# Anomaly Detection for Smart Home Based on User Behavior

Masaaki Yamauchi[1], Yuichi Ohsita[1], Masayuki Murata[1], Kensuke Ueda[2], Yoshiaki Kato[3]

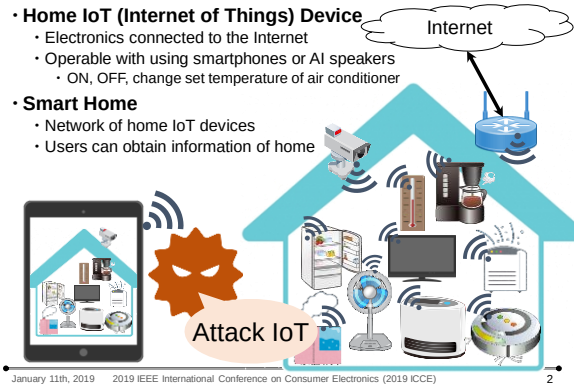
[1]Graduate School of Information Science and Technology, Osaka University.
[2]Advanced Technology R&D Center, Mitsubishi Electric Corporation.
[3]Information Technology R&D Center, Mitsubishi Electric Corporation.

OSAKA UNIVERSITY
Mitsubishi Electric Cybersecurity Research Alliance Laboratories



## Home IoT, Smart Home

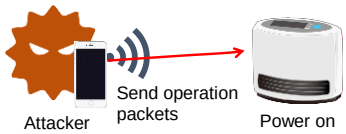
- **Home IoT (Internet of Things) Device**
  - Electronics connected to the Internet
  - Operable with using smartphones or AI speakers
    - ON, OFF, change set temperature of air conditioner
- **Smart Home**
  - Network of home IoT devices
  - Users can obtain information of home






## Anomalous Operation of Home IoT

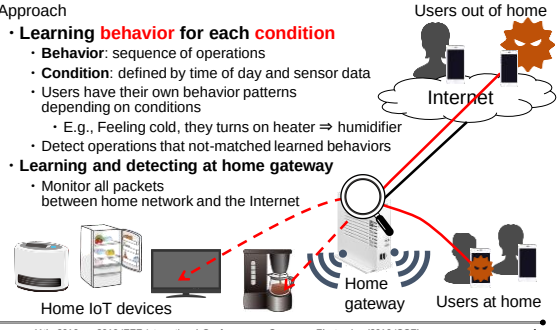
- **Attackers send operation packets to home IoT devices**
  - Make users unsafe and may even harm them
    - Operating heater causes fire
    - Change settings of healthcare devices may harm users
- **Difficult to detect attacks by the pattern matching**
  - Sending same packets as sent by legitimate users
  - Sending packets via compromised smartphones of legitimate user






## Goal and Approach

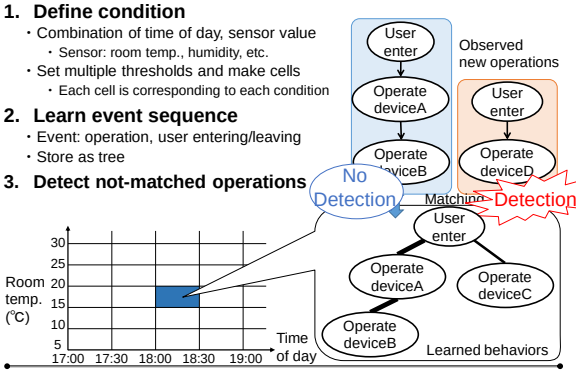
- Goal
  - **Detect the anomalous operation of home IoT devices**
- Approach
  - **Learning behavior for each condition**
    - **Behavior**: sequence of operations
    - **Condition**: defined by time of day and sensor data
    - Users have their own behavior patterns depending on conditions
      - E.g., Feeling cold, they turns on heater ⇒ humidifier
    - Detect operations that not-matched learned behaviors
  - **Learning and detecting at home gateway**
    - Monitor all packets between home network and the Internet






## Learning Behaviors and Detection Model

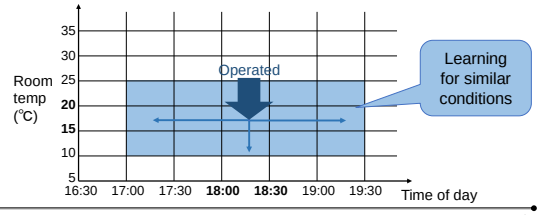
1. **Define condition**
   - Combination of time of day, sensor value
     - Sensor: room temp., humidity, etc.
   - Set multiple thresholds and make cells
     - Each cell is corresponding to each condition
2. **Learn event sequence**
   - Event: operation, user entering/leaving
   - Store as tree
3. **Detect not-matched operations**





