SCIENCE CHINA
Information Sciences

• LETTER •

July 2023, Vol. 66 179203:1–179203:2
https://doi.org/10.1007/s11432-021-3428-y

# Nonlinear fusion estimation for false data injection attack signals in cyber-physical systems

Yawen TAN[1,2], Pindi WENG[1,2], Bo CHEN[1,2*] & Li YU[1,2]

[1]*Department of Automation, Zhejiang University of Technology, Hangzhou* 310023*, China;*
[2]*Institute of Cyberspace Security, Zhejiang University of Technology, Hangzhou* 310023*, China*

Received 12 April 2021/Revised 20 August 2021/Accepted 23 December 2021/Published online 11 January 2023

**Citation** Tan Y W, Weng P D, Chen B, et al. Nonlinear fusion estimation for false data injection attack signals in cyber-physical systems. Sci China Inf Sci, 2023, 66(7): 179203, https://doi.org/10.1007/s11432-021-3428-y

Cyber-physical systems (CPSs) that integrate computation, network, and physical objects play essential roles in the era of Industry 4.0 [1,2]. However, the introduction of networks makes it face the threat of cyber-attacks [3]. Among various types of cyber-attacks, a false data injection (FDI) attack degrades the estimation performance for CPSs by injecting wrong signals and is one of the most dangerous attacks [4,5]. Therefore, the joint estimation of FDI attacks and system states is of great significance to the security of CPSs.

This study investigates the distributed fusion estimation problem for nonlinear CPSs, where the control signals are tampered with by FDI attacks. By combining the recursive least squares (RLS) method and multi-distribution particle filter, nonlinear local and fusion estimators are proposed to estimate system states and FDI attack signals. Simulations, as presented in Appendix B, and experiments are employed to demonstrate the effectiveness of the proposed methods.

*Problem formulations.* Consider nonlinear CPSs, where the physical process and sensor measurements are modeled as

$$\begin{cases} x(k) = f(x(k-1)) + B(k)u_a(k) + \omega(k-1), \\ y_i(k) = h_i(x(k)) + \nu_i(k),\ i = 1, 2, \ldots, L, \end{cases} \tag{1}$$

where $x(k) \in \mathbb{R}^n$ is the system state, $y_i(k) \in \mathbb{R}^m$ is the measurement of the $i$-th sensor, $u_a(k) \in \mathbb{R}^p$ is the control signal after being attacked, $B(k)$ is the control input matrix, $f$ and $h_i$ are the nonlinear state and measurement function, respectively, and $\omega(k)$ and $\nu_i(k)$ are mutually uncorrelated zero-mean Gaussian noises with covariance $Q$ and $R_i$.

Then, the local and fusion estimators are given as follows:

$$\begin{aligned} &\hat{a}_i(k) = \frac{1}{M}\sum_{j=1}^{M}\hat{a}_i^{(j)}(k), \quad \hat{x}_i(k) = \frac{1}{M}\sum_{j=1}^{M}\hat{x}_i^{(j)}(k), \\ &\hat{a}(k) = \sum_{i=1}^{L}W_i^a(k)\hat{a}_i(k), \quad \hat{x}(k) = \sum_{i=1}^{L}W_i^x(k)\hat{x}_i(k), \end{aligned} \tag{2}$$

where $M$ is the particle number; $\hat{a}_i(k)$, $\hat{x}_i(k)$, $\hat{a}(k)$, and $\hat{x}(k)$ are the local attack estimate (LAE), local state estimate (LSE), the fusion attack estimate (FAE), and fusion state estimate (FSE), respectively; $\hat{a}_i^{(j)}(k)$ and $\hat{x}_i^{(j)}(k)$ are the $j$-th LAE and the $j$-th LSE particles of the $i$-th local estimator, respectively. $W_i^a(k)$, $W_i^x(k)$ are weighting fusion matrices.

*Methodology.* According to the results in [6], $W^a(k)$ and $W^x(k)$ in (2) can be obtained as follows:

$$\begin{cases} W^a(k) = (e_a P_a^{-1}(k) e_a^{\mathrm{T}})^{-1} e_a P_a^{-1}(k), \\ W^x(k) = (e_x P_x^{-1}(k) e_x^{\mathrm{T}})^{-1} e_x P_x^{-1}(k), \end{cases} \tag{3}$$

where $P_a(k) = \{P_{ij}^a(k)\}$, $P_x(k) = \{P_{ij}^x(k)\}$, $W^a(k) = [W_1^a(k), \ldots, W_L^a(k)]$, $W^x(k) = [W_1^x(k), \ldots, W_L^x(k)]$, $e_a = [I_p, \ldots, I_p] \in \mathbb{R}^{p\times Lp}$, $e_x = [I_n, \ldots, I_n] \in \mathbb{R}^{n\times Ln}$. $P_{ij}^a(k)$, $P_{ij}^x(k)$ are the estimation error cross-covariance of the state and attack signal between the local estimators $i$ and $j$.

