SCIENCE CHINA
Information Sciences

• LETTER •

February 2024, Vol. 67, Iss. 2, 129203:1–129203:2
https://doi.org/10.1007/s11432-022-3921-0

Critical observability of partially observed discrete event systems under cyber attacks

Liyun TONG[1], Jinling LIANG[2*] & Yang LIU[3]

[1]*Department of Mathematics, School of Sciences, Hangzhou Dianzi University, Hangzhou* 310018*, China;*
[2]*School of Mathematics, Southeast University, Nanjing* 210096*, China;*
[3]*College of Mathematics and Computer Science, Zhejiang Normal University, Jinhua* 321004*, China*

Received 7 November 2022/Revised 4 May 2023/Accepted 28 September 2023/Published online 11 January 2024

The discrete event system (DES) is a dynamic system driven by asynchronous/sudden events and has been widely used in many critical infrastructures, such as electric transportation networks and intelligent transportation systems [1]. Cyber-physical systems (CPSs) modeled by DESs are particularly vulnerable to cyber attacks in a networked environment surrounded by malicious intruders. Cyber attacks may alter the readings from sensors, thereby changing the observer's observations and causing the controller to make wrong or inappropriate decisions. In [2], the concept of attackability has been proposed, and the attack under changing bounded sensor readings has been modeled as a finite state automaton (FSA). Moreover, cyber security is receiving increasing attention in the field of DES.

Critical security is crucial for the application and development of CPSs, where critical observability is one of the main research focuses. Critical observability corresponds to detecting whether the current state of FSA belongs to a set of critical states, where the critical states represent potentially unsafe or most interesting operations [3]. Concerning the concept of critical observability mentioned here, the inevitable occurrence of cyber attacks must be considered. To avoid complicated work based on the formal automata language, a matrix method called semi-tensor product (STP) of matrices has been widely used in FSA [4]. Inspired by the above extensive application of the STP method, we employ this method to study the form of nondeterministic FSA (NFSA) under cyber attacks and determine its impact on critical observability.

The innovation of this study is summarized in three aspects. (1) The attack function and the corresponding compromised transition are explicitly characterized, and the destroyed observation system $\tilde{G}^a_{\rm obs}$ is constructed. Different from [3], the common phenomena of cyber attacks in networked DESs are considered, which reflect the generality of the concerned system when investigating the critical observability problem. (2) Based on the Boolean STP, the cyber attack model is transformed into an algebraic matrix form, and the corresponding algebraic forms of the observing automaton $\tilde{G}_{\rm obs}$ and the attacked one $\tilde{G}^a_{\rm obs}$ are established. (3) Due to the event string generated by the attacks, a virtual state x_e is introduced to system $\tilde{G}^a_{\rm obs}$. Thus, the corrupted state transition observable matrix F^a can be derived reasonably. Compared with [5], in addition to the corresponding cyber attacks, the introduction of x_e also makes the matrix method more feasible and the meaning of the state transition matrix clearer. Furthermore, several novel criteria for critical observability were obtained, and an online algorithm was proposed to detect the critical observability of the addressed NFSA under cyber attacks.

Notations. $|X|$ denotes the cardinality of set X. $\mathbb{N}$ ($\mathbb{N}_+$) denotes the set of nonnegative (positive) integers. δ^i_p represents the ith column vector of the identity matrix I_p. $\mathcal{D} := \{0,1\}$ and $\Delta_p := \{\delta^i_p : i = 1,2,\ldots,p\}$. A matrix $P \in \mathbb{R}^{j\times k}$ is called a logical matrix if its column set $\mathrm{Col}(P)$ belongs to Δ_j. $\mathcal{L}_{p\times q}$ represents the set of all $p\times q$ logical matrices. $\mathrm{Col}_i(P)$ represents the ith column vector of matrix P. δ^0_n denotes the zero column vector $\mathbf{0}_n \in \mathbb{R}^n$. $[c,d]_{\mathbb{Z}}$ denotes the set $\{c,c+1,\ldots,d\}$ for integers c and d with $d \geqslant c$. $\mathcal{B}^{m\times n}$ denotes the set of all $m\times n$ Boolean matrices. Θ_η denotes the set-indicator column vector in $\mathcal{B}^m$ corresponding to $\eta \subseteq \Delta_m$.

