Secure Control Systems: A Quantitative Risk Management Approach

Analisi e commento

Introduzione e
Reti di controllo sotto attacco

Giacomo Gaddoni

Introduzione

Le infrastrutture critiche devono poter operare in sicurezza anche a fronte di eventuali disturbi esterni. Si tratta in genere di sistemi distribuiti, ricchi di sensori e ricevitori che comunicano tramite sistemi informatici.

1. **Sicurezza rispetto ai disturbi**: tipicamente attenuati grazie alla teoria del controllo, si tratta di disturbi casuali provenienti dall'ambiente
2. **Sicurezza da attacchi coordinati**: più complessi, poiché con l'intento di rovinare il funzionamento del sistema, spesso con l'ingresso coordinato in più punti

Alcuni esempi includono: Reti di potenza elettrica. processi industriali, reti di trasporto intelligenti e altro...

Sistemi di controllo a rete, sotto attacco

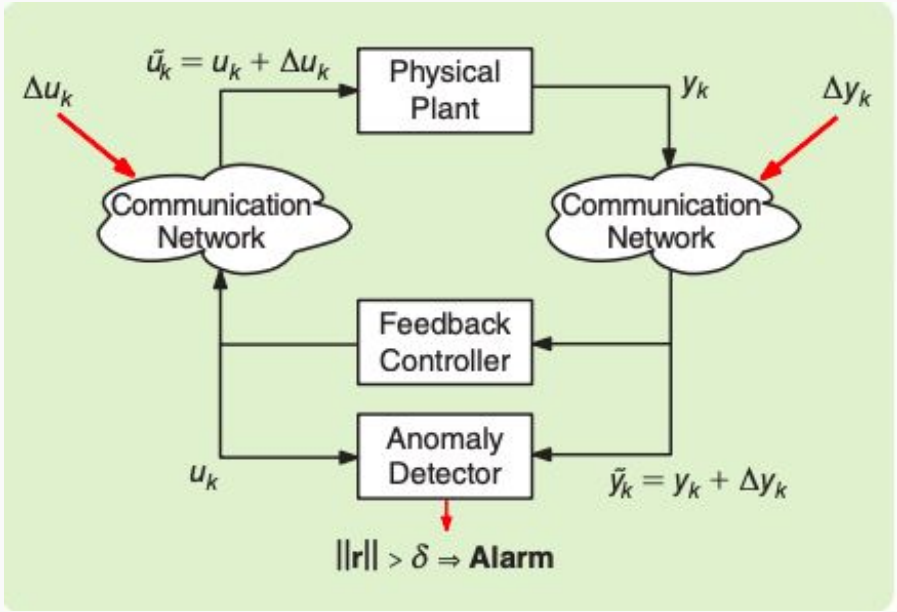
Un tipico sistema di controllo a network presenta 4 oggetti:

I. Sistema fisico
II. Rete di comunicazione
III. Retroazione di controllo digitale
IV. Rilevatore di anomalie digitale

u_k : segnale di controllo
y_k : segnale misurato
Δy_k Δu_k : disturbi esterni

Sistema nello spazio degli stati

$$\begin{cases} x_{k+1} = f_x(x_k, \tilde{u}_k, d_k), \\ y_k = g_x(x_k, \tilde{u}_k, d_k), \end{cases}$$



Definizioni utili

Comportamento nominale: avviene quando ũ = u, y˜ = y, d=0, quindi quando il sistema risulta non disturbato da attacchi maligni esterni, in caso contrario parliamo di **comportamento anormale**

Sistema sicuro: Definito un set di stati accettabili S, il sistema è detto sicuro se la sua traiettoria rimane all'interno di S

$$\begin{cases} z_{k+1} = f_z(z_k, \tilde{y}_k), \\ u_k = g_z(z_k, \tilde{y}_k), \end{cases}$$

Feedback controller

$$\begin{cases} s_{k+1} = f_s(s_k, u_k, \tilde{y}_{k+1}), \\ r_k = g_s(s_k, u_k, \tilde{y}_{k+1}), \end{cases}$$

Anomaly detector

$$\| \mathbf{r} \|_p \triangleq \left(\sum_{i=1}^{(k_f - k_0 + 1)n_r} |r_i|^p \right)^{\frac{1}{p}} > \delta,$$

Norma-lp del residuo

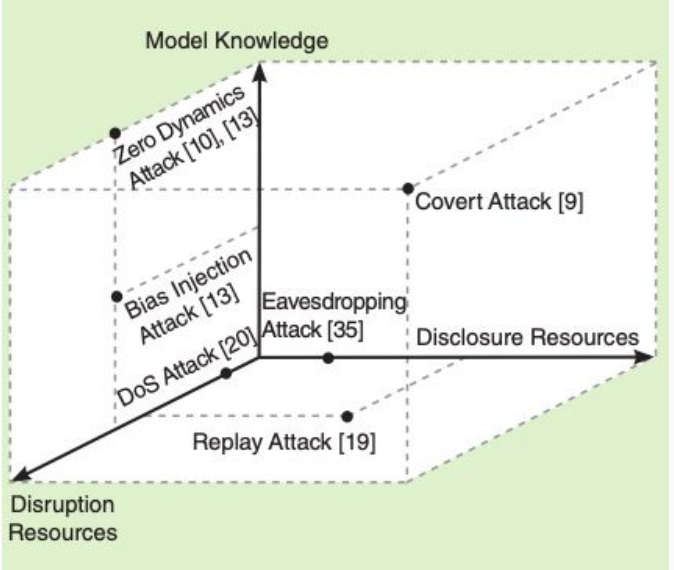
Adversary model

Disclosure attack: permettono all'avversario di estrapolare dati conoscendo le sequenze u e y del sistema. Sono molto difficili da rilevare

Deception attack: introducono variazioni nei vettori u e y con il seguente modello

$$\tilde{u}_k \triangleq u_k + \Delta u_k,$$
$$\tilde{y}_k \triangleq y_k + \Delta y_k,$$

