**Introduction**

The paper proposes a lightweight defense mechanism against battery drain denial-of-service (DoS) attacks in wireless sensor networks (WSNs) using game theory and cyber deception. It models the interaction between a malicious attacker and a sensor node using signaling theory. The node strategically emits deceptive signals to mislead the attacker, reducing attack success. The proposed model determines optimal strategies through a Perfect Bayesian Nash Equilibrium (PBNE) analysis. Simulation results show that deceptive signaling enhances network security while conserving energy. The study highlights how game-theoretic deception can mitigate energy depletion attacks, ensuring longer WSN lifespans.

**Installation**

1. Clone the repository

git clone <https://github.com/YourUsername/WSN-Game-Theory-Defense.git>

cd WSN-Game-Theory-Defense

1. Install dependencies

pip install -r requirements.txt

**Usage**

1. Run the simulation

python main.py

Modify parameters in main.py to customize the simulation:

* attackCost
* successBenefit
* lowEnergyCost
* highEnergyCost
* priorBeliefs

Table of gain use for simulation

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

**Simulation Overview**

The simulation performs the following steps:

1. Initializes game parameters using equations from the research paper.
2. Computes expected utilities for the defender and attacker based on Nash Equilibrium calculations.
3. Plot result showing the evolution of player utility in pure and mixed Nash equilibrium
4. Tracks RAM and ROM usage throughout the simulation.
5. Plots results showing how RAM usage evolves with different prior beliefs (q).