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

Cyberattack Detection for a Class of Nonlinear Multi-Agent Systems Using Set-Membership Fuzzy Filtering

Mahshid Rahimifard, Amir M. Moradi Sizkouhi, and Rastko R. Selmic, *Senior Member, IEEE*

Abstract— **This paper studies cyberattack detection in discrete-time, leader-following, nonlinear, multi-agent systems subject to unknown but bounded (UBB) system noise. The Takagi–Sugeno (T-S) fuzzy model is used to approximate the nonlinear systems over the true value of the state. A new method is developed for simultaneous distributed cyberattack detection and leader-following consensus control. The approach is based on a fuzzy set-membership filtering technique that consists of two steps: a prediction step and a measurement update step. An estimation ellipsoid set is found by updating the prediction ellipsoid set with the current sensor measurement data. A criterion is provided to detect cyberattacks that inject malicious signals into sensor data. The criterion is based on the intersection between the ellipsoid sets. If there is no intersection between the prediction set and the estimation set of an agent at the current time instant, a cyberattack on its sensors is declared. Recursive algorithms for solving the consensus protocol and calculating the two ellipsoid sets for detecting attacks are proposed. Moreover, a recovery mechanism that can mitigate the adversarial effects of cyberattacks is introduced. Simulation results are provided to demonstrate the effectiveness of the proposed method when replay attacks occur on the sensor data.**

I. Introduction

Multi-agent systems (MAS) have a wide range of applications, including the Internet of Things (IoT), electrical grids, water distribution systems, transportation systems, Unmanned Aerial Vehicles (UAVs), and autonomous vehicles [1], [2]. Reaching consensus in a distributed manner is a fundamental problem in MAS. The agents transmit their data to neighboring agents through communication channels in distributed consensus protocols, which are vulnerable to cyberattacks. Some distributed and decentralized methods for cyberattack detection have been proposed in [3]–[5].

Recent research has extensively investigated the utilization of a commonly employed state estimation method (i.e., Kalman filter), and attack detector (i.e., performance index test) [6]–[8]. Cyberattack detection methods that are based on state estimation necessitate system noise in a stochastic framework, leading to probabilistic state estimation. For many real-world applications, accuracy in state estimation is crucial. However, estimation based on a probabilistic approach, such as the Kalman filtering method, necessitates using mean and variance to describe the state distributions modeled as random variables. Consequently, considering unknown but bounded (UBB) noise is a more suitable approach for modeling state distributions [9].

Due to the nature of the Kalman filtering technique, the estimated and predicted states are single vectors, and accordingly, it cannot be guaranteed that a state belongs to a certain region. Also, the attack detection is unreliable due to the sub-optimal performance of Kalman-type filtering in the presence of UBB noises. The ellipsoidal state estimation technique was developed in [10]. This method, known as the set-membership or set-valued state estimation filtering approach, has been extensively studied in filtering problems [11], [12] and provides a set of state estimates in the state-space that contains the system's true state [13], [14]. By using convex optimization, an optimal ellipsoid with minimal size can be determined for set-membership estimation, thus improving state estimation and detection performance.

The authors in [9] have studied a cyberattack detection method for linear networked control systems using set-membership filtering. However, they considered the attack detection problem without the control of the system, and the system is not a multi-agent system.

There are few works on the detection of replay attacks, mainly focusing on linear systems [9], [15]. The detection of these attacks for nonlinear systems is of prime importance as they affect the system's performance. Replay attacks are a special kind of deception attack and take place in two phases: (i) recording data from the system and (ii) replaying the recorded data.

Except a few results [16], [17], most research on set-membership filtering considers linear systems [9], [18], [19]. Linearization should best fit the nonlinear functions over a state estimate set rather than a state estimate point when we use the set-membership framework. Due to linearization around the estimated value of the state rather than the true value, the approximations in [16] bring a base point error [20].

The fuzzy model of Takagi-Sugeno (T-S) is an effective and universal approximator for a certain class of nonlinear dynamical systems [21], [22]. There are several advantages of the T-S fuzzy model over neural networks when it comes to approximating nonlinear systems. T-S fuzzy models are often more robust to noise and uncertainty in the input data than neural networks, which can be sensitive to small variations in the input. Moreover, T-S fuzzy models are simpler to train and implement than neural networks and are, therefore, faster and easier to use in real-world applications.

In this paper, we use T-S to approximate a class of nonlinear systems. We linearize the nonlinear systems over the true value of the state and eliminate the base point error. Our

M. Rahimifard, A. M. Moradi Sizkouhi, and R. R. Selmic are with the Department of Electrical and Computer Engineering, Concordia University, Montreal, QC, Canada. seyedehmahshid.rahimifard@concordia.ca, amirmohammad.moradis@concordia.ca, rastko.selmic@concordia.ca.

979-8-3503-0123-6/23/$31.00 ©2023 IEEE

objective is to design a simultaneous distributed cyberattack detection strategy and leader-following consensus control based on a new, two-step fuzzy set-membership filtering approach. By utilizing the fuzzy modeling approach and the S-procedure technique [23], we determine bounding ellipsoidal sets for each agent. We apply a recursive algorithm in the state-space, which guarantees enclosing of the system's true state [13], [14], regardless of UBB noise, assuming no attacks are being made on the agent.

Each agent has a prediction and a measurement update step in its state estimation algorithm. While our method is designed to detect cyberattacks that inject malicious signals into the sensor data, we specifically focus on detecting replay attacks, given the need for more research in this area for nonlinear systems. Replay attacks are often detected using active detection methods with watermarking injection [15], but these methods can reduce control performance. A key benefit of the proposed approach is the ability to detect replay attacks without signal injection.

Compared with the previous works, the contributions of this paper are as follows:

- We developed a cyberattack detection method for a class of *nonlinear* multi-agent systems.
- We developed the fuzzy set-membership filtering approach for cyberattack detection on a class of nonlinear multi-agent systems.
- We are able to mitigate the effects of the attack and recover system performance.
- In the presence of an attack, the method still achieves the control goal – the leader-following consensus.

II. Problem Formulation

Interaction and communication are modeled as a connected directed graph $\mathscr{G} = \{\mathscr{V}, \mathscr{E}, \mathscr{A}\}$, $\mathscr{V} = \{1,2,...,N\}$, $\mathscr{E} = \{(i,j), i,j \in \mathscr{V}\}$, and $\mathscr{A} = (a_{ij}) \in \mathbb{R}^{N\times N}$, which are the vertex set, the directed edge set and the weighted adjacency matrix of $\mathscr{G}$, respectively. The weights are defined as $a_{ij} = 1$, if $(j,i) \in \mathscr{E}$ and $a_{ij} = 0$, otherwise. An agent (node) from which an edge is connected to the node i is a neighbor of node i. The set of the neighbors N_i of node i is $N_i = \{j | (j,i) \in \mathscr{E}\}$. Moreover, the Laplacian matrix $\mathscr{L} = [l_{i,j}] \in \mathbb{R}^{N\times N}$ is defined as $\mathscr{L} = \mathscr{D} - \mathscr{A}$, and $\mathscr{D} = \operatorname{diag}_{i=1}^N \{d_i\}$, with $d_i = \sum_{j=1}^N a_{ij}$.

Consider a discrete-time nonlinear multi-agent system of N agents and the dynamics of the i-th agent that is given by

$$\begin{aligned} x_i(k+1) &= f_i(x_i(k)) + G_i u_i(k) + I_i(x_i(k))\omega_i(k) \\ y_i(k) &= h_i(x_i(k)) + F_i(x_i(k))v_i(k), \end{aligned} \tag{1}$$

$i \in \{1,...,N\}$, where $x_i(k) \in \mathbb{R}^{n_x}$, $u_i(k) \in \mathbb{R}^{n_u}$, and $y_i(k) \in \mathbb{R}^{n_y}$ represent state variables, control input, and measurable output, respectively. The functions $f_i(x_i(k))$, $I_i(x_i(k))$, $h_i(x_i(k))$, and $F_i(x_i(k))$ are the nonlinear functions of $x_i(k)$, with $f_i(0) = 0$, $I_i(0) = 0$, $h_i(0) = 0$, $F_i(0) = 0$, and G_i's are known matrices. A process uncertainty is denoted by $\omega_i(k) \in \mathbb{R}^{n_\omega}$, and a measurement noise by $v_i(k) \in \mathbb{R}^{n_v}$, which are assumed to be confined to specified ellipsoidal sets.

