot{V}_1(t) \le{}& \frac{1}{2}\tilde{\eta}^T\Big[(I_N \otimes S)^T Q + Q(I_N \otimes S) + a_1 QQ \\
&+ \frac{1}{a_2}(\mathcal{H} \otimes I_n)^T PP(\mathcal{H} \otimes I_n)\Big]\tilde{\eta} \\
&+ \hat{g}^T\left(\frac{1}{2a_1}I + \frac{a_2}{2}I - P\right)\hat{g} + \hat{g}^T Pv + \hat{g}^T P\zeta \\
&+ \frac{1}{\kappa}\sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\tilde{\zeta}\dot{\tilde{\zeta}} \\
\le{}& -\lambda_{\min}(Q_{\tilde{\eta}})||\tilde{\eta}||^2 - \lambda_{\min}(Q_{\hat{g}})||\hat{g}||^2 + \hat{g}^T Pv + \hat{g}^T P\zeta \\
&+ \frac{1}{\kappa}\sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\tilde{\zeta}\dot{\tilde{\zeta}}
\end{aligned}$$

where

$$Q_{\tilde{\eta}} = -\Big[(I_N \otimes S)^T Q + Q(I_N \otimes S) + a_1 QQ + \frac{1}{a_2}(\mathcal{H} \otimes I_n)^T PP(\mathcal{H} \otimes I_n)\Big]$$
$$Q_{\hat{g}} = -\left(\frac{1}{2a_1} I + \frac{a_2}{2} I - P\right)$$

According to the fact of attack signal satisfying $|\zeta_{ij}(t)| \leq \bar{\zeta}_{ij}$, from (10) and (11), one has the following

$$\begin{aligned}
&\hat{g}^T P v + \hat{g}^T P \zeta + \frac{1}{\kappa}\sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\tilde{\zeta}_{ij}\dot{\tilde{\zeta}}_{ij} \\
&\leq \sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\hat{g}_i^T(t)P_i v_{ij}(t) + \sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}||\hat{g}_i^T(t)P_i||\bar{\zeta}_{ij} \\
&\quad - \frac{1}{\kappa}\sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\tilde{\zeta}_{ij}\dot{\hat{\zeta}}_{ij} \\
&\leq \sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\hat{g}_i^T(t)P_i\left(-\frac{P_i^T\hat{g}_i(t)\hat{\zeta}_{ij}(t)}{||\hat{g}_i^T(t)P_i|| + \sigma_{ij}(t)}\right) \\
&\quad + \sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}||\hat{g}_i^T(t)P_i||\bar{\zeta}_{ij} \\
&\quad - \frac{1}{\kappa}\sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\left(\bar{\zeta}_{ij} - \hat{\zeta}_{ij}\right)\left(-\kappa\sigma_{ij}(t)\hat{\zeta}_{ij}(t) + \kappa||\hat{g}_i^T(t)P_i||\right) \\
&\leq \sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\left(-\frac{||\hat{g}_i^T(t)P_i||^2\hat{\zeta}_{ij}(t)}{||\hat{g}_i^T(t)P_i|| + \sigma_{ij}(t)}\right) \\
&\quad + \sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\sigma_{ij}(t)\bar{\zeta}_{ij}\hat{\zeta}_{ij}(t) \\
&\quad - \sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\sigma_{ij}(t)\hat{\zeta}_{ij}^2(t) + \sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}||\hat{g}_i^T(t)P_i||\hat{\zeta}_{ij} \\
&\leq \sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\left(\frac{||\hat{g}_i^T(t)P_i||\sigma_{ij}(t)\hat{\zeta}_{ij}(t)}{||\hat{g}_i^T(t)P_i|| + \sigma_{ij}(t)}\right) \\
&\quad + \sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\sigma_{ij}(t)\bar{\zeta}_{ij}\hat{\zeta}_{ij}(t) - \sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\sigma_{ij}(t)\hat{\zeta}_{ij}^2(t)
\end{aligned}$$

