Synergy: Collaborative Research: Security and Privacy-Aware Cyber-Physical Systems

Insup Lee, University of Pennsylvania (lee@upenn.edu)
Miroslav Pajic, Duke University (miroslav.pajic@duke.edu)
Kang G Shin, University of Michigan (kgshin@umich.edu)

2015 CPS PI MEETING

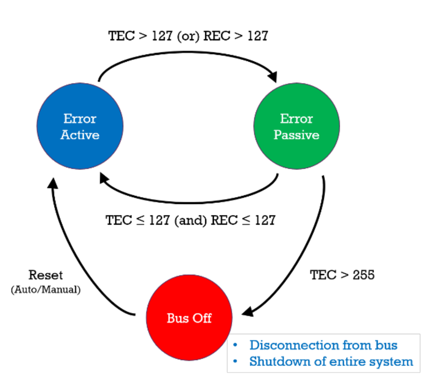
Platform support for security

Attack Model: "Bus-off Attack"

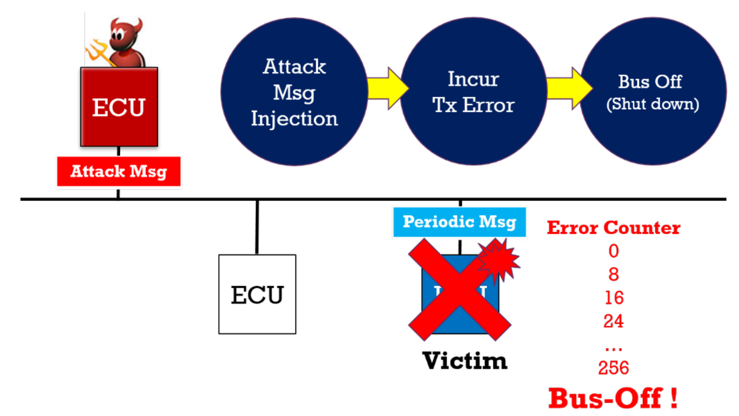
- Attacker's objective is to shut down or disconnect uncompromised (healthy) in-vehicle ECUs with minimal number of injections.

How to shut down the victim ECU?

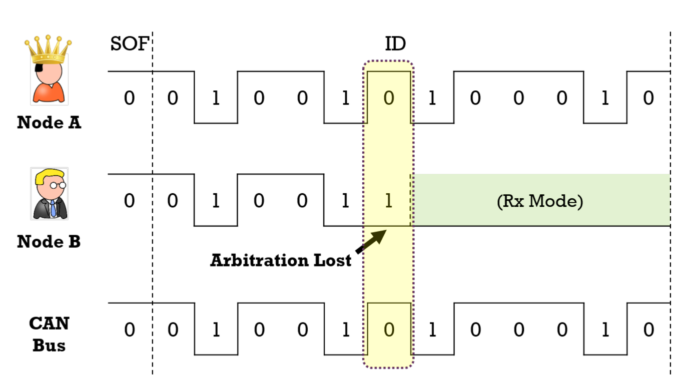
- Exploit the error handling mechanism in CAN and deceive the victim into thinking it is erroneous while is actually under attack.



