

PhD Forum 2022 - Design of False Data Injection Attacks and their Detection and Mitigation in Cyber-Physical Systems

Sushree Padhan, Department of Computer Science and Engineering, NIT Rourkela, Odisha, India

Guide: Prof. Ashok Kumar Turuk, Department of Computer Science and Engineering, NIT Rourkela, Odisha, India

Abstract—False data injection (FDI) attacks are more common in Cyber-Physical Systems (CPSs). In an FDI attack, an attacker can inject an attack sequence at any location in the CPS. Rather than analyzing attacks at a specific location, it is necessary to analyze the system's behavior in the presence of FDI attacks at multiple locations. Both the cyber and physical systems are vulnerable to FDI attacks. In this work, we study FDI attacks at multiple locations in a CPS. We examine FDI attacks at the sensor, actuator, and physical system. In the worst-case scenario, an attacker could guess the system parameters and remain stealthy by carefully planning the attack sequences. An attacker may inject zero-mean or non-zero-mean attack sequences, which brings the system to an unsafe state. Therefore, it is required to design a suitable detection and mitigation schemes to secure the CPS against FDI attacks. We design an FDI attack scheme in a single sensor and actuator framework and multiple sensors and actuators framework of the CPS. A detection and mitigation strategy against FDI attacks is also proposed.

Index Terms—Cyber-physical systems, false data injection attacks, attack detection, attack mitigation, CPS security.

I. INTRODUCTION

Cyber-physical systems (CPSs) are in-depth integration of computation, communication, and control technology. It employs a closed-loop feedback system to control physical processes automatically. CPSs are widely used in various applications like smart grids, autonomous transportation, smart industry, agriculture, smart home, and the healthcare system. CPSs are vulnerable to a variety of malicious attacks due to their wide range of applications. Among them, integrity attacks like false data injection (FDI) attacks can target the maximum possible locations in a CPS at a time. An FDI attacker can design false data and insert it into the actual data to alter the system's correct operation while remaining undetected.

The study of FDI attacks can be divided into two categories: attack design and defence mechanisms against FDI attacks. Many researchers have proposed FDI attacks and their countermeasures like detection and mitigation considering a specific location or cyber-system security [1–9]. Some of them have worked on multiple locations of cyber-system [10–12]. A few of them have worked on both physical, and cyber-system security [13, 14]. So, it is necessary to analyze the system from maximum possible vulnerable locations. Some authors have worked on FDI attacks considering multiple sensors and actuators framework of CPSs. Some of them have proposed FDI attacks based on a single sensor and actuator framework. But, a few literatures are available on defense mechanism

against FDI attacks. Therefore, it is required to design security schemes against FDI attacks on a CPS of a single sensor and actuator framework as well as multiple sensors and actuators framework.

We found from the literature that an attacker's objective is to directly modify the sensor measurements, actuator inputs, and the physical system. In this work, we design FDI attacks considering multiple compromised locations: sensor, actuator, and physical system. We have examined the system under FDI attack at individual compromised locations as well as FDI attacks at multiple compromised locations at a time. In this work, we propose FDI attacks on the sensor, actuator, and physical system, individually and in combination. We propose detection, and mitigation scheme for the FDI attacks. The proposed schemes help the CPS to perform its operations securely even if an attacker injects FDI attack sequences on sensor measurements, actuator inputs, and physical system.

II. SYSTEM MODEL

The CPS is modeled as a discrete-time linear time-invariant (LTI) system with white Gaussian noise. The sensors monitor the physical system's state (process). A remote estimator with an χ^2 detector receives the sensor measurement (observation) of the physical process state. The estimator's output is transmitted to an LQG controller, which provides appropriate input to the physical system via an actuator. The Kalman filter is used as an estimator. It mitigates the impact of the system's Gaussian process noise and measurement noise. The following equations represent the state space model of the LTI system:

