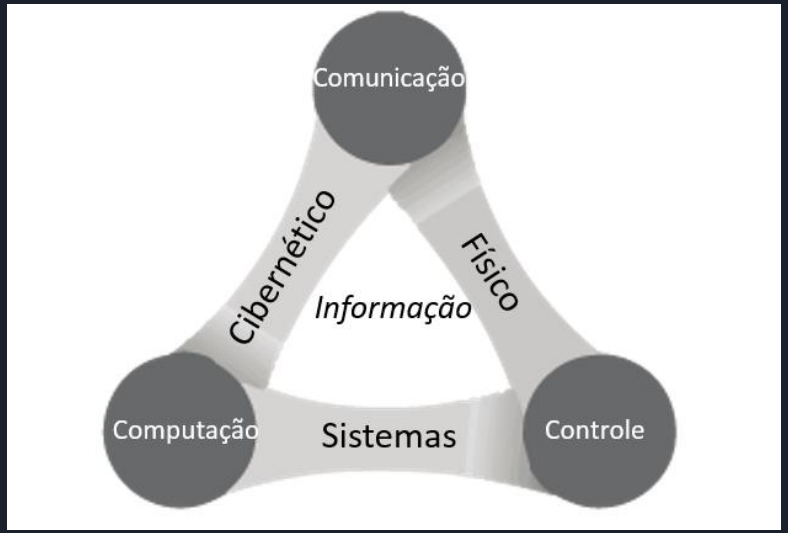
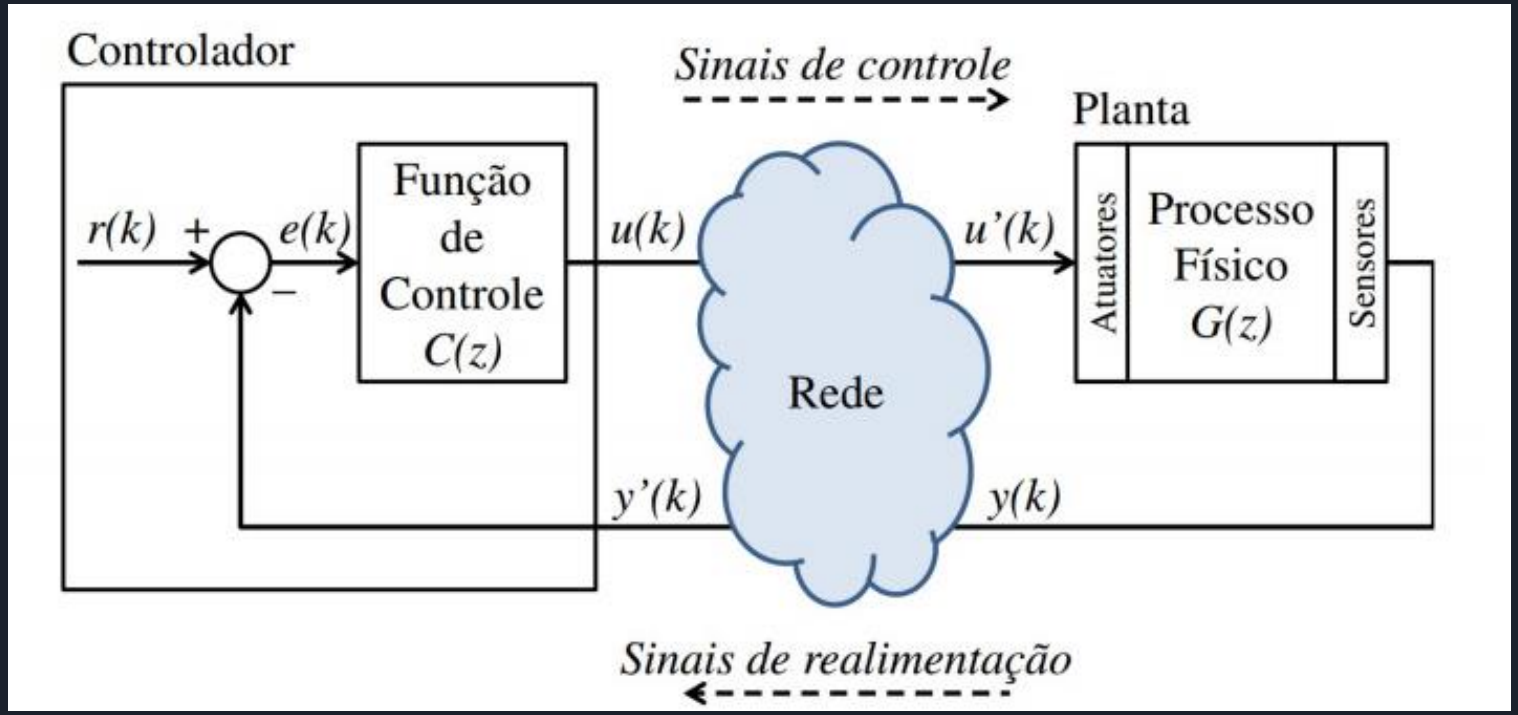
Análise do artigo: Ataque furtivo em Sistemas de Controle Físicos Cibernéticos

