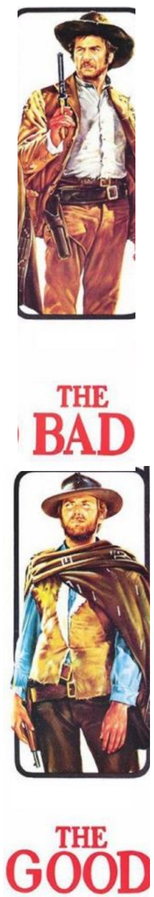
Adversary Control Strategy for Cyberphysical Networked Systems

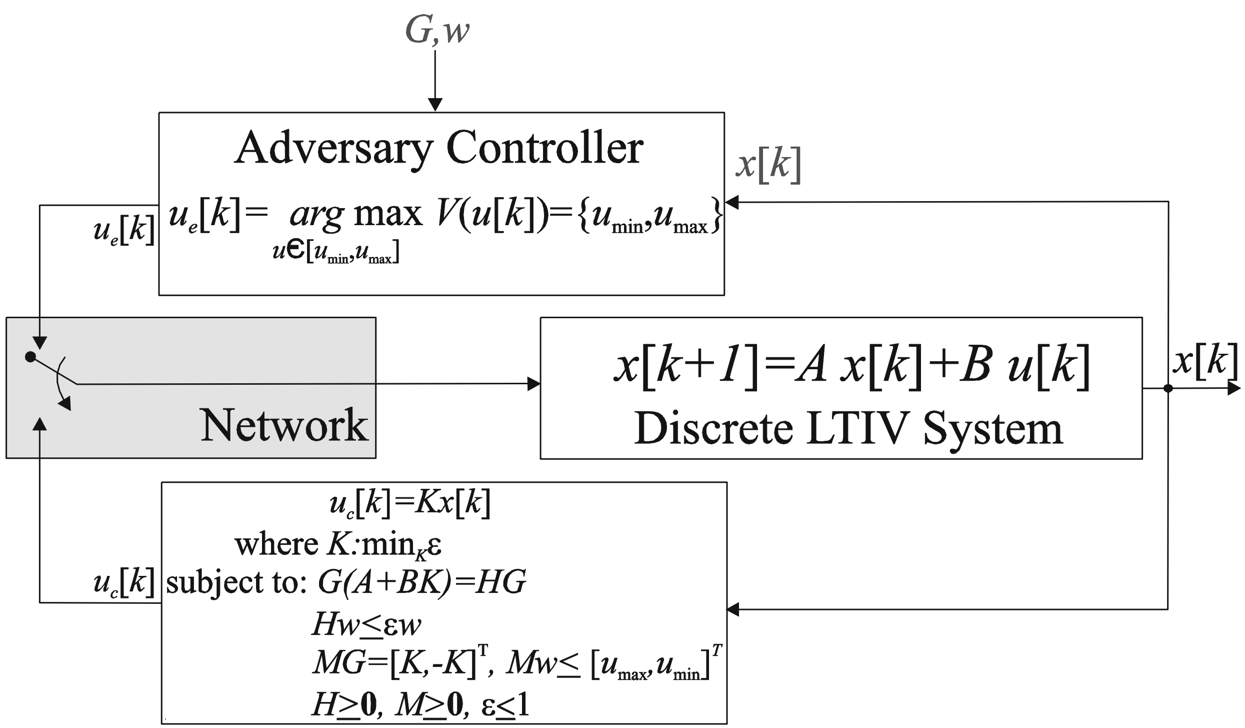
Efstathios Kontouras and Anthony Tzes

University of Patras

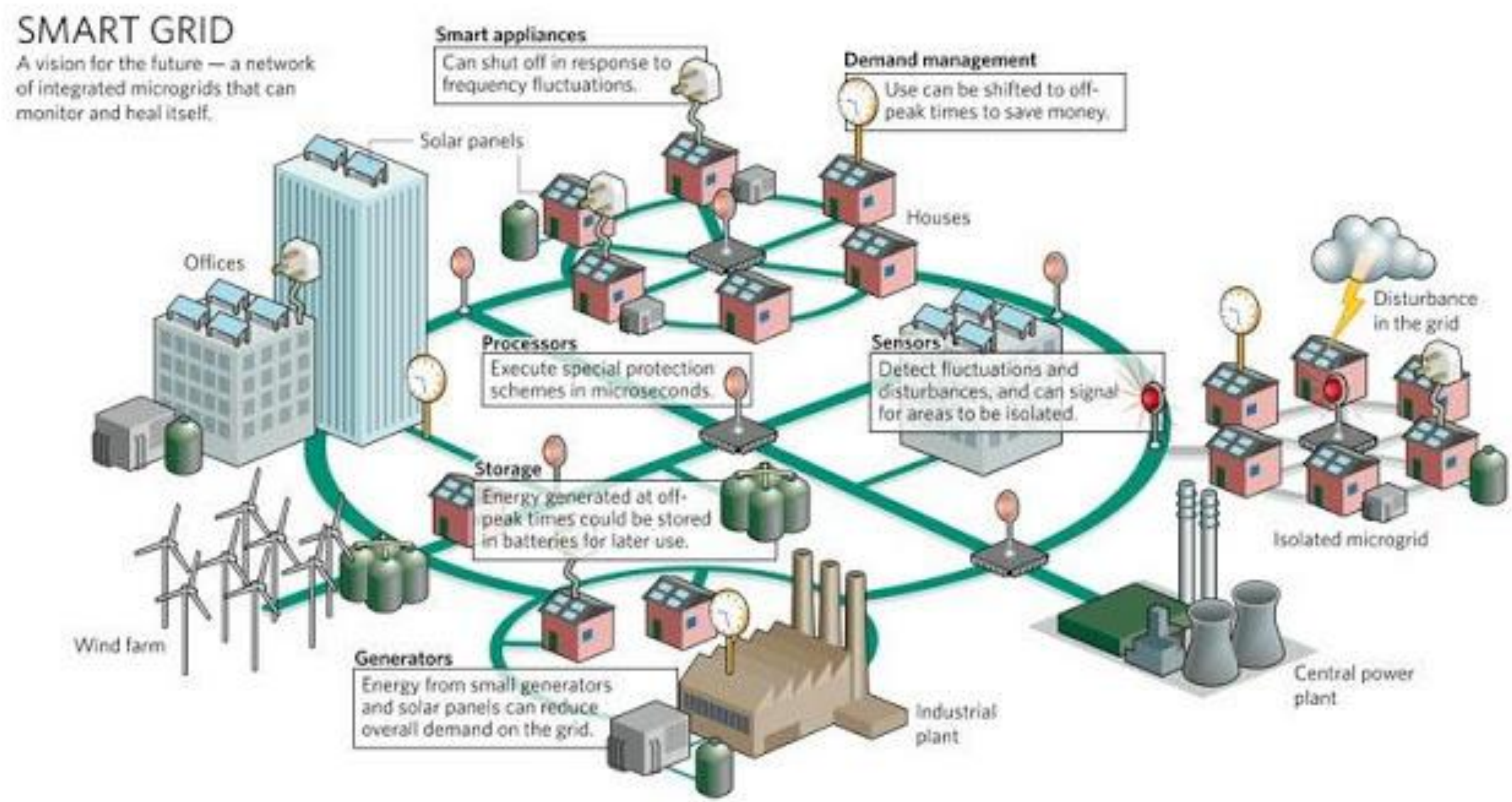
Electrical & Computer Engineering Department

