2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Resilient Synchronization of Networked Lagrangian Systems in Adversarial Environments

Hongjian Chen, Xiaolei Li, Changyun Wen, Xu Fang

Abstract— **This paper considers the resilient synchronization problems of multiple Euler-Lagrange (EL) systems, where the communication network is affected by the external attacks or internal non-participant agents. The considered adversarial environments can cover several types of cyber-attacks, such as misbehaving agents and false data injection attacks. The remaining normal agents aim to reach a common decision despite the influence of faulty agents. To this end, a "safe kernel" based secure control scheme is proposed for the networked Lagrangian systems. According to the scheme, each healthy agent generates a convex hull based on the states of its neighbors and updates its reference state toward this kernel only in each sampling instant to reduce the computational burden. The "average sampling interval" is used to define the number of sampling instants for faster convergence. With an assumption on the number of misbehaving agents, the proposed scheme guarantees consensus of Euler-Lagrange systems even in adversarial environments. Mathematical proofs and a numerical example are presented to verify the resilience and validity of the proposed scheme.**

I. Introduction

Over the past few decades, there has been considerable research interests in the synchronization of multi-agent systems, which investigates how to design distributed controllers such that agents can cooperate with each other to make a common decision or optimum [1], [2]. In the early years, synchronization protocols were primarily based on the assumption that every agent in the network was trustworthy and cooperatively followed the algorithm throughout its execution, thus cooperative control problem has been well resolved [3]–[5]. However, as the scale of these systems has grown, it has become increasingly challenging to secure each agent in adversarial environments. On the one hand, external attackers can transmit malicious information through the communication link between agents [6]. On the other hand, some misbehaving or faulty agents may fail to follow the predefined protocols [7]. In either case, the network may be prevented from reaching the expected common decision [8].

This work was supported in part by the Ministry of Education (MOE), Singapore under Grant MOE2020-T1-1-067, in part by the National Natural Science Foundation of China under Grant 62103352, and also is partially supported by the Wallenberg AI, Autonomous Systems and Software Program (WASP) funded by the Knut and Alice Wallenberg Foundation.

H. Chen, C. Wen are with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore HONGJIAN001@e.ntu.edu.sg, ecywen@ntu.edu.sg

X. Li is with the School of Electrical Engineering, Yanshan University, Qinhuangdao, China xiaolei@ysu.edu.cn

X. Fang is with with the Division of Decision and Control Systems at KTH Royal Institute of Technology, Stockholm, Sweden xufang@kth.se

Some resilient protocols have already been designed to address security issues in the synchronization of multi-agent systems. However, many of these protocols simply ignore suspicious values. In one approach presented in [9], each healthy agent discards the most extreme values of its neighbors' states and updates its own state with the remaining values. Building on this idea, researchers have proposed a resilient consensus algorithm called the Mean Subsequence Reduced (MSR) protocol in several existing works [10]–[12]. This algorithm, which can tolerate up to F malicious agents, selects updating values within a range limited by upper and lower bounds or discards F largest or smallest incoming values. The goal of this protocol is to ensure that the final agreement is bounded by the minimum and maximum initial values of the normal agents. However, because the bounds of MSR are fixed, some valuable information may be lost during the updating process. To address this issue, researchers in [13] introduced a modified algorithm called the Weighted Mean Subsequence Reduced (W-MSR) algorithm. This protocol only removes suspicious values that are significantly larger or smaller than the current state value of the normal agent.

The aforementioned resilient synchronization algorithms assumed the states of agents are scalar variables. In most practical scenarios, such as consensus problems in 3D spaces, agents' states should be modeled as multi-dimensional vectors. Intuitively, applying W-MSR to each entry of state vectors can allow the final states of healthy agents converges to a multi-dimensional "box". The edges of "box" are confined by the maximum and minimum values of initial states of healthy agents. However, the "box" is usually larger than the convex hull formed by the initial states of healthy agents. A specific explanation is presented in Fig. 1.

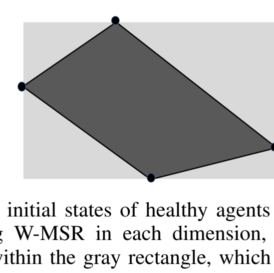


Fig. 1: In 2D plane, initial states of healthy agents are marked with black circles. By applying W-MSR in each dimension, the final agreement is guaranteed to stay within the gray rectangle, which is larger than the valid solid gray area.

To provide a more accurate convergence result, Yan et al. developed a resilient protocol in multi-dimensional spaces named "safe kernel" in [14]. With the application of "safe kernel", each normal agent creates a kernel under certain conditions and updates its state toward this kernel. This updating strategy ensures that the final agreement will converge to the convex hull of initial values of benign agents. Since the synchronization is one of fundamental concepts in designing a distributed algorithm, the "safe kernel" rule is generalized in some consensus-based scenarios such as containment control [15], distributed optimization [16] to increase the security and resilience. In [15], the "safe kernel" is generalized to second-order systems. However, the mentioned algorithms cannot be directly used to the networked EL systems due to inherent nonlinearities of EL systems.

Euler-Lagrange equation has been used to formulate a wide range of physical systems. For instance, four-wheel intelligent vehicles are modeled using EL systems in [17], and 6-DOF vehicles are described by EL systems in [18]. The synchronization issues of networked Lagrangian systems are investigated with the assumption that each agent could exchange information with its neighbors continuously in [19], [20]. In more practical applications, synchronization algorithms are implemented in digital platforms, which means the communication between agents can only happen at sampling instants. This setting stimulates the sampled-data control of networked EL systems [21], [22]. Because of nonlinearities of EL systems, sampled-data control is more complex as illustrated in [23]. In [24] the control protocols are assumed to be unchanged during each sampling interval, which may lead to overprovisioning of hardware, as mentioned in [25]. Consequently, a time-varying sampled-data control method is proposed to handle this problem. The control inputs are designed to be time-varying during each sampling interval and only needs to work on a specific duration in the sampling interval. It is worth noting that these approaches ignore cybersecurity threats and cannot handle the misbehaving agents.

