TerraSwarm

An Architectural Mechanism for Resilient IoT Services

Hokeun Kim[1], **Eunsuk Kang**[1], David Broman[2], Edward A. Lee[1]

[1]University of California, Berkeley

[2]KTH Royal Institute of Technology

SafeThings 2017

November 5, 2017

Sponsored by the TerraSwarm Research Center, one of six centers administered by the STARnet phase of the Focus Center Research Program (FCRP) a Semiconductor Research Corporation program sponsored by MARCO and DARPA.

Safety and Security of the IoT

- Safety & Security: No longer separate issues!


Light Blue Touchpaper
Security Research, Computer Laboratory, University of Cambridge

Home About the site Security Group

When safety and security become one

2017-06-01 Academic papers, Legal issues, Open-source security, Operating systems, Security economics, Security engineering Ross Anderson

What happens when your car starts getting monthly upgrades like your phone and your laptop? It's starting to happen, and the changes will be profound. We'll be able to improve

https://www.lightbluetouchpaper.org/2017/06/01/when-safety-and-security-become-one/


Tesla's 8.1 software update brings Autopilot 2.0 cars up to speed

Posted Mar 29, 2017 by Darrell Etherington (@etherington)

https://techcrunch.com/2017/03/29/teslas-8-1-software-update-brings-autopilot-2-0-cars-up-to-speed/

Availability and Safety

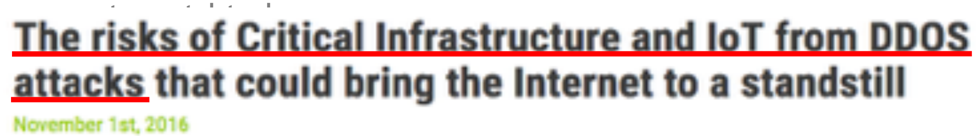
- Shutting down critical IoT services can cause disastrous problems!
  - Power grids
  - Hospitals
  - Transportation
  - many more…


Is critical infrastructure the next DDoS target?

A massive Distributed Denial of Service attack shut down a portion of the internet recently. Experts say it is unlikely a similar attack could take down the grid or other critical infrastructure but acknowledge that security remains weak in the industry

By Taylor Armerding

http://www.csoonline.com/article/3141601/critical-infrastructure/is-critical-infrastructure-the-next-ddos-


The risks of Critical Infrastructure and IoT from DDOS attacks that could bring the Internet to a standstill

November 1st, 2016

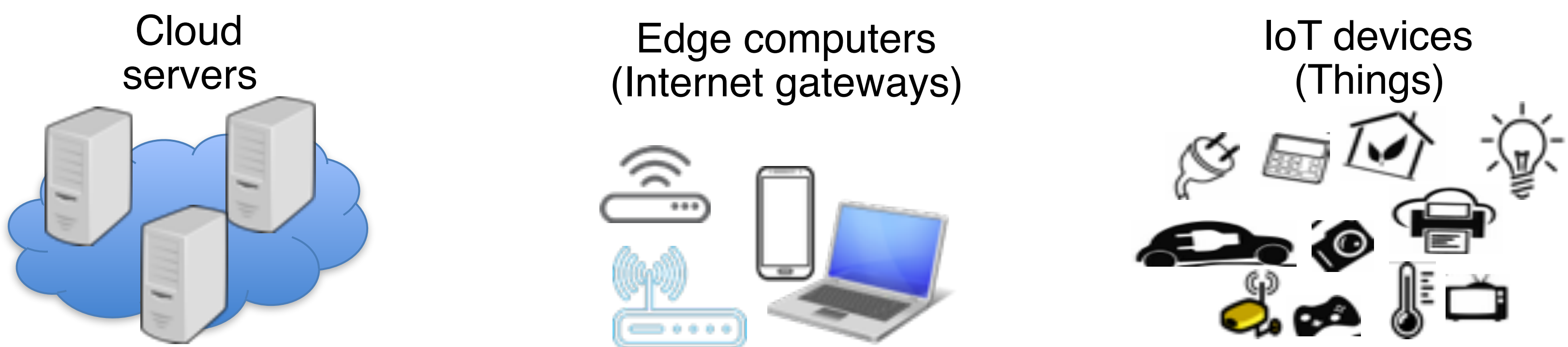
https://thycotic.com/company/blog/2016/11/01/the-risks-of-critical-infrastructure-and-iot-from-ddos-attacks-that-could-bring-the-internet-to-a-standstill/

Research Question

How do we design an IoT network to be resilient against availability & other types of attacks?