Note that $P_{ij}^a(k)$ and $P_{ij}^x(k)$ are not easy to obtain in nonlinear systems. Thus, this study adopts particle filter as the local estimator and uses statistical cross-covariance $\bar{P}_{ij}^a(k)$ and $\bar{P}_{ij}^x(k)$ to approximate $P_{ij}^a(k)$ and $P_{ij}^x(k)$.

$$\begin{cases} \bar{P}_{ij}^a(k) = \dfrac{1}{M-1}\displaystyle\sum_{j=1}^{M}(\hat{a}_i(k) - \hat{a}_i^{(j)}(k))(\hat{a}_j(k) - \hat{a}_j^{(j)}(k))^{\mathrm{T}}, \\ \bar{P}_{ij}^x(k) = \dfrac{1}{M-1}\displaystyle\sum_{j=1}^{M}(\hat{x}_i(k) - \hat{x}_i^{(j)}(k))(\hat{x}_j(k) - \hat{x}_j^{(j)}(k))^{\mathrm{T}}. \end{cases} \tag{4}$$

For $\hat{a}_i^{(j)}(k)$ and $\hat{x}_i^{(j)}(k)$ in (2), they can be obtained by

$$\begin{cases} \hat{a}_i^{(j)}(k) \sim N(\bar{a}_i^{(l)}(k), S_i^{(l)}(k)), \\ \hat{x}_i^{(j)}(k) \sim N(\bar{x}_i^{(l)}(k), P_i^{(l)}(k)), \end{cases} \tag{5}$$

where $\bar{a}_i^{(l)}(k)$, $S_i^{(l)}(k)$ and $\bar{x}_i^{(l)}(k)$, $P_i^{(l)}(k)$ are intermediate variable and covariance of the $l$-th LAE and LSE particles, respectively. "$\sim$" denotes the sampled process.

Using Theorem 1 (see Appendix A), $\bar{a}_i^{(j)}(k)$ and $\bar{x}_i^{(j)}(k)$

* Corresponding author (email: bchen@zjut.edu.cn)

 

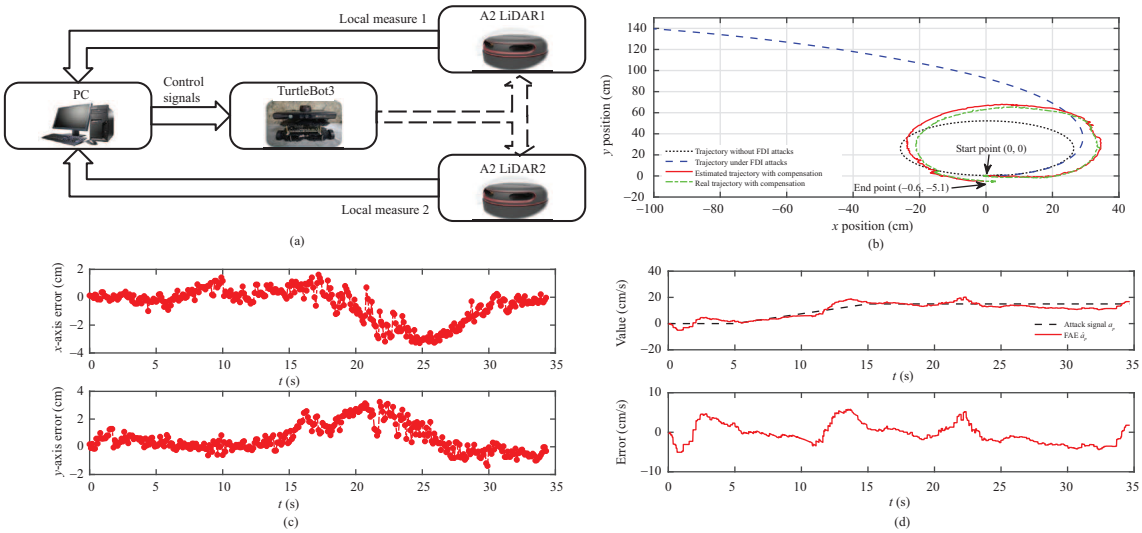


**Figure 1** (Color online) (a) Illustration of mobile robot experiment platform; (b) trajectories of the mobile robot; (c) estimation error of FSE; (d) top: real and FAE values of attack signal $a_p$; bottom: estimation error of FAE.

