SCIENCE CHINA
Information Sciences

• LETTER •

June 2023, Vol. 66 169202:1–169202:2
https://doi.org/10.1007/s11432-021-3260-0

# Event-triggered state estimation for cyber-physical systems with partially observed injection attacks

Le LIU[1], Xudong ZHAO[1*], Bohui WANG[2], Yuanqing WU[3] & Wei XING[1]

[1] *The Key Laboratory of Intelligent Control and Optimization for Industrial Equipment (Dalian University of Technology), Ministry of Education, Dalian* 116000*, China;*
[2] *School of Aerospace Science and Technology, Xidian University, Xi'an* 710010*, China;*
[3] *School of Automation, Guangdong University of Technology, Guangzhou* 510006*, China*

Received 1 February 2021/Revised 18 March 2021/Accepted 30 April 2021/Published online 14 November 2022

**Citation** Liu L, Zhao X D, Wang B H, et al. Event-triggered state estimation for cyber-physical systems with partially observed injection attacks. Sci China Inf Sci, 2023, 66(6): 169202, https://doi.org/10.1007/s11432-021-3260-0

Dear editor,

Recently, because of the high-efficiency requirements of modern industrial engineering, cyber-physical systems (CPSs) have received increasing attention. A CPS often contains a huge communication network, making it work more efficiently. Owing to CPSs' high efficiency in industrial engineering, they have been extensively studied and explored in practice. However, there are challenges to be solved in the design of CPSs, e.g., the state estimation problem of CPSs. Since sensor data are transmitted to the fusion center over communication networks, the transmission causes high communication costs. An event-triggered estimation algorithm can provide an effective strategy to overcome these limitations. The event-triggered state estimation has recently attracted considerable attention [1–6]. For example, in [1], an optimal stochastic event-triggered estimation policy has been studied. However, the sensor network must transmit data together in the network's architecture. To overcome this limitation, the authors of [2] extended the single sensor case to the multisensor case. Because sensors usually have energy constraints in practical cases, an event-triggered estimation with energy constraints was probed in [3] based on hidden Markov models. However, secure state estimation with event-triggered policy has rarely been discussed. Inspired by [7–9], we propose a secure event-triggered estimation algorithm with side information. Under certain conditions, optimal state estimation in CPSs with partially observed injection attacks is studied. A recursive optimal estimation algorithm with a specified stochastic event-triggered schedule is proposed, and its stability is analyzed in this study.

*Problem formulation.* Consider the state estimation problem of the following linear time-varying CPS under attacks:

$$x_{k+1} = A_k x_k + G_k d_k + w_k, \tag{1}$$

where $x_k \in \mathbb{R}^n$ and $d_k \in \mathbb{R}^m$ are the state and injection attack signal in the process, respectively; $w_k \in \mathbb{R}^n$ is a zero mean independent and identically distributed (i.i.d.) Gaussian noise with covariance $Q_k \in \mathbb{R}^{n\times n}$, and $A_k$, $G_k$ are time-varying system matrices with appropriate dimensions. The initial state $x_0$ is Gaussian with $\mathbb{E}(x_0) = \hat{x}_0$ and covariance $P_0$.

A sensor network equipped with an event-triggered scheduler monitors the system described in (1). It is assumed that an attacker can launch injection attacks on the sensors. Hence, the observation equation can be written as follows:

$$y_k = C_k x_k + H_k e_k + v_k, \tag{2}$$

where $y_k \in \mathbb{R}^p$ is the sensor output manipulated by the attacker, $e_k \in \mathbb{R}^l$ is the injection attack signal in the measurement process, $v_k \in \mathbb{R}^p$ is a zero mean i.i.d. Gaussian noise with covariance $R_k \in \mathbb{R}^{p\times p}$, and $C_k$ is a time-varying system matrix with appropriate dimensions.

Following the conventions employed in [9], we assume that $\mathrm{rank}(H_k) = l$ and $\mathrm{rank}(G_k) = m$ in this study. Notably, we can interpret this $G_k$ as suspicious, malicious controllers; hence, it can be known by the system. The assumption on $G_k$ is quite common (e.g., [9] and references therein). In addition, it is unlikely to realize an optimal estimation if $G_k$ is unknown to the system. Although entries in $H_k$ will be 1 or 0 after the detection process in [7], we assume $H_k$ to be an arbitrary known matrix in this study because there is no difference between processing an arbitrary $H_k$ and processing a matrix with only 0 or 1 entries.

