

Probabilistic Fault Detection in Networked Discrete Event Systems

Christoforos Hadjicostis

Decision and Control Laboratory
Coordinated Science Laboratory and Dept. of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign

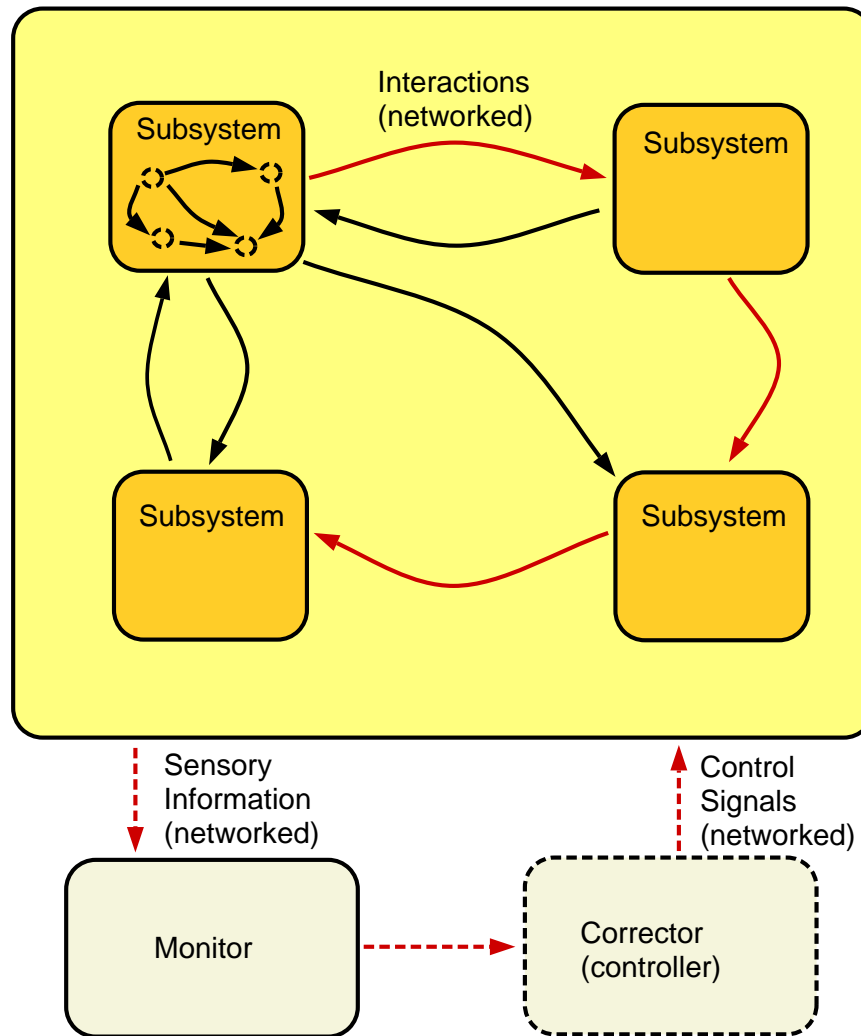
MOTIVATION: FAULT DIAGNOSIS AND MONITORING IN NETWORKED DES

Structural issues:

- Local v.s. global
- Sensitivity to failures/delays
- Observability/controllability

Monitoring architecture:

- Hierarchical v.s. distributed
- Sensor/actuator allocation
- Communication overhead
- Robustness to incomplete and/or incorrect data, delays



PREVIOUS WORK (1): “DETERMINISTIC” FAULT DIAGNOSIS

- **Related Previous Work**

- Automata (e.g., Teneketzis, Lafortune, Varaiya, Kumar, etc.)
- Communication networks (e.g., Schwartz, Benveniste, Fabre)
- Timed systems (e.g., Wonham, Holloway)

- **Challenges in Diagnoser/Monitor Design**

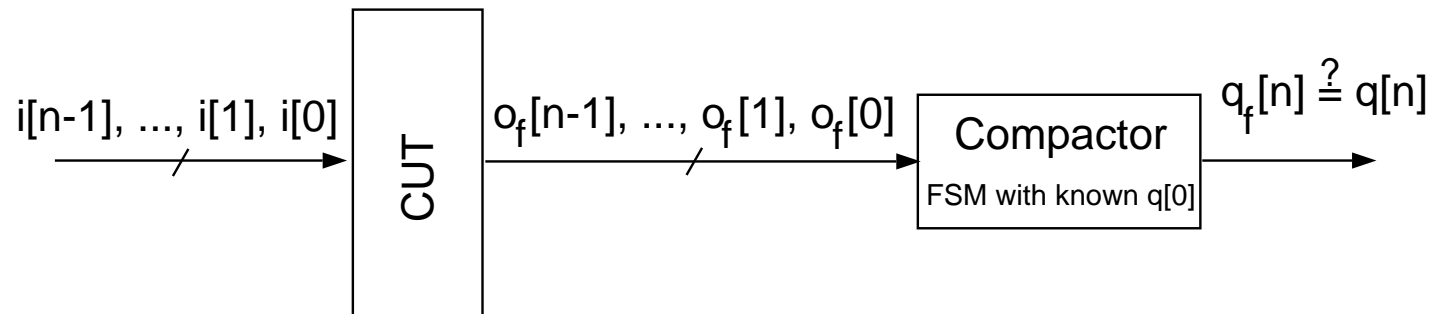
- Infrastructure constraints (e.g., distributivity, observability)
- Hardware, communication, algorithmic overhead and trade-offs
- Synthesis-oriented design (e.g., sensor allocation)
- Other (e.g., model uncertainty, detection delay)

