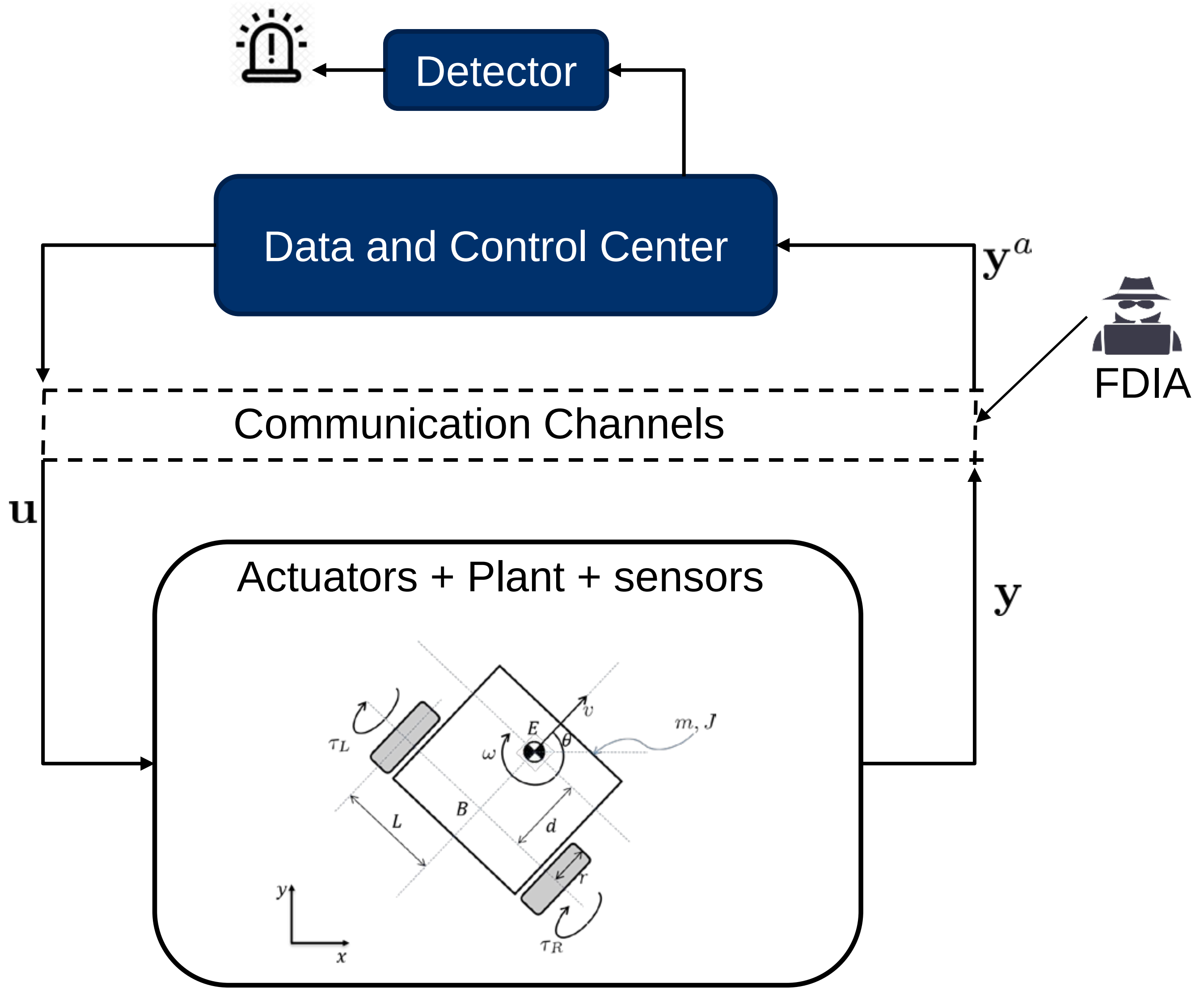
ATTACK-RESILIENT OBSERVER PRUNING FOR PATH-TRACKING CONTROL OF WHEELED MOBILE ROBOT

