A Lyapunov-based Control Design for Centralized Networked Control Systems under False-Data-Injection Attacks

Arman Sargolzaei

***Abstract*—A central processing unit receives data from all agents and transmits control commands in a Networked Control System (NCS) which is centralized. Centralized NCSs have numerous applications in industrial settings due to their efficiency, simplicity, and cost-effective design. However, centralized NCSs are vulnerable to false data injection (FDI) attacks. Despite the fact that researchers have developed detection and mitigation defense mechanisms during past several years, most of these methods have focused on systems with linear dynamics. Furthermore, the existing literature only assumes the injection of FDI attacks on measurement signals. In this paper, we assume that an adversary has injected the FDI attack into both state measurements and control signals with nonlinear dynamics while considering communication noises and disturbances. We propose a secure nonlinear control design that mitigates FDI attacks in real-time by combining learning and model-based approaches. We used Lyapunov stability analysis to design the controller, estimator, and updating laws of the neural network (NN). In addition, we selected a network of two robots with Euler-Lagrange dynamics to illustrate the robustness of the proposed controller and estimator.**

***Index Terms*—Nonlinear systems; Networked control systems; Lyapunov stability; False-Data-Injection attack; Nonlinear Observer;**

I. Introduction

Over the past several years, networked control systems (NCSs) have emerged as a promising solution for various industrial applications. These systems have demonstrated the ability to enhance performance and efficiency by integrating control algorithms with network communication. In a centralized NCSs, agents transmit their data to a central processing unit from which they receive control signals. Such centralized NCSs have many application in various industrial settings, including the load frequency control in smart grid systems, formation flight, manufacturing automation, robotics, and search and rescue operations [1]–[3]. However, studies illustrated that that centralized NCSs are not immune to False Data Injection (FDI) attack [4], [5].

Researchers have studied the negative impacts of attacks such as FDI attacks during past several years [6]–[10]. Authors in [7] introduced a category of FDI attacks that are not detectable by detection algorithms. Another study investigates the injection of FDI attacks in a control system which is implemented by a Kalman filter [8]. An optimal attack strategy against the economic dispatch in integrated energy systems, underscoring the delicate balance between maintaining operational efficiency and ensuring system security is explored in [11]. A study demonstrated that adversaries can inject FDI attacks with limited knowledge of the system [9]. Similarly, authors in [10] demonstrated that the smallest set of hackers could carry out an undetectable attack. These studies collectively emphasize the vulnerability of NCSs to FDI attacks, highlighting the importance of designing secure controllers that can mitigate such threats in the next generation of systems.

Researchers have spent a considerable amount of time on developing defense mechanism to detect and compensate FDI attacks. These techniques fall into two categories: learning-based [12]–[17] and model-based techniques [18]–[24]. Model-based techniques depend on the presence of a precise observer to estimate the states of a system,. They have a low computing complexity and are especially well suited for FDI attack detection in real-time. However, because of their dependency on a mathematical model, they are not robust to uncertainties. Despite model-based techniques, learning-based techniques learn complicated nonlinear systems using machine learning algorithms. This makes them a great candidate for systems that are under uncertainties, noises, and disturbances. They are therefore quite useful for identifying FDI attacks. However, due to their computational complexity, these methods are not ideal for online detection. In addition, the stability analysis of these methods is frequently more complicated than that of model-based methods. Here, we combined both model and learning based techniques and propose a nonlinear controller and observer to enhance the accuracy of the nonlinear observer and FDI attack mitigation while reducing computational complexity.

Mitigation and detection of FDI attacks injected into systems with linear dynamics has been investigated in the literature; however, there are a limited number of studies focusing on real-time mitigation of these attacks. State estimation challenges under FDI attacks are investigated in [25]. The study offers strategies to to improve system resilience. Another study analyzed the strategic dynamics of FDI attacks on NCSs through a Switched Stackelberg game model and revealed critical insights into defense and attack strategies [26]. An investigation carried out by [8] developed a technique involving a likelihood ratio test to mitigate FDI attacks. An observer is developed in [10] to estimate FDI attacks. A joint algorithm for FDI attack mitigation was formulated in [27], which simultaneously estimates states and inputs. However, this technique treated the FDI attacks as an input which is unknown and utilized a Kalman filter-based observer for mitigation purposes. These approaches rely significantly on an accurate system model. An alternative algorithm for FDI attack mitigation was suggested by [28]. In this method a NN-based architecture has been developed for mitigation of FDI attacks. However, this algorithm is designed for linear control systems

This research is supported in part by the National Science Foundation under Grant No. ECCS-EPCN-2241718. Any opinions, findings, and conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the sponsoring agency.

Arman Sargolzaei is with Mechanical Engineering Department at the University of South Florida, Tampa, USA. a.sargolzaei@gmil.com

and cannot be used for NCSs with nonlinear dynamics. In addition, the existing techniques in the literature are not able to mitigate FDI attacks injected to both state measurement and control input signals.

Despite the existing challenges for mitigation of FDI attacks, the challenges escalate when dealing with NCSs with nonlinear dynamics. Various methods investigated FDI attacks injected into NCSs with nonlinear dynamics. Yet, these strategies exhibit limitations under specific circumstances. For instance, the work presented by [29] developed an approach to mitigate FDI attacks within a distinct subset of nonlinear systems, employing a retrospective cost-driven adaptive controller. Nevertheless, this strategy's applicability is restricted when dealing with second-order nonlinear systems. In another investigation, a nonlinear-based estimator to compensate faults injected into state measurement signals is proposed [30]. The algorithm uses the power of NNs to perform real-time fault estimation. However, the stability analysis of this technique remained unexplored and this strategy is not applicable for NCSs with second-order nonlinear dynamics. Addressing these concerns, [31] developed a Lyapunov-based control algorithm tailored explicitly to alleviate the influence of FDI attacks. This developed controller can mitigate the overall effect FDI attacks effectively. However, this technique cannot mitigate the effect of FDI attacks if they are injected into both control input and measurement signals. Addressing the existing gap, this paper proposes a novel Lyapunov-based controller and observer to mitigate the effect of FDI attacks injected into both measurement and control input signals of an NCS with nonlinear dynamics while considering noises and disturbances.

This paper has three main contributions which are summarized as (i) a novel nonlinear observer is developed which uses a three-layer feed-forward NN in its design, providing a comprehensive defense mechanism; (ii) a nonlinear controller is designed using Lyapunov analysis for a class of second order control system when both of the state measurement and control input signals are under FDI attacks. This novel control strategy addresses the challenges posed by FDI attacks, ensuring the system's robustness and stability in the face of attacks, disturbances, and measurement noises; (3) the controller, observer, and updating laws of NN are developed through stability analysis ensuring the stability and robustness of the system under FDI attacks. In addition, we showed that the tracking error remains bounded while the NCS is under FDI attacks, disturbances, and measurement noises.

The paper's structure is described here: Section II describes the dynamic model of NCS along with the model of FDI attacks. In Section III, the error signals are defined, along with the control objectives. The subsequent portion delves into the design process of the controller and observer. Section V illustrates the development of FDI attack estimation. Moving ahead, Section VI delves into the stability analysis which is used to develop the controller, observer, and FDI attack estimator. To conclude, the assessment of the nonlinear controller and observer's performance takes center stage in Section VII.

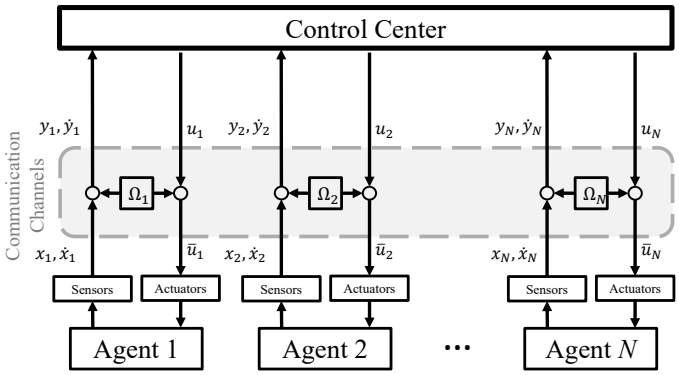

Fig. 1: A centralized NCS under FDI attacks. An adversary injects FDI attacks into both measurement and control signals.