$$x_{t+1} = Ax_t + Bu_t + w_t \quad (1)$$

$$y_t = Cx_t + v_t \quad (2)$$

The process state equation is represented by equation (1). The measurement or observation equation is represented by equation (2). The process state is denoted by $x_t \in \mathbb{R}^n$, where $t \in \mathbb{N}$ is the time step. The measurement vector is represented by $y_t \in \mathbb{R}^m$. The controller's output vector is represented by $u_t \in \mathbb{R}^p$. \mathbb{R} represents a set of real numbers. The process noise and measurement noise are represented by w_t and v_t , respectively. Both the process noise and measurement noise are white Gaussian noise with covariance $Q \in \mathbb{R}^{n \times n}$ and $R \in \mathbb{R}^{m \times m}$ that meets the requirement $\mathbb{E}[w_t w_j^T] = \delta_{tj} Q$, $\mathbb{E}[v_t v_j^T] = \delta_{tj} R$, $\mathbb{E}[w_t v_j^T] = 0$, $\forall t, j \in \mathbb{N}$. δ_{ij} is the Kronecker

delta function typically applied in a discrete-time system. When $i = j$, the value of δ_{ij} is 1; otherwise, it is 0. The initial state of the process is $x_0 \sim \mathcal{N}(0, \Sigma_x)$. x_0 , process noise, and measurement noise are independent. $A \in \mathbb{R}^{n \times n}$, $B \in \mathbb{R}^{n \times p}$ and $C \in \mathbb{R}^{m \times n}$ are the state transition, control input, and measurement matrices, respectively. We assume that (A, B) is controllable and (C, A) is observable, which makes the Kalman filter stable. The attacker can modify the sensor measurement, the actuator input, and the physical system. Figure 1 shows the system model compromised by the attacker.

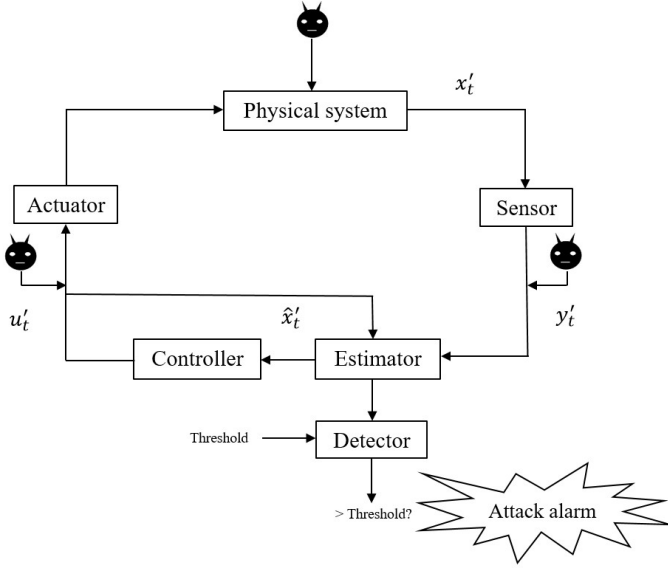


Figure 1: Model of a Cyber-Physical System with possible attack locations.

The attacker can design the attack sequences whose mean value may be zero or non-zero. We consider both the zero-mean and non-zero-mean attack cases. Let the attack sequence (for non-zero mean attack sequence) generated by the attacker to alter the actuator input, the physical system, and the sensor measurement be denoted as a_t^c , a_t^p , and a_t^s , respectively, where $\alpha, \beta, \gamma \in \{0, 1\}$. In the presence of an attack, the value of α , β , and γ is 1; otherwise, it is 0. Equations (3) and (4) represent the state and measurement equations of the compromised system.

$$x'_{t+1} = Ax'_t + B(u'_t + \alpha a_t^c) + \gamma a_t^p + w_t \quad (3)$$

$$y'_t = Cx'_t + \beta a_t^s + v_t \quad (4)$$

The Kalman filter is mathematically modeled as:

$$\hat{x}'_{t|t-1} = A\hat{x}'_{t-1} + Bu'_{t-1} \quad (5)$$

$$P_{t|t-1} = AP_{t-1}A^T + Q \quad (6)$$

$$K_t = P_{t|t-1}C^T(CP_{t|t-1}C^T + R)^{-1} \quad (7)$$

$$\hat{x}'_t = \hat{x}'_{t|t-1} + K_t(y'_t - C\hat{x}'_{t|t-1}) \quad (8)$$

$$P_t = (I - K_tC)P_{t|t-1} \quad (9)$$

Equations (5) and (6) represent the time update equations. $\hat{x}'_{t|t-1}$ is a priori estimate of the system state at the time step t , and its error covariance is $P_{t|t-1}$. The system state is initially estimated to be $\hat{x}_{0|-1} = 0$, and its error covariance is $P_{0|-1} = \Sigma_x$. $(\cdot)^T$ denotes transpose of a matrix. Equations (7), (8), and (9) are called measurement update equations. K_t represents the Kalman filter gain. \hat{x}'_t is a posteriori estimate of the system state at the time step t , and its error covariance is P_t . The expression $y'_t - C\hat{x}'_{t|t-1}$ is defined as residue z'_t in equation (10), and the expression $x'_t - \hat{x}'_t$ is defined as the state estimation error e'_t in equation (11).