STP of matrices. The Boolean STP of $E \in \mathcal{B}^{m\times n}$ and $F \in \mathcal{B}^{p\times q}$ is defined as $E \ltimes_{\mathcal{B}} F := (E \otimes I_{\alpha/n}) \times_{\mathcal{B}} (F \otimes I_{\alpha/p})$, where "$\times_{\mathcal{B}}$" is the Boolean product, $\alpha = \mathrm{lcm}(n,p)$ is the least common multiple of n and p. Hereafter, we omit the symbol "$\ltimes_{\mathcal{B}}$". The Boolean STP of E with order κ is defined as $E^{[\kappa]} := E \ltimes_{\mathcal{B}} E \ltimes_{\mathcal{B}} \cdots \ltimes_{\mathcal{B}} E$. Readers can refer to [4] for more details on Boolean STP.

System model and problem formulation. An NFSA is used to model a DES: $\tilde{G} = (X,\Sigma,f,X_0,C)$, where X is a set of finite states, $X_0 \subseteq X$ is the initial state set, $C \subseteq X$ is a critical state set; Σ is a set of finite events partitioned into unobservable event set Σ_{uo} and observable event set Σ_o, i.e., $\Sigma = \Sigma_{uo} \cup \Sigma_o$ and $\Sigma_{uo} \cap \Sigma_o = \emptyset$; $f : X \times \Sigma \to 2^X$ is a nondeterministic transition function, where 2^X represents the power set of X. The natural projection $P : \Sigma^* \to \Sigma_o^*$ is defined as $P(\varepsilon) = \varepsilon$, $P(s\sigma) = P(s)\sigma$ for $\sigma \in \Sigma_o$, and $P(s\sigma) = P(s)$ for $\sigma \in \Sigma_{uo}$, where $s \in \Sigma^*$. Here, Σ^* is the set with all possible event strings, and Σ_o^* is the set of all finite observable event strings. The unobservable reach of a state $x \in X$ is defined as $\mathrm{UR}(x)$.

Definition 1. A partially observed NFSA $\tilde{G} = (X,\Sigma,f,X_0,C)$ with projection P is critically observable at the kth time step if $(f(x_0,t) \subseteq C) \vee (f(x_0,t) \subseteq \bar{C})$ holds for any

* Corresponding author (email: jinlliang@seu.edu.cn)

string s with $|P(s)=t|=k$, $x_0\in X_0$, and $\bar{C}=X\backslash C$.

In this study, we consider a sensor attacker that could change the observable event strings $t=P(s)$ by inserting some events that do not occur or replacing/erasing some events that do occur, and the observation string t is replaced by the corrupted one $t^a=\mathcal{H}_a(t)$, where $\mathcal{H}_a:\Sigma_o^*\to 2^{\Sigma_o^*}$ is a set-valued function. Additionally, the defender (i.e., the considered NFSA $\tilde{G}$) is assumed to identify and detect the attack and further understand the attack model. The definition of critical observability for NFSA $\tilde{G}$ under cyber attacks is given below.

Definition 2. Under cyber attacks, a partially observed NFSA $\tilde{G}=(X,\Sigma,f,\ X_0,C)$ with projection P is critically observable at the kth time step if $(f(x_0,t^a)\subseteq C)\vee(f(x_0,t^a)\subseteq\bar{C})$ holds for any string s with $|P(s)=t|=k$, $t^a=\mathcal{H}_a(t)$, and $x_0\in X_0$.

Main results. We first give the algebraic form of the NFSA $\tilde{G}$. Consider an NFSA $\tilde{G}$ with $X=\{x_1,x_2,\dots,x_n\}$, $\Sigma_o=\{\sigma_1,\sigma_2,\dots,\sigma_m\}$, and $C=\{x_{c_1},x_{c_2},\ \dots,x_{c_\iota}\}\subseteq X$. Consider δ_n^i ($i\in[1,n]_{\mathbb{Z}}$) as the vector form of state x_i, i.e., $x_i\sim\delta_n^i$, and let the observable event $\sigma_q\sim\delta_m^q$ ($q\in[1,m]_{\mathbb{Z}}$). To derive the algebraic form of system $\tilde{G}$, we first give its observing automaton $\tilde{G}_{\rm obs}=(2^X,\Sigma_o,f,P,X_{0,\rm obs},C)$, where $X_{0,\rm obs}=\mathrm{UR}(X_0)$ is the set of initial states in $\tilde{G}_{\rm obs}$. The symbolic transition function f can be expressed as a unique matrix F with $F=[F_1,F_2,\dots,F_m]$, called the state transition observable matrix of system $\tilde{G}_{\rm obs}$. An algebraic form of the dynamics for $\tilde{G}_{\rm obs}$ can be constructed as $\bar{x}(k+1)=F\sigma(k)\bar{x}(k)$, where $k\in\mathbb{N}$, $\bar{x}(k)\in\mathcal{B}^n$, and $\sigma(k)\in\Delta_m$. Refer to [4] for more details.

