THE UNIVERSITY OF BRITISH COLUMBIA

Stopping the Barbarians at the Gate: Protecting End User Devices from Security Attacks

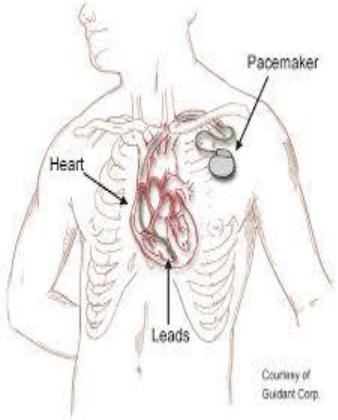
Karthik Pattabiraman

Pritam Dash, Mehdi Karimi, Farid Molazem Tabrizi, Ekta Aggarwal,

Maryam Raiyat, Amita Kamath, Julien Gascon-Samson, Andre Ivanov

University of British Columbia, Vancouver, Canada

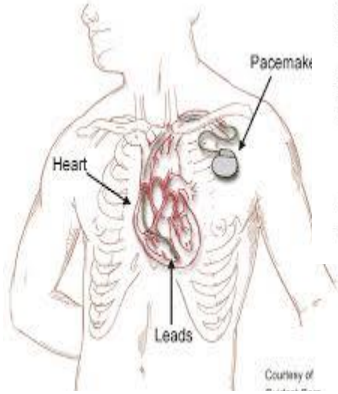
Cyber-Physical Systems (CPS): End User Devices



Cyber-Physical Systems (CPS): End User Devices

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses



Smart meters can be hacked to cut power bills

By Mark Ward
Technology correspondent, BBC News

16 October 2014 | Technology

Smart meters could help people do a better job of managing power use

Smart meters widely used in Spain can be hacked to under-report energy use, security researchers have found.

Nest Thermostat Glitch Leaves Users in the Cold

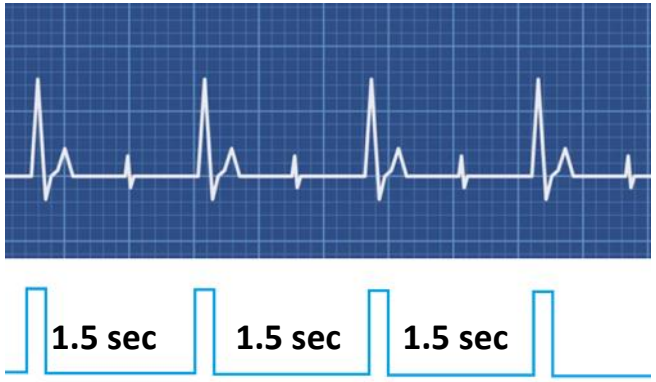
Disruptions
By NICK BILTON JAN. 13, 2016

The Nest Learning Thermostat is dead to me, literally. Last week, my once-beloved "smart" thermostat suffered from a mysterious software bug that drained its battery and sent our home into a chill in the middle of the night.

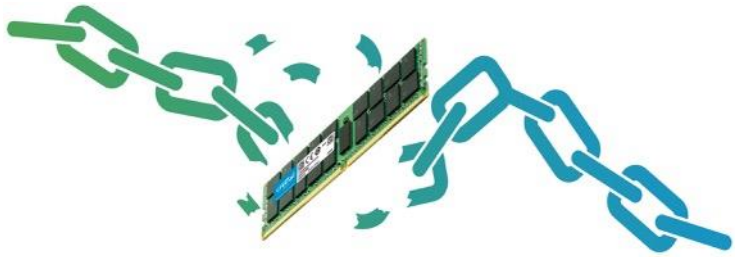
Although I had set the thermostat to 70 degrees overnight, my wife and I were woken by a crying baby at 4 a.m. The thermometer in his room read 64 degrees, and the Nest

CPS Challenges

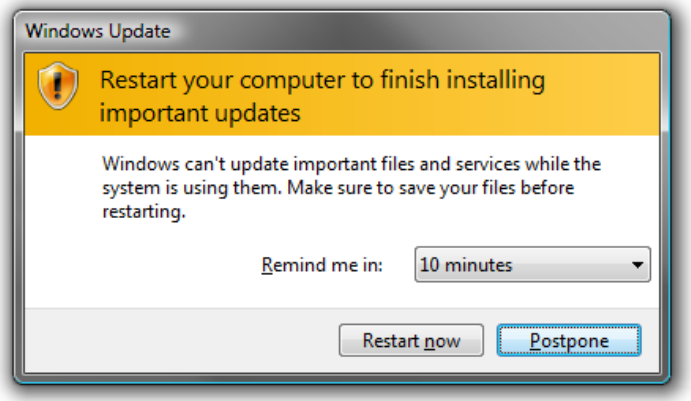
Real-time constraints



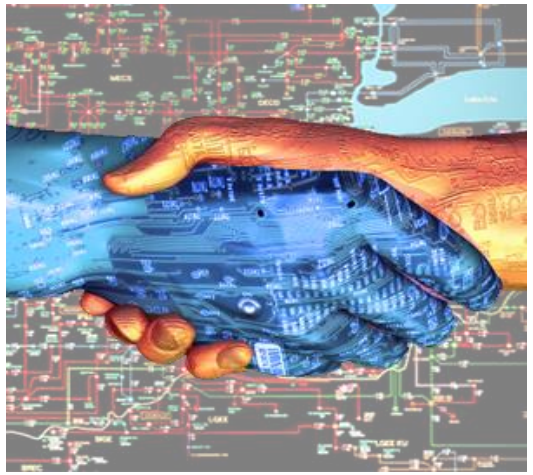
Resource constraints



Hard to Upgrade



Have human interactions



Why should we care about end device security ?

- Often the first entry point for attackers (weakest link in the trust chain)
- Cause large-scale disruptions by taking over many end-user devices

BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid

Saleh Soltan
Department of Electrical Engineering
Princeton University
ssoltan@princeton.edu

Prateek Mittal
Department of Electrical Engineering
Princeton University
pmittal@princeton.edu

H. Vincent Poor
Department of Electrical Engineering
Princeton University
poor@princeton.edu

Abstract

We demonstrate that an Internet of Things (IoT) botnet of high wattage devices–such as air conditioners and heaters–gives a unique ability to adversaries to launch large-scale coordinated attacks on the power grid. In particular, we reveal a new class of potential attacks on power grids called the Manipulation of demand via IoT (MadIoT) attacks that can leverage such a botnet in order to manipulate the power demand in the grid. We study five variations of the MadIoT attacks and evaluate their effectiveness via state-of-the-art simulators on real-world power grid models. These simulation results demonstrate that the MadIoT attacks can result in local power outages and in the worst cases, large-scale blackouts. Moreover, we show that these attacks can rather be used to increase the operating cost of the grid to benefit a few utilities in the electricity market. This work sheds light upon the interdependency between the vulnerability of the IoT and

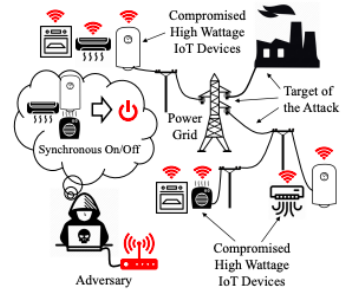


Figure 1: The MadIoT attack. An adversary can disrupt the power grid's normal operation by synchronously switching on/off compromised high wattage IoT devices.