$$z'_t \triangleq y'_t - C\hat{x}'_{t|t-1} \quad (10)$$

$$e'_t \triangleq x'_t - \hat{x}'_t \quad (11)$$

When the time approaches infinity, the values of $P_{t|t-1}$ and K_t are constant, and the Kalman filter is said to be in a steady state. In the steady state of the Kalman filter, $P_{t|t-1}$ and K_t equations can be rewritten as equations (12) and (13), respectively.

$$P \triangleq \lim_{t \rightarrow \infty} P_{t|t-1} \quad (12)$$

$$K \triangleq PC^T(CPC^T + R)^{-1} \quad (13)$$

In the steady-state of the Kalman filter, the value of P is obtained by solving the discrete-time algebraic Riccati equation [10]:

$$-P + APA^T - APC^T(CPC^T + R)^{-1}CPA^T + Q = 0.$$

The Kalman filter is assumed to be in a steady state. The posteriori estimated state equation can be rewritten as:

$$\begin{aligned} \hat{x}'_{t+1} &= A\hat{x}'_t + Bu'_t + K(y'_{t+1} - C(A\hat{x}'_t + Bu'_t)) \\ &= A\hat{x}'_t + Bu'_t + Kz'_{t+1}. \end{aligned} \quad (14)$$

The estimated state calculated in equation (14) is transmitted to the controller to reduce the cost function:

$$J = \min \lim_{T \rightarrow \infty} \frac{1}{T} \mathbb{E} \left[\sum_{t=0}^{T-1} (x'^T_t G x'_t + u'^T_t H u'_t) \right]$$

where G and H are positive weight matrices [6]. $\mathbb{E}[\cdot]$ denotes expectation (or mean). The controller sends input to the physical system. The controller output is $u'_t = L\hat{x}'_t$. The controller gain, L , is calculated as:

$$L = -(B^T F B + H)^{-1} B^T F A$$

where F is the solution of the Riccati equation:

$$F = G + A^T F A - A^T F B (H + B^T F B)^{-1} B^T F A.$$

We use the χ^2 test to detect FDI attacks. The detector tests χ^2 value of observation, i.e., $(y'_t - C\hat{x}'_{t|t-1})^T \Sigma_z^{-1} (y'_t - C\hat{x}'_{t|t-1})$. In the absence of an attack, $z'_t = y'_t - C\hat{x}'_{t|t-1}$ has zero-mean and covariance $(CPC^T + R)$. An appropriate threshold value, $\eta > m$, is fed into the detector where m is the degree of freedom and $\mathbb{E}[z'^T_t \Sigma_z^{-1} z'_t] = m$. If the χ^2 value is greater than η , there is an attack; otherwise, there is no attack. Two

hypotheses, H_1 and H_0 are assumed based on the presence or absence of attack. If the χ^2 value of observation, $z_t'^T \Sigma_z^{-1} z_t'$, is greater than η , we accept H_1 hypothesis and reject H_0 and vice versa. This is indicated as: $z_t'^T \Sigma_z^{-1} z_t' \underset{H_1}{\overset{H_0}{\leq}} \eta$. The attacker always attempts to remain undetected by keeping the χ^2 value less than or equal to η and increasing the state estimation error.

