BehavIoT: Measuring Smart Home IoT Behavior Using Network-Inferred Behavior Models

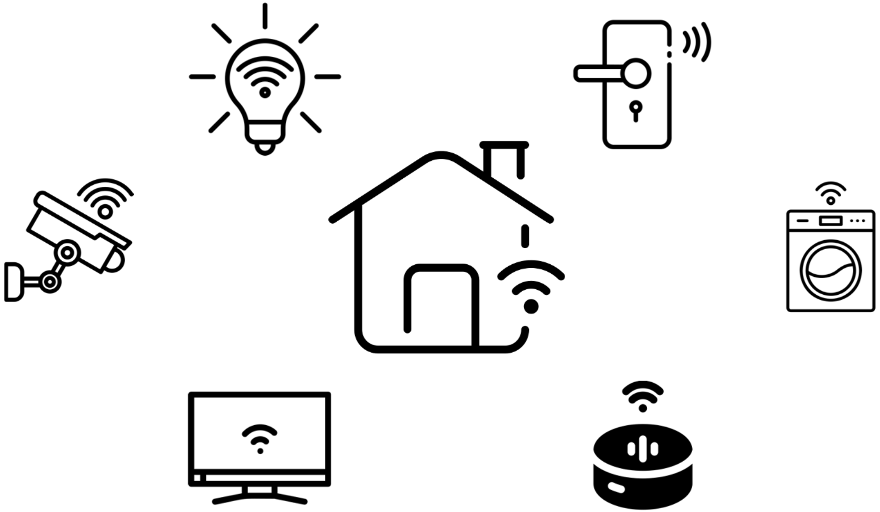
Tianrui Hu, Daniel J. Dubois, David Choffnes

Northeastern University
Khoury College of Computer Sciences

ProperData

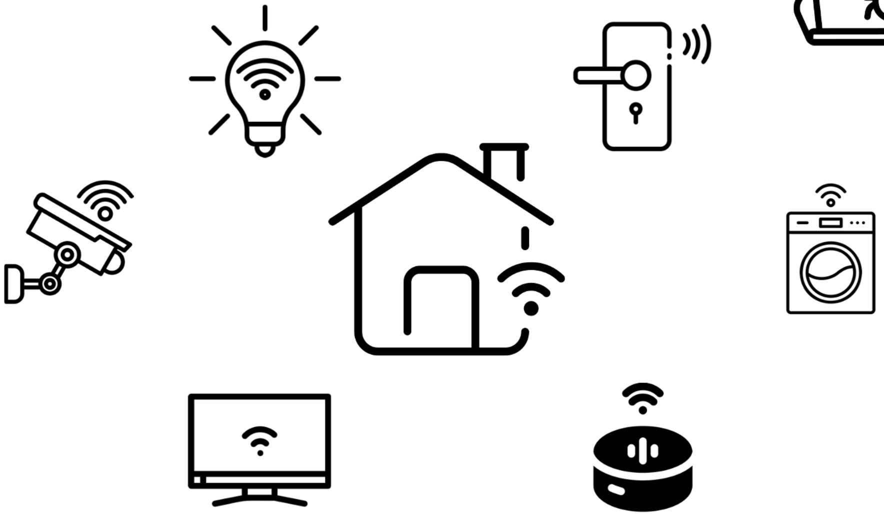
Background

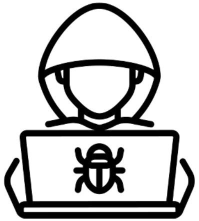
Internet-enabled smart home



Background

Internet-enabled smart home

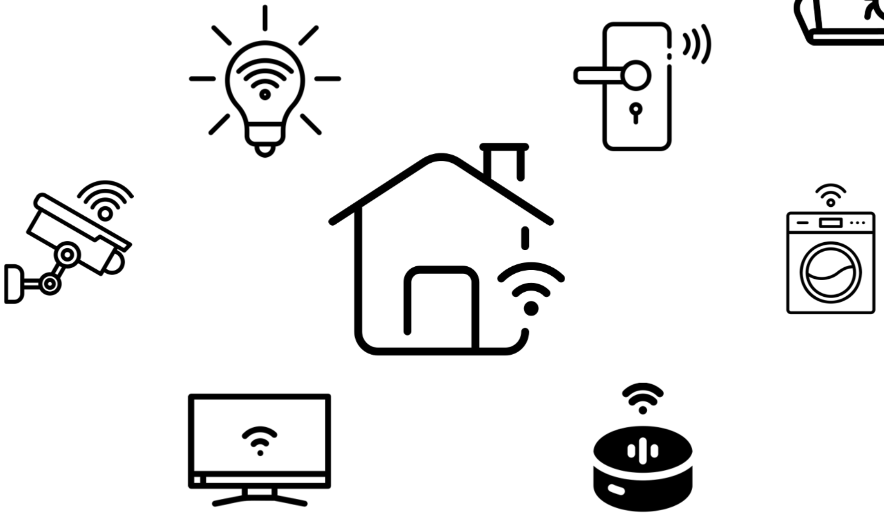


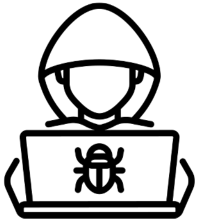


The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet

Background

Internet-enabled smart home

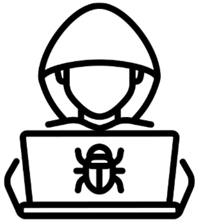




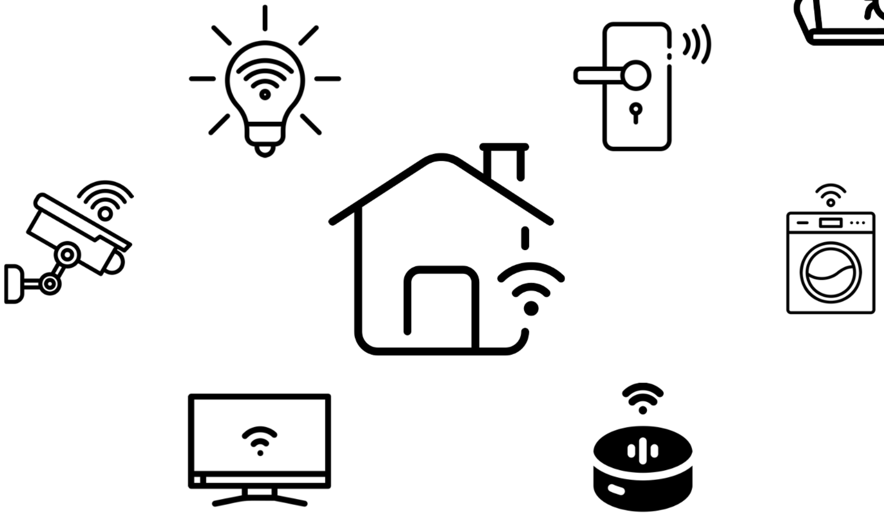
The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet

Google admits its new smart speaker was eavesdropping on users

Background



Internet-enabled smart home



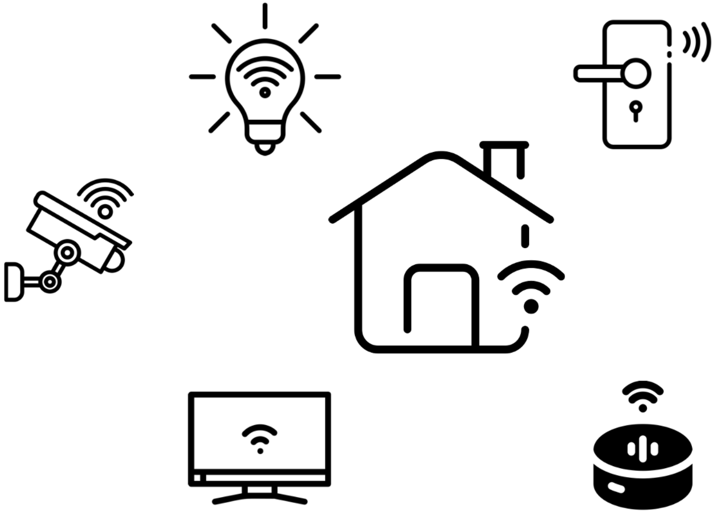
The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet

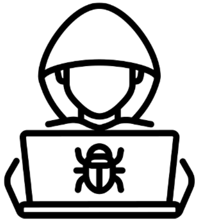
Google admits its new smart speaker was eavesdropping on users

Amazon Outage Shuts Down IoT Vacuums, Doorbells, Fridges, Even Home Locks

Background

Internet-enabled smart home





The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet

Google admits its new smart speaker was eavesdropping on users

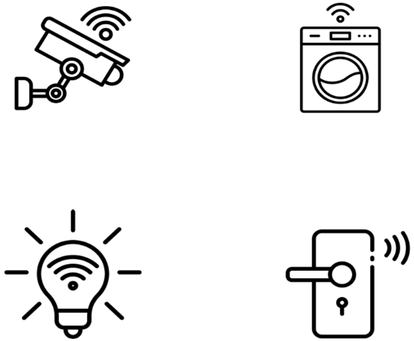
Amazon Outage Shuts Down IoT Vacuums, Doorbells, Fridges, Even Home Locks

- Diverse security, privacy, and safety issues
- Due to attacks, malfunctions, misconfigurations, etc.

Why is it hard to model IoT behavior?

Why is it hard to model IoT behavior?

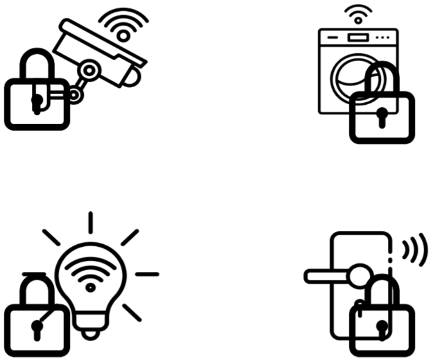
Diversity



Why is it hard to model IoT behavior?

Diversity

Opaqueness



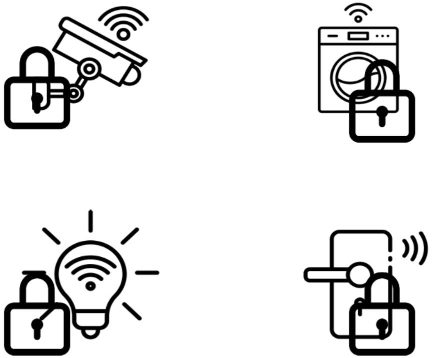
Why is it hard to model IoT behavior?

Diversity

Opaqueness

Hard to fully understand

- **what is normal device behavior**
- **how it changes over time**



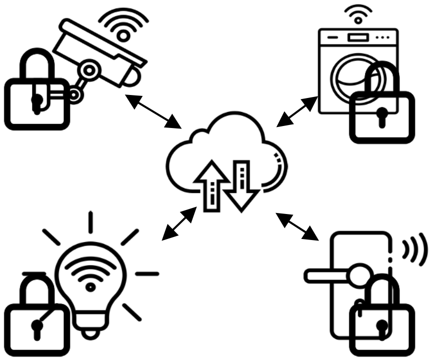
Why is it hard to model IoT behavior?

Diversity

Opaqueness

Hard to fully understand

- **what is normal device behavior**
- **how it changes over time**



Key observation: IoT reveals behavior via **network traffic**

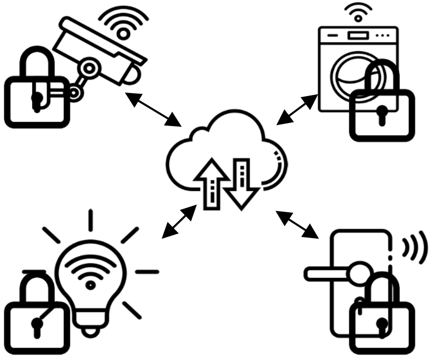
Why is it hard to model IoT behavior?

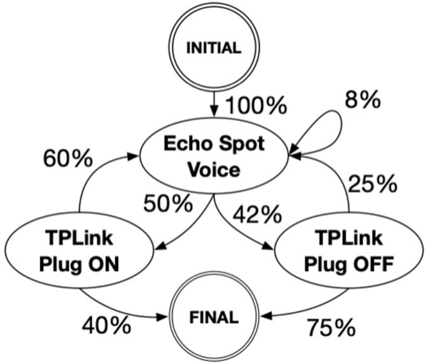
Diversity

Opaqueness

Hard to fully understand

- **what is normal device behavior**
- **how it changes over time**

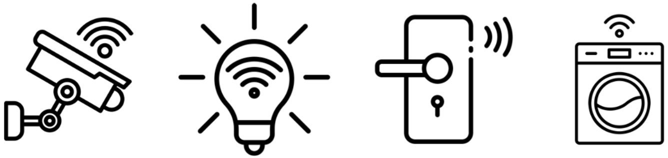




Key observation: IoT reveals behavior via **network traffic**

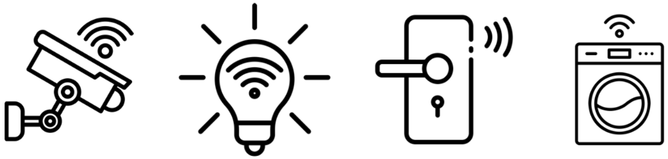
Open question: *Can we model IoT behavior based on this traffic?*