Y. Zheng
O. M. Anubi

FLORIDA STATE UNIVERSITY
CENTER FOR ADVANCED POWER SYSTEMS

Motivation

Output feedback control for WMR based on communication network



System and problem statement

- System construction
  - Plant model
  - Path-tracking control design
  - Measurement model
  - Observer scheme
- False data injection attack
  - Residual-based monitor
  - FDIA design
- Resilient estimation
  - Compressed sensing
  - Attack detection and localization

Plant model: (dynamic and kinematic model)

$$M\dot{\mathbf{q}} + D(\mathbf{q})\mathbf{q} = B\tau$$

$$\begin{bmatrix} \dot{\theta} \\ \cdots \\ \dot{\mathbf{z}} \end{bmatrix} = \bar{C}(\theta)\mathbf{q} = \begin{bmatrix} 0 \quad 1 \\ \cdots \\ C(\theta) \end{bmatrix} \mathbf{q} \qquad (1)$$

$$\mathbf{q} = \begin{bmatrix} v \\ \omega \end{bmatrix} \qquad \mathbf{z} = \begin{bmatrix} x \\ y \end{bmatrix}$$

$$M = \begin{bmatrix} m & 0 \\ 0 & md^2 + J \end{bmatrix}, \quad D = \begin{bmatrix} 0 & -md\omega \\ md\omega & 0 \end{bmatrix}$$

$$B = \frac{1}{r}\begin{bmatrix} 1 & 1 \\ L & -L \end{bmatrix}, \quad C(\theta) = \begin{bmatrix} \cos(\theta) & -d\sin(\theta) \\ \sin(\theta) & d\cos(\theta) \end{bmatrix}.$$

Error System: (dynamic and kinematic model)

Target trajectory: $[\theta_d \quad x_d \quad y_d]^\top$

$$\mathbf{e} = \begin{bmatrix} \theta - \theta_d \\ \mathbf{z} - \mathbf{z}_d \end{bmatrix} = \begin{bmatrix} \mathbf{e}_\theta \\ \mathbf{e}_\mathbf{z} \end{bmatrix} \qquad (2)$$

$$\widetilde{\mathbf{q}} = \mathbf{q} - \mathbf{q}_d$$

Path-tracking control

Path-tracking control design:

$$\tau = B^{-1}(M\mathbf{u} + D\mathbf{q}) \qquad (3)$$
$$\mathbf{u} = -k_q(\mathbf{q} - \mathbf{q}_d) + \dot{\mathbf{q}}_d - \bar{C}(\theta)^\top \mathbf{e}$$

$$\mathbf{q}_d = C^{-1}(\theta)(\dot{\mathbf{z}}_d - k_e\mathbf{e_z})$$
$$\dot{\mathbf{q}}_d = -k_e(\dot{C}^{-1}(\theta)\mathbf{e_z} + \mathbf{q}) + C^{-1}(\theta)[\ddot{\mathbf{z}}_d + (k_e + C(\theta)\dot{C}^{-1}(\theta))\dot{\mathbf{z}}_d]$$

Stability criterion: Consider the control law given in (3), if the control gains k_q and k_e are chosen as $k_q > 0, k_e > 0$, then the tracking errors in (2) converges to zero asymptotically. Furthermore, the generalized velocities tracking error $\tilde{\mathbf{q}} = \mathbf{q} - \mathbf{q}_d$ converges to zero asymptotically with $\dot{\mathbf{z}}_d = C(\theta)\mathbf{q}_d$ satisfied in the limit.

Proof: Candidate Lyapunov function: $V = \frac{1}{2}\|\tilde{\mathbf{q}}\|^2 + \frac{1}{2}\|\mathbf{e}\|^2$

$$\dot{V} \leq -k_q\|\tilde{\mathbf{q}}\|^2 - k_e\|\mathbf{e}_z\|^2 \qquad (5)$$

(Negative semi-definite)

$\tilde{\mathbf{q}}, \mathbf{e} \in \mathcal{L}_\infty$

$$\left.\begin{aligned} \dot{\tilde{\mathbf{q}}} &= -k_q\tilde{\mathbf{q}} - \bar{C}(\theta)^\top\mathbf{e} \in \mathcal{L}_\infty \\ \dot{\mathbf{e}} &= \bar{C}(\theta)\tilde{\mathbf{q}} - k_e\begin{bmatrix}0\\ \mathbf{e_z}\end{bmatrix} \in \mathcal{L}_\infty \end{aligned}\right\}$$

$\mathbf{e}$ and $\tilde{\mathbf{q}}$ are uniformly continuous.