GREECE

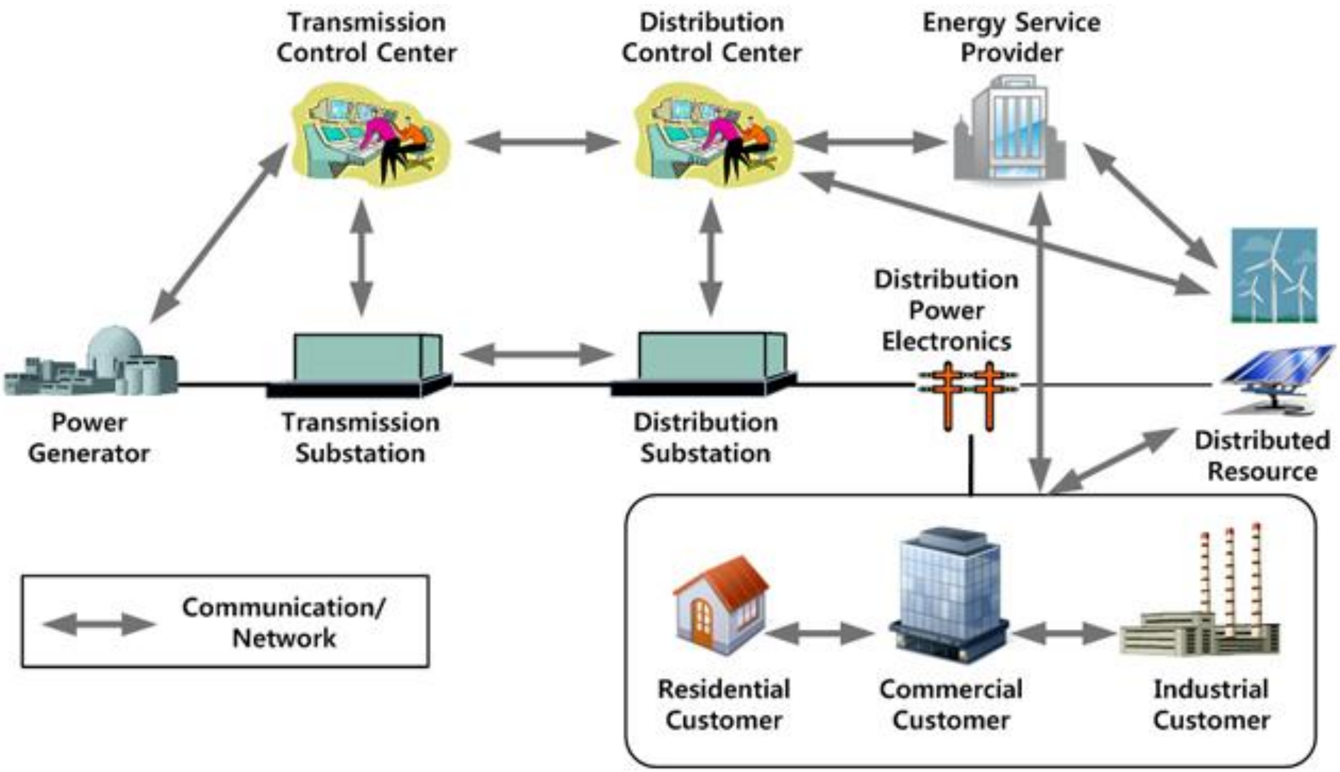




Motivation: Adversary Control for Frequency Instability in Distributed Power Systems



Adversary Attacks at Communications Network of the «Transmission and Distribution Control Center»



