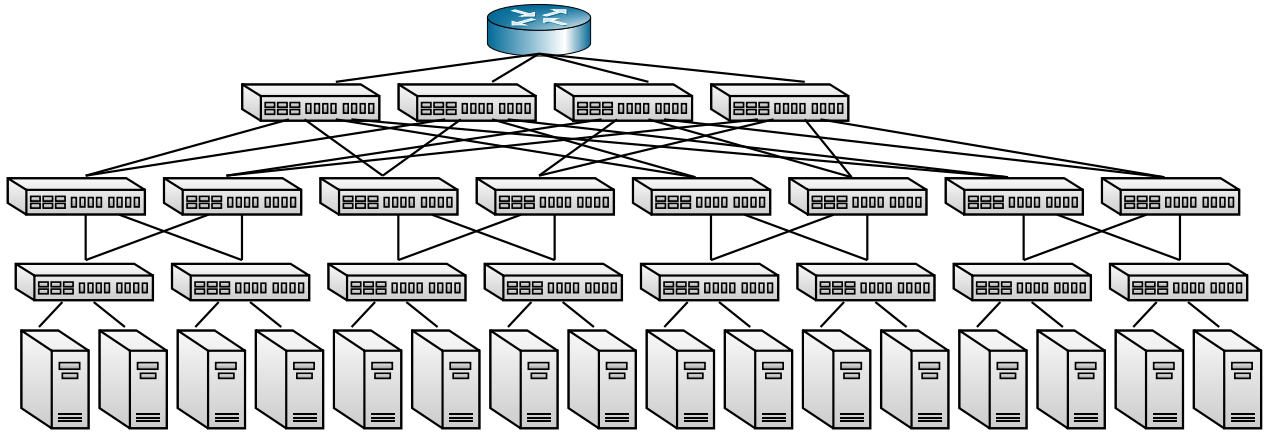
Optimal Security Management through Learning-based Control