III. FDI ATTACK DESIGN

The attacker attempts to alter the system's state while avoiding detection ($z_t'^T \Sigma_z^{-1} z_t' \leq \eta$). To remain undetected, the attacker will carefully plan attack sequences. We consider each possible attack location—actuator, physical system, and sensor—individually and in combination while designing the attack sequence ($a_t^c, a_t^p, a_t^s, \{a_t^c, a_t^p\}, \{a_t^s, a_t^c\}, \{a_t^s, a_t^p\}, \{a_t^c, a_t^p\}$) [15]. We assume that the attacker knows the vital system parameters, including the χ^2 detector. The expected value of the attack sequence is non-zero. The attacker can change the actuator input, physical system, and sensor measurement. The above leads to seven possible attack types. They are:

- i. a_t^c : Attacker can compromise the actuator only ($\alpha = 1, \gamma = 0$ and $\beta = 0$).
- ii. a_t^p : Attacker can compromise the physical system only ($\alpha = 0, \gamma = 1$ and $\beta = 0$).
- iii. a_t^s : Attacker can compromise the sensor only ($\alpha = 0, \gamma = 0$ and $\beta = 1$).
- iv. $\{a_t^c, a_t^p\}$: Attacker can compromise both the actuator and physical system ($\alpha = 1, \gamma = 1$ and $\beta = 0$).
- v. $\{a_t^s, a_t^c\}$: Attacker can compromise both the sensor and actuator ($\alpha = 1, \gamma = 0$ and $\beta = 1$).
- vi. $\{a_t^s, a_t^p\}$: Attacker can compromise both the sensor and physical system ($\alpha = 0, \gamma = 1$ and $\beta = 1$).
- vii. $\{a_t^c, a_t^p, a_t^s\}$: Attacker can compromise the sensor, actuator, and physical system ($\alpha = 1, \gamma = 1$, and $\beta = 1$).

We have proposed the non-zero-mean FDI attack sequences for each attack type in our previous work [15].

For zero-mean Gaussian distributed FDI attack sequences, the proposed attack design mechanism is as follows:

The zero-mean FDI attack sequences for the compromised actuator, physical system, and sensor are denoted as a_t^{c*}, a_t^{p*} , and a_t^{s*} , respectively. Similar to non-zero-mean attack sequences, the seven possible zero-mean Gaussian distributed attack sequences are $a_t^{c*}, a_t^{p*}, a_t^{s*}, \{a_t^{c*}, a_t^{p*}\}, \{a_t^{s*}, a_t^{c*}\}, \{a_t^{s*}, a_t^{p*}\}$, and $\{a_t^{c*}, a_t^{p*}, a_t^{s*}\}$. The attack sequence follows zero-mean Gaussian distribution with certain covariance, which is computed so that the attack remains undetected. If there is no attack in the system, the residue of observation follows $z_t' \sim \mathcal{N}(0, \Sigma_z)$. That means z_t' has zero mean and covariance $\Sigma_z = CPC^T + R$. If there is an attack in the system, the probability distribution of the residue will be different. The residue of the observation follows $z_t' \sim \mathcal{N}(0, \Sigma_z')$. The attacker wants to maximize the difference between Σ_z and Σ_z' and also wants to remain stealthy. The difference in probability distributions between the observation residue without attack

and with attack can be calculated using Kullback Leibler (KL) divergence. The attacker wants to maximize the difference between two probability distributions and maintain the detector output less than or equal to the threshold value. Let us take the probability distribution function of z_t' without attack and with attack as $pd_0 = \mathcal{N}(0, \Sigma_z)$ and $pd_1 = \mathcal{N}(0, \Sigma_z')$, respectively. The KL divergence between two probability distributions is denoted as $D(pd_0 || pd_1)$. Let the attack sequences follow $a_t^{c*} \sim \mathcal{N}(0, \Sigma_c)$, $a_t^{p*} \sim \mathcal{N}(0, \Sigma_p)$, and $a_t^{s*} \sim \mathcal{N}(0, \Sigma_s)$. To calculate the covariance of each attack sequence, we have derived a formula for the covariance matrix of each attack type. It is required to compute the covariance Σ_z' for the calculation of covariance matrix of each attack type. We have proposed a formula for the optimized value of the covariance matrix Σ_z' . The proposed formula is derived by solving an optimization problem: maximize Σ_z' such that $z_t'^T \Sigma_z^{-1} z_t' \leq \eta$.

