Game-Theoretic Methods for Security Investment in Cyber-physical Control Systems

Pratishtha Shukla, Dr. Alexandra Duel-Hallen and Dr. Aranya Chakrabortty

Overview

1. PROBLEM OBJECTIVE

- Security of control systems is becoming a pivotal concern in critical national infrastructures.
- Identify critical nodes for protecting against cyber-attacks
- Maintain stability and control objectives
- Relate control performance to protection and attack resources
- Attacker and Defender's resource allocation

2. SYSTEM DESCRIPTION

- Consider a multi-agent dynamic system with n nodes.

SYSTEM MODEL -

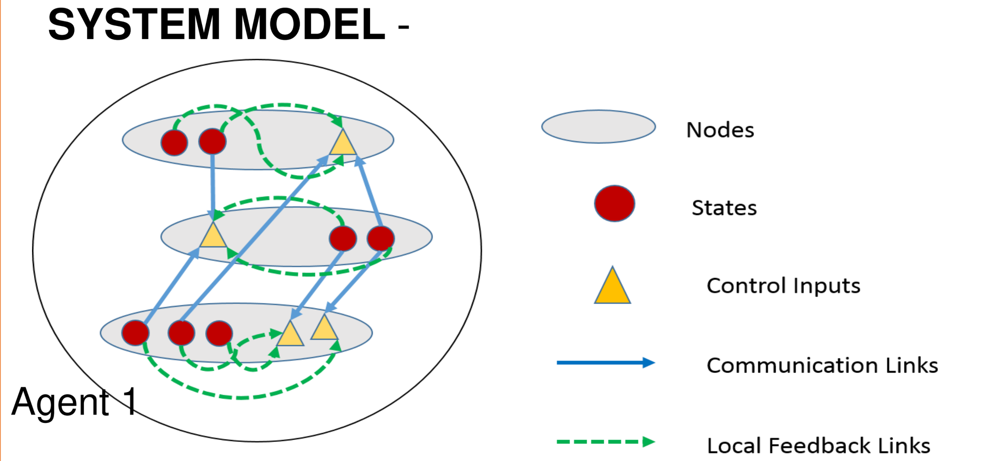


Fig. 1. System Model (one agent)

- Let us consider the linear dynamic system

$$\dot{x}(t) = Ax(t) + Bu(t)$$
$$y = Cx(t)$$

- We assume linear static feedback is employed, $u(t) = -Kx(t)$

- The LQR Objective

$$J = \int [x^T(t)Qx(t) + u^T(t)Ru(t)]dt,$$

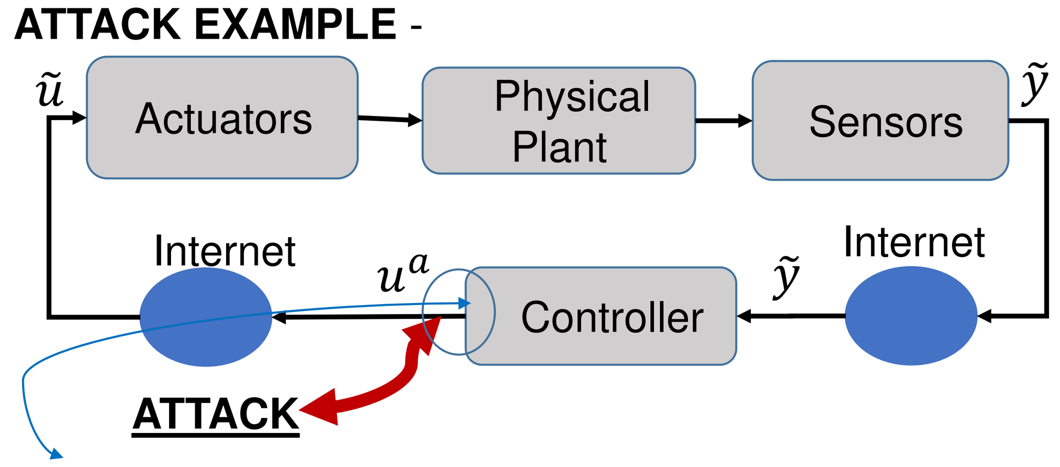
Where $Q \geq 0, R > 0$

Theory

1. ATTACK ON SYSTEM

- A device attack is an exploit that takes advantage of a vulnerable device to gain access to a network.