Barbalat's Lemma → $\mathbf{e}(t) \to 0, \tilde{\mathbf{q}}(t) \to 0.$

$$V - V(0) \leq -\int_0^t \left(k_q\|\tilde{\mathbf{q}}(\tau)\|^2 + k_e\|\mathbf{e_z}(\tau)\|^2\right)d\tau \text{ implies } \tilde{\mathbf{q}}, \mathbf{e_z} \in \mathcal{L}_2.$$

Measurement system and monitor

Measurement model:

$$\mathbf{y} := f(\mathbf{x}) + \mathbf{v} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1/4r & L/4r \\ 1/4r & -L/4r \\ \cos(\theta) & -d\sin(\theta) \\ \sin(\theta) & d\cos(\theta) \end{bmatrix} \cdot \mathbf{q} + \mathbf{v}$$

Observer: Unscented Kalman Filter

$$\min E[(\mathbf{x}_0 - \hat{\mathbf{x}}_0)(\mathbf{x}_0 - \hat{\mathbf{x}}_0)^\top]$$

Residual-based monitor:

$$\Psi_T : \{Y_T, U_T\} \mapsto \{\Psi_1, \Psi_2\}$$

$Y_T \in R^{m \times T}$: measurements during time horizon T

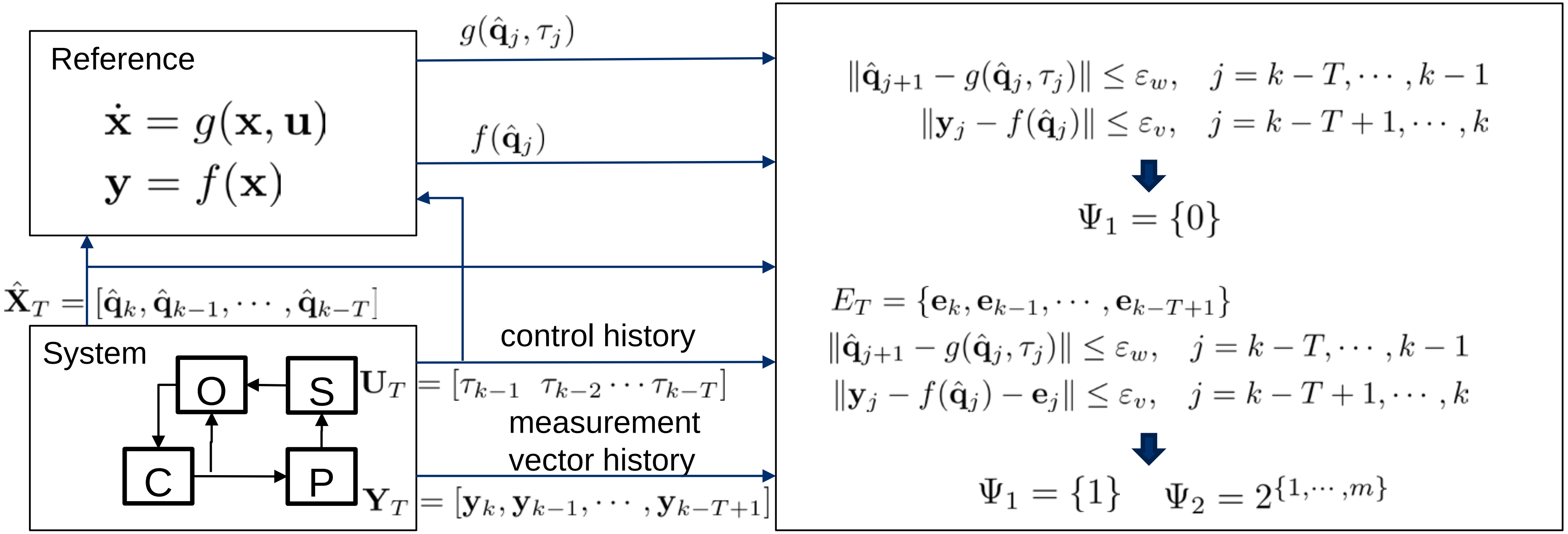
$U_T \in R^{l \times T}$: controlled inputs during time horizon T

