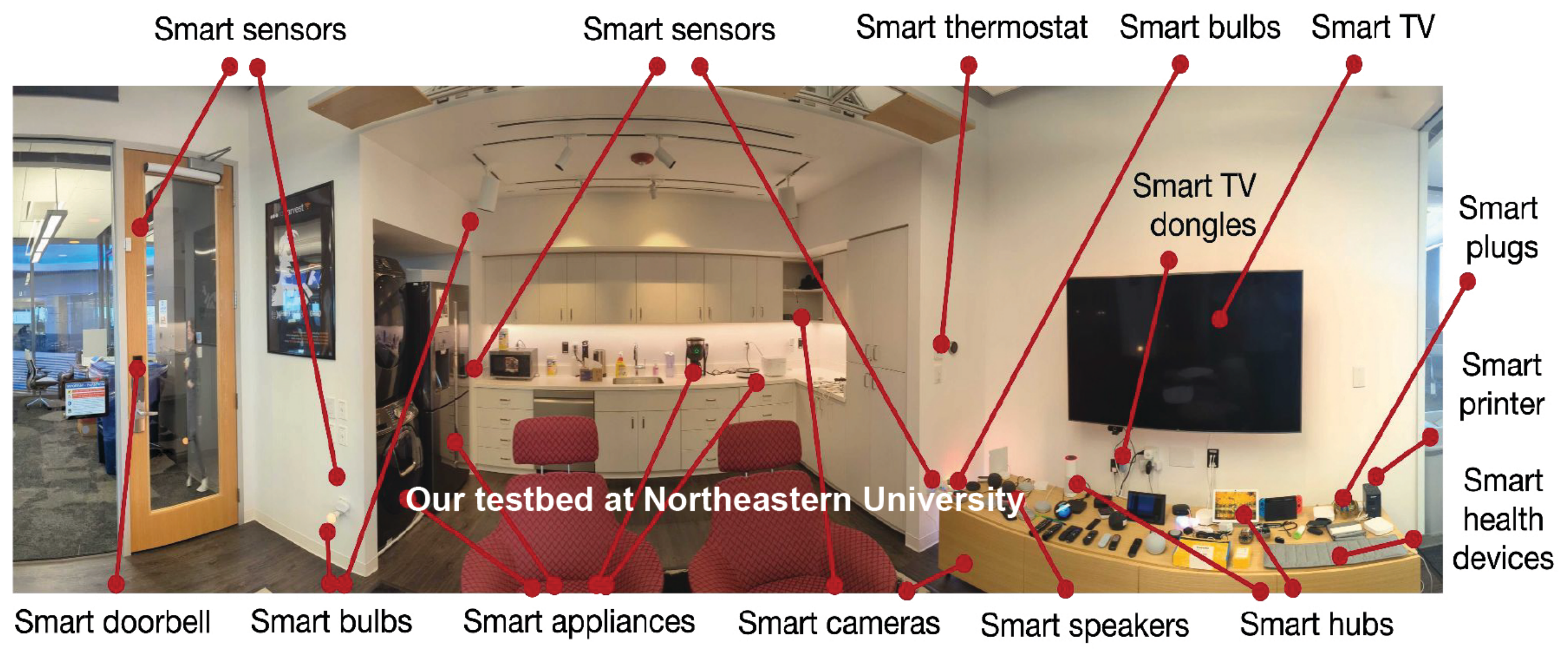
BehavIoT: Using Network-Inferred Behavior Models to Detect Anomalous IoT Behavior