History Lesson: Barbarians at the Gate (410 AD)

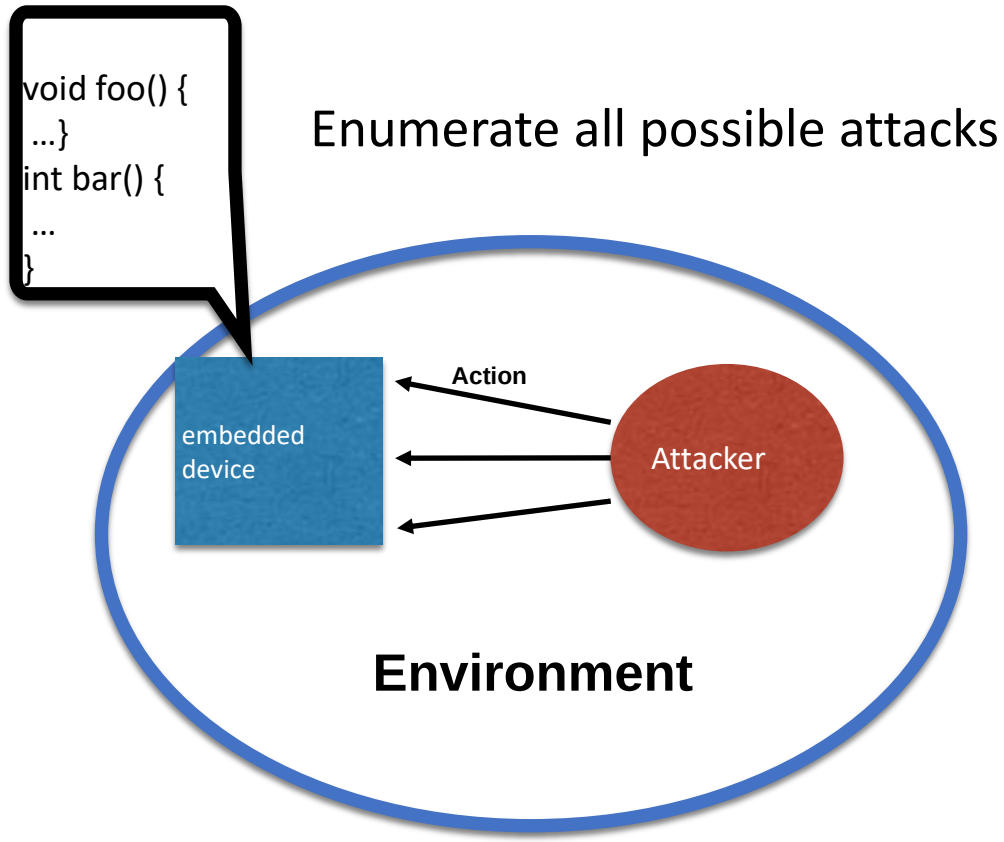
Image source: https://ludwigheinrichdyck.wordpress.com/2018/03/24/barbarians-at-the-gate-the-410-sack-of-rome/

This Talk

- Motivation
- Attacks on Embedded and IoT devices [DTRAP][ACSAC'19][ACSAC'16][TECS'20 best paper award]
- Intrusion Detection Systems for Smart Devices [FSE'17][CPS-SPC'18][EDCC'16 – best paper award]
- Ongoing work and conclusion

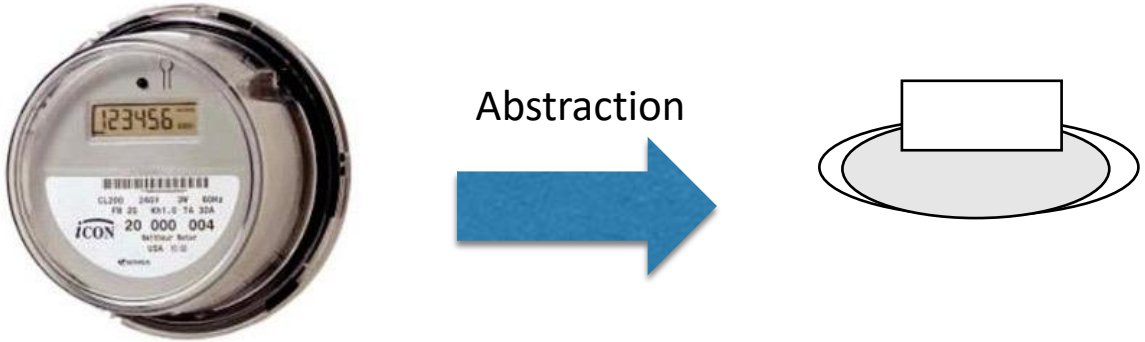
Challenge

- **No systematic technique to automatically find security vulnerabilities in IoT devices**
  - Large attack surface
  - Attacker often has physical access
  - Devices are often resource constrained