PREVIOUS WORK (2): “PROBABILISTIC” FAULT DIAGNOSIS

- **Related Previous Work**

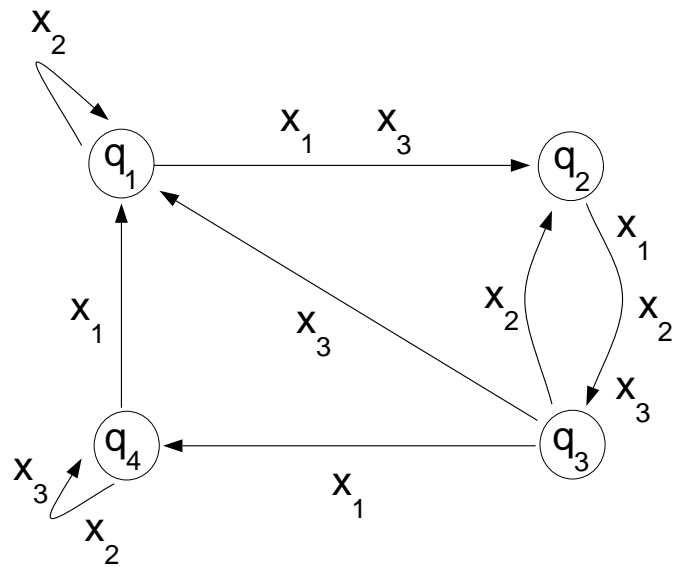
- Change detection in stochastic systems (e.g., Nikiforov, Lai, Hart)
- Fault detection in dynamic DES (Bouloutas, Fabre, Benveniste)
- Circuit testing, compaction (e.g., Damiani, Wagner)
- Probabilistic verification (e.g., Yannakakis)

- **Motivating Example: Aliasing Probability for Combinational CUT**



Aliasing probability: Probability that $q[n] = q_f[n]$ for randomly selected sequence $i[0], i[1], i[2], \dots, i[n - 1]$

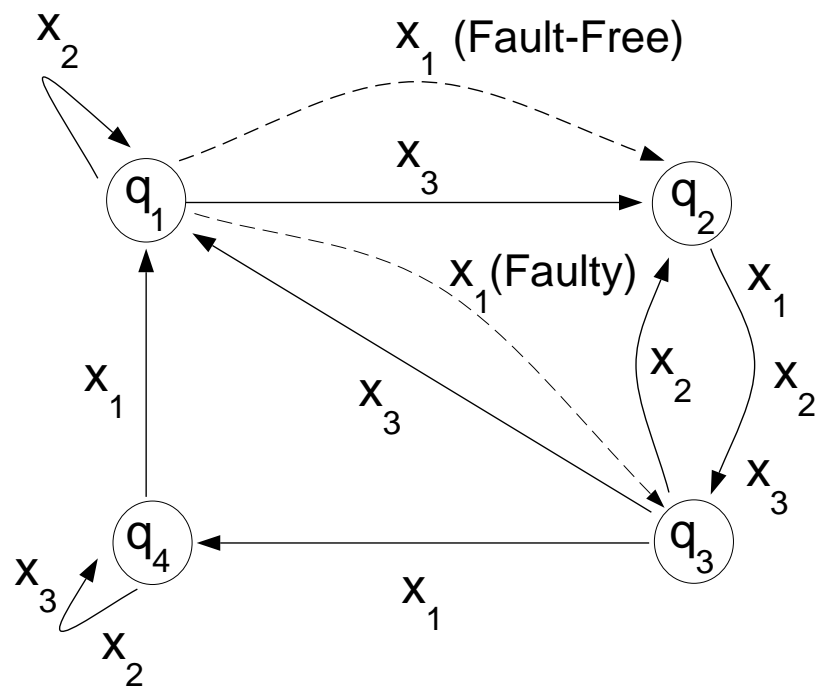
NOTATION



$$\mathbf{A}_1 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

- **State Set:** $Q = \{q_1, q_2, \dots, q_N\}$ **Input Set:** $X = \{x_1, x_2, \dots, x_K\}$
- **Next-State Function:** $q[k+1] = \delta(q[k], x[k])$
- **N-dimensional Indicator State Vector:** $\mathbf{q}[k]$
- **Transition Matrix Notation:** $\mathbf{q}[k+1] = \mathbf{A}_{x[k]}\mathbf{q}[k], \quad x[k] \in \{x_1, x_2, \dots, x_K\}$

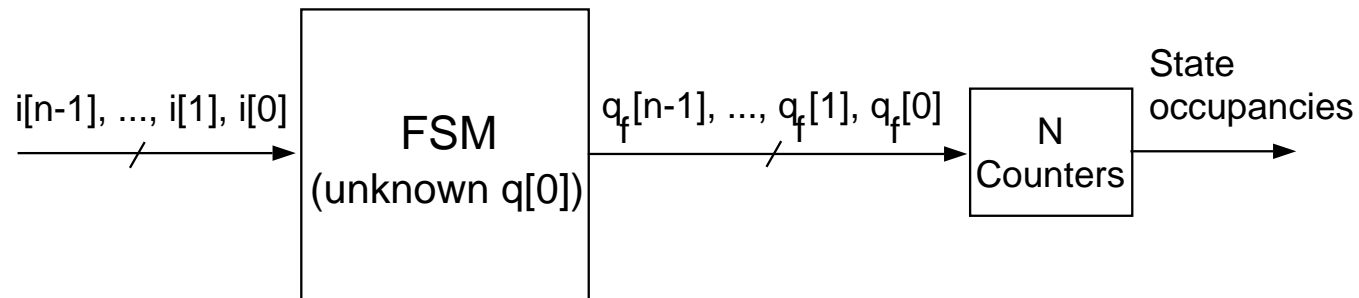
STATE-TRANSITION FAULTS



- State-transition fault “at state q_1 under input x_1 ” (permanent or transient)