Motivation



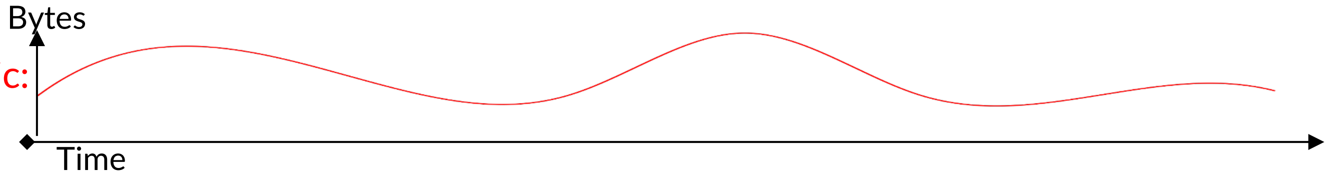
- **Predictable** network traffic patterns

Motivation

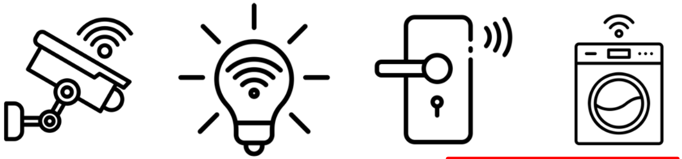


- **Predictable** network traffic patterns

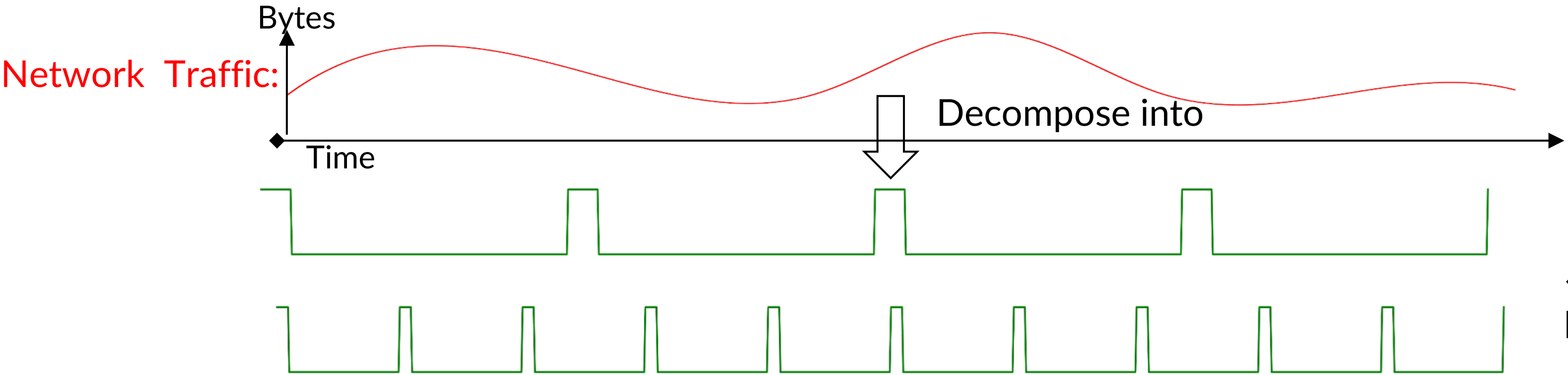
Network Traffic:



Motivation

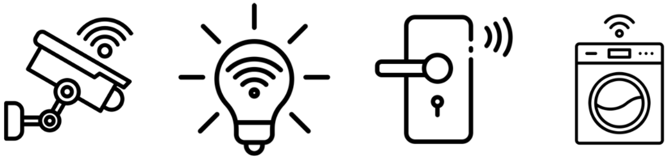


- **Predictable** network traffic patterns → **periodic**

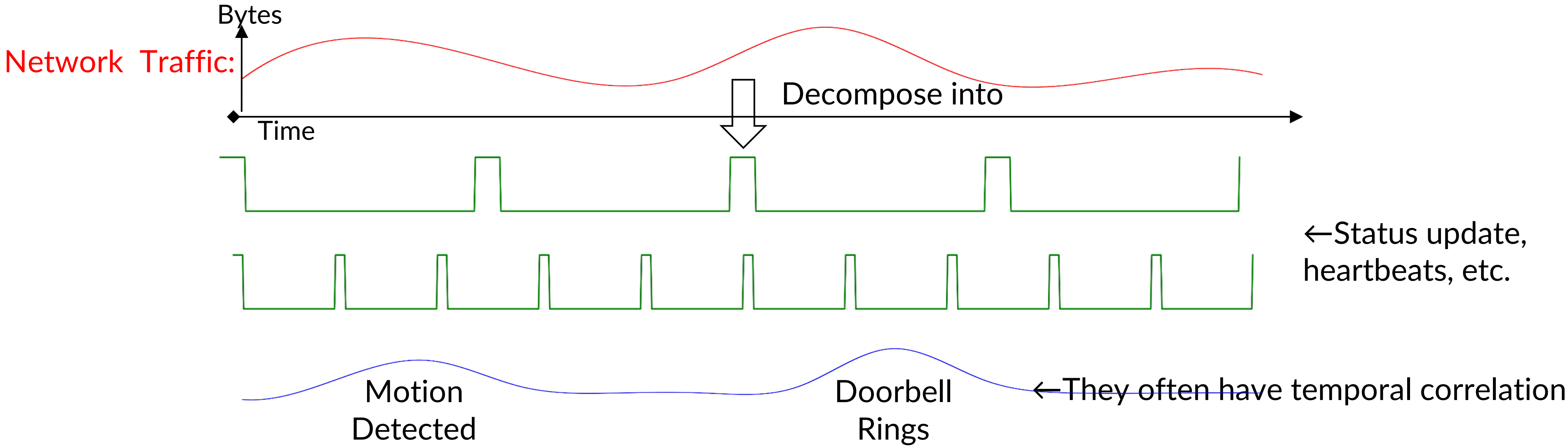


←Status update, heartbeats, etc.