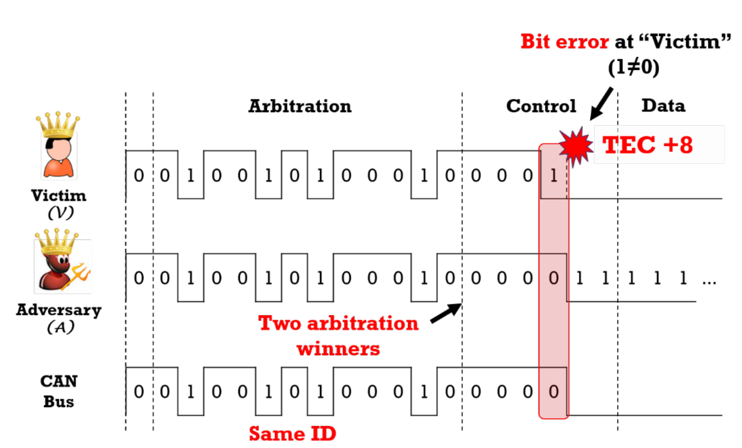
CAN Error Handling Mechanism



Bus-off Attack



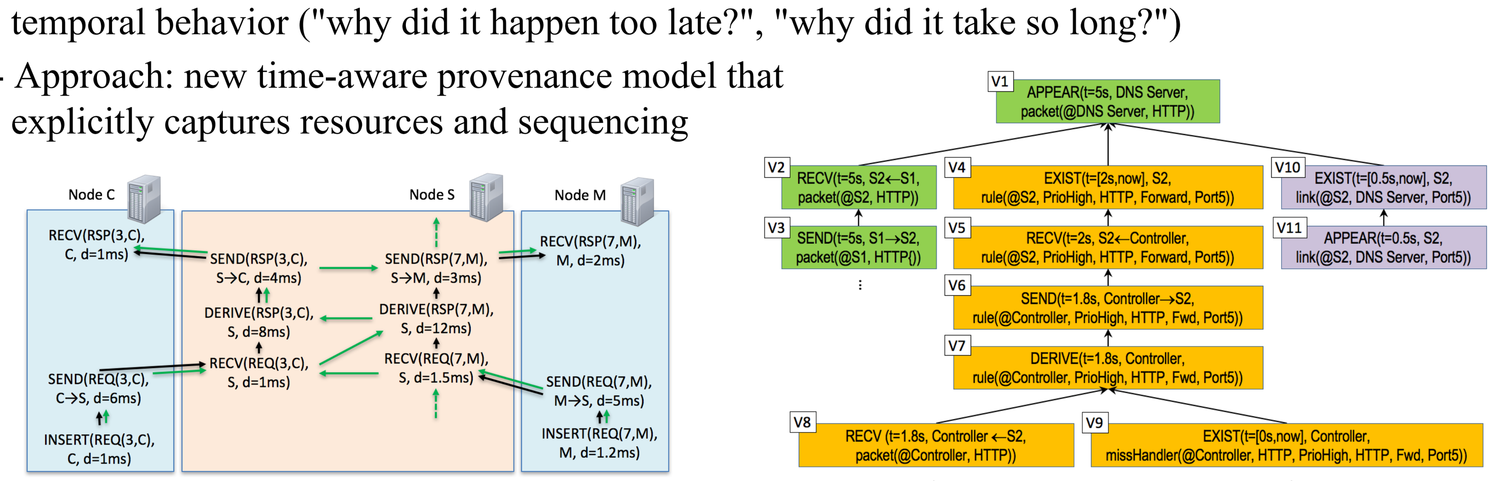
Only ONE arbitration winner !



But in the bus-off attack… TWO arbitration winners

How do we figure out what happened?

- Goal: System should be able to 'explain' to a forensic investigator why a given event occurred
- Idea: adapt the concept of data provenance from the database literature
- Problem: existing solutions only explain functional behavior ("why did this happen?") but not temporal behavior ("why did it happen too late?", "why did it take so long?")
- Approach: new time-aware provenance model that explicitly captures resources and sequencing



