SCIENCE CHINA
Information Sciences

• LETTER •

April 2026, Vol. 69, Iss. 4, 140212:1–140212:2
https://doi.org/10.1007/s11432-025-4778-5

Special Topic: Logical System Control

STP-based sensor attack-resilient supervisory control of logical finite state machines with encrypted channel

Zhipeng ZHANG[1], Aocheng WANG[2] & Chengyi XIA[1*]

[1]*School of Artificial Intelligence, Tiangong University, Tianjin 300387, China*
[2]*School of Control Science and Engineering, Tiangong University, Tianjin 300387, China*

Received 5 September 2025/Revised 18 November 2025/Accepted 20 January 2026/Published online 10 March 2026

Citation Zhang Z P, Wang A C, Xia C Y. STP-based sensor attack-resilient supervisory control of logical finite state machines with encrypted channel. Sci China Inf Sci, 2026, 69(4): 140212, https://doi.org/10.1007/s11432-025-4778-5

As cyber-physical systems become more interconnected and complex, their vulnerability to cyberattacks has increased significantly. Among these attacks, sensor attacks pose a particular risk as they can manipulate measurement data, rendering the system to operate under false assumptions and potentially leading to catastrophic consequences. Logic finite state machines (LFSMs) [1] provide an effective framework for identifying these cyberattacks and controlling them before harm or violations occur [2].

In general, the system model will improve the system's resilience to attacks by introducing encrypted channels, which can prevent attackers from manipulating sensor data. Previous research, such as [3], proposes detecting replay and covert attacks by embedding permutation matrices in sensor and actuator channels. This approach can disrupt the stealthiness of the attacker and enable the localization of compromised signals. However, the permutation matrices in that work were static and were not based on the system's current state. Meanwhile, how to design a supervisory control mechanism, which can prevent transitions to unsafe states even after an attack is detected and located, has not been fully studied and is a very challenging problem.

In this study, based on semi-tensor product (STP) method [4], we develop a novel supervisory control scheme for LFSMs subject to sensor substitution attacks over the encrypted channel. The main contributions are threefold. (1) We formulate the LFSMs substitution attack model and the permutation-based encryption-decryption channel within the STP framework. (2) We derive a necessary and sufficient algebraic condition for real-time detection of substitution attacks on observable events. (3) We design a sensor-attack resilient supervisory controller that can dynamically restrict hazardous transitions within the safe state set. This unified framework provides a novel solution that combines detection, encryption, and control to address the security issue of cyber-physical systems.

Problem statement. This research aims to develop a secure supervisory control scheme based on the STP algebraic framework for LFSMs with encrypted channel, which can effectively detect sensor substitution attacks and prohibit the system from transitioning to unsafe states.

Preliminaries. Let $\mathbb{B}_{m\times n}$ denote the set of $m\times n$ Boolean matrices, $|S|$ the cardinality of finite set S, $\mathbf{1}_n$ the all-ones column vector, M^{T} the transpose of matrix M, and v^i the i-th element of vector v. Denote by δ_n^k the k-th column of the identity matrix I_n, with $\Delta_n=\{\delta_n^1,\ldots,\delta_n^n\}$. The Boolean semi-tensor product is denoted by $\ltimes_B$.

System model. An LFSM can be expressed as $G=(Q,\Sigma,\delta,q_0)$, where $Q=Q_s\cup Q_u$ is the partition of states into safe (Q_s) and unsafe (Q_u) states, and $\Sigma=\Sigma_o\cup\Sigma_{uo}=\Sigma_c\cup\Sigma_{uc}$ is the set of events with observable/unobservable and controllable/uncontrollable subsets. The transition function is $\delta: Q\times\Sigma\to Q$, and $q_0\in Q_s$ is the initial state. The extended transition function is $\delta: Q\times\Sigma^*\to Q$, Σ^* is the Kleene closure of Σ.

The states and observable events are encoded as vectors $Q=\Delta_n$ and $\Sigma_o=\Delta_m$, where $n=|Q|$ and $m=|\Sigma_o|$. The transition behavior of each state is represented by a block matrix $F_i\in\mathbb{B}_{n\times m}$, with each entry $F_i(r,j)$ defined by

$$F_i(r,j)=\begin{cases}1, & \text{if } \exists q'\in UR(q_i), q_r\in UR(\delta(q',\sigma_j)),\\ 0, & \text{otherwise}\end{cases} \tag{1}$$

with the unobservable reachability set $UR(q_i)$ for state q_i, defined by $UR(q_i)=\{q\in Q\mid \exists s\in\Sigma_{uo}^*: q=\delta(q_i,s)\}$.