Sistemas Ciber-físicos

Sistemas ciber-físicos são sistemas computacionais e colaborativos os quais as operações são monitoradas, coordenadas, controladas e integradas por núcleos de comunicação e computação.



Sistema de Controle em Rede (NCS)



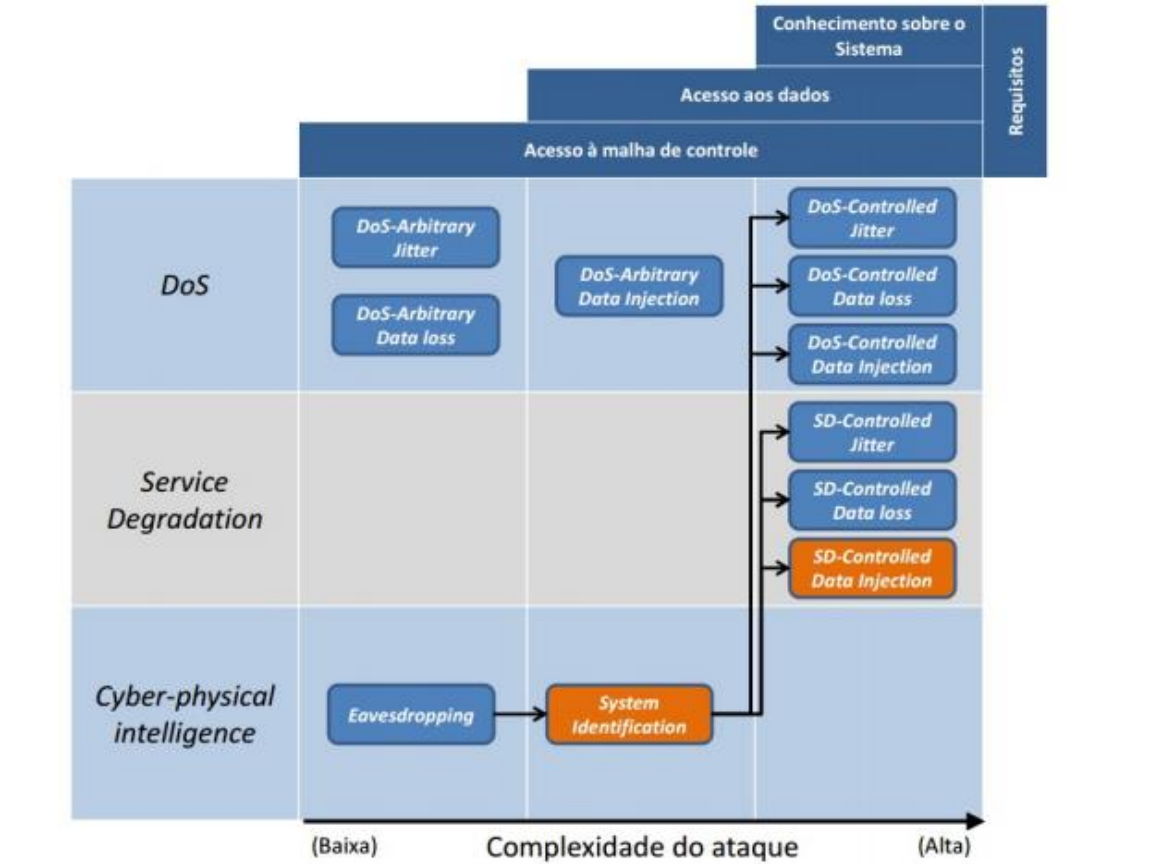
Vantagens e Desvantagens de um NSC

- Vantagens
  - Melhor capacidade operacional
  - Melhor capacidade gerencial
  - Redução de Custos
- Desvantagens
  - Ameaças típicas de falhas de segurança no domínio cibernético

Categorias de Ataques a NSC's

- Denial-of-Service (DoS): negação a operação dos processos físicos
- Service Degradation (SD): redução de eficiência dos serviços
- Cyber-physical Intelligence (CPI): colhe informações sobre o sistema e/ou sobre o projeto

Tipos de Ataque



Ataques do tipo DoS

- DoS-Arbitrary Jitter: neste tipo de ataque, o atraso dos sinais de controle e /ou realimentação e alterado arbitrariamente.
- DoS-Arbitrary Data Loss: neste tipo de ataque, o atacante impede que os dados cheguem aos atuadores e/ou controladores.
- DoS-Arbitrary Data Injection: nesses ataques, o atacante envia dados falsos e arbitrários ao controlador.