Ellipsoid: An ellipsoidal set has the form $\mathscr{X} \triangleq \{\zeta : \zeta = c + \Xi z, \|z\| \le 1\}$, where $c \in \mathbb{R}^{n_x}$ is the center, and $\Xi \in \mathbb{R}^{n_x \times m}$ is the shape matrix, with $\operatorname{rank}(\Xi) = m \le n_x$. Alternatively, the ellipsoidal set can be represented as $\mathscr{X} \triangleq \left\{\zeta : (\zeta - c)^{\mathrm{T}} P^{-1} (\zeta - c) \le 1\right\}$, where $P = \Xi\Xi^{\mathrm{T}} > 0$. The size of the ellipsoid is dependent on matrix P and can be calculated as $\operatorname{tr}(P)$, which is the sum of the squared semi-axes lengths [19].

Assumption 1. The process noise $\omega_i(k)$, and the measurement noise $v_i(k)$ are UBB, belonging to the ellipsoidal sets:

$$\begin{aligned} \mathscr{W}_i(k) &\triangleq \left\{\omega_i(k) : \omega_i(k)^{\mathrm{T}} Q_i(k)^{-1} \omega_i(k) \le 1\right\} \\ \mathscr{V}_i(k) &\triangleq \left\{v_i(k) : v_i^{\mathrm{T}}(k) R_i^{-1}(k) v_i(k) \le 1\right\}, \end{aligned} \tag{2}$$

where $Q_i(k) = Q_i(k)^T > 0$, $R_i(k) = R_i(k)^T > 0$ are known matrices with compatible dimensions.

To design an appropriate filter for the i-th agent of the nonlinear discrete-time system (1), the following T-S fuzzy model is given [17]:

Plant Rule l_i : IF $\theta_{i,1}(k)$ is $\mu_{l_i,1}$ and $\theta_{i,2}(k)$ is $\mu_{l_i,2} \ldots$ and $\theta_{i,q}(k)$ is $\mu_{l_i,q}$, THEN

$$\begin{aligned} x_i(k+1) &= A_{l_i} x_i(k) + B_{l_i} u_i(k) + M_{l_i} \omega_i(k) \\ y_i(k) &= C_{l_i} x_i(k) + D_{li} v_i(k), \end{aligned} \tag{3}$$

where $l_i = 1, \ldots, r$ (r stands for the total number of plant IF-THEN rules), $\mu_{l_i,1}, \ldots, \mu_{l_i,q}$ are fuzzy sets, $\theta_i(k) = \left[\theta_{i,1}^T(k)\theta_{i,2}^T(k) \cdots \theta_{i,q}^T(k)\right]^T$ denotes the premise variable, and A_{l_i}, B_{l_i}, M_{l_i}, C_{l_i}, and D_{l_i} are the system matrices with appropriate dimensions. The nonlinear multi-agent dynamics is given by

$$\begin{aligned} x_i(k+1) = {} & \sum_{l_i=1}^r g_{l_i}(\theta_i(k)) A_{l_i} x_i(k) + \Delta f_i(x_i(k)) + \sum_{l_i=1}^r g_{l_i}(\theta_i(k)) B_{l_i} u_i(k) \\ & + \sum_{l_i=1}^r g_{l_i}(\theta_i(k)) M_{li} \omega_i(k) + \Delta I_i(x_i(k)) \omega_i(k) \\ y_i(k) = {} & \sum_{l_i=1}^r g_{l_i}(\theta_i(k)) C_{l_i} x_i(k) + \Delta h_i(x_i(k)) \\ & + \sum_{l_i=1}^r g_{l_i}(\theta_i(k)) D_{li} v_i(k) + \Delta F_i(x_i(k)) v_i(k), \end{aligned} \tag{4}$$

where $g_{l_i}(\theta_i(k)) = \psi_{l_i}(\theta_i(k)) / \sum_{l_i=1}^r \psi_{l_i}(\theta_i(k))$ is the normalized weight for each rule with $\psi_{l_i}(\theta_i(k)) = \Pi_{v=1}^q \mu_{l_iv}(\theta_{iv}(k)) \geqslant 0$ and $\sum_{l_i=1}^r g_{l_i}(\theta_i(k)) = 1$, where $\mu_{l_iv}(\theta_{iv}(k))$ is the grade of membership of $\theta_{iv}(k)$ in μ_{l_iq} and

$$\begin{aligned} \Delta f_i(x_i(k)) &= f_i(x_i(k)) - \sum_{l_i=1}^r g_{l_i}(\theta_i(k)) A_{l_i} x_i(k) \\ \Delta I_i(x_i(k)) &= I_i(x_i(k)) - \sum_{l_i=1}^r g_{l_i}(\theta_i(k)) M_{l_i} \\ \Delta h_i(x_i(k)) &= h_i(x_i(k)) - \sum_{l_i=1}^r g_{l_i}(\theta_i(k)) C_{l_i} x_i(k) \\ \Delta F_i(x_i(k)) &= F_i(x_i(k)) - \sum_{l_i=1}^r g_{l_i}(\theta_i(k)) D_{l_i} \end{aligned} \tag{5}$$

denote the approximation (or interpolation) errors between the nonlinear system and the fuzzy model.

Assumption 2. In order to fully use the advantage of employing the fuzzy model [17] for the nonlinear system, we assume

$$\begin{aligned}\Delta f_i\left(x_i(k)\right) &= H_{i,1}\Delta_{i,1}E_{i,1}x_i(k), \quad \Delta l_i\left(x_i(k)\right) = H_{i,2}\Delta_{i,2}E_{i,2}\\ \Delta h_i\left(x_i(k)\right) &= H_{i,3}\Delta_{i,3}E_{i,3}x_i(k), \quad \Delta F_i\left(x_i(k)\right) = H_{i,4}\Delta_{i,4}E_{i,4},\end{aligned} \tag{6}$$

where for $d = 1,\dots,4$, $H_{i,d}$ and $E_{i,d}$ are known matrices, and $\Delta_{i,d}$ are unknown, but bounded, with $\left\|\Delta_{i,d}\right\| \le 1$.

In this paper, we developed the fuzzy-based leader-following consensus protocol that utilizes the estimated state instead of the full system state. Consider the leader agent's dynamics that is given by the following IF-THEN rules:
Plant Rule l_i : IF $\theta_{i,1}(k)$ is $\mu_{l_i,1}$ and $\theta_{i,2}(k)$ is $\mu_{l_i,2}\dots$ and $\theta_{i,q}(k)$ is $\mu_{l_i,q}$, THEN

$$x^l(k+1) = A^l_{l_i}x^l(k), \tag{7}$$

where $x^l(k) \in \mathbb{R}^{n_x}$ is the state of the leader, and $A^l_{l_i}$ are the system matrices with appropriate dimensions. The leader often acts as a command generator, providing followers with a reference state. Consequently, the state of the leader may change irrespective of the state of the followers. It can be assumed, without loss of generality, that the leader's movement is not affected by UBB process noise, but it is deterministic to the followers since some of them receive information from the leader. Also, it is assumed that the leader does not have any inputs in order to reduce the complexity of the method. The above-mentioned system can be inferred as:

$$x^l(k+1) = \sum_{l_i=1}^{r} g_{l_i}\left(\theta_i(k)\right)A^l_{l_i}x^l(k). \tag{8}$$

Assumption 3. The initial states $x_i(0)$ and $x^l(0)$ belong to a given ellipsoid

$$\begin{aligned}\mathscr{X}_i(0\mid 0) &\triangleq \left\{x_i(0) : \left(x_i(0)-\hat{x}_i(0\mid 0)\right)^{\mathrm{T}} P_i(0\mid 0)^{-1}\left(x_i(0)-\hat{x}_i(0\mid 0)\right) \le 1\right\}\\ \mathscr{U}_i(0) &\triangleq \left\{x_i(0) : \left(x_i(0)-x^l(0)\right)^{\mathrm{T}} U_i(0)^{-1}\left(x_i(0)-x^l(0)\right) \le 1\right\},\end{aligned} \tag{9}$$

where $\hat{x}_i(0\mid 0)$ is the given estimate of $x_i(0)$, and $P_i(0\mid 0) = P_i(0\mid 0)^{\mathrm{T}} \succ 0$ and $U_i(0\mid 0) = U_i(0\mid 0)^{\mathrm{T}} \succ 0$ are known matrices.

We propose a distributed attack detector using set-membership fuzzy filtering to detect cyberattacks on a class of nonlinear multi-agent systems. The modules are tasked to detect attacks, as well as to ensure that the desired control specifications are satisfied. Also, the method can recover the system's performance and mitigate the effects of the attacks. The structure of the system with the detector is shown in Fig. 1.