In this paper, we focus on the synchronization problems of networked EL systems in adversarial environments. The approaches and main contributions of this paper are summarized as below:

- The "safe kernel" technique is generalized into networked EL systems to achieve a resilient synchronization with the presence of attackers or non-participant agents. Specifically, we derive the reference states of healthy agents by "safe kernel" which will converge into an agreement and then design a proportional derivative (PD) controller to drive the actual states of EL systems towards reference values.
- The approach of characterizing the sampling frequency through the "average sampling interval" is inspired by the concept of "average dwell time" in switching control. We apply this technique to determine the reference states at each sampling instant, thereby reducing the computational workload. By incorporating a time-varying term into control inputs, this method can address the issue of overprovisioning in systems.

The rest parts of this paper are structured as follows: Section II introduces some preliminaries results about EL systems and robust networks. Section III gives a detailed explanation of the research problem. A resilient synchronization algorithm is proposed in section IV and the analysis of the algorithm is presented in section V. A numerical example is provided in section VI and the paper is conclude in section VII.

II. Preliminaries

A. Networked Euler-Lagrange systems

Consider a group of N agents as follows

$$M_i\left(x_i\right)\ddot{x}_i + C_i\left(x_i,\dot{x}_i\right)\dot{x}_i + g_i\left(x_i\right) = \tau_i \tag{1}$$

where $i=1,2,...,N$, the vector $x_i=\left[x_{i1},x_{i2},\dots,x_{im}\right]^T\in\mathbb{R}^m$ represents the configuration variable, $M_i\left(x_i\right)\in\mathbb{R}^{m\times m}$ denotes the inertia matrix, $C_i\left(x_i,\dot{x}_i\right)\in\mathbb{R}^{m\times m}$ is the Coriolis and centrifugal torques, $\tau_i=\left[\tau_{i1},\tau_{i2},\dots,\tau_{im}\right]^T\in\mathbb{R}^m$ is the control input, and $g_i(x_i)\in\mathbb{R}^m$ is gravitational torque vector.

The properties associated with the networked Euler-Lagrange systems are shown as follows

(i) $M_i\left(x_i\right)$ is a positive definite symmetric matrix.

(ii) For any $y\in\mathbb{R}^m$, $y^T\left(\dot{M}_i\left(x_i\right)-2C_i\left(x_i,\dot{x}_i\right)\right)y=0$, which means $\dot{M}_i\left(x_i\right)-2C_i\left(x_i,\dot{x}_i\right)$ is skew-symmetric matrix.

B. Robust network

Denote $\mathcal{G}=\{\mathcal{V},\mathcal{E}\}$ as the graph of the networked Euler-Lagrangian systems, where $\mathcal{V}$ is the set of nodes, and $\mathcal{E}\subset\mathcal{V}\times\mathcal{V}$ is the set of edges. $e_{ij}\in\mathcal{E}$ denotes an edge between agents i and j. Any two nodes connected by an edge can exchange information directly with each other. The set of neighbors of node i is $\mathcal{N}_i=\{j\in\mathcal{V}\mid e_{ij}\in\mathcal{E}\}$.

As introduced in [13], the implementation of W-MSR requires a close coupling in graph structure. A new property, network robustness is hereby introduced to characterize the connectivity of the network. The formal definitions in [16] are given as follows

Definition 1. *[16] For any disjoint and nonempty subsets $\mathcal{V}_1,\mathcal{V}_2\subsetneq\mathcal{V}$, if at least one of the following statements holds:*

1) $\exists\ i\in\mathcal{V}_1$, s.t. node i has at least r neighbors outside $\mathcal{V}_1$,

2) $\exists\ i\in\mathcal{V}_2$, s.t. node i has at least r neighbors outside $\mathcal{V}_2$,

then, the network $\mathcal{G}=\{\mathcal{V},\mathcal{E}\}$ is said to be ***r-robustness****.*

Definition 2. *[16] For any disjoint and nonempty subsets $\mathcal{V}_1,\mathcal{V}_2\subsetneq\mathcal{V}$, if at least one of the following statements holds*

1) $\forall\ i\in\mathcal{V}_1$ has at least r neighbors outside $\mathcal{V}_1$,

2) $\forall\ i\in\mathcal{V}_2$ has at least r neighbors outside $\mathcal{V}_2$,

3) There are no less than s nodes in $\mathcal{V}_1\cup\mathcal{V}_2$, s.t. each of them has at least r neighbors outside the set it belongs to,

then, the network $\mathcal{G}=\{\mathcal{V},\mathcal{E}\}$ is said to be ***(r,s)-robustness****.*

III. Problem formulation

A. Resilient synchronization problems

Suppose there are N agents modeled as EL systems which cooperate over an undirected graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ and $x_i(t_k)$ denotes the state of node i at time t_k. Consider the influence of attackers or faulty agents in adversarial environments, the resilient synchronization is said to be achieved if the following conditions are satisfied:

- *Agreement*: For normal agents $i, j \in \mathcal{V}$, it holds that

$$\lim_{t\to\infty} \left(x_i\left(t\right) - x_j\left(t\right)\right) = 0, \quad \lim_{t\to\infty} \dot{x}_i\left(t\right) = 0, \tag{2}$$

  where $\dot{x}_i\left(t\right)$ represents the velocity of agent i.
- *Validity*: At each update iteration, the state of any normal agent is preserved in the convex hull formed by the initial states of all normal agents.