• Faulty transition matrix:
$$\mathbf{A}'_1 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \underbrace{\begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}}_{\mathbf{A}_1} + \underbrace{\begin{bmatrix} 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}}_{\mathbf{E}_1}$$

PROBLEM FORMULATION



- Exact input sequence $i[0], i[1], \dots, i[n-1]$ unknown

Input x_d chosen with probability p_d

- Occupancy measurements (variations and extensions possible)

$$\mathbf{m}_n = [m_n(1) \ m_n(2) \ \dots \ m_n(N)]^T$$

- **Potential advantages:** Out-of-order observations, random sampling

HYPOTHESIS TESTING

- **Known:**
 - (i) *A priori* probabilities p_{f_l}
 - (ii) *A priori* probability for no fault p_{f_0}
 - (iii) Distribution of initial state
- **MAP Rule:** Minimize probability of error

Choose hypothesis that maximizes
$$\arg \max_{f_l} \{p_{f_l} \Pr(\mathbf{m}_n | f_l)\}$$

- **Neyman-Pearson Criterion:** Minimize probability of *false alarm* for specified probability of *detection*
Probability of false alarm $\Pr(FA)$: Probability of determining that system is faulty given no fault
Probability of detection $\Pr(D)$: Probability of determining that system is faulty given a fault
- **Problem:** Complexity of evaluating $\Pr(\mathbf{m}_n | f_l)$

ASSOCIATED MARKOV CHAINS

- **Finite-state machine driven by random inputs \Rightarrow Markov chain**

- Transition probabilities determined by \mathbf{A}_d, p_d for $d = 1, 2, \dots, K$
- N states, probability vector $\mathbf{v}[k]$ at time step k

- **Fault-free case:** $\mathbf{v}[k + 1] = \mathbf{A}\mathbf{v}[k]$ where $\mathbf{A} = \sum_{d=1}^K p_d \mathbf{A}_d$

- Steady-state \mathbf{v} satisfies $\mathbf{v} = \mathbf{A}\mathbf{v}$

- **Single-fault case:** $\mathbf{v}'[k + 1] = \mathbf{A}'\mathbf{v}'[k]$ where $\mathbf{A}' = \mathbf{A} + p_i \mathbf{E}_i$

- Steady-state \mathbf{v}' satisfies $\mathbf{v}' = \mathbf{A}'\mathbf{v}'$

- **Fact:** \mathbf{m}_n “converges” to \mathbf{v} or \mathbf{v}'

<p>Questions: (i) “Separation” between \mathbf{v} and \mathbf{v}' (ii) Rate of “convergence” of \mathbf{m}_n to \mathbf{v} or \mathbf{v}'</p>

SEPARATION

- **Distance in Variation:** $d_V(\mathbf{v}, \mathbf{v}') = \frac{1}{2} \sum_{l=1}^N |\mathbf{v}(l) - \mathbf{v}'(l)|$

\mathbf{v} and \mathbf{v}' are N -dimensional probability vectors

- **Theorem:**
 - (i) State-transition fault at state q_j under input x_i
 - (ii) Faulty machine remains connected
 - (iii) Steady-state vectors \mathbf{v} and \mathbf{v}'

$$\boxed{\frac{p_i \mathbf{v}(j)}{1 - \alpha + \beta} \leq d_V(\mathbf{v}, \mathbf{v}') \leq \frac{p_i \mathbf{v}'(j)}{1 + \alpha - \beta}}$$

$$\alpha = \max\{0, -p_i + \min_{l, l'} \mathbf{A}(l, l')\}$$

$$\beta = \min\{1, p_i + \max_{l, l'} \mathbf{A}(l, l')\}$$

- **Lemma:** $\boxed{d_V(\mathbf{v}, \mathbf{v}') \geq \frac{1}{2} p_i \mathbf{v}(j) \geq \frac{1}{2} p_{\min} v_{\min}}$

$$p_{\min} \equiv \min_d \{p_d\}$$

$$v_{\min} \equiv \min_l \{\mathbf{v}(l)\}$$

CONVERGENCE

- **Under No Fault:**

(i) Aperiodic Markov chain, transition matrix \mathbf{A} , steady-state \mathbf{v}

(ii) M smallest integer such that $\mathbf{A}^M > \mathbf{0}$ (element-wise)

(iii) $\lambda = \min_{l,l'} \left\{ \frac{\mathbf{A}^M(l,l')}{\mathbf{v}(l)} \right\}$

For all $j \in \{1, 2, \dots, N\}$ and $n > \frac{2M}{\lambda\epsilon}$

$$\Pr(|m_n(j) - \mathbf{v}(j)| \geq \epsilon) \leq \exp\left(-\frac{\lambda^2 \left(n\epsilon - \frac{2M}{\lambda}\right)^2}{2nM^2}\right)$$

- **Under Fault:** Similar situation (with \mathbf{A}' and \mathbf{v}')