According to the following inequality

$$\frac{\alpha\beta}{\alpha+\beta} \leq \alpha \quad \forall\alpha > 0, \quad \beta > 0$$

one can obtain the following

$$\begin{aligned}
&\hat{g}^T P v + \hat{g}^T P \zeta + \frac{1}{\kappa}\sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\tilde{\zeta}_{ij}\dot{\tilde{\zeta}}_{ij} \\
&\quad \leq \sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\sigma_{ij}(t)\hat{\zeta}_{ij}(t) + \sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\sigma_{ij}(t)\bar{\zeta}_{ij}\hat{\zeta}_{ij}(t) \\
&\quad - \sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\sigma_{ij}(t)\hat{\zeta}_{ij}^2(t) \leq \sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\sigma_{ij}(t) \\
&\quad \times \left(-\left(\hat{\zeta}_{ij}(t) - \frac{1}{2}\left(\bar{\zeta}_{ij}+1\right)\right)^2 + \frac{1}{4}\left(\bar{\zeta}_{ij}+1\right)^2\right) \\
&\quad \leq \frac{1}{4}\sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\sigma_{ij}(t)\left(\bar{\zeta}_{ij}+1\right)^2
\end{aligned}$$

Consequently, the following is true

$$\begin{aligned}
\dot{V}_1(t) &\leq -\lambda_{\min}(Q_{\tilde{\eta}})||\tilde{\eta}||^2 - \lambda_{\min}(Q_{\hat{g}})||\hat{g}||^2 \\
&\quad + \frac{1}{4}\sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\sigma_{ij}(t)\left(\bar{\zeta}_{ij}+1\right)^2 \\
&\leq -\lambda_{\min}(Q_{\tilde{\eta}\hat{g}})||\tilde{\varphi}||^2 + \frac{1}{4}\sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\sigma_{ij}(t)\left(\bar{\zeta}_{ij}+1\right)^2
\end{aligned} \tag{19}$$

where $\tilde{\varphi} = [||\tilde{\eta}|| \ \ ||\hat{g}||]^{\mathrm{T}}$, $Q_{\tilde{\eta}\hat{g}} = diag\{\lambda_{\min}(Q_{\tilde{\eta}}), \lambda_{\min}(Q_{\hat{g}})\}$.

Let $\widehat{\varphi} = [\tilde{\eta}^T \tilde{\varphi}^T \tilde{\zeta}^T]^{\mathrm{T}}$, it follows from (18) and there exists a constant $\varsigma > 0$ such that

$$0 \leq \varsigma||\widehat{\varphi}|| \leq V_1(\widehat{\varphi}) \tag{20}$$

integrating (19) over $[t_0, t]$ yields

$$\begin{aligned}
V_1(\widehat{\varphi}(t)) - V_1(\widehat{\varphi}(t_0)) &\leq -\int_{t_0}^{t}\lambda_{\min}(Q_{\tilde{\eta}\hat{g}})||\tilde{\varphi}||^2 d\tau \\
&\quad + \frac{1}{4}\int_{t_0}^{t}\sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\sigma_{ij}(\tau)\left(\bar{\zeta}_{ij}+1\right)^2 d\tau
\end{aligned} \tag{21}$$

From (12), it is known that

$$\begin{aligned}
&\lim_{t\to\infty}\frac{1}{4}\int_{t_0}^{t}\sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\sigma_{ij}(\tau)\left(\bar{\zeta}_{ij}+1\right)^2 d\tau \\
&\qquad \leq \frac{1}{4}\sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\bar{\sigma}_{ij}\left(\bar{\zeta}_{ij}+1\right)^2
\end{aligned}$$

let $\bar{\sigma} = \frac{1}{4}\sum_{i=1}^{N}\sum_{j\in\mathcal{N}_i} a_{ij}\bar{\sigma}_{ij}\left(\bar{\zeta}_{ij}+1\right)^2$, (21) can be rewritten as

$$V_1(\widehat{\varphi}(t)) \leq V_1(\widehat{\varphi}(t_0)) + \bar{\sigma} \tag{22}$$

From (20) and (22), it is clear that

$$\varsigma||\widehat{\varphi}|| \leq V_1(\widehat{\varphi}(t_0)) + \bar{\sigma} \tag{23}$$

which implies that $\widehat{\varphi}$ is uniformly bounded. Moreover, by (21) and $V_1(\widehat{\varphi}(t)) \geq 0$, one has

$$\lim_{t\to\infty}\int_{t_0}^{t}\lambda_{\min}(Q_{\tilde{\eta}\hat{g}})||\tilde{\varphi}||^2 d\tau \leq V_1(\widehat{\varphi}(t_0)) + \bar{\sigma}$$

Then, according to the Barbalat't lemma [31], it is obvious that

$$\lim_{t\to\infty}\lambda_{\min}(Q_{\tilde{\eta}\hat{g}})||\tilde{\varphi}||^2 = 0$$

which implies $\lim_{t\to\infty}||\tilde{\varphi}|| = 0$. So, one has the following

$$\lim_{t\to\infty}||\tilde{\eta}|| = 0, \quad \lim_{t\to\infty}||\hat{g}|| = 0 \tag{24}$$

Thus, the adaptive attack compensator (10) with the attack upper bound estimator (11) can be used to eliminate the deception attack by the distributed filter (9), and the distributed observer (8) can be used accurately estimate the state of the leader.