B. Attack model

In this subsection, the scope of threats is characterized. We denote $\mathcal{F}$ as the set of malicious agents and $\mathcal{B}$ as the set of benign agents, where $\mathcal{F} \cap \mathcal{B} = \emptyset$ and $\mathcal{F} \cup \mathcal{B} = \mathcal{V}$. Considering F faulty nodes in the network, the formal definitions of two attack models given in [16] are described as follows:

1) F-total attack model: $|\mathcal{F}| \leq F$, that is, the number of faulty agents is no more than F.
2) F-local attack model:$|\mathcal{F} \cap \mathcal{N}_i| \leq F$, that is, for any agent $i \in \mathcal{V}$, there are no more than F misbehaviors in the neighborhood of agent i.

There is no restriction on the transmitted information of the adversarial agents in the network. Since we need to consider the worst case of communication situations. However, the number of neighbors of any node in the topology should satisfy the following assumption:

Assumption 1. *For any agent in the network, it is held that* $|\mathcal{N}_i| \geq (d+1)F + 1$*, where* d *is the dimensionality of states.*

Since the "safe kernel" is the intersection of some particular convex hulls. This assumption is used to ensure the existence of the intersection.

IV. A resilient synchronization algorithm

Before proposing the resilient synchronization algorithm, some definitions are given to identify the "safe kernel" and "average sampling interval".

A. Safe kernel

Definition 3. $\mathcal{X}^i(t) \subset \mathbb{R}^d$ *with cardinality* $|\mathcal{N}_i|$ *denotes the set states received from neighbors of agent* $i \in \mathcal{B}$ *at time instant* t*. For some*$F \in \mathbb{Z}_{\geq 0}$ *and* $F < |\mathcal{N}_i|$*, let* $\mathcal{S}(\mathcal{X}^i(t), \mathcal{F})$ *denote the set of all its subsets with cardinality* $\mathcal{N}_i - F$*.*

The set $S\left(\mathcal{X}^i(t), F\right)$ contains $\begin{pmatrix} |\mathcal{N}_i| \\ F \end{pmatrix}$ elements, each of which is associated with a convex hull. The intersection of these convex hulls is exactly what is called "safe kernel". The formal definition is given as follows:

Definition 4. *Given a set* $X^i(t) \subset \mathbb{R}^d$ *with cardinality* $|\mathcal{N}_i|$*, for the number of misbehaviors* $F \in \mathbb{Z}_{\geq 0}$ *and* $F < |\mathcal{N}_i|$*, we define the intersection as the set*

$$\Psi\left(X^i(t), F\right) \triangleq \bigcap_{S \in S(X^i(t), F)} \mathrm{Conv}\left(S\right) \tag{3}$$

For simplicity, $\mathrm{Conv}(S)$ is the set of all convex combinations of the points in a set $S \subset \mathbb{R}^d$ and denote $\Psi\left(\mathcal{X}^i(t), F\right)$ as $\mathcal{S}_i(t)$. From (3), we know that $\mathcal{S}_i(t)$ is a subset of convex hulls. To give an intuitive representation of the intersection set, a 2D example with 6 nodes in total and 1 faulty node is shown in 2.

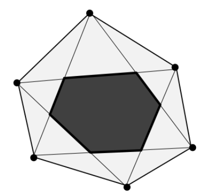


Fig. 2: A 2D example of "safe kernel", where each black circle stands for the location (state) of the agent in the network. The number of each agent's neighbor is 5 and $F = 1$. The deep gray region represents the "safe kernel", $\Psi\left(X^i(t), F\right)$.

B. Average sampling interval

In this paper, the networked EL systems are operated at a digital platform which is sampled at time instants $t_k, k = 0, 1, 2, \ldots (t_0 = 0$ and $t_k \to \infty$ as $t \to \infty)$. The sampling interval is defined as $h_k = t_{k+1} - t_k$. The formal definition of "average sampling interval" introduced in [25] is shown as below.

Definition 5. *The "average sampling interval" is said to be no more than* T*, if* $\exists T > 0$ *and* $N_0 > 0$*, s.t.*

$$N\left(t, t_0\right) \geq \frac{t - t_0}{T} - N_0, \tag{4}$$

where $t > t_0$ *and* $N(t, t_0)$ *denotes the number of sampling instants in the interval* $[t_0, t)$*.*

Remark 1. *Definition 5 is intended to characterize the sampling frequency of the controller. In early states, increasing the sampling frequency can provide more information for achieving faster tracking of actual states to reference states. In later stages, when the actual and reference states are very close, we can consider lowering the sampling frequency as compensation. Overall, we only need to ensure that the number of sampling instants is greater than* $N\left(t, t_0\right)$ *within a certain interval. The performance of "average sampling interval" is compared with the fixed sampling interval in Section VI.*

C. Algorithm design

The security updating protocol is composed of two existing approaches, namely, "safe kernel" and "average sampling interval". The state of agent i is denoted as $x_i\left(t_k\right) \in \mathbb{R}^d$ at time instant t_k. The sampling sequence $\{t_k\}$ satisfies the property introduced in Definition 5. Each benign agent has an initial state $x_i(0)$. At any sampling instant $t_k > 0$, all normal agents will update their own states as outlined in Algorithm 1.

Algorithm 1 Resilient synchronization of EL systems

1: Receive the states $x_j(t_k), j \in \mathcal{N}_i$ from all neighbors of agent i and collect them in $\mathcal{X}^i(t_k)$.
2: Compute $\Psi\left(\mathcal{X}^i(t_k), F\right)$ with the method in [26] and denote this set as $\mathcal{S}_i(t_k)$ for simplicity.
3: Let $p = t_k \bmod d$. Compute $l_p(x) = e_p^T x$, where e_p is the p-th canonical basis vector in $\mathbb{R}^d$ and each state $x \in \mathcal{X}^i(t_k)$.
4: Let $\underline{m}^l$ be the $dF+1$ smallest value among $l_p(x)$. Derive $y_i(t_k) \in \mathcal{S}^i(t_k)$, such that $l_p(y_i(t_k)) \leq \underline{m}^l$.
5: Let $\overline{M}^l$ be the $dF+1$ largest value among $l_p(x)$. Derive $z_i(t_k) \in \mathcal{S}^i(t_k)$, such that $l_p(z_i(t_k)) \geq \overline{M}^l$.
6: Compute the reference states of agent i in $[t_k, t_{k+1})$:
$$x_{r,i}(t) = \frac{x_i(t_k) + y_i(t_k) + z_i(t_k)}{3}. \tag{5}$$
7: Design PD control torque τ_i for agent i:
$$\tau_i = -K_p \tilde{x}_i - K_D \dot{x}_i + g(x_i), \tag{6}$$
where $\tilde{x}_i = x_i(t) - x_{r,i}(t)$, K_D and K_P are constant symmetric positive definite matrices. The sampling periods are defined in (4).

