1ZA-05

システム時刻のずれに基づくディジタル機器における特徴量の抽出

並木 涼 † 千川 尚人 † 下馬場 朋禄 ‡ 伊藤 智義 ‡
国立高等専門学校機構 小山高専 † 千葉大学 ‡

1 はじめに

Internet of Things (IoT) 技術の発展に伴い，多様なディジタルデバイスがプラットフォームに依らず通信可能になることで，オープン IoT 社会 [1] が到来すると言われている．しかし，オープン化された IoT 機器を用いたサービスでは，なりすましによる情報漏えいや不正アクセスに対するリスクが高まるため，意図しない相手との通信を避けるために適切に機器を識別する必要がある．我々はこの課題に対する機器識別法として，半導体チップが生成するクロック特性を用いたクロックフィンガープリント手法 [2] を提案し，ディジタル機器固有の特徴量の採取を試みている．本稿では，20 台の Raspberry Pi 3 に対してクロックフィンガープリント手法で用いるシステム時刻のずれを計測し，その結果から機器識別を試みた結果について報告する．

2 研究動機

本研究の以前の成果 [3] ではクロック信号に基づくシステム時刻のずれ方（時刻ドリフト）を計測することでディジタル機器固有の特徴量を抽出した．しかし，この実験では計測した機器の数が少なく，時刻ドリフトの固有性を示すことが困難であった．また，基準サーバの時刻同期にインターネット上の Network Time Protocol (NTP) サーバを利用していたため，ネットワーク遅延が計測誤差に影響を及ぼしてしまう可能性があった．これらの課題に対して我々はローカルネットワーク内に NTP サーバを構築し，より多くの機器に対して時刻ドリフトの計測を行い，その結果を用いてそれぞれの機器の識別を試みた．

Trait Extraction for Digital Equipment Based on Clock Drift
†Ryo NAMIKI, †Naoto HOSHIKAWA,
‡Tomoyoshi SHIMOBABA, and ‡Tomoyoshi ITO
†National Institute of Technology, Oyama College
‡Chiba University

3 機器識別方式

時刻 0 から t までに生じる時刻ドリフトを $D(t)$ とおく．一定間隔で時刻ドリフトを計測する際，i 番目の計測が時刻 t_i に行われるとすると，i, j 番目（$1 \leq i < j$）の計測の間における時刻ドリフト量 $d(i,j)$ は

$$d(i,j) = D(t_j) - D(t_i) \tag{1}$$

と表される．学習用，テスト用としてそれぞれ N 個，M 個の時刻ドリフトデータが与えられるとき，N 個の学習用データに対して，あるサンプリング周期 $S(1 \leq S \leq N-1)$ ごとの時刻ドリフト量の平均 $d_{\mathrm{avg}}(S)$ は

$$d_{\mathrm{avg}}(S) = \frac{\sum_{i=1}^{N-S} d(i, i+S)}{N-S} \tag{2}$$

と求められる．この $d_{\mathrm{avg}}(S)$ をその機器における基準特徴量とする．次に，M 個のテスト用データから学習用データと同一のサンプリング周期 S ごとの時刻ドリフト量の差を求め，この特徴量を予め求めた基準特徴量と比較し，その残差が最小となる機器を識別結果とする．

4 実験内容

実験システムの構成を図 1 に示す．計測対象機器として Raspberry Pi 3(以下，RasPi) を 20 台用意し，Raspbian(April 2018) をインストールしてそれぞれ A から T までの識別子を割り振った．計測対象機器は NTP による時刻同期機能を無効化して実験室内のローカルネットワークに接続された状態であり，時刻の基準サーバは Global Positioning System (GPS) 衛星からの信号に基づき正確な時刻を供給している．基準サーバは 10 分ごとに計測対象機器と基準サーバにおけるシステム時刻の差分を NTP を用いて計測する．ただし，基準サーバが供給する時刻の正確性を保証するため，時刻ドリフトの計測とあわせて情報通信研究機構 (NICT) が運用する Stratum 1 NTP サーバとの時刻差分を記

録する．以上の条件に基づき，2018 年 11 月 19 日から同年 12 月 10 日にかけて時刻ドリフトの計測を行った．機器識別については計測の結果得られた時刻ドリフトを学習用，テスト用データに等分してサンプリング周期を計測の最小単位である 10 分から変化させ，テスト用データから得られた個々の特徴量に対して識別結果の正解率を計算した．