II. Mathematical Model

In this study, we considered a centralized NCS with $N \in \mathbb{Z}_{>0}$ agents which are indicated by $\mathcal{V} \triangleq \{1, 2, \ldots, N\}$. As shown in Figure 1, an adversary can inject FDI attacks into both measurement and control signals. In the proposed centralized NCS, the control center receives the state measurements and generates and transmits the control inputs to the agents. The communication topology is indicated by a graph $\mathcal{G} \triangleq (\mathcal{V}, \mathcal{E})$ which is an undirected, connected, and static, where $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ is the edge set and $\mathcal{V}$ is the node-set.

A. FDI Attacks Model

An FDI attack is defined by the ability of an adversary to get to control communication channels and inject faults into the data shared between agents and the centralized control unit. This form of attack possesses the potential to render an NCS unstable or less efficient and can be modeled as

$$\Omega_i(\eta_i, \beta_{j_i}) \triangleq \eta_i(t) + \Delta_{j_i}(t), \tag{1}$$

where $\Omega_i \in \mathbb{R}^{n_i}$ is a known linear function, $\eta_i \in \mathbb{R}^{n_i}$ is a signal under FDI attack and $\Delta_{j_i}(t) \in \mathbb{R}^{n_i}$ is defined as

$$\Delta_{j_i}(t) = \beta_{j_i}(t) + \theta_{j_i}(t), \tag{2}$$

where $\beta_{j_i} \in \mathbb{R}^{n_i}$ are unknown, continuous, and bounded FDI attacks, $j \in \mathbb{Z}_{>0}$, and $\theta_{j_i}(t)$ is the already existed Gaussian noises in the communication channel. The term θ_{j_i} represents the existing Gaussian noise in the communication channel. For simplicity of the equations, we modeled it as part of the FDI attack.

Assumption 1. It is assumed that $\Delta_{j_i}(t)$ are bounded and differentiable for all i and j, such that $|\Delta_{j_i}(t)| \leq \bar{\Delta}_{j_i}$ can be hold for all time. In addition, $\bar{\Delta}_{j_i}$ are known and positive constants[1].

[1]The adversary's aim is to perturb the system's stable operation by injecting faulty information while remaining undetected by the anomaly detection mechanism. Consequently, these FDI attacks can be considered bounded.

B. Dynamic Model of Nonlinear Agents under FDI Attacks

In this paper, we considered a second order model for the agent $i \in \mathcal{V}$ as described below

$$\ddot{x}_i(t) = f_i(x_i(t), \dot{x}_i(t)) + \bar{u}_i(t) + d_i(t), \tag{3}$$

where $x_i, \dot{x}_i, \ddot{x}_i \in \mathbb{R}^{n_i}$ are the states, n_i is the number of state variables, the control input under FDI attack is denoted by $\bar{u} \in \mathbb{R}^{n_i}$, $d_i \in \rightarrow \mathbb{R}^{n_i}$ is a bounded exogenous disturbance, and $f_i \in \mathbb{R}^{2n_i} \times [0, \infty) \rightarrow \mathbb{R}^{n_i}$ is a known and uniformly bounded nonlinear C^2 function. The control input and state measurement signals under FDI attacks can be defined as

$$\begin{aligned} \bar{u}_i(t) &= \Omega_i(u_i(t), \beta_{3_i}(t)), \\ y_i(t) &= \Omega_i(x_i(t), \beta_{1_i}(t)), \\ \dot{y}_i(t) &= \Omega_i(\dot{x}_i(t), \beta_{2_i}(t)). \end{aligned} \tag{4}$$

where the state measurement signals under FDI attacks are denoted by $y_i, \dot{y}_i \in \mathbb{R}^{n_i}$, $u \in \mathbb{R}^{n_i}$ is the control input. In the real world, should an adversary gain access to the communication channels, they could inject FDI attacks into both types of signals, significantly increasing the complexity of the problem. Addressing and mitigating FDI attacks that target both state measurements and control signals represent one of the main contributions of this paper.

Assumption 2. This study assumed that the disturbance is continuous and bounded and can be shown as $\|d_i(t)\| < \bar{d}_i$ for all time $t \geq t_0$, where the initial time is denoted by t_0 and $\bar{d}_i \in \mathbb{R}_{>0}$ is a known and positive constant [32].

Remark 1. The focus of our study is on a specific type of nonlinear NCS characterized by a second-order model for each agent. This model is used where the dynamics of the agents involve both inertia and damping effects, typical of mechanical systems like robotic arms or vehicles. Such a model allowing for a more accurate representation of their motion and interaction within the network.

III. Error Signals and Objective

This paper's primary goal revolves around developing a centralized controller that regulates state measurements toward predetermined trajectories despite the presence of FDI attacks, measurement noises, and bounded disturbances. Within this context, a tracking error $e_i \in \mathbb{R}^{n_i}$ can be calculated as

$$e_i(t) \triangleq x_{d_i}(t) - x_i(t), \tag{5}$$

where $x_{d_i} \in \mathbb{R}^{n_i}$ is the desired trajectory. To facilitate the stability analysis, let $r_i \in \mathbb{R}^{n_i}$ be an auxiliary tracking error as

$$r_i(t) \triangleq \alpha_i e_i(t) + \dot{e}_i(t), \tag{6}$$

where $\alpha_i \in \mathbb{R}$ is a positive gain [2].

Assumption 3. It is assumed that the reference trajectory, x_{d_i} is bounded. In addition, we assumed that the first two derivatives of reference trajectory are bounded by positive and known constants, i.e. $x_{d_i}, \dot{x}_{d_i}, \ddot{x}_{d_i} \in \mathcal{L}_\infty$ [6].

[2]The value of α_i can be selected by the control engineer through a tuning process. Several tuning algorithms exist, offering optimization to find the best values for user defined parameters [33].

The first challenge of this study pertains to the unavailability of measurement signals, x_i, under FDI attacks. As a result, the error signal e_i becomes unmeasurable under attacks. Therefore, while an adversary injected FDI attacks into an NCS, the control center receives faulty measurement signals—namely, y_i and $\dot{y}_i$ from agents which are faulty ones. Consequently, one of the primary objective of this study is to ensure an accurate tracking even when the state measurements are under FDI attacks. The second challenge is that the control signals are under FDI attacks. As the results, while the control centers transmits u_i, the agent i receives $\bar{u}_i$ under FDI attacks that results in faulty actions by agents. To tackle these challenges, the secondary objective of this study is to design a novel observer that can accurately estimate the state measurements and control signals simultaneously. On another word, the main objective is to ensure the uniformly ultimately bounded (UUB) tracking under FDI attacks. The effectiveness of the proposed nonlinear observer can be quantified by defining an state estimate error signal $\tilde{x}_i \in \mathbb{R}^{n_i}$ as

$$\tilde{x}_i(t) \triangleq x_i(t) - \hat{x}_i(t), \tag{7}$$

where $\hat{x}_i \in \mathbb{R}^{n_i}$ is the estimation of state signals. To facilitate the stability analysis, an auxiliary tracking errors $\tilde{r} \in \mathbb{R}^{n_i}$ is defined to facilitate the stability analysis as

$$\tilde{r}_i \triangleq \alpha_i \tilde{x}_i + \dot{\tilde{x}}_i. \tag{8}$$

Since NCS is measurement noises and disturbances, a fully model-based nonlinear observer cannot accurately estimate states. Therefore, there is a need to infuse a NN-based estimation algorithms for estimation of the overall effect of attacks. The following error signals is defined to quantify the performance of the FDI attack estimator as

$$\tilde{\Delta}_i(t) \triangleq \Delta_i(t) - \hat{\Delta}_i(t), \tag{9}$$

where $\hat{\Delta}_i \in \mathbb{R}^{n_i}$ is the estimate of the overall effect of FDI attacks $\Delta_i \in \mathbb{R}^{n_i}$ and it is defined as

$$\Delta_i(t) \triangleq \Delta_{2_i}(t) + \alpha_i \Delta_{1_i}(t) - K_{u_i}^{-1} \Delta_{3_i}, \tag{10}$$

where $K_{u_i} \in \mathbb{R}$ is a positive user-defined gain.

