A Meta-Game Theoretic Approach to Cyber-Physical Co-Design of Secure and Resilient Control Systems

CNS-1544782

Zhiheng Xu and Quanyan Zhu, New York University, E-mail: {zx383, quanyan.zhu}@nyu.edu

INTRODUCTION

- The new challenge of **Cyber-Physical Systems** (CPSs) comes from the high **interdependency** between the **cyber** and **physical** layers. The interdependency provides opportunities for adversaries to damage the **physical parts** through **cyber attacks**.
- Classical security solutions, such as **cryptography** and **intrusion detection**, are insufficient to protect the CPSs from sophisticated cyber-physical attacks.
- We use a **cross-layer design** to study the interdependency between the cyber and physical layers of a CPS.
- The main objective of the work is to enhance the **security** and **resiliency** to the **cyber-physical attacks**.
- We present different applications: UAVs, 3D printers, and train control systems, to illustrate the cross-layer design.

Cross-Layer Design

Cross-Layer Approach: The security objectives vary for different layers of the CPSs. We leverage control, game theory, decision theory, and cryptography to protect CPSs from cyber-physical attacks.

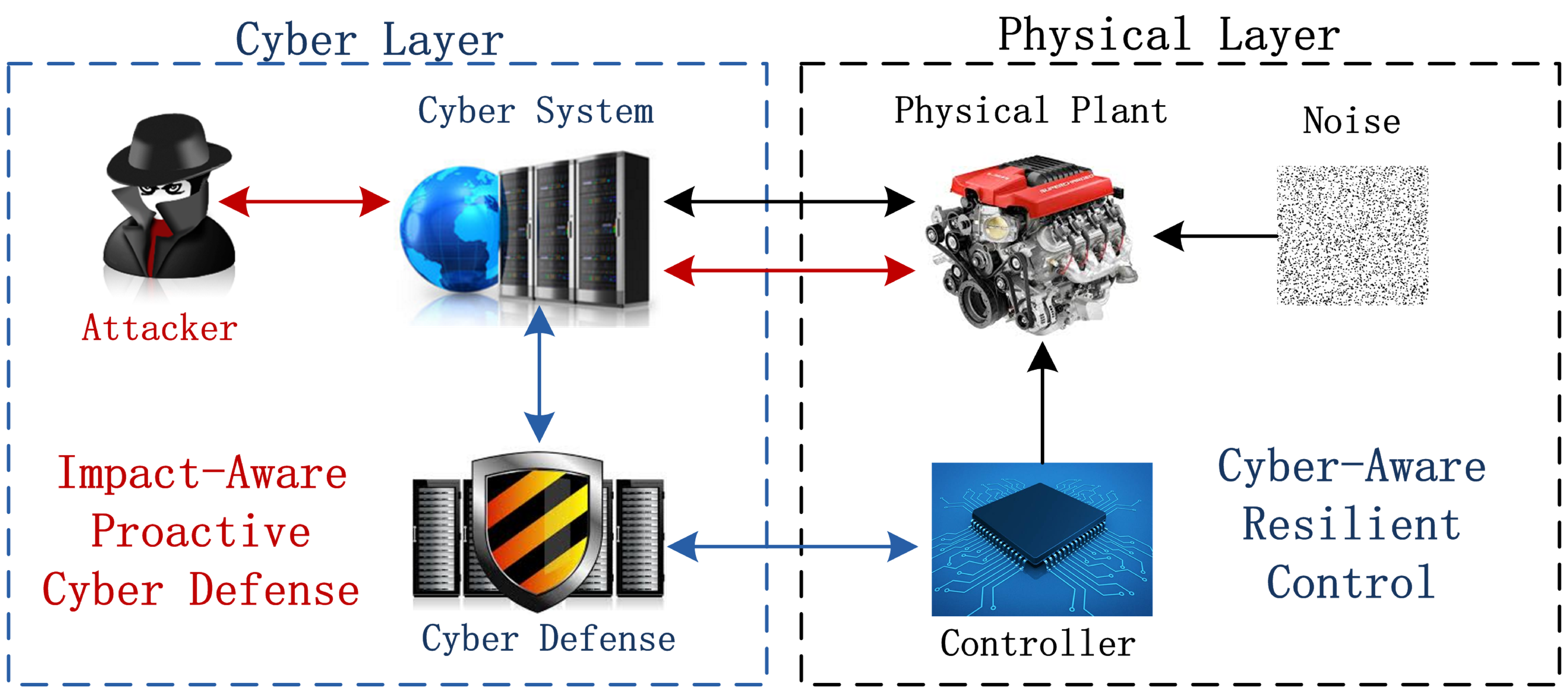
Cyber Layer: We develop an *impact-aware proactive cyber defense*, which depends on the physical performance (e.g., stability and robustness).

