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

- 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

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

Method

- Leave-one-out cross-validation
  - Test data: one of data separated by day
  - Retaining data of others
  - Sum-up results of each day and calculate detection and misdetection ratio
- Compared with method(s) using only condition defined by the time-of-day

Metrics

- Detection ratio = \[ \frac{\text{# detected anomalous operations}}{\text{# added anomalous operations}} \]
- Misdetection ratio = \[ \frac{\text{# misdetection legitimate operations}}{\text{# legitimate operations}} \]

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

September 22nd, 2020 ITC32 PhD Workshop