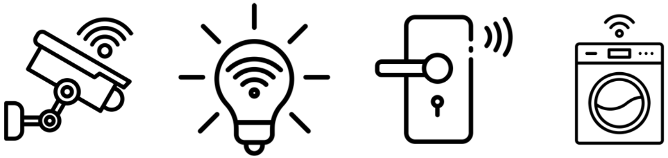
Motivation



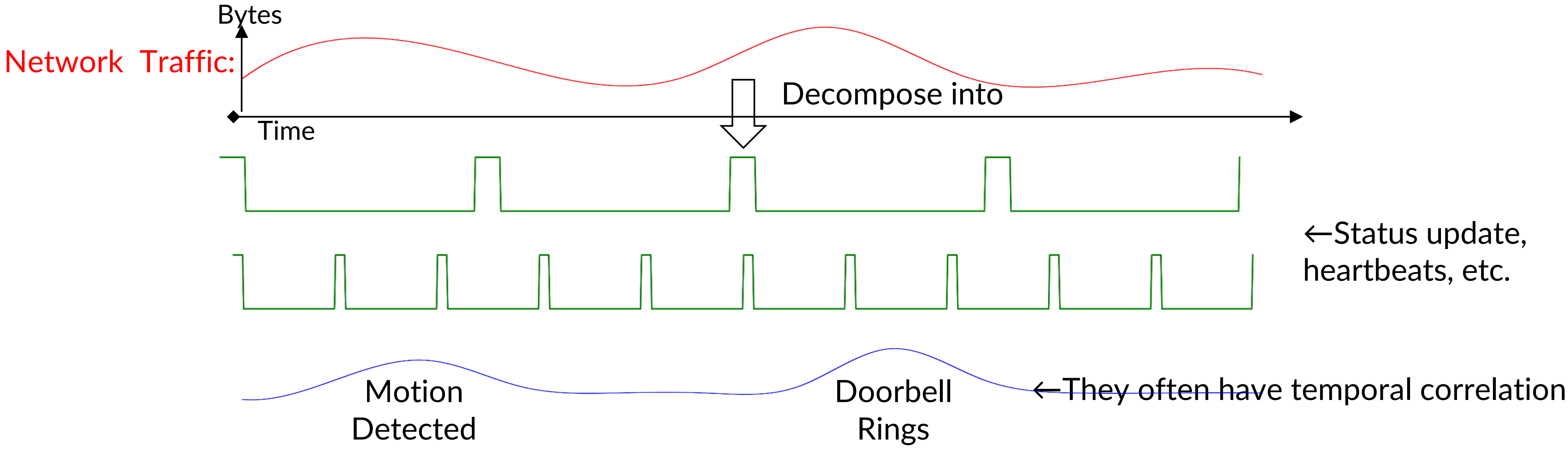
- **Predictable** network traffic patterns
  - → periodic
  - → **correlate with the actual functions**



Motivation



- **Predictable** network traffic patterns
  - → **periodic**
  - → **correlate with the actual functions**



- **Relatively simple** — having **a limited set of functionalities and states.**

Research Questions

Research Questions

RQ1: How do we measure and characterize the behaviors of smart home system from their (mostly encrypted) network traffic?

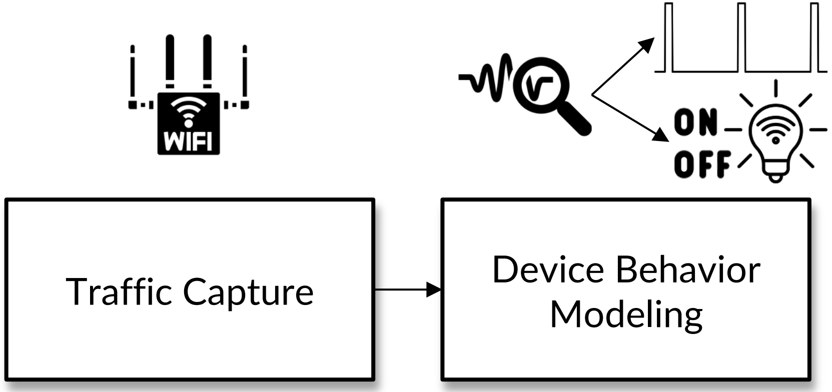
RQ2: How do we measure and characterize behavior deviations of a smart home system?

Our Approach - BehavIoT

Traffic Capture

1. **Capture** IoT devices' encrypted **network traffic**

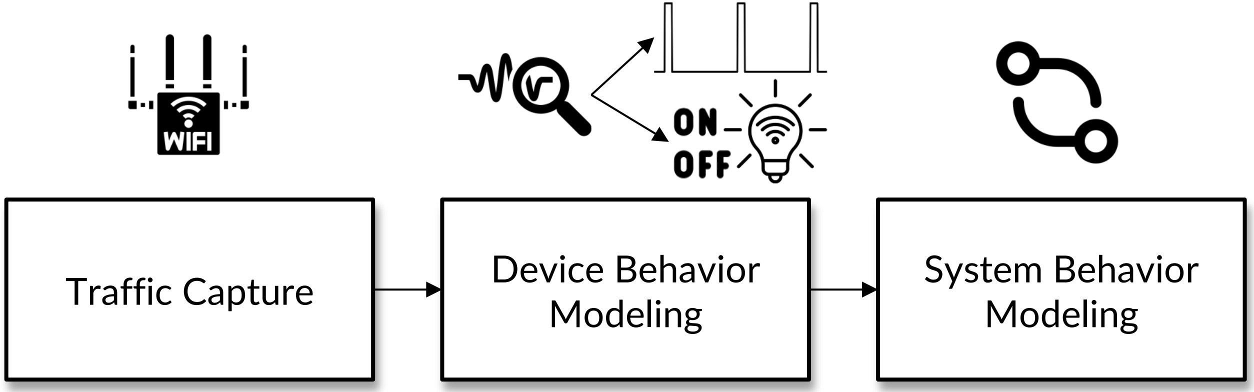
Our Approach - BehavIoT



1. **Capture** IoT devices' encrypted **network traffic**

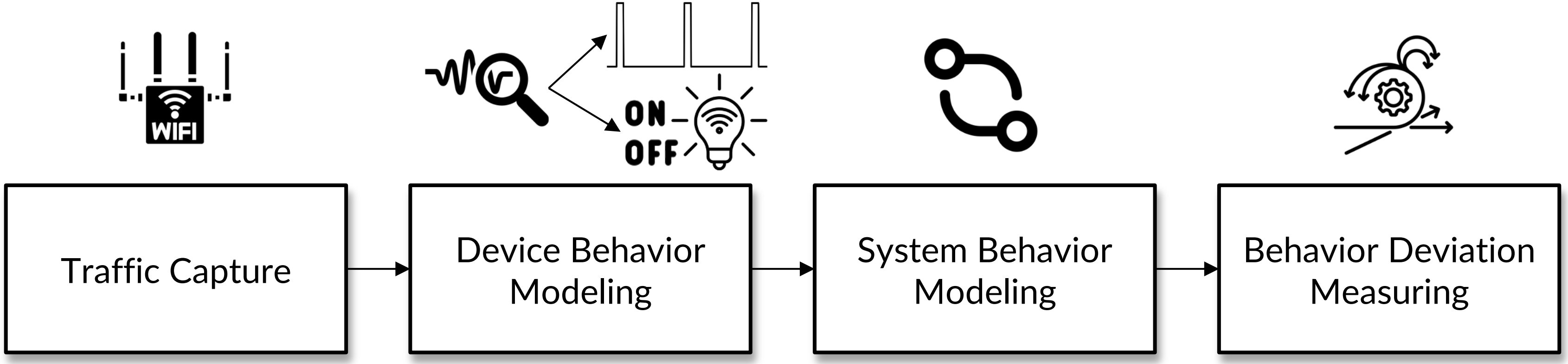
2. **Characterize** individual **device behavior**