Physical Layer: We use control and game theory to develop a *cyber-aware resilient control* for the system in a noisy and adversarial environment.

Cyber-Physical Attack Models to CPSs

- **Data Privacy Attack**: Eavesdropping sensitive information communicated at different layers of a CPS (App. #1).
- **Advanced Persistent Threat**: Intruding the system and staying undetected for a long period of time (App. #2).
- **Availability Attack**: Jamming the communication between sender and receiver in the systems (App. #1 & 3).

The Cyber-Physical Structure of a CPS and the Potential Threats



APP. 1: Cloud-Enabled UAVs (Homomorphic Cryptos + Model Predictive Control)

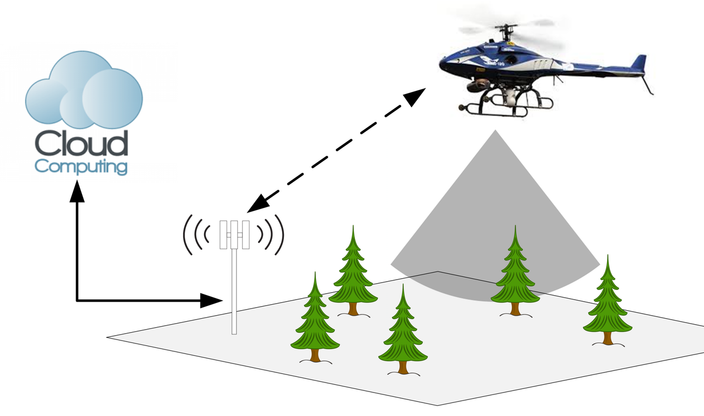


Figure 1: An unmanned helicopter conducts a search mission and outsources its computations to a cloud. The cloud returns desired results, including control inputs and verification codes to authenticate the data, to the UAV.

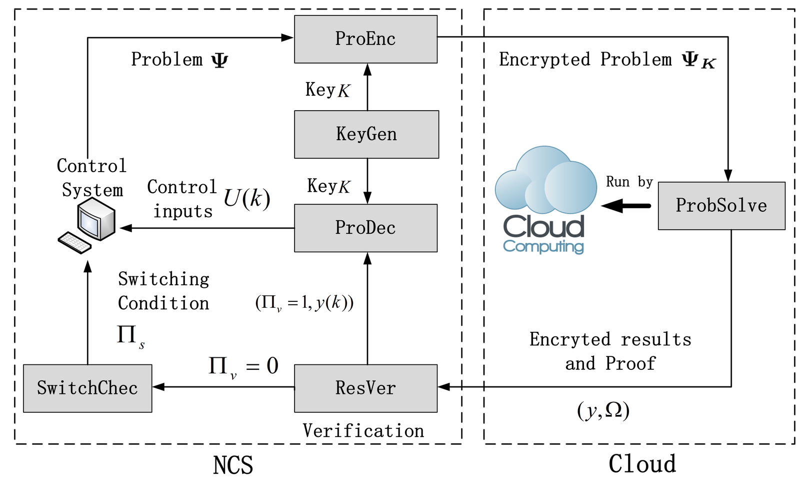


Figure 2: The mechanism achieves data confidentiality and integrity and allows the UAV to switch to a safe mode when the cloud is unavailable.