IV. Control and Observer Design

A. Nonlinear Controller

The proposed controller is developed using the subsequent stability analysis. The control signal is designed as

$$u_i(t) \triangleq K_{u_i} \hat{r}_i(t) + \ddot{x}_{d_i}(t) - f_i(x_{d_i}(t), \dot{x}_{d_i}(t)), \tag{11}$$

where $\hat{r}_i \in \mathbb{R}^{n_i}$ is designed as

$$\hat{r}_i(t) \triangleq \alpha_i \hat{e}_i(t) + \dot{\hat{e}}_i(t) + \hat{\Delta}_i(t), \tag{12}$$

where $\hat{e}_i(t) \triangleq x_{d_i}(t) - y_i(t)$ is a measurable error signal even under FDI attacks.

Taking time derivative of (6) and using (3) results the open-loop tracking error as

$$\dot{r}_i(t) \triangleq \ddot{x}_{d_i}(t) - f_i(x_i(t), \dot{x}_i(t)) - \bar{u}_i(t) - d_i(t) + \alpha_i \dot{e}_i(t), \tag{13}$$

Substituting the control signal (11) into (13) and utilizing (4) and (1) results

$$\begin{aligned}\dot{r}_i(t) = &-f_i(x_i(t),\dot{x}_i(t)) + f_i(x_{d_i}(t),\dot{x}_{d_i}(t)) - d_i(t) \\ &- K_{u_i}\alpha_i\big[x_{d_i}(t) - x_i(t) - \Delta_{2_i}(t)\big] \\ &- K_{u_i}\big[\dot{x}_{d_i}(t) - \dot{x}_i(t) - \Delta_{1_i}(t)\big] \\ &- \Delta_{3_i}(t) + \alpha_i\dot{e}_i(t) - K_{u_i}\hat{\Delta}_i \pm e_i(t),\end{aligned} \tag{14}$$

Using (6) and further simplification yields

$$\begin{aligned}\dot{r}_i(t) = &-f_i(x_i(t),\dot{x}_i(t)) + f_i(x_{d_i}(t),\dot{x}_{d_i}(t)) - d_i(t) \\ &- K_{u_i}r_i(t) + K_{u_i}\big[\Delta_{1_i}(t) + \alpha_i\Delta_{2_i}(t) - K_{u_i}^{-1}\Delta_{3_i}(t)\big] \\ &- K_{u_i}\hat{\Delta}_i(t) + \alpha_i r_i(t) - \alpha_i^2 e_i(t),\end{aligned} \tag{15}$$

Rearranging (15) and utilizing (9) yields

$$\dot{r}_i = -K_{u_i}r_i(t) + K_{u_i}\tilde{\Delta}_i(t) - e_i(t) + \chi_{1_i}(t) + d_i(t), \tag{16}$$

where the above auxiliary term $\chi_{1_i} \in \mathbb{R}^{n_i}$ is defined as

$$\begin{aligned}\chi_{1_i}(t) \triangleq &\alpha_i r_i(t) - \alpha_i^2 e_i(t) + e_i(t) \\ &- f_i(x_i(t),\dot{x}_i(t)) + f_i(x_{d_i}(t),\dot{x}_{d_i}(t)).\end{aligned} \tag{17}$$

B. Nonlinear Observer

The subsequent stability analysis is used to develop the state observer as

$$\ddot{\hat{x}}_i(t) \triangleq f_i(\hat{x}_i(t),\dot{\hat{x}}_i(t)) + u_i(t) + L_{x_i}\Phi_i(t), \tag{18}$$

where $L_{x_i} \in \mathbb{R}$ denotes a positive user-defined gain and $\Phi_i \in \mathbb{R}^{n_i}$ is a measurable feedback signal which is defined as

$$\Phi_i(t) \triangleq \dot{y}_i(t) - \dot{\hat{x}}_i(t) + \alpha_i y_i(t) - \alpha_i\hat{x}_i(t) - \hat{\Delta}_i(t). \tag{19}$$

By substituting (18) and (3) into the time derivative of (8), the closed-loop observer error can be calculated as

$$\dot{\tilde{r}}_i(t) = -L_{x_i}\tilde{r}_i(t) - \tilde{x}_i - K_{u_i}\tilde{\Delta}_i + \chi_{2_i} + N_{1_i}, \tag{20}$$

where $\chi_{2_i} \in \mathbb{R}^{n_i}$ is an auxiliary term which is descibed as

$$\begin{aligned}\chi_{2_i}(t) \triangleq &f_i(x_i(t),\dot{x}_i(t)) - f_i(\hat{x}_i(t),\dot{\hat{x}}_i(t)) + \tilde{x}_i(t) \\ &+ \alpha_i\tilde{r}_i(t) - \alpha_i\tilde{x}_i(t).\end{aligned} \tag{21}$$

and $N_{1_i} \in \mathbb{R}^{n_i}$ is defined as

$$N_{1_i}(t) \triangleq d_i(t) + \mu_i\Delta_{3_i} + (K_{u_i} - L_{x_i})\tilde{\Delta}_i, \tag{22}$$

where $\mu_i \triangleq 1 - L_{x_i}K_{u_i}^{-1}$.

Remark 2. We can use Assumptions 2 and 3 and the Mean Value Theorem (MVT) to conclude that

$$\|\chi_{1_i}\| \leq \rho_{1_i}(\|z_i\|)\|z_i\|, \tag{23}$$

and

$$\|\chi_{2_i}\| \leq \rho_{2_i}(\|z_i\|)\|z_i\|, \tag{24}$$

where $\rho_{1_i}(\|z_i\|)$ and $\rho_{2_i}(\|z_i\|)$ Are functions that exhibit global invertibility, positivity, and non-decreasing behavior [34]. In addition, $z_i \in \mathbb{R}^{4n_i}$ is defined as

$$z_i \triangleq [e_i^T,\ r_i^T,\ \tilde{x}_i^T,\ \tilde{r}_i^T]^T. \tag{25}$$

In the subsequent equations, we have excluded the inclusion of time dependencies to enhance the simplicity of the analysis.

V. Estimation of FDI attack

$$\mathcal{M}_{\Delta_i} \triangleq \frac{\mathcal{K}_{\Delta_i}(t - t_0)}{\mathcal{K}_{\Delta_i}(t - t_0) + 1}, t \in [t_0, \infty), \tag{26}$$

where $\mathcal{M}_{\Delta_i} : [t_0,\infty) \to [0,1]$ denotes the nonlinear mapping, and $\mathcal{K}_{\Delta_i} \in \mathbb{R}$ denotes a positive gain which is user-defined. Since $\mathcal{M}_{\Delta_i}^{-1} : [0,1] \to [t_0,\infty)$, the overall effect of FDI attack is able to be mapped into ν which a compact domain. Therefore, the overall effect of FDI attack, Δ_i, can be written as

$$\Delta_i(t) = \Delta_i(\mathcal{M}_{\Delta_i}^{-1}(\nu)) \triangleq \Delta_{\mathcal{M}_{\Delta_i}}(\nu), \nu \in [0,1]. \tag{27}$$

With the proposed nonlinear mapping, $\Delta_{M_{\Delta_i}} : [0,1] \to \mathbb{R}^{n_i}$ is defined over a compact domain[3]. Thus, a NN structure can be used to represent the overall effect of FDI attacks as

$$\Delta_{\mathcal{M}_{\Delta_i}}(\nu) = W_{\Delta_i}^T\sigma\left(V_{\Delta_i}^T\delta_i\right) + \varepsilon_i, \tag{28}$$

where the NN ideal and unknown weights are denoted by $W_{\Delta_i} \in \mathbb{R}^{(n_{n_i}+1)\times n_i}$ and $V_{\Delta_i} \in \mathbb{R}^{(n_i+1)\times n_{n_i}}$, the number of neurons in the hidden layer is denoted by n_{n_i}, $\sigma(\cdot) \in \mathbb{R}^{(n_{n_i}+1)}$ is a vector for activation functions [4], and imputes of the NN is denoted by $\delta_i \in \mathbb{R}^{(n_i+1)\times 1}$. In addition, $\varepsilon_i \in \mathbb{R}^{n_i}$ denotes an error signal which is bounded such that $\|\varepsilon_i\| \leq \bar{\varepsilon}_i$, where $\bar{\varepsilon}_i \in \mathbb{R}$ denotes a positive known constant.