Our Approach - BehavIoT



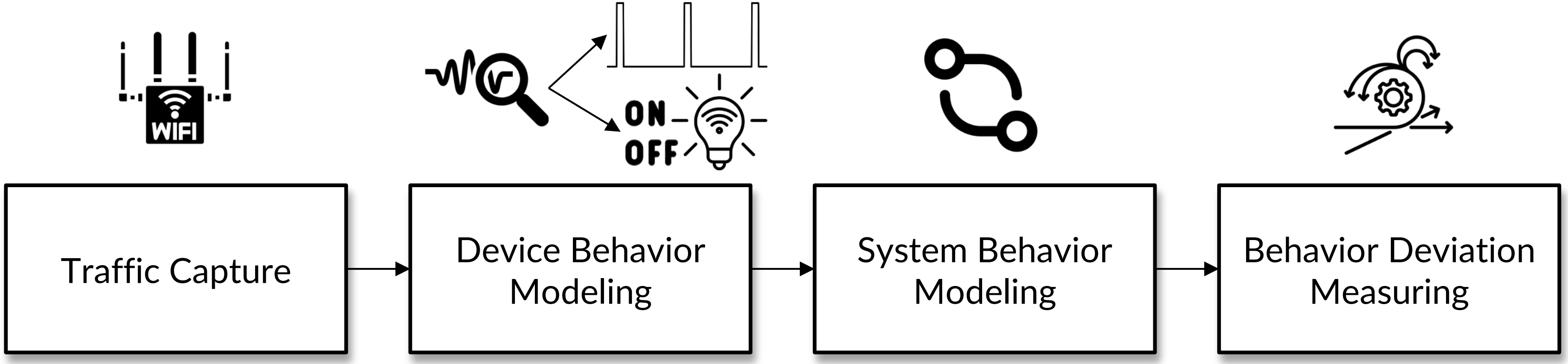
1. **Capture** IoT devices' encrypted **network traffic**
2. **Characterize** individual **device behavior**
3. **Characterize** smart home **system behavior**

Our Approach - BehavIoT



1. **Capture** IoT devices' encrypted **network traffic**
2. **Characterize** individual **device behavior**
3. **Characterize** smart home **system behavior**
4. **Measure and quantify behavior deviation**

Our Approach - BehavIoT



Key advantages of the approach

- works across **a wide range of IoT devices**.
- requires **no privileged access** to devices or APIs. Deployable on routers.
- models behaviors of both **individual devices and a smart home system**

Testbed & Datasets

Traffic Capture → Device Behavior Modeling → System Behavior Modeling → Behavior Deviation Measuring

49 devices from a wide range of categories

Testbed & Datasets

Traffic Capture — Device Behavior Modeling — System Behavior Modeling — Behavior Deviation Measuring

- **Controlled interactions** (4,230 experiments):

  Capture device behaviors of actual functions.

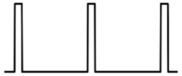
49 devices from a wide range of categories

Traffic Capture → Device Behavior Modeling → System Behavior Modeling → Behavior Deviation Measuring

Testbed & Datasets

- **Controlled interactions** (4,230 experiments):
  Capture device behaviors of actual functions.

- **Idle experiments** (5 days):
  Capture device periodic background behaviors.



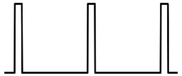
49 devices from a wide range of categories

Testbed & Datasets

Traffic Capture → Device Behavior Modeling → System Behavior Modeling → Behavior Deviation Measuring

- **Controlled interactions** (4,230 experiments):
  Capture device behaviors of actual functions.

- **Idle experiments** (5 days):
  Capture device periodic background behaviors.



- **Routines** (16 routines, 24 hours):
  Capture smart home system behaviors.

IFTTT

49 devices from a wide range of categories

Traffic Capture — Device Behavior Modeling — System Behavior Modeling — Behavior Deviation Measuring

Testbed & Datasets

- **Controlled interactions** (4,230 experiments):
  Capture device behaviors of actual functions.
- **Idle experiments** (5 days):
  Capture device periodic background behaviors.
- **Routines** (16 routines, 24 hours):
  Capture smart home system behaviors.
- **Uncontrolled interactions** (3 months, 40 participants, IRB-approved):
  Measure behavior deviation over time.

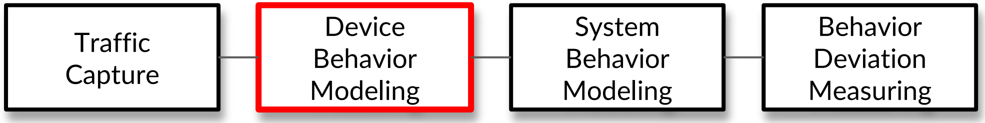
49 devices from a wide range of categories

Research Questions

RQ1: How do we measure and characterize the behaviors of smart home system from their mostly encrypted network traffic?

RQ2: How do we measure and characterize behavior deviations of a smart home system?

Methods

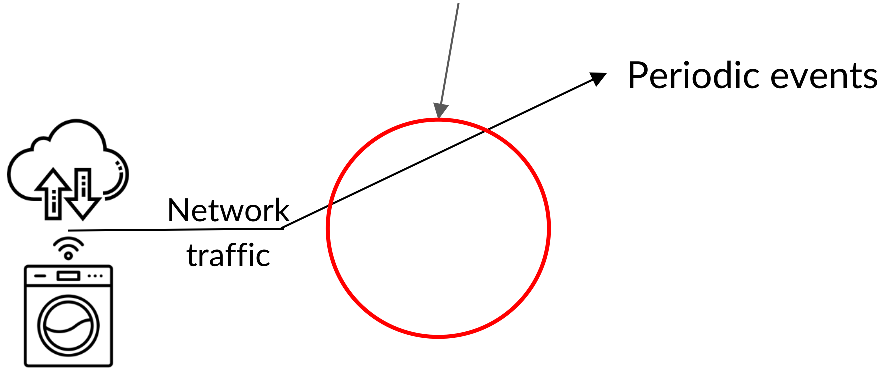

Traffic Capture
Device Behavior Modeling
System Behavior Modeling
Behavior Deviation Measuring

Traffic Capture — Device Behavior Modeling — System Behavior Modeling — Behavior Deviation Measuring

Methods

→ periodic

Event Inference:
Classify traffic → events



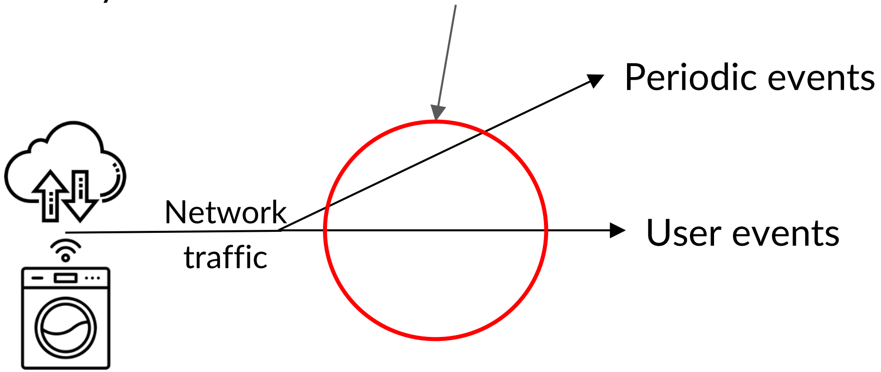
Methods

Traffic Capture → **Device Behavior Modeling** → System Behavior Modeling → Behavior Deviation Measuring