Let the parameter estimate error be $\tilde{\theta}_i = \hat{\theta}_i - \theta_i$. From (1), (3) and (4), the dynamics of s_i and $\tilde{\theta}_i$ can be written as

$$\dot{s}_i = M_i^{-1}(q_i)[Y_i(q_i, \dot{q}_i, \dot{q}_{ri}, \ddot{q}_{ri})\tilde{\theta}_i - C_i(q_i, \dot{q}_i)s_i - K_i s_i] \tag{25}$$

$$\dot{\tilde{\theta}}_i = -\Lambda_i^{-1}Y_i(q_i, \dot{q}_i, \dot{q}_{ri}, \ddot{q}_{ri})s_i \tag{26}$$

Choose the Lyapunov function candidate as follow

$$V_2(t) = \frac{1}{2}\sum_{i=1}^{N} s_i^T M_i(q_i)s_i + \tilde{\theta}_i^T\Lambda_i^{-1}\tilde{\theta}_i \tag{27}$$

its derivative follows

$$\dot{V}_2(t) = -\sum_{i=1}^{N} s_i^T K_i s_i \tag{28}$$

From (28), one has $\dot{V}_2(t) \le 0$, which implies that $\tilde{\theta}_i$ and s_i are bounded. By (5), one has

$$\dot{q}_i = -\alpha q_i + s_i + S\eta_i - \alpha\eta_i \tag{29}$$

since s_i and η_i are bounded, (29) can be viewed as a stable linear system with a bounded input $s_i + S\eta_i - \alpha\eta_i$. Therefore, both q_i and $\dot{q}_i$ must be bounded. Then by (5), $\dot{q}_{ri}$ is bounded. The derivative of $\dot{q}_{ri}$ is $\ddot{q}_{ri} = S\dot{\eta}_i - \alpha(\dot{q}_i - \dot{\eta}_i)$, so $\ddot{q}_{ri}$ and $Y_i(q_i, \dot{q}_i, \dot{q}_{ri}, \ddot{q}_{ri})$ are bounded. Since $M_i(q_i)$ is positive definite, $M_i^{-1}(q_i)$ exists and is bounded. From (25), $\dot{s}_i$ is bounded. Since $\ddot{V}_2(t) = -2\sum_{i=1}^{N} s_i^T K_i \dot{s}_i$, where s_i and $\dot{s}_i$ are bounded, we can have $\ddot{V}_2(t)$ is bounded. Then, according to the Barbalat's lemma [34], it is obvious that $\lim_{t\to\infty}\dot{V}_2(t) = 0$ and then $\lim_{t\to\infty} s_i = 0$. Next, from (13), (24) and (29), one has the following

$$\dot{q}_i - \dot{\eta}_i + \alpha(q_i - \eta_i) = s_i \tag{30}$$

since (30) can be viewed as a stable first order differential equation in $(q_i - \eta_i)$ with s_i as the bounded input and tends to zero, one concludes that both $(q_i - \eta_i)$ and $(\dot{q}_i - \dot{\eta}_i)$ are bounded and $\lim_{t\to\infty}(q_i - \eta_i) = 0$, $\lim_{t\to\infty}(\dot{q}_i - \dot{\eta}_i) = 0$. Therefore, by the following identities

$$q_i - q_0 = (q_i - \eta_i) + (\eta_i - q_o)$$
$$\dot{q}_i - \dot{q}_0 = (\dot{q}_i - \dot{\eta}_i) + (\dot{\eta}_i - \dot{q}_o)$$

one has $\lim_{t\to\infty}(q_i - q_0) = 0$ and $\lim_{t\to\infty}(\dot{q}_i - \dot{q}_0) = 0$. The proof is completed.

Remark 7: Theorem 1 introduces deception attack on the basis of reference [32], and discusses the security consensus problem when the observer (6) is attacked by unknown injection data. But the difference from the reference [32] is that the theorem mainly focuses on solving the unknown injection data attack in the communication process, ignoring the time-varying topology, and assuming that all individuals can obtain the leader's system matrix S.