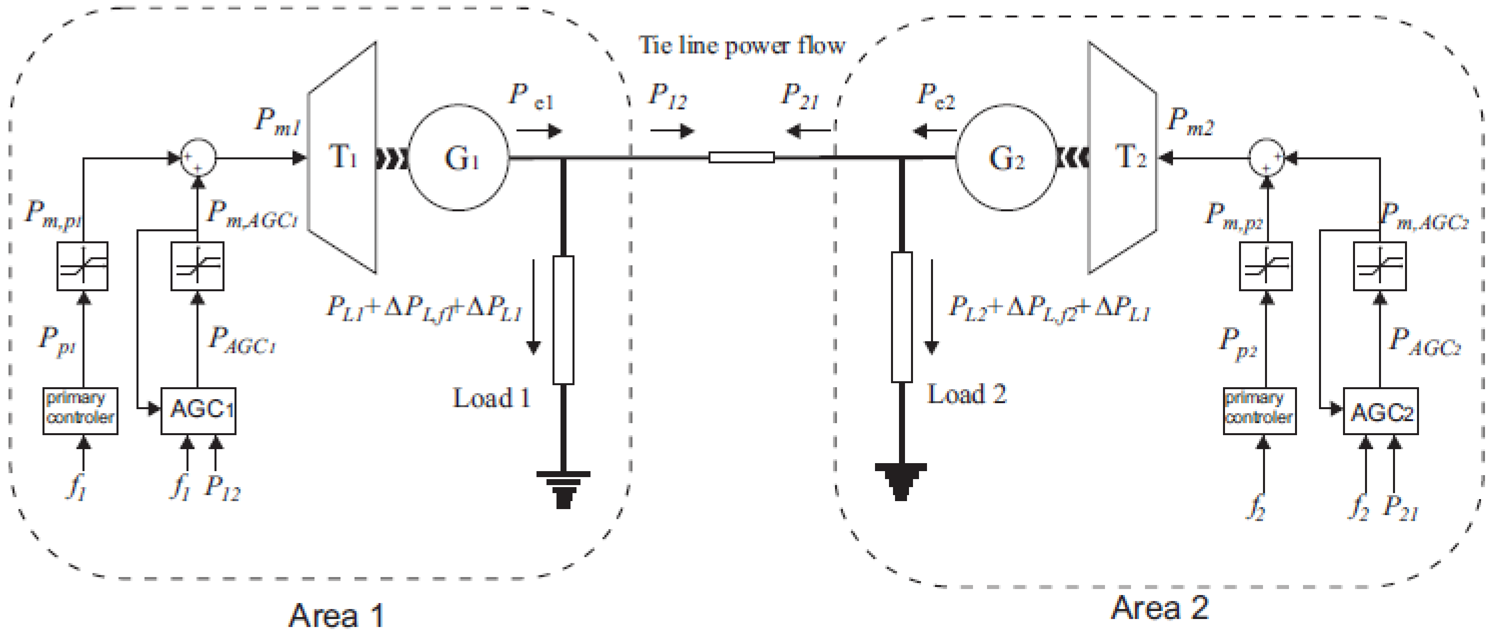


Fig. 1. Two-Area Power System with AGC

Lygeros et al, ACC09

$$\Delta \dot{f}_1 = \frac{f_0}{2H_1 S_{B_1}}\Big(\Delta P_{m,p_1} + \Delta P_{m,AGC_1} - \frac{1}{D_{l_1}}\Delta f_1 - P_T \sin(\Delta\phi + \phi_0) + P_{0_{12}}\Big),$$

$$\Delta \dot{f}_2 = \frac{f_0}{2H_2 S_{B_2}}\Big(\Delta P_{m,p_2} + \mathbf{u} - \frac{1}{D_{l_2}}\Delta f_2 + P_T \sin(\Delta\phi + \phi_0) - P_{0_{12}}\Big),$$

$$\Delta\dot{\phi} = 2\pi(\Delta f_1 - \Delta f_2),$$

$$\begin{aligned}\Delta \dot{P}_{AGC_1} = & \Big(\frac{1}{D_{l_1}}\frac{C_{p_1} f_0}{2S_1 H_1 S_{B_1}} - \frac{1}{S_1}\frac{1}{T_{N_1}}\Big)\Delta f_1 \\ & - \frac{C_{p_1} f_0}{2S_1 H_1 S_{B_1}}\Delta P_{m,p_1} - \frac{C_{p_1} f_0}{2S_1 H_1 S_{B_1}}\Delta P_{m,AGC_1} \\ & - \Big(\frac{1}{T_{N_1}} - \frac{C_{p_1} f_0}{2S_1 H_1 S_{B_1}}\Big)(P_T \sin(\Delta\phi + \phi_0) - P_{0_{12}}) \\ & - 2\pi C_{p_1} P_T(\Delta f_1 - \Delta f_2)\cos(\Delta\phi + \phi_0) - \frac{K_{a_1}}{T_{N_1}} p_1. \qquad (1)\end{aligned}$$

$$\dot{x} = f(x, w) + g(x, w)u$$

***u*: disturbance**

$$\Delta P_{p_i} = -1/S_i \text{ for i=1,2}$$

$$\dot{x} = f(x, w) + g(x, w)u$$

S_{B_i}	f_0	D_{l_i}	S_i	C_{p_i}	T_{N_i}
$10\ GW$	$50Hz$	$\frac{1}{200}\ MW/Hz$	$0.002Hz/MW$	0.1	30
$\Delta P^{max}_{AGC_i}$	$\Delta P^{min}_{AGC_i}$	$\Delta P^{max}_{p_i}$	$\Delta P^{min}_{p_i}$	P_T	K_a
$350MW$	$-350MW$	$75\ MW$	$-75\ MW$	$1000\ MW$	100