Define $\mathcal{I}_k$ as the set of all the information available to the remote estimator up to time $k$, i.e.,

$$\mathcal{I}_k \triangleq \{\gamma_0, \ldots, \gamma_k, \gamma_0 y_0, \ldots, \gamma_k y_k\}, \tag{3}$$

where $\gamma_k = 1$ and $\gamma_k = 0$ indicate, respectively, that the measurement $y_k$ is transmitted or not.

The following stochastic event-triggered schedule equipped in the sensor is employed in this study:

$$\phi_k(y_k) = \exp\left\{-\frac{1}{2} y_k^{\mathrm{T}} Y_k y_k\right\}, \tag{4}$$

[*] Corresponding author (email: xdzhaohit@gmail.com)

$$\Pr\left(\gamma_k = 0 | y_k = y, \mathcal{I}_{k-1}\right) = \phi_k(y), \tag{5}$$

$$\Pr\left(\gamma_k = 1 | y_k = y, \mathcal{I}_{k-1}\right) = 1 - \phi_k(y). \tag{6}$$

One can see Appendix C for more detailed discussion on the event-triggered policy.

In some real scenarios, partial data of the attack are available to the estimator (refer to Appendix B for an example). Hence, the system can improve estimation performance with the partial data. Therefore, we assume that some linear combinations of attacks $r_k$ and $q_k$ can be observed using the estimator:

$$r_k = D_k d_k, \quad q_k = E_k e_k, \tag{7}$$

where $r_k$ and $q_k$ stand for the partially observed data of $d_k$ and $e_k$ by the estimator, respectively, $D_k$ is a $p_1 \times m$-dimensional known matrix with $0 \leqslant p_1 \leqslant m$, and $E_k$ is a $p_2 \times l$-dimensional known matrix with $0 \leqslant p_2 \leqslant l$. Notably, if $D_k = O$ and $E_k = O$, no information about attacks can be observed using the estimator. Thus, the proposed method can handle the problem with no partial data.

Let $F_{0k}$ and $F_{1k}$ be orthogonal complements of $D_k^{\mathrm{T}}$ and $E_k^{\mathrm{T}}$. We also assume that information about $\delta_k^x = F_{0k}^{\mathrm{T}} d_k$ and $\delta_k^y = F_{1k}^{\mathrm{T}} e_k$ is unavailable to the system because of the random attack behavior, which means

$$f\left(\delta_k^x\right) \propto 1, \quad f\left(\delta_k^y\right) \propto 1. \tag{8}$$

*Estimation algorithm design.* Based on the event-triggered policy, we present the proposed estimation algorithm below.

**Theorem 1.** Provided matrix $\Pi_k = [{}^{D_{k-1}}_{N_k C_k G_{k-1}}]$ has a full column-rank, then for CPSs (1) and (2) with partially observed data specified by (7) and (8), the conditional mean $\hat{x}_k$ and covariance $P_{k|k}$ evolve according to the following recursive form:

$$\begin{aligned} \hat{x}_{k|k} =& A_{k-1}\hat{x}_{k-1|k-1} + P_{k|k}M_{k-1}^{\mathrm{T}} \\ & \times (M_{k-1}P_{k|k-1}M_{k-1}^{T})^{-1}\tilde{r}_{k-1} \\ & + K_k(\gamma_k N_k y_k - \tilde{q}_k - N_k C_k A_{k-1}\hat{x}_{k-1|k-1}), \end{aligned} \tag{9}$$

$$\begin{aligned} K_k =& P_{k|k-1}(N_kC_k)^{\mathrm{T}}\Theta_k^{-1} \\ & + \left[F_{k-1} - P_{k|k-1}(N_kC_k)^{T}\Theta_k^{-1}N_kC_kF_{k-1}\right] \\ & \times \left[F_{k-1}^{\mathrm{T}}(N_kC_k)^{\mathrm{T}}\Theta_k^{-1}N_kC_kF_{k-1}\right]^{-1} F_{k-1}^{\mathrm{T}}C_k^{\mathrm{T}}\Theta_k^{-1}, \end{aligned} \tag{10}$$

$$\begin{aligned} P_{k|k} =& P_{k|k-1} - P_{k|k-1}(N_kC_k)^{\mathrm{T}}\Theta_k^{-1}N_kC_kP_{k|k-1} \\ & + \left[F_{k-1} - P_{k|k-1}(N_kC_k)^{\mathrm{T}}\Theta_k^{-1}N_kC_kF_{k-1}\right] \\ & \times \left[F_{k-1}^{\mathrm{T}}(N_kC_k)^{\mathrm{T}}\Theta_k^{-1}N_kC_kF_{k-1}\right]^{-1} \\ & \times \left[F_{k-1} - P_{k|k-1}(N_kC_k)^{\mathrm{T}}\Theta_k^{-1}N_kC_kF_{k-1}\right]^{\mathrm{T}}. \end{aligned} \tag{11}$$

*Proof.* See Appendix D.