Denial-of-service attack: bloccano la comunicazione tra nodi del sistema



Adversary model

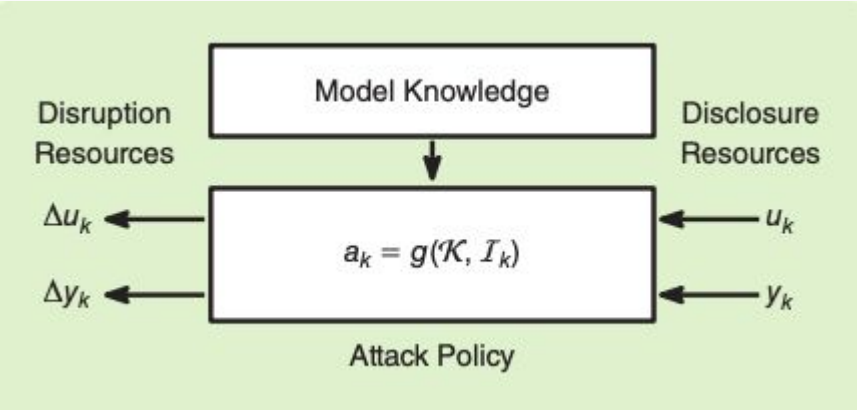
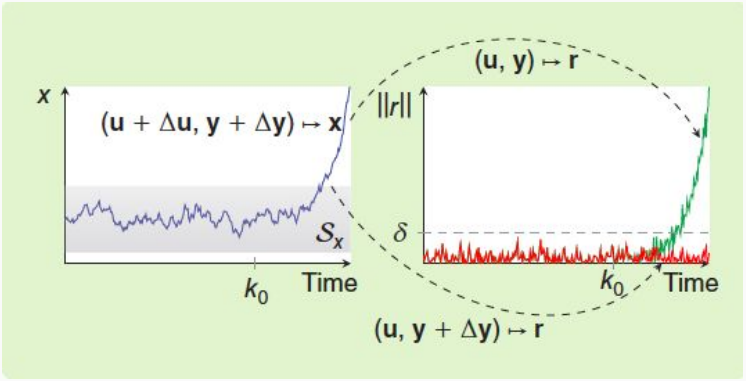


Diagramma del modello avversario:
K conoscenza già posseduta dall'avversario
I sono informazioni ottenute dai sensori
A è l'attack vector risultante

Si considera come interesse principale dell'avversario, quello di riuscire a portare lo stato del sistema in un set non sicuro rimanendo nascosto. Questa è quindi un metodo per misurare l'efficacia di un attacco.



Metodologia di Difesa

È importante minimizzare il rischio di attacco.
Il rischio è definito tramite la tripla Rischio={(Scenario, Impatto, Probabilità)}.
Il rischio si può riassumere in una matrice bidimensionale e il suo ciclo si divide in:
Analisi: identificazione delle minacce e quanto impattano sul sistema
Trattamento: gestione della minaccia
Monitoraggio: controllo a posteriori della minaccia
Ci sono metodi qualitativi e quantitativi anche basati su simulazioni per capire l'importanza e l'incidenza del rischio

Strategie difensive

Le differenti azioni possono essere classificate come:

Prevenzione: cercando di minimizzare la probabilità di minaccia aumentando la sicurezza generale del sistema (firewalls, encrypting, …)

Rivelazione: si cerca di tenere costantemente controllato il sistema per identificare un attacco il prima possibile

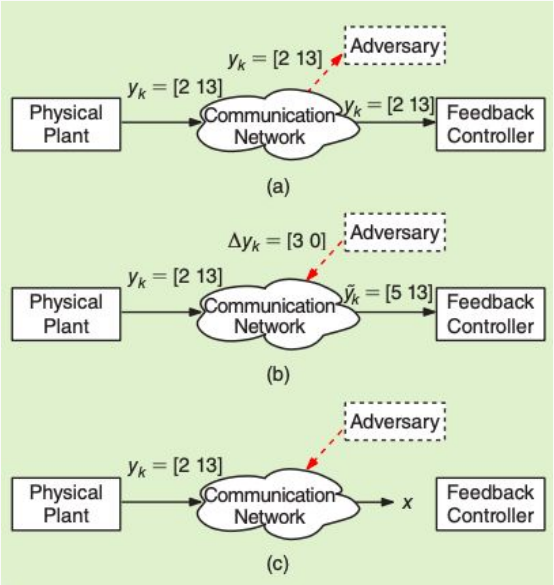
Mitigazione: eliminazione della minaccia, in genere sostituendo i componenti compromessi

CIA in Network Control System

Ci sono tre proprietà fondamentali in ambito di trasmissione di informazioni: confidentiality, integrity, and availability (CIA). Il fatto che i dati siano disponibili solo a determinati agenti, siano corretti e rimangano usufruibili per un tempo ben preciso.

Ognuna delle tre tipologie di attacco viste in precedenza mira a far cadere uno dei tre parametri della CIA.

Inoltre in scienze informatiche in genere questo genere di attacchi va solo a modificare dati, in questo caso invece, poiché si parla di controllo, sia hanno veri a propri effetti anche sul sistema fisico esterno.



Analisi del rischio

Kevin Michael Frick

Attacchi nascosti

- Modifica di dati e stato non sicuro
- Desiderata minima variazione dell’output -> risorse limitate

Modello utilizzato

- Sistema in esame, controllore di retroazione e rilevatore di anomalie sono SLTI
- Primo modello: caso statico semplificato (generatore di energia)
- Secondo modello: caso dinamico (quattro sistemi connessi: quadruple-tank process)

Caso statico - Minacce

- Probabilità minaccia := minimo sensori compromessi necessario al rilevamento
- lp: vettore degli stati costante
- lp: no controllore di retroazione
- Modello := relazione tra stati della macchina e misurazioni del rilevatore di anomalie
- Attacchi con la stessa matrice dei pesi del sistema non generano differenze nelle uscite distinguibili dal rumore

Caso statico - Indici di sicurezza

- Modello valutazione rischio: $\tilde{y} = C_y x + \Delta y$
- Attacco nascosto: $\Delta y = C_y \Delta x$
- Indice di sicurezza: $\alpha_j = \min_{\Delta x \in \mathbb{R}^n} \|C_y \Delta x\|_0$
- Il calcolo dell'indice è un problema NP-hard
- Indice di sicurezza basso ⇔ vulnerabilità

Caso statico - Metodo *big M*

- Ricerca di $\min_{\mathbf{w},\Delta x} : C_y \Delta x \in [-Mw, Mw])$
- Cond: $\mathbf{w}(i) \in \{0, 1\}$
- Cond: $(C_y)_{j,*}\Delta x = 1$ (più stringente di $(C_y)_{j,*}\Delta x \neq 0$)
- Soluzione ottimale per $M > \max_i (C_y \Delta x)_i$
- Problema MILP