can be obtained from the following equations:

$$\begin{cases} \bar{a}_i^{(j)}(k) = \hat{a}_i^{(j)}(k-1) + \Gamma_i^{(j)}(k)\varepsilon_i^{(j)}(k), \\ \bar{x}_i^{(j)}(k) = x_{p,i}^{(j)}(k) + [K_i^{(j)}(k) + \Upsilon_i^{(j)}(k)\Gamma_i^{(j)}(k)]\varepsilon_i^{(j)}(k). \end{cases} \tag{6}$$

In summary, the computation procedures for deriving $\hat{x}(k)$ and $\hat{a}(k)$ are shown in Algorithm 1.

**Algorithm 1** Nonlinear fusion estimator against FDI attacks

1: Calculate $\bar{x}_i^{(j)}(k)$ and $\bar{a}_i^{(j)}(k)$ by (6);
2: Obtain $\hat{x}_i^{(j)}(k)$ and $\hat{a}_i^{(j)}(k)$ by (5);
3: Calculate $\hat{x}_i(k)$ and $\hat{a}_i(k)$ by (2);
4: Calculate $\bar{P}_{ij}^x(k)$, $\bar{P}_{ij}^a(k)$ and $W_i^x(k)$, $W_i^a(k)$ by (4) and (3), respectively;
5: Calculate $\hat{x}(k)$ and $\hat{a}(k)$ by (2);

**Remark 1.** To reduce the impact of FDI attacks, the control signal $u_a(k)$ in (1) is compensated by

$$u_c(k) = u(k) + a(k) - \hat{a}(k-1). \tag{7}$$

Then, Eq. (7) shows that when the attack signal changes slowly, the higher the accuracy of the fusion estimation is, the less damage the system will suffer.

*Experiment result.* Consider a mobile robot tracking experimental platform whose structure is shown in Figure 1(a) (see Appendix C for details of the experimental platform). In this experiment, only the linear velocity is tampered with by FDI attacks, causing the mobile robot to quickly deviate from the original trajectory.

The experiment results are shown in Figures 1(b)–(d). As shown in Figure 1(b), the proposed nonlinear fusion estimator can estimate the real trajectory of the mobile robot well. Meanwhile, Figure 1(c) shows that the tracking error is smaller than the size of the mobile robot. Figure 1(b) also shows that the impact of FDI attacks can be reduced by implementing the compensation method in Remark 1. Figure 1(d) shows the trajectories of the attack signal and its estimated value, demonstrating that the proposed methods can estimate the attack signal. However, the estimation performance in the experiment is slightly worse than the simulation in Appendix B. The main reasons for the estimation performance deterioration in the experiment are discussed in Appendix D.

*Conclusion.* This study investigated the distributed fusion estimation problem in nonlinear CPSs, where control signals are tampered with by FDI attacks. First, local estimators were designed using the RLS method and multi-distribution particle filter jointly to estimate the system state and attack signal. Then, the weighting fusion criteria were designed based on statistical information of particles to improve the estimation accuracy. In particular, the fusion estimate of the attacks was used to reduce the impact caused by FDI attacks. Finally, the effectiveness of the proposed method was demonstrated by simulations and experiments.

**Acknowledgements** This work was supported in part by National Natural Science Foundation of China (Grant Nos. 61973277, 62073292) and Zhejiang Provincial Natural Science Foundation of China (Grant Nos. LR20F030004, LY20F020030).

**Supporting information** Appendixes A–D. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

## References

1 Liu L, Ma L F, Zhang J, et al. Sliding mode control for nonlinear Markovian jump systems under denial-of-service attacks. IEEE CAA J Autom Sin, 2019, 7: 1638–1648
2 Ding D, Han Q L, Ge X H, et al. Secure state estimation and control of cyber-physical systems: a survey. IEEE Trans Syst Man Cybern Syst, 2021, 51: 176–190
3 Ge X H, Han Q L, Zhong M Y, et al. Distributed Krein space-based attack detection over sensor networks under deception attacks. Automatica, 2019, 109: 108557
4 Weng P D, Chen B, Yu L. Fusion estimate of FDI attack signals (in Chinese). Acta Autom Sin, 2021, 47: 2292–2300
5 Gao L J, Chen B, Yu L. Fusion-based FDI attack detection in cyber-physical systems. IEEE Trans Circ Syst II, 2019, 67: 1487–1491
6 Sun S L, Deng Z L. Multi-sensor optimal information fusion Kalman filter. Automatica, 2004, 40: 1017–1023