IEEE NOMS, Dissertation Digest
Rome, Italy *May 20, 2026*

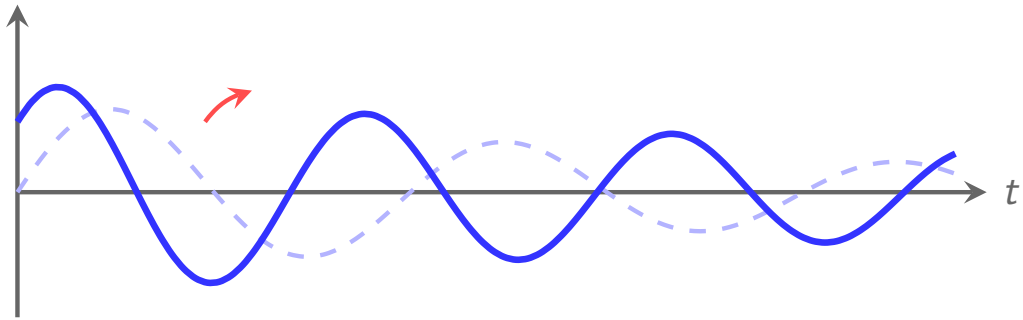
Kim Hammar
kimham@kth.se

Networked Systems

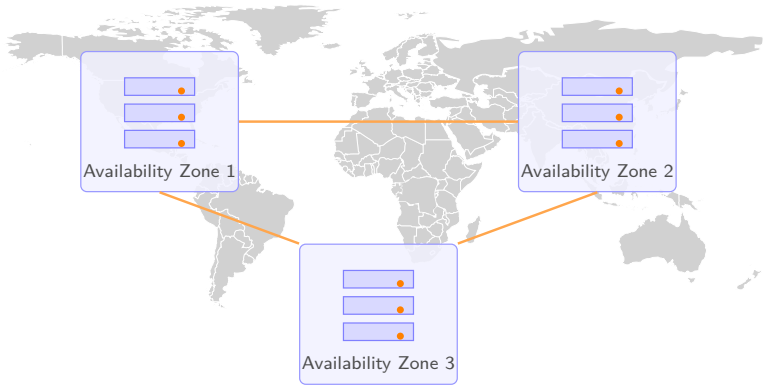
Complex



Dynamic



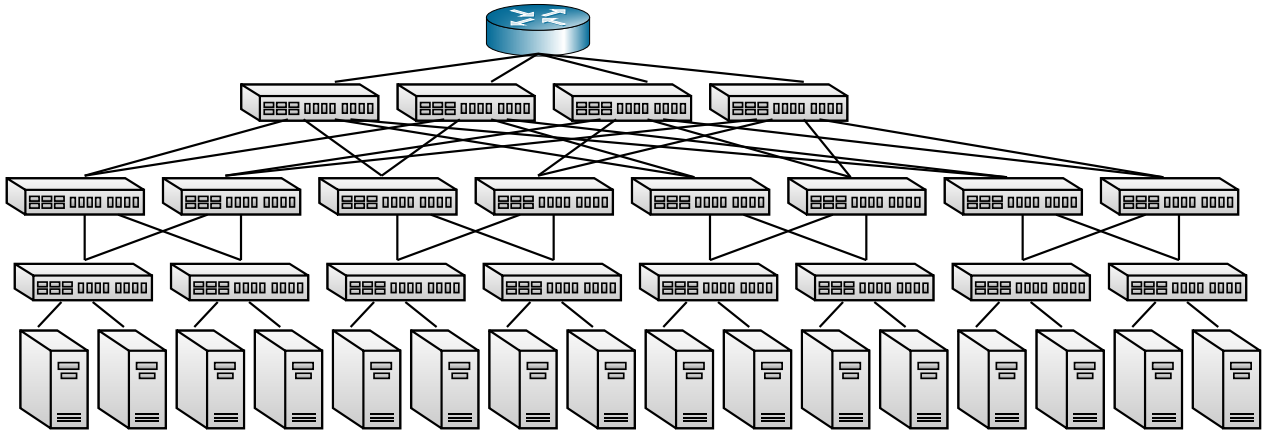
Distributed



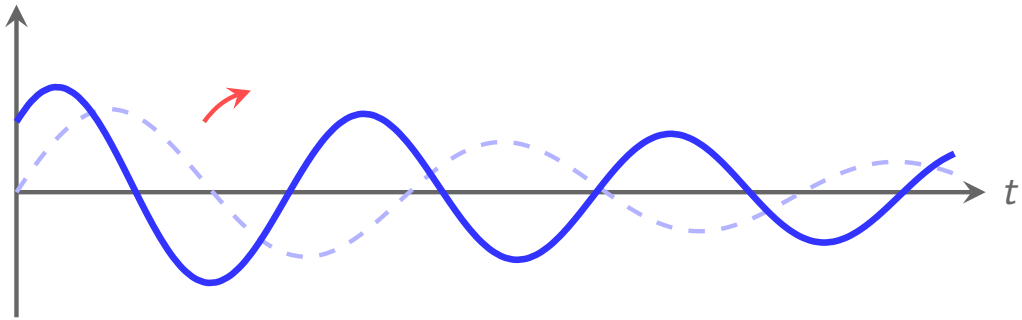
Networked Systems

Complex

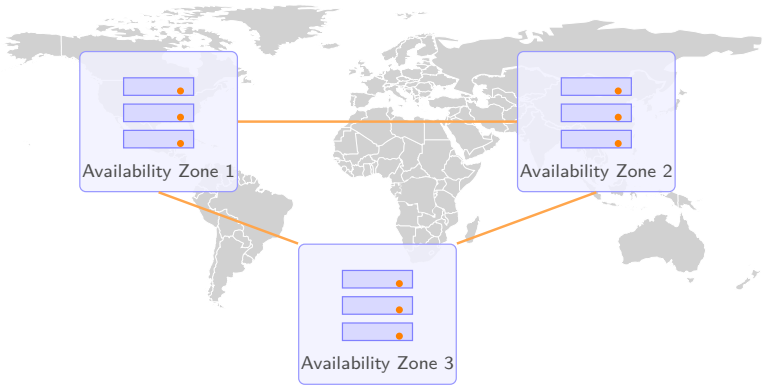
Automation



Dynamic



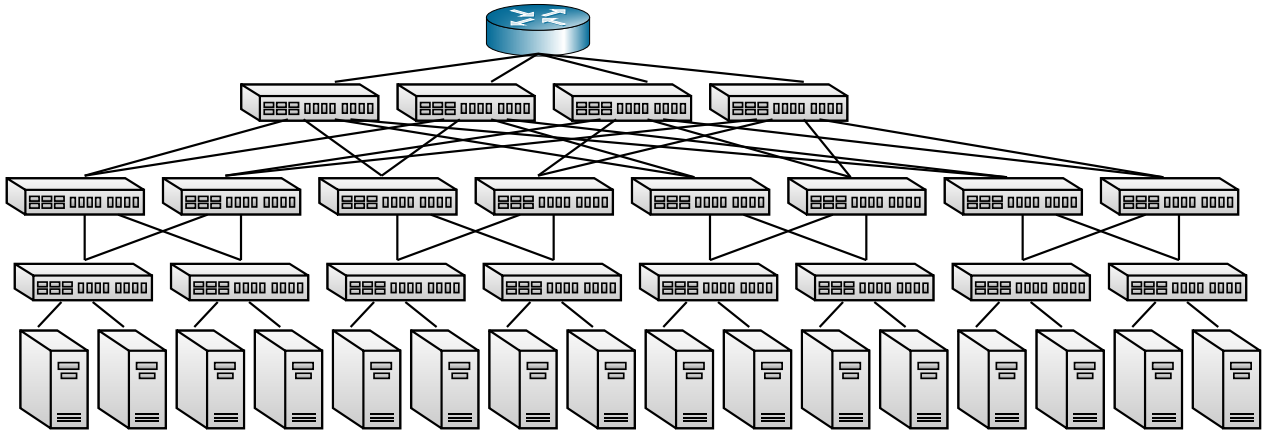
Distributed



Networked Systems

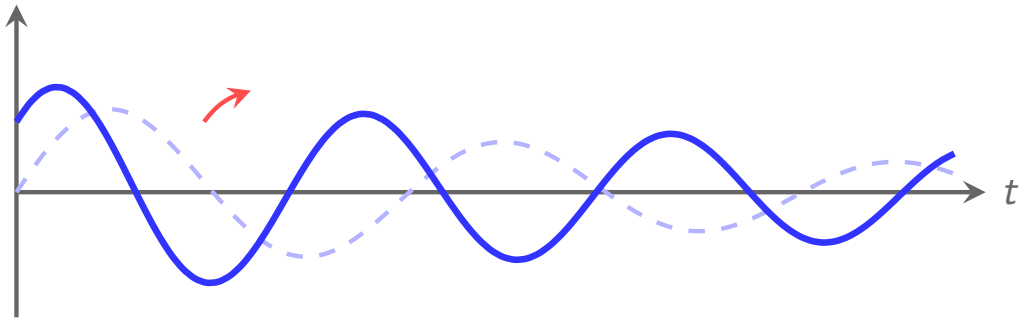
Complex

Automation

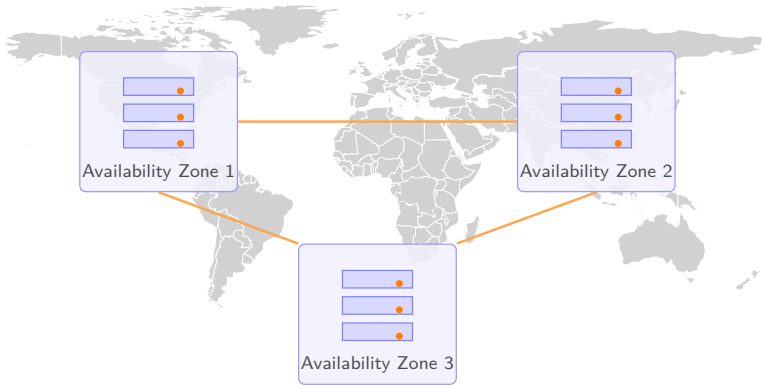


Dynamic

Control



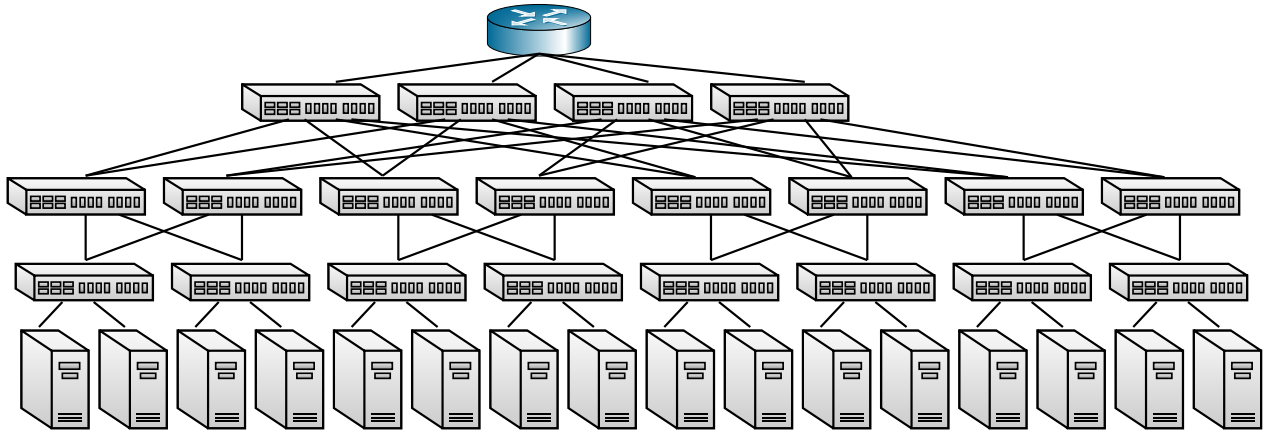
Distributed