- DoS- Controlled - interferem na malha de controle do NCS da mesma forma que seus respectivos ataques DoS-Arbitrary, tendo como diferença o conhecimento acurado do modelo do NCS

Ataques do Tipo SD

- SD-Controlled Jitter
- SD-Controlled Data Loss
- SD-Controlled Data Injection

Esse ataques não tem a intenção de interromper o processo físico em um curto prazo. O ataque visa manter o processo funcionando com a eficiência reduzida ou, por vezes, causar a deterioração física e gradual dos dispositivos controlados.

Furtividade Cibernética x Física

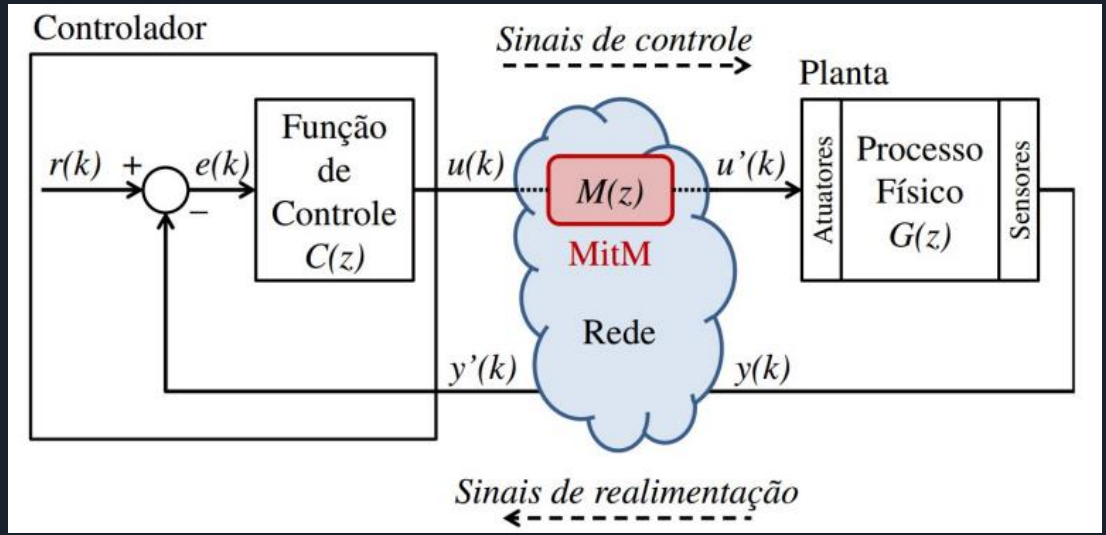
- **Ataques ciberneticamente furtivos:** são ataques que têm baixa probabilidade de serem detectados por algoritmos que monitoram os softwares, a comunicação e os dados do sistema, ou por sistemas que monitoram a dinâmica da planta.
- **Ataques fisicamente furtivos:** são ataques que causam efeitos físicos que nào são facilmente percebidos ou identificados por um observador humano. O ataque modifica sutilmente alguns comportamentos do sistema de forma a afetar fisicamente a planta, mas o efeito não é facilmente percebido ou, eventualmente, pode ser entendido como uma consequência cuja causa seja outra, diferente de um ataque.