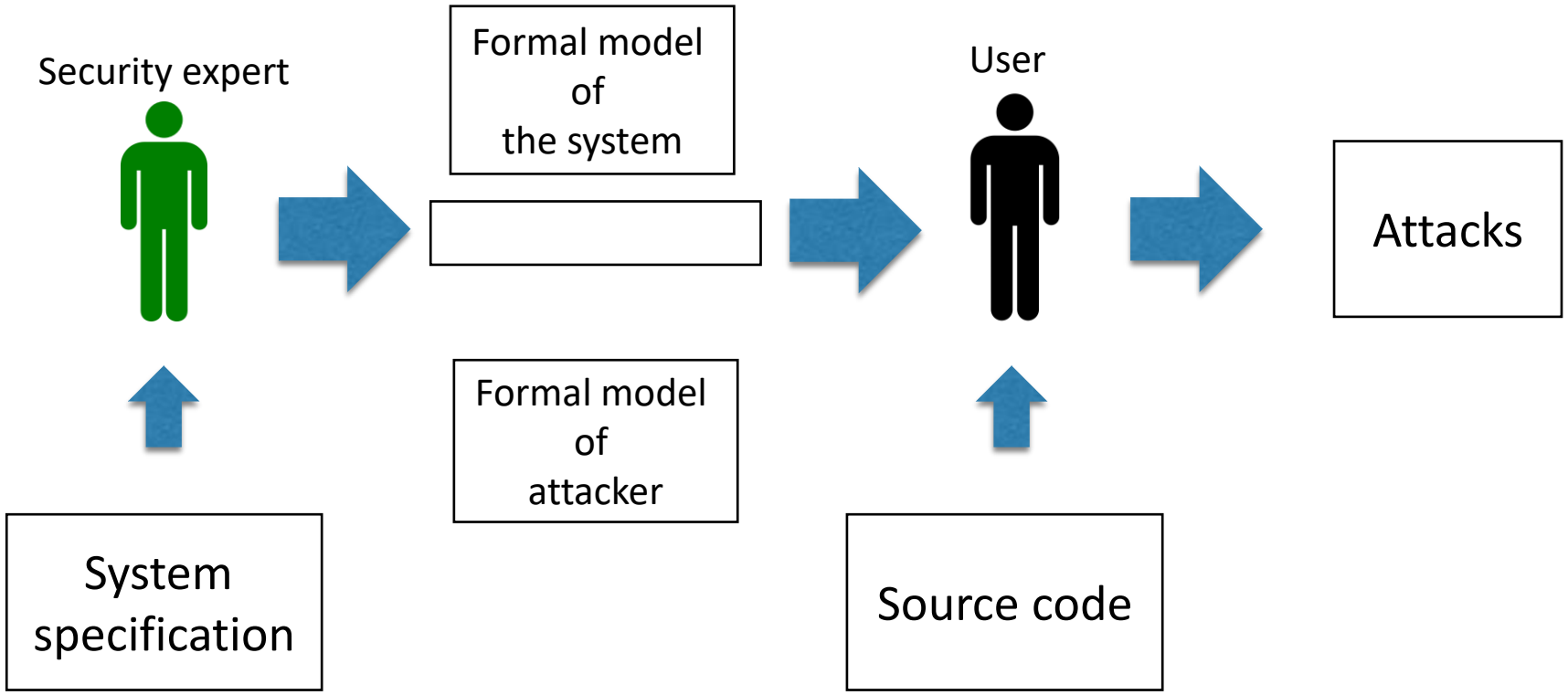


Our Insight

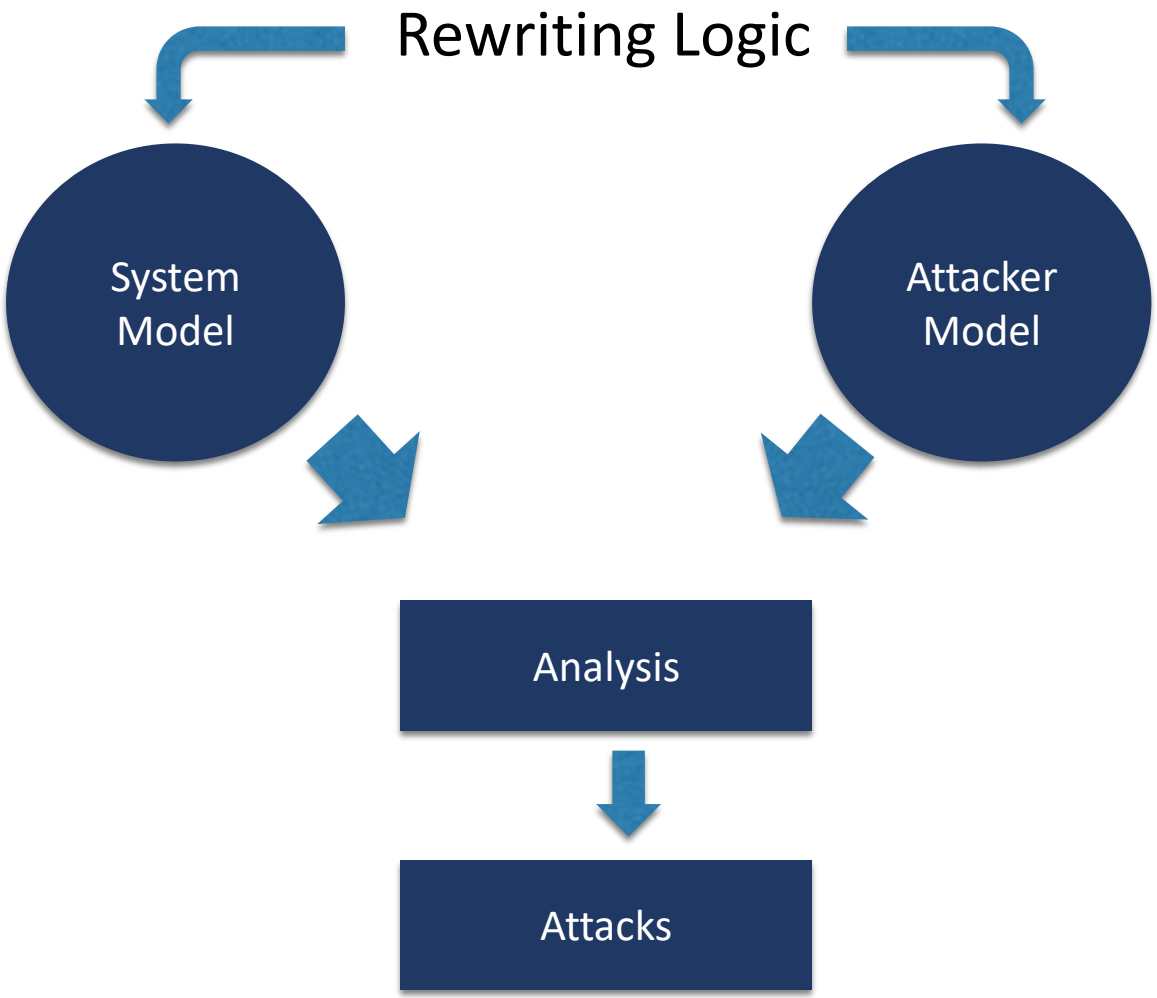
- IoT devices perform *specific* tasks
  - Define the right abstraction
    - Not too low level, not too high level



High-level picture



Abstraction



Abstraction: System Model

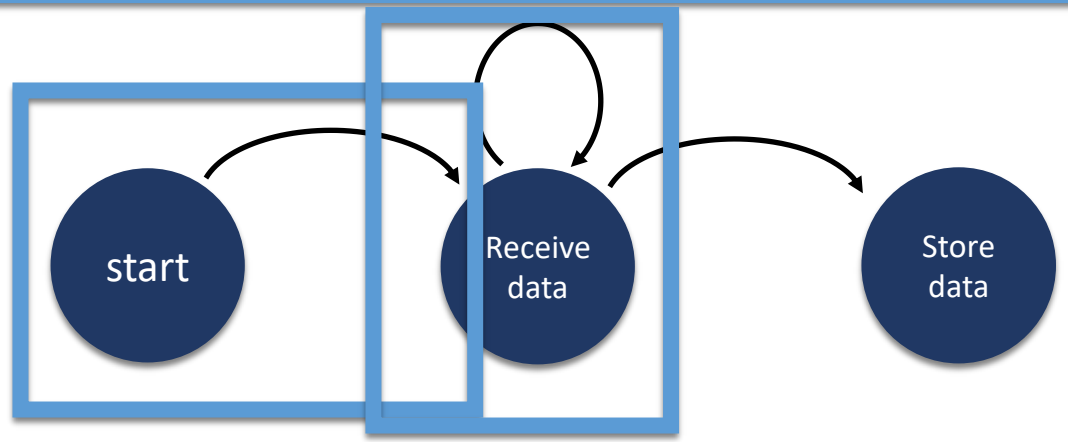
Rewriting logic:

- Rewrite rules
- Equations

Start ➔ sensorData(0, 0)

sensorData(r, n) ➔ sensorData(r, n) sensorData(r+1, 0)

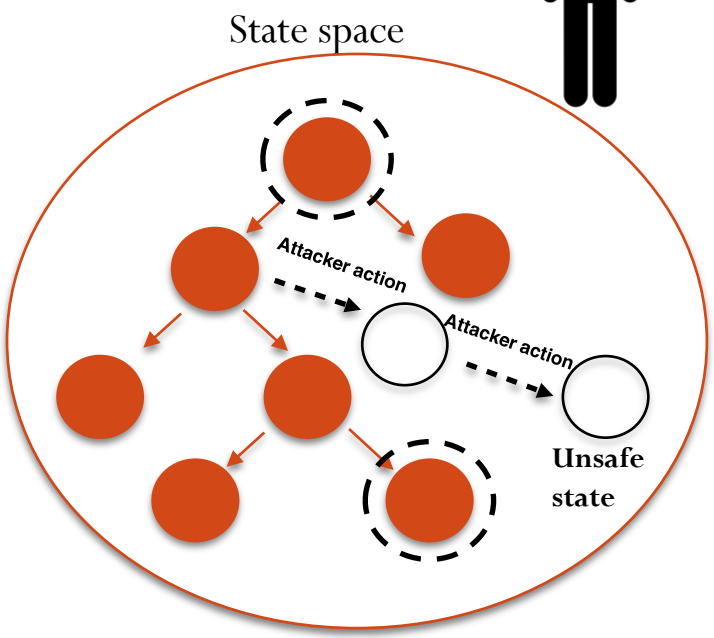
sensorData(r, n) ➔ sensorData(r, n+1)



Abstraction: Attacker Model

Attacker action:
e.g. access to the i*th* sensor channel

sensorData(c1, v1) sensorData(c2, v2) sensorData(c3, v3)➔
sensorData(c1, v1) sensorData(c3, v3) *if c2 = i*

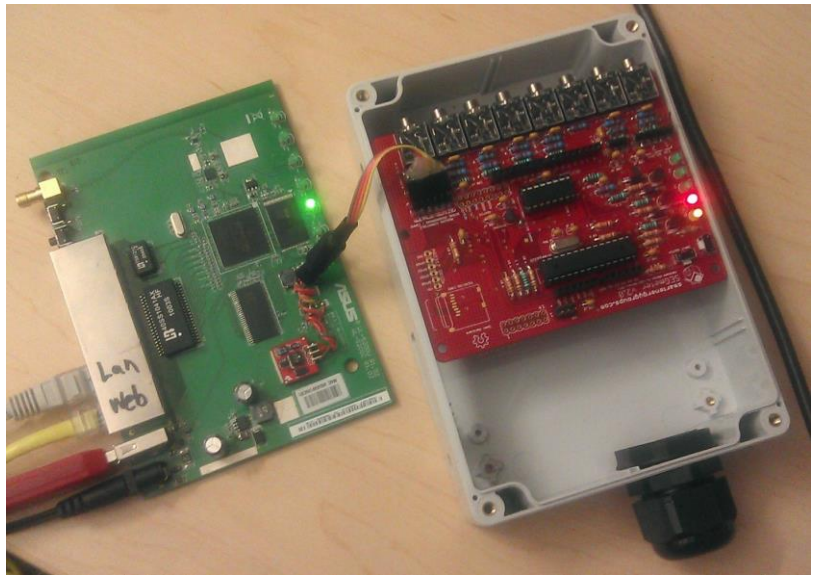


Explicit model checking:

Start ➔ receive(c1, v1) *where v1 < 0*

Case study

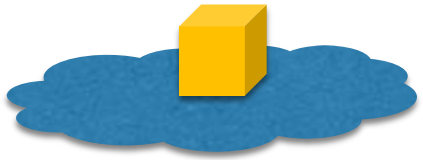
- SEGMeter: an open source smart meter
- Sensor board: Receive raw data
- Communication board: talk to server
- Code base: Lua and C (~ 3000 LOC)



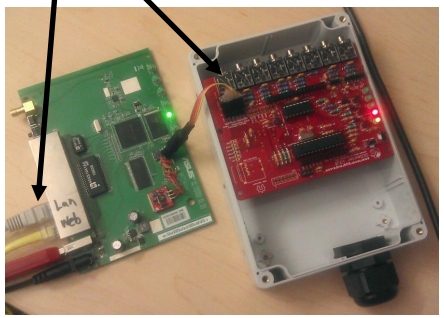
Threat model

- Access

Root access to a node in grid network [Mo et al. 2012]



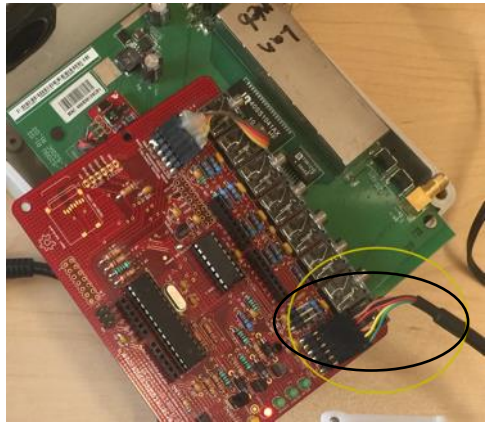
Read/Write access to communication interfaces[McLaughlin et al. 2010]



- Actions
  - Drop messages
  - Replay messages
  - Reboot meter

Results: Found 3 types of attacks

- Found by model checker within a few minutes (< 1 hr)
- Mounted on real meter with specialized equipment (total cost ~ $50) – based on model checker's output
- All three attacks were successful – 100% precision



Consequences of Attacks on Smart Meter

- Loss energy data in smart meter, infinite loop, demand inflation etc.

http://www.ece.ubc.ca/~faridm/acsac.html

Robotic Vehicles (RV)

- Autonomous UAVs and Rovers.
  - Delivery
  - Warehouse Management
  - Surveillance
  - Cinematography

Autonomous RVs are increasingly becoming popular.
RV missions are time critical.