Tianrui Hu, Daniel J. Dubois, David Choffnes
Northeastern University



Motivation: IoT diversity and opaqueness

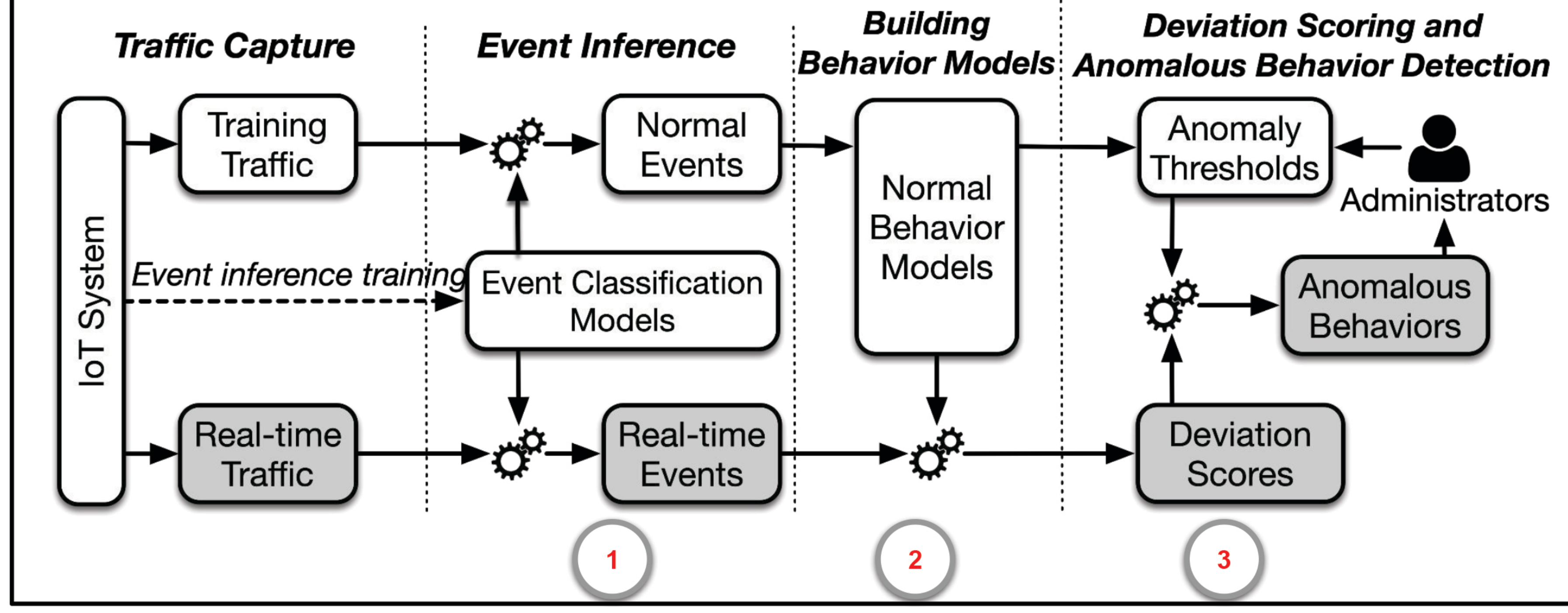
Key challenges for mitigating the security, privacy, and safety risks of smart home IoT deployments:

- **diversity: a wide variety of** devices and behaviors
- **opaqueness:** typically **closed systems** that provide little insight

We need a solution that

- detects **a variety of** anomalous behaviors
- works across **a wide range of** IoT devices.
- requires **no privileged access** to devices or APIs.
- provides **insight and contextual information** about how behavior changed.

BehavIoT



Contributions

1. A platform- and protocol-agnostic **event inference** method.
2. An efficient way to **model IoT behaviors** from events.
3. A system to **measure behavior deviations and detect anomalous behaviors**.
4. An evaluation both in a **controlled** and in an **uncontrolled setting** in our testbed that consists of **49 devices** as a part of a **3-month user study involving 40 participants.**
5. **Datasets and software artifacts available** to facilitate follow-up research.