Cloud & Edge Computing

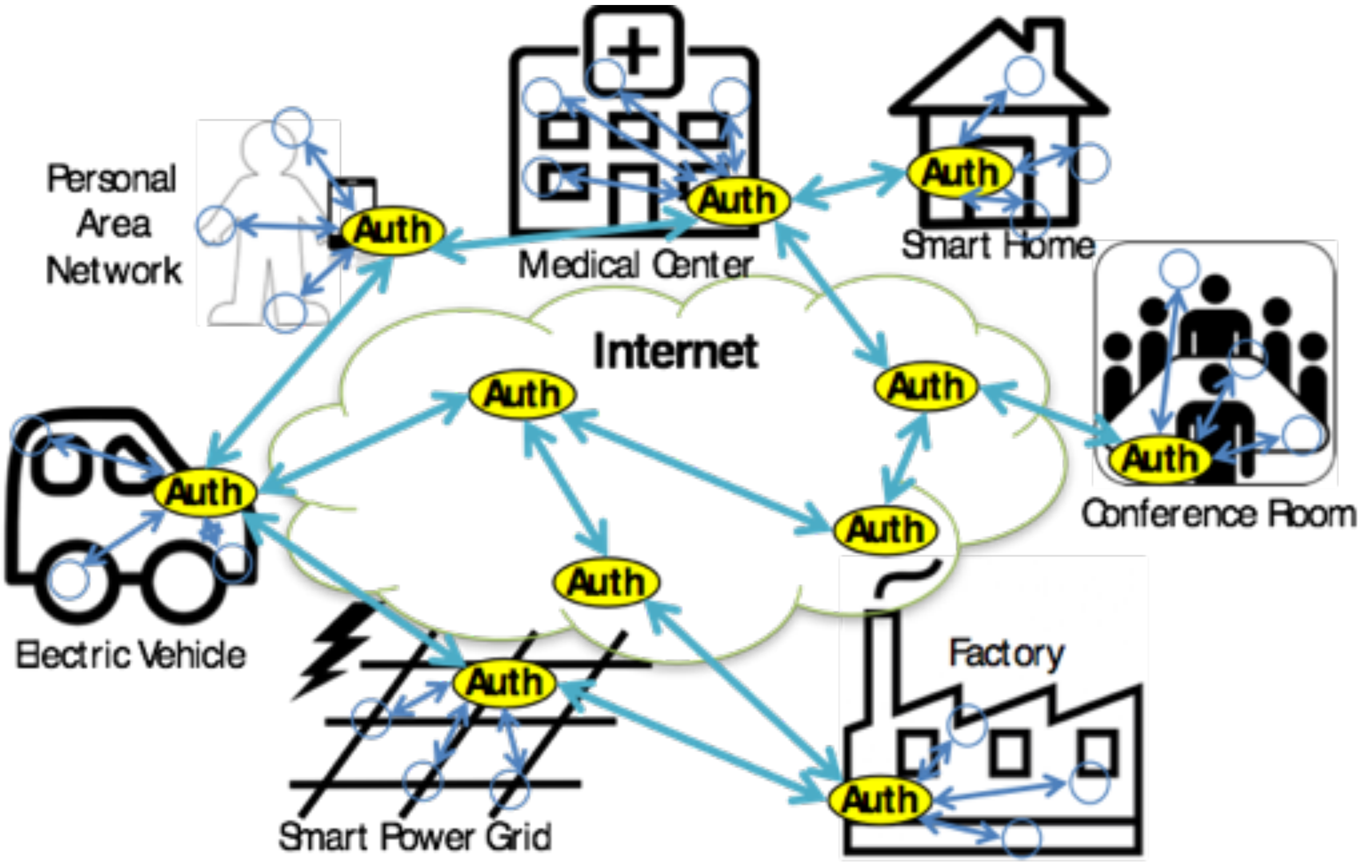
- Many existing IoT solutions are based on clouds
- Alternative emerging architecture: **Edge Computing**