- Adopted from Glynn and Ormoneit (other possibilities exist)

FAULT DETECTION STRATEGY

- **Rule:**

$d_V(\mathbf{m}_n, \mathbf{v}) \begin{array}{c} > \\ < \end{array} \theta$
<div style="display: flex; justify-content: space-between; width: 100%;"> Fault No Fault </div>

with $0 < \theta < \frac{1}{2}p_{\min}v_{\min}$

- **Resulting Bounds on $\Pr(D)$ and $\Pr(FA)$:**

$\Pr(\text{FA}) \leq N \exp\left(-\frac{\lambda_u^2 \left(\frac{2n\theta}{N} - \frac{2M_u}{\lambda_u}\right)^2}{2nM_u^2}\right)$
$\Pr(D) \geq 1 - N \exp\left(-\frac{\lambda_u^2 \left(\frac{n(p_{\min}v_{\min} - 2\theta)}{N} - \frac{2M_u}{\lambda_u}\right)^2}{2nM_u^2}\right)$

where $M_u = N$, $\lambda_u = (p_{\min})^N$, and n “large enough”

- **Distance Property:**

$d_V(\mathbf{m}_n, \mathbf{v}) + d_V(\mathbf{m}_n, \mathbf{v}') \geq d_V(\mathbf{v}, \mathbf{v}') \geq \frac{1}{2}p_{\min}v_{\min}$

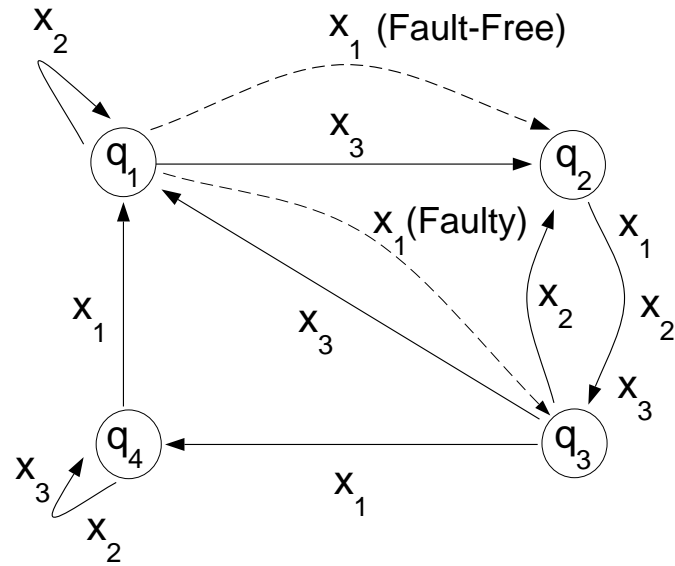
EXAMPLE (1)

Input Probabilities:

$$p_1 = \frac{1}{2}$$

$$p_2 = \frac{1}{3}$$

$$p_3 = \frac{1}{6}$$



$$\mathbf{A} = \begin{bmatrix} .333 & 0 & .167 & .500 \\ .667 & 0 & .333 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & .500 & .500 \end{bmatrix}$$

$$\mathbf{v} = [.25 \quad .25 \quad .25 \quad .25]^T$$

$$M = 3, \quad \lambda = 0.4444$$

$$\mathbf{A}' = \begin{bmatrix} .333 & 0 & .167 & .500 \\ .167 & 0 & .333 & 0 \\ .500 & 1 & 0 & 0 \\ 0 & 0 & .500 & .500 \end{bmatrix}$$

$$\mathbf{v}' = [0.286 \quad 0.143 \quad 0.286 \quad 0.286]^T$$

$$M' = 3, \quad \lambda' = 0.1944$$

EXAMPLE (2)