Key Insights: predictable and simple IoT devices

Most consumer IoT devices:

- **network traffic** typically exhibits **predictable patterns**, though mostly encrypted.
- **relatively simple**, having **a limited set of functionalities and states.**

Our Solution: infer events, model behaviors, detect changes

Our idea is to:

1. **infer events** from IoT devices' network traffic
2. **model normal IoT behaviors** from inferred events
   - ○ function-related events as a probabilistic state-machine [Fig 1]
   - ○ periodic events as timers [Fig 2]
3. **detect anomalous behaviors** that are significantly inconsistent with the inferred behavior models based on statistical metrics and data [Fig 3]

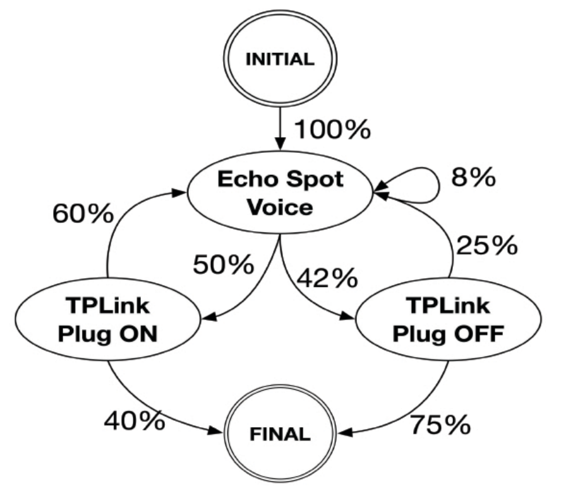


Figure 1. Function-related behavior model

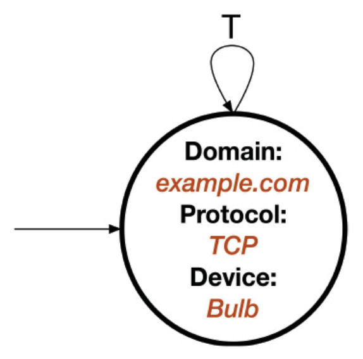


Figure 2. Periodic event behavior model

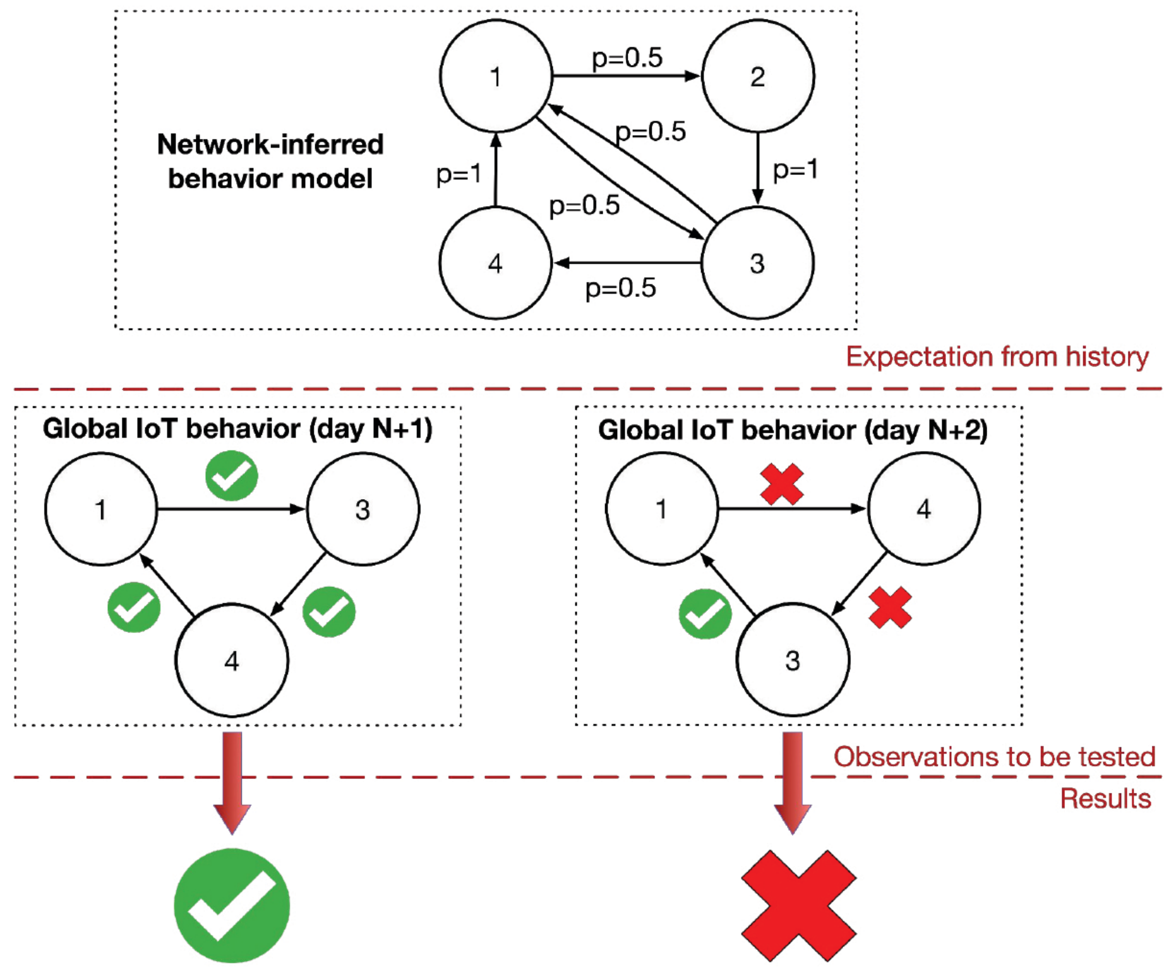

Network-inferred behavior model
1
2
3
4
p=0.5
p=0.5
p=1
p=1
p=0.5
p=0.5
Expectation from history
Global IoT behavior (day N+1)
Global IoT behavior (day N+2)
Observations to be tested
Results

Figure 3. An example of anomalous behavior detection

Evaluation

RQ1: Can we infer events from IoT device network traffic?
Yes, we can accurately infer events.

- 98.91% ACC on **function-related events** that meet or exceed existing approach.
- Majority of traffic exhibits periodicity.