Motivation

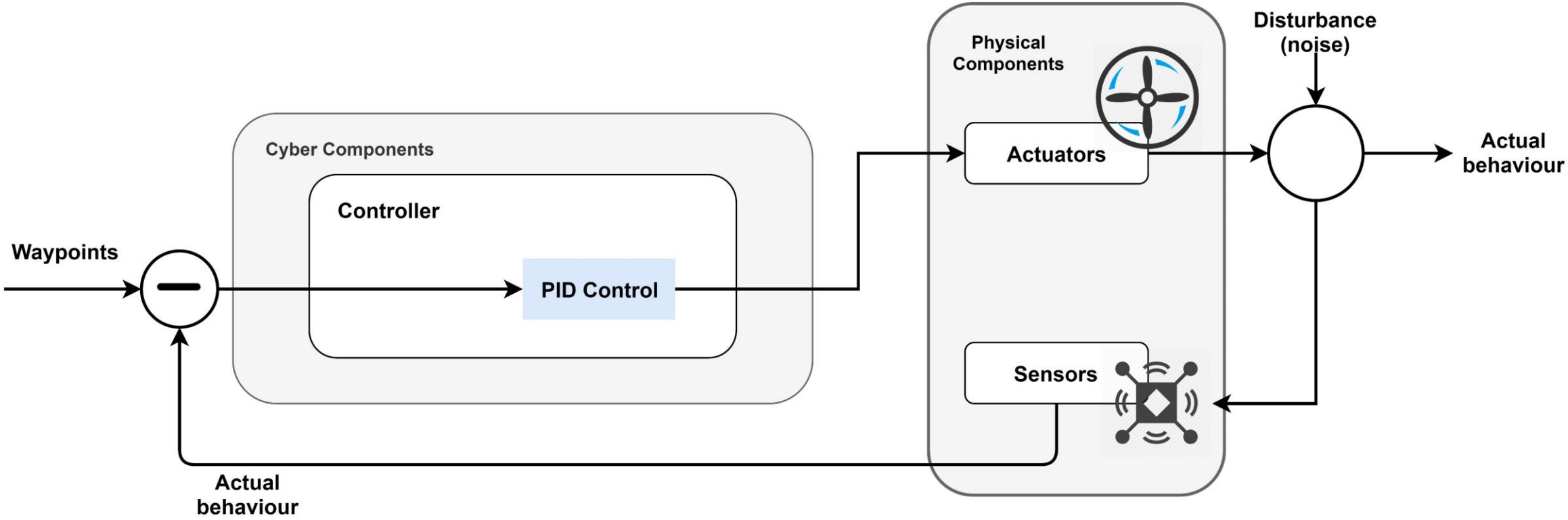
- GPS spoofing [ION GNSS'12], Optical spoofing [CCS'11]
- Acoustic noise injection in MEMS gyroscope [Usenix'15],
- MEMS accelerometer [Euro S&P'17]

However, all these techniques assume there's no protection deployed.

Can an attacker remain stealthy and trigger adversarial actions?

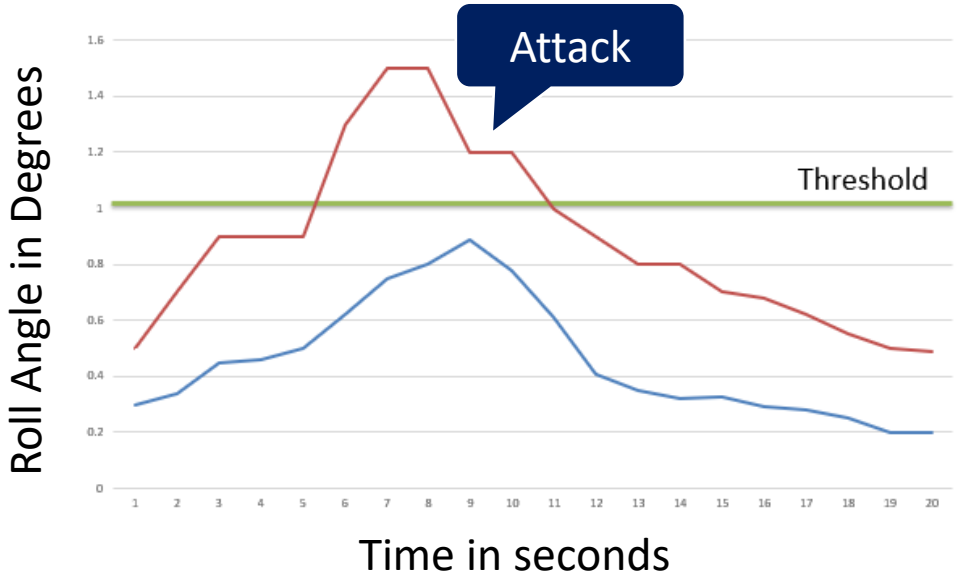
Robotic Vehicle System

- Cyber component
- Physical component



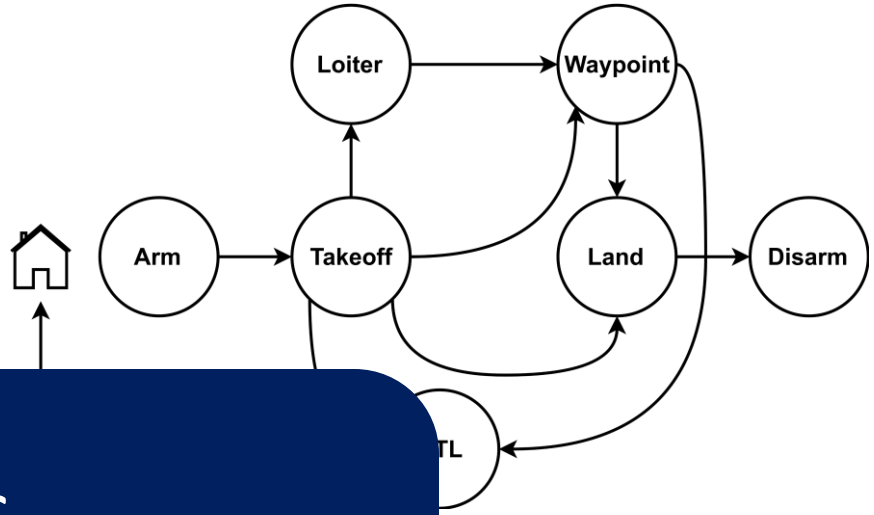
Control-based Attack Detection Techniques

- Control Invariants (CI) [CCS'18]
- Extended Kalman Filter (EKF)
- Model to learn and predict RV's runtime behavior
- Error analysis to detect attacks
  - $|V_{predicted} - V_{observed}| > \tau$



Limitations in Control-based Detection

- Fixed threshold
  - Large threshold to reduce False Positives (FP).
    - Environmental factors – friction, wind
    - Sensor faults.
- Fixed Monito
- Often fail to
  - Takeoff
  - Waypoi