→ periodic

→ correlate wit device functionality

Event Inference:
Classify traffic → events



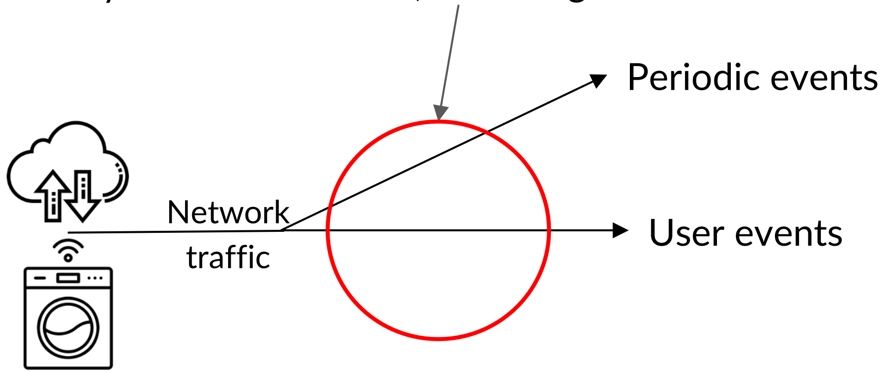
Methods

Traffic Capture | Device Behavior Modeling | System Behavior Modeling | Behavior Deviation Measuring

→ periodic

→ correlate wit device functionality

Event Inference:
Classify traffic → events
DFT + Autocorrelation
ML (Clustering & Random Forest)



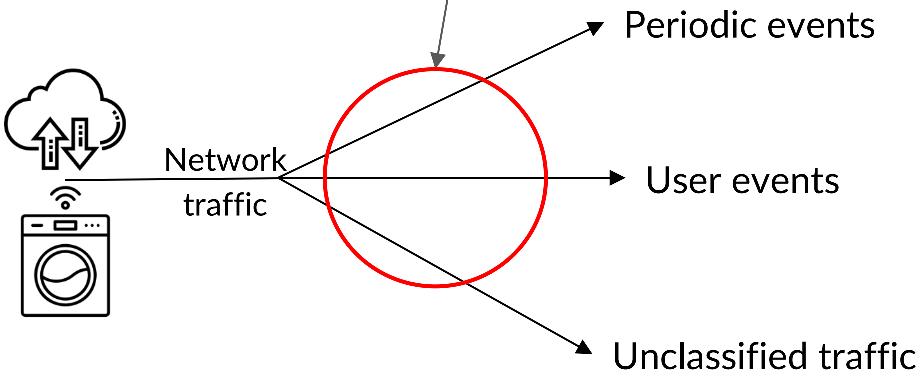
Traffic Capture | **Device Behavior Modeling** | System Behavior Modeling | Behavior Deviation Measuring

Methods

→ periodic

→ correlate wit device functionality

Event Inference:
Classify traffic → events
DFT + Autocorrelation
ML (Clustering & Random Forest)



Methods

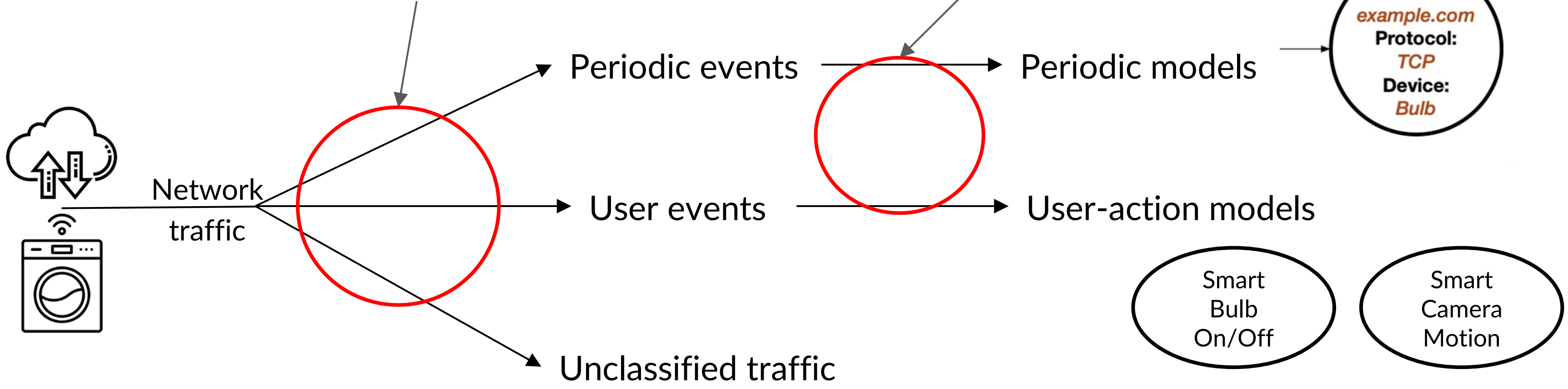
Traffic Capture — **Device Behavior Modeling** — System Behavior Modeling — Behavior Deviation Measuring

→ periodic

→ correlate wit device functionality

Event Inference:
Classify traffic → events
DFT + Autocorrelation
ML (Clustering & Random Forest)

Model generation:
Annotate with labels



Key Takeaways

RQ1: How do we measure and characterize the behaviors of smart home system from their network traffic?

Key Takeaways

RQ1: How do we measure and characterize the behaviors of smart home system from their network traffic?

The vast majority of IoT (mostly encrypted) traffic (99.3%) **can be modeled**.

Key Takeaways

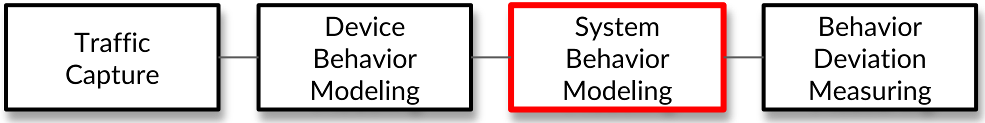
RQ1: How do we measure and characterize the behaviors of smart home system from their network traffic?

The vast majority of IoT (mostly encrypted) traffic (99.3%) **can be modeled**.

The vast majority of IoT traffic (97.8%) i**s periodic**.

A small portion of traffic (0.675%) cannot be modeled — most from devices running complex software.

Methods



Key insight: can be modeled as a finite state machine

09:15:10 Echo Spot Voice
09:15:12 TP-Link Plug On
09:16:13 Echo Spot Voice
09:16:15 TP-Link Plug Off
......