III. Consensus Protocol and Fuzzy-Based Set-Membership Estimation

A. Prediction Step

The prediction filter is considered in the following form:
Plant Rule l_i : IF $\hat{\theta}_{i,1}(k)$ is $\mu_{l_i,1}$ and $\hat{\theta}_{i,2}(k)$ is $\mu_{l_i,2}\dots$ and $\hat{\theta}_{i,q}(k)$ is $\mu_{l_i,q}$, THEN

$$\hat{x}_i(k+1\mid k) = \hat{A}_{l_i}\hat{x}_i(k\mid k), \tag{10}$$

where $\hat{x}_i(k\mid k)$ is the estimation of the state $x_i(k)$, $\hat{A}_{l_i}$ is the fuzzy filter parameter to be determined, and $\hat{\theta}_i(k) = \left\{\hat{\theta}_{i,1}(k), \hat{\theta}_{i,2}(k), \dots, \hat{\theta}_{i,q}(k)\right\}$ are premise variables, which are functions of the state estimates. The overall fuzzy filter can be written as [24], [25]

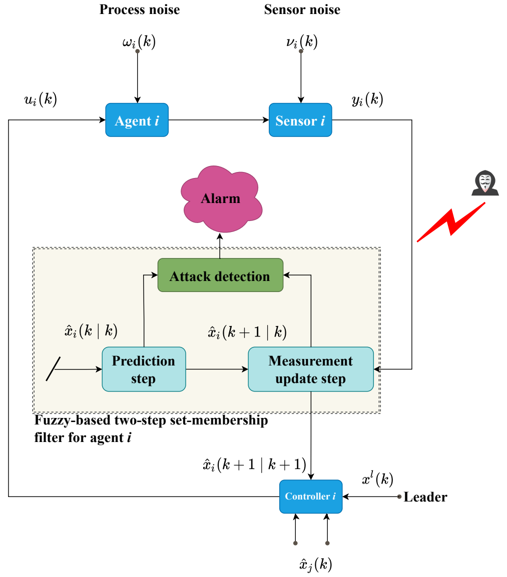


Fig. 1. The structure of a leader-following MAS with a fuzzy-based set-membership filtering detection method.

$$\hat{x}_i(k+1\mid k) = \sum_{l_i=1}^{r} g_{l_i}\left(\hat{\theta}_i(k)\right)\hat{A}_{l_i}\hat{x}_i(k\mid k). \tag{11}$$

For the given state estimation ellipsoid set $\mathscr{X}_i(k\mid k)$, with the center $\hat{x}_i(k\mid k)$ and the shape matrix $\Xi_i(k\mid k)$, the state $x_i(k)$ is given by

$$x_i(k) = \hat{x}_i(k\mid k) + \Xi_i(k\mid k)z_i. \tag{12}$$

Our goal is to obtain the prediction ellipsoid set

$$\begin{aligned}\mathscr{X}_i(k+1\mid k) \triangleq \Big\{x_i(k+1) : &\left(x_i(k+1)-\hat{x}_i(k+1\mid k)\right)^{\mathrm{T}} P_i^{-1}(k+1\mid k)\\ &\times \left(x_i(k+1)-\hat{x}_i(k+1\mid k)\right) \le 1\Big\}.\end{aligned} \tag{13}$$

Note that the state $x_i(k+1)$ belongs to such an ellipsoid set for any value of the system noise in their specified sets.

B. Measurement Update Step

The update, based on the current measurement, for the system (4) is given by
Plant Rule l_i : IF $\hat{\theta}_{i,1}(k)$ is $\mu_{l_i,1}$ and $\hat{\theta}_{i,2}(k)$ is $\mu_{l_i,2}\dots$ and $\hat{\theta}_{i,q}(k)$ is $\mu_{l_i,q}$, THEN

$$\hat{x}_i(k+1\mid k+1) = \hat{x}_i(k+1\mid k) + L_{l_i}\left(y_i(k+1) - \hat{y}_i(k+1\mid k)\right), \tag{14}$$

where L_{l_i} is the filter parameter to be determined. The overall fuzzy update can be written as

$$\begin{aligned}\hat{x}_i(k+1\mid k+1) = &\hat{x}_i(k+1\mid k) + \sum_{l_i=1}^{r} g_{l_i}\left(\hat{\theta}_i(k)\right)L_{l_i}\\ &\times \left(y_i(k+1) - \hat{y}_i(k+1\mid k)\right).\end{aligned} \tag{15}$$

According to the prediction ellipsoid set $\mathscr{X}_i(k+1\mid k)$, given by (13), the state $x_i(k+1)$ is given by

$$x_i(k+1) = \hat{x}_i(k+1\mid k) + \Xi_i(k+1\mid k)z_i. \tag{16}$$

The objective is to update this prediction set with the one yielding from the current measurement $y_i(k+1)$. In other words, we look for an updated ellipsoid set $\mathscr{X}_i(k+1 \mid k+1)$, with the center $\hat{x}_i(k+1 \mid k+1)$ and the shape matrix $\Xi_i(k+1 \mid k+1)$ for the state $x_i(k+1)$, given by the current measurement information at the time instant $k+1$. Thus, the updated ellipsoid set satisfies the following

$$\begin{aligned}(x_i(k+1)-\hat{x}_i(k+1 \mid k+1))^{\mathrm{T}} P_i^{-1}(k+1 \mid k+1)&\\ \times (x_i(k+1)-\hat{x}_i(k+1 \mid k+1)) \leq 1,&\end{aligned} \tag{17}$$

whenever the output constraint

$$\begin{aligned} y_i(k+1) = &\sum_{l_i=1}^{r} g_{l_i}\left(\theta_i(k)\right) C_{l_i}\left(\hat{x}_i(k+1 \mid k)+\Xi_i(k+1 \mid k) z_i\right) \\ &+ H_{i,3} \Delta_{i,3} E_{i,3}\left(\hat{x}_i(k+1 \mid k)+\Xi_i(k+1 \mid k) z_i\right) \\ &+\left(\sum_{l_i=1}^{r} g_{l_i}\left(\theta_i(k)\right) D_{l_i}+H_{i,4} \Delta_{i,4} E_{i,4}\right) v_i(k+1)\end{aligned} \tag{18}$$

holds for some $\|z_i\| \leq 1$.

C. Leader-Following Consensus Protocol

The distributed, observer-based, leader-following consensus protocol [26] in which the estimated states instead of the full system states are used can be expressed as

$$u_i(k) = K_{l_i}\left(\sum_{j \in \mathscr{N}_i} a_{ij}\left(\hat{x}_i(k \mid k)-\hat{x}_j(k \mid k)\right)+\lambda_i\left(\hat{x}_i(k \mid k)-x^l(k)\right)\right), \tag{19}$$

where K_{l_i} are constant matrices to be designed and $\lambda_i >= 0$ are pinning gains of protocol i in which $\lambda_i > 0$ if follower i receives information from the leader, otherwise $\lambda_i = 0$.

The leader-following multi-agent system (1), (7) achieves set-membership leader-following consensus under protocol (19) and two-step filter (11), (15), if the existence of desired gain sequences $K_{l_i}, \hat{A}_{l_i}$, and L_{l_i} can guarantee that the one step ahead states $x_i(k+1), \forall i \in \nu$ for all the followers, reside in a leader state ellipsoid $\mathscr{U}_i(k+1)$, enclosing all the followers' true states

$$\begin{aligned}\mathscr{U}_i(k+1) \triangleq \Big\{x_i(k+1): &\left(x_i(k+1)-x^l(k+1)\right)^T U^{-1}(k+1)\\ &\times\left(x_i(k+1)-x^l(k+1)\right) \leq 1\Big\}.\end{aligned} \tag{20}$$

For the given leader ellipsoid set $\mathscr{U}_i(k)$, with the center $x^l(k)$ and the shape matrix $\xi_i(k)$, the state $x_i(k)$ can be described by

$$x_i(k) = x^l(k)+\xi_i(k) z_i. \tag{21}$$

IV. Attack Detection Using Set-Membership Fuzzy Filtering

Here we describe the proposed cyberattack detection using a set-membership filter.

A. The Prediction Ellipsoid Set Design Based on Leader-Following Consensus

First, we developed the prediction ellipsoidal sets and the leader ellipsoidal sets based on the leader-following consensus protocol (19).