IV. FDI ATTACK DETECTION

We follow a watermarking principle for faster detection of FDI attacks. Assume that a watermarking signal is used on the sensor measurement before an attack happens. The measurement equation before an attack is:

$$\bar{y}_t = \varphi(Cx_t + v_t) \quad (15)$$

where φ is a watermark multiplied to the measurement $y_t = Cx_t + v_t$ and $\varphi \in \mathbb{R}^{m \times m}$ is invertible. We also assume that the attacker does not know the watermark. When an attacker injects false data into the measurement, then the measurement equation is:

$$\bar{y}_t' = \varphi(Cx_t' + v_t) + a_t^s \quad (16)$$

When the compromised measurement goes to the estimator, it is multiplied with the inverse of φ to get the original measurement. Then the measurement becomes:

$$\varphi^{-1} \bar{y}_t' = \varphi^{-1} \varphi Cx_t' + \varphi^{-1} \varphi v_t + \varphi^{-1} a_t^s = Cx_t' + v_t + \varphi^{-1} a_t^s \quad (17)$$

Figure 3 shows the detection mechanism. We propose the necessary condition for the watermark signal and its effect on the system after using the watermarking scheme. The purpose of the watermarking scheme is to help the χ^2 test in faster detection of attacks. The attacker can inject a stealthy attack using zero-mean Gaussian noise or non-zero mean stealthy attack sequence.

V. FDI ATTACK MITIGATION

We have considered the steady-state of the Kalman filter. There are a few papers on attack mitigation under steady state filter gain. We use a concept similar to [12]. We consider the LTI system as mentioned in this report and define the operating regions of the CPS first. The operating region is classified into two sub-regions: safe region and preferable operating region as shown in Figure 2. The safe and the preferable operating regions are denoted as \mathcal{X}_S and \mathcal{X}_O , respectively, where $\mathcal{X}_O \subset \mathcal{X}_S$. If the system goes beyond the \mathcal{X}_S region, then the system goes to an unsafe state. The \mathcal{X}_O region means starting from

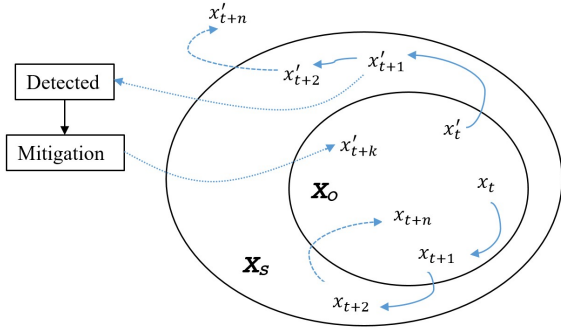


Figure 2: System's operating regions (safe region \mathcal{X}_S and preferable operating region \mathcal{X}_O).

any point inside \mathcal{X}_O the system will remain within the \mathcal{X}_S region when there is no attack. If the detector detects any attack, the controller's job is to perform the mitigation process and return the system to the \mathcal{X}_O region within a time frame.

We know that the system's correct operation depends on the true state (x_t) and the estimated state (\hat{x}_t) of the system. So the \mathcal{X}_O size depends on these x_t and \hat{x}_t . We take an augmented system state $\mathcal{X}_t = \begin{bmatrix} x_t \\ \hat{x}_t \end{bmatrix}$ and the required augmented matrices. We define an optimization problem that needs to be solved to get the required \mathcal{X}_O region using the augmented state, matrices, and sensor and actuation limit of the system. The optimization problem is solved by the YALMIP tool in MATLAB.

It is assumed that the system is inside the region $\mathcal{X}_S \setminus \mathcal{X}_O$ after an attack gets detected, which can be safely considered [12] as we will perform attack mitigation before incorporating the control inputs. We can say that there exist some control inputs from any initial state \mathcal{X}_0 that belongs to the region $\mathcal{X}_S \setminus \mathcal{X}_O$ such that after time k it will be back to the region \mathcal{X}_O . So we compute k control inputs. The goal to bring back the system to the \mathcal{X}_O region should be fulfilled from every initial state inside the $\mathcal{X}_S \setminus \mathcal{X}_O$ region. To ensure the system never goes beyond the \mathcal{X}_S region while bringing back the system to \mathcal{X}_O region, we plan the problem of control input computation into a Satisfiability Modulo Theory (SMT) process as in [12]. Similarly, we combine the LQG controller with an open loop control inputs so that according to the computed control inputs, the system returns to the \mathcal{X}_O region. The mitigation process is called to get the required control inputs if the detector detects an attack as shown in Figure 3. Otherwise, we use the normal LQG control process.