• **Distance in Variation:** $d_V(\mathbf{v}, \mathbf{v}') = 0.1071$

$$- d_V(\mathbf{v}, \mathbf{v}') \geq \frac{1}{2}p_1v(1) = \frac{1}{16}$$

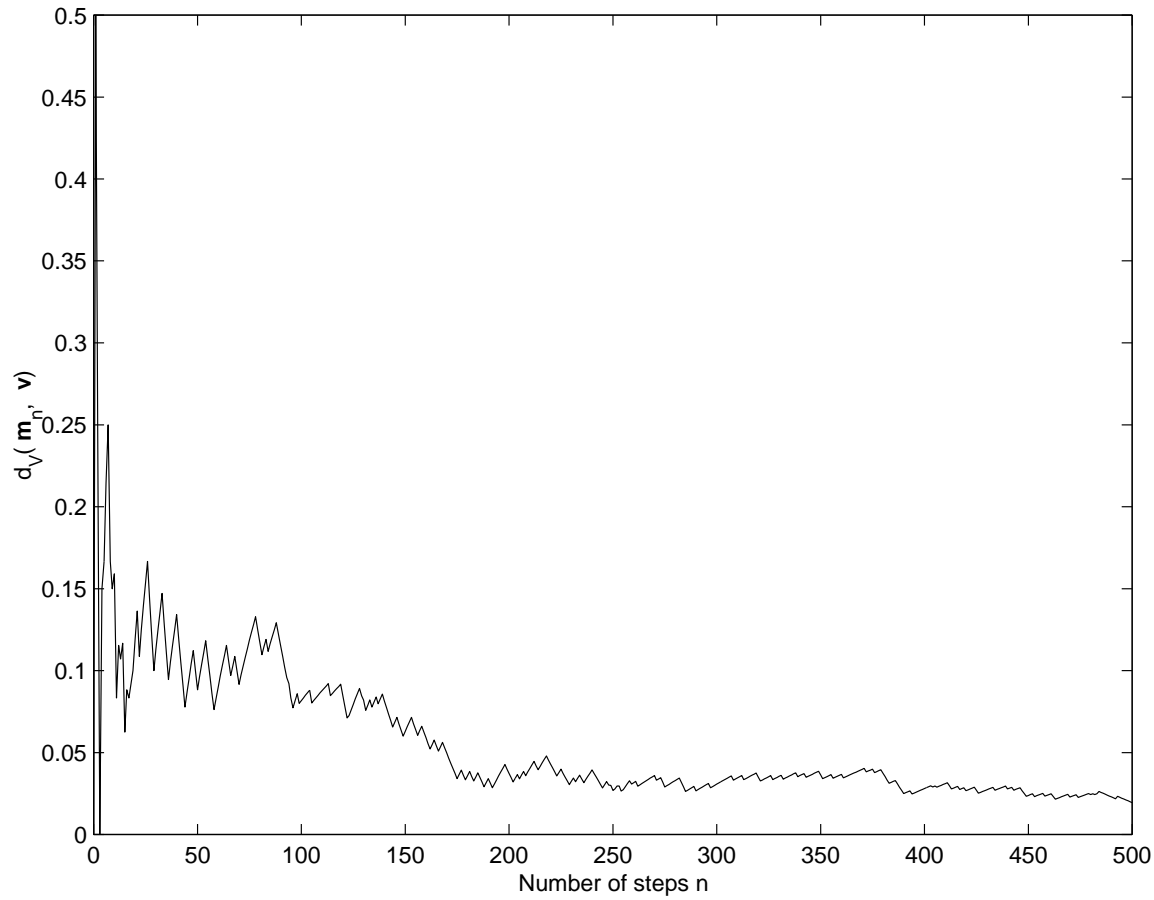
$$- d_V(\mathbf{v}, \mathbf{v}') \geq \frac{1}{2}p_{\min}v_{\min} = \frac{1}{48} \text{ (where } p_{\min} = 1/6 \text{ and } v_{\min} = 1/4)$$

• **Lower Bound:** $\frac{1}{2}p_{\min}v_{\min} = \frac{1}{48}$ lower bound on $d_V(\mathbf{v}, \mathbf{v}_{f_l})$

(single state-transition fault f_l that keeps the machine connected)

EXAMPLE (3)

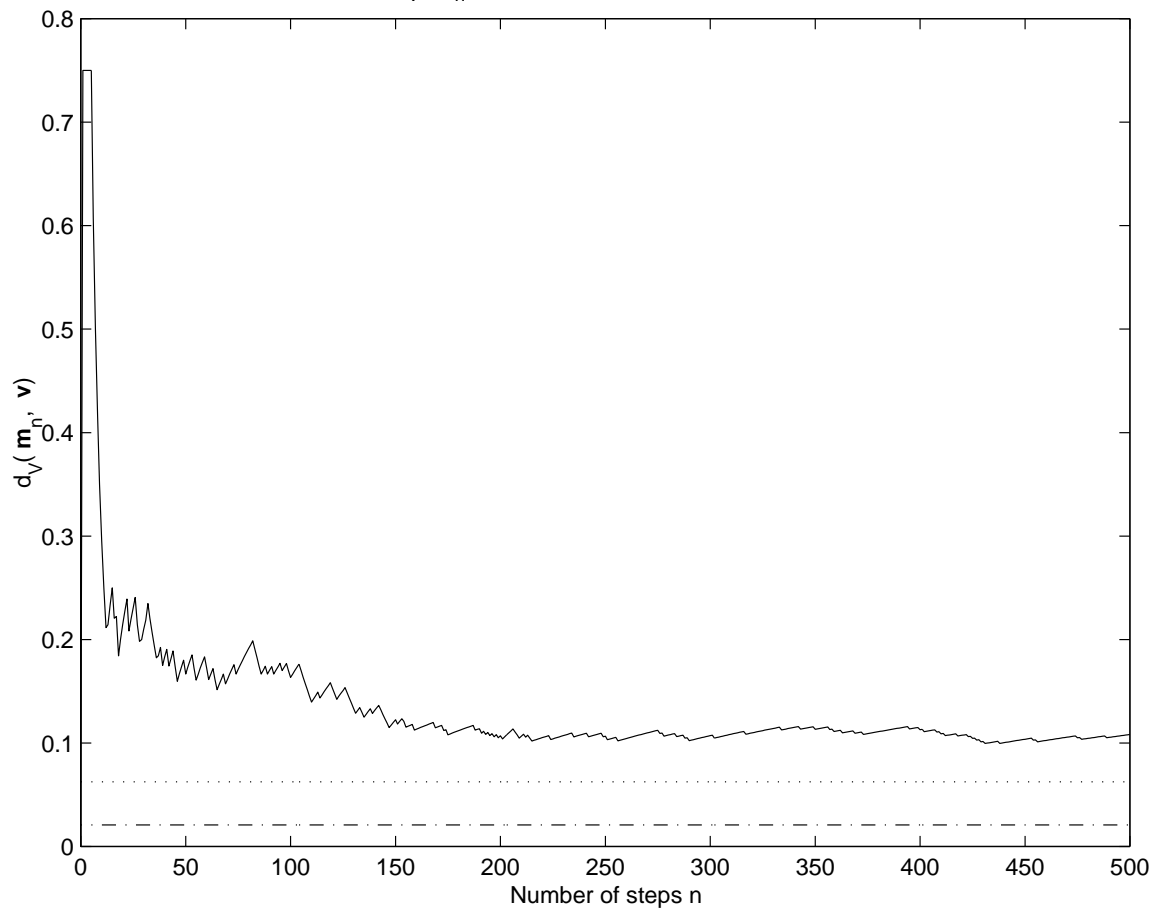
Plot of $d_V(\mathbf{m}_n, \mathbf{v})$ on a typical run of the fault-free machine