Esempio statico - *Standard minimum cut*

- Problema: partizionare un grafo non diretto in due parti, una contenente un nodo *s* e l'altra contenente un nodo *t*, minimizzando il costo totale del taglio degli archi
- Un grafo con n nodi ha (al più) n(n - 1) / 2 possibili *min cut*
- Esistono algoritmi diretti (e.g. programmazione lineare)
- Problema duale: *network flow*

Esempio statico - *Network flow* (approfondimento)

- Problema: in un grafo non diretto nel quale gli archi hanno una *capacità* ben definita trovare il *flusso* massimo da un nodo *s* a un nodo *t*
- Duale dello SMCP: il percorso con flusso massimo è composto dagli archi da tagliare per ottenere una partizione s-t minima
- Algoritmo *Ford-Fulkerson* (O(Mf))
  - Per ogni cammino da s a t, riempirlo con il flusso massimo fino al collo di bottiglia
  - Una volta terminati i cammini disponibili, il flusso che arriva a *t* è il massimo possibile

Power trasmission network

Le reti di trasmissione elettrica sono sistemi complessi e spazialmente distribuiti.

Aspetti importanti:

Sistemi SCADA: Sistemi informatici distribuiti per il monitoraggio e la supervisione dei sistemi fisici

RTU: Unità terminali remote

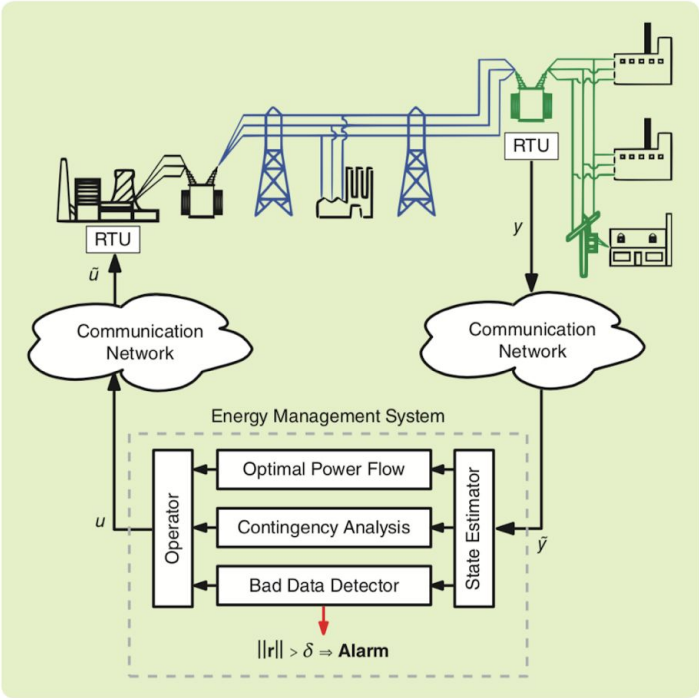
EMS: Sistemi di gestione dell'energia

Il comportamento del sistema è quasi-statico.

Un sistema si dice statico se il legame ingresso-uscita è istantaneo.

$$y(t) = g(u(t)) \quad \forall t$$

Vulnerabilità: manomissione RTU, canali di comunicazione RTU-centro di controllo, EMS, database del centro di controllo



DC power flow measurament model

Per l'analisi della sicurezza cyber-fisica è consuetudine descrivere la dipendenza delle grandezze della rete elettrica attraverso un modello approssimato chiamato DC power flow measurement model.

La struttura:

n+1 bus

L reti di trasmissione elettrica

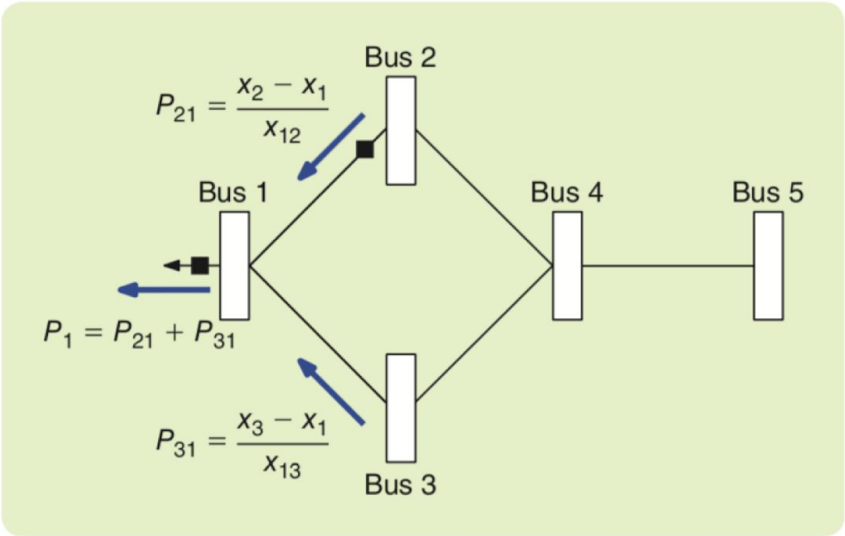
Lo stato del sistema è dato dal $2n + 2$-vettore:

$$(x_0, \dots, x_n, V_0, \dots, V_n)$$

dove x_i, V_i rappresentano rispettivamente l'angolo di fase ed il modulo del voltaggio complesso presso il bus i

Ai fini della trattazione è lecito assumere $V_i = 1 \; \forall i = 1, \dots, n$

Il modello sarà dunque in funzione dei soli $x_0, \dots, x_n$



Secure Control System

A QUANTITATIVE RISK MANAGEMENT APPROACH di A. Marini

DC power flow measurament model

Per l'analisi della sicurezza cyber-fisica è consuetudine descrivere la dipendenza delle grandezze della rete elettrica attraverso un modello approssimato chiamato DC power flow measurement model.

In questo modello il flusso di corrente dal bus *i* al bus *j* sarà:

$$P_{ij} = \frac{x_{ij}}{X_{ij}}$$

con $x_{ij} := x_i - x_j$ e X_{ij} la reattanza della linea che connette il bus *i* al bus *j*.

