Anomaly Detection in Smart Home Networks using Situation Estimation in-Home Activities

田中　雅弘

大阪大学　大学院情報科学研究科
村田研究室

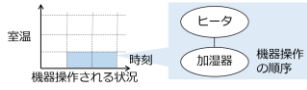
ホームIoT 機器における不正操作

- **深刻な問題に直結**
  - 生命に危険がおよぶ可能性[1]
    - 例：ヒータの不正操作による火傷/火災
  - 電力網への損害の可能性[2]
- **従来のパターンマッチングによる検知が困難**
  - 乗っ取ったスマートフォン、スマートスピーカを経由する可能性
    - 正常な操作と同じプロトコルに従って不正操作
  - 機器操作に関するデータの数が少ない
    - 統計的手法や深層学習が困難

[1]N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart homesecurity: Issues, challenges and countermeasures,"IEEE Communications Surveys &Tutorials, vol. 16, no. 4, pp. 1933–1954, 2014.
[2]S. Soltan, P. Mittal, and H. V. Poor, "Blackiot: Iot botnet of high wattage devicescan disrupt the power grid," in27th USENIX Security Symposium (USENIX Security18), 2018, pp. 15–32.

宅内のユーザの行動パターンに基づく異常検知手法[3]

- **手法**
  - 機器操作時の状況と行動順序を、行動パターンとして学習
    - 状況：操作が行われた時刻、室温
    - 行動順序：機器の操作やユーザの入退室などが行われる順序
  - 各状況の行動パターンと一致しない操作を検知



- **単独で使用される機器の検知精度が低い**
  - 行動順序が存在しないため
- **「状況」の定義について詳しく検討が必要**
  - 同じ時刻、室温でも操作される確率は異なる
  - 例)コンロが操作される状況
    - 家族が夕飯の準備中：頻繁に使用
    - 家族が全員睡眠中：使用されない

[3]M. Yamauchi, Y. Ohsita, M. Murata, K. Ueda, and Y. Kato, "Anomaly detection for smart home based on user behavior," in 2019 IEEE International Conference on Consumer Electronics (ICCE). IEEE, 2019, pp. 1–6.

研究目的と提案手法

- **研究目的**

**機器が操作される宅内の状況を判別し、
IoT 機器の不正操作の検知精度を向上させる**

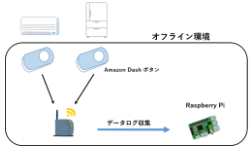
- **アプローチ**

**機器操作履歴とセンサデータから宅内の状態の遷移を推定し、
機器が操作されやすい状況を学習する**

1. 機器操作とセンサデータから状態遷移モデルを定義
2. 遷移確率の各状態の操作確率を計算し学習
3. 機器操作履歴とセンサデータから現在の状態を推定

研究方法　データ収集のためのシステム

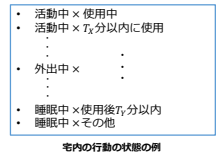
- **データ収集のためのシステムを構築**
  - 各家電に対応したAmazon Dash ボタンを設置
  - 家電を使用した際、対応したAmazon Dash ボタンを押す
  - Raspberry Pi でボタンを押したタイミングを記録



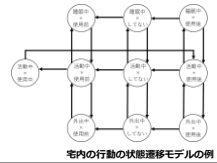
- **実際の家庭においてデータを収集**
  - 上記のシステムを実際の家庭に導入
  - IoT センサを設置
    - 室温センサ、湿度センサ、騒音センサ、気圧センサ、CO2センサ
    - プライバシーを考慮

宅内の活動の状態遷移モデル

- **宅内の活動の状態を定義**
  - ユーザの状態と機器の状態の組み合わせによって定義
    - ユーザの状態
      - センサデータから推定される宅内のユーザの状態
      - 取得できるセンサデータの種類、精度から決定
      - 例）「活動中」「睡眠中」「外出中」
    - 機器の状態
      - 不正操作検出の対象である機器の状態
      - 「使用中」「T_X分以内に使用」「使用後T_Y分以内」「その他」の４状態
- **遷移確率と各状態での機器操作確率によりモデル化**



宅内の行動の状態の例



宅内の行動の状態遷移モデルの例

現在の宅内の状態推定と不正操作検知

1. 初期化
- 開始時はどの状態であるか不明
- 全ての状態が同じ確率になるよう初期化
- $\alpha_0(i) = \frac{1}{C}$

C：状態数
$\alpha_t(i)$: 時刻tにおける状態iである確率

2. 状態遷移
- 学習した状態遷移確率を掛け合わせることにより遷移
- $\hat{\alpha}_t(i) = \sum_C \alpha_{t-1}(c)\, a_{T(t-1)}(c,i)$

a：状態遷移確率

3. 観測値による補正
- 観測された機器操作、センサデータを使用
- ベイズ推定を行うことにより補正
- $P(x_t|S_t = i) = \prod_n \beta(x)(x_t,i,n) \quad \beta(x)(x_t,i,n) = \begin{cases} b(i,n) & n \in x_t \\ 1 & n \notin x_t \end{cases}$
- $\alpha_t(i) = \frac{P(x_t|S_t=i)\hat{\alpha}_t(i)}{\sum_j P(x_t|S_t=j)\hat{\alpha}_t(i)}$

b：機器操作確率

4. 検知
- 現在の状態確率を用いて不正操作を検知

評価方法

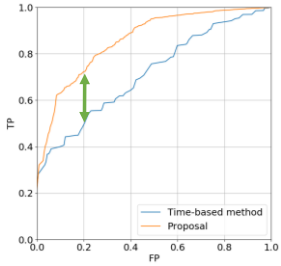
- **比較対象：時間帯のみを利用した手法**
- **検知対象：コンロ**
  - 実際の家庭で頻繁に使用
  - 火災などの深刻な問題
- **評価方法**
  - 1家庭の4か月間 (2018年12月 ～ 2019年3月)
  - テストデータに毎分不正操作を混入
  - LOO-CV (Leave-One-Out Cross-Validation)
    - 学習データ：特定の1日分を除くデータ
    - テストデータ：特定の１日分
    - 各日の結果を合算し検知率、誤検知率を算出
- **評価指標**
  - 検知率 $= \frac{\text{検知した不正操作数}}{\text{混入した不正操作の総数}}$
  - 誤検知率 $= \frac{\text{誤検知した正常操作数}}{\text{正常操作の総数}}$

パラメータの設定

T_X	30
T_Y	30
T_Z	30

評価結果

- **誤検知率 20.1% で、検知率72.3%**
- **時刻のみを用いた状況定義手法よりもAUCにおいて改善**



比較手法と提案手法のROC曲線

まとめと今後の課題

- **本研究のまとめ**
  - 実家庭においてデータ収集
  - 宅内の行動の推定を用いた手法を提案
    - 機器操作とセンサデータから宅内の行動を状態遷移モデルで定義
    - 遷移確率と各状態の操作確率を計算することで学習
    - 学習された確率と、現在の観測値から現在の宅内の状態を推定
    - 推定された宅内の状態から不正操作の検知
  - 実際の家庭から得られたデータを用いた評価
    - 既存手法のうち、状況情報 (時刻) のみを利用した手法よりも改善
- **今後の課題**
  - 操作パターンを用いた手法とかけ合わせた場合の評価
  - 他の機器での評価
    - ヒータ、エアコン、照明、扇風機、洗濯機、TV