Theorem 1. Consider the leader-following multi-agent system (1), (7) that satisfies Assumptions 1 – 3. Suppose that the state $x_i(k)$ belongs to its state estimation ellipsoid $(x_i(k)-\hat{x}_i(k \mid k))^{\mathrm{T}} P_i^{-1}(k \mid k)(x_i(k)-\hat{x}_i(k \mid k)) \leq 1$ and leader state ellipsoid $\left(x_i(k)-x^l(k)\right)^{\mathrm{T}} U_i^{-1}(k)\left(x_i(k)-x^l(k)\right) \leq 1$. Then, the one-step ahead state $x_i(k+1)$ resides in its state prediction ellipsoid $(x_i(k+1)-\hat{x}_i(k+1 \mid k))^{\mathrm{T}} P_i^{-1}(k+1 \mid k)(x_i(k+1)-\hat{x}_i(k+1 \mid k)) \leq 1$ as well as leader state ellipsoid $\left(x_i(k+1)-x^l(k+1)\right)^{\mathrm{T}} U_i^{-1}(k+1)\left(x_i(k+1)-x^l(k+1)\right) \leq 1$, if there exist $P_i(k+1 \mid k) > 0, U_i(k+1) > 0, \hat{A}_{l_i}, K_{li}, \tau_{i,m}(k) \geq 0$, for $m = 1, \ldots, 10$, such that the linear matrix inequalities (LMI)

$$\begin{bmatrix} -P_i(k+1 \mid k) & \Gamma_{i,1,l_i j_i} \\ \Gamma_{i,1,l_i j_i}^{\mathrm{T}} & -\Theta_{i,1}(k) \end{bmatrix} \leq 0, \begin{bmatrix} -U_i(k+1) & \Gamma_{i,2,l_i} \\ \Gamma_{i,2,l_i}^{\mathrm{T}} & -\Theta_{i,2}(k) \end{bmatrix} \leq 0 \tag{22}$$

hold for all $l_i, j_i = 1, \ldots, r$, where

$$\begin{aligned}
\Gamma_{i,1,l_i j_i} &= \begin{bmatrix} P_{i,1,l_i,j_i} & A_{l_i}\Xi_i(k \mid k) & M_{l_i} & H_{i,1} & H_{i,1} & H_{i,2} \end{bmatrix}\\
P_{i,1,l_i,j_i} &= \left(A_{l_i}-\hat{A}_{j_i}\right)\hat{x}_i(k \mid k)-B_{l_i}K_{l_i}\lambda_i x^l(k)+B_{l_i}K_{l_i}\sum_{j=1}^{N}\tilde{l}_{ij}\hat{x}_j(k \mid k)\\
\Theta_{i,1}(k) &= \operatorname{diag}\{1-\tau_{i,1}(k)-\tau_{i,2}(k)-\tau_{i,3}(k)\hat{x}_i^T(k \mid k)E_{i,1}^T E_{i,1}\hat{x}_i(k \mid k),\\
&\quad \tau_{i,1}(k)I-\tau_{i,4}(k)\Xi_i^T(k \mid k)E_{i,1}^T E_{i,1}\Xi_i(k \mid k), \tau_{i,2}(k)Q_i^{-1}(k)\\
&\quad -\tau_{i,5}(k)E_{i,2}^T E_{i,2}, \tau_{i,3}(k)I, \tau_{i,4}(k)I, \tau_{i,5}(k)I\}\\
\Gamma_{i,2,l_i} &= \begin{bmatrix} P_{i,2,l_i} & A_{l_i}\xi_i(k) & M_{l_i} & H_{i,1} & H_{i,1} & H_{i,2} \end{bmatrix}\\
P_{i,2,l_i} &= \left(A_{l_i}+A_{li}^l-B_{l_i}K_{l_i}\lambda_i\right)x^l(k)+B_{l_i}K_{l_i}\sum_{j=1}^{N}\tilde{l}_{ij}\hat{x}_j(k \mid k)\\
\Theta_{i,2}(k) &= \operatorname{diag}\{1-\tau_{i,6}(k)-\tau_{i,7}(k)-\tau_{i,8}(k)\hat{x}_i^T(k \mid k)E_{i,1}^T E_{i,1}\hat{x}_i(k \mid k),\\
&\quad \tau_{i,6}(k)I-\tau_{i,9}(k)\Xi_i^T(k \mid k)E_{i,1}^T E_{i,1}\Xi_i(k \mid k), \tau_{i,7}(k)Q_i^{-1}(k)\\
&\quad -\tau_{i,10}(k)E_{i,2}^T E_{i,2}, \tau_{i,8}(k)I, \tau_{i,9}(k)I, \tau_{i,10}(k)I\}\\
\tilde{\mathscr{L}} &= \mathscr{L}+\Lambda = \left[\tilde{l}_{ij}\right]_{N\times N}, \quad \Lambda = \operatorname{diag}\{\lambda_1, \lambda_2, \ldots, \lambda_N\}.
\end{aligned} \tag{23}$$

Proof. For the detailed proof, please see Appendix A. □

According to Theorem 1, in order to find the optimal state prediction ellipsoid containing $x_i(k+1)$, the convex optimization is carried out:

$$\min_{\substack{P_i(k+1|k), U_i(k+1), \hat{A}_{li}(k), K_{li},\\ \tau_{i,1}(k), \tau_{i,2}(k), \tau_{i,3}(k), \tau_{i,4}(k), \tau_{i,5}(k),\\ \tau_{i,6}(k), \tau_{i,7}(k), \tau_{i,8}(k), \tau_{i,9}(k), \tau_{i,10}(k)}} \operatorname{Tr}\left(T_i(k+1 \mid k)\right) \tag{24}$$

subject to (22), for all $l_i, j_i = 1, \ldots, r$ in which the trace of $T_i(k+1 \mid k) = \operatorname{diag}\{U_i(k+1), P_i(k+1 \mid k)\}$.

B. Update Prediction Ellipsoid Set With Current Measurement

Here, we present a scheme to determine the shape matrix $\Xi_i(k+1 \mid k+1)$ and the filter gain $L_{l_i}(k+1)$ with the output constraint (18).

Theorem 2. Consider the leader-following multi-agent system (1), (7) that satisfies Assumptions 1-3. If the state $x_i(k+1)$ belongs to its state prediction ellipsoid $(x_i(k+1)-\hat{x}_i(k+1 \mid k))^{\mathrm{T}} P_i^{-1}(k+1 \mid k)(x_i(k+1)-\hat{x}_i(k+1 \mid k)) \leq 1$, then such a state also resides in its updated state estimation ellipsoid $\left(x_i(k+1)-\hat{x}_i^{\mathrm{T}}(k+1 \mid k+1)\right) P_i^{-1}(k+1 \mid k+1)(x_i(k+1)-\hat{x}_i(k+1 \mid k+1)) \leq 1$, with the center determined by (14), where $P_i(k+1 \mid k+1) > 0$ satisfies the matrix inequality

$$\begin{bmatrix} -P_i(k+1 \mid k+1) & \Gamma_{i,3,l_i j_i} \\ \Gamma^{\mathrm{T}}_{i,3,l_i j_i} & -\Theta_{i,4}(k) \end{bmatrix} \leq 0, \tag{25}$$

$$\begin{aligned}
&\Gamma_{i,3,li j_i} = \begin{bmatrix} 0 & P_{i,2,l_i,j_i} & -L_{j_i}D_{li} & -L_{j_i}H_{i,3} & -L_{j_i}H_{i,3} & -L_{j_i}H_{i,4} \end{bmatrix} \\
&P_{i,2,l_i,j_i} = (I - L_{j_i}C_{li})\,\Xi_i(k+1 \mid k) \\
&\Theta_{i,4}(k) = \Theta_{i,3}(k) - Z_i^{\mathrm{T}}(k+1)\Gamma_{l_i y_i}(\hat{x}_i(k+1 \mid k)) \\
&\qquad - \Gamma^{\mathrm{T}}_{l_i y_i}(\hat{x}_i(k+1 \mid k))\,Z_i(k+1) \\
&\Theta_{i,3}(k) = \mathrm{diag}\{1 - \tau_{i,11}(k) - \tau_{i,12}(k) - \tau_{i,13}(k)\hat{x}_i^T(k+1 \mid k)E_{i,3}^T \\
&\qquad \times E_{i,3}\hat{x}_i(k+1 \mid k), \tau_{i,11}(k)I - \tau_{i,14}(k)\Xi_i^T(k+1 \mid k)E_{i,3}^T \\
&\qquad \times E_{i,3}\Xi_i(k+1 \mid k), \tau_{i,12}(k)R_i^{-1}(k+1) - \tau_{i,15}(k)E_{i,4}^T E_{i,4}, \\
&\qquad \tau_{i,13}(k)I, \tau_{i,14}(k)I, \tau_{i,15}(k)I\} \\
&\Gamma_{l_i y_i}(\hat{x}_i(k+1 \mid k)) = \begin{bmatrix} P_{l_i y_i,1} & P_{l_i y_i,2} & D_{l_i} & H_{i,3} & H_{i,3} & H_{i,4} \end{bmatrix} \\
&P_{l_i y_i,1} = C_{l_i}\hat{x}_i(k+1 \mid k) - y_i(k+1), \quad P_{l_i y_i,2} = C_{l_i}\Xi_i(k+1 \mid k).
\end{aligned} \tag{26}$$

Proof. For detailed proof, see Appendix B. □

The convex optimization approach is applied to determine an optimal ellipsoid with a minimal size, and $P_i(k+1 \mid k+1)$ is obtained by solving the following optimization problem:

$$\min_{\substack{P_i(k+1|k+1), L_{li}(k+1), \\ \tau_{i,11}(k), \tau_{i,12}(k), \tau_{i,13}(k), \\ \tau_{i,14}(k), \tau_{i,15}(k), Z_i(k+1)}} \mathrm{Tr}\left(P_i(k+1 \mid k+1)\right) \tag{27}$$

subject to (25).