The complete transition matrix $F=[F_1\ F_2\ \cdots\ F_n]\in\mathbb{B}_{n\times nm}$, and the system dynamics can be represented by

$$x(t+1)=F\ltimes_B x(t)\ltimes_B e_o(t), \tag{2}$$

where $x(t)$ is the state vector and $e_o(t)$ is the observable event vector at time t.

Sensor attack. The attacker can perform a sensor substitution attack, in which an observable event is substituted with another from a predefined set. Only observable events are vulnerable. For each vulnerable event $\sigma\in\Sigma_v\subseteq\Sigma_o$, a substitution function $\phi:\Sigma_v\to 2^{\Sigma_o}$ maps σ to a set of possible substitutions, including itself (no attack). This work focuses on sensor substitution attacks, where attackers can modify event signals but cannot insert or delete events. Our model reflects real-world scenarios with limited attacker access. Extending this framework to more general attack models is a key direction for future work.

Let $\mathcal{A}\in\mathbb{B}_{m\times m}$ denote the attack matrix encoding possible

* Corresponding author (email: cyxia@tiangong.edu.cn)

event substitutions. It is defined by

$$\mathcal{A}(r,j)=\begin{cases}1, & \text{if } \sigma_r\in\phi(\sigma_j) \text{ or } (r=j \text{ and } \sigma_j\notin\Sigma_v),\\ 0, & \text{otherwise.}\end{cases} \tag{3}$$

It can be observed that the attack matrix represents all possible substitutions for vulnerable events and indicates no change for non-vulnerable events.

In practice, the attacker may apply a specific and unknown substitution sub-matrix $A(t)\in\mathbb{B}_{m\times m}$, and in each column there is a "1" that indicates the selected substitution. The attacker's behavior is characterized by

(1) **Stealthiness.** Substitutions are valid in the current state, avoiding detection unless designed to detect them.

(2) **Time-varying choices.** $A(t)$ evolves over time based on the attacker's decisions and represents the substitutions selected from the full attack matrix $\mathcal{A}$ at time t.

Encrypted channel via permutation matrices. To enhance security and detect potential attacks, an encrypted channel based on the permutation matrix is established between the system and the supervisor. The permutation matrix alters the signal's position for encryption, and its inverse decrypts it at the receiving end. The permutation matrix satisfies the following properties.

(1) **Undefined substitution mapping.** The permutation matrix $P(t)\in\mathbb{B}_{m\times m}$, based on state $x(t)$ and event vector $e_o(t)$, ensures that any attacker substitution maps to an undefined event during the decryption.

(2) **Secure transmission.** The permutation matrix is securely transmitted, preventing tampering or decoding by the attacker, who can modify event data but not the matrix.

These properties will guarantee that all substitution attacks can be detected while ensuring no interference with normal system operation in the absence of attacks. To achieve the above characteristics, the corresponding permutation matrices can be configured in the following steps.

(1) From the received vector $e_o(t)$, extract the set of vulnerable events $\Sigma_v(t)=\{\delta_m^i\in\Sigma_v\mid e_o(t)\wedge\delta_m^i\neq\mathbf{0}_m\}$.

(2) From set $\phi(\delta_m^i)$ of each $\delta_m^i\in\Sigma_v(t)$, seek the substitution events $\Phi(t)=\bigcup_{\delta_m^i\in\Sigma_v(t)}\phi(\delta_m^i)\setminus\{\delta_m^l\in\Delta_m|e_o(t)\wedge\Delta_m=e_o(t)\}$, and calculate $Q(t)=\{\delta_n^k\in\Delta_n|x(t)\wedge\Delta_n=x(t)\}$.

(3) Construct $P(t)\in\mathbb{B}_{m\times m}$ such that for each $\delta_m^j\in\Phi(t)$, $\sigma_p=P^{-1}(t)(\delta_m^j)$ satisfies $\delta(\delta_n^k,\sigma_p)$ is undefined for all $\delta_n^k\in Q(t)$.

Attack detection. After obtaining the permutation matrix $P(t)$, the encrypted event vector $e'(t)=P(t)\ltimes_B e_o(t)$ is modified by the attacker as $\hat{e}(t)=A(t)\ltimes_B e'(t)$. After decryption using $P^{-1}(t)$, the event vector becomes $\tilde{e}_o(t)=P^{-1}(t)\ltimes_B\hat{e}(t)$.

Definition 1 (Attack detection)**.** The substitution sensor attack can be detected if the decrypted event vector contains undefined events in the current state.

Theorem 1. The substitution sensor attack is detected if and only if there exists at least one element in $\mathbf{v}(t)=\mathbf{d}(t)-\tilde{e}_o(t)\in\mathbb{B}_m$ that equals to -1, where $\mathbf{d}(t)=\left(\mathbf{1}_n^{\mathrm{T}}\ltimes_B(F\ltimes_B x(t))\right)^{\mathrm{T}}$ is the defined event vector, and $\tilde{e}_o(t)$ is the decrypted event vector after the attack.