Cloud servers		IoT devices
More available resources	←	Restricted resources
Higher latency Less stable connections	→	Better connectivity Lower latency
More challenging to guarantee data privacy	→	Greater control over data
Limited context awareness (of local system)	→	Better context awareness (of local system)

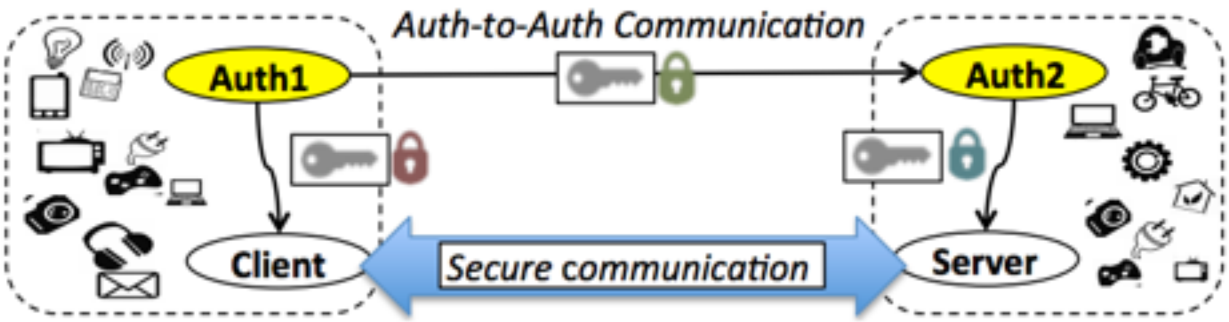
Secure Swarm Toolkit (SST)

- Locally centralized, globally distributed architecture



SST Overview

- **Auth**
  - Software solution deployed on edge devices
  - Local authentication/authorization entity
  - Responsible for authorization of local Things through key distribution
  - Manages trust relationship with other Auths



Challenges in Securing the IoT

- Authentication/Authorization
- Heterogeneity
- Open environment
- Scalability
- Availability

Addressed our previous work [*]

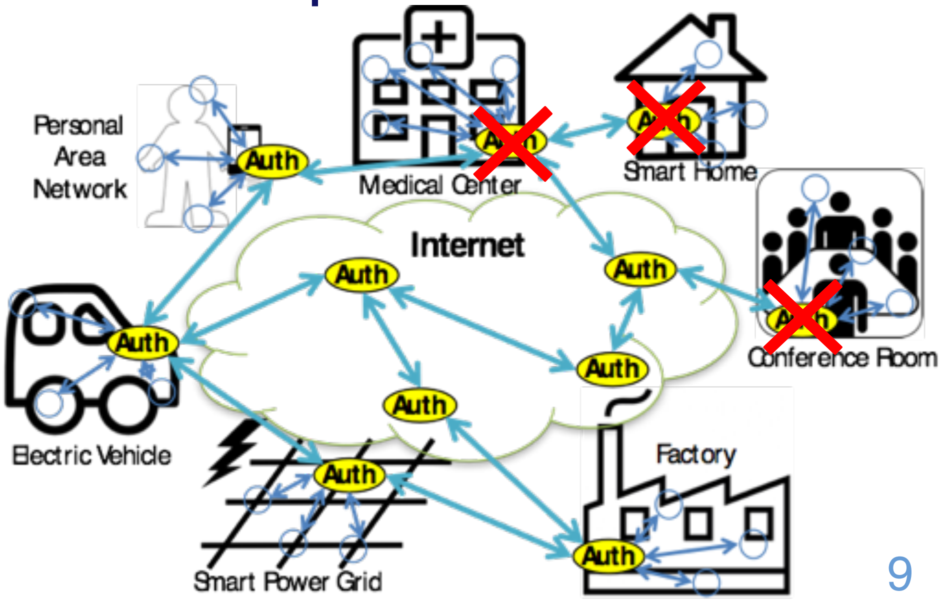
Addressed in this paper

[*] “A Toolkit for Construction of Authorization Service Infrastructure for the Internet of Things”, ACM/IEEE IoTDI ’17, CPSWeek

