False Data Injection Detection in Cyber-Physical System

Álan Crístoffer e Sousa
(alan.e-sousa@univ-reims.fr)

CReSTIC

UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE

Supervisor: Prof. Dr. Nadhir Messai
Cosupervisor: Prof. Dr. Noureddine Manamanni

Reims
June 2022

Index

False Data Injection

- ✓ **Static False Data Injection**: the attacker changes the sensor reading sent, replacing it statically.
- ✗ **Dynamic False Data Injection**: the attacker changes the sensor reading dynamically, slowly changing it so residuals change slowly.

$$\tilde{x}_j = x_i, \tag{1}$$

$$\tilde{x}_j = x_j + \delta, \tag{2}$$

$$\tilde{x}_j = x_j \cdot \alpha, \tag{3}$$

Functional Observer

- $y(t)$ are the measured outputs.
- $z(t)$ are the states we wish to estimate.
- The observer has a reduced order dynamics system which is equivalent to the original one.
- Problem 1: how to find a $w(t)$ that correctly estimates $z(t)$.
- Problem 2: how to find the observer's matrices N, J, H and E.

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) + Lf(t), \\ y(t) &= Cx(t), \\ z(t) &= Fx(t), \end{aligned} \tag{4}$$

$$\begin{aligned} \dot{w}(t) &= Nw(t) + Jy(t) + Hu(t), \\ \hat{z}(t) &= w(t) + Ey(t). \end{aligned} \tag{5}$$

Observability

- All desired states $z(t)$ must be observable from the outputs $y(t)$.
- The observability of (A, C, F) cannot be greater than that of (A, C).
- There must be a path from every output $y(t)$ to every output $z(t)$ in the dynamics graph.

$$rank \begin{bmatrix} C \\ CA \\ F \\ FA \end{bmatrix} = rank \begin{bmatrix} C \\ CA \\ F \end{bmatrix}. \quad (6)$$

Path Finder Algorithm

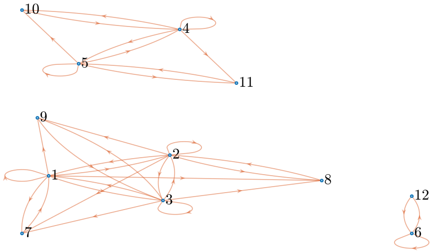

Figure: Puma 560 dynamic's graph representation.

Bank of Observers

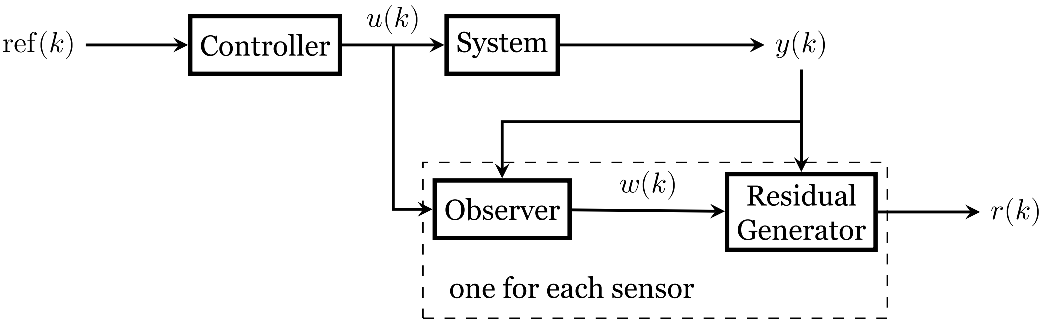

Figure: Observer's block diagram

Observer Design

$$\begin{aligned} \arg\min \ & \|P\|_2 \\ \text{s.t. } & \dot{V} \prec 0 \\ & P \succ 0, \end{aligned} \tag{7}$$

where

$$\dot{V} \equiv \begin{bmatrix} X & W \\ W^\top & -I \end{bmatrix}, \tag{8}$$

$\lambda \in \mathbb{R}^+$ is a free constant,

P is a semidefinite positve matrix

with

$$\begin{aligned} X =& \hat{A}^\top F^\top P - \hat{A}^\top C^\top \hat{E}^\top - \\ & \hat{C}^\top \hat{K}^\top + PF\hat{A} - \hat{E}C\hat{A} - \hat{K}\hat{C} - \lambda I, \end{aligned} \tag{9}$$

$$W = \sqrt{\lambda}(PF - \hat{E}C). \tag{10}$$

$$\begin{aligned} \hat{A} &= AF^+, \\ \hat{C} &= CF^+, \\ \hat{E} &= PE = PU + \hat{Y}V, \\ \hat{K} &= PK, \\ \hat{Y} &= PY. \end{aligned} \tag{11}$$

$$\begin{aligned} K &= P^{-1}\hat{K}, \\ Y &= P^{-1}\hat{Y}, \\ E &= U + YV, \\ R &= F - EC, \\ N &= (RA - KC)F^+, \\ J &= K + NE, \\ H &= RB. \end{aligned} \tag{12}$$