The overall effect of FDI attack with respect to the spatial domain can be estimated as

$$\hat{\Delta}_i \triangleq \hat{W}_{\Delta_i}^T\sigma(\hat{V}_{\Delta_i}^T\delta_i), \tag{29}$$

where $\hat{V}_{\Delta_i} \in \mathbb{R}^{(n_i+1)\times n_{n_i}}$ and $\hat{W}_{\Delta_i} \in \mathbb{R}^{(n_{n_i}+1)\times n_i}$ are weights of the FDI attack estimate, and δ_i can be defined as

$$\delta_i \triangleq [1, \hat{\Delta}_i^T]^T. \tag{30}$$

Substituting (27), (28), and (29) into (9) yields

$$\tilde{\Delta}_i = W_{\Delta_i}^T\sigma\left(V_{\Delta_i}^T\delta_i\right) - \hat{W}_{\Delta_i}^T\sigma\left(\hat{V}_{\Delta_i}^T\delta_i\right) + \varepsilon_i \tag{31}$$

Using a Taylor's series approximation, we can write the FDI attack estimation error $\tilde{\Delta}_i$ as

$$\tilde{\Delta}_i = \tilde{W}_{\Delta_i}^T\sigma\left(\hat{V}_{\Delta_i}^T\delta_i\right) + \hat{W}_{\Delta_i}^T\sigma\prime\left(\hat{V}_{\Delta_i}^T\delta_i\right)\tilde{V}_{\Delta_i}^T\delta_i + N_{n_i} \tag{32}$$

where

$$N_{n_i} \triangleq \tilde{W}_{\Delta_i}^T\sigma\prime\left(\hat{V}_{\Delta_i}^T\delta_i\right)\tilde{V}_{\Delta_i}^T\delta_i + W_i^T\mathcal{H}\left(\tilde{V}_{\Delta_i}^T\delta_i\right) + \varepsilon_i, \tag{33}$$

where $\mathcal{H}$ is the higher order terms, $\tilde{V}_{\Delta_i} = V_{\Delta_i} - \hat{V}_{\Delta_i}$ and $\tilde{W}_{\Delta_i} \triangleq W_{\Delta_i} - \hat{W}_{\Delta_i}$ are the the outer and inner errors for the weights of NN respectively, and finally σ' is defined as

$$\sigma'\left(\hat{V}_{\Delta_i}^T\delta_i\right) \triangleq \left.\frac{\partial\sigma\left(V_i^T\delta_i\right)}{\partial V_i^T\delta_i}\right|_{\hat{V}_{\Delta_i}^T\delta_i}. \tag{34}$$

Remark 3. It has been shown in the literature that N_{n_i} is bounded, i.e., $\|N_{n_i}\| \leq \bar{n}_{n_i}$, and $\bar{n}_{n_i} \in \mathbb{R}$ is a positive constant [37].

[3]The mapping is conducted to satisfy the Stone-Weierstrass Theorem described in [35].

[4]The activation functions should be chosen to be C^2 [36].

The updating laws for the NN is calculated based on the stability analysis in Section VI as

$$\dot{\hat{W}}_{\Delta_i} = \text{proj}\left(\xi_{1_i} K_i \sigma(\hat{V}_{\Delta_i}^T \delta_i)(\Psi_i)^T\right) \tag{35}$$

and

$$\dot{\hat{V}}_{\Delta_i} = \text{proj}\left(\xi_{2_i} K_i \delta_i (\Psi_i)^T \hat{W}_{\Delta_i}^T \sigma\prime(\hat{V}_{\Delta_i}^T \delta_i)\right), \tag{36}$$

where $\xi_{1_i} \in \mathbb{R}^{n_i \times n_i}$ and $\xi_{2_i} \in \mathbb{R}^{n_i \times n_i}$ are positive definite matrices, proj$(\cdot)$ denotes the projection operator implemented based on [38], and the signal Ψ_i is defined as

$$\Psi_i \triangleq \dot{x}_{d_i} - \hat{x}_i + \alpha_i x_{d_i} - \alpha_i \hat{x}_i. \tag{37}$$

Remark 4. The use of proj$(\cdot)$ function ensures that $\hat{W}_{\Delta_i}$ and $\hat{V}_{\Delta_i}$ remain bounded. Therefore, $\hat{W}_{\Delta_i}$ and $\sigma(\hat{V}_{\Delta_i}^T \delta_i)$ remain bounded. So, we can conclude that $\hat{\Delta}_i$ remains bounded. In addition, based on Assumption 1, the overall effect of FDI attack, Δ_i, is bounded. therefore, the FDI attack estimation error, $\tilde{\Delta}_i$, remains bounded and we can conclude that $\|\tilde{\Delta}_i\| \leq \bar{\Delta}_i$, $\forall t \geq t_0, i \in \mathcal{V}$, and $\bar{\Delta}_i \in \mathbb{R}_{>0}$ is a known positive constant.

Remark 5. Assumptions 1 and 3 along with Remark 4 can be utilized to conclude that

$$\|N_{1_i}\| \leq \bar{n}_{1_i}, \tag{38}$$

where $\bar{n}_{1_i} \in \mathbb{R}$ is a positive known constant.

VI. Stability Analysis

Let $\epsilon_{1_i}, \epsilon_{2_i}, \epsilon_{3_i}, \epsilon_{4_i}, \epsilon_{5_i} \in \mathbb{R}_{>0}$ be user-defined gains to satisfy the following sufficient conditions

$$\begin{aligned} K_{u_i} &> \frac{K_{u_i}\epsilon_{1_i}}{2} + \frac{\epsilon_{2_i}}{2} + \frac{\epsilon_{3_i}}{2}, \\ L_{x_i} &> \frac{\epsilon_{4_i}}{2} + \frac{\epsilon_{3_i}}{2} + \frac{K_{u_i}\epsilon_{5_i}}{2}, \end{aligned} \tag{39}$$

and let $\xi_{1_i} \triangleq \frac{1}{2}\|z_i\|^2$ and $\xi_{2_i} \triangleq \|z_i\|^2$. In addition, Let $H_{L_{x_i}} : [t_0, \infty) \to \mathbb{R}_{\geq 0}$ be defined as

$$H_{L_{x_i}} \triangleq \frac{1}{2}\text{tr}(\tilde{W}_{\Delta_i}^T \xi_{1_i}^{-1} \tilde{W}_{\Delta_i}) + \frac{1}{2}\text{tr}(\tilde{V}_{\Delta_i}^T \xi_{2_i}^{-1} \tilde{V}_{\Delta_i}), \tag{40}$$

Remark 6. Based on Remark 4, we can show that $\tilde{W}_{\Delta_i}$ and $\tilde{V}_{\Delta_i}$ are bounded. Thus, $H_{L_{x_i}}$ is bounded and we can show that $|H_{L_{x_i}}| \leq H_{L_{x_i},\max}$, and $H_{L_{x_i},\max} \in \mathbb{R}$ is a positive and known constant.