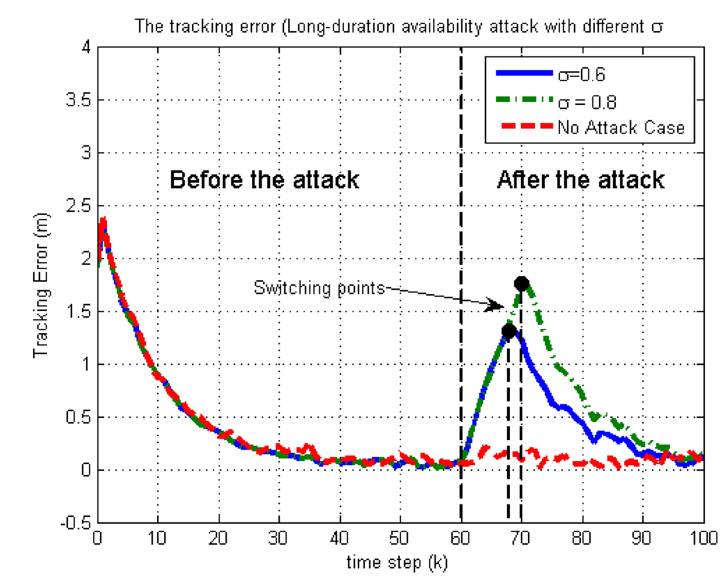


Figure 3: The tracking performance under a cyber attack with the secure and resilient mechanism.

APP. 2: Networked 3D Printer (*FlipIt* Game + Stackelberg Game)

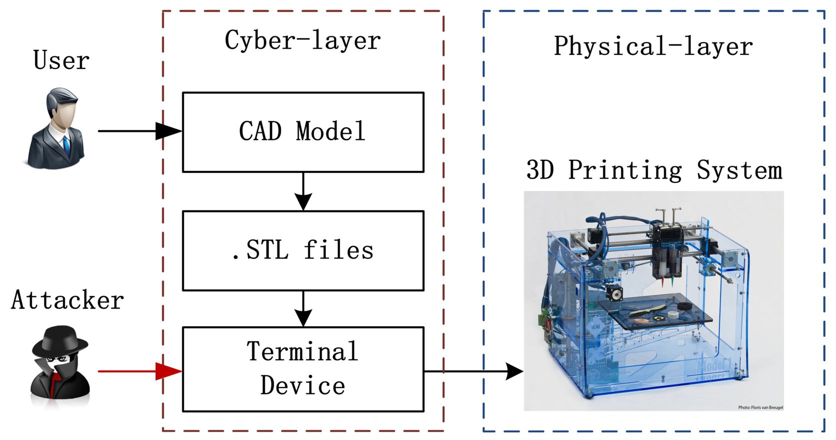


Figure 4: The cyber-physical structure of a 3D-printing system: The adversary can sabotage the system by ultimately taking over the terminal device, which stores reference files of the corresponding products.