$\Psi_1 = \{0(safe), 1(unsafe)\}$ Alarm

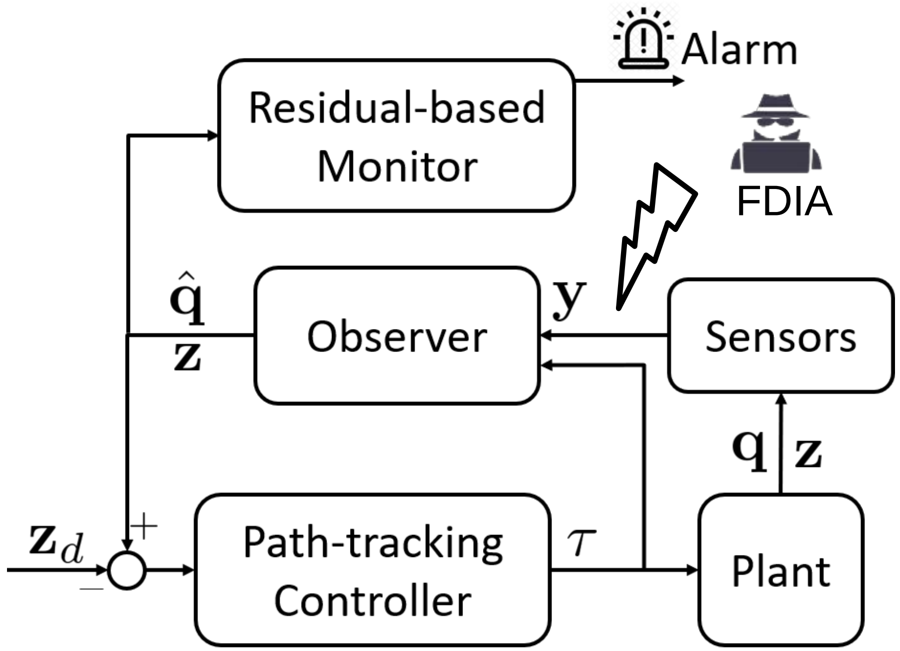
$\Psi_2 = 2^{\{1,2,\cdots,m\}}$ Alarm location

Monitor

Residual-based monitor:



False-data Injection Attacks



FDIA Design:

$$Y_f = H\mathbf{x}_k + G\mathbf{u}_f + e$$

$$H = \begin{bmatrix} C_d \\ C_d A_m \\ C_d A_m^2 \\ \vdots \\ C_d A_m^{T_f} \end{bmatrix}, G = T_s \begin{bmatrix} 0 & 0 & \cdots & 0 \\ C_d B_m & 0 & \cdots & 0 \\ C_d A_m B_m & C_d B_m & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ C_d A_m^{T_f-1} B_m & C_d A_m^{T_f-2} B_m & \cdots & C_d B_m \end{bmatrix}$$

$$H = [U_1 \;\; U_2] \begin{bmatrix} \Sigma_1 \\ 0 \end{bmatrix} V$$

Given selction vector $\mathcal{T}$ under upper-bound of attack percentage P_A, one successful FDIA can be constructed by:

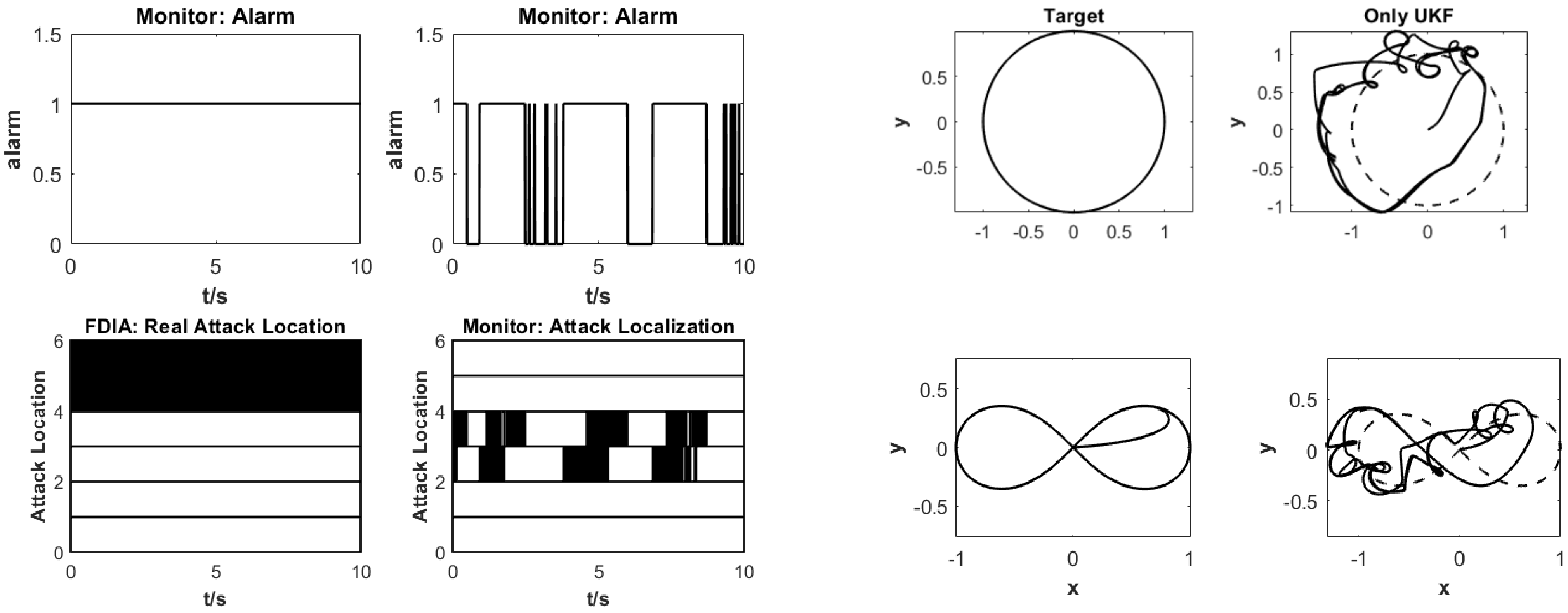
$$\text{Maxmize}: \quad \|U_{1,\mathcal{T}.}^{\top}\mathbf{e}\|,$$

$$\text{Subject to}: \quad \|(U_{2,\mathcal{T}.}^{\top})_j \mathbf{e}_j\| \leq \tau_j, \quad j \in \mathcal{T}$$

(where, τ_j is the escaping parameter of bad data detector defined by $\|(U_{2,\mathcal{T}.}^{\top})_j\| \cdot \varepsilon_v$)

False-data Injection Attacks

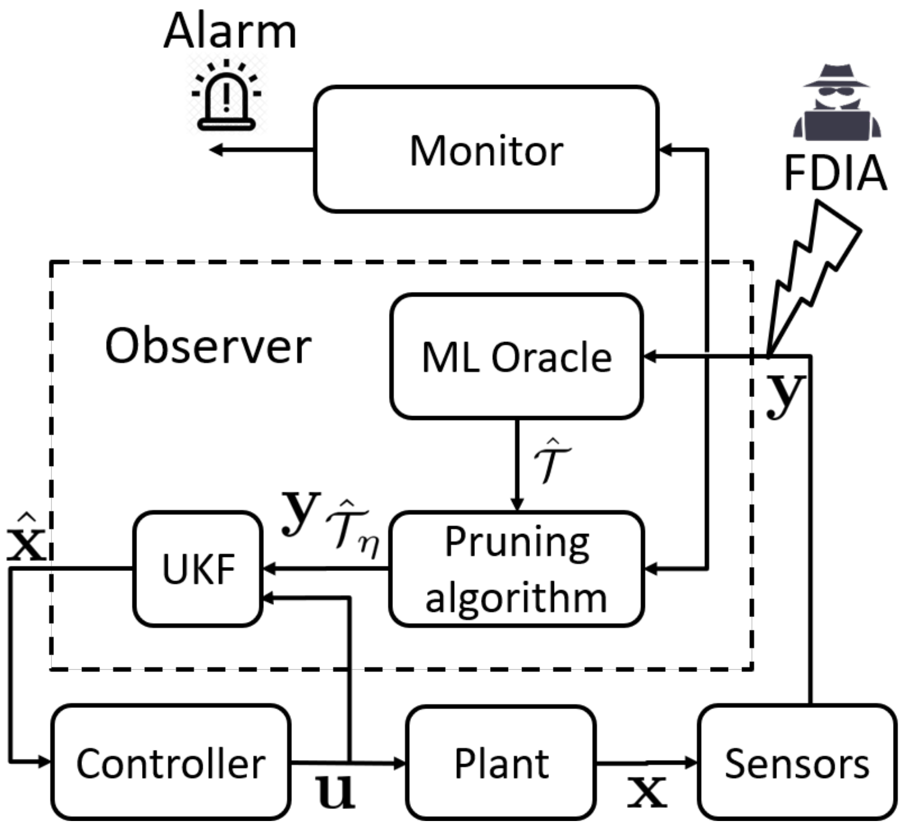
FDIA Design:



Resilient estimation

Resilient estimation：

Attack localization ✚ Robust estimation algorithm



Main results

Uncertainty of Oracle：

Actual support

$\mathcal{T}^c$

$$\mathbf{q}_i = \begin{cases} 1 & \text{if } \ i \in \mathcal{T}^c \\ 0 & \text{otherwise} \end{cases}$$

Oracle support

$\hat{\mathcal{T}}^c$

$\hat{\mathbf{q}}$

Uncertainty model

$$\mathbf{q}_i = \epsilon_i \hat{\mathbf{q}}_i + (1 - \epsilon_i)(1 - \hat{\mathbf{q}}_i)$$

$\epsilon_i \sim \mathcal{B}(1, p_i)$ is the agreement defined by: $\epsilon_i = \begin{cases} 1 & \text{if } \ \hat{\mathbf{q}}_i = \mathbf{q}_i \\ 0 & \text{if } \ \hat{\mathbf{q}}_i = 1 - \mathbf{q}_i \end{cases}$

probability mass function: $Pr\left(\sum_{i=1}^{m} \epsilon_i = k - 1\right) = \mathbf{r}(k), k = 1, \cdots, m+1$

$$\mathbf{r} = \prod_{i=1}^{m} P_i \cdot \mathbf{g}_1 * \cdots * \mathbf{g}_i * \cdots * \mathbf{g}_m, \ \mathbf{r} \in R^{m+1}, \text{ and } \mathbf{g}_i = \begin{bmatrix} \frac{1-P_i}{P_i} \\ 1 \end{bmatrix}$$

Main results

Pruning Algorithm：

1. Obtaining reliable trust parameter：

Given reliability level $\eta \in (0,1)$, return the maximum integer $l_\eta \leq N$ such that l_η safe nodes are correctly localized with a probability of at least η:

$$l_\eta = \max\left\{k \mid \Pr\left\{\sum_{i\in\hat{\mathcal{T}}^c} \epsilon_i \geq k\right\} \geq \eta\right\}$$
$$= \max\left\{k \mid \sum_{i=1}^{k+1} \mathbf{r}_{\hat{\mathcal{T}}^c}(i) \leq 1-\eta\right\}$$

2. Pruning：

A new support is obtained through a robust extraction:

$$\hat{\mathcal{T}}_\eta^c = \left\{\text{argsort} \downarrow (\mathbf{p} \circ \hat{\mathbf{q}})\right\}_1^{l_\eta}$$

where, $\{\cdot\}_1^{l_\eta}$ is an index extraction from the first elements to l_η elements.

Remark： If the underlying machine learning algorithm works better than random flip of fair coin, then through pruning algorithm, it follows