C. Recursive Algorithm For Attack Detection

The recursive algorithm, based on the set-membership filtering, which computes the state ellipsoids such that a cyberattack can be detected, is summarized below. Algorithm 1 recursively computes the prediction ellipsoid $\mathscr{X}_i(k+1 \mid k)$ and its update $\mathscr{X}_i(k+1 \mid k+1)$ with the current measurement $y_i(k+1)$. Step 4 of the algorithm is proposed to detect cyberattacks that affect sensor measurements.

Remark 1. The optimization problems specified by (24) and (27) are based on linear matrix inequalities (LMIs) (22) and (25), as described in Theorem 1 and Theorem 2. These LMIs are linear with respect to variables such as $P_i(k+1 \mid k)$, $U_i(k+1)$, $P_i(K+1 \mid K+1)$, $\hat{A}_{l_i}(k)$, K_{l_i}, $L_{l_i}(k+1)$, $Z_i(k+1)$, and $\tau_{i,m}(k)$, where m ranges from 1 to 15. To solve these optimization problems, semidefinite programming and an interior-point algorithm can be utilized at each time step. The interior-point algorithm used in this process has a computational complexity of $O\left(\ell \mathscr{M}^3\right)$, where ℓ is the total row size of the main LMIs and $\mathscr{M}$ is the number of scalar decision variables in the main LMIs ((22) and (25)). The complexity of the solution depends on variables such as n_x, n_u, n_y, n_w, n_v, which correspond to the number of elements in each subscript.

Remark 2. We have shown that the optimal ellipsoidal sets can be determined by the feasibility problem of recursive LMIs, (22) and (25). A system not under attack has an intersection of the two sets, which means that the resulting intersection set is not empty since they both contain the true state $x(k+1)$. However, if there is an attack on the sensor measurement, the sensor $y(k+1)$ is affected. As a result, the center of the estimation ellipsoid set has been affected by the attack, and this set may not contain the true state. Because of the attacks impacting the center of the estimation ellipsoid set, it follows that the ellipsoidal sets do not intersect, which means that the resulting intersection set is empty, and Theorem 1 and Theorem 2 may be infeasible. This situation can be overcome by taking step 5. By modifying the ellipsoidal sets, they become free of attacks for their subsequent steps in Algorithm 1. As a result, the proposed LMI problems are kept feasible at each time step.

Remark 3. Note that if an attacker causes a relatively small abrupt change, then a proposed detection algorithm cannot detect it since an intersection may occur between the two ellipsoidal sets until the measurement output deviates enough and reaches a threshold such that there is no intersection between the two ellipsoid sets. However, the size of the ellipsoid sets, and thus the threshold of the attack detection algorithm, is minimized by solving optimization problems (24) and (27). Hence, our proposed attack detection algorithm is optimized to minimize the damages inflicted by attacks that a resilient control algorithm may tolerate.

V. Simulation Results

We consider the following multi-agent, discrete-time, nonlinear system:

$$\begin{aligned}
&x_{1,1}(k+1) = 0.2x_{1,1}(k) - 0.3\left(x_{1,2}(k) - (x_{1,1}(k))^2\right) + u_1(k) + \omega_1(k) \\
&x_{1,2}(k+1) = 0.3x_{1,1}(k) + 0.2\left(x_{1,2}(k) - (x_{1,1}(k))^2\right) + u_1(k) + \omega_1(k) \\
&y_1(k) = x_{1,1}(k) + 0.1(x_{1,1}(k))^2 + x_{1,2}(k) + v_1(k) \\
&x_{2,1}(k+1) = 0.5x_{2,1}(k) - 0.1\left(x_{2,2}(k) - (x_{2,1}(k))^2\right) + u_2(k) + \omega_2(k) \\
&x_{2,2}(k+1) = 0.9x_{2,1}(k) + 0.5\left(x_{2,2}(k) - (x_{2,1}(k))^2\right) + u_2(k) + \omega_2(k) \\
&y_2(k) = x_{2,1}(k) + 0.1(x_{2,1}(k))^2 + x_{2,2}(k) + v_2(k), \\
&x_{3,1}(k+1) = 0.4x_{3,1}(k) - 0.6\left(x_{3,2}(k) - (x_{3,1}(k))^2\right) + u_1(k) + \omega_1(k) \\
&x_{3,2}(k+1) = 0.5x_{3,1}(k) + 0.3\left(x_{3,2}(k) - (x_{3,1}(k))^2\right) + u_3(k) + \omega_1(k) \\
&y_3(k) = x_{3,1}(k) + 0.1(x_{3,1}(k))^2 + x_{3,2}(k) + v_3(k)
\end{aligned} \tag{28}$$

where for $i \in \{1,2,3\}$, the state is $x_i(k) = [x_{i,1}(k) \quad x_{i,2}(k)]^T$. We construct the following fuzzy models to approximate the above nonlinear multi-agent system for each agent:

Agent i:

- Rule 1: IF $x_{i,1}(k)$ is about 1,THEN

$$\begin{aligned} x_i(k+1) &= A_{i,1}x_i(k) + B_{i,1}u_i(k) + M_{i,1}\omega_i(k) \\ y_i(k) &= C_{i,1}x_i(k) + D_{i,1}v_i(k), \end{aligned} \tag{29}$$

- Rule 2: IF $x_{i,1}(k)$ is about 0, THEN

$$\begin{aligned} x_i(k+1) &= A_{i,2}x_i(k) + B_{i,2}u_i(k) + M_{i,2}\omega_i(k) \\ y_i(k) &= C_{i,2}x_i(k) + D_{i,2}v_i(k), \end{aligned} \tag{30}$$

where

$$\begin{aligned}
A_{1,1} &= \begin{bmatrix} 0.5 & -0.3 \\ 0.1 & 0.2 \end{bmatrix} \quad A_{2,1} = \begin{bmatrix} 0.6 & -0.1 \\ 0.4 & 0.5 \end{bmatrix} \quad A_{3,1} = \begin{bmatrix} 1 & -0.6 \\ 0.2 & 0.5 \end{bmatrix} \\
B_{i,1} &= \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad M_{i,1} = 1 \quad C_{i,1} = \begin{bmatrix} 1.1 & 1 \end{bmatrix} \quad D_{i,1} = 1 \\
A_{1,2} &= \begin{bmatrix} 0.2 & -0.3 \\ 0.3 & 0.2 \end{bmatrix} \quad A_{2,2} = \begin{bmatrix} 0.5 & -0.1 \\ 0.9 & 0.5 \end{bmatrix} \quad A_{3,2} = \begin{bmatrix} 0.4 & -0.6 \\ 0.5 & 0.3 \end{bmatrix} \\
B_{i,2} &= \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad M_{i,2} = 1 \quad C_{i,2} = \begin{bmatrix} 1.0 & 1.0 \end{bmatrix} \quad D_{i,2} = 1.
\end{aligned} \tag{31}$$