Ataque de Identificação de Sistema

Os ataques que visam identificar as funções de transferência da planta e controlador requerem a captura de informações que trafegam pela rede industrial (dados atuação e de sensores) e o uso posterior de um algoritmo para estimar as funções com base nos dados.
O artigo usa o algoritmo BSA (Algoritmo de Busca por Retrocesso)

Ataque Furtivo para Degradação do Serviço

- Causa: O atacante intervém no processo de comunicação do NSC a fim de injetar, de forma controlada, dados falsos no sistema. Para tal, o atacante atua como um MitM que executa uma função de ataque M(z).

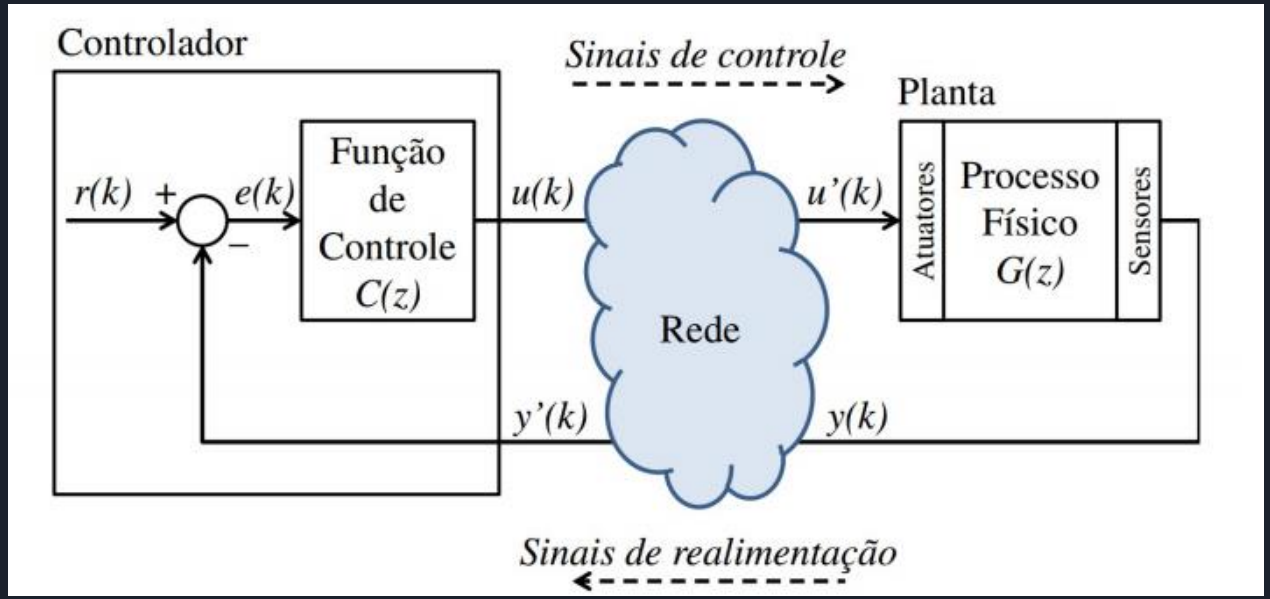


Ataque Furtivo para Degradação do Serviço

- Resultados esperados
  - Indução de um overshoot durante o regime transitório da planta;
  - Erro estacionário constante na planta