Typical Plot: $d_V(\mathbf{m}_n, \mathbf{v})$ for the fault-free FSM

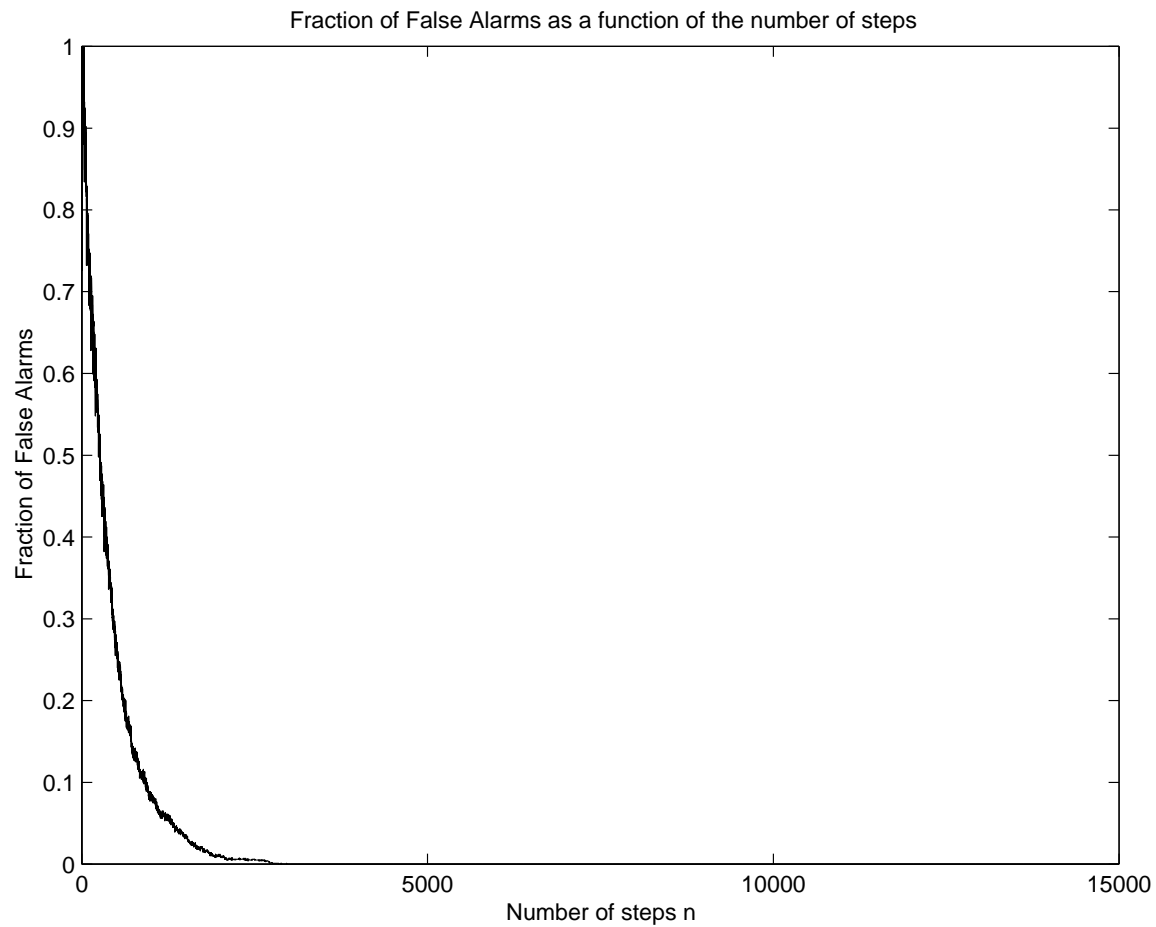
EXAMPLE (4)