Con $P_i = \sum_{j \in N_i} P_{ij}$ indichiamo l'iniezione di corrente al bus *i* dove N_i è l'insieme degli indici dei bus vicini al bus *i*

$$y = \begin{bmatrix} T_l D \mathcal{A}^\top x \\ T_i \mathcal{A}_0 D \mathcal{A}^\top x \end{bmatrix} =: C_y x$$

Denotiamo con $\boldsymbol{x = (x_1, \dots, x_n)}$ il vettore degli angoli di fase del voltaggio su tutti i bus eccetto il bus di riferimento.

Il bus di riferimento è arbitrariamente definito, con angolo di fase del voltaggio fissato a 0.

Sia $\boldsymbol{y}$ il vettore dei flussi di energia e delle misurazione di iniezioni di energia.

$$\mathcal{A}_0(i,l) = \begin{cases} 1 & \text{line } l \text{ starts from bus } i, \\ -1 & \text{line } l \text{ ends at bus } i, \\ 0 & \text{otherwise,} \end{cases} \quad \text{for each transmission line } l.$$

$\boldsymbol{A_0}$ matrice di incidenza, $\boldsymbol{A}$ matrice di incidenza senza la riga inerente al bus di riferimento, $\boldsymbol{D}$ matrice diagonale degli inversi delle reattanze. Le matrici $\boldsymbol{T_l}$ e $\boldsymbol{T_i}$ indicano quali valori sono in realtà misurati.

DC power flow measurament model

Per l'analisi della sicurezza cyber-fisica è consuetudine descrivere la dipendenza delle grandezze della rete elettrica attraverso un modello approssimato chiamato DC power flow measurement model.

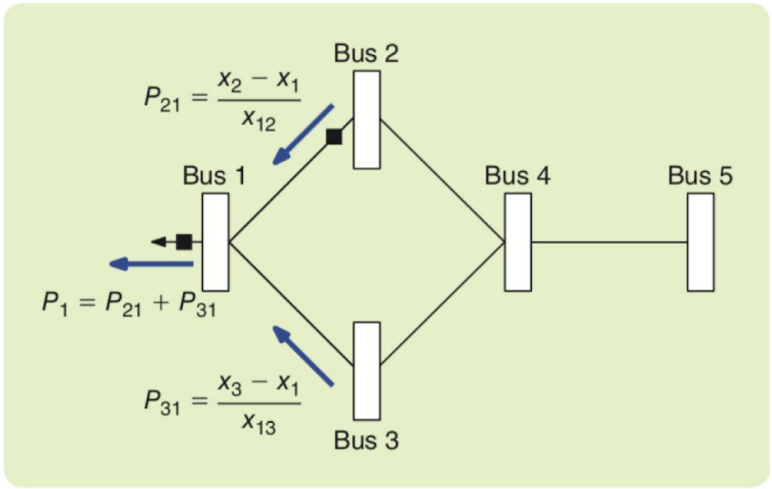
1. Un particolare $\boldsymbol{x}$ corrisponde ad un'assegnazione degli angoli di fase presso i bus.

2. Le differenze degli angoli di fase tra due bus vicini induce un flusso di energia lungo la linea connettente.

Il vettore del flusso di energia della linea indotto è descritto da $D\mathcal{A}^\top x$

3. Ad ogni bus, una differenza tra i flussi di energia della linea entranti ed uscenti deve essere bilanciato da un'iniezione esterna di energia o da un'estrazione.

Il vettore dell'iniezione esterna di energia presso i bus è descritta da $\mathcal{A}_0 D\mathcal{A}^\top x$



Standard minimum cut problem

Un problema standard di taglio minimo su un grafo non orientato è un problema di ottimizzazione.

Partizionare in due insiemi contenenti s e t

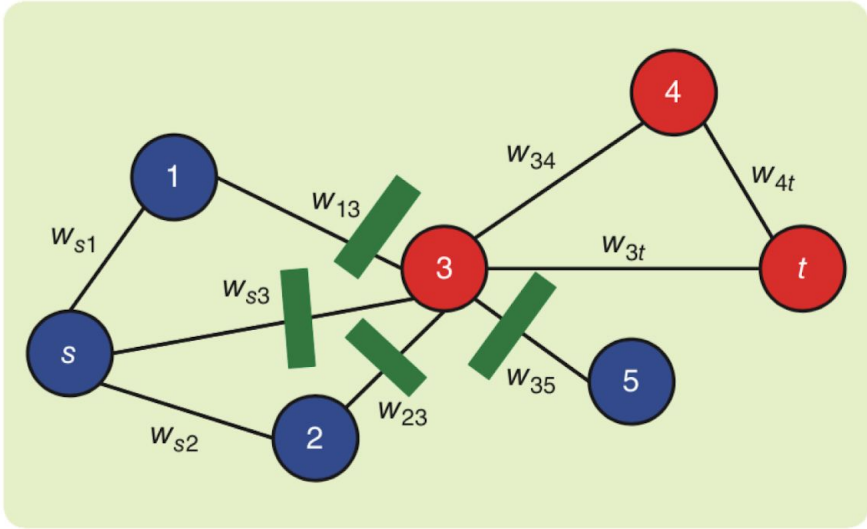
La somma degli **spigoli tagliati** deve essere **minima**.

Uno **spigolo** si dice **tagliato** se esso connette due nodi uno dei quali appartiene al blocco della partizione contenente s e l'altro al blocco contenente t

Se consideriamo il grafo in figura come una rete di energia elettrica con s generatore e t richiedente.

Se tutti i pesi degli spigoli sono unitari, allora la soluzione al problema del taglio minimo specifica il **numero minimo di linee di trasmissione da rompere per causare un'interruzione della fornitura dell'energia.**

Algoritmi efficienti sono **disponibili** per **risolvere il problema standard del taglio minimo** con sforzo computazionale proporzionale ad una funzione polinomiale della dimensione del problema.



Grafo non orientato con nodi source s, sink t e pesi non negativi w_{ij} tra ogni nodo i e j.

Secure Control System

A QUANTITATIVE RISK MANAGEMENT APPROACH di A. Marini

Il problema dell'indice di sicurezza

Nel contesto corrente il problema dell'indice di sicurezza (8) dovrebbe essere interpretato con la matrice delle misurazioni C_y ristretta alla forma in (15).

Il vettore Δx può essere considerato come un assegnamento fittizio di angoli di fase.