Proof. ($\Rightarrow$) If an attack occurs, $\tilde{e}_o(t)$ will contain at least one undefined event in the current state. This causes $\mathbf{v}(t)$ to have an entry equal to -1, indicating an attack.

($\Leftarrow$) If $\mathbf{v}(t)$ contains -1, it means that an event in $\tilde{e}_o(t)$ is not defined in the current state, which confirms the attack.

Supervisory control. The goal of supervisory control is to develop strategies that prevent transitions to unsafe states based on state estimation. We propose a state estimation algorithm (Algorithm 1) with attack detection, where a modified event vector is used if an attack is detected.

Algorithm 1 State estimation with attack detection.

Input: $F\in\mathbb{B}_{n\times nm}$, $\mathcal{A}\in\mathbb{B}_{m\times m}$, $x(t)$, $\tilde{e}_o(t)$, $P(t)$.
Output: $\hat{x}(t+1)\in\mathbb{B}_n$.
1: $d\leftarrow\left(\mathbf{1}_n^{\mathrm{T}}\ltimes_B(F\ltimes_B x(t))\right)^{\mathrm{T}}$;
2: $v\leftarrow d-\tilde{e}_o(t)$;
3: **if** $\exists\, i\in\{1,2,\ldots,m\}: v^i<0$ **then**
4: $\quad\alpha\leftarrow\left[\alpha^i=1 \text{ if } v^i<0 \text{ else } 0\right]\in\mathbb{B}_m$;
5: $\quad\beta\leftarrow\mathcal{A}^{\mathrm{T}}\ltimes_B P(t)\ltimes_B\alpha\vee(\tilde{e}_o(t)-\alpha)$;
6: **else**
7: $\quad\beta\leftarrow\tilde{e}_o(t)$;
8: **end if**
9: $\hat{x}(t+1)\leftarrow F\ltimes_B x(t)\ltimes_B\beta$.

Remark 1. The algorithm checks for an attack using Theorem 1. If no attack is detected, the state estimate is computed directly from the decrypted event vector. If an attack is detected, the algorithm identifies all possible original event vectors by leveraging the full attack matrix and the permutation matrix.

Remark 2. The overall complexity of Algorithm 1 is $O(n^2m+m^2)$, with $O(n^2m)$ from state transition calculations and $O(m^2)$ from attack detection and event processing.

Let $\mathbf{C}(t+1)$ denote the control strategy applied at time $(t+1)$ to avoid unsafe state transitions. The following theorem tells us how to calculate the control strategy.

Theorem 2. Given the state estimate $\hat{x}(t+1)$, the control strategy that ensures the system avoids unsafe states can be computed as

$$\mathbf{C}(t+1)=\mathbf{1}_{|\Sigma|}-B\ltimes_B\hat{x}(t+1), \tag{4}$$

where $B\in\mathbb{B}_{|\Sigma|\times n}$ is the forbidden event matrix, defined by

$$B(i,j)=\begin{cases}1, & \text{if } \sigma_i\in\Sigma_c\wedge\exists w\in\Sigma_{uc}^*:\delta(\delta(q_j,\sigma_i),w)\in Q_u,\\ 0, & \text{otherwise.}\end{cases}$$

Proof. The forbidden event matrix B defines the events that must be disabled to avoid unsafe state transitions, and identifies controllable events σ_i that can lead to unsafe states, directly or via uncontrollable transitions. The term $B\ltimes_B\hat{x}(t+1)$ represents the prohibited events based on the current state estimate. $\mathbf{1}_{|\Sigma|}-B\ltimes_B\hat{x}(t+1)$ includes both the allowed events and the uncontrollable events, ensuring that only safe transitions occur.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 62573316, 62203328).

References

1 Zhang Z P, Xia C Y, Qi G Y, et al. Multi-step state-based opacity for unambiguous weighted machines. Sci China Inf Sci, 2024, 67: 212204
2 Chen Q R, Su R, Li Z W. Synthesis of sensor attacks for tampering detectability of partially observed discrete-event systems. IEEE Trans Autom Control, 2026, 71: 443–457
3 Fritz R, Zhang P. Detection and localization of stealthy cyberattacks in cyber-physical discrete event systems. IEEE Trans Automat Contr, 2023, 68: 7895–7902
4 Yan Y Y, Cheng D Z, Feng J E, et al. Survey on applications of algebraic state space theory of logical systems to finite state machines. Sci China Inf Sci, 2023, 66: 111201