TABLE I

PARAMETER VALUES FOR THE TWO AREA POWER SYSTEM

$$\Delta P_{m,p_i} = \begin{cases} \Delta P^{min}_{p_i} & \text{if} \quad \Delta P_{p_i} \leq \Delta P^{min}_{p_i} \\ \Delta P_{p_i} & \text{if} \quad \Delta P^{min}_{p_i} < \Delta P_{p_i} < \Delta P^{max}_{p_i} \\ \Delta P^{max}_{p_i} & \text{if} \quad \Delta P_{p_i} \geq \Delta P^{max}_{p_i} \end{cases}$$

$$\Delta P_{m,AGC_1} = \begin{cases} \Delta P^{min}_{AGC_1} & \text{if} \quad \Delta P_{AGC_1} \leq \Delta P^{min}_{AGC_1} \\ \Delta P_{AGC_1} & \text{if} \quad \Delta P^{min}_{AGC_1} < \Delta P_{AGC_1} < \Delta P^{max}_{AGC_1} \\ \Delta P^{max}_{AGC_1} & \text{if} \quad \Delta P_{AGC_1} \geq \Delta P^{max}_{AGC_1} \end{cases}$$

$$p_1 = \begin{cases} 0 \quad \text{if} \quad \Delta P^{min}_{AGC_1} < \Delta P_{AGC_1} < \Delta P^{max}_{AGC_1} \\ \Delta P_{AGC_1} - \Delta P_{m,AGC_1} \qquad \text{else} \end{cases}$$

$$\Delta P_{12} = P_T \sin(\Delta\phi + \phi_0) - P_{0_{12}}$$

where ϕ_0 is the angle difference that corresponds to the scheduled transferred power i.e. $P_{0_{12}} = P_T \sin(\phi_0)$

Frequency Control $|\Delta f|$<1.5 Hz

Otherwise

Load shedding

Generator tripping

:

:

System Blackout

Adversary Control: Computation of optimal ***u***, such that the system's state vector to be found outside of its safe operating region (relative to its frequency)

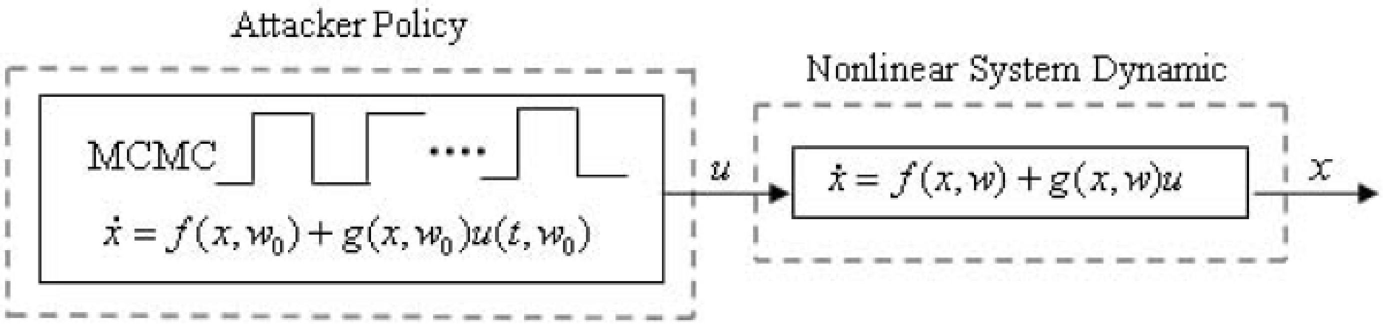
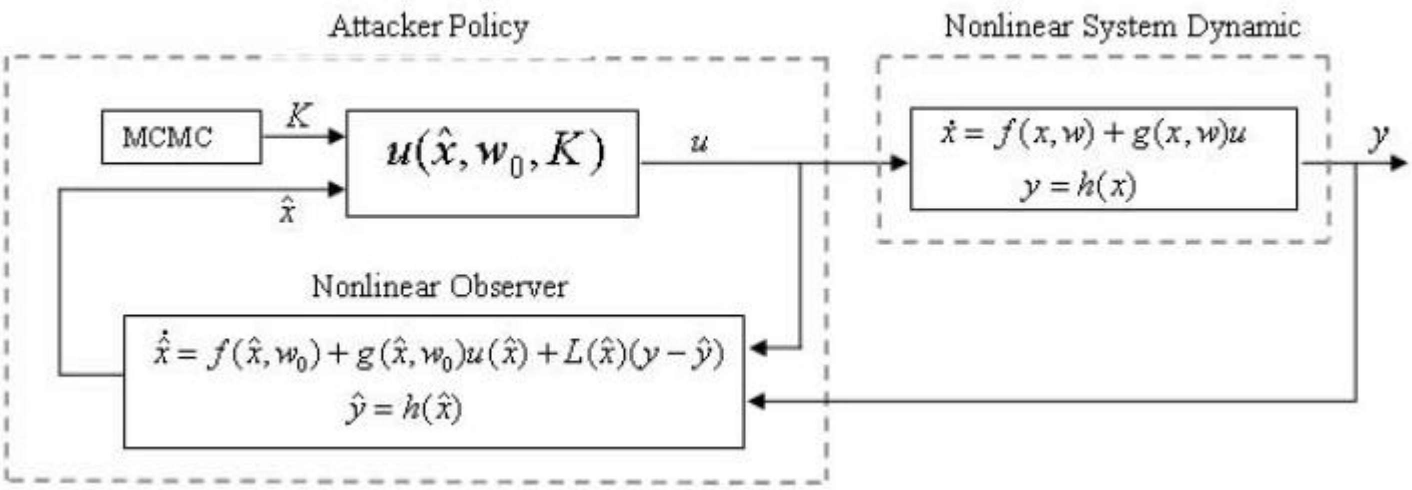