Theorem 1. *Provided that all of the sufficient conditions in* (39) *are satisfied, the proposed nonlinear controller in* (11)*, FDI attack estimator in* (29)*, and nonlinear observer in* (18) *ensure globally UUB tracking such that*

$$\limsup_{t\to\infty} \|z_i\| \leq \sqrt{\frac{1}{\xi_{1_i}}\left(H_{L_{i,\max}} + \frac{\xi_{2_i}\varphi_i}{\alpha_{3_i}}\right)}. \tag{41}$$

Proof. Let $V_{L_{x_i}} : \mathbb{R}^{4n_i+1} \times [0, \infty) \to \mathbb{R}$ be a positive definite, radially unbounded, and continuously differentiable Lyapunov candidate function that is described as

$$V_{L_{x_i}} \triangleq \frac{1}{2}e_i^T e_i + \frac{1}{2}r_i^T r_i + \frac{1}{2}\tilde{x}_i^T \tilde{x}_i + \frac{1}{2}\tilde{r}_i^T \tilde{r}_i + H_{L_{x_i}}. \tag{42}$$

The function V_{L_i} in (42) is bounded Lyapunov candidate function such that

$$\xi_{1_i} \leq V_{L_{x_i}} \leq \xi_{2_i} + H_{L_{x_i},\max}. \tag{43}$$

To proof Theorem 1, we first take the derivative of (42) with respect to time and substitute (6), (8), (16), and (20), which yields

$$\begin{aligned} \dot{V}_{L_{x_i}} =& e_i^T\left(r_i - \alpha_i e_i\right) + r_i^T\Big(-K_i r_i - e_i + K_{u_i}\tilde{\Delta}_i \\ &+ \chi_{1_i} + d_i\Big) + \tilde{x}_i^T\left(\tilde{r}_i - \alpha_i \tilde{x}_i\right) + \tilde{r}_i^T\Big(-L_{x_i}\tilde{r}_i \\ &- \tilde{x}_i - K_{u_i}\tilde{\Delta}_i + \chi_{2_i} + N_{1_i}\Big) + \dot{H}_{L_{x_i}}, \end{aligned} \tag{44}$$

Acknowledging the fact that $\dot{\tilde{V}}_{\Delta_i} = -\dot{\hat{V}}_{\Delta_i}$ and $\dot{\tilde{W}}_{\Delta_i} = -\dot{\hat{W}}_{\Delta_i}$, equation (44) can be written as

$$\begin{aligned} \dot{V}_{L_{x_i}} =& e_i^T\left(r_i - \alpha_i e_i\right) + r_i^T\Big(-K_i r_i - e_i + K_{u_i}\tilde{\Delta}_i \\ &+ \chi_{1_i} + d_i\Big) + \tilde{x}_i^T\left(\tilde{r}_i - \alpha_i \tilde{x}_i\right) + \tilde{r}_i^T\Big(-L_{x_i}\tilde{r}_i \\ &- \tilde{x}_i - K_{u_i}\tilde{\Delta}_i + \chi_{2_i} + N_{1_i}\Big) \\ &- \text{tr}(\tilde{W}_{\Delta_i}^T \xi_{1_i}^{-1} \dot{\hat{W}}_{\Delta_i}) - \text{tr}(\tilde{V}_{\Delta_i}^T \xi_{2_i}^{-1} \dot{\hat{V}}_{\Delta_i}), \end{aligned} \tag{45}$$

Rearranging further yields

$$\begin{aligned} \dot{V}_{L_{x_i}} =& -\alpha_i e_i^T e_i - K_i r_i^T r_i + r_i^T \chi_{1_i} + r_i^T d_i \\ &- \alpha_i \tilde{x}_i^T \tilde{x}_i - L_{x_i}\tilde{r}_i^T \tilde{r}_i + K_{u_i}(r_i - \tilde{r}_i)^T \tilde{\Delta}_i + \tilde{r}_i^T \chi_{2_i} \\ &+ \tilde{r}_i^T N_{1_i} - \text{tr}(\tilde{W}_{\Delta_i}^T \xi_{1_i}^{-1} \dot{\hat{W}}_{\Delta_i}) - \text{tr}(\tilde{V}_{\Delta_i}^T \xi_{2_i}^{-1} \dot{\hat{V}}_{\Delta_i}), \end{aligned} \tag{46}$$

Utilizing Assumption 2, Remark 3 and 4, an upper bound for (46) can be obtained as

$$\begin{aligned} \dot{V}_{L_{x_i}} \leq& -\alpha_i \|e_i\|^2 - K_i \|r_i\|^2 + \|r_i\| \|\chi_{1_i}\| \\ &+ \|r_i\| \|d_i\| - \alpha_i \|\tilde{x}_i\|^2 - L_{x_i} \|\tilde{r}_i\|^2 \\ &+ \|\tilde{r}_i\| \|\chi_{2_i}\| + \|\tilde{r}_i\| \|N_{1_i}\| + K_{u_i} \|r_i\| \|N_{n_i}\| \\ &+ K_{u_i} \|\tilde{r}_i\| \|N_{n_i}\| \\ &+ K_{u_i} \|r_i + \tilde{r}_i\| \left(\tilde{W}_{\Delta_i}^T \sigma\left(\hat{V}_{\Delta_i}^T \delta_i\right)\right. \\ &\left. + \hat{W}_{\Delta_i}^T \sigma\prime\left(\hat{V}_{\Delta_i}^T \delta_i\right) \tilde{V}_{\Delta_i}^T \delta_i\right) \\ &- \text{tr}(\tilde{W}_{\Delta_i}^T \xi_{1_i}^{-1} \dot{\hat{W}}_{\Delta_i}) - \text{tr}(\tilde{V}_{\Delta_i}^T \xi_{2_i}^{-1} \dot{\hat{V}}_{\Delta_i}) \end{aligned} \tag{47}$$

Knowing that $\Psi_i = r_i + \tilde{r}_i$ results

$$\begin{aligned} \dot{V}_{L_{x_i}} \leq& -\alpha_i \|e_i\|^2 - K_i \|r_i\|^2 + \|r_i\| \|\chi_{1_i}\| \\ &+ \|r_i\| \|d_i\| - \alpha_i \|\tilde{x}_i\|^2 - L_{x_i} \|\tilde{r}_i\|^2 \\ &+ \|\tilde{r}_i\| \|\chi_{2_i}\| + \|\tilde{r}_i\| \|N_{1_i}\| + K_{u_i} \|r_i\| \|N_{n_i}\| \\ &+ K_{u_i} \|\tilde{r}_i\| \|N_{n_i}\| \\ &+ K_{u_i} \|\Psi_i\| \left(\tilde{W}_{\Delta_i}^T \sigma\left(\hat{V}_{\Delta_i}^T \delta_i\right) + \hat{W}_{\Delta_i}^T \sigma\prime\left(\hat{V}_{\Delta_i}^T \delta_i\right) \tilde{V}_{\Delta_i}^T \delta_i\right) \\ &- \text{tr}(\tilde{W}_{\Delta_i}^T \xi_{1_i}^{-1} \dot{\hat{W}}_{\Delta_i}) - \text{tr}(\tilde{V}_{\Delta_i}^T \xi_{2_i}^{-1} \dot{\hat{V}}_{\Delta_i}) \end{aligned} \tag{48}$$