Methods

Traffic Capture — Device Behavior Modeling — System Behavior Modeling — Behavior Deviation Measuring

Key insight: can be modeled as a finite state machine

09:15:10 Echo Spot Voice
09:15:12 TP-Link Plug On
09:16:13 Echo Spot Voice
09:16:15 TP-Link Plug Off
……

1. Combine temporally **correlated user events into traces**

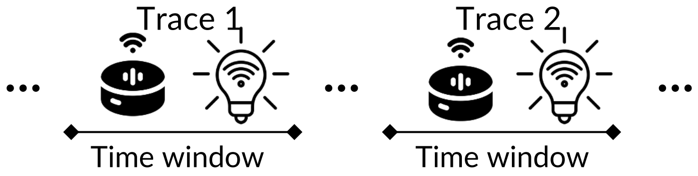
Traffic Capture | Device Behavior Modeling | System Behavior Modeling | Behavior Deviation Measuring

Methods

Key insight: can be modeled as a finite state machine

09:15:10 Echo Spot Voice
09:15:12 TP-Link Plug On
09:16:13 Echo Spot Voice
09:16:15 TP-Link Plug Off
……

1. Combine temporally **correlated user events into traces**

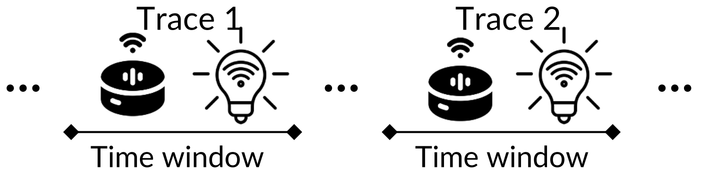


Methods

Traffic Capture | Device Behavior Modeling | **System Behavior Modeling** | Behavior Deviation Measuring

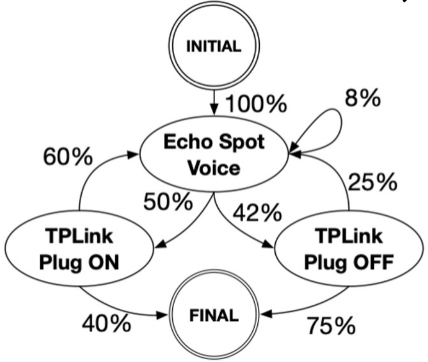
Key insight: can be modeled as a finite state machine

09:15:10 Echo Spot Voice
09:15:12 TP-Link Plug On
09:16:13 Echo Spot Voice
09:16:15 TP-Link Plug Off
……



1. Combine temporally **correlated user events into traces**

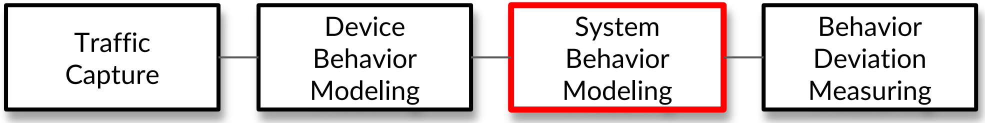
2. Generate a **probabilistic finite state machine (PFSM) model from traces** using Synoptic [1]



- State: user activity
- Transition: probability

[1] Beschastnikh, Ivan, et al. "Leveraging existing instrumentation to automatically infer invariant-constrained models." *Proceedings of the 19th ACM SIGSOFT symposium and the 13th European conference on Foundations of software engineering*. 2011.

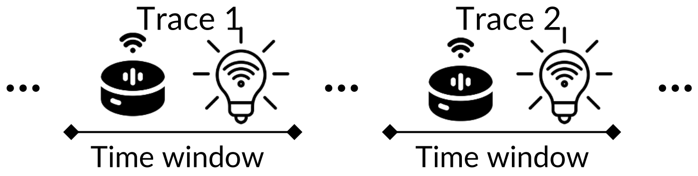
Methods



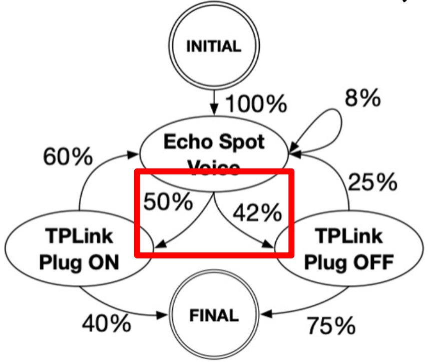
Key insight: can be modeled as a finite state machine

09:15:10 Echo Spot Voice
09:15:12 TP-Link Plug On
09:16:13 Echo Spot Voice
09:16:15 TP-Link Plug Off
……

1. Combine temporally **correlated user events into traces**



2. Generate a **probabilistic finite state machine (PFSM) model from traces** using Synoptic [1]



- State: user activity
- Transition: probability

[1] Beschastnikh, Ivan, et al. "Leveraging existing instrumentation to automatically infer invariant-constrained models." *Proceedings of the 19th ACM SIGSOFT symposium and the 13th European conference on Foundations of software engineering*. 2011.

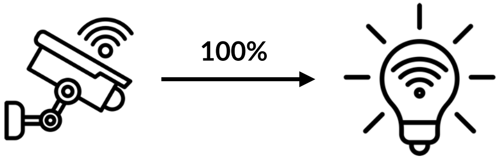
Key Takeaways

RQ1: How do we measure and characterize the behaviors of smart home system from their (mostly encrypted) network traffic?

Key Takeaways

RQ1: How do we measure and characterize the behaviors of smart home system from their (mostly encrypted) network traffic?

- Capture both
  - programmed behaviors introduced by automations

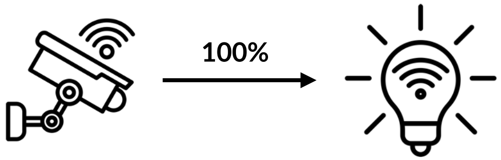


Automation: turn on light if motion is detected

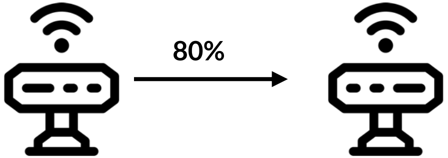
Key Takeaways

RQ1: How do we measure and characterize the behaviors of smart home system from their (mostly encrypted) network traffic?

- Capture both
  - programmed behaviors introduced by automations
  - non-programmed behaviors introduced by human interactions



Automation: turn on light if motion is detected



Co-located motion sensors

Research Questions

RQ1: How do we measure and characterize the behaviors of smart home system from their mostly encrypted network traffic?

RQ2: How do we measure and characterize behavior deviations of a smart home system?