For the convenience of implementation, triangular member-

```
Algorithm 1 Recursive State Estimation
1. Initialization:
    Given an initial ellipsoid $\mathscr{X}_i(0 \mid 0), \mathscr{U}_i(0)$, recursive times $T_N$, and set $k=0$. Let $x_i(k)=x_i(0), \hat{x}_i(k \mid k)=\hat{x}_i(0 \mid 0), \Xi_i(k \mid k)=\Xi_i(0 \mid 0), x^l(k)=x^l(0)$, and $\xi_i(k)=\xi_i(0)$.
2. Prediction:
    1) Calculate $P_i(k+1 \mid k), U_i(k+1), \hat{A}_{l_i}(k), K_{l_i}$ by solving the optimization problem (24).
    2) Obtain the matrix $\Xi_i(k+1 \mid k)$, and $\xi_i(k+1 \mid k)$ according to $P_i(k+1 \mid k)=\Xi_i(k+1 \mid k)\Xi_i^{\mathrm{T}}(k+1 \mid k)$, and $U_i(k+1)=\xi_i(k+1)\xi_i^{\mathrm{T}}(k+1)$.
    3) Calculate the centre of the prediction ellipsoid $\hat{x}_i(k+1 \mid k)$ by (10).
3. Measurement Update:
    1) Calculate $P_i(k+1 \mid k+1)$ and $L_{l_i}(k+1)$ by solving the optimization problem (27).
    2) Obtain the new $\Xi_i(k+1 \mid k+1)$ according to $P_i(k+1 \mid k+1)=\Xi_i(k+1 \mid k+1)\Xi_i^{\mathrm{T}}(k+1 \mid k+1)$.
    3) Calculate the centre of the updated estimation ellipsoid $\hat{x}_i(k+1 \mid k+1)$ by (14).
4. Attack Detection: Sensor Measurement Data Cyber Attack Detection
    1) If $\mathscr{X}_i(k+1 \mid k+1) \bigcap \mathscr{X}_i(k+1 \mid k) \neq \varnothing$, there is no attack and go to step 6.
    2) If $\mathscr{X}_i(k+1 \mid k+1) \bigcap \mathscr{X}_i(k+1 \mid k) = \varnothing$, data is subject to attack and go to step 7.
5. Recovery Step and Attack Mitigation:
    Set $\mathscr{X}_i(k+1 \mid k+1) \leftarrow \mathscr{X}_i(k+1 \mid k), y_i(k+1) \leftarrow y_i(k)$ and go to step 6.
6. Loop:
    If $k == T_N$ then Exit, Else $k \leftarrow k+1$ and go to step 2.
```

ship functions are used for Rule 1 and Rule 2 in this example.

In the above fuzzy models, the approximation errors between the nonlinear system and the fuzzy models are assumed to satisfy (6), where $H_{1,1}=[0.1\ \ 0.1]^T$, $H_{2,1}=[0.3\ 0.3]^T$, $H_{3,1}=[0.2\ 0.2]^T$, $E_{1,1}=[0\ 0.5]$, $E_{2,1}=[0\ 0.6]$, $E_{3,1}=[0\ 0.4]$, $H_{i,2}=[0\ 0]^T$, $E_{i,2}=0$, $H_{i,3}=0.1$, $E_{i,3}=[0\ 0.5]$, $H_{i,4}=0$, $E_{i,4}=0$. The leader's matrices described in (8) are given by

$$A_1^l=\begin{bmatrix} 0.5 & 0.2 \\ -0.6 & 0.7 \end{bmatrix} \quad A_2^l=\begin{bmatrix} 0.5 & 0.2 \\ -0.4 & 0.7 \end{bmatrix}. \tag{32}$$

We have selected $\omega_i(k)=0.5\sin(2k)$ and $v_i(k)=0.5\sin(20k)$. The initial state is set as $x_i(0)=[0\ \ 0]^T$, which belongs to the ellipsoids $(x_i(0 \mid 0)-\hat{x}_i(0))^T P_i^{-1}(0 \mid 0)\,(x_i(0)-\hat{x}_i(0 \mid 0)) \leq 1$ and $\left(x_i(0)-x^l(0)\right)^T U_i^{-1}(0)\,(x_i(0)-x_l(0)) \leq 1$, where $\hat{x}_i(0)=x^l(0)=[1\ \ 1]^T$, and $P_i(0 \mid 0)=U_i(0)=diag\{100,100\}$, $Q_i(k)=1-k/50$, and $R_i(k)=1-k/50$. The communication topology between the agents and the leader is shown in Fig. 2

We obtained the simulation results using MATLAB 9.8 with YALMIP and SDPT3. We considered the following two scenarios in 50 sampling steps.

A. Attack Free System

In this case, the prediction ellipsoid set and the updated estimation ellipsoid set always have intersections. Fig. 3 (a) shows the existence of the intersection at $k=22$ between these sets for Agent 1.

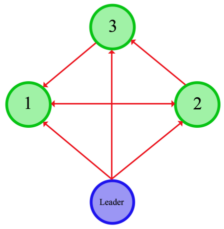
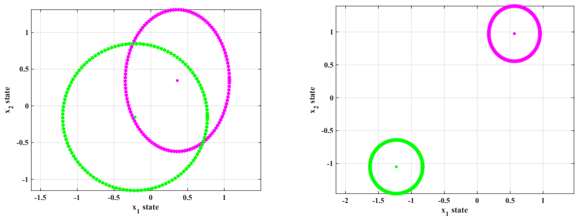


Fig. 2. Multi-agent system with a leader.



(a) Agent 1

(b) Agent 3

Fig. 3. Prediction ellipsoid $\mathscr{X}_i(k+1 \mid k)$ (pink) and the updated estimation ellipsoid $\mathscr{X}_i(k+1 \mid k+1)$ (green).

B. Replay Attacks on Sensor Data

A successful replay attack does not need an a priori knowledge of the system components. It is assumed that the attacker can record the sensor's measurement data from k_i until k_r, with the window size $\tau=k_r-k_i$ in the first phase. Then, in the second phase, the attacker replays the recorded data to the system from $k=k_r+d$ until the end of the attack at $k=k_f$, where d is the delay between the recording time and replaying time. We model the attack as [9]

$$a^{y_i}(k)=y_i(k-\tau)-y_i(k). \tag{33}$$

Thus, the sensor's data affected by the attack are

$$\tilde{y}_i(k)=y_i(k)+a^{y_i}(k). \tag{34}$$

We assume that the attacker records the data from $k=5$ to $k=10$ and replaces the sensor data from $k=20$ to $k=25$ with them. Fig. 3(b) confirms that the prediction ellipsoid set and the updated measurement set for the current time instant do not have an intersection during this attack period. We show only the result for one agent because of the space constraint. The figure shows the results at $k=23$.

Finally, Fig. 4 illustrates the leader-following consensus in the attack-free system and in the presence of replay attacks.

VI. Conclusion

In this paper, we studied cyberattack detection in discrete-time, leader-following, nonlinear multi-agent systems subject to UBB system noise. For the approximation of the nonlinear systems over the true value of the state, the T-S fuzzy model has been used. A new fuzzy set-membership filtering method was developed for each agent to detect cyberattacks at the time of their occurrence. We developed a method for detecting cyberattacks that inject a malicious signal into sensor data and affect the leader-following consensus. We proposed recursive algorithms to achieve the consensus protocol and find the two ellipsoid sets for attack detection based on their intersection. Furthermore, the proposed method can recover the system's performance and mitigate the effects of the attacks. Finally, simulation results have been provided to demonstrate the effectiveness of the proposed method.

APPENDIX

A. Proof of Theorem 1

Proof. From the system model (4), (6), and (7) and the filter (11), (12), and (21), and by considering the fact that $\sum_{l_i=1}^{r} g_{l_i}(\theta_i(k)) = 1$, the errors $x_i(k+1) - \hat{x}_i(k+1 \mid k)$ and $x_i(k+1) - x^l(k+1 \mid k)$ can be written in compact forms as

$$\begin{aligned} x_i(k+1) - \hat{x}_i(k+1 \mid k) &= \sum_{l_i=1}^{r} g_{l_i}(\theta_i(k)) \sum_{j_i=1}^{r} g_{j_i}\left(\hat{\theta}_i(k)\right) \Gamma_{i,1,l_i j_i} \eta_{i,1}(k), \\ x_i(k+1) - x^l(k+1) &= \sum_{l_i=1}^{r} g_{l_i}(\theta_i(k)) \sum_{j_i=1}^{r} \Gamma_{i,2,l_i} \eta_{i,1}(k). \end{aligned} \tag{35}$$

where

$$\eta_{i,1}(k) = \begin{bmatrix} 1 & z_i & \omega_i(k) & q_{i,1} & q_{i,2} & q_{i,3} \end{bmatrix}^T, \tag{36}$$

and

$$\begin{aligned} q_{i,1} &= \Delta_{i,1} E_{i,1} \hat{x}_i(k \mid k) \\ q_{i,2} &= \Delta_{i,1} E_{i,1} \Xi_i(k \mid k) z_i \\ q_{i,3} &= \Delta_{i,2} E_{i,2} \omega_i(k). \end{aligned} \tag{37}$$

