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).

ATTACK TOPOLOGY:

ATTACK EXAMPLE:

2. GAME FORMULATION

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

Mixed Strategy Nash Equilibrium

The utility matrices are

\[ U_a = L - y_a(N) \]
\[ U_d = -L - y_d(N) \]

Where \( L \) is Loss matrix formed by

\[ L_i = f(K) - f(K_d) \]

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

Simulation Results

IEEE 39 New England Power Grid Model

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

Axes represent the cost ratios \( y_a \) and \( y_d \).

Increasing \( y_a \) implies the attacker would need to spend more of its resources, decreasing its attack and increasing \( E_a \).

Increasing \( y_d \) will lead to more use of defender’s resources.

CONCLUSION

The defender is able to defend successfully 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