We will use Z3py to solve the problem, which requires a Python environment. For the effectiveness of the proposed work, we will perform all simulations through numerical examples in MATLAB. Our current work is on a CPS of a single sensor and actuator framework, and attack sequences are based on either zero-mean or non-zero mean. We will work on FDI attacks considering multiple sensors and actuators framework of the CPS for both attack cases. The proposed scheme is expected to secure the CPS against FDI attacks at

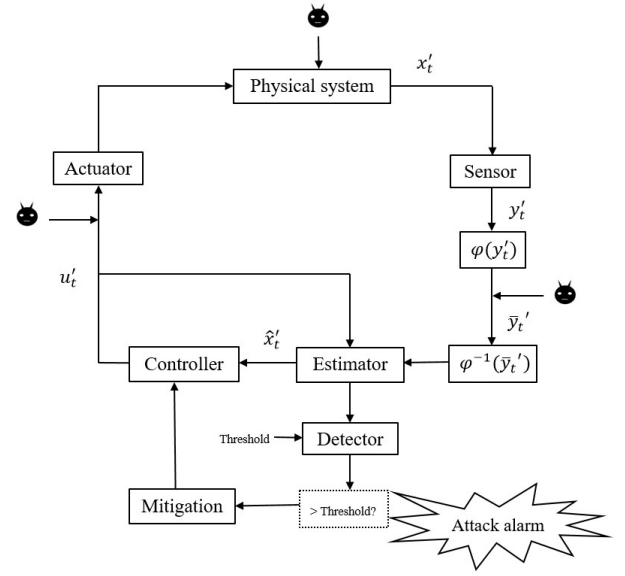


Figure 3: Model of a CPS with possible attack locations and defense mechanisms.

the compromised sensor, actuator, and physical system.

VI. RESULTS

In this section, we observe the effects of each type of FDI attack through a numerical example. The parameters are set as follows [15]: $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, $C = [1 \ 1]$, $Q = G = I_{2 \times 2}$, $R = H = 1$, $\Sigma_x = I_{2 \times 2}$ and $\eta = 6.635$. Here, the system state is $x_t \in \mathbb{R}^2$, $x_t = \begin{bmatrix} x_{1t} \\ x_{2t} \end{bmatrix}$. The plots for state estimation error with respect to x_1 , i. e., e_1 and state estimation error with respect to x_2 , i. e., e_2 are shown in Figures 4 and 5, respectively.

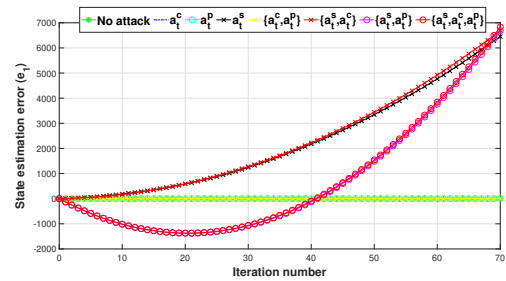


Figure 4: State Estimation Error (e_1) under different FDI attacks.

It is observed from Figures 4 and 5 that $\{a_t^s, a_t^c, a_t^p\}$ generates more state estimation error than other types. Error is unbounded in a_t^s , $\{a_t^s, a_t^c\}$, $\{a_t^s, a_t^p\}$ and $\{a_t^s, a_t^c, a_t^p\}$ with increasing time step. Attack types a_t^c , a_t^p and $\{a_t^c, a_t^p\}$ generates less error and is bounded. It is observed from Figure 4 that state estimation error increases exponentially in a_t^s , $\{a_t^s, a_t^c\}$, $\{a_t^s, a_t^p\}$ and $\{a_t^s, a_t^c, a_t^p\}$ with increasing time steps. But, some negative state estimation error is initially generated in $\{a_t^s, a_t^p\}$ and $\{a_t^s, a_t^c, a_t^p\}$ types. It is observed from Figure

5 that state estimation error increases linearly in a_t^s , $\{a_t^s, a_t^c\}$, $\{a_t^s, a_t^p\}$ and $\{a_t^s, a_t^c, a_t^p\}$ with increasing time steps. The plot for the stealthiness of each attack type is shown in Figure 6. It is observed from Figure 6 that a_t^s is strictly stealthy, but other types get detected at some points.

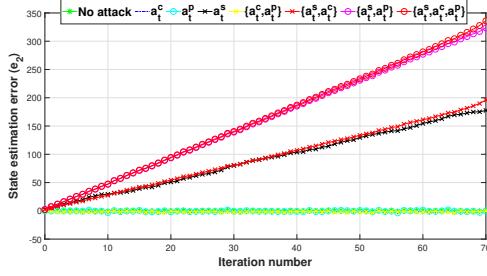


Figure 5: State Estimation Error (e_2) under different FDI attacks.