Networked Systems

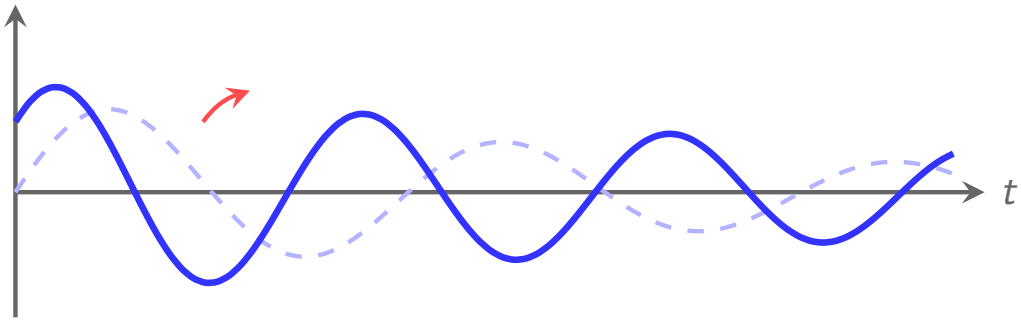
Complex

Automation



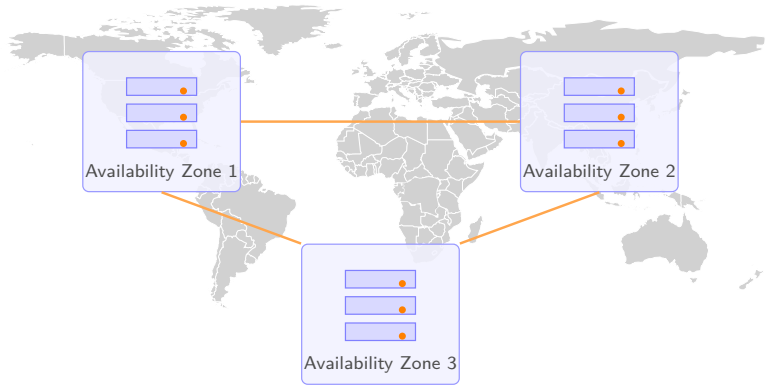
Dynamic

Control

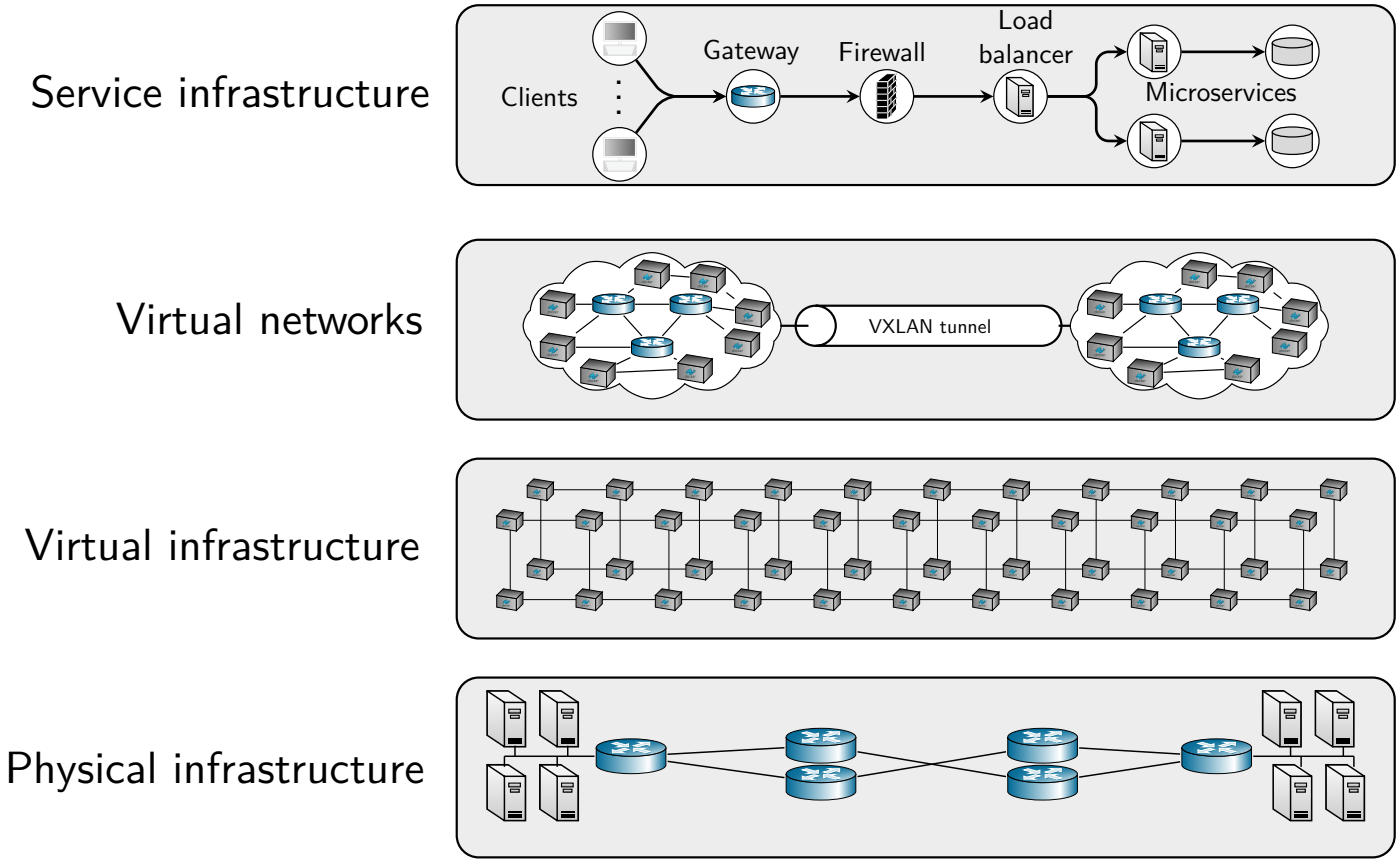


Distributed

Coordination

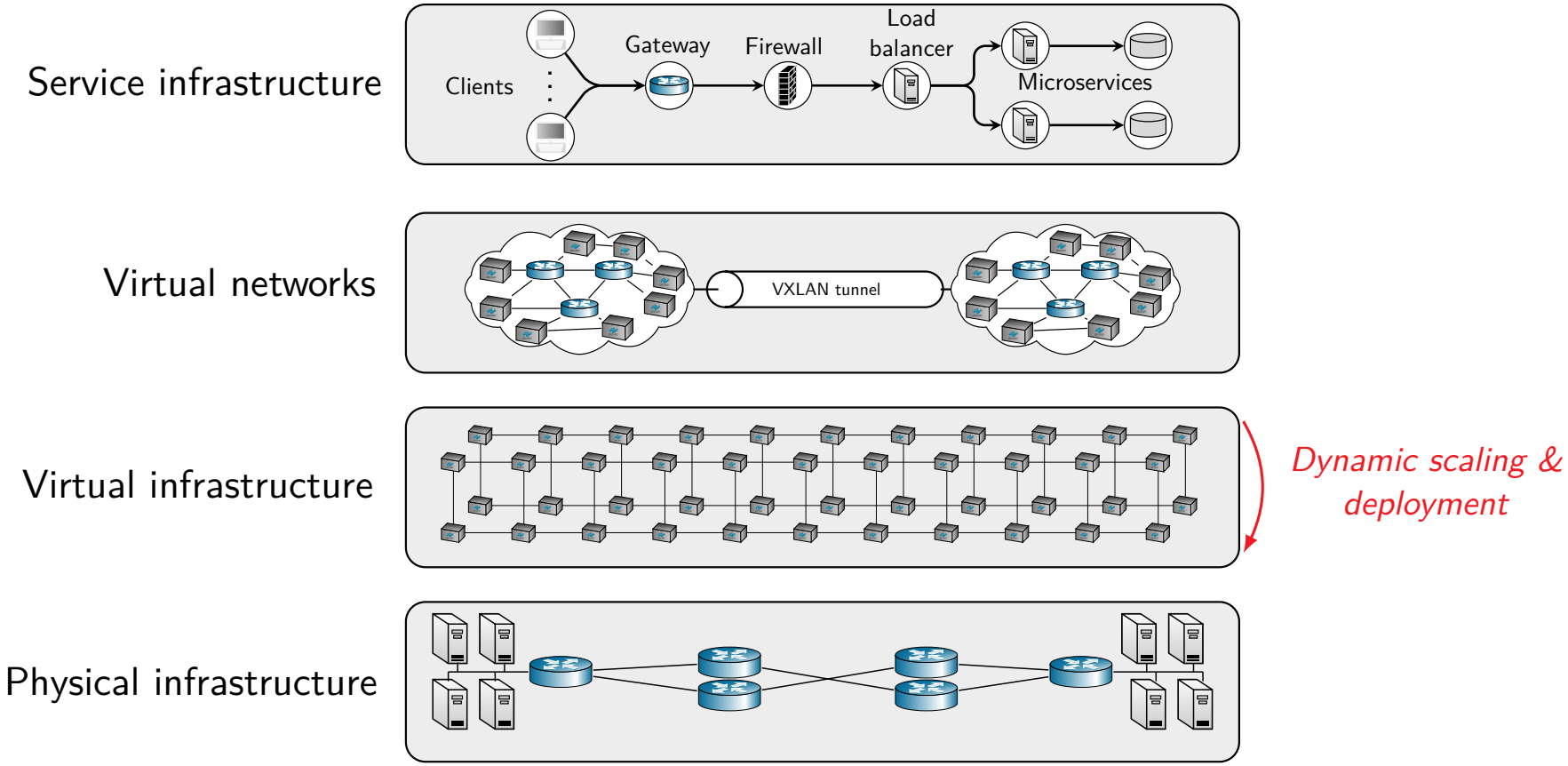


From Manual Configuration to Automatic Control



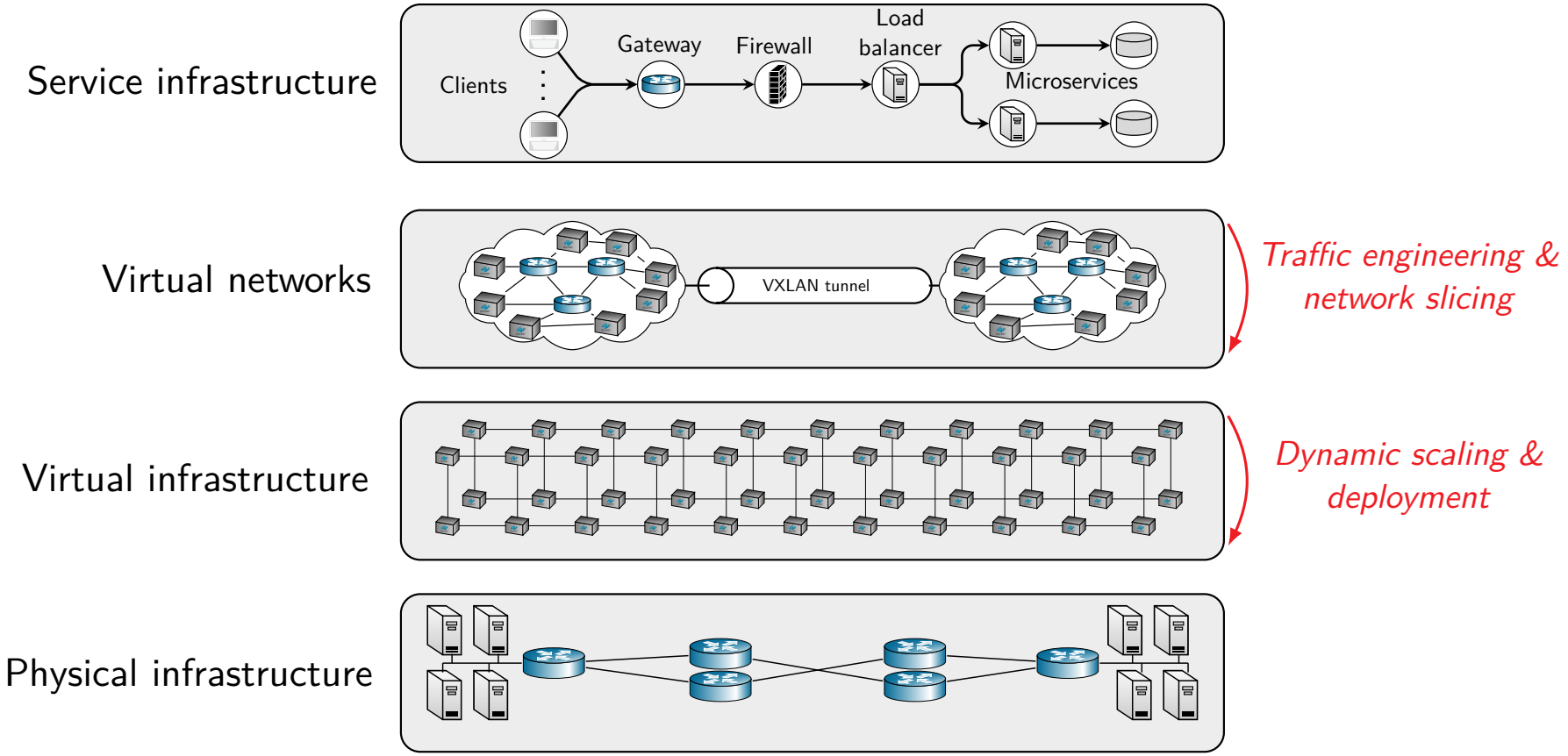
- Networked systems have undergone a shift from hardware-defined architectures to **software-defined** stacks.

From Manual Configuration to Automatic Control



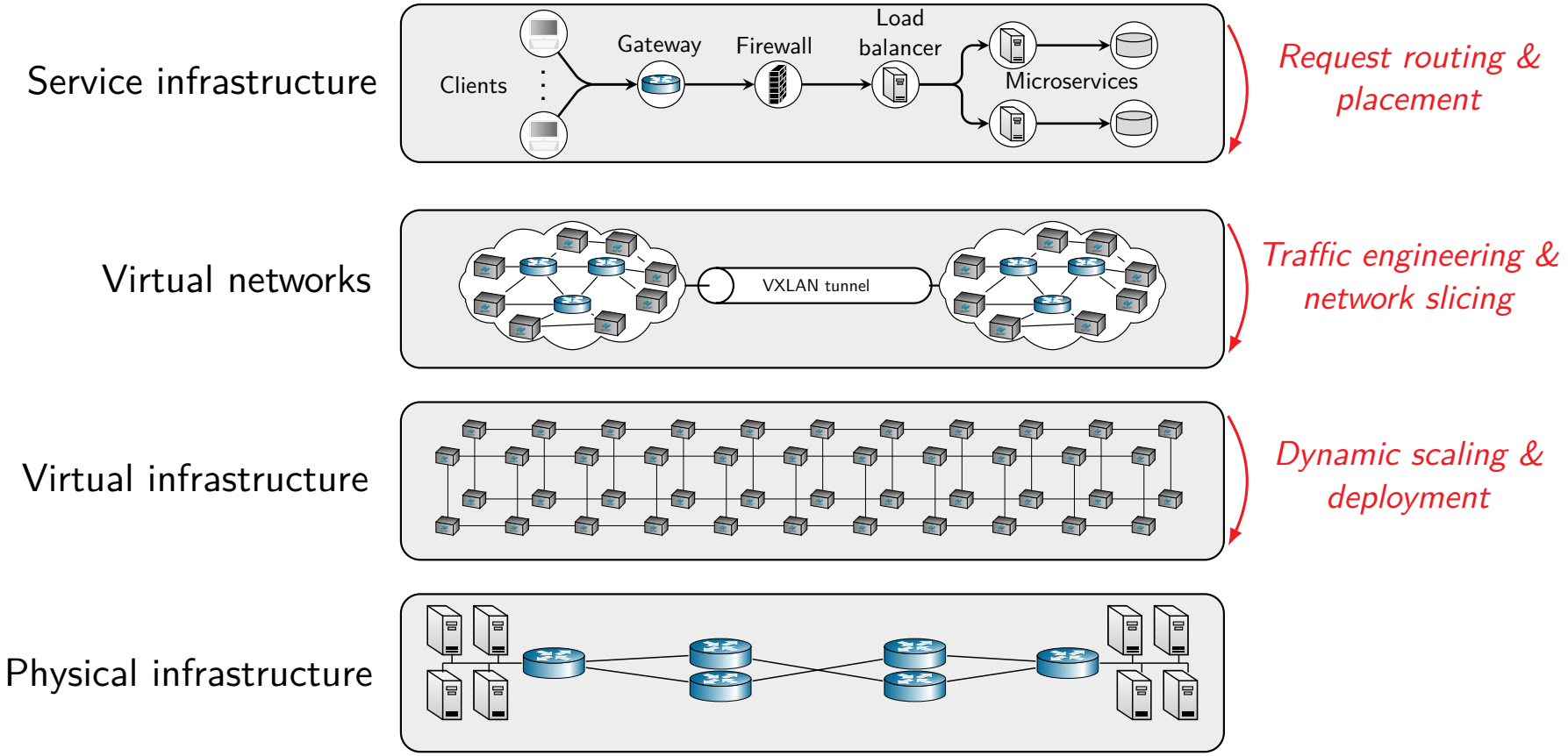
- Networked systems have undergone a shift from hardware-defined architectures to **software-defined** stacks.