Remark 2. *The reference state of each faulty-free agent is computed by "safe kernel" method in Steps 1 to 6. To decrease computational workload, the reference states for the next sampling interval is only calculated in the sampling instant. Unlike simply using W-MSR to remove extreme information in each dimension, the "safe kernel" only requires each faulty-free agent to sort all neighbor state vectors in dimension p at time t_k, obtaining vectors $y_i(t_k)$ and $z_i(t_k)$ that do not contain the F largest and F smallest information, respectively. These two vectors are then averaged with the agent's actual state at instant t_k to obtain a reference state for the next sampling interval. This reference state fully utilizes the information of all neighbors and limits the impact of F faulty agents. The following lemmas will prove that the healthy agents will not update their reference states outside the "safe kernel," and the "safe kernel" is vanishing exponentially, which means that the reference states will achieve an agreement exponentially. To enable each healthy agent's actual state to track its reference state, we design distributed PD controllers.*

V. Algorithm analysis

A. Reliability

To guarantee the implementation of the algorithm, we need to analyze the nonempty property of $\mathcal{S}^i(t_k)$ and the existence of $y_i(t_k)$ and $z_i(t_k)$. The Helly's Theorem [27] is a useful tool to demonstrate that $\mathcal{S}^i(t_k)$ is nonempty:

Helly's Theorem: Let $X_1, X_2, \ldots, X_p$ be a finite set consisting of convex subsets in $\mathbb{R}^d$, where $p > d$. If the intersection of every $d+1$ convex hulls is nonempty, then we have:
$$\bigcap_{j=1}^{p} X_j \neq \emptyset. \tag{7}$$

From the definition of $S\left(X^i(t), F\right)$, each convex hull is constructed by deleting F elements in $X^i(t_k)$. Then, if we select any $d+1$ convex hulls, at most $F(d+1)$ elements in $X^i(t_k)$ will be removed. According to Assumption 1, the cardinality of $X^i(t_k)$ is larger than or equal to $(d+1)F+1$, which guarantees that at least one point is retained by all convex hulls. This means that any $d+1$ convex hulls have a nonempty intersection. With the application of Helly's Theorem, $\mathcal{S}^i(t_k)$ is said to be nonempty.

To verify the existence of $y_i(t_k)$, we firstly introduce a lemma in [16] which has been well proved.

Lemma 1. *[16] If any two sets, $\mathcal{A}_1$ with cardinality m_1 and $\mathcal{A}_2$ with cardinality m_2, satisfy $\mathcal{A}_1 \subset \mathcal{A}_2$, then for any $n \leq m_1 \leq m_2, \Psi(\mathcal{A}_1, n) \subset \Psi(\mathcal{A}_2, n)$ holds.*

Then, define a set $\mathcal{A} \subset X^i(t_k)$ with cardinality $(d+1)F+1$, such that it contains $dF+1$ points $\bar{x}$ satisfying $l_p(\bar{x}) \leq \underline{m}^l$. Because $\Psi(\mathcal{A}, F) \subset \Psi\left(X^i(t_k), F\right)$ from Lemma 1 , we have that any x in $\mathcal{S}^i(t_k)$ also has $l_p(x) \leq \underline{m}^l$. So, there must exist $y_i(t_k)$. And the existence of $z_i(t_k)$ can be proved similarly.

B. Validity

For simplicity, we denote the convex hull formed by the benign agents' states at time t_k as $\Omega(t_k)$.

Lemma 2. *If the misbehaving agents in graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ follow the F-total or F-local attack model, we have the following relation with the application of Algorithm 1:*
$$\Omega(t_{k+1}) \subset \Omega(t_k). \tag{8}$$

Proof. With the existence of F misbehaving agents, $\Omega(t_k)$ is constructed by $|\mathcal{N}_i| - F$ state values of healthy agents. Since $\mathcal{S}_i(t_k)$ is the intersection of all convex hulls formed by $|\mathcal{N}_i| - F$ neighboring states, we can derive that $\mathcal{S}_i(t_k) \subset \Omega(t_k)$. From the definition of "safe kernel", the reference state of each healthy agent holds that $x_{r,i}(t_{k+1}) \in \Omega(t_k)$. Lemma 1 is proved. ☐

Hence, by lemma 2, the benign agents will never update their states out of the convex hull formed by initial states, namely $\Omega(0)$. So far, the validity of Algorithm 1 is guaranteed.

C. Agreement

Now two lemmas are established to show the consensus of all benign agents' reference states.