L'obiettivo è di minimizzare $\|C_y \Delta x\|_0$, ossia la somma del numero di linee con flussi non nulli e di bus con iniezioni non nulle.

Assunzione di piena misurazione:

T_l e T_i sono matrici identità di appropriate dimensioni

Assegnazione di Δx utilizzando solo due valori distinti (e.g. 0 e 1)

(16)
$$\begin{aligned} \underset{\Delta x \in \{0,1\}^n}{\text{minimize}} \quad & \| C_y \Delta x \|_0 \\ \text{subject to} \quad & C_y(j,:)\Delta x \neq 0. \end{aligned}$$

Con le soprastanti assunzioni, il problema non è più NP-hard

L'assegnazione 0-1 delle entrate di Δx porta con se un'interpretazione grafica del problema.

La scelta binaria delle entrate di Δx definisce un partizionamento dei bus in due insiemi disgiunti: un insieme con bus con angolo di fase nullo ed il suo complementare.

Una linea che connette due bus in due insiemi differenti è tagliata.

L'obiettivo è di minimizzare la somma dei numeri delle linee tagliate con misuratori di flusso di energia ed il numero di bus che hanno rilevatori di iniezione e sono incidenti alla linea tagliata.

Come risultato, (16) può essere interpretato come una generalizzazione del problema standard di minimo taglio.

(8)
$$\begin{aligned} \alpha_j \triangleq \min_{\Delta x \in \mathbb{R}^n} \quad & \| C_y \Delta x \|_0 \\ \text{subject to} \quad & C_y(j,:)\Delta x \neq 0, \end{aligned}$$

(15)
$$y = \begin{bmatrix} T_l D \mathcal{A}^\top x \\ T_i \mathcal{A}_0 D \mathcal{A}^\top x \end{bmatrix} =: C_y x$$

Crittografia

Andrea Pari

Gestione del rischio nel caso di “stealthy deception attacks”

Crittografia dei dati e dei canali di trasmissione dei dati.

Può essere, però, dispendiosa dal punto di vista computazionale in particolare nel caso di equipaggiamento obsoleto.

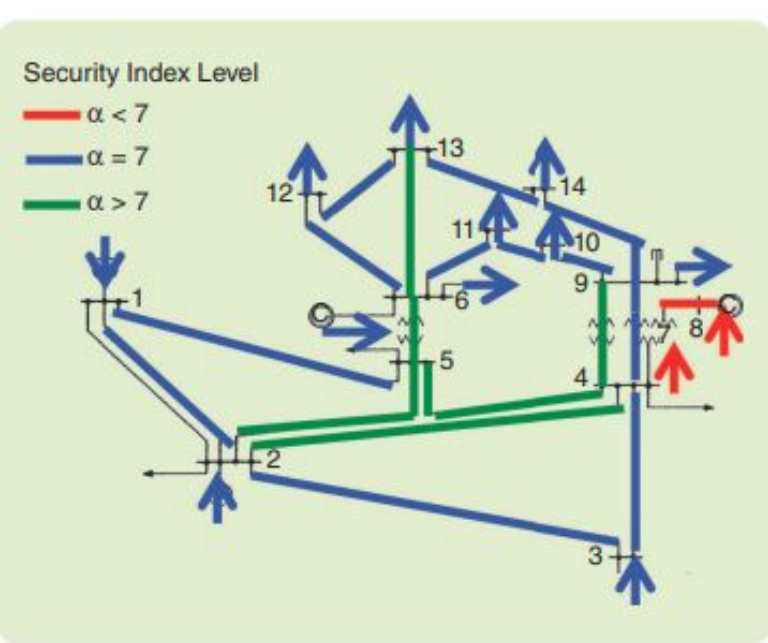
Viene crittogafata solo una parte dei dati

Quali dati crittografare per massimizzare la protezione delle risorse ?

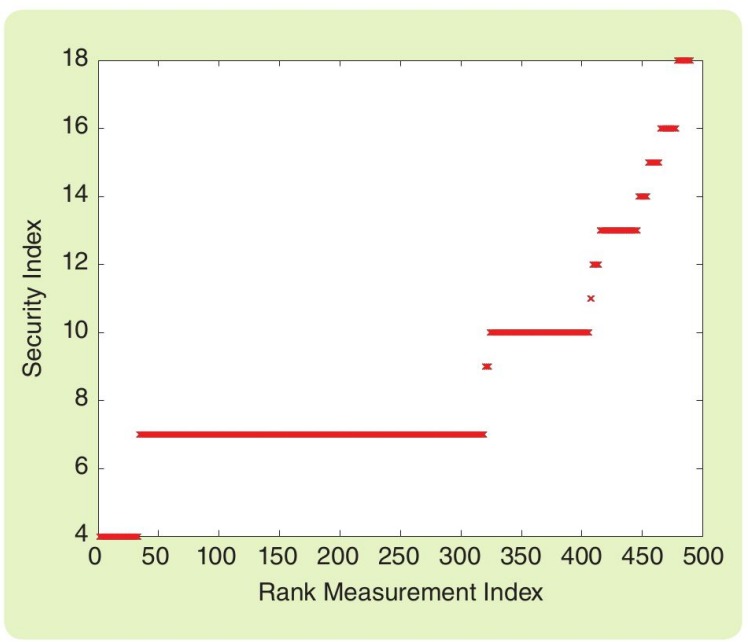
- Misura degli indici di sicurezza
- Valutazione delle strategie di protezione