From Manual Configuration to Automatic Control



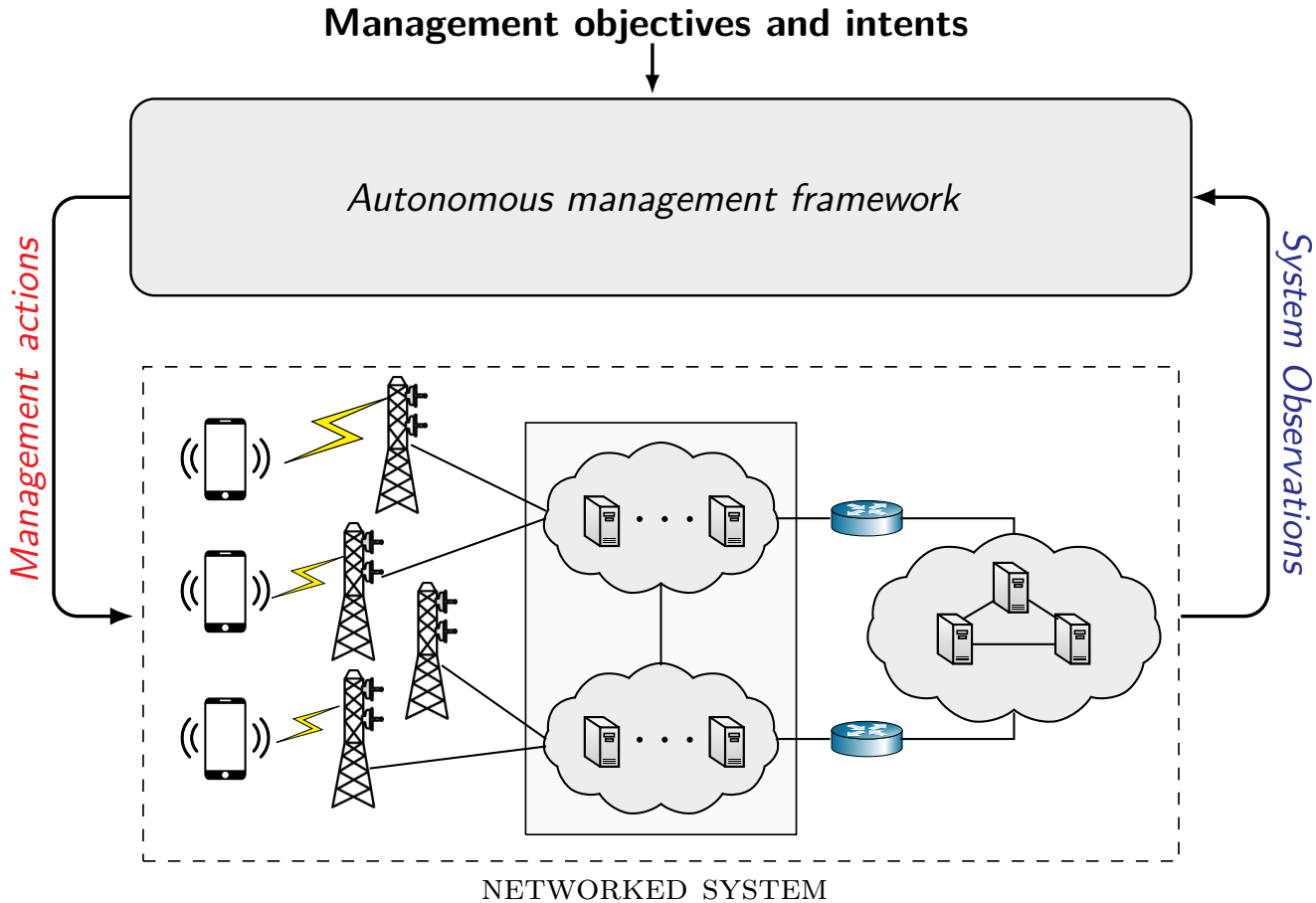
- Networked systems have undergone a shift from hardware-defined architectures to **software-defined** stacks.

From Manual Configuration to Automatic Control



- Networked systems have undergone a shift from hardware-defined architectures to **software-defined** stacks.

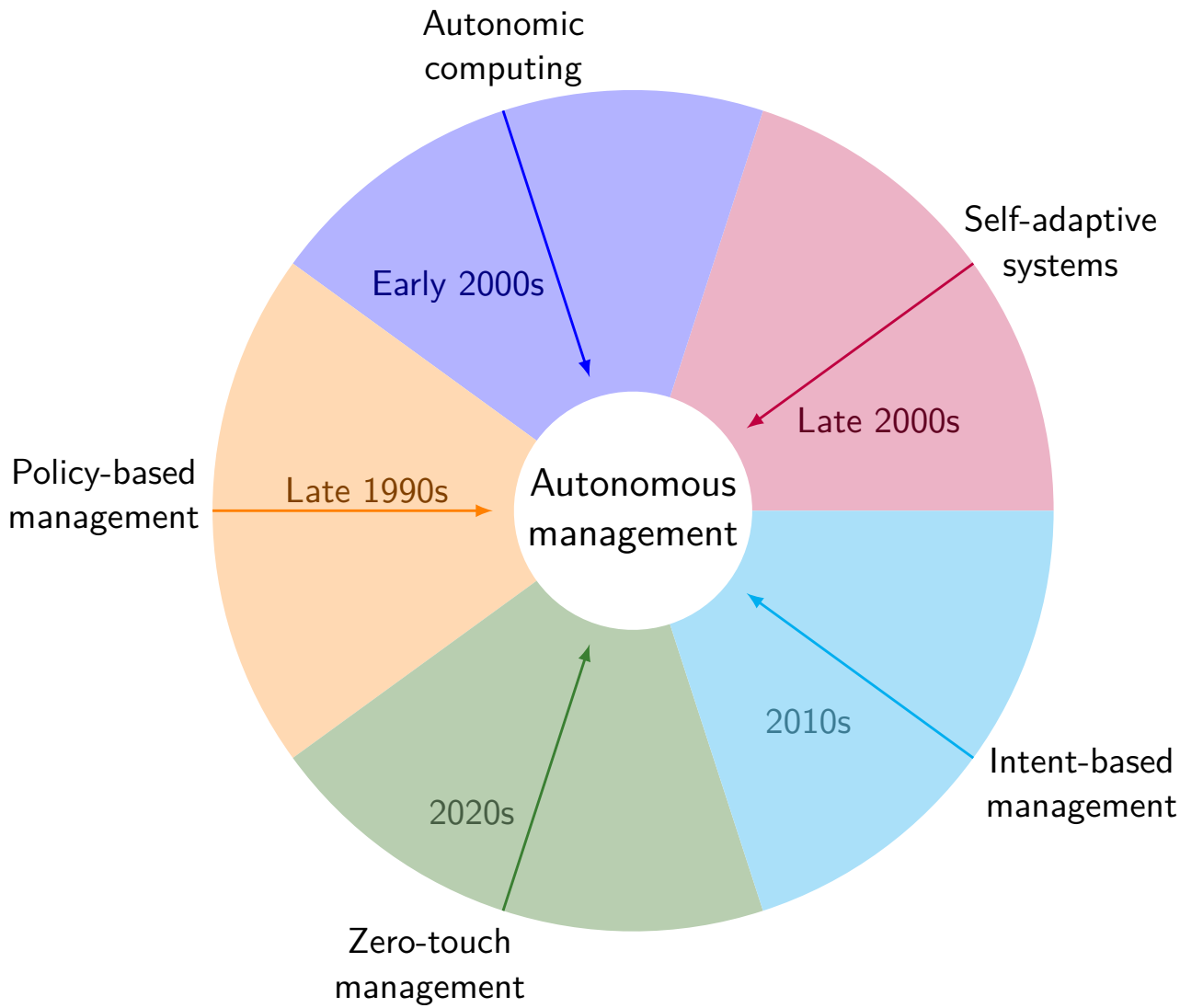
Autonomous Security Management of Networked Systems



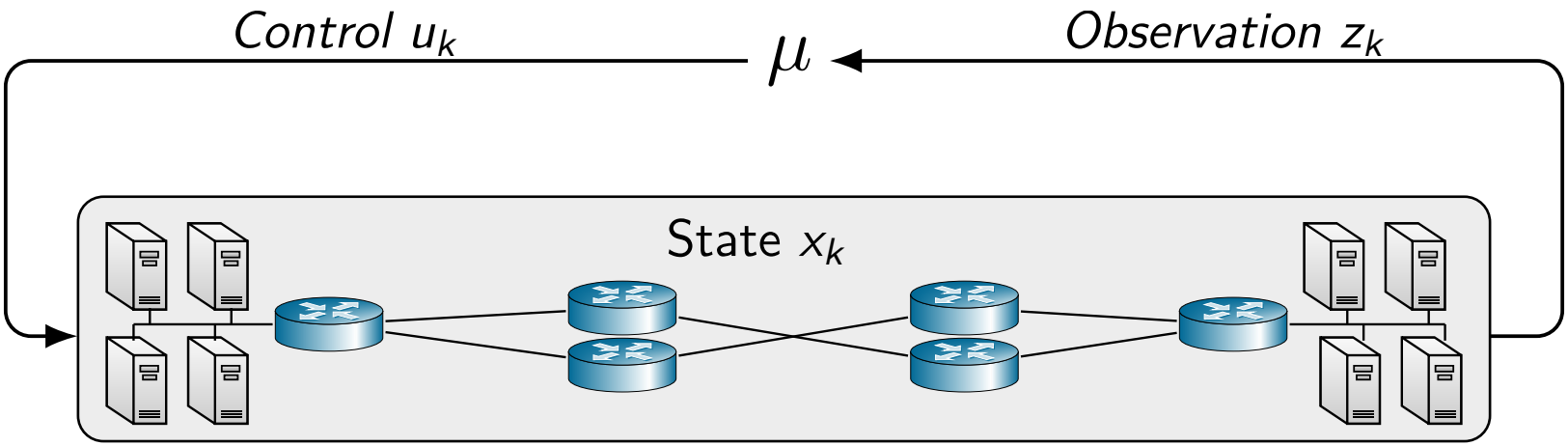
- Autonomous security management is needed to cope with the increasing complexity and dynamism of networked systems.
- The programmability and controllability of network and system functions is a prerequisite for autonomous management.

