Modeling Home IoT Traffic using Users' in-Home Activities for Detection of Anomalous Operations

Masaaki Yamauchi†, Masahiro Tanaka†, Yuichi Ohsita†,
Masayuki Murata†, Kensuke Ueda††, Yoshiaki Kato†††

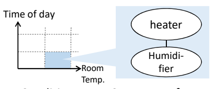
† Graduated School of Information Science and Technology, Osaka University, Japan.
†† Advanced Technology R&D Center, Mitsubishi Electric Corporation, Japan.
††† Information Technology R&D Center, Mitsubishi Electric Corporation, Japan.

Anomalous operations of home IoT

- **Attackers send operation packets to home IoT devices**
  - Make users unsafe and may even harm them
    - Operating heater causes burn
    - 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

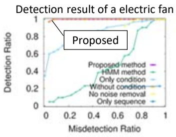
Detection method of anomalous operations [1]

- **Modeling behavior as "sequence of event" for each "condition"**
  - "Sequence of event": order of IoT device's operation, users' entering / leaving
  - "Condition": time of day and observable sensor values (e.g., room temp., noise, …)
  - Detecting unmatched sequences of operations with learned behaviors



- **Detected 90% anomalous operations with 10% misdetections**
  - Evaluation environment:
    - Installed multiple IoT devices in our lab.
  - "Sequence of event" is effective for detection
  - **"Condition" is not well considered**

Detection result of a electric fan



goal: Improving the "condition" by modeling the legitimate traffic focusing on the home conditions especially on the in-home activities

[1] Masaaki Yamauchi, Yuichi Ohsita, Masayuki Murata, Kensuke Ueda, and Yoshiaki Kato, "Anomaly Detection in Smart Home Operation from User Behaviors and Home Conditions," IEEE Transactions on Consumer Electronics, vol. 66, no. 2, pp. 183-192, May 2020.

Modeling home IoT traffic using users' in-home activities

- **Defining states about in-home activities by the combination of**
  - State of users: estimated from home IoT sensors (out of home, sleep, active)
  - State of devices: whose operations are targets of anomaly detection
- **Labeling states to dataset for each time slot**
- **Calculating**
  - state transition probability for each time-of-day
  - probabilities of operating device in each state

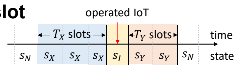


Fig.: Definition of state of devices

slot	date	used device	sensors	state of users	state of devices
1	08:59	---	Noise: 30, CO2: 35, …	sleeping	s_X
2	09:00	cooking stove	Noise: 50, CO2: 55, …	active	s_I
3	09:01	---	Noise: 40, CO2: 40, …	active	s_Y
4	09:02	house key	Noise: 35, CO2: 40, …	out	s_N

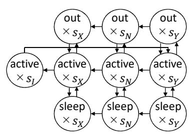
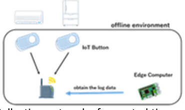


Fig.: State transition model

Evaluation

- **Collecting time of operating home appliances in a real home for 4 months**
  - Set buttons to record the operating time
  - Sensed temp., humidity, CO2 concentration, noise
- **Target: cooking stoves**
  - Used for many times
  - Anomalous operation of the cooking stoves causes fire

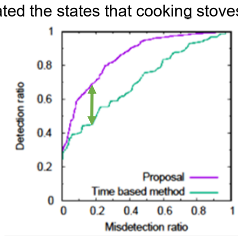


Collecting network of operated time

- **Method**
  - Leave-one-out cross-validation
    - Test data: one of data separated by day
      - adding an anomalous operation in each minute
    - Training data: the others
    - Sum up results of each day and calculate detection and misdetection ratio
  - Compared with method[1] using only condition defined by the time-of-day
- **Metrics**
  - Detection ratio = $\frac{\#\ of\ \mathbf{detected}\ anomalous\ operations}{\#\ of\ \mathbf{added}\ anomalous\ operations}$
  - Misdetection ratio = $\frac{\#\ of\ \mathbf{misdetected}\ legitimate\ operations}{\#\ of\ legitimate\ operations}$

Result

- **Detected 72.3% anomalous operations with 20.1% misdetections**
- **More higher detection ratio than the time based method**
  - Based on the AUC
  - Accurately estimated the states that cooking stoves tend to be used



Conclusion

- **Modeled home IoT traffic based on users' in-home activities**
  - Defined by state transition model from device operation and sensor data
  - Calculating the transition probability and the operation probability of each state
  - Estimate the current state from the learned model and current observations
- **Demonstrated estimation accuracy by anomaly detection**
  - More higher detection ratio than the time based method
    - Detected 72.3% anomalous operations with 20.1% misdetections
    - Used dataset collected in a real home
- **[Future work]**
  - Evaluate the case that combining our model and the method using the operation sequences
  - Evaluate the detection results of other devices
    - Heater, air conditioner, lighting, fan, washing machine, TV