- 99.24% ACC on **periodic events.**
- Only 0.52% of traffic flows are neither function-related nor periodic events.

Device	Func-related Event Accuracy	Periodic Event Accuracy
Home Auto & Sensor	99.15%	99.86%
Camera	98.95%	99.94%
Smart Speakers	96.52%	97.65%
Hub	100%	98.01%
Appliance	100%	99.62%
Total	98.91%	99.24%

Event inference accuracy per IoT device category.

Our solution:

- **only relies on network traffic**
- works well on **a wide range of devices**

showing the **generalizability** and **deployability** of our approach.

RQ2: Can we model IoT behaviors from inferred events?
Yes, we can model a variety of IoT behaviors.

- cover **all network traffic flows** by three behavior models.
- provide **more flexibility and scalability** for representing IoT behaviors.

RQ3: Can we use behavior models to detect anomalous behavior and help admin determine whether such behavior is harmful?
Yes, we show that

- our deviation metrics and thresholds chosen from statistical data are good for measuring differences in behaviors and detect significant ones as anomalous behaviors. [Fig 4]
- BehavIoT can detect many anomalous behaviors both in controlled and uncontrolled experiment in our testbed. [Fig 5]
- BehavIoT provides contextual information of each detected anomalous behaviors and can help identify a variety of real-world threats that may cause privacy, security, and/or safety issues.