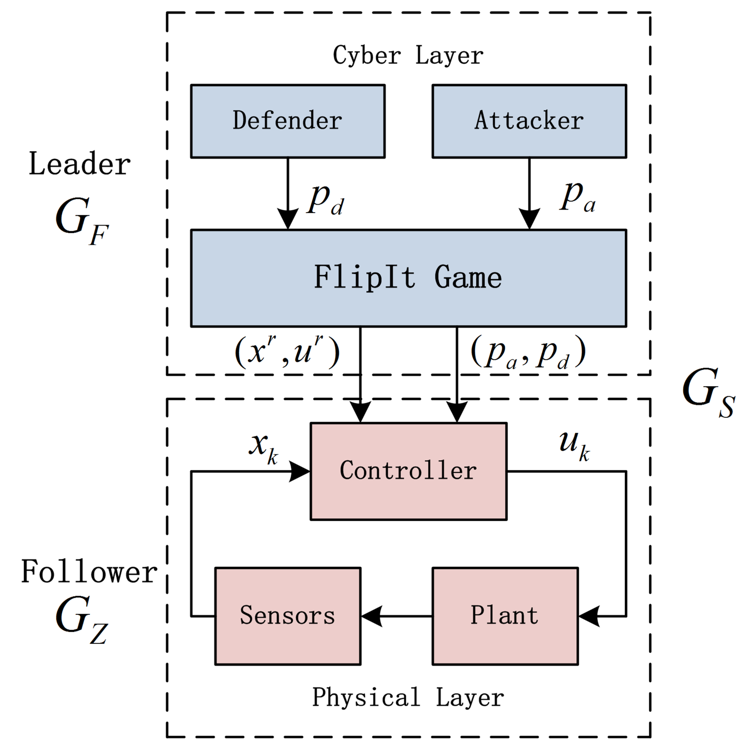


Figure 5: The cyber-physical Stackelberg meta-game.

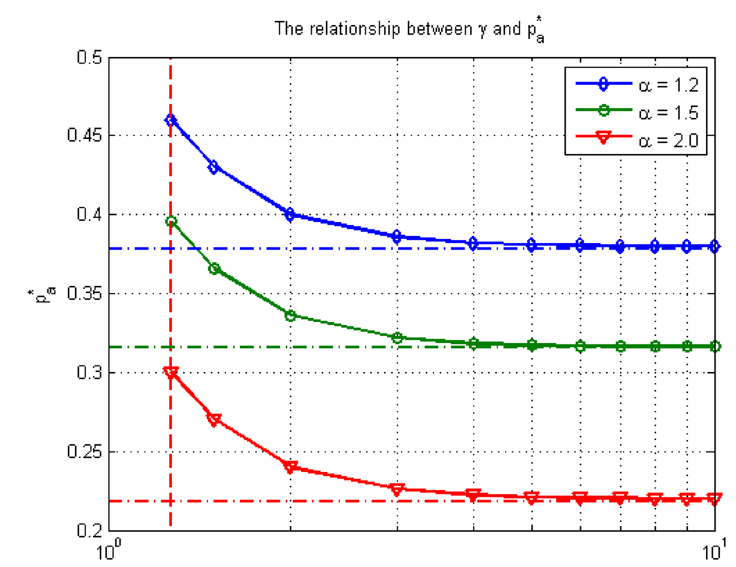


Figure 6: The tradeoff between robustness and security: a large attack cost α leads to a small threat p_a^*, and a high robustness (small γ) leads to a large threat p_a^*.

APP. 3: Communication-Based Train Control (Zero-Sum Game + Stochastic Game)

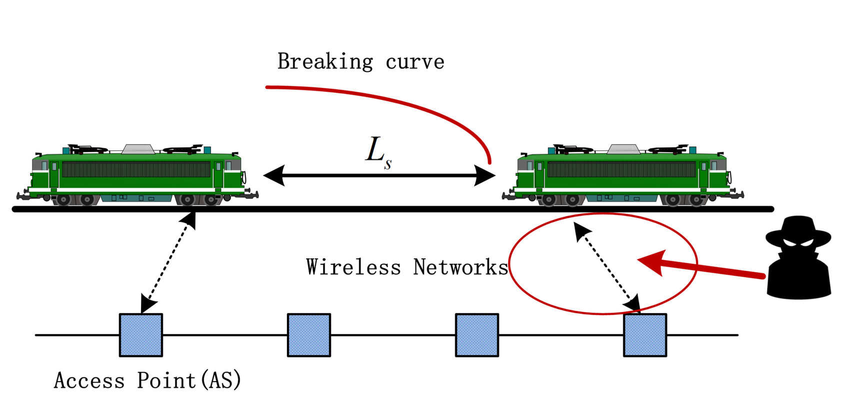


Figure 7: Two trains communicate with each other via wireless links to the time interval between trains travailing along the line. An adversary aims to jam the wireless communication between two trains, increasing the packet drop rate (PDR).