Theorem 1 solves the secure consensus of problem under deception attack with unknown boundary when the directed topology is fixed. If it is assumed that the upper bound of the deception attack signal is known, the following Corollary 1 gives the design method for the security consensus problem of the multiple Euler-Lagrange system.

Assumption 3: The upper bound of the attack signal is known as $\bar{\zeta}_{ij}(t)$.

For the known magnitude of attack signal, one can design the following adaptive attack compensator

$$v_{ij}(t) = -\frac{P_i^T\hat{g}_i(t)\bar{\zeta}_{ij}(t)}{||\hat{g}_i^T(t)P_i|| + \sigma_{ij}(t)} \tag{31}$$

where $\bar{\zeta}_{ij}(t)$ is the upper bound of the attack signal form j$^{\text{th}}$ Euler-Lagrange system to i$^{\text{th}}$ one.

Remark 8: In adaptive attack compensator (10), the magnitude of attack signal is unknown which is more realistic because an attacker is usually secrete and is not easily detected. But there exists some special case such that the magnitude of attack signal is known, for example, attacker is detected. Therefore, the adaptive attack compensator (10) can be rewritten as (31).

Corollary 1: Suppose that Assumptions 1, 2 and 3 hold. If there exists symmetric matrics $P > 0$ and $Q > 0$ to make the following LMI holds:

$$\begin{bmatrix} ((I_N \otimes S)^T Q + Q(I_N \otimes S)) & Q & (\mathcal{H} \otimes I_n)^T P \\ * & -\frac{1}{a_1}I & 0 \\ * & * & -a_2 I \end{bmatrix} < 0$$
$$\frac{1}{2a_1}I + \frac{a_2}{2}I - P < 0 \tag{32}$$

where $a_1 > 0, a_2 > 0$. Thus, the generalized position and velocity consensus of the multiple Euler-Lagrange system (1) with leader (2) are achieved by using the adaptive parameter control laws (3) - (5) and distributed observer (8) - (9) and (31) when deception attack (7) occurred over the communication channel.

Proof: The proof process is the same as Theorem 1.

IV. SIMULATION

In this simulation, we consider a teleoperation system which composed of four agents, the dynamic can be written as Euler-Lagrange equation form [35].

$$M_i(q_i)\ddot{q}_i + C_i(q_i, \dot{q}_i)\dot{q}_i + G_i(q_i) = \tau_i, \quad i = 1, 2, 3, 4$$

where $q_i = col(q_{ix}, q_{iy})$, and

$$M_i(q_i) = \begin{bmatrix} a_{i1} + a_{i2} + 2a_{i3}\cos q_{iy} & a_{i2} + a_{i3}\cos q_{iy} \\ a_{i2} + a_{i3}\cos q_{iy} & a_{i2} \end{bmatrix}$$
$$C_i(q_i, \dot{q}_i) = \begin{bmatrix} -a_{i3}\dot{q}_{iy}\sin q_{iy} & -a_{i3}(\dot{q}_{ix} + \dot{q}_{iy})\sin q_{iy} \\ a_{i3}\dot{q}_{ix}\sin q_{iy} & 0 \end{bmatrix}$$

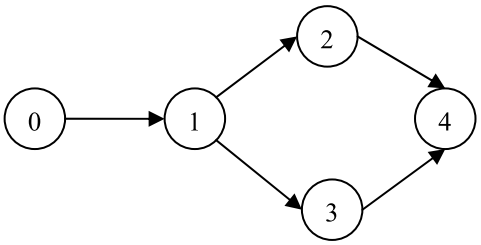

FIGURE 3. Network communication topology.

$$G_i(q_i) = \begin{bmatrix} a_{i4}g\cos q_{ix} + a_{i5}g\cos(q_{ix}+q_{iy}) \\ a_{i5}g\cos(q_{ix}+q_{iy}) \end{bmatrix}$$

with $g = 9.801m/s^2$, $\theta_i = col(a_{i1}, a_{i2}, a_{i3}, a_{i4}, a_{i5})$. The actual values of θ_i are given as

$$\begin{aligned}\theta_1 &= col(0.64, 1.10, 0.08, 0.64, 0.32)\\ \theta_2 &= col(0.76, 1.17, 0.14, 0.93, 0.44)\\ \theta_3 &= col(0.91, 1.26, 0.22, 1.27, 0.58)\\ \theta_4 &= col(1.10, 1.36, 0.32, 1.67, 0.73)\end{aligned}$$

respectively. Let the initial position of the four followers be given by $[10, 2]^T, [1, -6]^T, [8, -2]^T, [-3, 7]^T$, the initial velocities of the four followers be chosen as $[0, 4]^T, [5, -3]^T, [-3, 1]^T, [-2, 7]^T$.