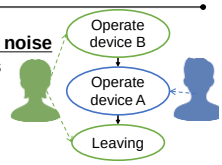

## Learning Small Data

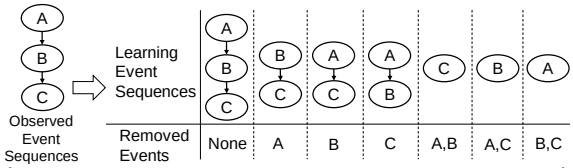
- Difficulty
  - **Only a small number of events for each condition**
    - Number of user's operation of home IoT devices are limited
- Idea
  - **Learning behaviors for similar conditions**
    - Users behave same as for similar conditions



## Removing Noise Events

- Difficulty
  - **Included events from other user as noise**
    - Typical smart home has multiple users
- Idea
  - **Generate multiple sequences by removing some events**
    - Learnable essential sequences
  - **Use only sequences for detection done for multiple times**
    - Essential behaviors would be done for multiple times

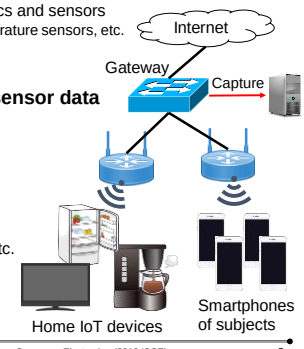





## Evaluation Environment

- **Construct a network of home IoT devices in our lab**
  - 15 kinds of consumer electronics and sensors
    - heaters, a coffee maker, temperature sensors, etc.
  - 4 subjects
- **Captured all packets and sensor data**
  - Recorded the times of
    - Operation of home IoT devices
    - Entering or leaving of users
- **Defined the condition by only the time of day**
  - Room temperature, humidity, etc. did not change significantly in our environment






## Evaluation

- **Dataset**
  - Adding 100 operations per day at random time into captured packets
  - Legitimate operations: operations of subjects in the captured data
  - Anomalous operations: added 100 operations per day
- **Parameter Setting**
  - Using data monitored in the 1st week for each month
- **Method**
  - LOO-CV (Leave-One-Out Cross-Validation)
    - Test data: one of data separated by day added 100 operations
    - Learning data: the others
    - Sum up results of each day and calculate $Detection$ and $Misdetection\ Ratio$
- **Metrics**
  - $Detection\ Ratio = \frac{\#\ of\ \textbf{Detected}\ Anomalous\ Operations}{\#\ of\ \textbf{Added}\ Anomalous\ Operations}$
  - $Misdetection\ Ratio = \frac{\#\ of\ \textbf{Misdetected}\ Legitimate\ Operations}{\#\ of\ Legitimate\ Operations}$



## Results – for 1 month

- **Detected 95-100% attacks with only a few misdetections**
  - Behaviors for each condition were enough learned
- **Difficult to detect device including "Single Operation"**
  - "Single Operation": not observed previous or subsequent event
  - Use only condition information, cannot use sequence information
  - Operated at various times of day
- **Difficult to detect that monitored event sequences vary quite a lot**
  - Rare operations

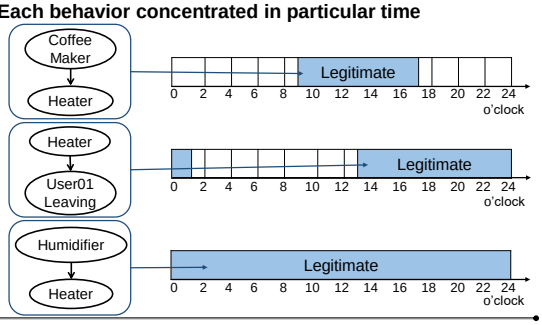
January 2017

| | Detection Ratio | Detected / Total | Misdetection Ratio | Misdetected / Total |
|---|---|---|---|---|
| Heater | **0.959** | 2110/2200 | 0.182 | **2**/11 |
| TV B | **1.000** | 2200/2200 | 0.000 | **0**/2 |
| Coffee maker | **0.157** | 346/2200 | 0.000 | 0/48 |
| Humidifier | **0.080** | 176/2200 | 0.000 | 0/38 |
| TV A | **1.000** | 2200/2200 | **1.000** | 8/8 |



## Learned Behaviors of Heater

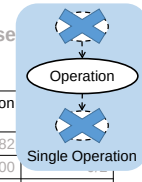
- **Heater's operation is related to other devices' operation and user's leaving**
- **Each behavior concentrated in particular time**