Threat Model

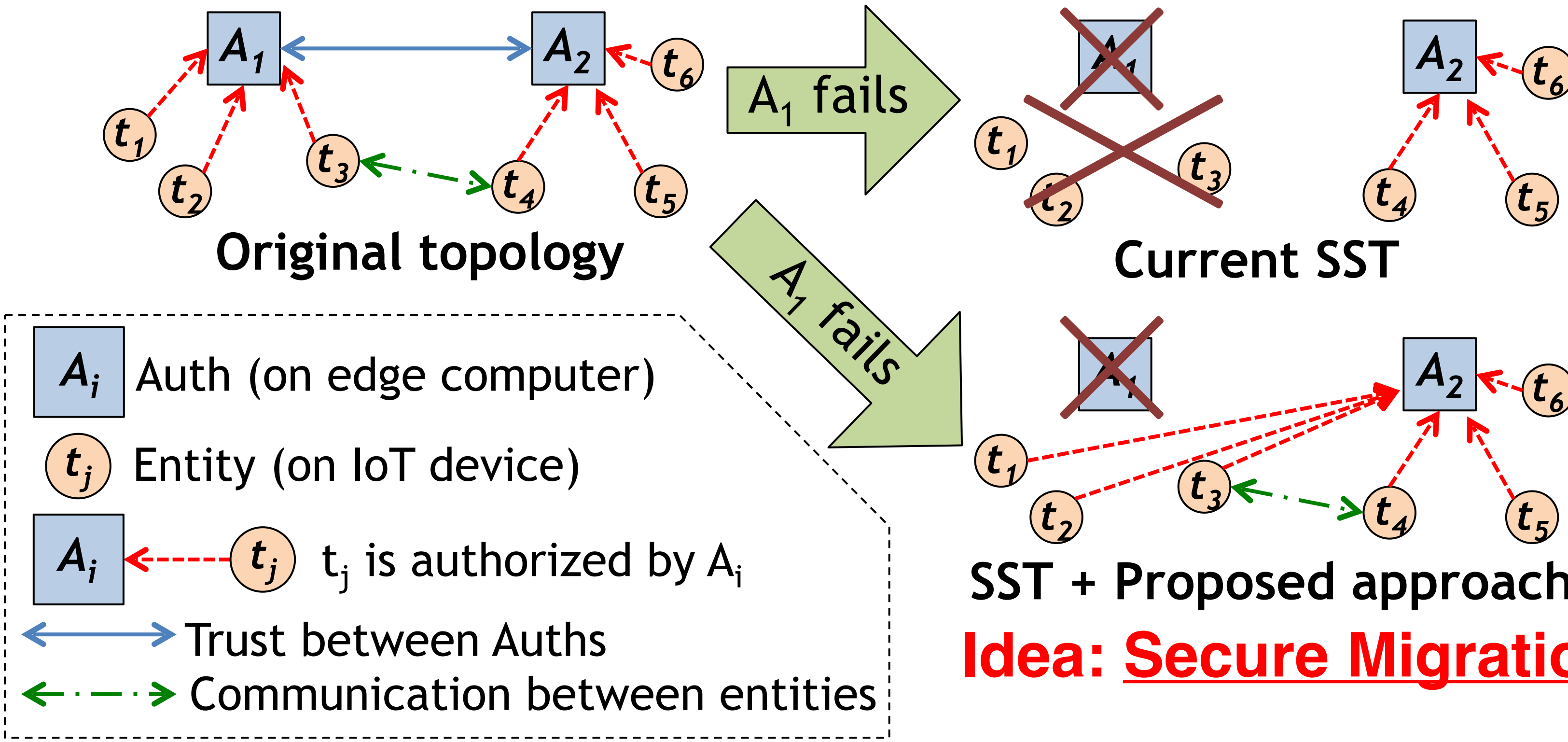
- Attacker Capabilities
  - Disrupt IoT services by targeting edge devices
  - DoS attacks (packet flooding, etc.,)
- Assumption
  - Some <u>subset</u> of edge devices exposed to attacker

Our Goal
Provide services to Things even in the presence of attacks on some Auths