Modeling Human Factors

***Problem*:**

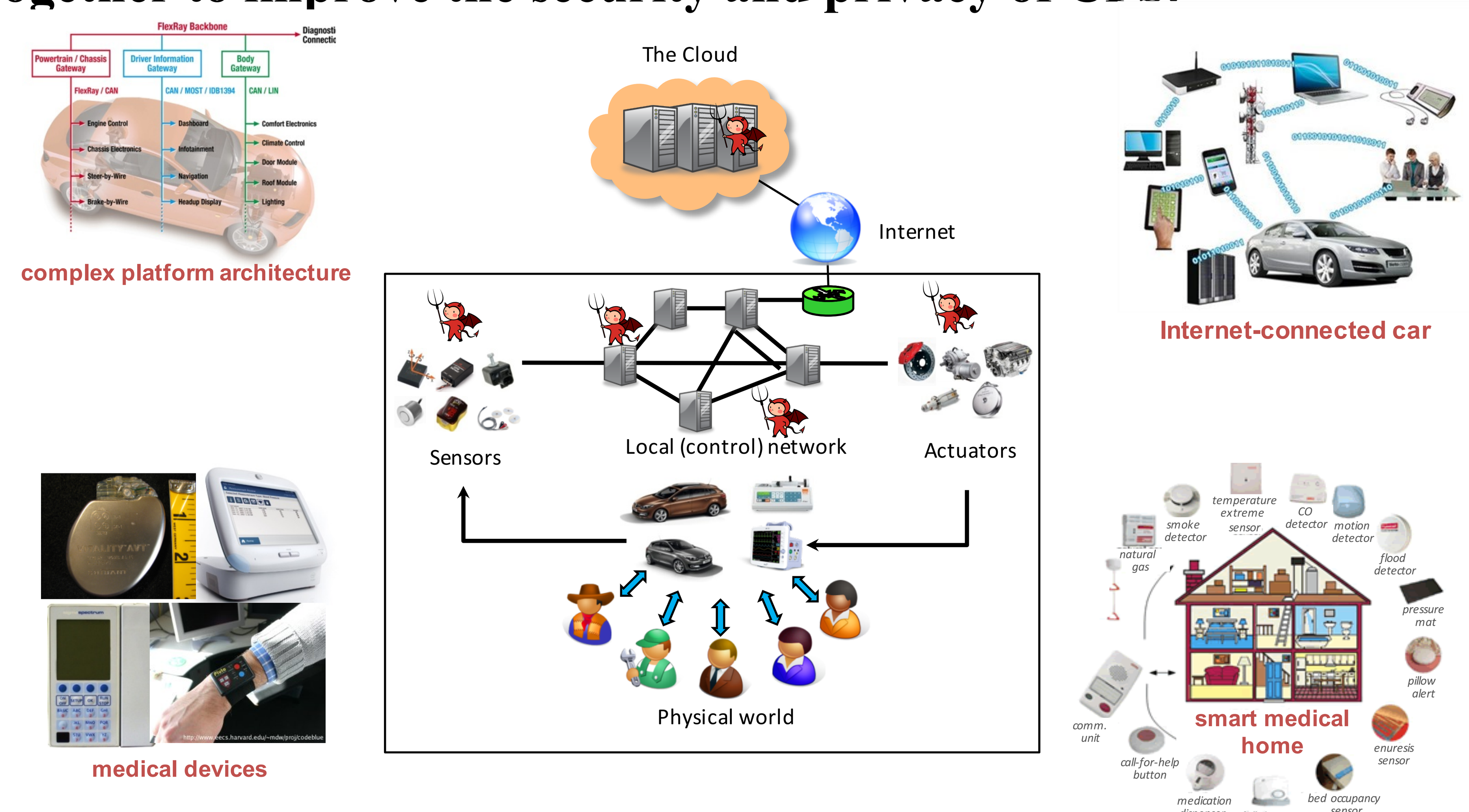
Users resort to workarounds when they feel that security features of a system prevent them from doing their work. How can we predict workarounds and analyze their effects?

***Approach*:**

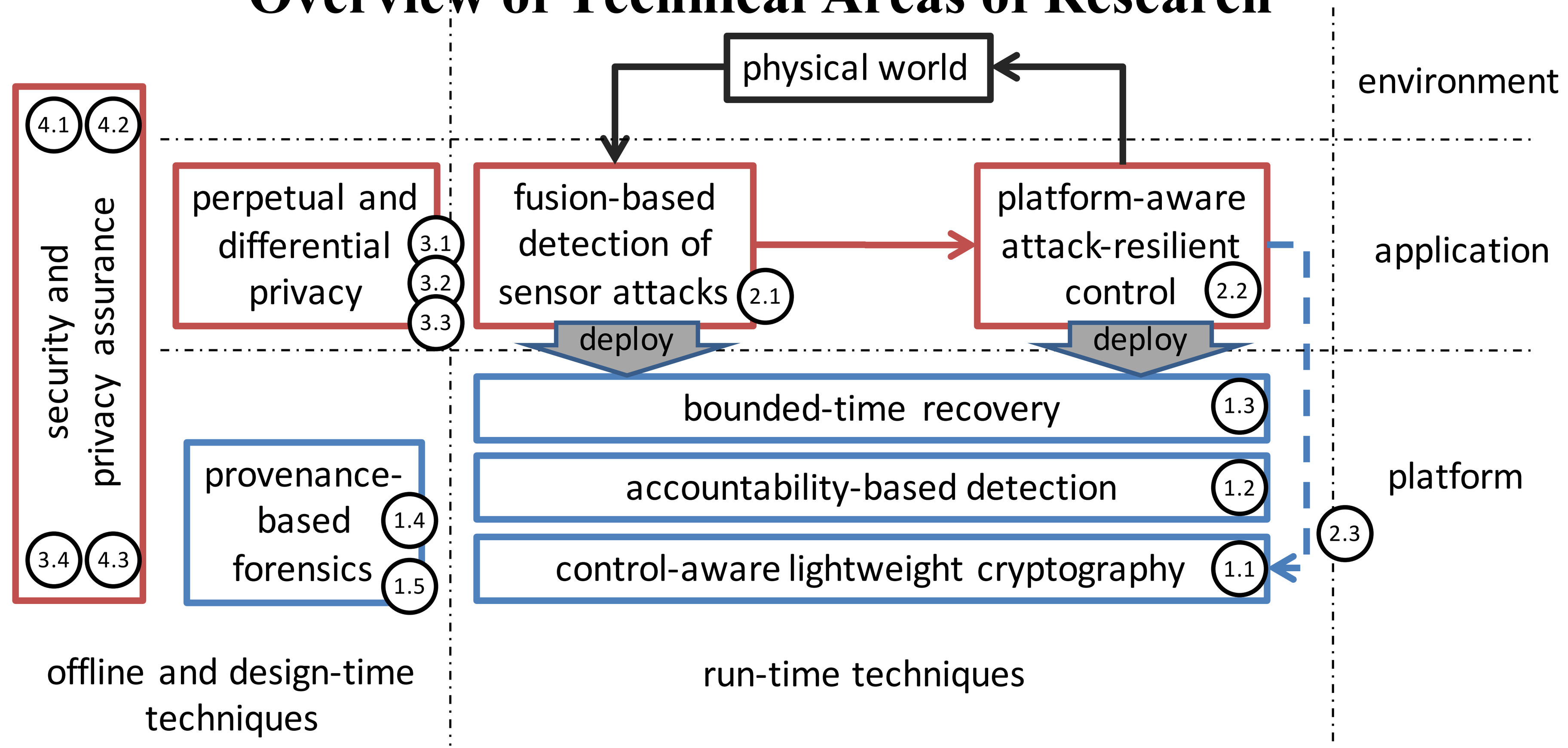
- Model potential workarounds as hazards and apply risk analysis
- Incorporate users' mental models into model-based design of CPS