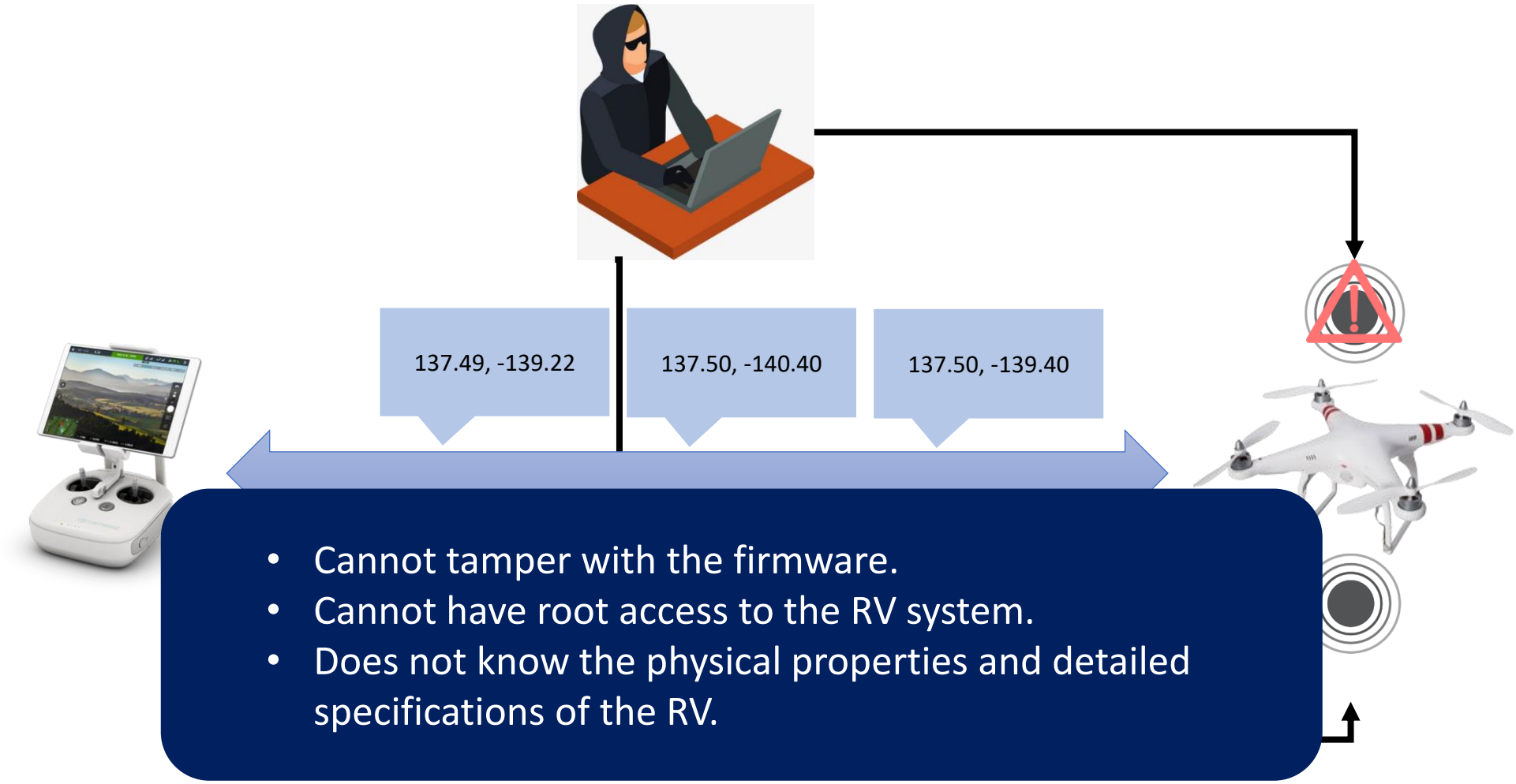
Stealthy Attacks

False Data Injection

Artificial Delay

Switch Mode Attack

Attack Model



Experimental Setup

- Real RV systems

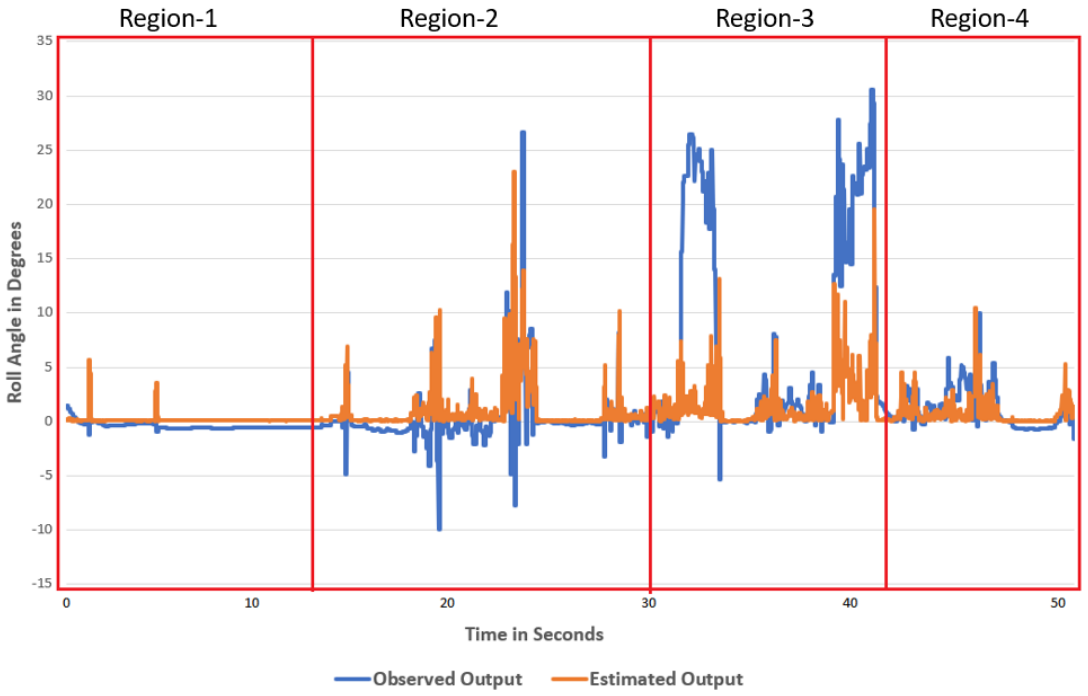
- Autopilot
  - ArduPilot, PX4, Paparazzi UAV

ArduPilot	PX4	Paparazzi
Arduino, ARM	Pixhawk series	ARM
EKF3	ECL EKF	EKF2
Manual and autonomous	Autonomous, FPV support	Drone racing

- R1 Rover - https://www.aionrobotics.com/r1
- Pixhawk – https://pixhawk.org
- ArduPilot - http://ardupilot.org/
- PX4 Autopilot - https://px4.io/
- Pararazzi UAV - https://wiki.paparazziuav.org/wiki/Main_Page

Attacker's Effort

- Attacker's effort in deriving the state estimation model.
  - Detection Threshold
  - Monitoring Window
- Convergence
  - 5-7 missions for all the subject RVs



Impacts of Stealthy Attacks - FDI

- False data injection (FDI) attack → Gradually deviates RV

Impacts of Stealthy Attacks - AD

- Artificial Delay (AD) attack → Injects Intermittent delays.