According to (35), one has

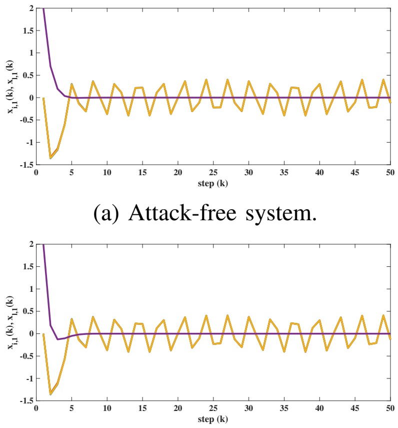
$$\begin{aligned} &(x_i(k+1) - \hat{x}_i(k+1 \mid k))^T P_i^{-1}(k+1 \mid k)(x_i(k+1) - \hat{x}_i(k+1 \mid k)) \\ &\quad \le \sum_{l_i=1}^{r} g_{l_i}(\theta_i(k)) \sum_{j_i=1}^{r} g_{j_i}\left(\hat{\theta}_i(k)\right) \eta_{i,1}^T(k) \Gamma_{i,1,l_i j_i}^T P_i^{-1}(k+1 \mid k) \\ &\quad\quad \times \Gamma_{i,1,l_i j_i} \eta_{i,1}(k), \\ &\left(x_i(k+1) - x^l(k+1)\right)^T U_i^{-1}(k+1)\left(x_i(k+1) - x^l(k+1)\right) \\ &\quad \le \sum_{l_i=1}^{r} g_{l_i}(\theta_i(k)) \eta_{i,1}^T(k) \Gamma_{i,2,l_i}^T U_i^{-1}(k+1) \Gamma_{i,2,l_i} \eta_{i,1}(k). \end{aligned} \tag{38}$$

The condition in (13) and (20) can be written as

$$\begin{aligned} &\eta_{i,1}^T(k)\left[\sum_{l_i=1}^{r} g_{l_i}(\theta_i(k)) \sum_{j_i=1}^{r} g_{j_i}\left(\hat{\theta}_i(k)\right) \Gamma_{i,1,l_i j_i}^T P_i^{-1}(k+1 \mid k) \Gamma_{i,1,l_i j_i}\right. \\ &\quad \left. - \operatorname{diag}\{1,0,0,0,0,0\}\right] \eta_{i,1}(k) \le 0. \\ &\eta_{i,1}^T(k)\left[\sum_{l_i=1}^{r} g_{l_i}(\theta_i(k)) \Gamma_{i,2,l_i}^T U_i^{-1}(k+1) \Gamma_{i,2,l_i} - \operatorname{diag}\{1,0,0,0,0,0\}\right] \\ &\quad \times \eta_{i,1}(k) \le 0. \end{aligned} \tag{39}$$

With $\|\Delta_{i,1}\| \le 1$, $\|\Delta_{i,2}\| \le 1$, and from (2), (12) and (37), the unknown z_i, $\omega_i(k)$, $q_{i,1}$, $q_{i,2}$, $q_{i,3}$ satisfy the following constraints

$$\begin{aligned} &\eta_{i,1}^T(k) \operatorname{diag}\{-1, I, 0,0,0,0\} \eta_{i,1}(k) \le 0 \\ &\eta_{i,1}^T(k) \operatorname{diag}\{-1, 0, Q_i^{-1}(k), 0,0,0\} \eta_{i,1}(k) \le 0 \\ &\eta_{i,1}^T(k) \operatorname{diag}\{-\hat{x}_i^T(k \mid k) E_{i,1}^T E_{i,1} \hat{x}_i(k \mid k), 0,0, I, 0,0\} \eta_{i,1}(k) \le 0 \\ &\eta_{i,1}^T(k) \operatorname{diag}\{0, -\Xi_i^T(k \mid k) E_{i,1}^T E_{i,1} \Xi_i(k \mid k), 0,0, I, 0\} \eta_{i,1}(k) \le 0. \\ &\eta_{i,1}^T(k) \operatorname{diag}\{0,0, -E_{i,2}^T E_{i,2}, 0,0, I\} \eta_{i,1}(k) \le 0. \end{aligned} \tag{40}$$



(a) Attack-free system.

(b) Replay attack on sensor data.

Fig. 4. Leader-following consensus of the agents $x_{i,1}$ and $x_{l,1}$, where $x_i = [x_{i,1} \quad x_{i,2}]$ and $x_l = [x_{l,1} \quad x_{l,2}]$ for all scenarios.

Applying S-procedure [23] to (39) and (40), and using Schur complements, we can conclude that the inequalities (39) hold if there exist nonnegative scalars $\tau_{i,m}(k)$, for $m = 1, \ldots, 10$, such that (22) holds.

According to the above discussion, if there exist $P_i(k+1 \mid k) > 0$, $U_i(k+1) > 0$, $\hat{A}_{l_i}$, K_{li}, $\tau_{i,m}(k) \ge 0$, for $m = 1, \ldots, 10$, such that (22) holds for all $l_i, j_i = 1, \ldots, r$, then

$$\begin{aligned} &\sum_{l_i=1}^{r} g_{l_i}(\theta_i(k)) \sum_{j_i=1}^{r} g_{j_i}\left(\hat{\theta}_i(k)\right) \eta_{i,1}^T(k) \Gamma_{i,1,l_i j_i}^T P_i^{-1}(k+1 \mid k) \Gamma_{i,1,l_i j_i} \eta_{i,1}(k) \le 1, \\ &\sum_{l_i=1}^{r} g_{l_i}(\theta_i(k)) \eta_{i,1}^T(k) \Gamma_{i,2,l_i}^T U_i^{-1}(k+1) \Gamma_{i,2,l_i} \eta_{i,1}(k) \le 1. \end{aligned} \tag{41}$$

Therefore, from (38), we obtain

$$\begin{aligned} &(x_i(k+1) - \hat{x}_i(k+1 \mid k))^{\mathrm{T}} P_i^{-1}(k+1 \mid k)(x_i(k+1) - \hat{x}_i(k+1 \mid k)) \le 1, \\ &\left(x_i(k+1) - x^l(k+1)\right)^{\mathrm{T}} U_i^{-1}(k+1)\left(x_i(k+1) - x^l(k+1)\right) \le 1, \end{aligned} \tag{42}$$

which completes the proof. □

B. Proof of Theorem 2

Proof. From the system (1), the prediction ellipsoid set (16), and the filter (15), the current estimation error $x_i(k+1) - \hat{x}_i(k+1 \mid k+1)$ can be written in a compact form

$$x_i(k+1) - \hat{x}_i(k+1 \mid k+1) = \sum_{l_i=1}^{r} g_{l_i}(\theta_i(k)) \sum_{j_i=1}^{r} g_{j_i}\left(\hat{\theta}_i(k)\right) \Gamma_{i,2,l_i j_i} \eta_{i,2}(k+1), \tag{43}$$

where

$$\eta_{i,2}(k+1) = \begin{bmatrix} 1 & z_i & v_i(k+1) & q_{i,4} & q_{i,5} & q_{i,6} \end{bmatrix}^T, \tag{44}$$

and

$$\begin{aligned} q_{i,4} &= \Delta_{i,3} E_{i,3} \hat{x}_i(k+1 \mid k) \\ q_{i,5} &= \Delta_{i,3} E_{i,3} \Xi_i(k+1 \mid k) z_i \\ q_{i,6} &= \Delta_{i,4} E_{i,4} v_i(k+1). \end{aligned} \tag{45}$$

Considering (43), one has

$$\begin{aligned} &(x_i(k+1) - \hat{x}_i(k+1 \mid k+1))^{\mathrm{T}} P_i^{-1}(k+1 \mid k+1) \\ &\quad \times (x_i(k+1) - \hat{x}_i(k+1 \mid k+1)) \\ &\le \sum_{l_i=1}^{r} g_{l_i}(\theta_i(k)) \sum_{j_i=1}^{r} g_{j_i}\left(\hat{\theta}_i(k)\right) \\ &\quad \eta_{i,2}^T(k+1) \Gamma_{i,3,l i j_i}^T \Gamma_{i,3,l i j_i} \eta_{i,2}(k+1) \end{aligned} \tag{46}$$

Therefore, the condition (17) in Section III-B is given by

$$\eta_{i,2}^{\mathrm{T}}(k+1)\left[\sum_{l_i=1}^{r} g_{l_i}\left(\theta_i(k)\right)\sum_{j_i=1}^{r} g_{j_i}\left(\hat{\theta}_i(k)\right)\Gamma_{i,3,l_ij_i}^{\mathrm{T}}P_i^{-1}(k+1\mid k+1)\Gamma_{i,3,l_ij_i} - \mathrm{diag}\{1,0,0,0,0,0\}\right]\eta_{i,2}(k+1)\le 0 \tag{47}$$