Project Overview

***Goals of the project*: to develop a framework in which the mix of prevention, detection, recovery and robust techniques work together to improve the security and privacy of CPS.**



Overview of Technical Areas of Research

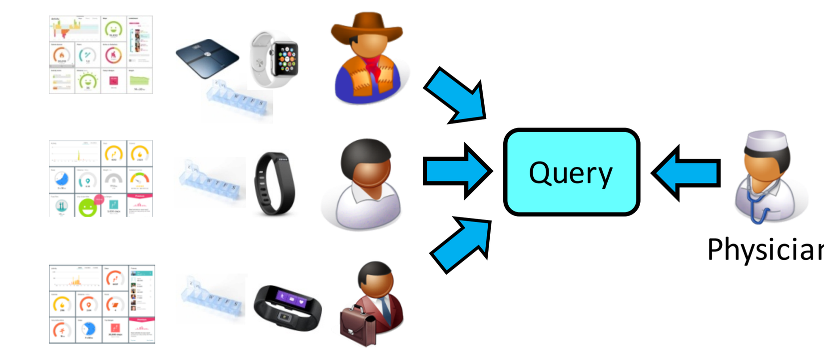


Team

Insup Lee (PI, Penn)	Miroslav Pajic (Duke)	Kang G. Shin (Michigan)
Andreas Haeberlen (Penn)	George Pappas (Penn)	Oleg Sokolsky (Penn)
Bill Hanson (UPHS)	Linh Phan (Penn)	Jeffrey Vagle (Penn)
Nadia Heninger (Penn)	Rita Powell (Penn)	Christopher Yoo (Penn)
Ross Koppel (Penn)		Jesse Walker (Intel)

This Project is supported by NSF CNS-1505799 and Intel-NSF Partnership for Cyber-Physical Systems Security and Privacy. https://rtg.cis.upenn.edu/cps-security

Working with Sensitive Data



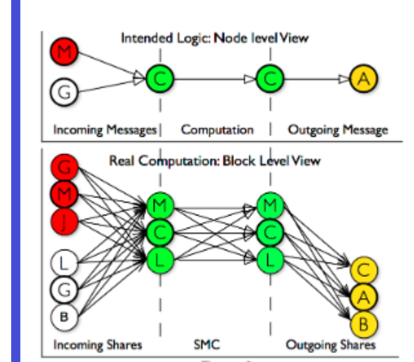
Who	What
Bob	Drug A
Charlie	Drug B
Fannie	Drug B
George	Drug A

Example: "Does drug X work better during rest periods, or during heavy exercise?"

***Problem*: Differential privacy guarantees for distributed systems while processing continuous data streams.**

Approaches

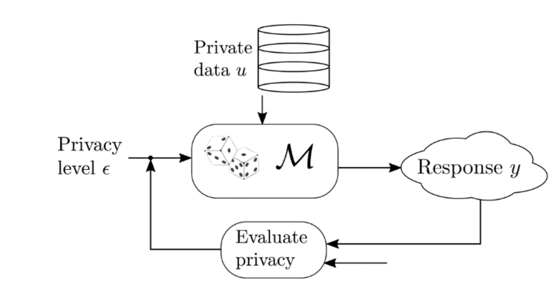
Distributed queries for differential privacy



- data never leaves user domain

Run-time differential privacy

A privacy-preserving mechanism that allows online relaxing privacy.