The network communication topology $\mathcal{G}$ of a leader and four followers is shown in Fig. 3, where the graph contains a spanning tree with the node 0 as the root. The system matric of the leader is $S = [0, 1; -1, 0]$, its initial position and velocity be given by $[20, 0]^T$, $[0, -20]^T$ respectively. Next, In order to verify the effectiveness of the proposed new distributed observer in eliminating deception attacks, it is assumed that the following attacks

$$\begin{aligned}\zeta_{10} &= [7, 7]^T, \quad \zeta_{21} = [4, 4]^T \sin(5t)\\ \zeta_{31} &= [6, 6]^T \cos(2t) + [5, 5]^T\\ \zeta_{42} &= [5, 5]^T \cos(3t), \quad \zeta_{43} = [2.5, 2.5]^T\end{aligned}$$

where the attacks occur in $[30, 50]\,s$. The decay function σ_{ij} is chosen as $5e^{-0.05t}$ and the parameter of (11) is chosen as $\kappa = 10$.

Firstly, to verify the impact of Euler-Lagrange systems on consensus performance for the case subjected to the deception stacks. Under the control laws (3) - (5), the original consensus observer (6) injected false data attacks. In this case, the position error $(q_i - q_0)$ and velocity error $(\dot{q}_i - \dot{q}_0)$ of the multiple Euler-Lagrange system are shown in Fig. 4, the states of the observer (6) and the leader (2) are shown in Fig. 5. It can be seen from the figure that the consensus observer (6) cannot accurately estimate the online state of leader when the attack occurs, thus four followers cannot effectively track the leader.

Secondly, by introducing an adaptive compensator (10) with an attack upper bound estimator (11), and use a new distributed filter (9) to filter out the attacks, the position error $(q_i - q_0)$ and velocity error $(\dot{q}_i - \dot{q}_0)$ of the multiple

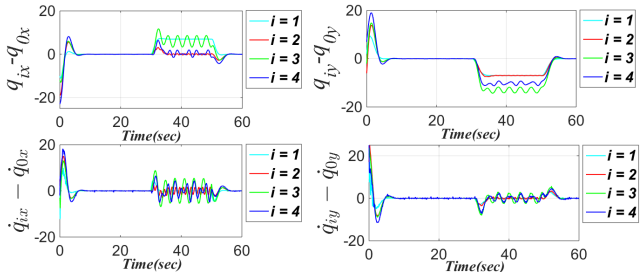

FIGURE 4. The position error $(q_i - q_0)$ and velocity error $(\dot{q}_i - \dot{q}_0)$ under the observer (6).

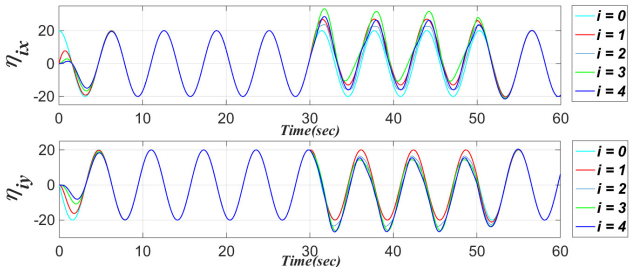

FIGURE 5. The state of the observer η_i under the observer (6).

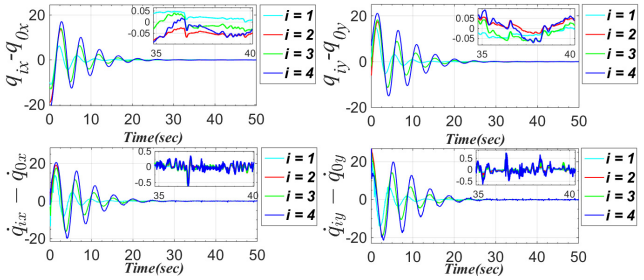

FIGURE 6. The position error $(q_i - q_0)$ and velocity error $(\dot{q}_i - \dot{q}_0)$ under the observer (8).