Prior Research

- Efforts towards automating the security management of networks and IT systems have been undertaken over the last 30 years.

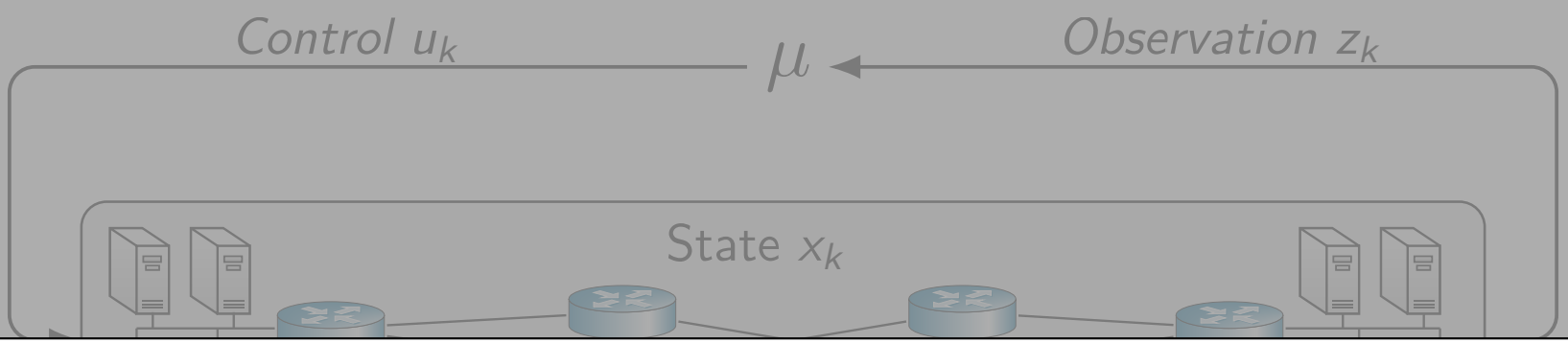


Autonomous Security Management as a Control Problem



- State x_k (e.g., security status and system configuration).
- Observation z_k (e.g., log files and security alerts).
- Control u_k (e.g., network segmentation and access control).
- **Goal**: find a strategy μ that meets security objectives.

Autonomous Security Management as a Control Problem

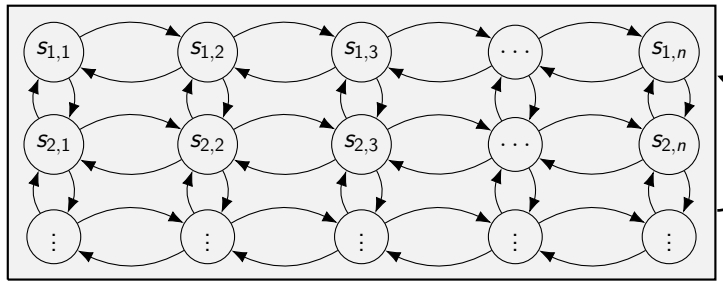


Current RL approaches are limited to abstract simulations and heuristics.

- State x_k (e.g., security status and system configuration).
- Observation z_k (e.g., log files and security alerts).
- Control u_k (e.g., network segmentation and access control).
- **Goal**: find a strategy μ that meets security objectives.