Furthermore, the logical form of set C is $\{\delta_n^{c_1},\delta_n^{c_2},\dots,\delta_n^{c_\iota}\}$, and the notation Θ_C is represented by $\Theta_{\{\delta_n^{c_1},\delta_n^{c_2},\dots,\delta_n^{c_\iota}\}}$. Similarly, $\Theta_{\bar{C}}\sim\Theta_{\Delta_n\backslash\{\delta_n^{c_1},\delta_n^{c_2},\dots,\delta_n^{c_\iota}\}}$. For simplicity, let $\tilde{F}:=FW_{[n,m]}$, $\tilde{F}^{[k]}\bar{x}(0):=\tilde{F}^{[k]}_{\bar{x}(0)}$, and $(\ltimes_{\mathcal{B}})_{j=0}^{k-1}\sigma(j):=\sigma^{k-1}$. Next, we provide the criterion of critical observability for system $\tilde{G}$ when there is no cyber attack.

Lemma 1. An NFSA $\tilde{G}=(X,\Sigma,f,X_0,C)$ is critically observable at the kth time step if and only if for any initial state $\bar{x}_0\in X_{0,\rm obs}$ of $\tilde{G}_{\rm obs}$ and the corresponding observable event string $t=\sigma_{i_0}\sigma_{i_1}\cdots\sigma_{i_{k-1}}$, one of the following inequalities holds: $\tilde{F}^{[k]}_{\bar{x}(0)}\sigma^{k-1}\leqslant\Theta_C$ or $\tilde{F}^{[k]}_{\bar{x}(0)}\sigma^{k-1}\leqslant\Theta_{\bar{C}}$.

To make the state transition of the addressed system clearer, we introduce a virtual state x_e for the attacked system $\tilde{G}$. In this way, for two adjacent states, the transition from one state to another can still be expressed through an observable event instead of an observable string. System $\tilde{G}$ destroyed by attacks is defined as $\tilde{G}^a=(\tilde{X},\Sigma,\tilde{f},X_0,C)$, where $\tilde{X}=X\cup\{x_e\}$ and the transition function is $\tilde{f}=f^a\cup f$ with the corrupted transition function f^a. The corresponding corrupted observing automaton is $\tilde{G}^a_{\rm obs}=(2^{\tilde{X}},\Sigma_o,\tilde{f},P,X_{0,\rm obs},C)$, and the dynamics of $\tilde{G}^a_{\rm obs}$ is described as $\bar{x}(k+1)=F^a\sigma(k)\bar{x}(k)$, where $k\in\mathbb{N}$, $\bar{x}(k)\in\mathcal{B}^{n+1}$, $\sigma(k)\in\Delta_m$, and F^a is called the corrupted state transition observable matrix of $\tilde{G}^a_{\rm obs}$. Then, for the attacked system $\tilde{G}^a$, a criterion for its critical observability is given as follows.

Theorem 1. An attacked NFSA $\tilde{G}^a=(\tilde{X},\Sigma,\tilde{f},X_0,C)$ is critically observable at the kth time step if and only if for any initial state $\bar{x}_0\in X_{0,\rm obs}$ of $\tilde{G}^a_{\rm obs}$ and the corresponding observable event string $\tilde{t}=\sigma_{r_0}\sigma_{r_1}\cdots\sigma_{r_{k-1}}$, one of the following inequalities holds:

$$(\tilde{F}^a)^{[k]}_{\bar{x}(0)}\sigma^{k-1}\leqslant\Theta_{\tilde{C}}\ \ \text{or}\ \ (\tilde{F}^a)^{[k]}_{\bar{x}(0)}\sigma^{k-1}\leqslant\Theta_{\tilde{\bar{C}}},\qquad(1)$$

where $\tilde{C}=C\cup\{x_e\}\sim\{\delta_{n+1}^{c_1},\delta_{n+1}^{c_2},\dots,\delta_{n+1}^{c_\iota},\delta_{n+1}^{n+1}\}$ and $\tilde{\bar{C}}=\bar{C}\cup\{x_e\}\sim\Delta_{n+1}\setminus\{\delta_{n+1}^{c_1},\delta_{n+1}^{c_2},\ \dots,\delta_{n+1}^{c_\iota}\}$.