Proposed Approach

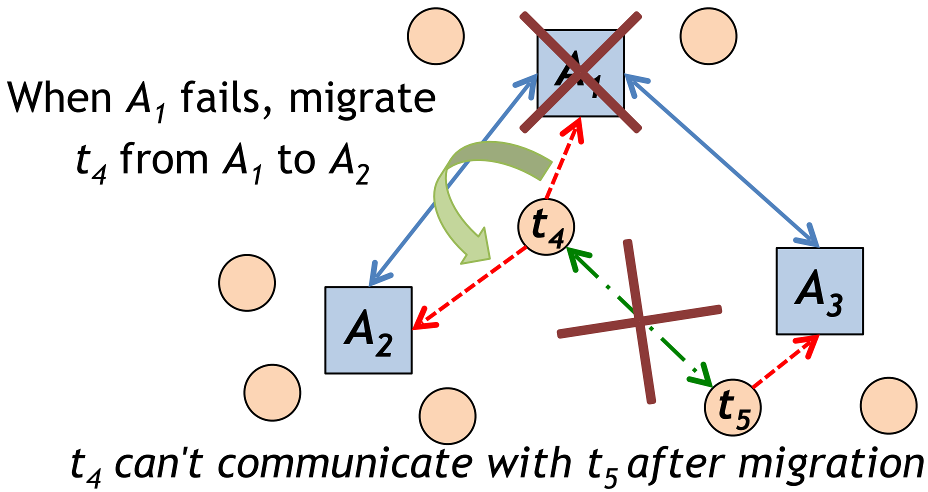
- A trusted Auth takes over authorization tasks of a failed Auth

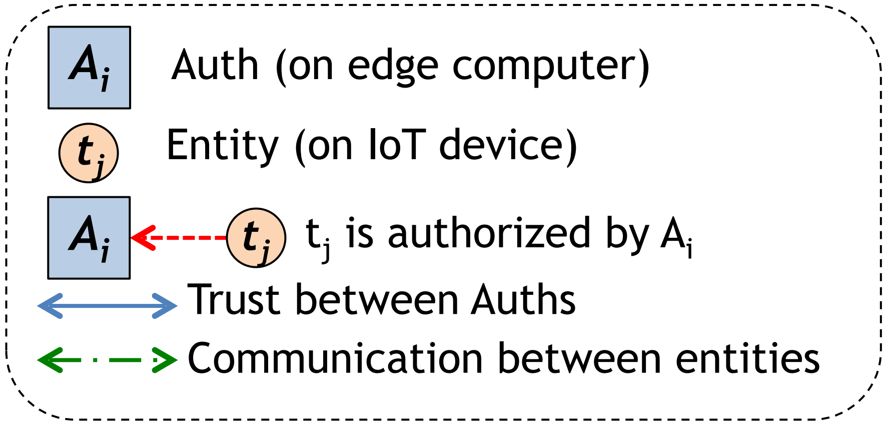


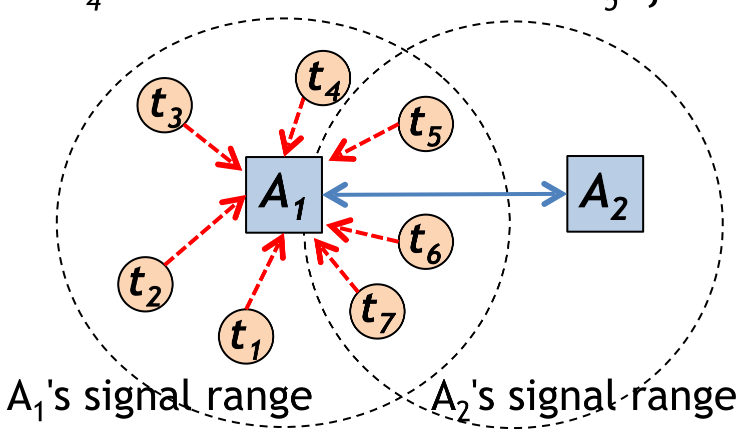
Idea: Secure Migration

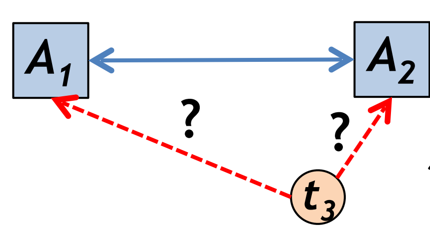
Migration Policies

- Which Auth should each Thing be migrated to?
- Non-trivial! Hard constraints & alternative costs









- Which Auth is directly reachable through wireless communication?
- Is Auth equipped with HW security support (e.g., TPM or Intel SGX)?
- Is Auth located in a restricted-access area?