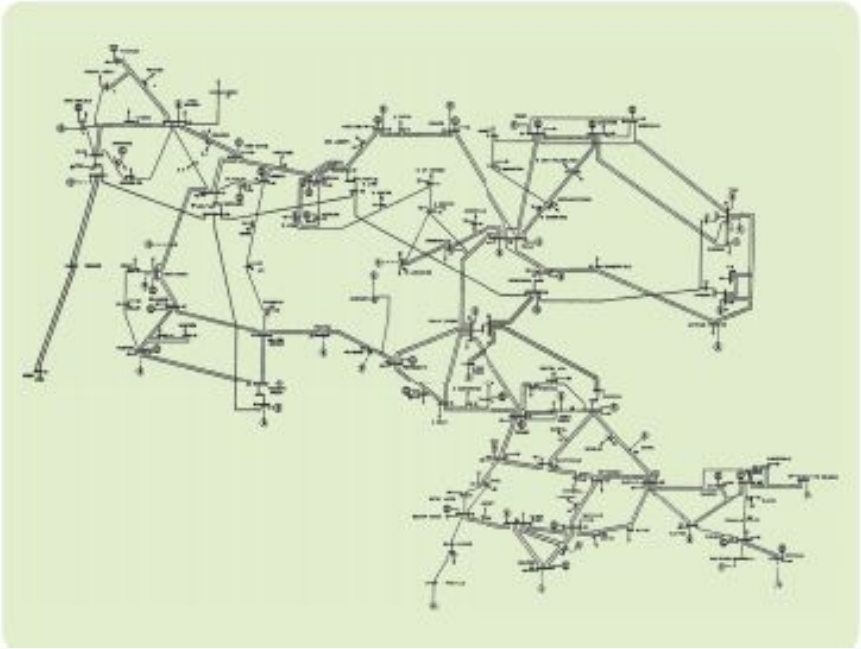
$$\begin{aligned} \underset{\Delta x \in \mathbb{R}^n}{\text{minimize}} \quad & \| C_y \Delta x \|_0 \\ \text{subject to} \quad & C_y(j,:)\,\Delta x \neq 0, \\ & C_y(P,:)\,\Delta x = 0, \end{aligned}$$

Esempio: IEEE 14-BUS



Esempio IEEE 118-bus





Problema degli indici di sicurezza

All’aumentare della complessità del sistema, il calcolo delle strategie per massimizzare la sicurezza richiede sempre più tempo e potenza di calcolo.

Procedure per ottimizzare la computazione del problema:

- Minimum cut based procedure
- Big M method

Analisi dei rischi nei sistemi dinamici

Obiettivo dell' avversario: perturbare il sistema di controllo e portare il sistema a uno stato non sicuro.

$$\mathcal{S}_x \triangleq \{\mathbf{x}: \| \mathbf{x} \|_p < \delta\}$$

x rappresenta la traiettoria dello stato
$||x||_p$ quantifica l'attacco

Analisi dei rischi nei sistemi dinamici

u_k : segnale di controllo
y_k : segnale misurato
Δy_k Δu_k : disturbi esterni

$$h_p(\mathbf{a}) \triangleq [\| \mathbf{a}_{(1)} \|_p \dots \| \mathbf{a}_{(n_a)} \|_p]^\top$$

Il numero di risorse usate per un attacco e` uguale al numero di elementi non nulli del vettore h_p

1. Poiché delta y è diverso da zero, l'avversario deve avere accesso ad un canale di comunicazione per iniettare dati corrotti. Corrompe il segnale misurato più volte non richiede risorse aggiuntive da parte dell' avversario.

$$\Delta y_k \neq 0$$

$$\Delta u_k \neq 0$$

2. Corrompere il segnale di controllo al tempo k richiede risorse aggiuntive, ovvero l'accesso al segnale di controllo.

$$\Delta y_k \neq 0$$

Maximum impact, minimum resource attack

$$
\begin{aligned}
\underset{\mathbf{a}}{\text{maximize}} \quad & \| \mathbf{x} \|_p \\
\text{subject to} \quad & \| \mathbf{r} \|_q \leq \delta, \\
& \| h_p(\mathbf{a}) \|_0 < \epsilon, \\
& \mathbf{n} = \mathcal{O}\eta_0 + \mathcal{T}\mathbf{a}, \\
& \mathbf{x} = \mathcal{C}_x \mathbf{n}, \\
& \mathbf{r} = \mathcal{C}_r \mathbf{n} + \mathcal{D}_r \mathbf{a}
\end{aligned}
$$

Esempio dinamico

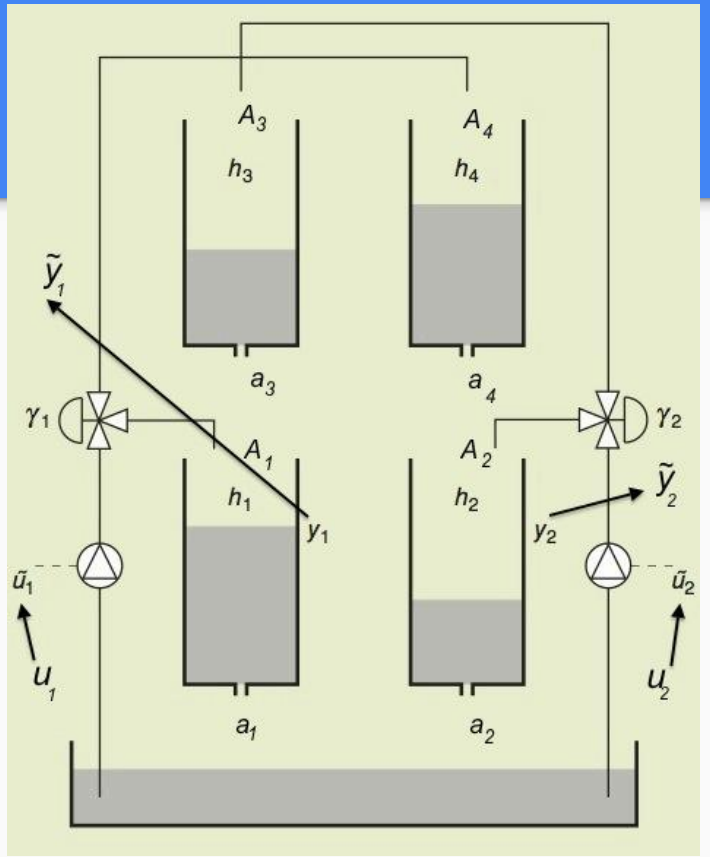
Lorenzo Obersnel

Esempio dinamico
Quadruple-tank process

- y_1 e y_2 sono le misurazioni dei livelli nei serbatoi inferiori
- u_1 e u_2 sono i segnali mandati alle pompe

- I dati trasmessi possono essere corrotti:

  Δy_1+y_1 Δy_2+y_2 Δu_1+u_1 Δu_2+u_2



Modello

$$\frac{dh_1}{dt} = -\frac{a_1}{A_1}\sqrt{2gh_1} + \frac{a_3}{A_1}\sqrt{2gh_3} + \frac{\gamma_1 k_1}{A_1}u_1,$$

$$\frac{dh_2}{dt} = -\frac{a_2}{A_2}\sqrt{2gh_2} + \frac{a_4}{A_2}\sqrt{2gh_4} + \frac{\gamma_2 k_2}{A_2}u_2,$$