Substituting NN updating laws of (35) and (36) into (48) cancels the NN terms and results

$$\begin{aligned} \dot{V}_{L_{x_i}} \leq& -\alpha_i \|e_i\|^2 - K_i \|r_i\|^2 + \|r_i\| \|\chi_{1_i}\| \\ &+ \|r_i\| \|d_i\| - \alpha_i \|\tilde{x}_i\|^2 - L_{x_i} \|\tilde{r}_i\|^2 \\ &+ \|\tilde{r}_i\| \|\chi_{2_i}\| + \|\tilde{r}_i\| \|N_{1_i}\| + K_{u_i} \|r_i\| \left\|\bar{N}_{n_i}\right\| \\ &+ K_{u_i} \|\tilde{r}_i\| \left\|\bar{N}_{n_i}\right\|. \end{aligned} \tag{49}$$

Applying the Young's Inequality, terms in (49) can be upper bounded as

$$\|r_i\|\|N_{n_i}\| \leq \frac{\epsilon_{1_i}}{2}\|r_i\|^2 + \frac{\bar{n}_{n_i}^2}{2\epsilon_{1_i}}, \tag{50}$$

$$\|r_i\|\|d_i\| \leq \frac{\epsilon_{2_i}}{2}\|r_i\|^2 + \frac{\bar{d}_i^2}{2\epsilon_{2_i}}, \tag{51}$$

$$\|r_i\|\|\chi_{1_i}\| \leq \frac{\epsilon_{3_i}}{2}\|r_i\|^2 + \frac{1}{2\epsilon_{3_i}}\rho_{1_i}^2(\|z_i\|)\|z_i\|^2, \tag{52}$$

$$\|\tilde{r}_i\|\|N_{1_i}\| \leq \frac{\epsilon_{4_i}}{2}\|\tilde{r}_i\|^2 + \frac{\bar{n}_{1_i}^2}{2\epsilon_{4_i}}, \tag{53}$$

$$\|\tilde{r}_i\|\|\chi_{2_i}\| \leq \frac{\epsilon_{3_i}}{2}\|\tilde{r}_i\|^2 + \frac{1}{2\epsilon_{3_i}}\rho_{2_i}^2(\|z_i\|)\|z_i\|^2, \tag{54}$$

$$\|\tilde{r}_i\|\|N_{n_i}\| \leq \frac{\epsilon_{5_i}}{2}\|\tilde{r}_i\|^2 + \frac{\bar{n}_{n_i}^2}{2\epsilon_{5_i}}. \tag{55}$$

Using (50)-(55), (49) can be written as

$$\begin{aligned}\dot{V}_{L_{x_i}} \leq & -\alpha_i\|e_i\|^2 - K_i\|r_i\|^2 + \frac{\epsilon_{3_i}}{2}\|r_i\|^2 \\ & + \frac{1}{2\epsilon_{3_i}}\rho_{1_i}^2(\|z_i\|)\|z_i\|^2 + \frac{\epsilon_{2_i}}{2}\|r_i\|^2 + \frac{\bar{d}_i^2}{2\epsilon_{2_i}} \\ & - \alpha_i\|\tilde{x}_i\|^2 - L_{x_i}\|\tilde{r}_i\|^2 + \frac{\epsilon_{3_i}}{2}\|\tilde{r}_i\|^2 \\ & + \frac{1}{2\epsilon_{3_i}}\rho_{2_i}^2(\|z_i\|)\|z_i\|^2 + \frac{\epsilon_{4_i}}{2}\|\tilde{r}_i\|^2 + \frac{\bar{n}_{1_i}^2}{2\epsilon_{4_i}} \\ & + \frac{K_{u_i}\epsilon_{1_i}}{2}\|r_i\|^2 + \frac{K_{u_i}\bar{n}_{n_i}^2}{2\epsilon_{1_i}} \\ & + \frac{K_{u_i}\epsilon_{5_i}}{2}\|\tilde{r}_i\|^2 + \frac{K_{u_i}\bar{n}_{n_i}^2}{2\epsilon_{5_i}}.\end{aligned} \tag{56}$$

Simplifying further results

$$\begin{aligned}\dot{V}_{L_{x_i}} \leq & -\alpha_i\|e_i\|^2 - \alpha_{1_i}\|r_i\|^2 - \alpha_i\|\tilde{x}_i\|^2 - \alpha_{2_i}\|\tilde{r}_i\|^2 \\ & + \frac{1}{2\epsilon_{3_i}}\rho_i^2(\|z_i\|)\|z_i\|^2 + \varphi_i,\end{aligned} \tag{57}$$

where φ_i is defined as

$$\varphi_i \triangleq \frac{K_{u_i}\bar{n}_{n_i}^2}{2\epsilon_{1_i}} + \frac{K_{u_i}\bar{n}_{n_i}^2}{2\epsilon_{5_i}} + \frac{\bar{d}_i^2}{2\epsilon_{2_i}} + \frac{\bar{n}_{1_i}^2}{2\epsilon_{4_i}}, \tag{58}$$

and $\rho_i^2(\|z_i\|)$ is defined as

$$\rho_i^2(\|z_i\|) \triangleq \rho_{1_i}^2(\|z_i\|) + \rho_{2_i}^2(\|z_i\|), \tag{59}$$

and α_{1_i} and α_{2_i} can be defined as

$$\alpha_{1_i} \triangleq K_{u_i} - \frac{K_{u_i}\epsilon_{1_i}}{2} - \frac{\epsilon_{2_i}}{2} - \frac{\epsilon_{3_i}}{2}, \tag{60}$$

$$\alpha_{2_i} \triangleq L_{x_i} - \frac{\epsilon_{4_i}}{2} - \frac{\epsilon_{3_i}}{2} - \frac{K_{u_i}\epsilon_{5_i}}{2}, \tag{61}$$

where α_{1_i} and α_{2_i} are positive constants given the sufficient conditions defined in (39). Therefore, inequality in (57) can be written as

$$\dot{V}_{L_{x_i}} \leq -\left(\frac{\alpha_{3_i}}{2} - \frac{1}{2\epsilon_{3_i}}\rho_i^2\left(\|z_i\|\right)\right)\|z_i\|^2 - \frac{\alpha_{3_i}}{2}\|z_i\|^2 + \varphi_i, \tag{62}$$

where $\alpha_{3_i} \triangleq \min\{\alpha_i, \alpha_{1_i}, \alpha_{2_i}\}$. Since, the Lyapunov candidate function in (42) is bounded based on the inequality in (43), the expression in (62) can be upper bounded as

$$\dot{V}_{L_{x_i}} \leq -\frac{\alpha_{3_i}}{\xi_{2_i}}V_{L_{x_i}} + \frac{\alpha_{3_i}}{\xi_{2_i}}H_{i,\max} + \varphi_i. \tag{63}$$

Solving the differential equation in (63) yields

$$\begin{aligned}V_{L_{x_i}} \leq & V_{L_{x_i}}(t_0)\exp\left(-\frac{\alpha_{3_i}}{\xi_{2_i}}(t-t_0)\right) \\ & + \left(H_{i,\max} + \frac{\xi_{2_i}\varphi_i}{\alpha_{3_i}}\right)\left(1 - \exp\left(-\frac{\alpha_{3_i}}{\xi_{2_i}}(t-t_0)\right)\right),\end{aligned} \tag{64}$$

Considering the inequality in (43), equation (64) can be used to get the upper bound given in (41). Therefore, we can conclude that z_i is bounded and subsequently we can show that $e_i, r_i, \tilde{x}_i \in \mathcal{L}_\infty$. The control designed in (11) can be used to conclude that $u_i \in \mathcal{L}_\infty$. ■