Impacts of Stealthy Attacks: SM

- Switch mode (SM) attack
  - Crash landing → 30% of the missions.
  - Ignore LAND command.

https://globalnews.ca/news/6235460/ubc-drone-hacking-research/

Robotic Vehicles: Summary

- Vulnerabilities in control theory based attack detection techniques
- Demonstrate three types of stealthy attacks on RV systems
  - Attacks deviate a RVs by more than 100 meters, increases duration of RV mission by 25-30%, even result in crashes.
- Demonstrate techniques to automate the attacks on a class of RVs.

Artifacts: https://github.com/DependableSystemsLab/stealthy-attacks

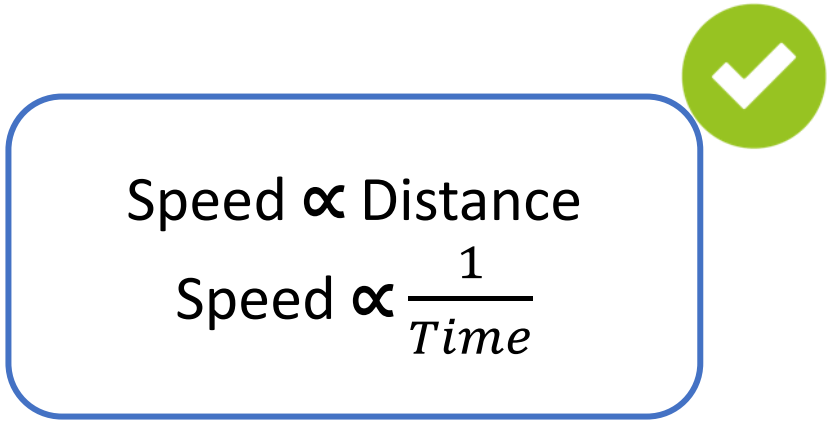
This Talk

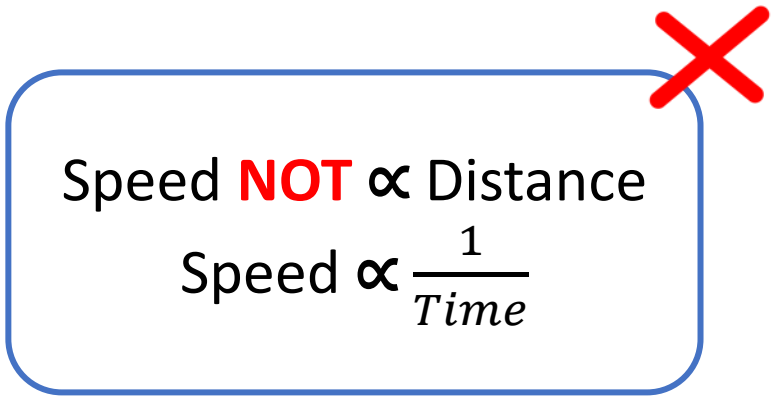
- Motivation
- Attacks on Embedded and IoT devices [DTRAP][ACSAC'19][ACSAC'16][TECS'20 best paper award]
- Intrusion Detection Systems for Smart Devices [FSE'17][CPS-SPC'18][EDCC'16 – best paper award]
- Ongoing work and conclusion

Motivation

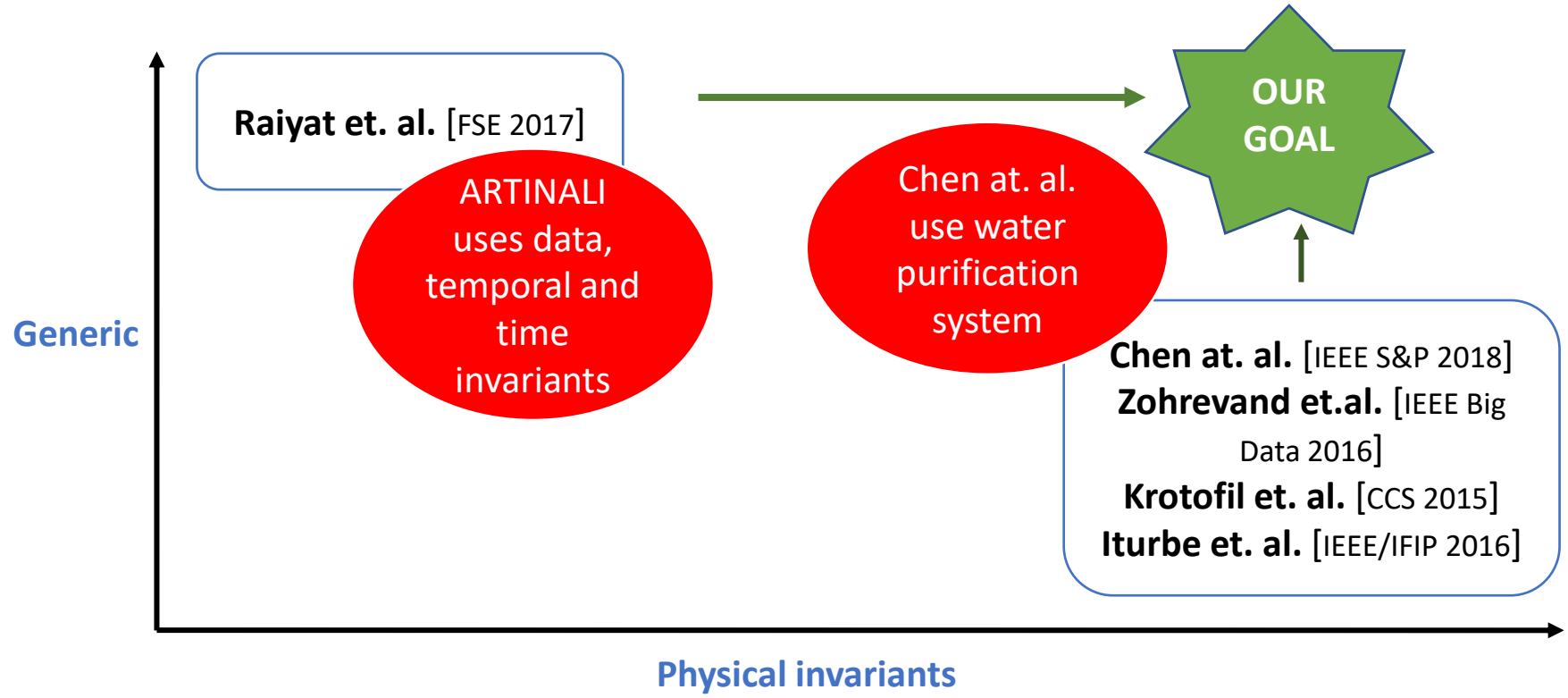
- **Goal: Provide low-cost security for CPS**
  - Satisfying resource and real-time constraints
  - No human intervention needed
  - Is able to detect zero day attacks

Insight: Leverage properties of CPS for intrusion detection
- Simplicity and timing predictability
- Learn invariants based on dynamic execution
- Monitor invariants at runtime for violations





CORGIDS: Correlation-Based Detection



Hidden Markov Model (HMM)

Finite model used to **describe probability** distribution over possible sequences of a given system.