Migration Policy Construction as ILP

- Computing a migration policy as an optimization problem!

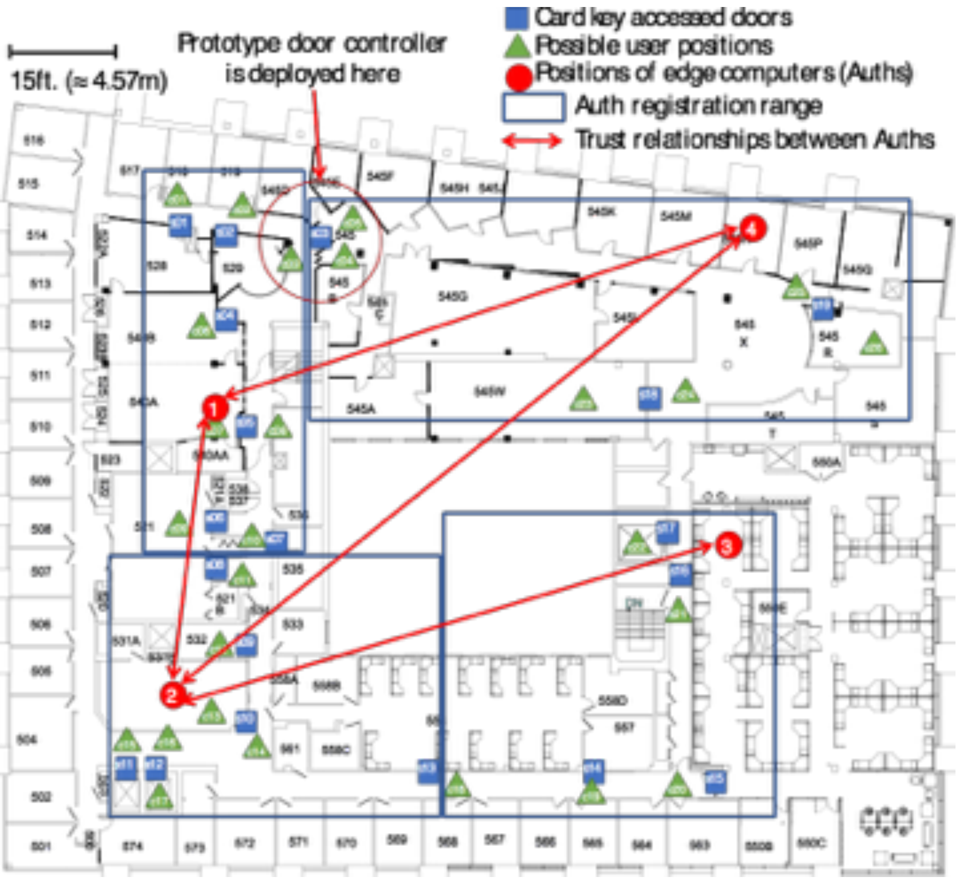
$$\begin{array}{ll} \text{minimize} & c^T x \\ \text{subject to} & Ax \leq b \end{array}$$

More details in paper!

- Formulation in Integer Linear Programming (ILP)
  - Variables: Boolean, set true if Thing X assigned to Auth Y
  - Coefficients: Communication costs
  - Constraints:
    - Thing-Thing communication requirements
    - Auth-Auth trust relationships
    - Auth capacity: Max # Things for each Auth