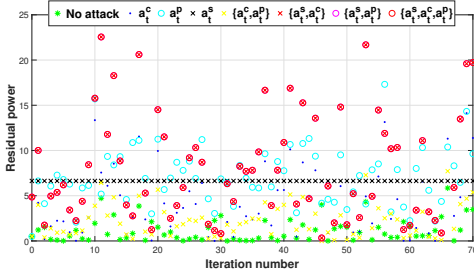


Figure 6: Detection result under different FDI attacks.

VII. CONCLUSIONS

In this paper, we have proposed FDI attacks at multiple vulnerable locations in a CPS of single sensor and actuator framework. It is assumed that the attacker knows the vital system parameters and can use non-zero mean or zero-mean FDI attack sequences to modify the system's state. We have proposed a detection scheme for faster detection of FDI attacks. We have assumed that the detector does not know about the attacker. Currently, we are implementing the proposed mitigation strategy. In future, we will work on FDI attacks and defense mechanisms considering multiple sensors and actuators framework of the CPS in MATLAB/Simulink.

REFERENCES

- [1] Y. Mo and B. Sinopoli, "On the performance degradation of cyber-physical systems under stealthy integrity attacks," *IEEE Transactions on Automatic Control*, vol. 61, no. 9, pp. 2618–2624, 2015.
- [2] F. Li and Y. Tang, "False data injection attack for cyber-physical systems with resource constraint," *IEEE transactions on cybernetics*, vol. 50, no. 2, pp. 729–738, 2018.
- [3] X. L. Wang, "Optimal attack strategy against fault detectors for linear cyber-physical systems," *Information Sciences*, vol. 581, pp. 390–402, 2021.
- [4] W. Tu, J. Dong, and D. Zhai, "Optimal ϵ -stealthy attack in cyber-physical systems," *Journal of the Franklin Institute*, vol. 358, no. 1, pp. 151–171, 2021.
- [5] C. Wang, J. Huang, D. Wang, and F. Li, "A secure strategy for a cyber physical system with multi-sensor under linear deception attack," *Journal of the Franklin Institute*, vol. 358, no. 13, pp. 6666–6683, 2021.
- [6] D. Ye and T. Zhang, "Summation detector for false data-injection attack in cyber-physical systems," *IEEE Transactions on Cybernetics*, vol. 50, no. 6, pp. 2338–2345, 2020.
- [7] J. Zhou, W. Yang, W. Ding, W. X. Zheng, and Y. Xu, "Watermarking-based protection strategy against stealthy integrity attack on distributed state estimation," *IEEE Transactions on Automatic Control*, vol. 68, no. 1, pp. 628–635, 2022.
- [8] J. Hua and F. Hao, "Fusion and detection for multi-sensor systems under false data injection attacks," *ISA transactions*, 2022.
- [9] E. Tian, Z. Wu, and X. Xie, "Codesign of fdi attacks detection, isolation, and mitigation for complex microgrid systems: An hbf-nn-based approach," *IEEE Transactions on Neural Networks and Learning Systems*, 2022.
- [10] C. Kwon, W. Liu, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," in *2013 American control conference*, pp. 3344–3349, IEEE, 2013.
- [11] G. Chen, Y. Zhang, S. Gu, and W. Hu, "Resilient state estimation and control of cyber-physical systems against false data injection attacks on both actuator and sensors," *IEEE Transactions on Control of Network Systems*, 2021.
- [12] I. Koley, S. Adhikary, and S. Dey, "Catch me if you learn: Real-time attack detection and mitigation in learning enabled cps," in *2021 IEEE Real-Time Systems Symposium (RTSS)*, pp. 136–148, IEEE, 2021.
- [13] Y. Guan and X. Ge, "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 48–59, 2017.
- [14] D. Ding, Q. L. Han, X. Ge, and J. Wang, "Secure state estimation and control of cyber-physical systems: A survey," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 1, pp. 176–190, 2021.
- [15] S. Padhan and A. K. Turuk, "Design of false data injection attacks in cyber-physical systems," *Information Sciences*, vol. 608, pp. 825–843, 2022.