Next, we attempt to detect whether system $\tilde{G}$ is still critically observable after the cyber attack at time step k. To detect the critical observability of the attacked system $\tilde{G}^a$, we need to determine whether the corrupted string t^a satisfies (1). For narrative clarity, suppose the corrupted observable strings set is $\varphi=\{t_1^a,t_2^a,\dots,t_\tau^a\}\sim\{\delta_{m^k}^{a_1},\delta_{m^k}^{a_2},\dots,\delta_{m^k}^{a_\tau}\}$.

Theorem 2. Under cyber attack, an originally critically observed NFSA $\tilde{G}=(X,\Sigma,f,\ X_0,C)$ remains critically observable at time step k if and only if for any initial state $\bar{x}_0\in X_{0,\rm obs}$ in $\tilde{G}_{\rm obs}$ and the corrupted observable event string t_z^a, the following inequalities $\mathrm{Col}_{a_z}((\tilde{F}^a)^{[k]}_{\bar{x}(0)})\leqslant\Theta_{\tilde{C}}$ or $\mathrm{Col}_{a_j}((\tilde{F}^a)^{[k]}_{\bar{x}(0)})\leqslant\Theta_{\tilde{\bar{C}}}$ hold for all $z\in[1,\tau]_{\mathbb{Z}}$.

Now, determining whether cyber attacks can make the uncritically observed system $\tilde{G}$ critically observable is the final major focus. For the original system $\tilde{G}$, define the set of observable event strings that will be attacked as $\tilde{\phi}=\{t_{\tilde{j}}^{\tilde{a}}:\exists\sigma\in\Sigma_o^a\ \text{s.t.}\ t_{\tilde{j}}^{\tilde{a}}=\sigma_{i_0}\sigma_{i_1}\cdots\sigma\cdots\sigma_{i_{k-2}},\tilde{j}\in[1,\tilde{p}]_{\mathbb{Z}}\}$, where $\tilde{p}\in\mathbb{N}_+$ indicates the total number of event strings that will be attacked. When a cyber attack occurs, each event string $t_{\tilde{j}}^{\tilde{a}}$ in set $\tilde{\phi}$ will be mapped into $t_{\hat{j}}^{a}\in\tilde{\phi}_a$ under the attack function $\mathcal{H}_a(\cdot)$. Let $\phi=\{\delta_{m^k}^{\tilde{a}_{\tilde{j}}}:\tilde{j}\in[1,\tilde{p}]_{\mathbb{Z}}\}$ denote the algebraic expression of set $\tilde{\phi}$ and ϕ_a denote the expression corresponding to $\tilde{\phi}_a$.

Theorem 3. An attacked NFSA $\tilde{G}_a=(\tilde{X},\Sigma,\tilde{f},X_0,C)$ is critically observable at time step k if and only if for any initial state $\bar{x}_0\in X_{0,\rm obs}$ in $\tilde{G}_{\rm obs}$, the following two conditions hold: (i) $\Lambda\subseteq\phi$; (ii) $\mathrm{Col}_{a_{\hat{j}}}((\tilde{F}^a)^{[k]}_{\bar{x}(0)})\leqslant\Theta_{\tilde{C}}$ or $\mathrm{Col}_{a_{\hat{j}}}((\tilde{F}^a)^{[k]}_{\bar{x}(0)})\leqslant\Theta_{\tilde{\bar{C}}}$ with $\phi_a=\{\delta_{m^k}^{a_{\hat{j}}}:\hat{j}\in[1,\hat{p}]_{\mathbb{Z}}\}$.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 62373103, 62173308).

References

1 Cassandras C G, Lafortune S. Introduction to Discrete Event System. New York: Springer, 2008
2 Su R. Supervisor synthesis to thwart cyber attack with bounded sensor reading alterations. Automatica, 2018, 94: 35–44
3 Pola G, de Santis E, di Benedetto M D, et al. Design of decentralized critical observers for networks of finite state machines: a formal method approach. Automatica, 2017, 86: 174–182
4 Tong L, Liang J. I-S detectability of partially-observed discrete event systems: a novel matrix-based method. J Franklin Institute, 2023, 360: 3436–3458
5 Yan Y, Deng H, Chen Z. A new look at the critical observability of finite state machines from an algebraic viewpoint. Asian J Control, 2022, 24: 3056–3065