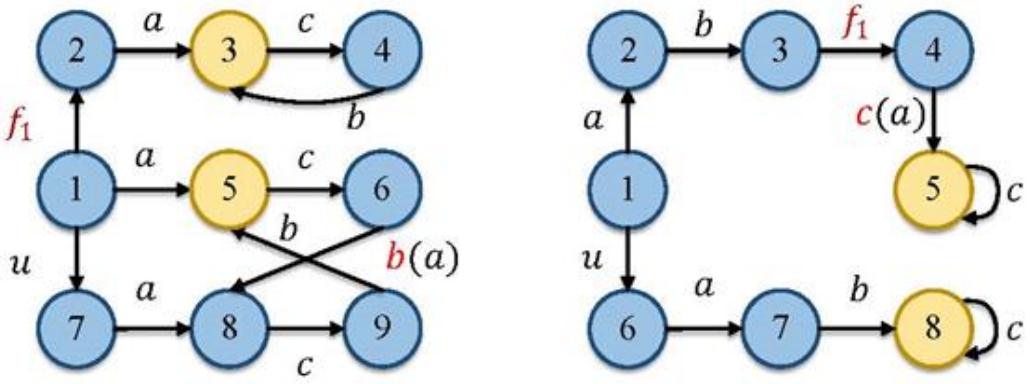
A novel efficient model for testing diagnosability of discrete event systems under sensor attacks

Qifei LI, Dantong OUYANG, Xiangfu ZHAO, Luyu JIANG, Ran TAI, Liming ZHANG

Frontiers of Computer Science, DOI: 10.1007/s11704-025-41289-1

Problems & Ideas

- The cyber-attack diagnosability (CA-diagnosability) of discrete event systems (DESs) assess the ability to diagnose issues when an attacker interferes with sensor-to-diagnostic communication.
- Ideas: This paper introduces a novel cyclic model (CM), which increases the efficiency of checking the system's CA-diagnosability without constructing the diagnoser.



On the left side of Figure, it is assumed that event a may be under attack and the attack is dynamic, with tr = (6, a, 8) and A_tr = { b }. On the right side of Figure, it is similarly assumed that event a may be under attack, with tr = (4, a, 5) and A_tr = c. Hence, o = {a, b, c}, uo = {u} f = f_1}.

Main Contributions

- Contributions:
  - The first contribution of the paper involves an efficient model known as the cyclic model (CM). This model employs our innovative detection of cycles (DC) algorithm to extract cyclic information, including cyclic states and cyclic-event sequences from the system after sensor attacks, thus constructing the CM.
  - The second contribution is the proposal of the concept of critical observations for checking the diagnosability of DES under sensor attacks
  - The third contribution pertains to developing an algorithm (CMDIC) within our CM for checking the CA-diagnosability of multi-fault systems.

Table 1 Experimental results of checking CA-diagnosability under deletion attacks using different methods.

	$\|X\|$	$\|\delta\|$	$\|X^e\|$	$\|\delta^e\|$	$\|\Sigma\|$	$\tilde{G}^e_{obs}$(ms)	**ours**(ms)	**percentage**(%)
Su [17]	10	14	3	3	9	1.352	**0.006**	**99.56**
Mehdi [35]	10	12	4	6	6	1.486	**0.004**	**99.73**
IOD1(f2.30) [36]	12	20	8	16	8	7.914	**0.017**	**99.79**
IOD2(cn3g) [36]	19	25	9	15	4	2.124	**0.008**	**99.62**
IOD3(2.16modified) [36]	9	11	5	7	3	1.562	**0.0511**	**96.72**

Table 2 Experimental results of checking CA-diagnosability under insertion attacks using different methods.

	$\|X\|$	$\|\delta\|$	$\|X^e\|$	$\|\delta^e\|$	$\|\Sigma\|$	$\tilde{G}^e_{obs}$(ms)	**ours**(ms)	**percentage**(%)
Su [17]	10	14	20	24	9	33.289	**0.371**	**98.89**
Mehdi [35]	10	12	16	18	6	25.951	**0.256**	**99.01**
IOD1(f2.30) [36]	12	20	16	24	8	38.678	**0.765**	**98.02**
IOD2(cn3g) [36]	19	25	29	35	4	18.761	**0.618**	**96.71**
IOD3(2.16modified) [36]	9	11	13	15	3	27.910	**0.182**	**99.35**

Table 3 Experimental results of checking CA-diagnosability under replacement attacks using different methods.

	$\|X\|$	$\|\delta\|$	$\|X^e\|$	$\|\delta^e\|$	$\|\Sigma\|$	$\tilde{G}^e_{obs}$(ms)	**ours**(ms)	**percentage**(%)
Su [17]	10	14	10	14	9	18.061	**0.125**	**99.31**
Mehdi [35]	10	12	10	12	6	19.282	**0.118**	**99.39**
IOD1(f2.30) [36]	12	20	12	20	8	25.764	**0.653**	**97.47**
IOD2(cn3g) [36]	19	25	19	25	4	5.269	**0.149**	**97.17**
IOD3(2.16modified) [36]	9	11	9	11	3	18.652	**0.101**	**99.46**

Tables 1-3 respectively present the experimental results of checking CA-diagnosability under three types of static attacks.