VII. Simulation Analysis

In this section, we proceed to assess the efficacy of the formulated nonlinear controller, observer, and FDI attack estimator within the context of NCSs characterized by nonlinear dynamics, while being exposed to FDI attacks, disturbances, and measurement noise. To facilitate this evaluation, an NCS involving two-link planar manipulators is taken into consideration. For the simulation simplicity, agents are considered to have an Euler-Lagrange dynamic model as described below [6], [34]:

$$\begin{aligned}&\begin{bmatrix}u_{1_i}(t)\\ u_{2_i}(t)\end{bmatrix} = \begin{bmatrix}p_{1_i} + 2p_{3_i}\cos(y_{2_i}) & p_{2_i} + p_{3_i}\cos(y_{2_i})\\ p_{2_i} + p_{3_i}\cos(y_{2_i}) & p_{2_i}\end{bmatrix}\begin{bmatrix}\ddot{x}_{1_i}\\ \ddot{x}_{2_i}\end{bmatrix} \\ &+ \begin{bmatrix}-p_{3_i}\sin(y_{2_i})\dot{x}_{2_i} & -p_{3_i}\sin(y_{2_i})(\dot{x}_{1_i}+\dot{x}_{2_i})\\ p_{3_i}\sin(y_{2_i})\dot{x}_{1_i} & 0\end{bmatrix}\begin{bmatrix}\dot{x}_{1_i}\\ \dot{x}_{2_i}\end{bmatrix} \\ &+ \begin{bmatrix}f_{d1_i} & 0\\ 0 & f_{d2_i}\end{bmatrix}\begin{bmatrix}\dot{x}_{1_i}\\ \dot{x}_{2_i}\end{bmatrix} + \begin{bmatrix}d_{1_i}\\ d_{2_i}\end{bmatrix}, \forall i \in \{1,2\},\end{aligned} \tag{65}$$

where $p_{1_i} = 3.473\ kg\cdot m^2$, $p_{2_i} = 0.196\ kg\cdot m^2$, $p_{3_i} = 0.242\ kg{\cdot}m^2$, $f_{d1_i} = 5.3\ Nm{\cdot}sec$, and finally $f_{d2_i} = 1.1\ Nm{\cdot}sec$.

Additionally, in (65), the measurements signals, y_{j_i} and $\dot{y}_{j_i}$ are not equal state variable when the system is under attack and measurement noises and they are defined as

$$y_{j_i} \triangleq \Omega_i(x_{j_i}, \beta_{1_i}), \forall j \in \{1,2\}, \tag{66}$$

and

$$\dot{y}_{j_i} \triangleq \Omega_i(\dot{x}_{j_i}, \beta_{2_i}), \forall j \in \{1,2\} \tag{67}$$

The desired trajectories for the initial agent are chosen similar to the literature [6] for comparison reasons as

$$x_{d_1}(t) = \begin{bmatrix}50[1-\exp(-0.01t^3)]\times\cos(1.5t)\\ 30[1-\exp(-0.01t^3)]\times\cos(1.5t)\end{bmatrix} deg,$$

and the desired trajectories of the second agent is selected as

$$x_{d_2}(t) = \begin{bmatrix}70[1-\exp(-0.01t^3)]\times\cos(1t)\\ 60[1-\exp(-0.01t^3)]\times\cos(1t)\end{bmatrix} deg.$$

In addition, we added exogenous disturbances to both of agents which are defined as

$$d_{1_i}(t) = 0.002\sin(0.1t), \tag{68}$$

and

$$d_{2_i}(t) = 0.001\sin(0.5t), \tag{69}$$

where $i \in [1, 2]$.

The FDI attacks denoted as β_{1_i}, β_{2_i}, and β_{3_i} which are attacks injected to state measurement and control input signals respectively. We considered that FDI attacks are injected to both of the robots and they are illustrated in Figures 2 and 3. The errors for the position and angular velocity are illustrated in Figures 2 and 3 where the first and second Figures are related to the first and second robots respectively. The results clearly illustrate that the proposed nonlinear controller is resilient to FDI attacks that are injected into both control input and measurement signals. To compare the proposed nonlinear controller with a traditional controller[5]. In addition, we simulated the proposed work in [6] and compared the result with our proposed secure controller. We calculated the root mean square error (RMSE) and included the results in Table I. Furthermore, we calculated the RMSE of the estimation error for the effect of FDI attack to quantify the performance of the FDI attack estimator. The FDI attack estimation for the first and second agents are 0.0738 and 0.5351 respectively.

TABLE I: The performance Comparison of the proposed controller with traditional controllers for agents under FDI attacks.

Agent	Proposed controller	Controller in [6]	Traditional controller
1	0.0164	0.0521	0.1093
2	0.0375	0.0625	0.1254

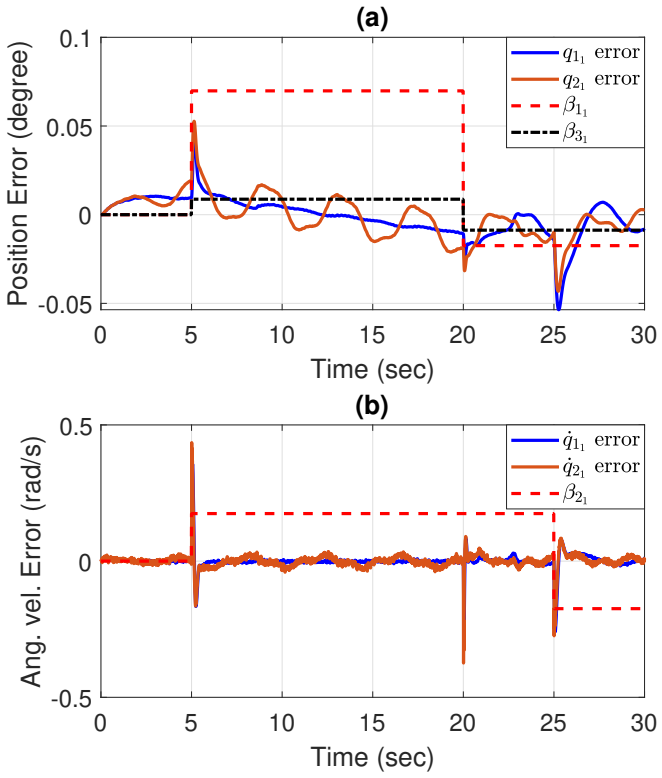

Fig. 2: Sub-figure (a) illustrates the Position error for the first robot and sub-figure (b) shows the angular Velocity error.

VIII. Conclusion

In this study, we have presented a novel Lyapunov-based control strategy with the primary objective of ensuring precise tracking within Nonlinear Control Systems operating under the influence of FDI attacks, external disturbances, and measurement noises. It is noteworthy that our approach differentiates itself from conventional control algorithms found in existing literature by addressing a specific and challenging scenario: the injection of FDI attacks into both state measurements and control input signals. To achieve this, we have introduced an innovative anomaly detection algorithm that seamlessly integrates model-based and learning-based observers. This amalgamation of techniques allows us to rapidly and accurately detect and estimate the impact of FDI attacks in real-time. Notably, the updating laws governing the behavior of the NN were developed through using Lyapunov stability analysis, ensuring the reliability and robustness of our proposed methodology. To comprehensively evaluate the efficacy and resilience of our proposed approach, simulation analysis was conducted. These simulation results demonstrate that our proposed controller, nonlinear observer, and FDI estimator, offering valuable resiliency to NCS used in real-world applications.

Data availability statement:

The data that support the findings of the numerical results are available from the authors upon reasonable request.

[5]The proposed controller without an FDI attack estimation is considered as a traditional controller.

References

[1] A. Sargolzaei, A. Abbaspour, and C. D. Crane, "Control of cooperative unmanned aerial vehicles: review of applications, challenges, and algorithms," *Optimization, Learning, and Control for Interdependent Complex Networks*, pp. 229–255, 2020.

[2] A. Sargolzaei, A. Abbaspour, M. A. Al Faruque, A. S. Eddin, and K. Yen, "Security challenges of networked control systems," in *Sustainable Interdependent Networks*, pp. 77–95, Springer, 2018.

[3] P. A. Bonab, J. Holland, and A. Sargolzaei, "An observer-based control for a networked control of permanent magnet linear motors under a false-data-injection attack," in *2023 IEEE Conference on Dependable and Secure Computing (DSC)*, pp. 1–8, IEEE, 2023.