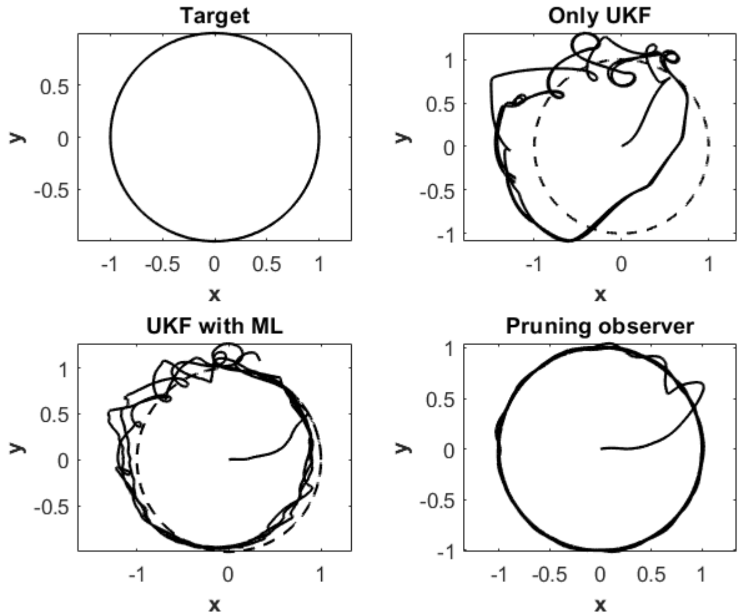
$$\Pr\{\hat{\mathcal{T}}_\eta^c \cap \mathcal{T} = \emptyset\} \geq \eta.$$

Simulation

Circle path tracking:

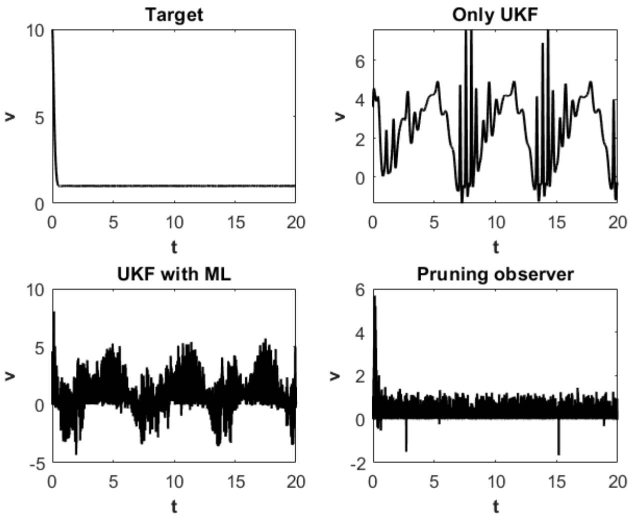
$$\text{Target: } \begin{bmatrix} t \\ cos(t) \\ sin(t) \end{bmatrix}$$

path tracking

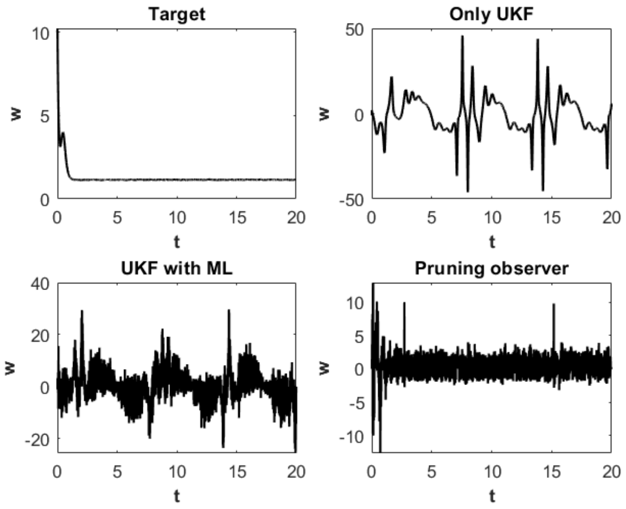


State estimation

Forward velocity (v)



angular velocity (w)



Conclusion

- Conclusion

  An attack-resilient control and estimation scheme for path-tacking task of WMR under false data injection attacks

  - Stable path-tracking control system for non-holonomic WMR
  - Optimization-based FDIA design scheme
  - Pruning-based observer design using UKF as the underlying observer

- Future work
  - **Measurement redundancy:** include L1-minimization with pruning algorithm
  - **Robustness:** L1-based Receding horizon estimation scheme
  - **Concurrency:** Concurrent learning model

THANK YOU

Olugbenga Moses Anubi – anubi@caps.fsu.edu

More information:

eng.famu.fsu.edu/~anubi/

Simulation codes: https://github.com/ZYblend/Resilient-Pruning-Observer-against-for-WMR-under-FDIA