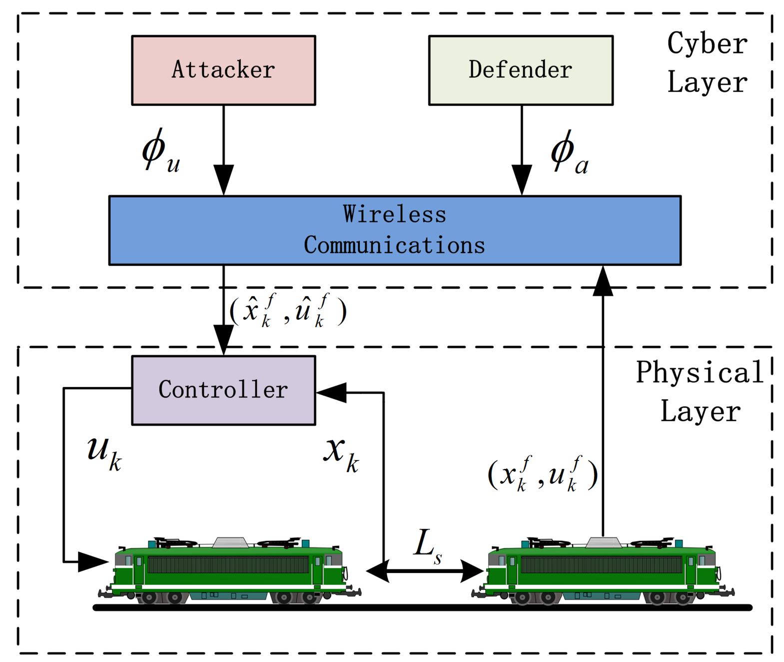


Figure 8: The architecture of a CBTC system: we compose two games to capture the cyber-physical interactions in an adversarial environment.

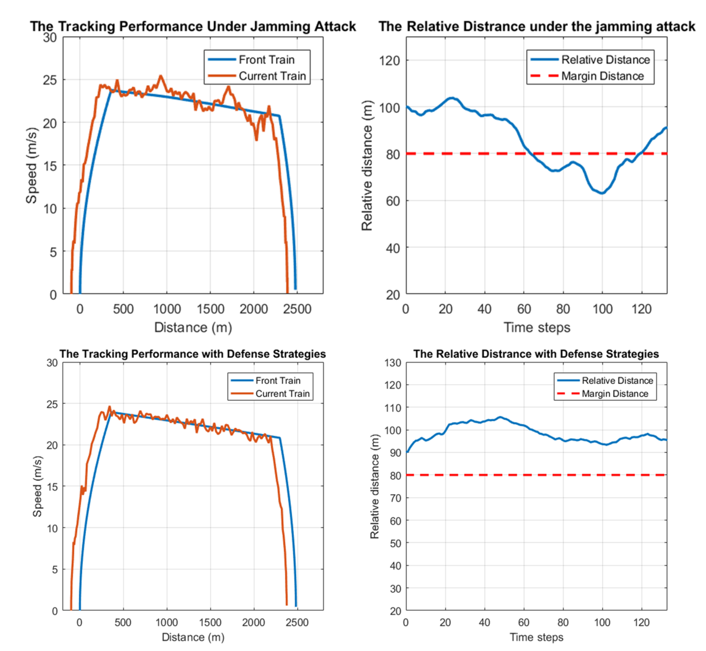


Figure 9: The trajectories and relative distance of the train under the attack-without-defense and the attack-with-defense cases.