From (2), (16), and (45) the unknown z_i, $v_i(k+1)$, $q_{i,4}$, $q_{i,5}$, and $q_{i,6}$ satisfy the following constraints

$$\begin{aligned}
&\eta_{i,2}^{\mathrm{T}}(k+1)\,\mathrm{diag}\{-1,I,0,0,0,0\}\eta_{i,2}(k+1)\le 0\\
&\eta_{i,2}^{\mathrm{T}}(k+1)\,\mathrm{diag}\{-1,0,R_i^{-1}(k+1),0,0,0\}\eta_{i,2}(k+1)\le 1\\
&\eta_{i,2}^{\mathrm{T}}(k+1)\,\mathrm{diag}\{-\hat{x}_i^T(k+1\mid k)E_{i,3}^TE_{i,3}\hat{x}_i(k+1\mid k),\\
&\qquad\qquad 0,0,I,0,0\}\eta_{i,2}(k+1)\le 1\\
&\eta_{i,2}^{\mathrm{T}}(k+1)\,\mathrm{diag}\{0,-\Xi_i^T(k+1\mid k)E_{i,3}^TE_{i,3}\Xi_i(k+1\mid k),0,0,I,0\}\\
&\qquad\qquad \times\eta_{i,2}(k+1)\le 1\\
&\eta_{i,2}^{\mathrm{T}}(k+1)\,\mathrm{diag}\{0,0,-E_{i,4}^TE_{i,4},0,0,,I\}\eta_{i,2}(k+1)\le 1
\end{aligned} \tag{48}$$

By applying S-procedure to (47) and (48), we can conclude that the inequality (47) holds if there exist non-negative scalars $\tau_{i,11}(k)$, $\tau_{i,12}(k)$, $\tau_{i,13}(k)$, $\tau_{i,14}(k)$, $\tau_{i,15}(k)$ such that

$$\Gamma_{i,3,l_ij_i}^TP_i^{-1}(k+1\mid k+1)\Gamma_{i,3,l_ij_i}-\Theta_{i,3}(k)\le 0. \tag{49}$$

Now, we deal with the output constraint (18) in Section III-B. First, it can be described by

$$\Gamma_{l_iy_i}\left(\hat{x}_i(k+1\mid k)\right)\eta_{i,2}(k+1)=0. \tag{50}$$

By virtue of Finsler's lemma [27], the inequality (47) under constraint (50) holds if there exists a $Z_i(k+1)$ such that (25) holds.

According to the above discussion, if there exist $P_i(k+1\mid k+1)>0$, $L_{l_i}(k+1)$, $N_i(k+1)$, $\tau_{i,m}(k)\ge 0$, for $m=11,\dots,15$ such that (25) holds for all $l_i, j_i=1,\dots,r$, then we have

$$\sum_{l_i=1}^{r} g_{l_i}\left(\theta_i(k)\right)\sum_{j_i=1}^{r} g_{j_i}\left(\hat{\theta}_i(k)\right) \eta_{i,2}^{\mathrm{T}}(k+1)\Gamma_{i,3,l_ij_i}^{\mathrm{T}}P_i^{-1}(k+1\mid k+1)\Gamma_{i,3,l_ij_i}\eta_{i,2}(k+1)\le 1. \tag{51}$$

Therefore, from (46), we obtain

$$\begin{aligned}(x_i(k+1)\ &-\hat{x}_i(k+1\mid k+1))^{\mathrm{T}}P_i^{-1}(k+1\mid k+1)\\ &\times(x_i(k+1)-\hat{x}_i(k+1\mid k+1))\le 1,\end{aligned} \tag{52}$$

which completes the proof. □

REFERENCES

[1] J. Shamma, *Cooperative control of distributed multi-agent systems*. John Wiley & Sons, 2008.

[2] A. M. M. Sizkouhi, M. Rahimifard, and R. R. Selmic, "Covert attack and detection through deep neural network on vision-based navigation systems of multi-agent autonomous vehicles," in *2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 2583–2590, 2022.

[3] F. Boem, A. J. Gallo, G. Ferrari-Trecate, and T. Parisini, "A distributed attack detection method for multi-agent systems governed by consensus-based control," in *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, pp. 5961–5966, IEEE, 2017.

[4] A. Barboni, H. Rezaee, F. Boem, and T. Parisini, "Detection of covert cyber-attacks in interconnected systems: A distributed model-based approach," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3728–3741, 2020.

[5] A. Mousavi, K. Aryankia, and R. R. Selmic, "Cyber-attack detection in discrete-time nonlinear multi-agent systems using neural networks," in *2021 IEEE Conference on Control Technology and Applications (CCTA)*, pp. 911–916, IEEE, 2021.

[6] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on scada systems," *IEEE Transactions on Control Systems Technology*, vol. 22, no. 4, pp. 1396–1407, 2013.

[7] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter," *IEEE transactions on control of network systems*, vol. 1, no. 4, pp. 370–379, 2014.

[8] Y. Mo, S. Weerakkody, and B. Sinopoli, "Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 93–109, 2015.

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

[10] A. Kurzhanski and I. Vályi, *Ellipsoidal calculus for estimation and control*. Springer, 1997.

[11] X. Ge, Q.-L. Han, and Z. Wang, "A dynamic event-triggered transmission scheme for distributed set-membership estimation over wireless sensor networks," *IEEE Transactions on Cybernetics*, vol. 49, no. 1, pp. 171–183, 2017.

[12] X. Ge, Q.-L. Han, and F. Yang, "Event-based set-membership leader-following consensus of networked multi-agent systems subject to limited communication resources and unknown-but-bounded noise," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 6, pp. 5045–5054, 2016.

[13] F. Schweppe, "Recursive state estimation: Unknown but bounded errors and system inputs," *IEEE Transactions on Automatic Control*, vol. 13, no. 1, pp. 22–28, 1968.

[14] D. Bertsekas and I. Rhodes, "Recursive state estimation for a set-membership description of uncertainty," *IEEE Transactions on Automatic Control*, vol. 16, no. 2, pp. 117–128, 1971.

[15] A. Khazraei, H. Kebriaei, and F. R. Salmasi, "Replay attack detection in a multi agent system using stability analysis and loss effective watermarking," in *2017 American Control Conference (ACC)*, pp. 4778–4783, IEEE, 2017.

[16] E. Scholte and M. E. Campbell, "A nonlinear set-membership filter for on-line applications," *International Journal of Robust and Nonlinear Control: IFAC-Affiliated Journal*, vol. 13, no. 15, pp. 1337–1358, 2003.

[17] F. Yang and Y. Li, "Set-membership fuzzy filtering for nonlinear discrete-time systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 40, no. 1, pp. 116–124, 2009.

[18] C. Durieu, E. Walter, and B. Polyak, "Multi-input multi-output ellipsoidal state bounding," *Journal of optimization theory and applications*, vol. 111, no. 2, pp. 273–303, 2001.

[19] L. El Ghaoui and G. Calafiore, "Robust filtering for discrete-time systems with bounded noise and parametric uncertainty," *IEEE Transactions on Automatic Control*, vol. 46, no. 7, pp. 1084–1089, 2001.

[20] J. De Geeter, H. Van Brussel, J. De Schutter, and M. Decréton, "A smoothly constrained kalman filter," *IEEE transactions on pattern analysis and machine intelligence*, vol. 19, no. 10, pp. 1171–1177, 1997.

[21] Y.-Y. Cao and P. M. Frank, "Robust h/sub/spl infin//disturbance attenuation for a class of uncertain discrete-time fuzzy systems," *IEEE Transactions on Fuzzy Systems*, vol. 8, no. 4, pp. 406–415, 2000.

[22] F. Delmotte, T. M. Guerra, and A. Kruszewski, "Discrete takagi–sugeno's fuzzy models: reduction of the number of lmi in fuzzy control techniques," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 38, no. 5, pp. 1423–1427, 2008.

[23] S. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan, *Linear matrix inequalities in system and control theory*. SIAM, 1994.

[24] Z. Gao, X. Shi, and S. X. Ding, "Fuzzy state/disturbance observer design for t–s fuzzy systems with application to sensor fault estimation," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 38, no. 3, pp. 875–880, 2008.

[25] C.-S. Tseng, "Robust fuzzy filter design for nonlinear systems with persistent bounded disturbances," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 36, no. 4, pp. 940–945, 2006.

[26] X. Ge, Q.-L. Han, and F. Yang, "Event-based set-membership leader-following consensus of networked multi-agent systems subject to limited communication resources and unknown-but-bounded noise," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 6, pp. 5045–5054, 2016.

[27] R. E. Skelton, T. Iwasaki, and K. Grigoriadis, "A unified algebraic approach to linear control design," 2013.