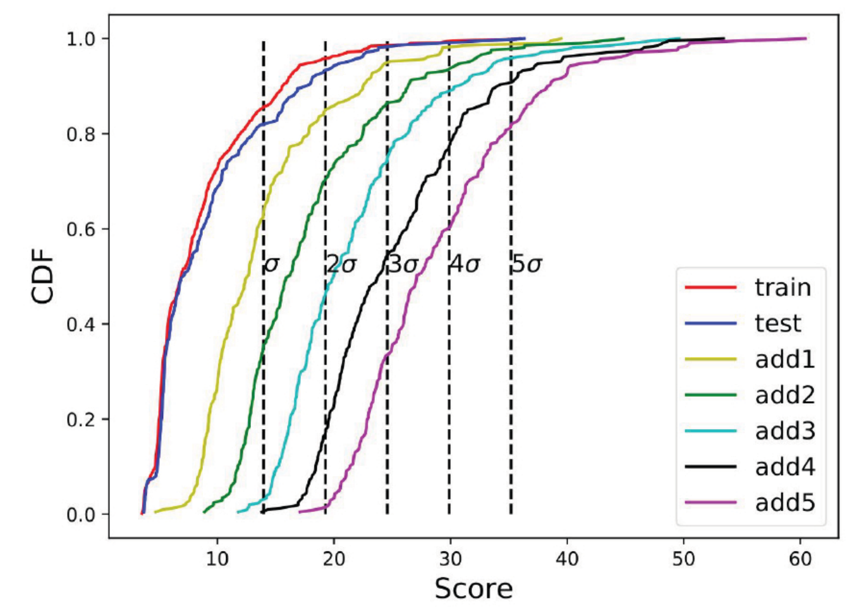


Figure 4. The deviation scores increase while adding more differences in behaviors. The thresholds are based on standard deviation σ of the scores.

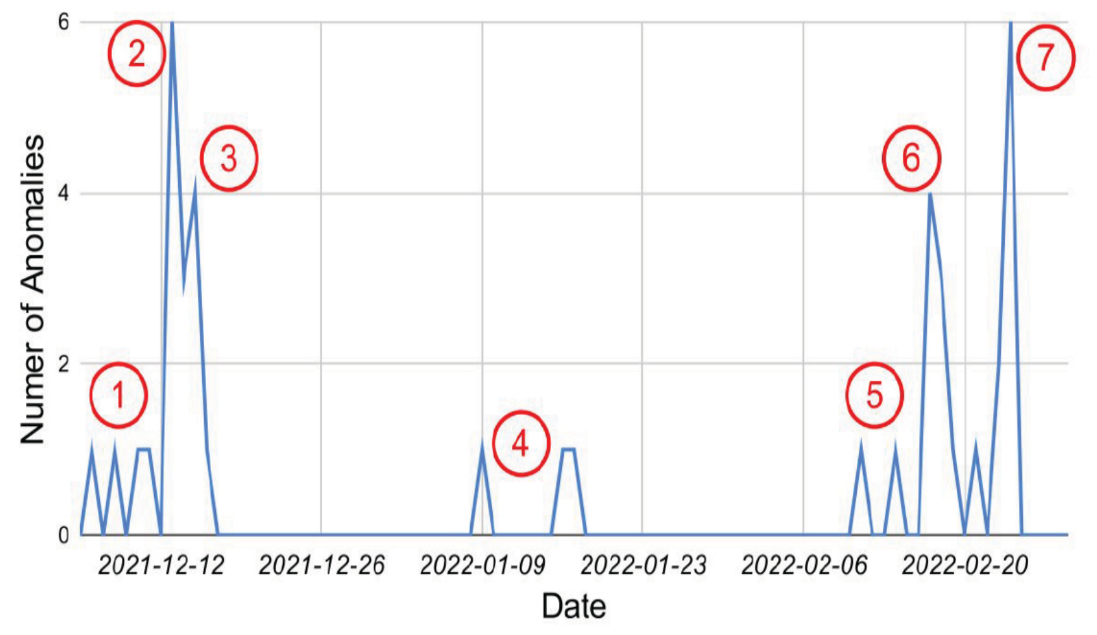


Figure 5. Anomalous behaviors due to function-related events over three month in the uncontrolled experiment.

Privacy: misactivation, data exfiltration
Security: malware, unauthorized access
Safety: DoS, malfunctions

SaTC Frontiers: Collaborative: *1956393* [1], *1955227* [2], *2103439* [3], *1956435* [4]
Institutions: UC Irvine [1], Northeastern Univ. [2], UC Davis [3], USC [4]
Lead PIs: A. Markopoulou [1], D. Choffnes [2], Z. Shafiq [3], K. Psounis [4]