Fig. 2. Block diagram of open loop policy for the attacker



System $S: x[k+1] = Ax[k] + Bu[k], \quad x[0] = x_0,$

State Constraints $\mathcal{R}(G, w) = \{x \in \mathbb{R}^n : Gx \leq w\},$

Control $u = Kx$

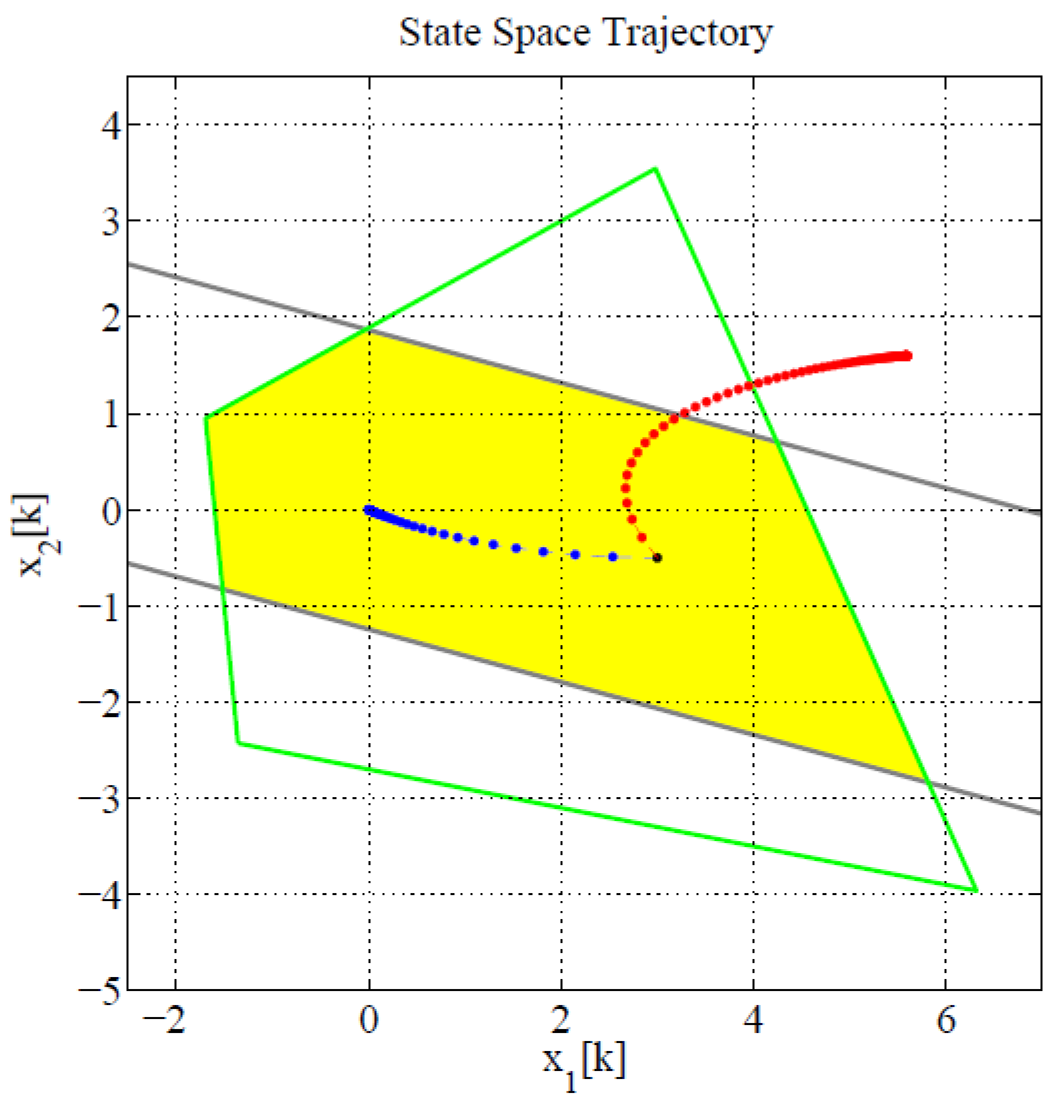
Command Constraints $\mathcal{Q}\left(K, u_{\min}, u_{\max}\right) = \left\{x \in \mathbb{R}^n : \begin{bmatrix} K \\ -K \end{bmatrix} x \leq \begin{bmatrix} u_{\max} \\ -u_{\min} \end{bmatrix}\right\}$