Euler-Lagrange system are shown in Fig. 6, the state of the observer (8) and the leader (2) are shown in Fig. 7. Thus, under deception attack (7), by using the adaptive parameter control laws (3) - (5) and distributed observer (8) - (11), the multiple Euler-Lagrange systems (1) can achieve generalized positon and velocity consensus with the leader (2). Meanwhile, as shown in Fig. 8, the attack upper bound estimator (11) is estimated to be close to zero for the un-attack situation before 30s. After 30s, the deception attack occurs, the attack upper bound estimator (11) adaptively compensates for the impact of the attack. Therefore, for the un-attack situation in the time $[0, 30]\,s$, the designed distributed filter can ensure that the tracking performance of the multi-Euler-Lagrange system is close to the traditional distributed controller.

Finally, when the upper bound of the attack is known, that is, Assumption 3 holds, under the control of distributed observers (8) - (9) and (31), the Euler-lagrange system (1) can also effectively track the leader (2). According to the

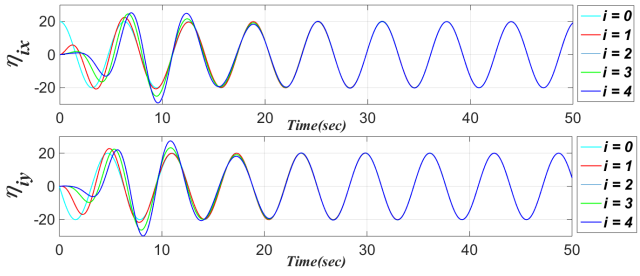

FIGURE 7. The state of the observer η_i under the observer (8).

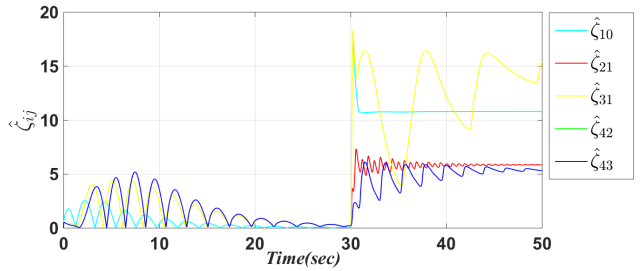

FIGURE 8. The state of the attack upper bound estimator $\hat{\zeta}_{ij}$ (11).

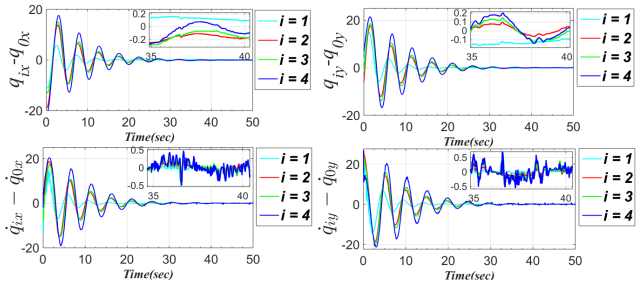

FIGURE 9. The position error ($q_i - q_0$) and velocity error ($\dot{q}_i - \dot{q}_0$) under the observer (8) with adaptive attack compensator (31).

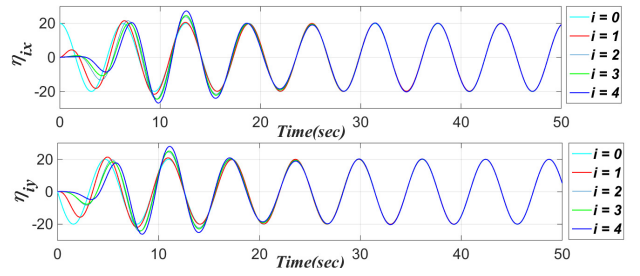

FIGURE 10. The state of the observer η_i under the observer (8) with adaptive attack compensator (31).

observation of Fig. 9 and Fig. 10, compared with Fig. 6 and Fig. 7, the tracking effect is roughly the same as the unknown deception attack, but it is still slightly worse after careful observation. This further verifies the effectiveness of the adaptive upper bound estimator (10). The adaptive upper bound estimator (10) can adaptively generate a compensation signal of a corresponding size with the change of the attack signal in real time, with better compensation effect and better tracking performance.

V. CONCLUSION

The consensus problem of multiple Euler-Lagrange systems with a moving leader under deception attacks in communication network are mainly addressed. We have proposed a novel consensus observer which equipped with an adaptive filter to eliminate the impact of deception attacks. By using Lyapunov stability theory and linear matrix inequality technology, the stability conditions of consensus control and the parameter design of adaptive attack compensator are given. Finally, a simulation example is given to verify the effectiveness of the proposed method. In the future, we will further study the leaderless consensus control of multiple Euler-Lagrange systems under deception attacks.