Preliminary Experiment

- Application: Smart Door Control through Mobile App



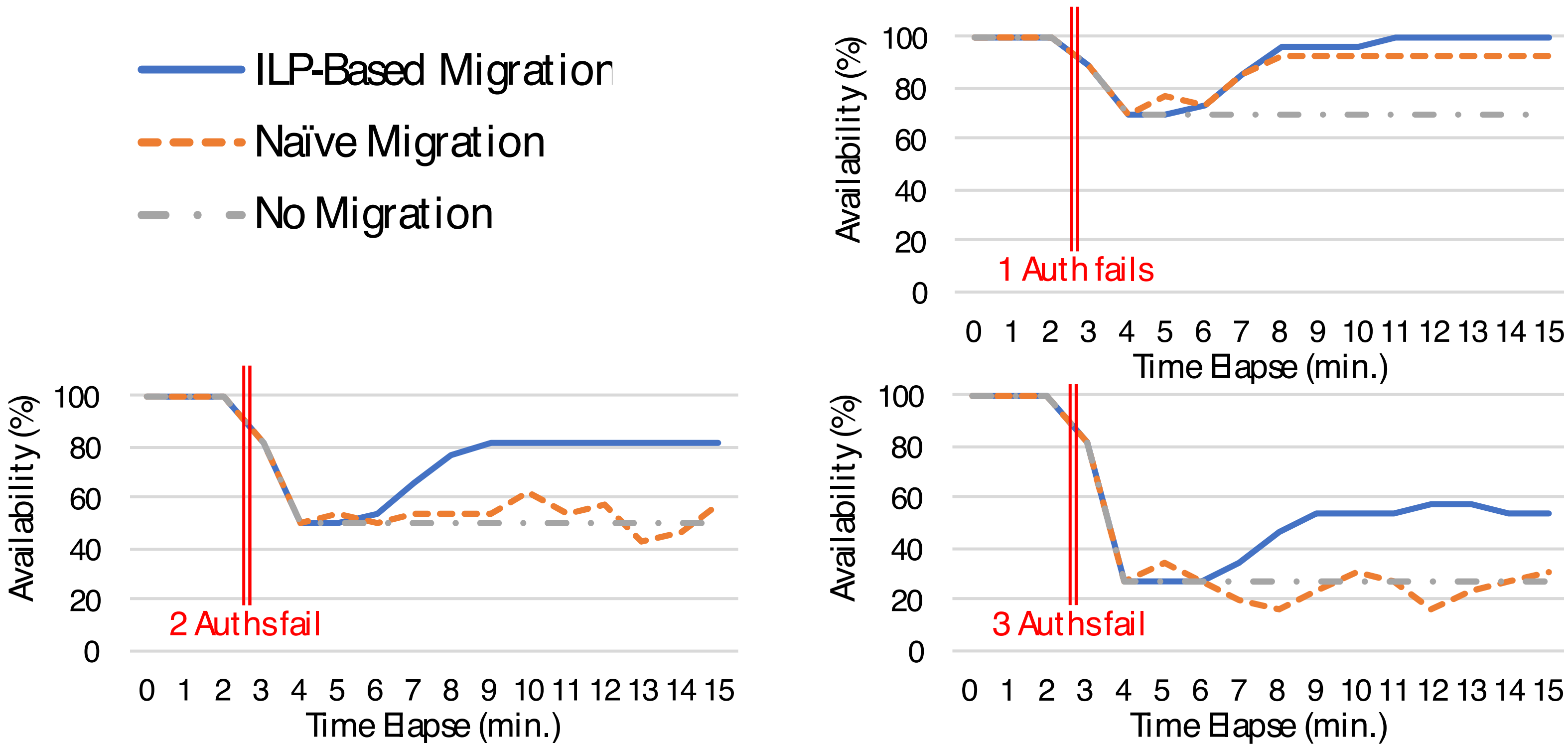
Floor map of 5th floor Cory Hall, UC Berkeley

Simulation environment:

- 4 Auths, 19 door controllers, 26 apps
- Implemented & running on Linux Containers
- ns-3 for simulating wired & wireless communication
- Gurobi as the ILP solver

Experimental Results

- Measuring availability (i.e, “open door” request accepted) when different numbers of Auths fail
  - Three different migration cases



Summary

- Edge-based architecture has certain advantages over cloud-based security solutions
- Proposed migration approach is promising for higher availability under failures of some edge computers
  - Suitable for safety-critical environments
- Computing migration policy can be formulated as an ILP problem

Future Work

- Scalability: For large networks, ILP may become too complex (on-going work)
- Hybrid solution for better availability (Auths on both clouds & edges)
- Theoretical bounds & resiliency analysis depending on network topology
- Advanced threat model
  - Selectively attack Auths to maximize damage (instead of random DoS)