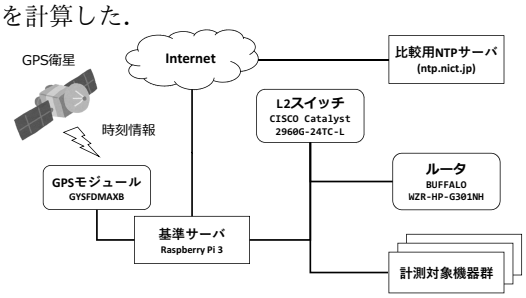

図 1　実験システム構成図

5　実験結果

本節では計測対象機器のうちその特性の傾向が異なる集団から一部を抽出した結果を示す．基準サーバが供給した時刻と NICT の NTP サーバとの時刻の差分は平均して 0.0999 秒であり，その標準偏差は 4.203×10^{-5} 秒であった．また，時刻ドリフトの計測結果からそれぞれの機器の識別を試みたところ，正解率の推移として図 2 に示す結果が得られた．すべての計測対象機器に対する識別結果の平均正解率の推移は図 3 に示す通りである．

6　考察

基準サーバが供給した時刻と NICT の NTP サーバとの時刻の差分はその標準偏差が小さいことからほぼ一定であると考えられる．また図 2 より，サンプリング周期を長くすることで識別結果の正解率が高くなる機器と高くならない機器が存在していることがわかる．これは，特徴量として用いている時刻ドリフト量がこれらの機器の間で類似している，あるいは時刻ドリフト量が変動し正しくない機器の特徴量として取り扱われることに起因すると考えられる．過去の研究 [4] では時刻ドリフト量の変動と環境温度の相関性について検討しているが，学習用データの計測時期とテスト用データの計測時期における環境温度の差が識別結果に影響を及ぼしている可能性がある．一方で図 3 に示したようにサンプリング周期を長くすることで機器識別の全体の正解率が高くなっているが，これは時間の経過によって各機器における特徴量の差が増幅されたことによるものと考えられる．

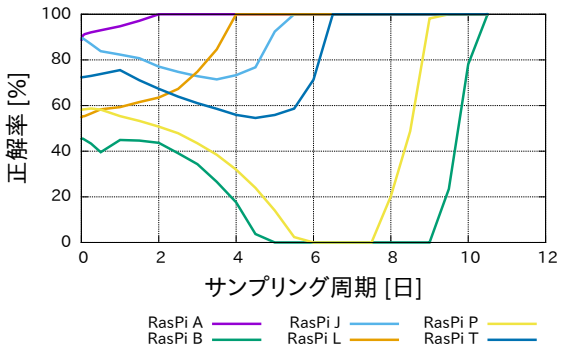

図 2　サンプリング周期に対する機器識別の正解率の推移

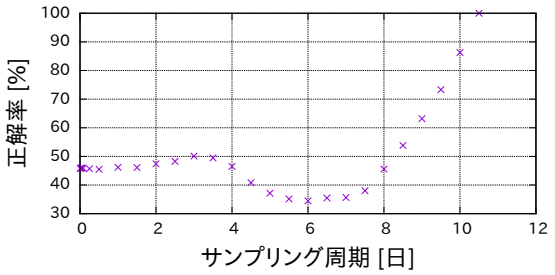

図 3　サンプリング周期に対する機器識別の平均正解率の推移

7　おわりに

本稿では，20 台の Raspberry Pi 3 に対して計測した時刻ドリフトからそれぞれの機器の識別を試みた．今回はサンプリング周期を長くすることで識別精度が高くなったが，長期計測が必要であり迅速性，汎用性に欠けるため，今後はこれらの課題解決に取り組んでいく．

参考文献

[1] 坂村健．オープン IoT 考え方と実践．パーソナルメディア, 12 2016.

[2] 干川尚人, 下馬場朋禄, 伊藤智義．デジタル機器のクロック周波数信号特性に基づく個体識別技術．電子情報通信学会第 16 回ネットワークソフトウェア研究会, 6 2018.

[3] 並木涼, 干川尚人, 下馬場朋禄, 伊藤智義．クロックフィンガープリントを用いた同機種のディジタル機器に対する個体識別手法．電子情報通信学会ソサイエティ大会, 9 2018.

[4] 並木涼, 干川尚人, 下馬場朋禄, 伊藤智義．ディジタル機器におけるシステム時刻のずれと環境温度の変動との相関性．電子情報通信学会第 18 回ネットワークソフトウェア研究会, 1 2019.