Lemma 3. *Consider a network with $[(d+1)F+1]$-robustness. Suppose that the misbehaving agents follow the F-local attack model. With the application of "safe kernel", the reference states of healthy agents are guaranteed to be exponential synchronization, regardless misbehaviors' states.*

Lemma 4. *Consider a network with $(dF+1, F+1)$-robustness. Suppose that the misbehaving agents follow the F-total attack model. With the application of "safe kernel", the reference states of healthy agents are guaranteed to be exponential synchronization, regardless of misbehaviors' states.*

Proof. To prove Lemma 3, two extreme values among $p-th$ components of normal agents' reference states at instant t_k are defined as follows

$$m^p(t_k) \triangleq \min_{i\in\mathcal{B}} x_{r,i}^p(t_k), M^p(t_k) \quad \triangleq \max_{i\in\mathcal{B}} x_{r,i}^p(t_k). \quad (9)$$

Considering the symmetry property between each dimension, we will analyze the synchronization condition at the first component for simplicity. Let $\Delta^1(t_k)$ denote the difference between its minimum and maximum values, i.e.

$$\Delta^1(t_k) = M^1(t_k) - m^1(t_k). \quad (10)$$

The consensus of reference states can be achieved when $\Delta^1(t_k)$ approaches 0 exponentially. Throughout the proof, we suppose $\Delta^1(t_k) > 0$. Then, for $\bar{t}_k \geq t_k, \bar{t}_k \bmod d = 1$ and $\epsilon \in \mathbb{R}$, we define two sets:

$$\begin{aligned} \mathcal{V}^M(t_k, \bar{t}_k, \epsilon) &\triangleq \left\{i \in \mathcal{V} : x_i^1(\bar{t}_k) > M^1(t_k) - \epsilon\right\}, \\ \mathcal{V}^m(t_k, \bar{t}_k, \epsilon) &\triangleq \left\{i \in \mathcal{V} : x_i^1(\bar{t}_k) < m^1(t_k) + \epsilon\right\}. \end{aligned} \quad (11)$$

Let $\mathcal{B}^M(t_k, \bar{t}_k, \epsilon)$ and $\mathcal{B}^m(t_k, \bar{t}_k, \epsilon)$ be two disjoint sets containing only benign agents' states in $\mathcal{V}^M(t_k, \bar{t}_k, \epsilon)$ and $\mathcal{V}^m(t_k, \bar{t}_k, \epsilon)$

$$\begin{aligned} \mathcal{B}^M(t_k, \bar{t}_k, \epsilon) &\triangleq \mathcal{V}^M(t_k, \bar{t}_k, \epsilon) \cap \mathcal{B} \\ \mathcal{B}^m(t_k, \bar{t}_k, \epsilon) &\triangleq \mathcal{V}^m(t_k, \bar{t}_k, \epsilon) \cap \mathcal{B}, \end{aligned} \quad (12)$$

which satisfy

$$\left|\mathcal{B}^M(t_k, \bar{t}_k, \epsilon)\right| + \left|\mathcal{B}^m(t_k, \bar{t}_k, \epsilon)\right| \leq |\mathcal{B}|. \quad (13)$$

In the proof procedure, we also suppose $\Delta^1(t_k) > 0$. Define $\epsilon_0 = \frac{\Delta^1(t_k)}{2}$. From the definition of $[(d+1)F+1]$-robustness network, $\mathcal{B}^M(t_k, t_k, \epsilon_0)$ or $\mathcal{B}^m(t_k, t_k, \epsilon_0)$ has at least one healthy agent with no less than $(d+1)F+1$ neighbors outside its own set at sampling instant t_k. Under the F-local attack model, at least $dF+1$ neighbors in $\mathcal{V}\backslash\mathcal{B}^M(t_k, t_k, \epsilon_0)$ have the property that $x_i^1(t_k) \leq M^1(t_k) - \epsilon_0$. In the algorithm, $\underline{m^l}$ is the $dF+1$ smallest values. Therefore, we have $y_i^1(t_k) \leq \underline{m^l} \leq M^1(t_k) - \epsilon_0$. Then, the reference state of agent i at next sampling instant can be transformed into

$$\begin{aligned} x_{r,i}(t_{k+1}) &= \frac{x_i(t_k) + y_i(t_k) + z_i(t_k)}{3} \\ &\leq \frac{1}{3}M^1(t_k) + \frac{1}{3}\left(M^1(t_k) - \epsilon_0\right) + \frac{1}{3}M^1(t_k) \\ &= M^1(t_k) - \frac{1}{3}\epsilon_0. \end{aligned} \quad (14)$$

This upper bound also applies to any healthy agents in $\mathcal{V}\backslash\mathcal{V}^M(t_k, \bar{t}_k, \epsilon)$. Similarly, we have $x_{r,i}(t_{k+1}) \geq m^1(t_k) + \frac{1}{3}\epsilon_0$ for any benign agent in $\mathcal{B}^m(t_k, t_k, \epsilon)$ from $z_i^1(t_k) \geq \overline{M^l} \geq m^1(t_k) + \frac{1}{3}\epsilon_0$. Also, this lower bound can apply to any healthy agent in $\mathcal{V}\backslash\mathcal{V}^m(t_k, \bar{t}_k, \epsilon)$.

Let $\epsilon_1 = \epsilon_0/3$. From above, it can be deduced that no less than one healthy agent in $\mathcal{B}^M(t_k, t_k, \epsilon_0)$ [resp.$\mathcal{B}^m(t_k, t_k, \epsilon_0)$] has its reference state' first component decreased below $M^1(t_k) - \epsilon_1$ [resp. increased above $m^1(t_k) + \epsilon_1$]. Thus, $\mathcal{B}^M(t_k, t_{k+1}, \epsilon_1) \subsetneq \mathcal{B}^M(t_k, t_k, \epsilon_0)$, or $\mathcal{B}^m(t_k, t_{k+1}, \epsilon_1) \subsetneq \mathcal{B}^m(t_k, t_k, \epsilon_0)$, or both hold.