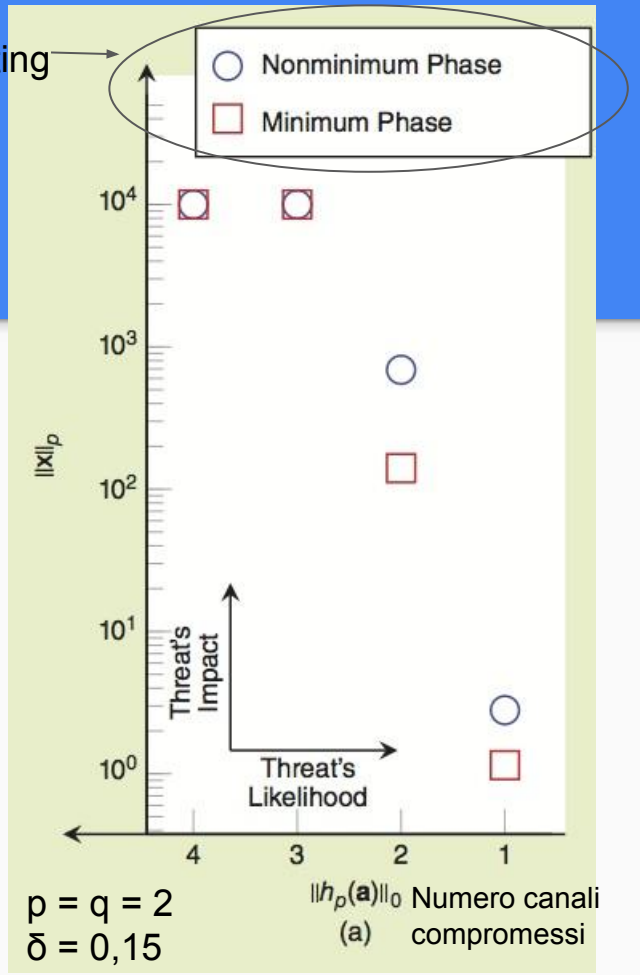
$$\frac{dh_3}{dt} = -\frac{a_3}{A_3}\sqrt{2gh_3} + \frac{(1-\gamma_2)k_2}{A_3}u_2,$$

$$\frac{dh_4}{dt} = -\frac{a_4}{A_4}\sqrt{2gh_4} + \frac{(1-\gamma_1)k_1}{A_4}u_1,$$

- Centralized linear-quadratic-Gaussian controller
- Minimum e Nonminimum phase
- Safe set: $S_x = \{x: ||x||_\infty <= 5\}$
- Kalman filter based anomaly detector
- maximum-impact resource-constrained attack

Risk analysis: Stealthy Deception Attack

Process setting



p = q = 2

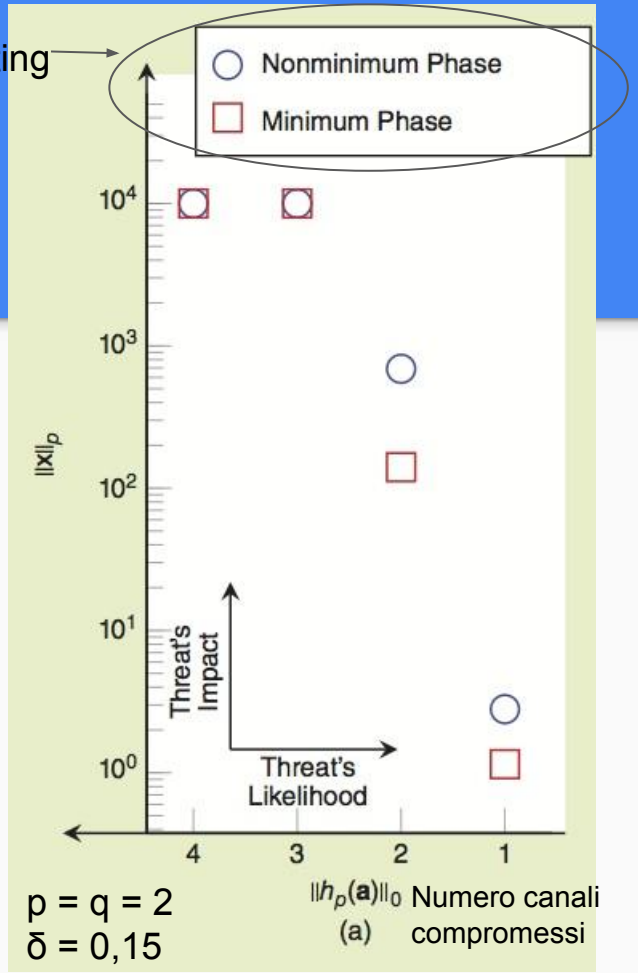
δ = 0,15

Risk analysis: Stealthy Deception Attack

TABLE 1 Risk analysis results for the quadruple-tank process. Each entry corresponds to the maximum impact $\|x\|_p$ for a given number of corrupted channels, computed through (20), with $p=q=2$ and $\delta=0.15$.

	Number of Compromised Channels			
	4	3	2	1
Minimum phase	∞	∞	140.39	1.15
Nonminimum phase	∞	∞	689.43	2.8

Process setting



p = q = 2

δ = 0,15

Numero canali compromessi

Trattamento del rischio

- Studia quali canali è più importante proteggere
- Canali protetti con crittografia

