Incremental Security Enforcement For Cyber Physical Systems

Guide: Dr K. S. Sudeep

Aaditya Muktavarapu, Lalit Narayanam , Vallabhu Vijay, Neriyanuri Karthik

Abstract

Problem Statement

- Cyber-Physical Systems (CPS) are vulnerable to cyber-physical attacks (CP-attacks) that exploit both digital and physical components.
- Traditional runtime enforcement (RE) methods lack incremental security updates, requiring full system revalidation and disrupting operations.

Proposed Solution

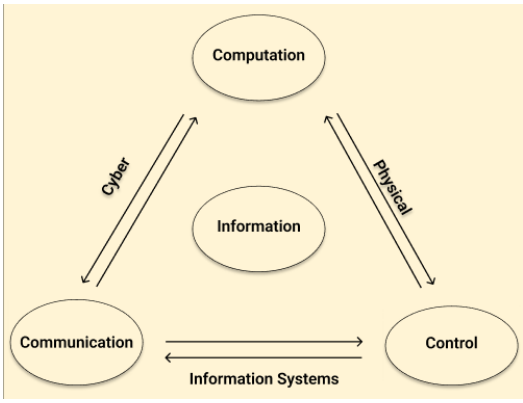
- We propose a Compositional Runtime Enforcement (CRE) framework for incremental security enforcement.
- It enables real-time policy adaptation without affecting existing policies.

Introduction

- Cyber-Physical Systems (CPS) are widely used in autonomous drones, industrial automation, and smart infrastructure, integrating both cyber and physical components for real-time operations.
- Their interconnected nature makes them vulnerable to cyber-physical attacks (CP-attacks) that exploit weaknesses in both digital communication and physical control mechanisms.
- Traditional security frameworks struggle to handle real-time constraints in CPS, as they require full system revalidation when introducing new security policies.
- This limitation leads to inefficiencies, system downtime, and scalability issues, making CPS security difficult to adapt to evolving threats.
- The proposed framework avoids state space explosion by applying security policies incrementally, ensuring scalable and efficient enforcement.
- It introduces a serial composition of enforcers, where each enforcer validates and modifies system inputs and outputs to maintain policy compliance.
- This approach ensures real-time security adaptation, allowing CPS to remain resilient against emerging cyber-physical attacks while maintaining system stability.

Methodology

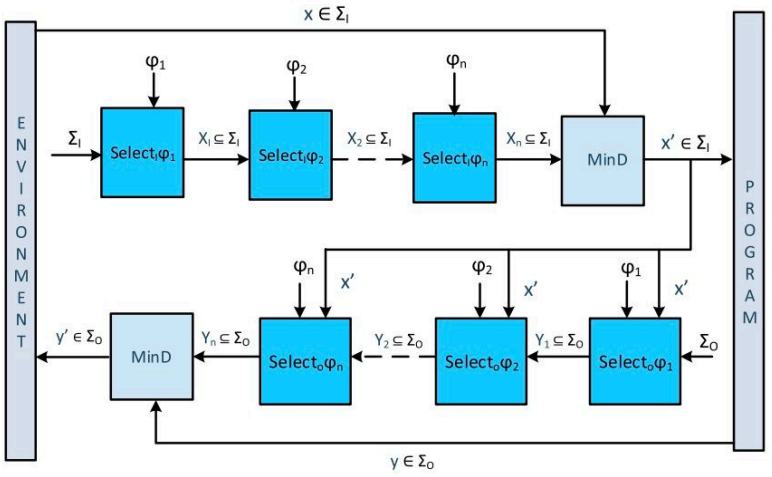
- Developed a bi-directional runtime enforcement framework using serial composition, enabling incremental security policy updates without full system revalidation.
- Implemented Input/Output Enforcement Functions for real-time data validation and modification, ensuring continuous policy compliance.
- Evaluated on a drone swarm simulation, preventing boundary breaches, conflicting signals, and resource exhaustion while maintaining scalability and linear execution efficiency.



Algorithm

Uses serial composition of enforcers, where each enforcer applies a specific policy. Sequential execution ensures that new policies can be added without revalidating the entire system.

- **Input Enforcement (EI)** – Checks and modifies incoming data to ensure policy compliance.
- **Output Enforcement (EO)** – Validates and adjusts system outputs before release.
- **Edit Functions (editIϕ, editOϕ)** – Replace non-compliant inputs/outputs with acceptable alternatives.
- **Select Functions (SelectIϕ, SelectOϕ)** – Choose the best policy-compliant option from a set of possible inputs/outputs.



Summary

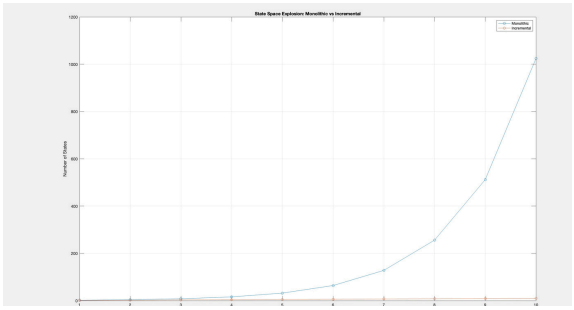


Fig (a)
Difference in state space between monolithic and incremental

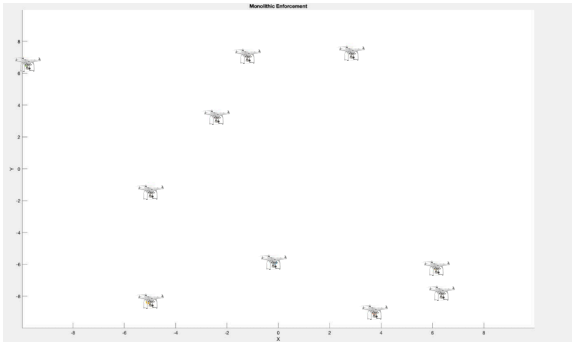


Fig (b)
Simulation of drones in a 2D space

- After creating a simulation of the monolithic enforcement technique and the incremental enforcement technique using a data set of a drone swarm on Matlab, we have obtained results that show the difference in state space.
- The Monolithic enforcement technique causes state space explosion whereas using the compositional runtime enforcement framework keeps the number of states almost constant

References

Incremental Security Enforcement for Cyber-Physical Systems by ABHINANDAN PANDA , ALEX BAIRD, SRINIVAS PINISETTY, AND PARTHA ROOP; Scalable Security Enforcement for Cyber Physical Systems by ALEX BAIRD , ABHINANDAN PANDA , HAMMOND PEARCE , SRINIVAS PINISETTY , AND PARTHA ROOP; Monitoring and Defense of Industrial Cyber-Physical Systems Under Typical Attacks: by Yuchen Jiang , Shimeng Wu , Renjie Ma , Ming Liu , Hao Luo , and Okyay Kaynak