Now, we consider the next updating instant t_{k+2}. We have $y_i^1(t_{k+1}) \leq \underline{m^l} \leq M^1(t_k) - \epsilon_1$. For any benign agent in $\mathcal{V}\backslash\mathcal{V}^M(t_k, t_{k+1}, \epsilon)$, we can obtain:

$$\begin{aligned} x_{r,i}(t_{k+2}) &= \frac{x_i(t_{k+1}) + y_i(t_{k+1}) + z_i(t_{k+1})}{3} \\ &\leq \frac{1}{3}M^1(t_{k+1}) + \frac{1}{3}\left(M^1(t_k) - \epsilon_1\right) + \frac{1}{3}M^1(t_{k+1}) \\ &\leq \frac{1}{3}\left(M^1(t_k) - \epsilon_1\right) + \frac{2}{3}M^1(t_k) \\ &= M^1(t_k) - \frac{1}{3}\epsilon_1 \\ &= M^1(t_k) - \epsilon_2 \end{aligned} \quad (15)$$

Define $\epsilon_d = \frac{\epsilon_0}{3^d}$ where integer $d \geq 1$. From the recursive process above, one can derive that $\mathcal{B}^M(t_k, t_{k+d}, \epsilon_d) \subset \mathcal{B}^M(t_k, t_{k+d-1}, \epsilon_{d-1}) \subset \cdots \subset \mathcal{B}^M(t_k, t_{k+1}, \epsilon_1) \subsetneq \mathcal{B}^M(t_k, t_k, \epsilon_0)$ as long as $\mathcal{B}^M(t_k, t_{k+d}, \epsilon_d)$ is nonempty. Similarly, $\mathcal{B}^m(t_k, t_{k+d}, \epsilon_d) \subsetneq \mathcal{B}^m(t_k, t_k, \epsilon_0)$. It is clear that one of sets $\mathcal{B}^M(t_k, \bar{t}_k, \epsilon)$ and $\mathcal{B}^m(t_k, \bar{t}_k, \epsilon)$ will vanish at next sampling instant. Because $\epsilon_d < \epsilon_0$, nonempty sets $\mathcal{B}^M(t_k, t_{k+d}, \epsilon_d)$ and $\mathcal{B}^m(t_k, t_{k+d}, \epsilon_d)$ are always disjoint. With the fact (12), at least one of the following conditions holds

$$\mathcal{B}^M\left(t_k, t_{k+|\mathcal{B}|}, \epsilon_{|\mathcal{B}|}\right) = \emptyset, \mathcal{B}^m\left(t_k, t_{k+|\mathcal{B}|}, \epsilon_{|\mathcal{B}|}\right) = \emptyset. \quad (16)$$

From (16), at instant $t+|\mathcal{B}|$, reference states' first components of all benign agents satisfy

$$\begin{aligned} M^1\left(t_{k+|\mathcal{B}|}\right) &\leq M^1(t_k) - \epsilon_{|\mathcal{B}|}, \\ m^1\left(t_{k+|\mathcal{B}|}\right) &\geq m^1(t_k) + \epsilon_{|\mathcal{B}|}. \end{aligned} \quad (17)$$

Combining the two inequalities above, it yields

$$\Delta^1\left(t_{k+|\mathcal{B}|}\right) \leq \left(1 - \frac{1}{2\times 3^{|\mathcal{B}|}}\right)\Delta^1(t_k). \quad (18)$$

As a result, the differences between maximum and minimum of healthy agents' reference states in the first entry will shrink exponentially. This proof is applicable in each dimension of the reference state vector. Similarly, we can prove Lemma 4. □

Based on the established lemmas above, we have the following main theorem.

Theorem 1. *Consider the networked Lagrangian systems under an undirected graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$, with the sampling instants sequence satisfying condition* (4)*. Suppose one of the following conditions is satisfied:*

1) *The network is ((d+1)F+1)-robust and under F-local attack model.*
2) *The network is (dF+1,F+1)-robust and under F-total attack model.*

With the application of Algorithm 1, normal agents asymptotically reach the resilient synchronization.

Proof. Lemmas 3 and 4 imply that normal agents' reference states will approach an agreement exponentially with the increment of sampling instants. Now, we need to ensure that actual states approach reference states asymptotically as follows

$$\lim_{t\to\infty} \tilde{x}_i(t) = 0, \quad \lim_{t\to\infty} \dot{x}_i(t) = 0, \tag{19}$$

where $i \in \mathcal{B}$. To this end, we construct a Lyapunov function inspired by the mechanical energy of EL systems, namely

$$V(t) = \frac{1}{2}\sum_{i=1}^{N}\left(\dot{x}_i^T M_i(x_i)\dot{x}_i + \tilde{x}_i^T K_P \tilde{x}_i\right), \tag{20}$$

Taking derivative of (20) over $[0, +\infty)$, applying (6) and properties (i), (ii) of EL systems, we obtain:

$$\begin{aligned}\dot{V}(t) &= \sum_{i=1}^{N}\left(\dot{x}_i^T M_i \ddot{x}_i\right) + \frac{1}{2}\sum_{i=1}^{N}\left(\dot{x}_i^T \dot{M}_i \dot{x}_i\right) + \sum_{i=1}^{N}\left(\dot{\tilde{x}}_i^T K_P \tilde{x}_i\right)\\ &= \sum_{i=1}^{N}\left[\dot{x}_i^T\left(M_i\ddot{x}_i + C_i(x_i, \dot{x}_i\dot{x}_i)\right)\right] + \sum_{i=1}^{N}\left(\dot{x}_i^T K_P \tilde{x}_i\right)\\ &= \sum_{i=1}^{N}\left(\dot{x}_i^T(-K_D)\dot{x}_i\right) \le 0\end{aligned}$$

as K_D is symmetric positive definite and $\alpha(t, t_k)$ is a semi-positive time-varying function. We have to ensure that closed-loop systems cannot be "stuck" at a point where $\dot{V} = 0$ while $\tilde{x}_i \neq 0$. For this purpose, we invoke the Global La Salle's Invariant Set Theorem[28]. As $\dot{V}(t) = 0$ results in $\dot{x}_i = 0, i \in \mathcal{B}$, it follows that $\ddot{x}_i = M_i^{-1}K_P\tilde{x}_i$. Therefore, $\dot{V}(t)$ can only be 0 if $\tilde{x}_i = 0$, which implies EL systems do converge to the reference states asymptotically.