Methodology for Building Autonomous Security Systems

Simulation System

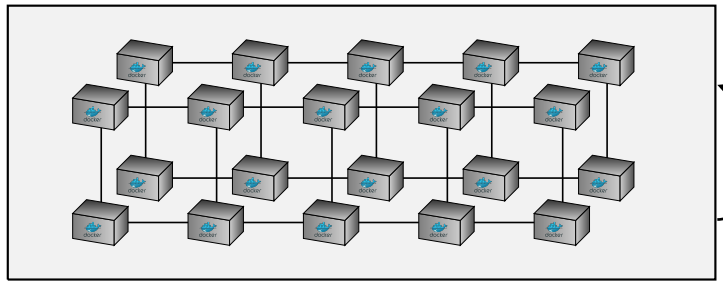


Mathematical Model & Reinforcement learning

Strategy Mapping π

System Identification

Emulation System

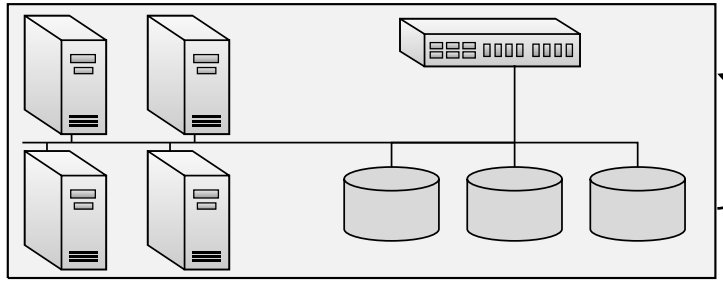


Strategy Evaluation & Model Estimation

Strategy Implementation π

Selective Replication

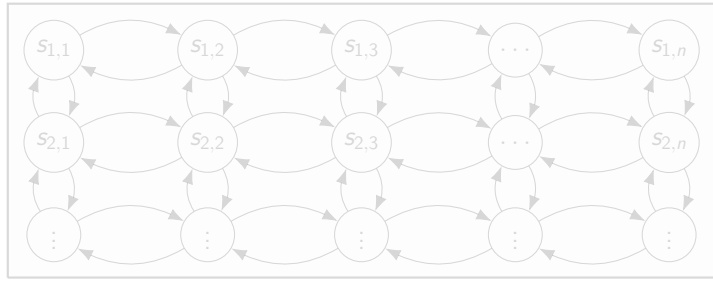
Target System



Autonomous Security Management

Methodology for Building Autonomous Security Systems

Simulation System

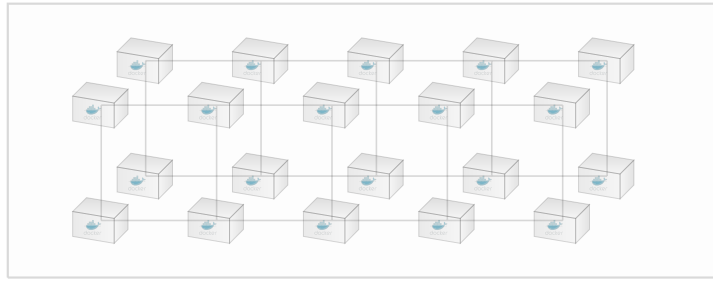


Mathematical Model & Reinforcement learning

Strategy Mapping π

System Identification

Emulation System

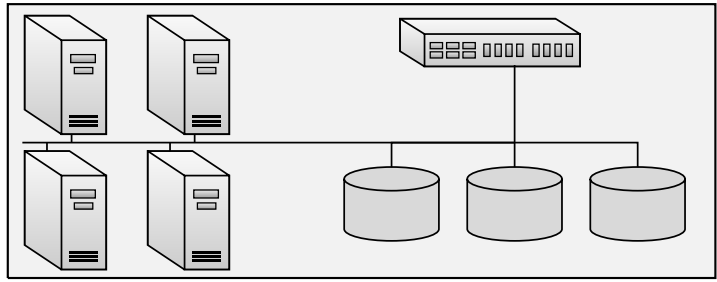


Strategy Evaluation & Model Estimation

Strategy Implementation π

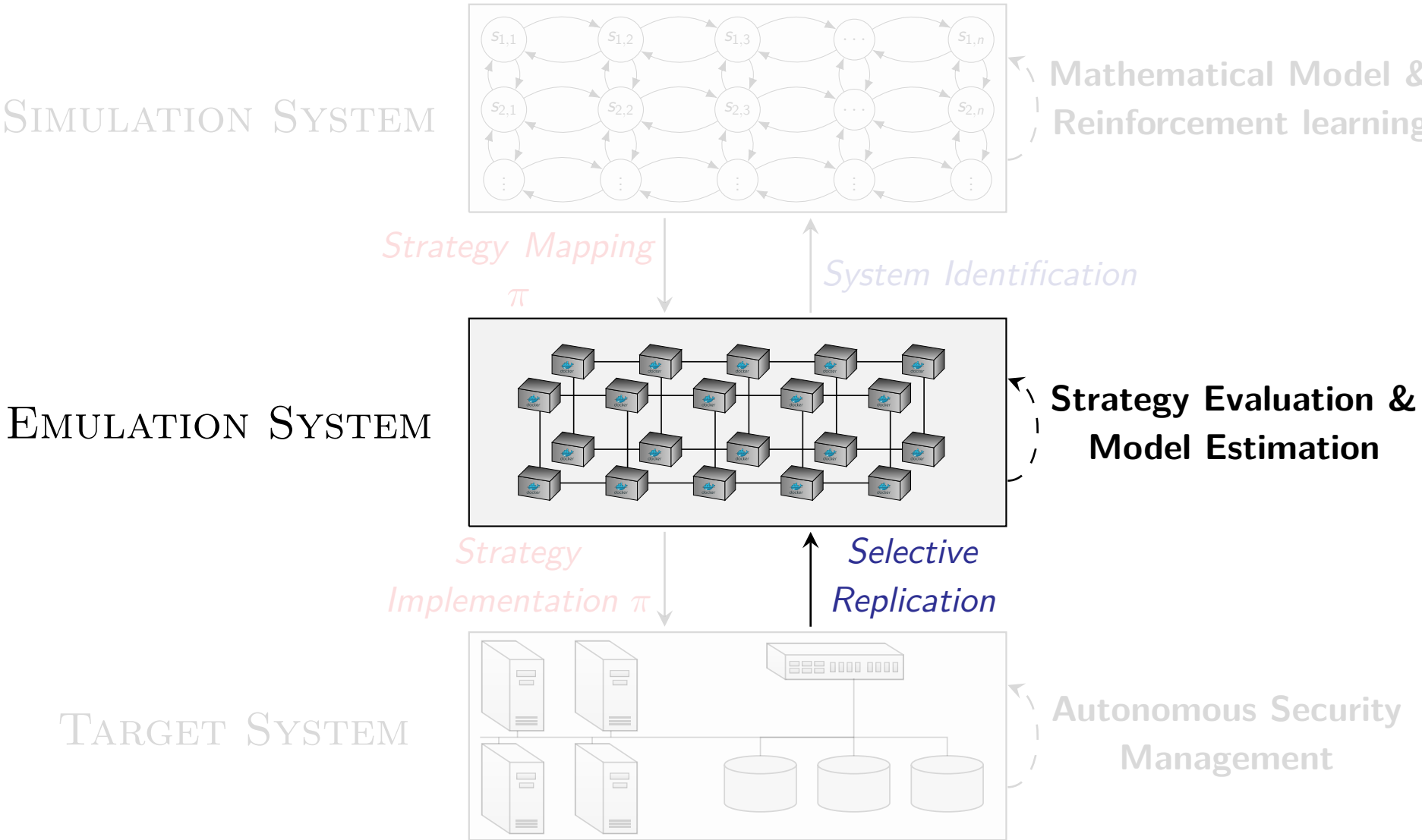
Selective Replication

Target System

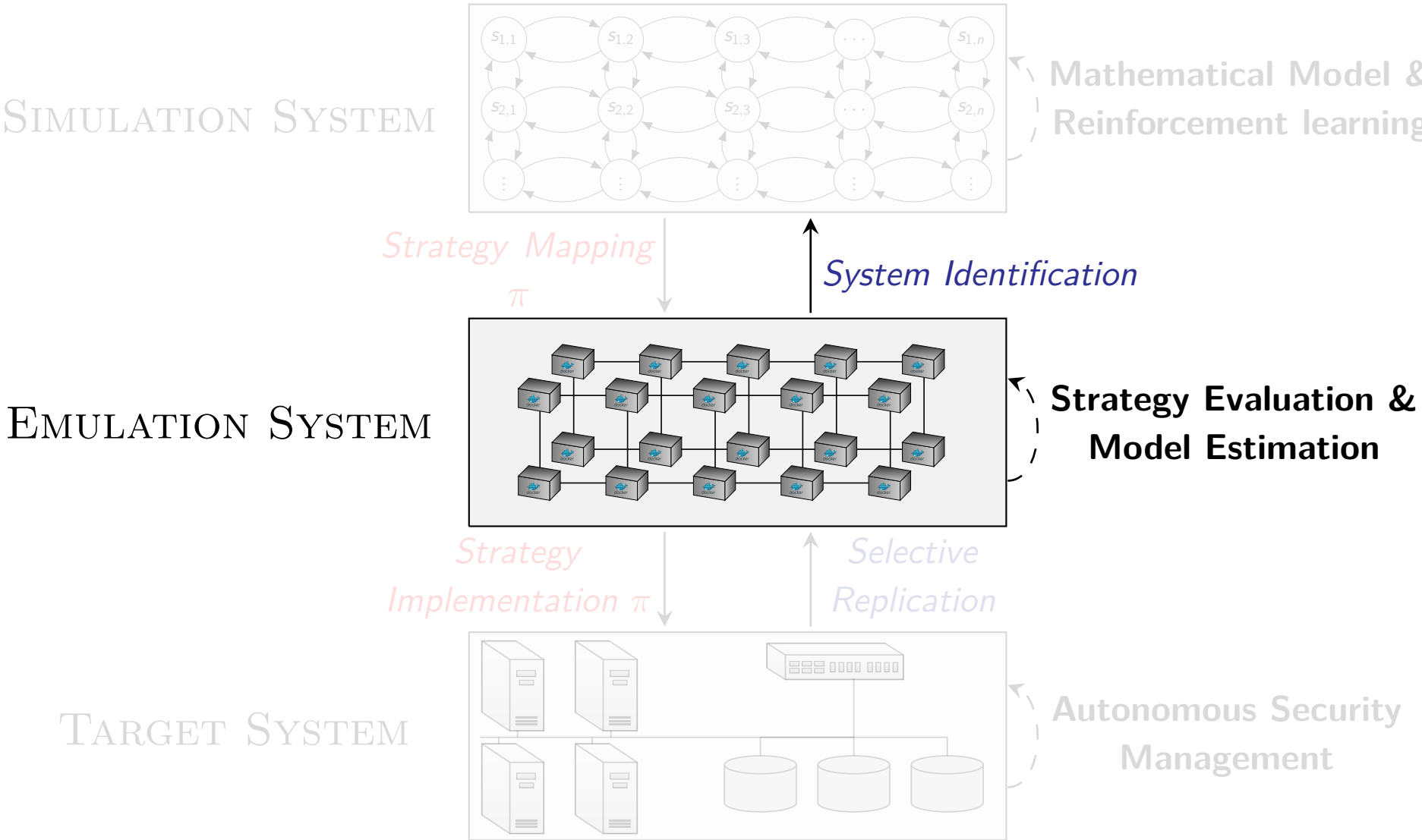


Autonomous Security Management

Methodology for Building Autonomous Security Systems

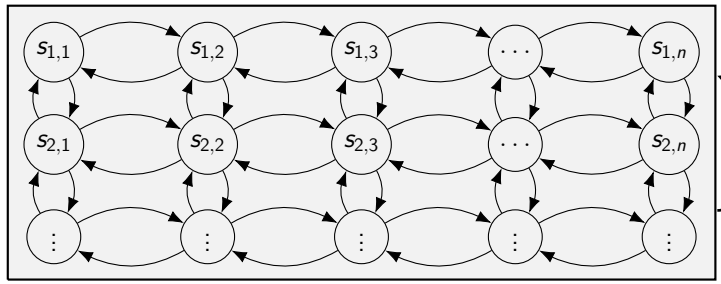


Methodology for Building Autonomous Security Systems



Methodology for Building Autonomous Security Systems

Simulation System

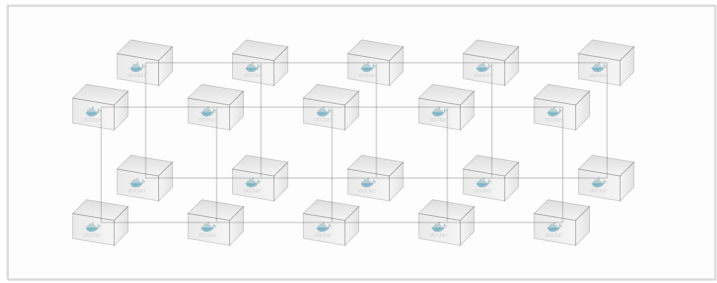


Mathematical Model & Reinforcement learning

Strategy Mapping π

System Identification

Emulation System