Plot of $d_V(\mathbf{m}_n, \mathbf{v})$ on a typical run of the faulty machine



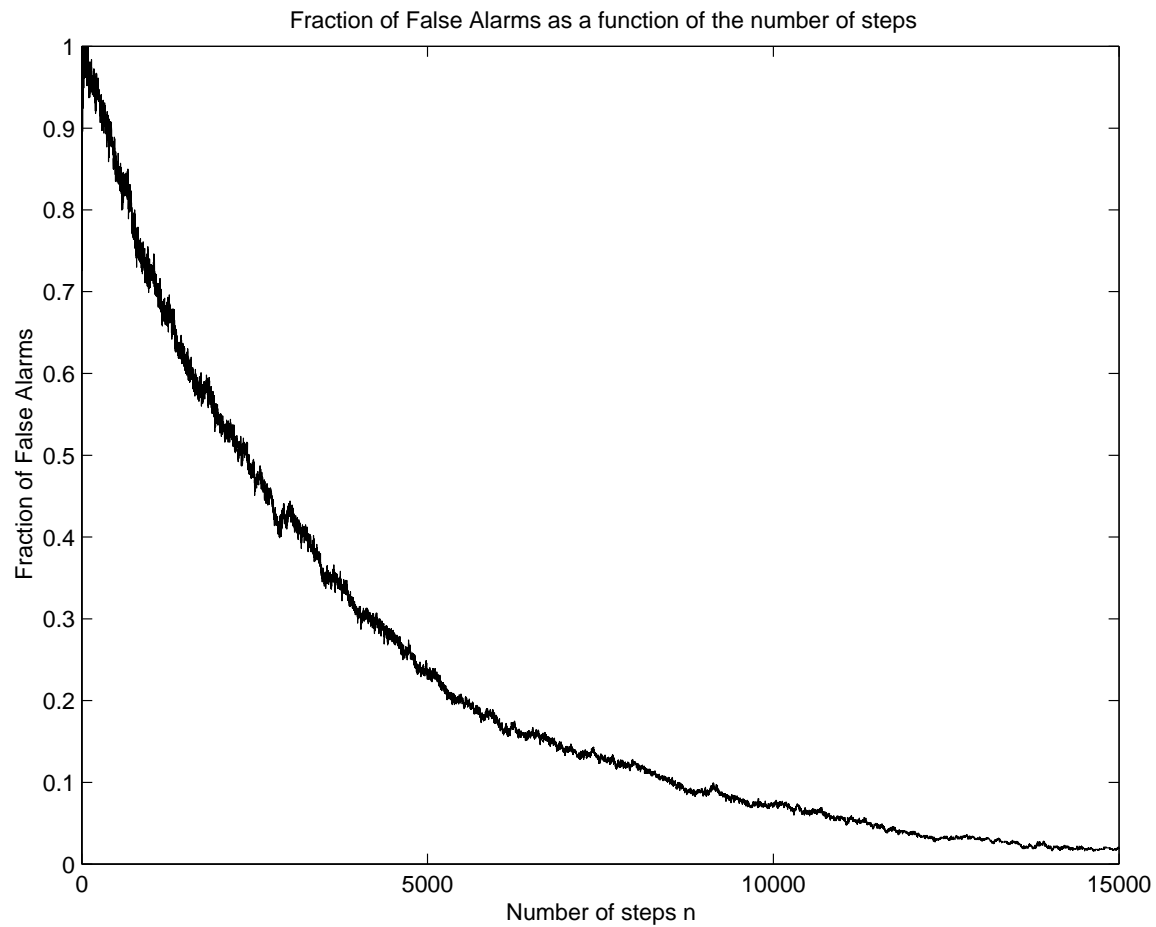
Typical Plot: $d_V(\mathbf{m}_n, \mathbf{v})$ for a faulty FSM

EXAMPLE (5)



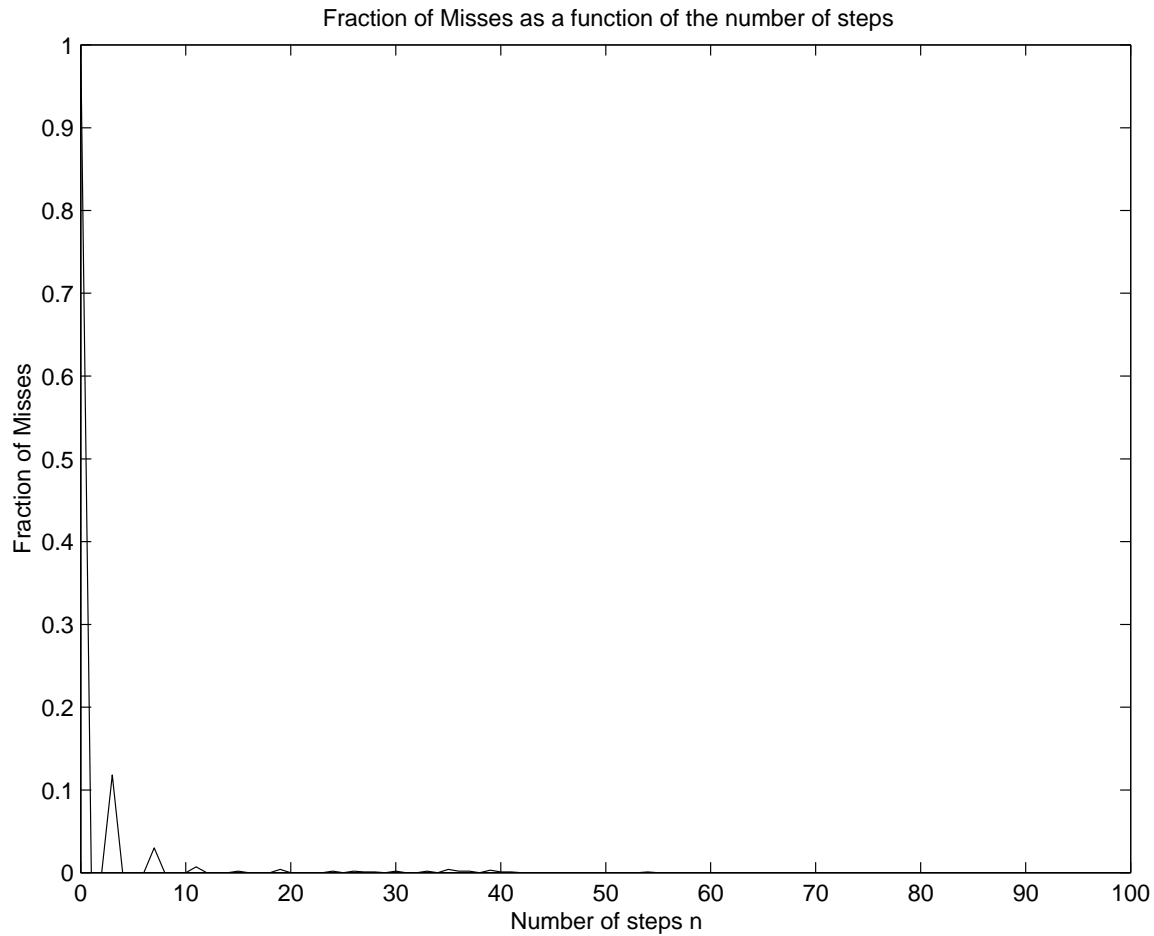
Fraction of False Alarms: Over 10^3 runs of the fault-free FSM for $\theta_1 = 1/16$