Il vettore di attacco per i canali criptati è nullo

Trattamento del rischio

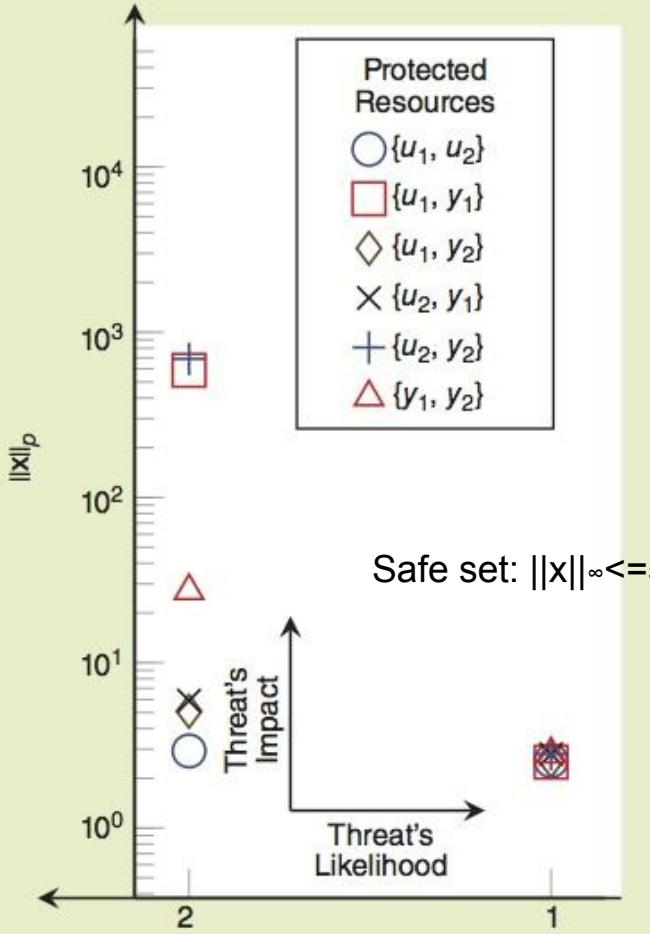
- Studia quali canali è più importante proteggere
- Canali protetti con crittografia

Il vettore di attacco per i canali criptati è nullo

$$\begin{aligned} \underset{a}{\text{Maximize}} \quad & \|x\|_p \\ \text{subject to} \quad & \|r\|_p <= \delta \\ & \|h_p(a)\|_0 < \varepsilon \\ & \underline{n} = O_{\eta 0} + T\underline{a} \\ & \underline{x} = C_x \underline{n} \\ & \underline{r} = C_r \underline{n} + D_r \underline{a} \\ & \underline{a}_i = 0, \ \forall \ i \in P \end{aligned}$$

Risultati dell’analisi

- Effetti più bassi proteggendo u_1 *e* u_2
- No impatto diretto, ma solo attraverso il feedback

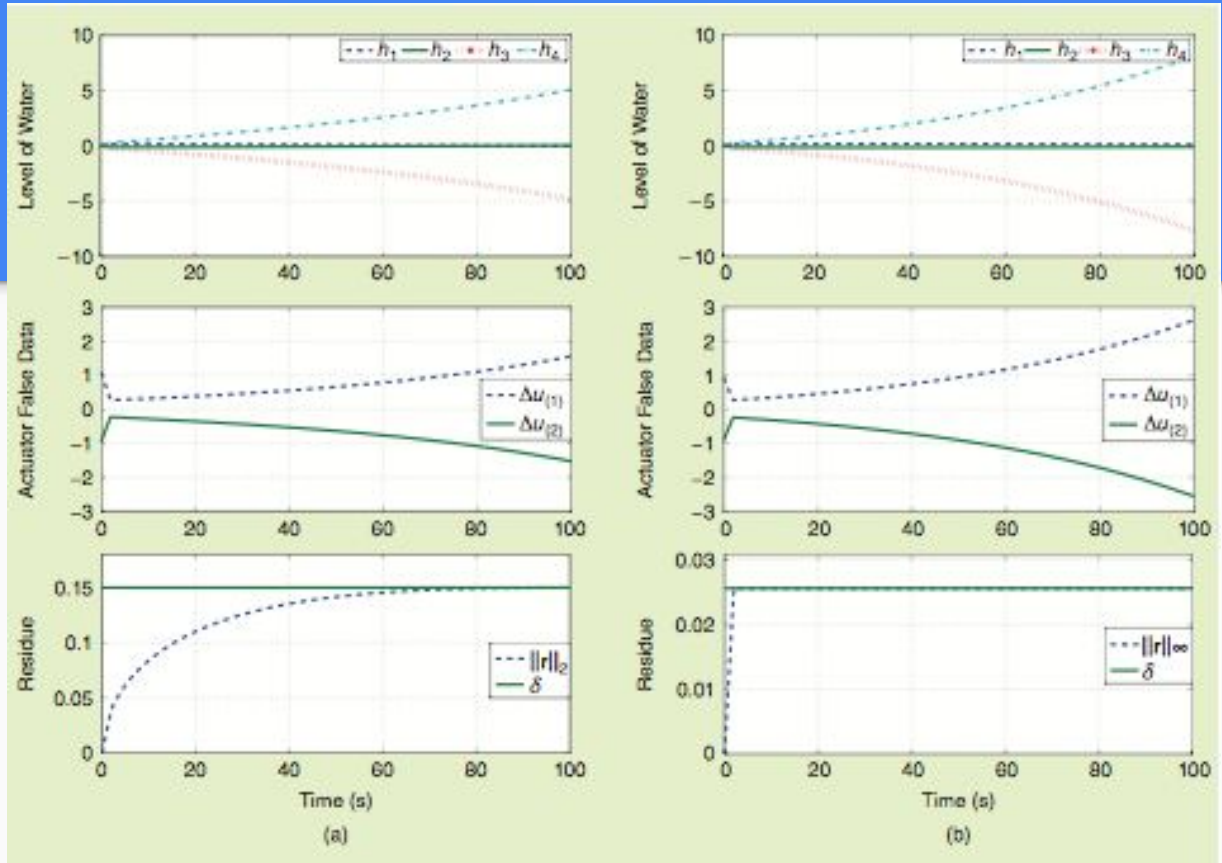


p = q = ∞
δ = 0,025

Numero canali compromessi

Simulazione: risultati

http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-96745



Immagini da:

A. Teixeira, K. C. Sou, H. Sandberg and K. H. Johansson, "Secure Control Systems: A Quantitative Risk Management Approach," in IEEE Control Systems Magazine, vol. 35, no. 1, pp. 24-45, Feb. 2015.

doi: 10.1109/MCS.2014.2364709

keywords: {control engineering computing;digital control;networked control systems;risk management;security of data;secure control system;quantitative risk management approach;critical infrastructure;digital controllers;information technology;IT infrastructure;networked control systems;Networked control systems;Computer crime;Communication networks;Detectors;Risk management;Power systems planning;Computer security},

URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7011201&isnumber=7011167

return 0;

Antonio Marini
Andrea Pari
Giacomo Gaddoni
Kevin Michael Frick
Lorenzo Obersnel

Collegio Superiore dell'Università di Bologna