REFERENCES

[1] L. Liu, B. Li, and R. Guo, "Consensus control for networked manipulators with switched parameters and topologies," *IEEE Access*, vol. 9, pp. 9209–9217, 2021.
[2] A. Abdessameud, I. G. Polushin, and A. Tayebi, "Synchronization of lagrangian systems with irregular communication delays," *IEEE Trans. Autom. Control*, vol. 59, no. 1, pp. 187–193, Jan. 2014.
[3] C. Guyeux, M. Haddad, M. Hakem, and M. Lagacherie, "Efficient distributed average consensus in wireless sensor networks," *Comput. Commun.*, vol. 150, pp. 115–121, Jan. 2020.
[4] Y. L. Jin, X. S. Zhang, and B. Yao, "Distributed synchronization in large-scale wireless sensor networks using group consensus protocol," *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 11, 2017, Art. no. 1550147717718114.
[5] K. Li, Q. Liu, S. Yang, J. Cao, and G. Lu, "Cooperative optimization of dual multiagent system for optimal resource allocation," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 50, no. 11, pp. 4676–4687, Nov. 2020.
[6] H. Xu, C. Liu, Y. Lv, and J. Zhou, "Adaptive bipartite consensus of second-order multi-agent systems with bounded disturbances," *IEEE Access*, vol. 8, pp. 186441–186447, 2020.
[7] Q. Qu, L. Sun, and Z. Li, "Adaptive critic design-based robust cooperative tracking control for nonlinear multi-agent systems with disturbances," *IEEE Access*, vol. 9, pp. 34383–34394, 2021.
[8] K. Li, C.-C. Hua, X. You, and X.-P. Guan, "Distributed consensus control for nonlinear multiagent systems under directed graphs of dynamic frequency switches," *IEEE Trans. Autom. Control*, vol. 66, no. 2, pp. 841–848, Feb. 2021.
[9] H. Zhao, L. Peng, and H. Yu, "Data driven distributed bipartite consensus tracking for nonlinear multiagent systems via iterative learning control," *IEEE Access*, vol. 8, pp. 144718–144729, 2020.
[10] X. Huang and J. Dong, "Reliable control policy of cyber-physical systems against a class of frequency-constrained sensor and actuator attacks," *IEEE Trans. Cybern.*, vol. 48, no. 12, pp. 3432–3439, Dec. 2018.
[11] Q. Su, Z. Fan, Y. Long, and J. Li, "Attack detection and secure state estimation for cyber-physical systems with finite-frequency observers," *J. Franklin Inst.*, vol. 357, no. 17, pp. 12724–12741, Nov. 2020.
[12] H. Zhang, C. Peng, H. Sun, and D. Du, "Adaptive state estimation for cyber physical systems under sparse attacks," *Trans. Inst. Meas. Control*, vol. 41, no. 6, pp. 1571–1579, Apr. 2019.
[13] Y. Yuan and Y. Mo, "Security for cyber-physical systems: Secure control against known-plaintext attack," *Sci. China Technol. Sci.*, vol. 63, no. 9, pp. 1637–1646, Sep. 2020.
[14] S. Lai, B. Chen, T. Li, and L. Yu, "Packet-based state feedback control under DoS attacks in cyber-physical systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 66, no. 8, pp. 1421–1425, Aug. 2019.
[15] H. Zhao, Y. Niu, and J. Zhao, "Event-triggered sliding mode control of uncertain switched systems under denial-of-service attacks," *J. Franklin Inst.*, vol. 356, no. 18, pp. 11414–11433, Dec. 2019.
[16] Y.-G. Li and G.-H. Yang, "Optimal stealthy false data injection attacks in cyber-physical systems," *Inf. Sci.*, vol. 481, pp. 474–490, May 2019.