ATTACK EXAMPLE -



The communication equipment (e.g.: a modem) responsible for sending and receiving data from the controller to the communication network is attacked including the local network (e.g.: a VPN or LAN)

Fig. 2. Attack Example: Modem attacked

ATTACK TOPOLOGY-

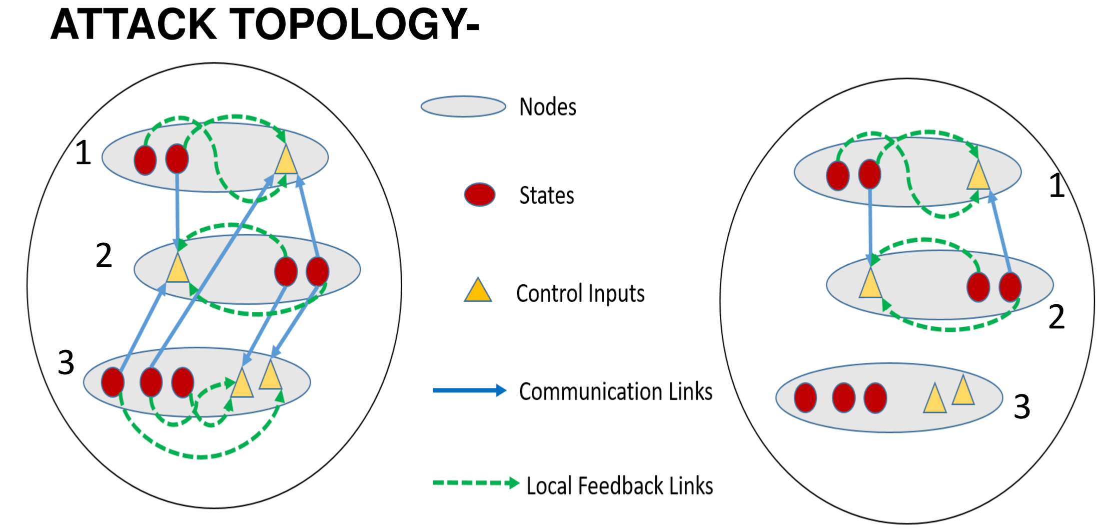


Fig. 3. Attack topology: Node 3 attacked and the defender does not protect

2. GAME FORMULATION

- The attacker tries to cause a noticeable amount of Loss in the system by increasing the energy of the system.

- With attacker and defender mixed strategy vectors r and d, the expected payoffs of the players become

$$E_a(r, d) = rU_a d^T$$
$$E_d(r, d) = rU_d d^T$$

- The utility matrices are

$$U_a = L - \gamma_a(N)$$
$$U_d = -L - \gamma_d(N)$$

- Where **L** is Loss matrix formed by

$$L_i = J(K) - J(K_i)$$

Where K_i is the structurally optimized sparse matrix for scenario S_i.

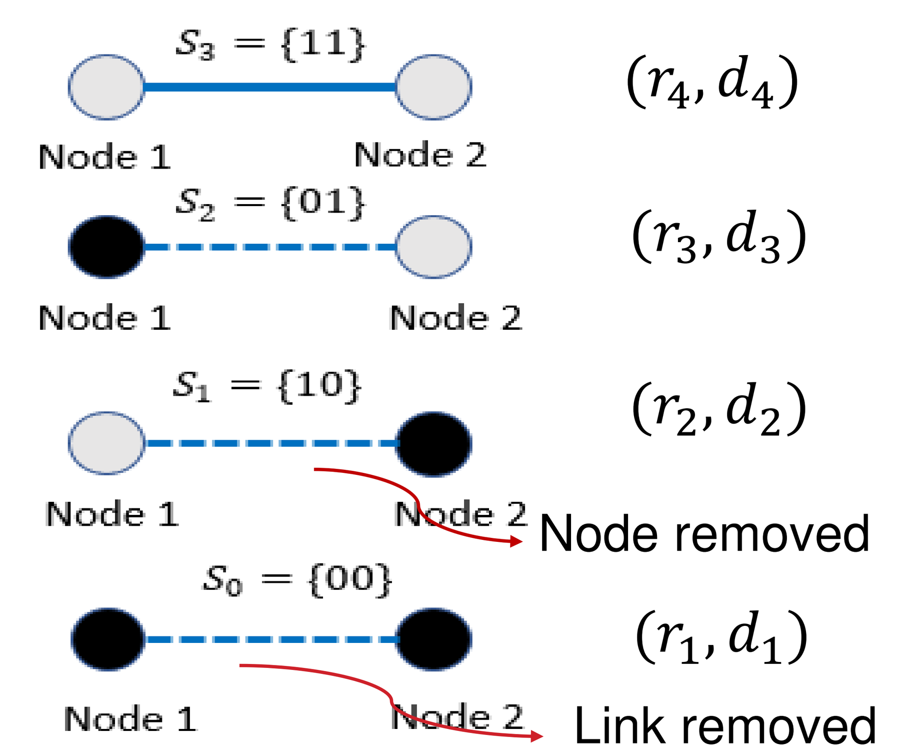


Fig. 4. Possible attack scenarios for 2-node system

- Mixed Strategy Nash Equilibrium

$$E_a(r^*, d^*) \geq E_a(r, d^*): \forall r \in A^*$$
$$E_d(r^*, d^*) \geq E_d(r^*, d): \forall d \in D^*$$