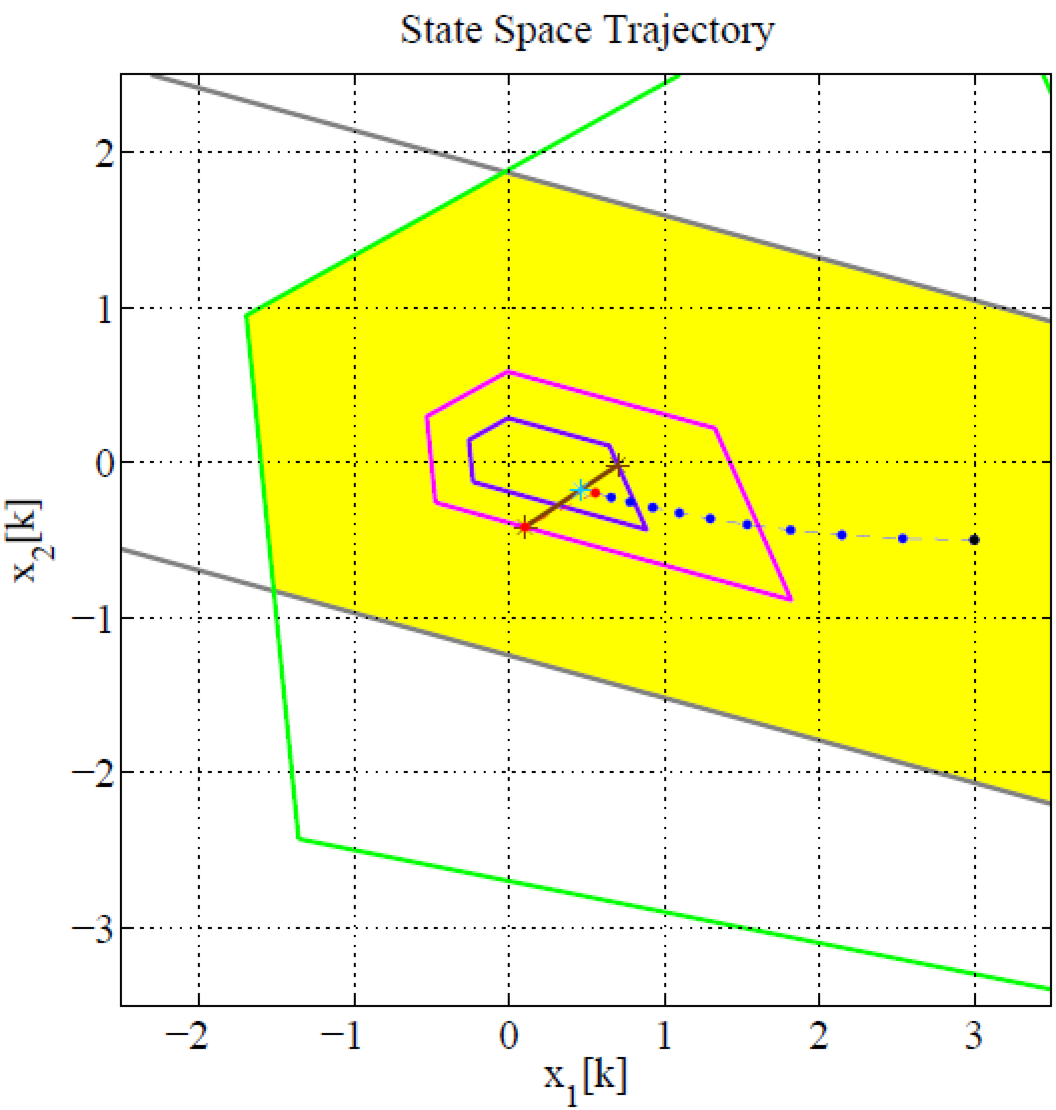
Optimal Feedback Control Objective

1) Ensure invariance of set $\mathcal{J} = \mathcal{R} \cap \mathcal{Q}$
2) Drive *x* to 0 at the fastest possible rate

Adversary Control Objective

Compute *u*: such that state vector *x* exits as fast as possible from set $\mathcal{J}$


State Space Trajectory
4
3
2
1
0
−1
−2
−3
−4
−5
−2
0
2
4
6
x2[k]
x1[k]



$V(x)$ isocontours, and adversary control command selection

Optimal Feedback Control

$$\min_{\varepsilon,K,H,M} \{\varepsilon\}, \qquad \text{subject to}$$

$$\begin{aligned} G(A+BK) &= HG \\ Hw &\leq \varepsilon w, \;\; H \in \mathbb{R}^{m\times m} \\ MG &= K, \quad Mw \leq \rho, \quad M \in \mathbb{R}^{2\times m} \\ \varepsilon &\leq 1, \;\; H \geq \mathbb{O}, M \geq \mathbb{O} \end{aligned}$$