Strategy Evaluation & Model Estimation

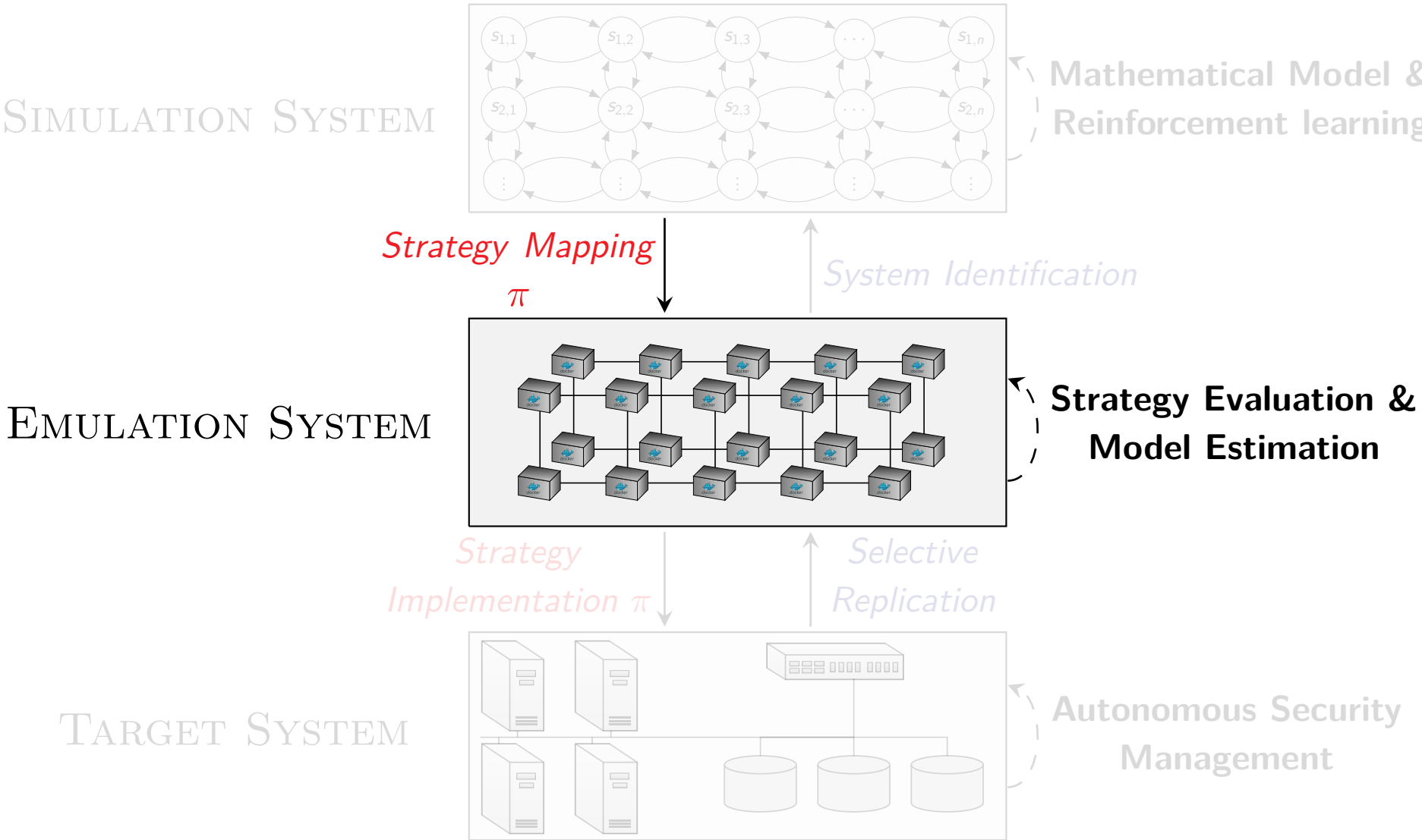
Strategy Implementation π

Selective Replication

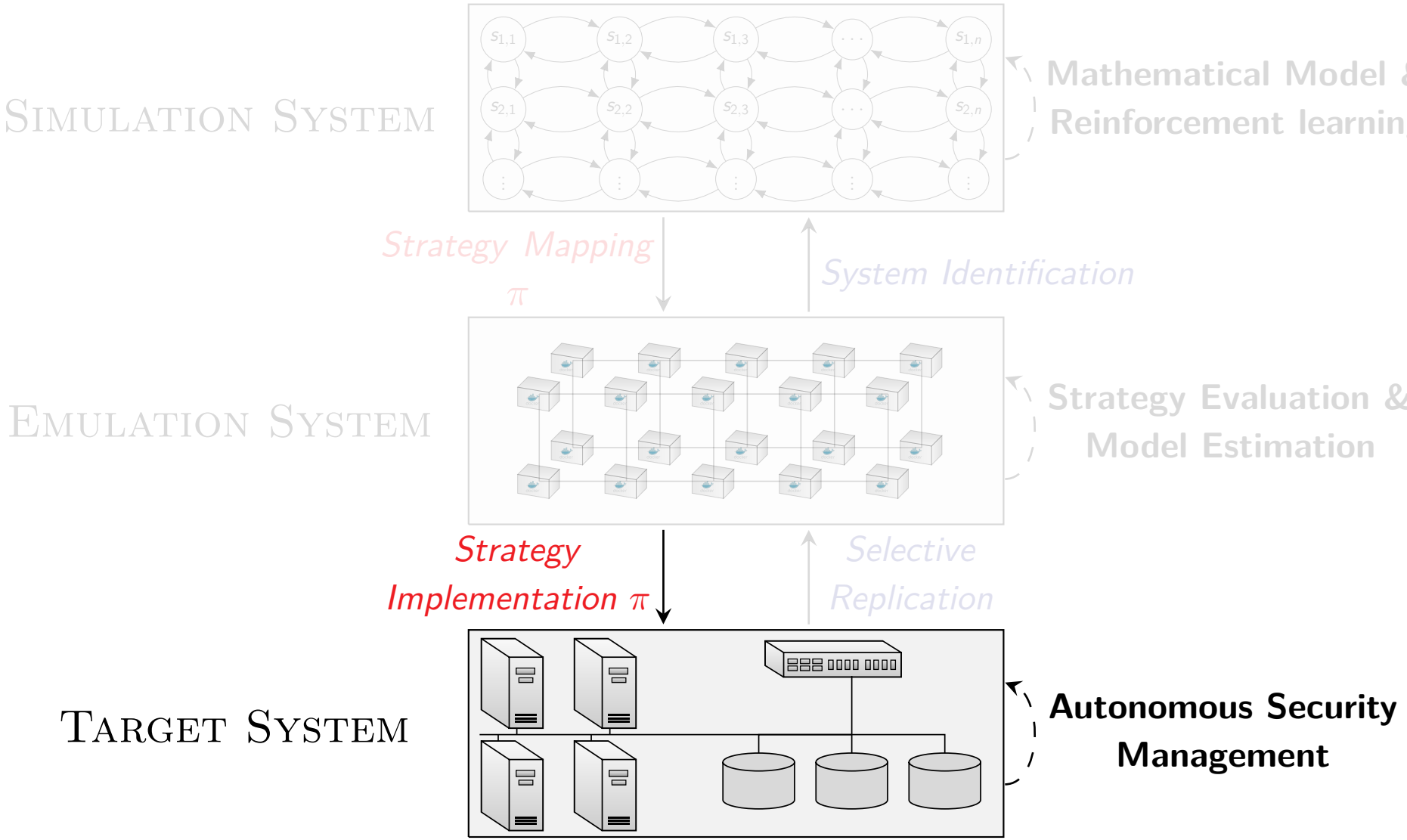
Target System

Autonomous Security Management

Methodology for Building Autonomous Security Systems

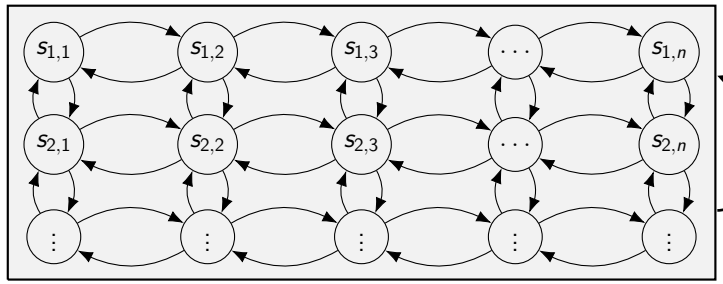


Methodology for Building Autonomous Security Systems



Methodology for Building Autonomous Security Systems

Simulation System

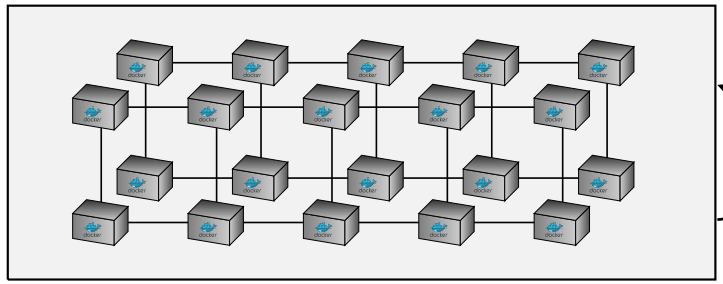


Mathematical Model & Reinforcement learning

Strategy Mapping π

System Identification

Emulation System

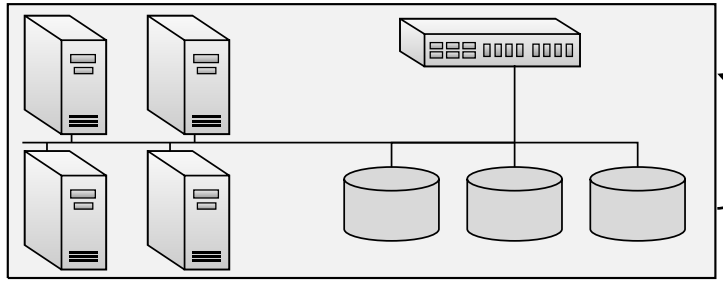


Strategy Evaluation & Model Estimation

Strategy Implementation π

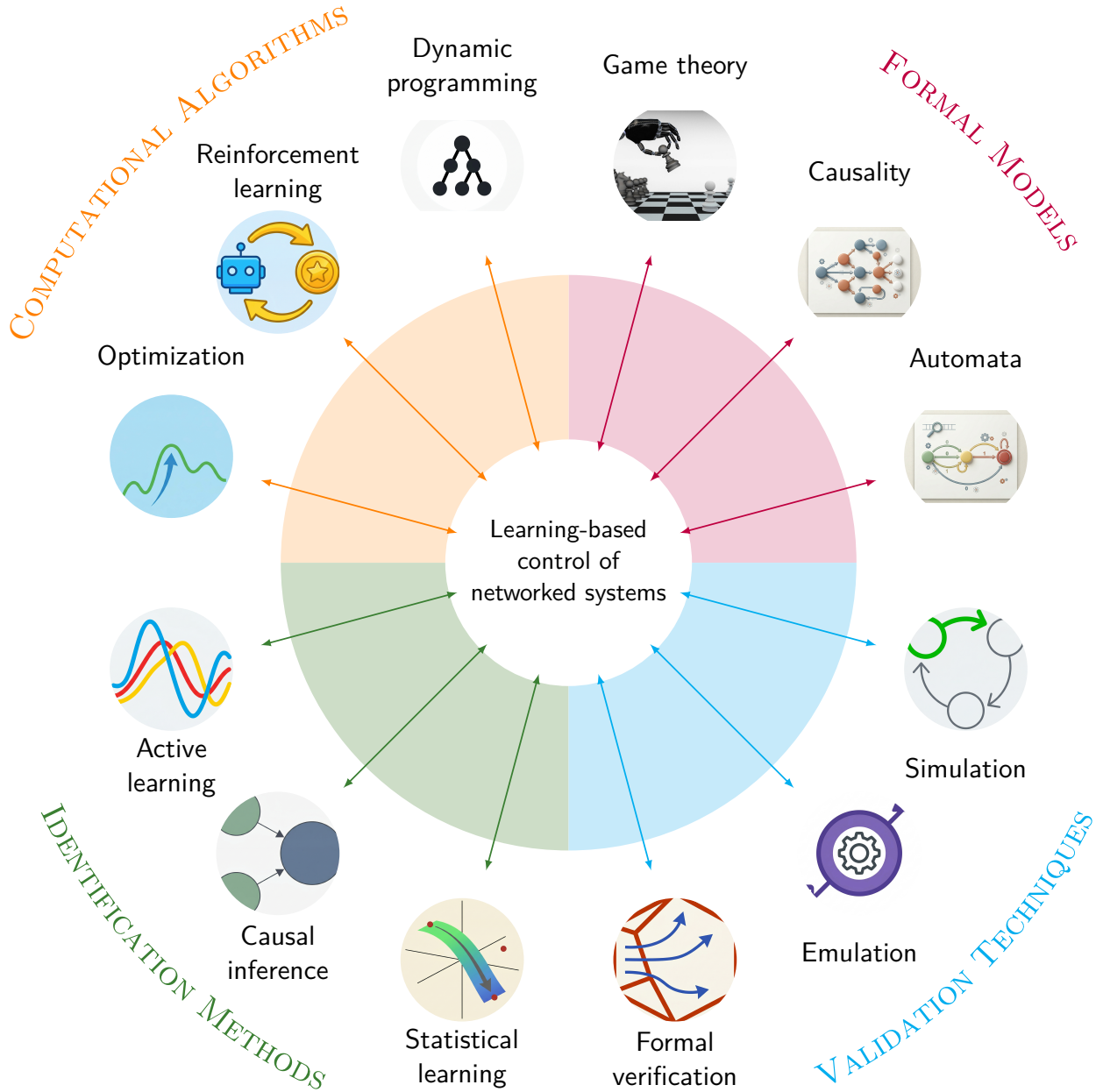
Selective Replication

Target System



Autonomous Security Management

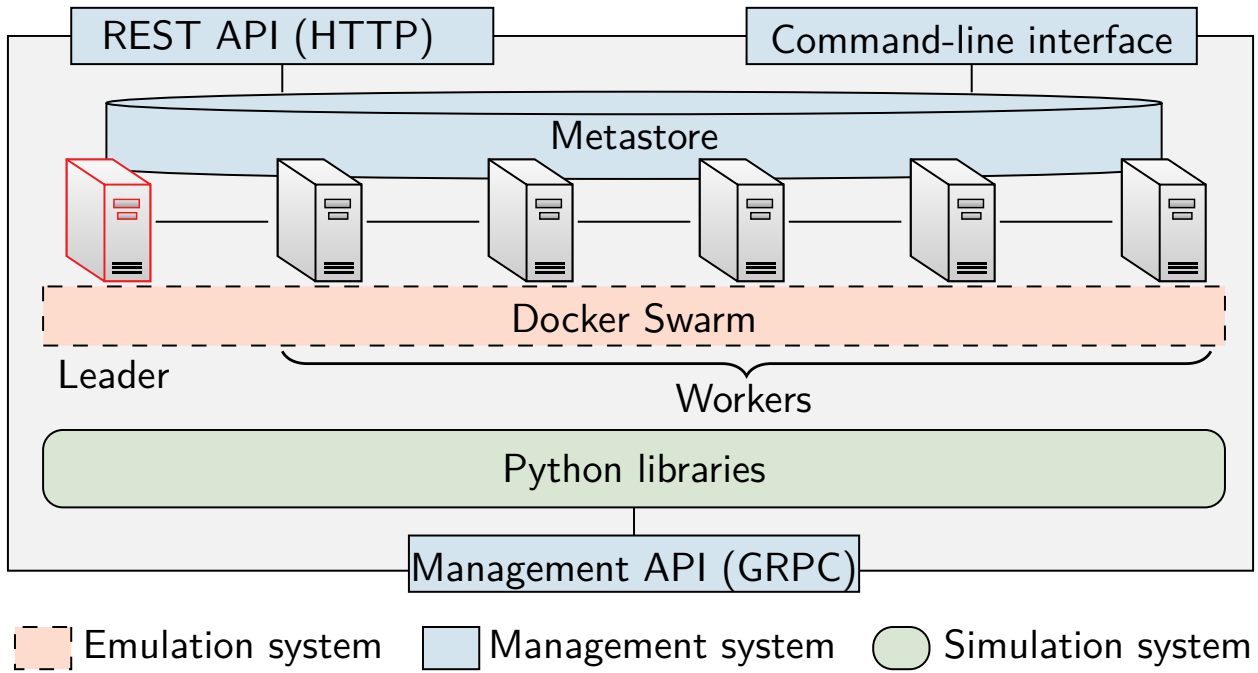
Foundations



CSLE: A Platform that Supports the Methodology

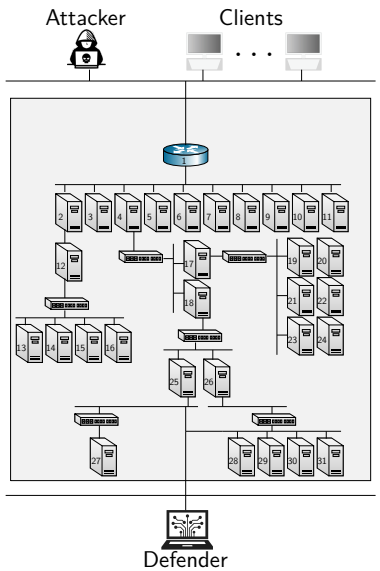
- The Cyber Security Learning Environment (CSLE) enables experimentation with reinforcement learning for autonomous security management under realistic conditions.
- Open source: `https://github.com/Kim-Hammar/csle`.

- The implementation of CSLE consists of three systems:
  - An emulation system for creating digital twins.
  - A simulation system for reinforcement learning.