Simulation Results

- IEEE 39 New England Power Grid Model

> - As the cost ratio varies, the expected payoffs of the players change.
> - Critical points is when the attacker's payoff becomes 0, which is when the cost is high.
> - At this point on-wards, the defense investment gives us important nodes

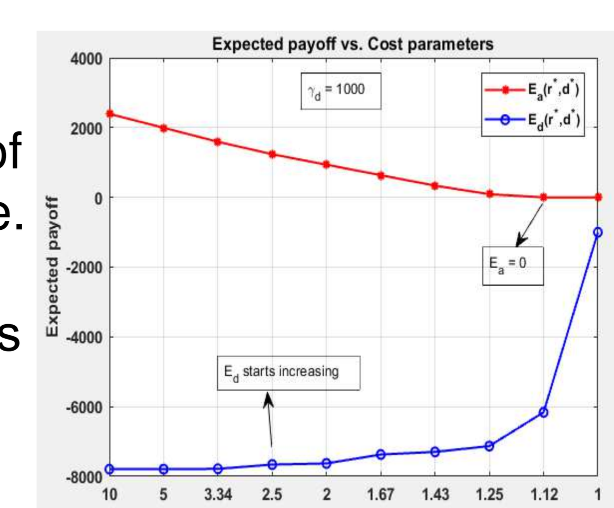


Fig. 5. Expected payoffs vs. cost ratios

- Obtaining expected payoff at varying cost ratios, summarizes the cost dependency.

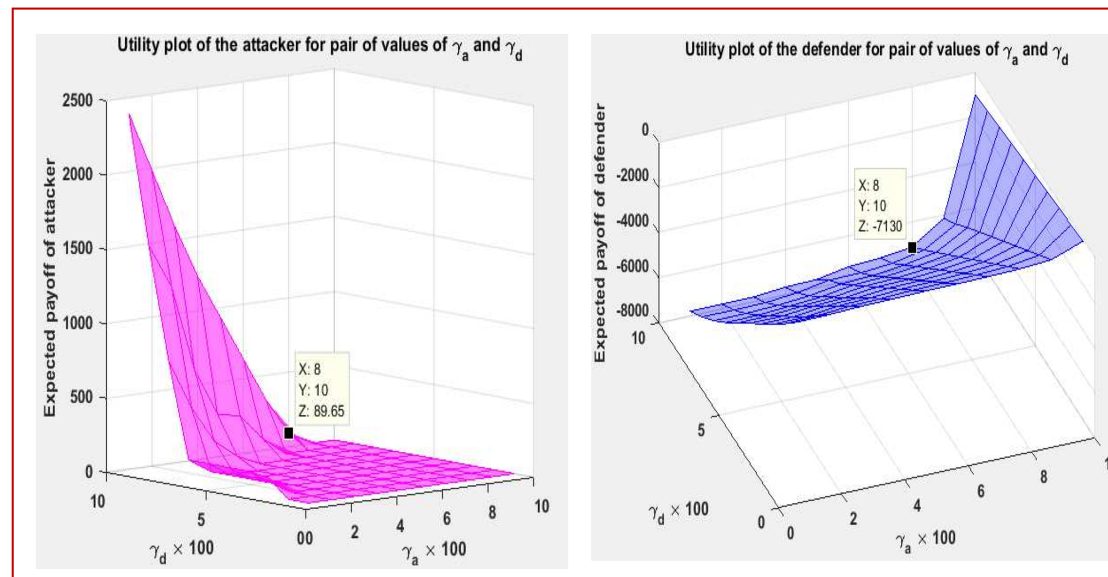


Fig. 6. Expected payoffs 3D plots

- Axes represent the cost ratios γ_a and γ_d.
- Increasing γ_a implies the attacker would need to spend more of its resources, decreasing its attack and increasing E_a
- Increasing γ_d will lead to more use of defender's resources.

γ_a increases, E_a decreases, E_d increases
γ_d increases, E_d decreases, E_a increases

CONCLUSION

The defender is able to defend with success from "device" attacks given sufficient resources. The game allows to place these resources strategically to save costs and optimize the impact for any multi-agent network.

References

1. A. Sarabi, P. Naghizadeh, and M. Liu, "Can Less Be More? A Game-Theoretic Analysis of Filtering vs. Investment", 2014
2. M. Fardad, F. Lin, M. Jovanovic, "On the optimal design of structured feedback gains for interconnected systems", 2009.