## Results – for 1 month

- **Detected 95-100% attacks with only a few misdetections**
  - Enough learned sequences for particular conditions
- **Difficult to detect device including "Single Operation"**
  - "Single Operation": not observed previous or subsequent event
  - Use only condition information, cannot use sequence information
  - Operated at various times of day
- **Difficult to detect that monitored event se quite a lot**
  - Rare operations




January 2017

| | Detection Ratio | Detected / Total | Misdetection Ratio | |
|---|---|---|---|---|
| Heater | 0.959 | 2110/2200 | 0.182 | |
| TV B | 1.000 | 2200/2200 | 0.000 | 0/2 |
| Coffee maker | **0.157** | 346/2200 | 0.000 | 0/48 |
| Humidifier | **0.080** | 176/2200 | 0.000 | 0/38 |
| TV A | 1.000 | 2200/2200 | **1.000** | 8/8 |

## Results – for 1 month

- Detected 95-100% attacks with only a few misdetections
  - Enough learned sequences for particular conditions
- Difficult to detect device including “Single Operation”
  - “Single Operation”: not observed previous or subsequent event
  - Use only condition information, cannot use sequence information
  - Operated at various times of day
- **Difficult to detect that monitored event sequences vary quite a lot**
  - Rare operations

January 2017

| | Detection Ratio | Detected / Total | Misdetection Ratio | Misdetected / Total |
|---|---|---|---|---|
| Heater | **0.959** | 2110/2200 | 0.182 | **2**/11 |
| TV B | **1.000** | 2200/2200 | 0.000 | **0**/2 |
| Coffee maker | **0.157** | 346/2200 | 0.000 | 0/48 |
| Humidifier | **0.080** | 176/2200 | 0.000 | 0/38 |
| TV A | **1.000** | 2200/2200 | **1.000** | 8/8 |



## Results – for 3 months

- **Detected more than 99% attacks with only a few misdetections**
- Misdetection ratios of TVs are smaller than 1 month
  - Using more event sequences to learn legitimate behaviors
- Difficult to detect devices including single operations

April, June, and August 2017

| | Detection ratio | Detected / Total | Misdetection ratio | Misdetected / Total |
|---|---|---|---|---|
| Electric fan A | **0.998** | 6384/6400 | 0.000 | **0**/9 |
| Electric fan B | **0.999** | 6399/6400 | 0.000 | **0**/6 |
| TV A | **0.996** | 6377/6400 | 0.171 | **7**/41 |
| TV C | **0.999** | 6397/6400 | 0.000 | **0**/10 |
| TV D | **0.999** | 6398/6400 | 0.111 | **1**/9 |
| Coffee maker | **0.611** | 3908/6400 | 0.058 | 3/52 |



## Results – for 3 months

- Detected more than 99% attacks with only a few misdetections
- **Misdetection ratios of TVs are smaller than 1 month**
  - Using more event sequences to learn legitimate behaviors
- Difficult to detect devices including single operations

April, June, and August 2017

| | Detection ratio | Detected / Total | Misdetection ratio | Misdetected / Total |
|---|---|---|---|---|
| Electric fan A | **0.998** | 6384/6400 | 0.000 | **0**/9 |
| Electric fan B | **0.999** | 6399/6400 | 0.000 | **0**/6 |
| TV A | **0.996** | 6377/6400 | 0.171 | **7**/41 |
| TV C | **0.999** | 6397/6400 | 0.000 | **0**/10 |
| TV D | **0.999** | 6398/6400 | 0.111 | **1**/9 |

January 2017

| | Detection Ratio | Detected / Total | Misdetection Ratio | Misdetected / Total |
|---|---|---|---|---|
| TV A | 1.000 | 2200/2200 | **1.000** | **8/8** |



## Results – for 3 months

- Detected more than 99% attacks with only a few misdetections
- Misdetection ratios of TVs are smaller than 1 month
  - Using more event sequences to learn legitimate behaviors
- **Difficult to detect devices including single operations**

April, June, and August 2017

| | Detection ratio | Detected / Total | Misdetection ratio | Misdetected / Total |
|---|---|---|---|---|
| Electric fan A | **0.998** | 6384/6400 | 0.000 | **0**/9 |
| Electric fan B | **0.999** | 6399/6400 | 0.000 | **0**/6 |
| TV A | **0.996** | 6377/6400 | 0.171 | **7**/41 |
| TV C | **0.999** | 6397/6400 | 0.000 | **0**/10 |
| TV D | **0.999** | 6398/6400 | 0.111 | **1**/9 |
| Coffee maker | **0.611** | 3908/6400 | 0.058 | 3/52 |



## Conclusion and Future Work

- **Detected 95—100% of anomalous operations**
  - With several misdetections (single operations, rare operations)
- **Future Work**
  - Detecting single operations
  - Mitigation of misdetection of rare operations
  - Comparing with other method
  - Using actual home data