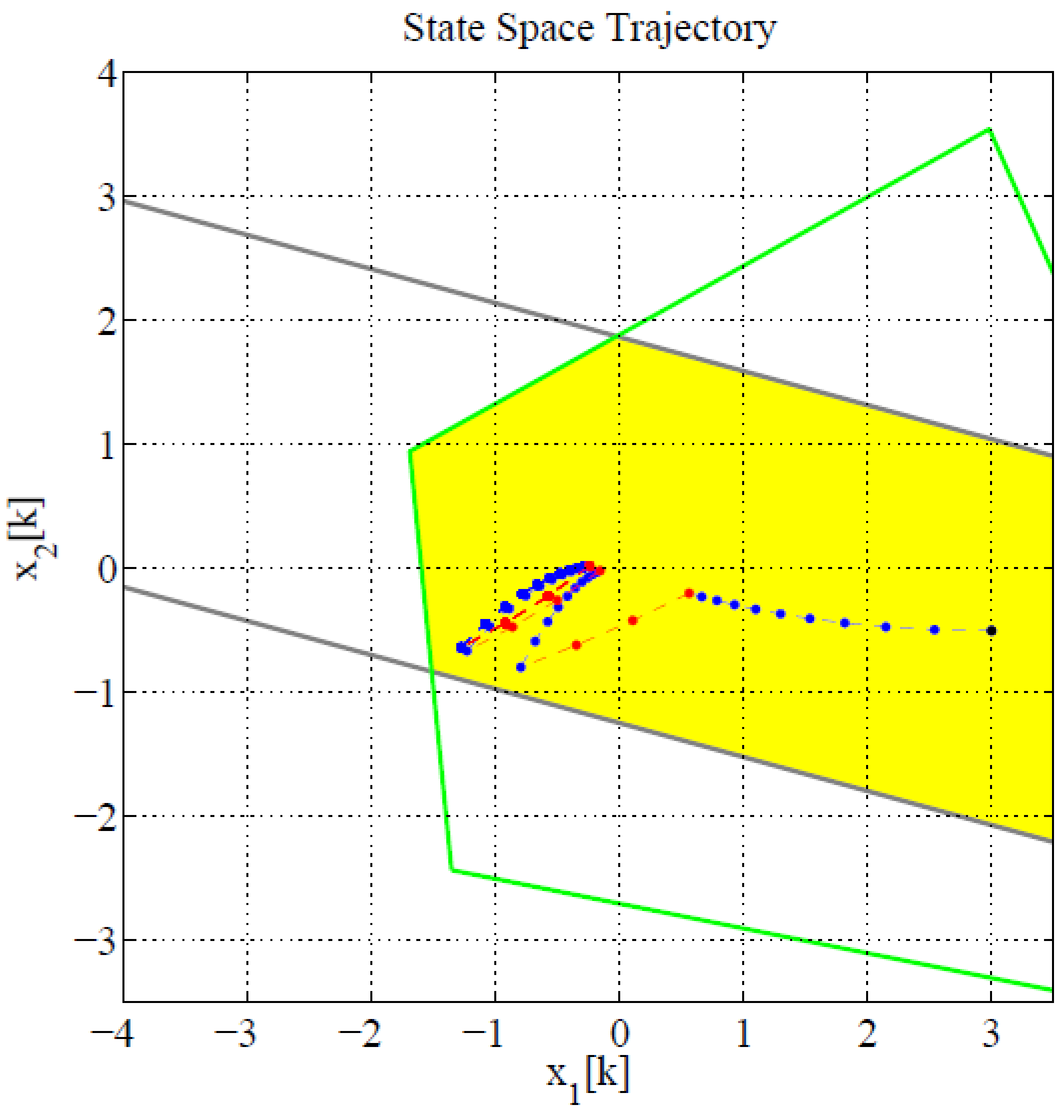
Adversary Control

$$V(x) = \max_{i=1,2,\ldots,m} \left\{ \max\left\{ \frac{(G'x)_i}{w'_i}, 0 \right\} \right\}$$

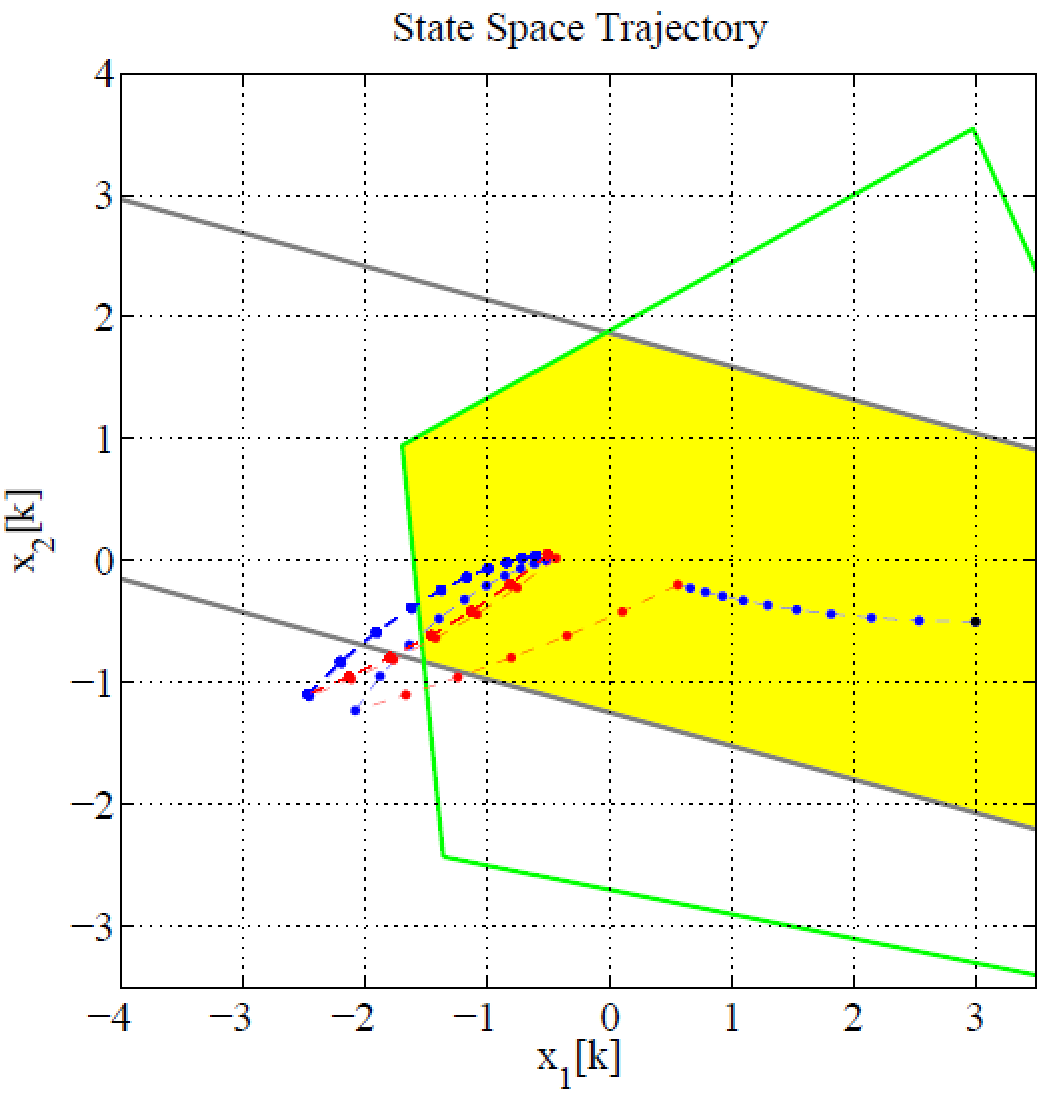
$(G'x)_i$ and w'_i denote the i-th element of vectors

$$G'x = \begin{bmatrix} G \\ K \\ -K \end{bmatrix} \text{ and } w' = \begin{bmatrix} w \\ u_{\max} \\ -u_{\min} \end{bmatrix}$$