Modelo adotado pelo autor

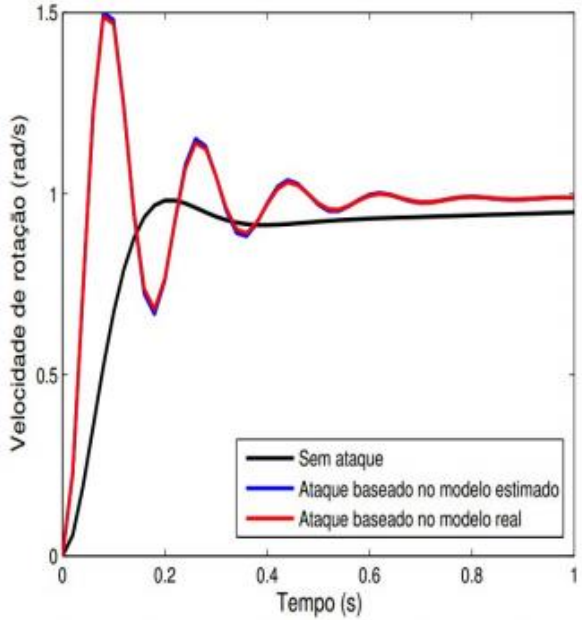
O NSC atacado consiste em um controlador Proporcional-Integral (PI) que controla a velocidade de rotação de um motor DC.



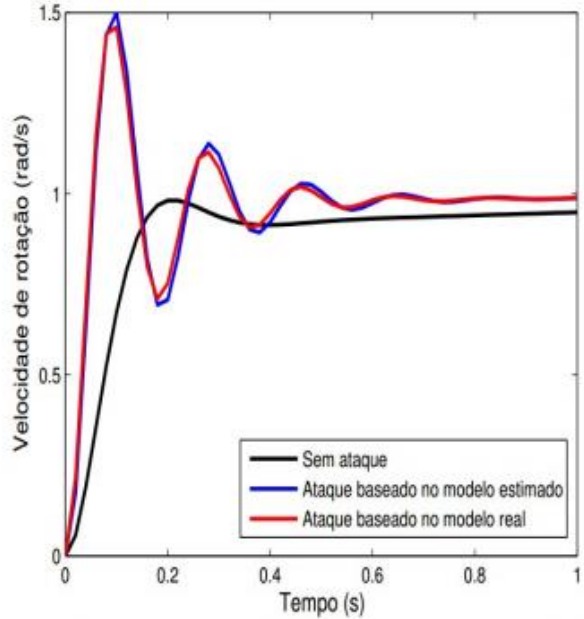
Experimento Realizado

- Objetivo
  - Simulação de ataques de injeção de dados do tipo SD (degradação de serviço) para obtenção no primeiro caso de overshoot de 50% na velocidade de rotação do motor e no segundo caso visa causar erro estacionário de -10% na velocidade de rotação.
- Materiais
  - Matlab
- Métodos
  - Algoritmo BSA

Resultados



(a) Ataque baseado nos dados obtidos sem perda de amostras



(b) Ataque baseado nos dados obtidos com 20% de perda de amostras

Conclusões

	Perda de amostras no ataque *System Identification*			
	0 %	5 %	10 %	20 %
$\mathcal{K}_o$	4,0451	4,0745	4,0828	3,796
Overshoot no modelo real	48,90 %	49,43 %	49,57 %	45,94 %
$\mathcal{K}_{Ess}$	5,7471	5,7803	5,8140	5,8823
Erro estacionário no modelo real	−10%	−10%	−9, 9%	−9, 8%

Overshoot: 45,95% objtivo:50%
Erro estacionário: -9,8%; Objetivo: -10%

Com base nos resultados obtidos, é possível afirmar que os ataques do tipo ***SD Controlled Data Infection*** (Ataque furtivo para degradação de serviços) com dados coletados através do ataque ***System Identification*** são capazes de modificar de forma acurada a resposta do sistema físico.