Security-Aware Control Design Attacks on Control Systems

Attack-Resilient State Estimation for Noisy Dynamical Systems

$$P_{0,\omega}: \min_{\bar{\mathbf{e}},\mathbf{x}} \|\bar{\mathbf{e}}\|_{l_2,l_0} \qquad P_{1,\omega}: \min_{\bar{\mathbf{e}},\mathbf{x}} \|\bar{\mathbf{e}}\|_{l_2,l_1}$$

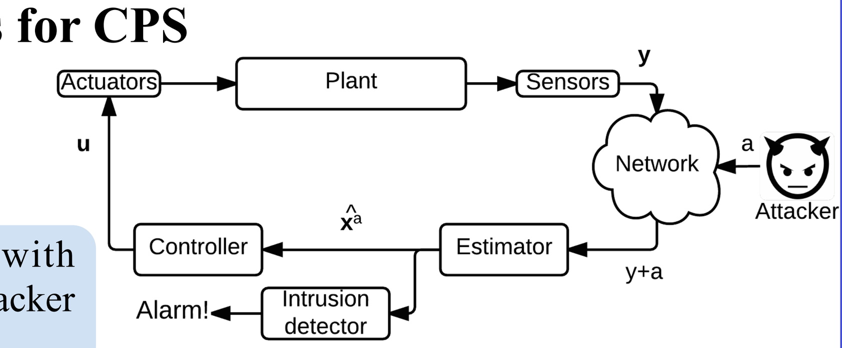
$$s.t. \quad \tilde{\mathbf{y}} - \mathbf{O}\,\mathbf{x}_0 - \bar{\mathbf{e}} = \bar{\mathbf{w}}, \quad \bar{\mathbf{w}} \in \Omega$$

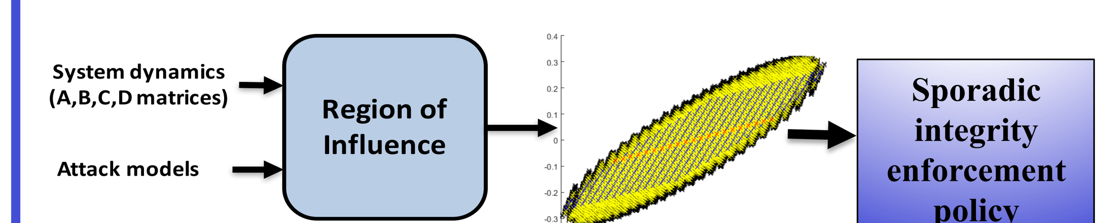
Formal robustness guarantees for the optimal l_0 and convex l_1 estimator

Relaxing Integrity Requirements for CPS

Sporadic integrity enforcement: If at step k, sensor integrity is enforced (e.g., with the use of MAC), then $\mathbf{a}_{\downarrow k} = 0$.

Theorem [Jovanov&Pajic'16]: Even with sporadic sensor integrity enforcement, the attacker cannot introduce unbounded estimation error.



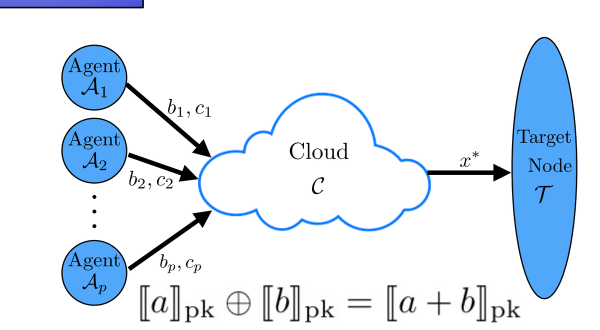


Limiting attack effects: Trajectory following study – attack induced estimation error < 5 cm when <20% of CAN packets contain MAC

Optimization and Control using Partially Homomorphic Encryption

Privacy-aware cloud-based optimization over sensitive data:

- Agents encrypt information before sending to untrusted cloud
- Cloud computes optimal solution **without learning** the **sensitive data** or the **final solution**



$$[\![a]\!]_{pk} \oplus [\![b]\!]_{pk} = [\![a+b]\!]_{pk}$$