Observer Design Development

$$
\begin{aligned}
e &= \hat{z} - z \\
&= w + Ey - Fx \\
&= w + ECx - Fx.
\end{aligned}
\tag{13}
$$

$$
\begin{aligned}
\dot{e} &= \dot{w} + (EC - F)\dot{x} \\
&= Nw + Jy + Hu + (EC - F)(Ax + Bu + Lf) \\
&= Ne + (NF - NEC + ECA - FA + JC)x + \\
&\quad (H + ECB - FB)u + (ECL - FL)f.
\end{aligned}
\tag{14}
$$

N must be Hurwitz-stable,

$$
\begin{aligned}
N(F - EC) - (F - EC)A + JC &= 0, \\
H - (F - EC)B &= 0.
\end{aligned}
\tag{15}
$$

$$
\begin{aligned}
(F - EC)L_i &= 0, \\
(F - EC)L_n &\neq 0.
\end{aligned}
\tag{16}
$$

Observer Design Development

$$V = e^\top P e, \tag{17}$$
$$\dot{e} = Ne - (F - EC)L_n f, \tag{18}$$
$$e \propto L_n f, \tag{19}$$
$$\|L_n f\| = \lambda \|e\|, \tag{20}$$
$$R = F - EC, \tag{21}$$
$$\dot{e} = Ne - R\lambda \|e\|. \tag{22}$$

$$\begin{aligned}
\dot{V} &= \dot{e}^\top P e + e^\top P \dot{e} \\
&= (Ne - \lambda R \|e\|)^\top P e + e^\top P (Ne - \lambda R \|e\|) \\
&= e^T (N^\top P + PN) e - 2\lambda \left\| e^\top P R \right\| \cdot \|e\| \\
&\leq e^T (N^\top P + PN) e - \lambda (\left\| e^\top P R \right\|^2 + \|e\|^2) \\
&= e^T (N^\top P + PN - \lambda P R R^\top P - \lambda I) e.
\end{aligned} \tag{23}$$

Observer Design Development

$$
\begin{aligned}
N(F-EC) &= RA - JC,\\
NF &= RA - (J - NE)C,\\
K &= J - NE,\\
N &= RAF^{+} - KCF^{+},
\end{aligned}
\tag{24}
$$

$$
\begin{aligned}
(F-EC)L_i &= 0,\\
ECL_i &= FL_i,\\
E &= FL_i(CL_i)^{+} + Y(I - (CL_i)(CL_i)^{+}),\\
U &= ECL_iL_i^{+},\\
V &= I - L_iL_i^{+},\\
E &= U + YV.
\end{aligned}
\tag{25}
$$

$$
\begin{aligned}
\dot{V} = e^{T}((&R\hat{A} - EC\hat{A} - K\hat{C})^{\top}P+\\
&P(R\hat{A} - EC\hat{A} - K\hat{C}) - \lambda PRR^{\top}P - \lambda I)e.\\
&= \hat{A}^{\top}F^{\top}P - \hat{A}^{\top}C^{\top}\hat{E}^{\top} - \hat{C}^{\top}K^{\top}+\\
&PF\hat{A} - \hat{E}C\hat{A} - K\hat{C} - \lambda PRR^{\top}P - \lambda I.
\end{aligned}
\tag{26}
$$

UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE

Residual Generator

$$r(t) = Gw(t) + My(t), \tag{27}$$

$$\begin{aligned} M &= (C(1 - L_i))^\top, \\ G &= -M(I - CF^+E)^{-1}CF^+, \end{aligned} \tag{28}$$

$$\begin{aligned} r &= Gw + My \\ &= Q(y - Cx) \\ &= Q(y - CF^{-1}\hat{z}) \\ &= Q(y - CF^{-1}(w + Ey)) \\ &= Q((I - CF^{-1}E)y - CF^{-1}w), \end{aligned} \tag{29}$$

$$\begin{aligned} M &= Q(I - CF^{-1}E), \\ G &= -QCF^{-1}. \end{aligned} \tag{30}$$

Results

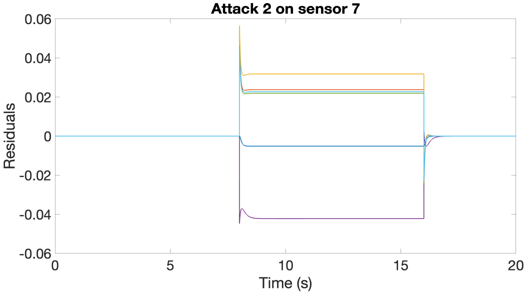

Figure: Residuals for attack on sensor 7, with $\delta = 1$.

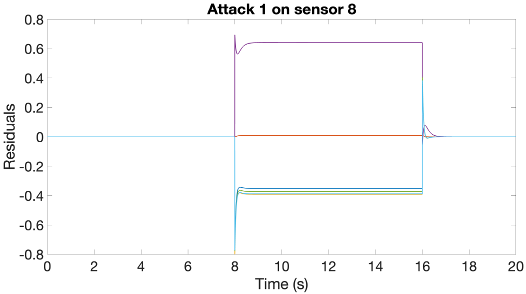

Figure: Residuals for attack on sensor 8, copying the values from sensor 9.

Final Considerations

- The formulation is straightforward, optimization based and extendable.
- The example was a simple system for didactic reasons, but this kind of observer is better suited for large, sparse systems.

Future Works Perspective

- Extend to detect Dynamic False Data Injection attacks.
- Discrete-time version.
- Use with other techniques to detect other types of attacks.