[4] A. Nguyen and B. Lee, "Security analysis of networked control systems under false data injection attacks: Challenges and solutions," *IEEE Transactions on Control of Network Systems*, vol. 7, no. 1, pp. 489–501, 2020.

[5] S. Martinez and J. Rodriguez, "Evaluating the impact of false data injection attacks on networked control systems," in *Proceedings of the IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids*, pp. 1–6, 2019.

[6] A. Sargolzaei, "A secure control design for networked control system with nonlinear dynamics under false-data-injection attacks," in *2021 American Control Conference (ACC)*, pp. 2693–2699, IEEE, 2021.

[7] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: characterizations and countermeasures π," in *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 232–237, IEEE, 2011.

[8] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645–658, 2011.

[9] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pp. 220–225, IEEE, 2010.

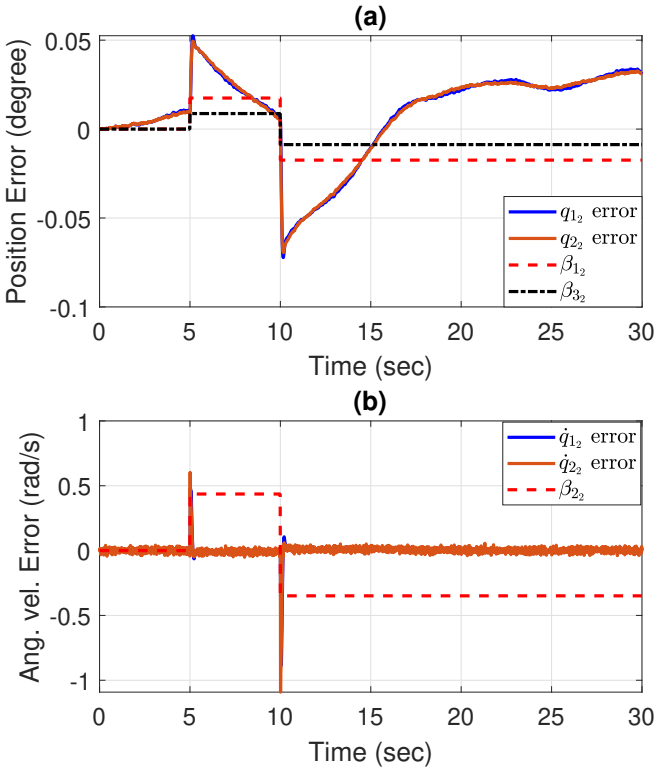

Fig. 3: Sub-figure (a) illustrates the Position error for the second robot and sub-figure (b) shows the angular Velocity error.

[10] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[11] Y. Zhang, X. Xie, W. Fu, X. Chen, S. Hu, L. Zhang, and Y. Xia, "An optimal combining attack strategy against economic dispatch of integrated energy system," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 70, no. 1, pp. 246–250, 2022.

[12] H. M. Khalid and J. C.-H. Peng, "Immunity toward data-injection attacks using multisensor track fusion-based model prediction," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 697–707, 2017.

[13] W. Ao, Y. Song, and C. Wen, "Adaptive cyber-physical system attack detection and reconstruction with application to power systems," *IET Control Theory & Applications*, vol. 10, no. 12, pp. 1458–1468, 2016.

[14] Z.-H. Yu and W.-L. Chin, "Blind false data injection attack using pca approximation method in smart grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 3, pp. 1219–1226, 2015.

[15] Z.-H. Pang, G.-P. Liu, D. Zhou, F. Hou, and D. Sun, "Two-channel false data injection attacks against output tracking control of networked systems," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 5, pp. 3242–3251, 2016.

[16] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 198–207, 2017.

[17] 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.

[18] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505–2516, 2017.

[19] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 27, no. 8, pp. 1773–1786, 2016.

[20] A. Abdullah, "Ultrafast transmission line fault detection using a dwt based ann," *IEEE Transactions on Industry Applications*, 2017.

[21] S. Jana and A. De, "A novel zone division approach for power system fault detection using ann-based pattern recognition technique," *Canadian Journal of Electrical and Computer Engineering*, vol. 40, no. 4, pp. 275–283, 2017.

[22] P. Bangalore and L. B. Tjernberg, "An artificial neural network approach for early fault detection of gearbox bearings," *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 980–987, 2015.

[23] J. Yan, H. He, X. Zhong, and Y. Tang, "Q-learning-based vulnerability analysis of smart grid against sequential topology attacks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 200–210, 2017.

[24] S. A. Foroutan and F. R. Salmasi, "Detection of false data injection attacks against state estimation in smart grids based on a mixture gaussian distribution learning method," *IET Cyber-Physical Systems: Theory & Applications*, vol. 2, no. 4, pp. 161–171, 2017.

[25] W. Xu, Z. Wang, L. Hu, and J. Kurths, "State estimation under joint false data injection attacks: Dealing with constraints and insecurity," *IEEE Transactions on Automatic Control*, vol. 67, no. 12, pp. 6745–6753, 2021.

[26] Y. Huang and J. Zhao, "Switched stackelberg game analysis of false data injection attacks on networked control systems," *Kybernetika*, vol. 56, no. 2, pp. 261–277, 2020.

[27] M. Khalaf, A. Youssef, and E. El-Saadany, "Joint detection and mitigation of false data injection attacks in agc systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 4985–4995, 2018.

[28] A. Sargolzaei, K. Yazdani, A. R. Abbaspour, C. D. Crane, and W. Dixon, "Detection and mitigation of false data injection attacks in networked control systems," *IEEE Transactions on Industrial Informatics*, 2019.

[29] M. Al Janaideh, E. Hammad, A. Farraj, and D. Kundur, "Mitigating attacks with nonlinear dynamics on actuators in cyber-physical mechatronic systems," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 9, pp. 4845–4856, 2019.

[30] A. Abbaspour, P. Aboutalebi, K. K. Yen, and A. Sargolzaei, "Neural adaptive observer-based sensor and actuator fault detection in nonlinear systems: Application in uav," *ISA transactions*, vol. 67, pp. 317–329, 2017.

[31] A. Sargolzaei, B. C. Allen, C. D. Crane, and W. E. Dixon, "Lyapunov-based control of a nonlinear multiagent system with a time-varying input delay under false-data-injection attacks," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 2693–2703, 2021.

[32] N. Sharma, S. Bhasin, Q. Wang, and W. E. Dixon, "Rise-based adaptive control of a control affine uncertain nonlinear system with unknown state delays," *IEEE Transactions on Automatic Control*, vol. 57, no. 1, pp. 255–259, 2011.

[33] J. C. Holland, F. Javidi-Niroumand, A. Ala'J, and A. Sargolzaei, "A testing and verification approach to tune control parameters of cooperative driving automation under false data injection attacks," *IEEE Access*, 2024.

[34] N. Fischer, R. Kamalapurkar, N. Fitz-Coy, and W. E. Dixon, "Lyapunov-based control of an uncertain euler-lagrange system with time-varying input delay," in *2012 American Control Conference (ACC)*, pp. 3919–3924, IEEE, 2012.

[35] N. E. Cotter, "The stone-weierstrass theorem and its application to neural networks," *IEEE Transactions on Neural Networks*, vol. 1, no. 4, pp. 290–295, 1990.

[36] R. R. Selmic and F. L. Lewis, "Neural-network approximation of piecewise continuous functions: application to friction compensation," *IEEE transactions on neural networks*, vol. 13, no. 3, pp. 745–751, 2002.

[37] I. Chakraborty, S. S. Mehta, E. Doucette, and W. E. Dixon, "Control of an input delayed uncertain nonlinear system with adaptive delay estimation," in *2017 American Control Conference (ACC)*, pp. 1779–1784, IEEE, 2017.

[38] M. Krstic, P. V. Kokotovic, and I. Kanellakopoulos, *Nonlinear and adaptive control design*. John Wiley & Sons, Inc., 1995.