[17] W. He, X. Gao, W. Zhong, and F. Qian, "Secure impulsive synchronization control of multi-agent systems under deception attacks," *Inf. Sci.*, vol. 459, pp. 354–368, 2018.
[18] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 9, no. 5, pp. 142–154, 2011.
[19] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, Apr. 2017.
[20] Y. Guan and X. Ge, "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks," *IEEE Trans. Signal Inf. Process. Over Netw.*, vol. 4, no. 1, pp. 48–59, Mar. 2018.
[21] L. Lei, W. Yang, C. Yang, and H. B. Shi, "False data injection attack on consensus-based distributed estimation," *Int. J. Robust Nonlinear Control*, vol. 27, no. 9, pp. 1419–1432, Jun. 2017.
[22] A. Mustafa, H. Modares, and R. Moghadam, "Resilient synchronization of distributed multi-agent systems under attacks," *Automatica*, vol. 3, no. 5, pp. 1–14, 2020.
[23] G. G. Wen, X. Q. Zhai, Z. X. Peng, and A. Rahmani, "Fault-tolerant secure consensus tracking of delayed nonlinear multi-agent systems with deception attacks and uncertain parameters via impulsive control," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 82, pp. 105043–105078, Mar. 2020.
[24] Y. M. Wu, M. Xu, N. Zheng, and X. X. He, "Event-triggered resilient consensus for multi-agent networks under deception attacks," *IEEE Access*, vol. 8, no. 3, pp. 121–129, 2020.
[25] X. Huang and J. Dong, "Reliable leader-to-follower formation control of multiagent systems under communication quantization and attacks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 50, no. 1, pp. 89–99, Jan. 2020.
[26] Z. Zuo, X. Cao, and Y. Wang, "Security control of multi-agent systems under false data injection attacks," *Neurocomputing*, vol. 404, pp. 240–246, Sep. 2020.
[27] M. Lu and L. Liu, "Leader–following consensus of multiple uncertain Euler–Lagrange systems with unknown dynamic leader," *IEEE Trans. Autom. Control*, vol. 64, no. 10, pp. 4167–4173, Oct. 2019.
[28] C. He and J. Huang, "Leader-following consensus for a class of multiple robot manipulators over switching networks by distributed position feedback control," *IEEE Trans. Autom. Control*, vol. 65, no. 2, pp. 890–896, Feb. 2020.
[29] G. Chen, Y. D. Song, and F. L. Lewis, "Distributed fault-tolerant control of networked uncertain Euler-Lagrange systems under actuator faults," *IEEE Trans. Cybern.*, vol. 47, no. 7, pp. 1706–1718, Jul. 2017.
[30] E. Nuño, "Consensus of Euler–Lagrange systems using only position measurements," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 1, pp. 489–498, Mar. 2018.
[31] D. Ding, Z. Wang, D. W. C. Ho, and G. Wei, "Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks," *IEEE Trans. Cybern.*, vol. 47, no. 8, pp. 1936–1947, Aug. 2017.
[32] H. Cai and J. Huang, "The leader-following consensus for multiple uncertain Euler-Lagrange systems with an adaptive distributed observer," *IEEE Trans. Autom. Control*, vol. 61, no. 10, pp. 3152–3157, Oct. 2016.
[33] J. Yu, J. Ji, Z. Miao, and J. Zhou, "Adaptive formation control of networked lagrangian systems with a moving leader," *Nonlinear Dyn.*, vol. 90, no. 4, pp. 2755–2766, Dec. 2017.
[34] H. K. Khalil, *Nonlinear Systems*, 3rd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2002.
[35] F. L. Lewis, C. T. Abdallah, D. M. Dawson, *Control of Robot Manipulation*, 1st ed. New York, NY, USA: Macmillan, 1993.

LIZHANG WANG is currently pursuing the M.S. degree in control science and engineering with the Nanjing University of Posts and Telecommunications, Nanjing, China.

His research interest includes distributed secure control of multiple Euler–Lagrange systems under deception attacks.

CHUNXIA FAN received the B.Sc. degree in electrical technology from Changchun University, Changchun, China, in 1995, the M.Sc. degree in basic mathematics from Guizhou University, Guiyang, China, in 2001, and the Ph.D. degree in control theory and control engineering from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2005.

In 2004, she joined the College of Automation, Nanjing University of Posts and Telecommunications, Nanjing, where she is currently a Professor. Her research interests include complex network theory with its applications, networked control, and robot control.

CONG XIE is currently pursuing the M.S. degree in control science and engineering with the Nanjing University of Posts and Telecommunications, Nanjing, China.

His research interest includes distributed secure control of multiple Euler–Lagrange systems under DoS attacks.

WEI ZHOU is currently pursuing the M.S. degree in control engineering with the Nanjing University of Posts and Telecommunications, Nanjing, China.

His current research interests include kinematic analysis and path planning methods of robots, and obstacle avoidance in complex environments.