Example: Reinforcement learning and pattern recognition such as speech, handwriting and gesture recognition

HMM

- **Finding correlations** in multidimensional, **non-linear time series** systems like **CPS**.
- **Likelihood of data** belonging from a dataset.

Experimental setup

- **Unmanned Aerial Vehicle (UAV)**

  ArudPilot's Software in the Loop (SITL)

  (http://ardupilot.org/dev/docs/sitl-simulator-software-in-the-loop.html)

- **Smart Artificial Pancreas (SAP)**

  Open Artificial Pancreas System (OpenAPS)

  (https://openaps.org/)

Evaluation

TESTBED	TARGETED ATTACKS	FP (%)	FN (%)
UAV	Battery Tampering	0.0	12.20
	Flooding	0.0	11.30
	Distance Spoofing	0.0	12.80
SAP	Insulin Tampering	5.60	4.20
	Glucose Spoofing	2.80	8.40

Summary of CORGIDS

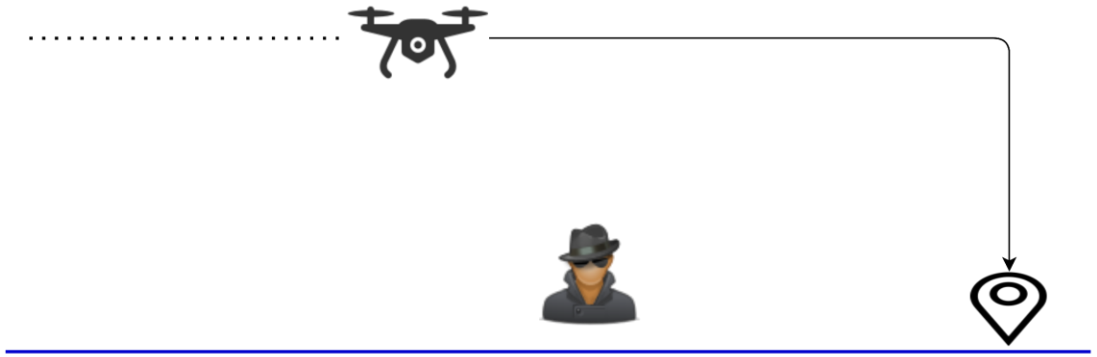
- **Physical properties** of CPS are **indicative** of its behavior.
- **HMM** are **good** at finding **correlations among properties**.
- **CORGIDS** had **higher Precision** and **Recall** than prior techniques

This Talk

- Motivation
- Attacks on Embedded and IoT devices [DTRAP][ACSAC'19][ACSAC'16][TECS'20 best paper award]
- Intrusion Detection Systems for Smart Devices [FSE'17][CPS-SPC'18][EDCC'16 – best paper award]
- Ongoing work and conclusion

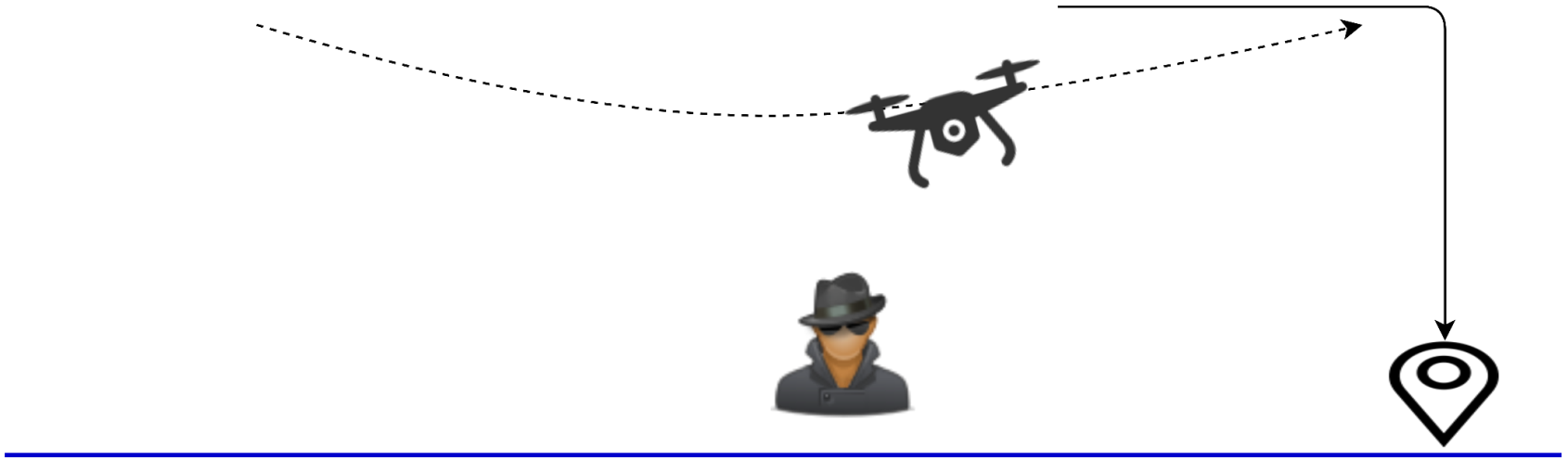
Future Directions

- Attack detection does ensure mission success.
- Current techniques
  - Attack response → trigger hardware fail-safe (e.g., landing in case of landing)



Future Directions

- RVs must be equipped with Recovery capabilities
  - Augmenting RV's controller → Robust actuator signals despite the attacks.
  - Complete the mission despite adversarial actions.



Conclusions

- **End Devices in CPS are important to be protected from attacks**
  - Provide a conduit for attackers to get a foot-hold into the system
  - Can cause large-scale disruptions of critical infrastructures

- **Attackers can remain stealthy by leveraging properties of the CPS**
  - Knowledge and physical access to the CPS
  - Need host-based intrusion detection systems for security

- **Host-based IDS for end-user devices**
  - Leverage invariants and machine learning to learn CPS behaviors
  - Detect attacks proactively with low false-positives

More info: http://blogs.ubc.ca/karthik