Methods

Traffic Capture — Device Behavior Modeling — System Behavior Modeling — **Behavior Deviation Measuring**

Identify significant changes in behavior

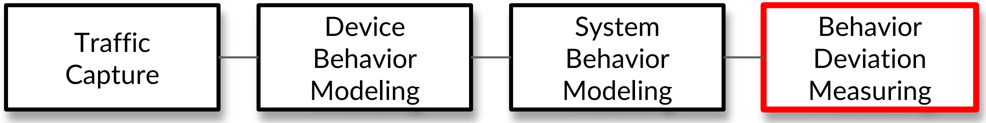
Methods

Traffic Capture — Device Behavior Modeling — System Behavior Modeling — **Behavior Deviation Measuring**

Identify significant changes in behavior

- **Deviation metrics** that quantify the amount of behavior change
- Thresholds to capture **statistically significant deviations**

Methods



Identify significant changes in behavior

- **Deviation metrics** that quantify the amount of behavior change
- Thresholds to capture **statistically significant deviations**

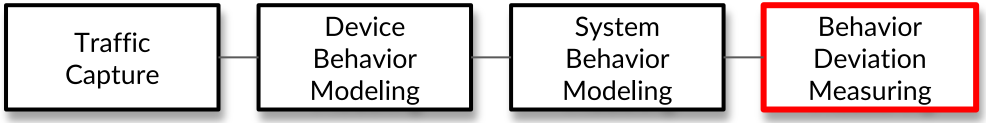
Traffic Capture → Device Behavior Modeling → System Behavior Modeling → **Behavior Deviation Measuring**

Methods

Identify significant changes in behavior

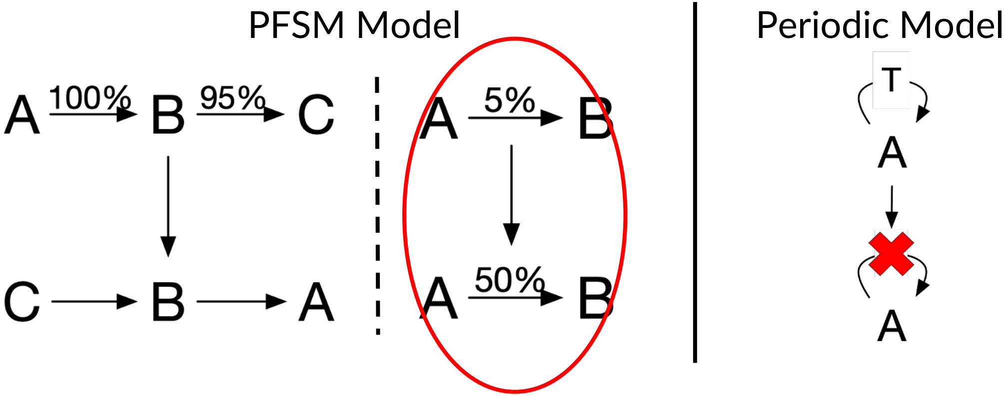
- **Deviation metrics** that quantify the amount of behavior change
- Thresholds to capture **statistically significant deviations**

Methods



Identify significant changes in behavior

- **Deviation metrics** that quantify the amount of behavior change
- Thresholds to capture **statistically significant deviations**



Key Takeaways

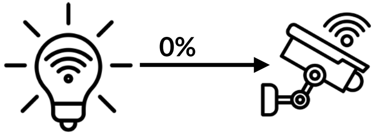
RQ2: How do we measure and characterize behavior deviations of a smart home system?

- Our metrics identify significant deviations from real-world examples

Key Takeaways

RQ2: How do we measure and characterize behavior deviations of a smart home system?

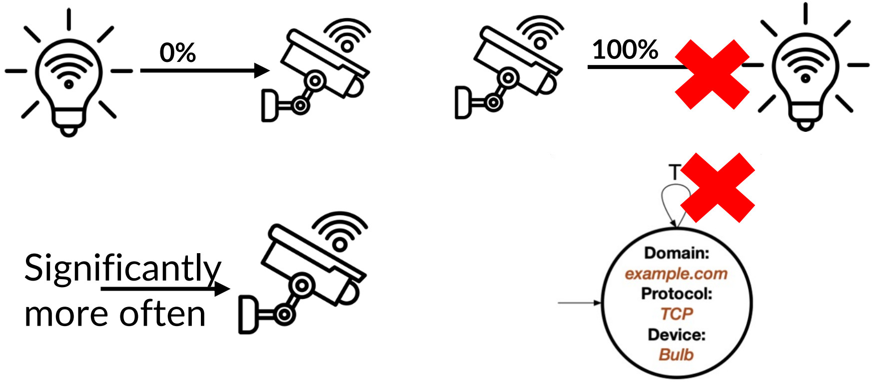
- Our metrics identify significant deviations from real-world examples



Key Takeaways

RQ2: How do we measure and characterize behavior deviations of a smart home system?

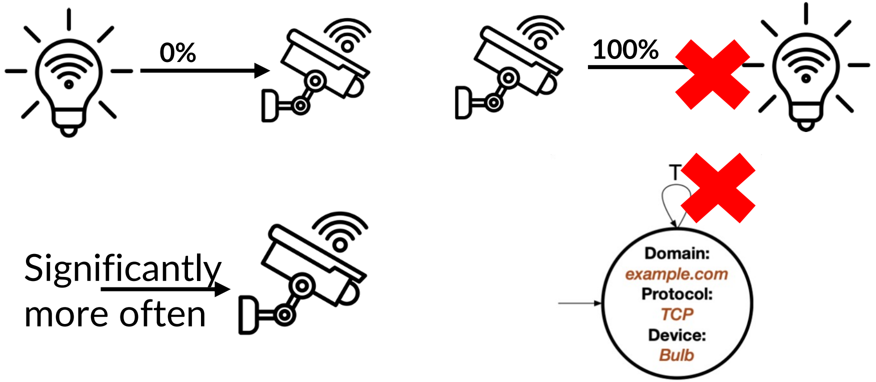
- Our metrics identify significant deviations from real-world examples



Key Takeaways

RQ2: How do we measure and characterize behavior deviations of a smart home system?

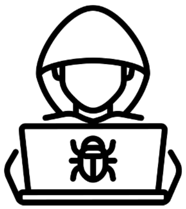
- Our metrics identify significant deviations from real-world examples



- We detect a total of 177 significant behavior deviations (2 per day on average) among three months
    - **Device malfunctions and misconfiguration**
    - **Misactivation**
    - **Network outages**
    - **Change of device positions**
    - **Change of user habits, etc.**

Behavior Model Applications

- **Create IoT profiles** (MUD RFC8520) and **verify compliance** to existing profiles.
- **Behavior triage to help with auditing** such as security, regulatory, and privacy.
- **Allocate attention to significant behavior deviation**



Conclusion

- **Characterize IoT device and system behaviors**:
  - Most smart home devices are **amenable to modeling** through network traffic.
  - 97% of traffic is periodic; 2.33% is due to user actions; 0.68% is unmodelable.
- **Measure behavior deviation over time:**
  - Detect and quantify a range of behavior deviations.
  - Behavior was relatively stable during a longitudinal study
- **BehavIoT benefits:** creating IoT profiles, triage behaviors and deviation

Thank you!

Datasets and code available here:

https://moniotrlab.khoury.northeastern.edu/behaviot/