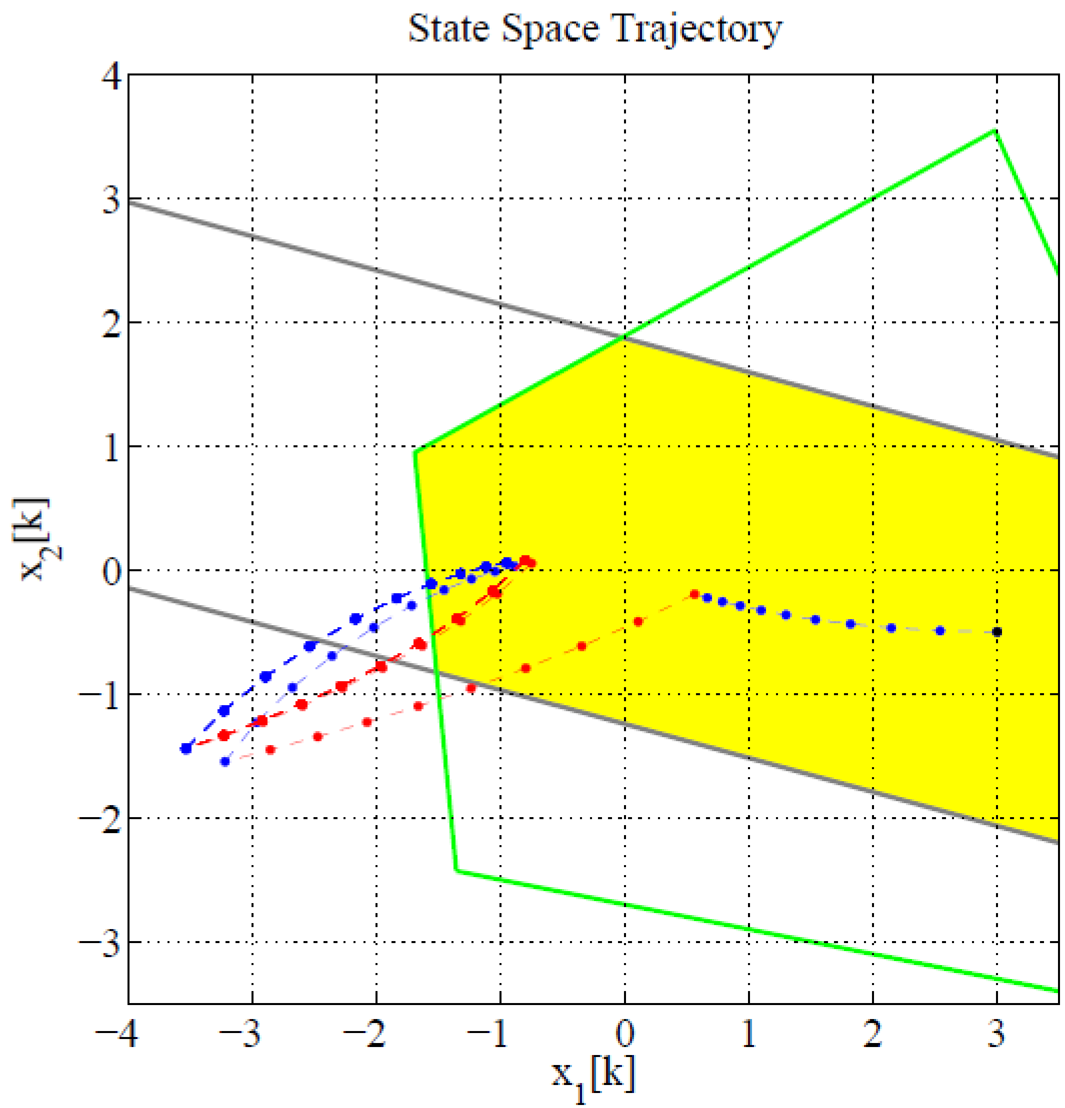
$$\begin{aligned} u_e[k] &= \arg\max_{u\in[u_{\min}, u_{\max}]} V(u[k]) \\ &= \begin{cases} u_{\min}, & \text{if } V(u_{\min}) \geq V(u_{\max}) \\ u_{\max}, & \text{if } V(u_{\min}) < V(u_{\max}) \end{cases} \end{aligned}$$



State vector behaviour for $n_c = 10$ and $n_e = 3$



State vector behaviour for $n_c = 10$ and $n_e = 6$



State vector behaviour for $n_c = 10$ and $n_e = 9$

Conclusions

If the Adversary Controller has access to:

1) **the description of the system's dynamics**
2) **the state vector measurements**
3) **the feedback control policy**
4) **the system's state and input constraints**

Then an optimum adversarial strategy was provided

Issues of future interest

1) **State vector measurement uncertainties may be used in a game-approach (between feedback and adversary control)**
2) **System Parametric Uncertainty**
3) **MIMO systems**
4) **Nonlinear systems**