□

VI. Numerical Example

The established theoretical results are now illustrated and verified by the following example. Given an undirected graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$, we present the communication topology in Fig. 3. The network is with $[(d+1)F+1]-$robustness, where $d = 2, F = 1$. The attack model is F-local type.

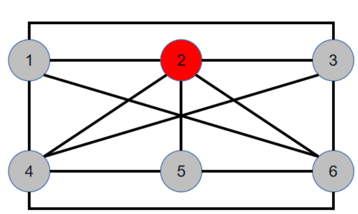


Fig. 3: Communication network

We suppose that Agent 2 is a faulty one, which will update its state as $x_2^1 = 1.5\sin\frac{t}{5}, x_2^2 = \frac{t}{25} + 1$. Other benign agents' states are initialized as: $x_1(0) = (0, 0)$, $x_3(0) = (2, 0)$, $x_4(0) = (1, 3)$, $x_5(0) = (2, 4)$, $x_6(0) = (3, 3)$.

The specific settings of EL equations are shown below:

$$M_i(x_i) = \begin{bmatrix} M_{i11} & M_{i12}\\ M_{i21} & M_{i22}\end{bmatrix}, \tag{21}$$

where $M_{i11} = a_1 + 2a_3\cos\left(x_i^2\right) + 2a_4\sin\left(x_i^2\right), M_{i22} = a_2$, $C_i(x_i, \dot{x}_i) = \begin{bmatrix} -b\dot{x}_i^2 & -b\left(\dot{x}_i^1 + \dot{x}_i^2\right)\\ b\dot{x}_i^1 & 0\end{bmatrix}$, $a_1 = 3.93, a_2 = 1.53$, $a_3 = 1.6\cos\frac{\pi}{6}$, $a_4 = 1.6\sin\frac{\pi}{6}$, $b = 1.6\cos\frac{\pi}{6}\sin\left(x_i^2\right) - 1.6\sin\frac{\pi}{6}\cos\left(x_i^2\right)$, and $g_i(x_i) = \begin{bmatrix} 9.8x_i^1\\ 9.8(x_i^1 - x_1^2)\end{bmatrix}$. Given $K_D = 5I_2$ and $K_P = 10K_D$, the PD control input is designed as:

$$\tau_i = -K_D\dot{x}_i - K_p\tilde{x}_i + g_i(x_i). \tag{22}$$

To satisfy the requirements of Definition 5, we suppose that sampling interval $T_1 = 0.25s$ in $t \in [0, 20)$ and $T_2 = 0.375s$ in $t \in [20, 40]$. All the simulations are implemented in MATLAB. The performance of Algorithm 1 is represented in Fig. 4, which verifies the result in Theorem 1.For comparisons, we also conducted a simulation with a fixed sampling length $T = 0.3125s$ to maintain the total number of sampling instants. Results of states x_i^1 of Agent i, i=1,2,...., 6, from the comparison simulations are shown in Fig. 5 as an example, which demonstrate that the "average sampling interval" can indeed accelerate the convergence of networked EL systems.

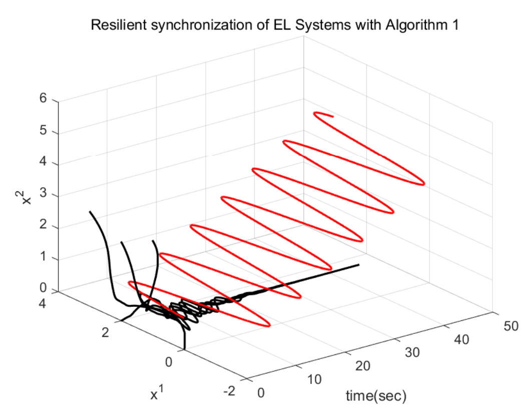
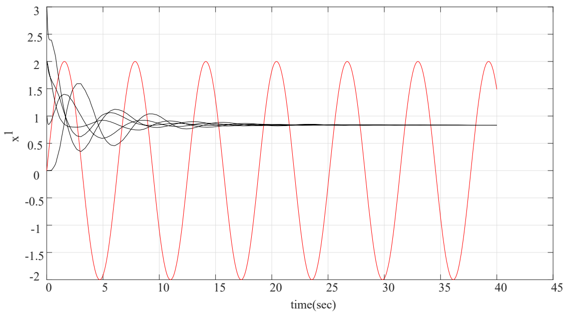


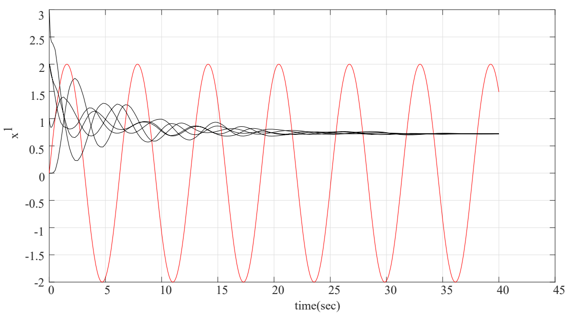
Fig. 4: Simulation results with application of Algorithm 1 (x_i^1 and x_i^2 against time(sec)). Red curve denoted the malicious agent.

VII. Conclusion

In this paper, we proposed a resilient synchronization scheme for networked Lagrangian systems. The key concept of this strategy is driving reference states of healthy agents into "safe kernel" and designing distributed PD controllers to enable actual states to track the reference states. Under the robust network and for certain attacks, normal agents asymptotically achieve consensus with application of our proposed scheme. Moreover, the "average sampling interval" is applied to adjust the sampling frequency for good tracking of actual states to reference states.