EXAMPLE (6)



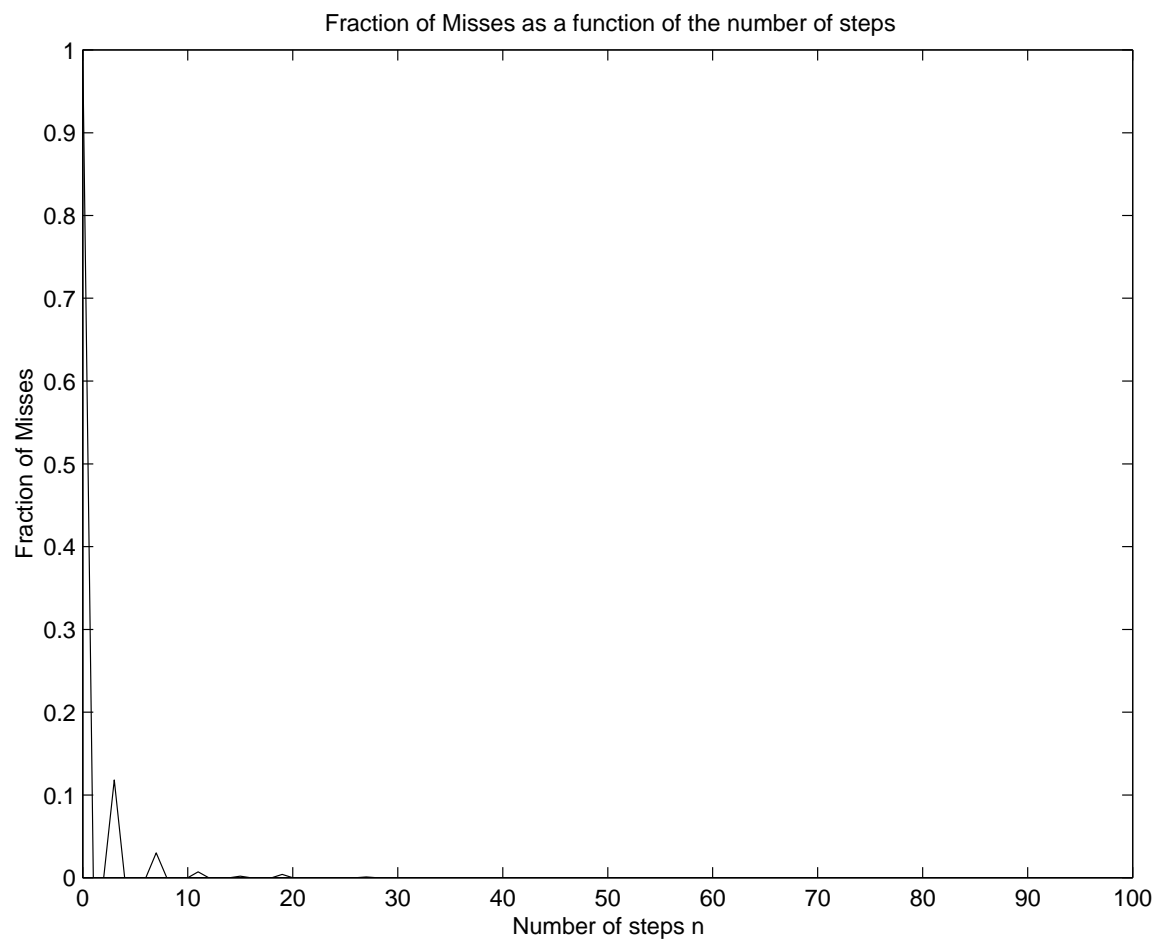
Fraction of False Alarms: Over 10^3 runs of the fault-free FSM for $\theta_2 = 1/48$

EXAMPLE (7)



Fraction of Misses: Over 10^3 runs of the faulty FSM for $\theta_1 = 1/16$

EXAMPLE (8)



Fraction of Misses: Over 10^3 runs of the faulty FSM for $\theta_2 = 1/48$

SUMMARY AND CONCLUSIONS

- **Contributions:**

- Probabilistic fault detection in deterministic FSMs
- Input sequence unknown, input statistics known
- State sequence unknown, state occupancies known
- Confidence measures as functions of n

- **Extensions:**

- Partial observations (e.g., output measurements)
- Tighter bounds
- Potential advantages (out-of-order observations, random sampling)
- Applications (circuit testing, verification, monitoring)

OTHER CONNECTIONS?

- Use lumped Markov chains for hierarchical fault diagnosis
- Use of hidden Markov models to capture fault-free and faulty system behavior
- Sampling techniques to capture partially known input/state sequences