In Theorem 1, it can be observed that the proposed filter (a) reduces to the filter in [9] when $H_k = 0$ and there is no information on $d_k$, and (b) reduces to the classical Kalman filter when the sensor transmits the data every time step and all entries of $d_k$ and $e_k$ are observed. In other words, our result is an extension of existing results.

**Theorem 2.** If there exists $\tilde{K}_k$ such that $A_k - \tilde{K}_k N_{k+1} C_{k+1} A_k$ is exponentially stable for every $k$ and $\Pi_k$ has a full column-rank, the covariance matrix satisfying (11) is asymptotically bounded. The expectation of covariance matrix is bounded by a sequence of $\overline{P}_{k|k}$, which means $\mathbb{E}(P_{k|k}) \leqslant \overline{P}_{k|k}$, where

$$\begin{aligned} \overline{P}_{k|k} = & [M_{k-1}^{\mathrm{T}}(M_{k-1}\overline{P}_{k|k-1}M_{k-1}^{\mathrm{T}})^{-1}M_{k-1} \\ & + (N_kC_k)^{\mathrm{T}}(V_k - V_kN_kW_kN_k^{\mathrm{T}}V_k)N_kC_k]^{-1} \end{aligned} \tag{12}$$

with

$$\overline{P}_{k|k-1} = A_{k-1}\overline{P}_{k-1|k-1}A_{k-1}^{\mathrm{T}} + Q_{k-1} \tag{13}$$

and $\overline{P}_{0|0} = P_{0|0}$.

*Proof.* See Appendix E.

Trivially, when $A_k$ is stable, the condition is satisfied; hence, the estimator is exponentially stable.

Simulation results are provided in Appendix F.

*Conclusion.* In this study, an event-based estimator with partially observed injection attacks is investigated. Under a specified transmission schedule and partially observed injection attacks, we prove that the conditional distribution of the state is Gaussian with a Bayesian inference approach. Then, an event-triggered minimum mean square error estimation algorithm is acquired. Moreover, we show that the proposed optimal estimator is exponentially stable under certain conditions.

**Acknowledgements** This work was supported by National Natural Science Foundation of China (Grant Nos. U21A20477, 61722302), Liaoning Revitalization Talents Program (Grant No. XLYC1907140), Fundamental Research Funds for the Central Universities (Grant No. DUT22ZD402), and National Science and Technology Major Project (Grant No. J2019-V-0010-0105)

**Supporting information** Appendixes A–F. 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 Han D, Mo Y, Wu J, et al. Stochastic event-triggered sensor schedule for remote state estimation. IEEE Trans Automat Contr, 2015, 60: 2661–2675

2 Weerakkody S, Mo Y, Sinopoli B, et al. Multi-sensor scheduling for state estimation with event-based, stochastic triggers. IFAC Proc Volumes, 2013, 46: 15–22

3 Huang J, Shi D, Chen T. Energy-based event-triggered state estimation for hidden Markov models. Automatica, 2017, 79: 256–264

4 Wu J, Ren X, Han D, et al. Finite-horizon Gaussianity-preserving event-based sensor scheduling in Kalman filter applications. Automatica, 2016, 72: 100–107

5 Jia Q S, Tang J X, Lang Z. Event-based optimization with random packet dropping. Sci China Inf Sci, 2020, 63: 212202

6 Jia Q S, Wu J. On distributed event-based optimization for shared economy in cyber-physical energy systems. Sci China Inf Sci, 2018, 61: 110203

7 Guo Z, Shi D, Quevedo D E, et al. Secure state estimation against integrity attacks: a Gaussian mixture model approach. IEEE Trans Signal Process, 2019, 67: 194–207

8 Li B. State estimation with partially observed inputs: a unified Kalman filtering approach. Automatica, 2013, 49: 816–820

9 Shi D, Chen T, Darouach M. Event-based state estimation of linear dynamic systems with unknown exogenous inputs. Automatica, 2016, 69: 275–288