  - A management system for orchestration.

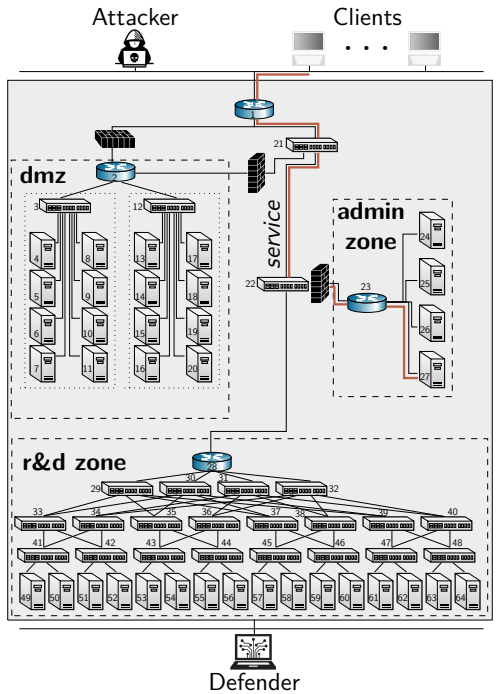


Example Use Cases for Experimental Evaluation

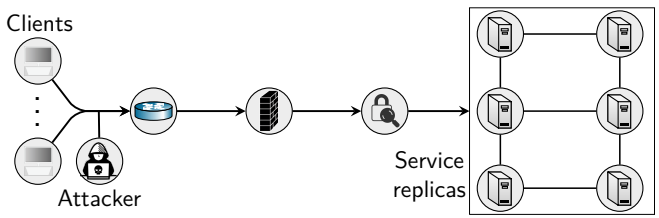
- We demonstrate the methodology through four use cases.
  - **Flow control**: block network flows to mitigate intrusions.
  - **Segmentation control**: direct network flows or create network zones to mitigate intrusions.
  - **Recovery control**: Decide when to recover components in a replicated system to maintain service availability.
  - **Replication control**: Select the number of replicas.



a) Target system for the flow control use case.



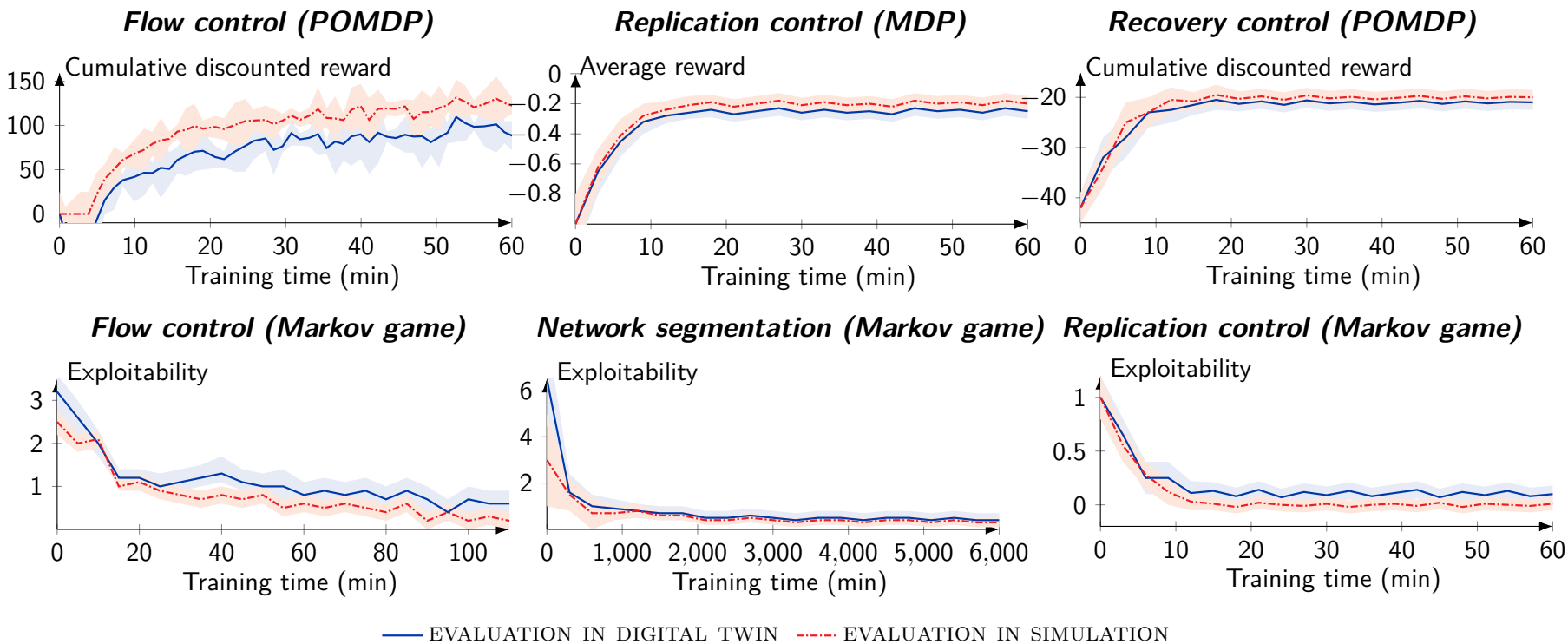
b) Target system for the segmentation use case.



c) Target system for the replication and recovery use cases.

Experimental Evaluation

- **Evaluation metrics:**
  - Reward for decision-theoretic models (↑ better).
  - Exploitability for game-theoretic models. (↓ better).



Performance on the simulator transfers to the digital twin.

Conclusion

- Networked systems grow increasingly complex and dynamic.
  - Require autonomous management and control.

- I advocate for a **learning-based control methodology**.
  - Identification of a system model.
  - Control optimization through learning-based methods.
  - Validation on a digital twin.