(a) Average Sampling Interval



(b) Fixed Sampling Interval

Fig. 5: State x_i^1 of two different sampling schemes.

References

[1] W. Ren, R. W. Beard, and E. M. Atkins, "Information consensus in multivehicle cooperative control," *IEEE Control Systems Magazine*, vol. 27, no. 2, pp. 71–82, 2007.

[2] M. Wang, Y. Xie, and S. Qin, "An adaptive memristor-programming neurodynamic approach to nonsmooth nonconvex optimization problems," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2023.

[3] P. Duan, L. He, Z. Duan, and L. Shi, "Distributed cooperative LQR design for multi-input linear systems," *IEEE Transactions on Control of Network Systems*, vol. 10, no. 2, pp. 680–692, 2023.

[4] X. Fang, L. Xie, and X. Li, "Distributed localization in dynamic networks via complex laplacian," *Automatica*, vol. 151, p. 110915, 2023.

[5] X. Fang, X. Li, and L. Xie, "Angle-displacement rigidity theory with application to distributed network localization," *IEEE Transactions on Automatic Control*, vol. 66, no. 6, pp. 2574–2587, 2020.

[6] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2011.

[7] S. Sundaram and B. Gharesifard, "Distributed optimization under adversarial nodes," *IEEE Transactions on Automatic Control*, vol. 64, no. 3, pp. 1063–1076, 2018.

[8] J. Chen and R. J. Patton, *Robust model-based fault diagnosis for dynamic systems*, vol. 3. Springer Science & Business Media, 2012.

[9] D. Dolev, N. A. Lynch, S. S. Pinter, E. W. Stark, and W. E. Weihl, "Reaching approximate agreement in the presence of faults," *Journal of the ACM (JACM)*, vol. 33, no. 3, pp. 499–516, 1986.

[10] R. M. Kieckhafer and M. H. Azadmanesh, "Reaching approximate agreement with mixed-mode faults," *IEEE Transactions on Parallel and Distributed Systems*, vol. 5, no. 1, pp. 53–63, 1994.

[11] N. H. Vaidya, L. Tseng, and G. Liang, "Iterative approximate byzantine consensus in arbitrary directed graphs," in *Proceedings of the 2012 ACM symposium on Principles of distributed computing*, pp. 365–374, 2012.

[12] M. M. de Azevedo and D. M. Blough, "Multistep interactive convergence: An efficient approach to the fault-tolerant clock synchronization of large multicomputers," *IEEE Transactions on Parallel and Distributed Systems*, vol. 9, no. 12, pp. 1195–1212, 1998.

[13] H. J. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram, "Resilient asymptotic consensus in robust networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 4, pp. 766–781, 2013.

[14] J. Yan, Y. Mo, X. Li, and C. Wen, "A "safe kernel" approach for resilient multi-dimensional consensus," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 2507–2512, 2020.

[15] J. Yan and C. Wen, "Resilient containment control in adversarial environment," *IEEE Transactions on Control of Network Systems*, vol. 7, no. 4, pp. 1951–1959, 2020.

[16] J. Yan, X. Li, Y. Mo, and C. Wen, "Resilient multi-dimensional consensus in adversarial environment," *Automatica*, vol. 145, p. 110530, 2022.

[17] C. Guo, L. Dong, and Y. Ge, "Trajectory tracking control for intelligent vehicle based on the euler-lagrange systems," in *The 26th Chinese Control and Decision Conference (2014 CCDC)*, pp. 1677–1681, IEEE, 2014.

[18] E. Borhaug and K. Y. Pettersen, "Formation control of 6-dof euler-lagrange systems with restricted inter-vehicle communication," in *Proceedings of the 45th IEEE Conference on Decision and Control*, pp. 5718–5723, IEEE, 2006.

[19] A. Mehrabian, S. Tafazoli, and K. Khorasani, "Velocity synchronization of networked euler-lagrange systems with switching network topologies subject to actuator faults," in *2010 Conference on Control and Fault-Tolerant Systems (SysTol)*, pp. 892–898, IEEE, 2010.

[20] J. Mei, W. Ren, and G. Ma, "Containment control for multiple euler-lagrange systems with parametric uncertainties in directed networks," in *Proceedings of the 2011 American control conference*, pp. 2186–2191, IEEE, 2011.

[21] X.-M. Zhang, Q.-L. Han, and X. Yu, "Survey on recent advances in networked control systems," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 5, pp. 1740–1752, 2015.

[22] Z.-G. Wu, P. Shi, H. Su, and J. Chu, "Stochastic synchronization of markovian jump neural networks with time-varying delay using sampled data," *IEEE Transactions on Cybernetics*, vol. 43, no. 6, pp. 1796–1806, 2013.

[23] H. Wang, "Consensus of networked mechanical systems with communication delays: A unified framework," *IEEE Transactions on Automatic Control*, vol. 59, no. 6, pp. 1571–1576, 2013.

[24] C. Ma, P. Shi, X. Zhao, and Q. Zeng, "Consensus of euler–lagrange systems networked by sampled-data information with probabilistic time delays," *IEEE Transactions on Cybernetics*, vol. 45, no. 6, pp. 1126–1133, 2014.

[25] W. Zhang, Y. Tang, T. Huang, and A. V. Vasilakos, "Consensus of networked euler–lagrange systems under time-varying sampled-data control," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 535–544, 2017.

[26] X. Wang, S. Mou, and S. Sundaram, "A resilient convex combination for consensus-based distributed algorithms," *arXiv preprint arXiv:1806.10271*, 2018.

[27] L. Danzer, B. Grunbaum, and V. Klee, "Helly's theorem and its relatives1," *Monatsh. Math*, vol. 31, pp. 60–97, 1921.

[28] J.-J. E. Slotine, W. Li, *et al.*, *Applied nonlinear control*, vol. 199. Prentice hall Englewood Cliffs, NJ, 1991.