IoT 部品・機器・ネットワークの
階層横断セキュリティ技術の研究開発（171503005）

Research and Development on Secure IoT Circuits, IoT Devices and IoT Networks

研究代表者
戸川 望　早稲田大学
Nozomu Togawa　Waseda University

研究期間　平成 29 年度～平成 30 年度

概要
本研究開発では、IoT（「もの」のインターネット）のための階層にまたがるセキュリティ技術の研究開発に取り組んだ。まず①IoT 機器を構成する個別の回路部品に不正部品（ハードウェアトロイと呼ばれる）がない安全な回路設計の実現のため、既知ハードウェアトロイ検出の開発技術を活用し、ハードウェアトロイ検出に機械学習を活用することで、設計レベル回路データに未知ハードウェアトロイが含まれていても、トロイ回路/非トロイ回路の信号線を極めて正確に自動識別する技術を確立した。続いて、②・③IoT 機器・IoT ネットワークのセキュリティを担保する技術に向けて、(ア)『エッジ監視』と『クラウド監視』の 2 つの監視技術を提案し、かつ、(イ) エッジ監視では個別 IoT 機器のサイドチャネル・メインチャネル情報の『局所的混合解析』、クラウド監視では全体 IoT 機器に対して『大局的混合解析』を実施した。特にエッジ監視にて、サイドチャネル情報として IoT 機器の「電力消費波形」に注目し、適切な特徴量を用いることで外れ値検知を行い、(ア) により総合的に IoT 機器の不正動作の検出に成功した。

１．まえがき

一般に、IoT（Internet of Things）機器は極めて多様な規格の組込みプロセッサや通信回路から構成される。これらは、IoT 機器の使用環境、動作環境が多種多様で「IoT 機器がその性質上、その場、その時に最適な構成を持つ」ための必然的な結果であり、今後、将来にわたりこうした状況は継続することが予想される。こうした IoT 機器のセキュリティに焦点を当てたとき、標準規格を持つ PC やサーバ機器が標準化された組込みソフトウェアとネットワーク監視によって比較的簡単にセキュリティ対策がとれるのに対し、IoT 機器は、上述のような多様性・複雑性のために、画一的・統一的なセキュリティ対策をとることができず、外部からの多様な「攻撃」を受ける危険性が極めて高い。IoT 化に伴う外部攻撃・不正侵入の危険性は、PC やサーバ機器と同等以上に大きいにも拘らず、IoT 機器のセキュリティリスクを回避する手段は極めて乏しいのが現実で、これに関する研究開発をさまざまな側面から早急に進めることは特に我が国の喫緊の課題と言える。
一方、一概に「IoT のセキュリティ」と言った場合、IoT 機器はネットワーク化され初めてその真価を発揮することから、本質的に IoT 機器単体のセキュリティを担保するだけでは不十分であり、その IoT 機器の構成部品、また複数の IoT 機器がネットワーク化されたシステム全体のセキュリティを担保する必要がある。

本研究開発では「IoT 全体のセキュリティ」を以下のように、不正動作なく正常に動作する IoT 部品・IoT 機器・IoT ネットワークの 3 階層（①～③）と位置付ける:

① （IoT 部品のセキュリティ）IoT 機器を構成する個別の回路部品に不正部品がない安全な回路設計を実現する(後述するようにこのような不正部品は総称して「ハードウェアトロイ」と呼ばれる)。つまり、ハードウェアトロイを検出し、ハードウェアトロイフリーの回路部品設計を実現する。
② （IoT 機器のセキュリティ）IoT 機器が不正動作や不正侵入なく正常動作することを担保する（エッジ側のセキュリティの担保)。
③ （IoT ネットワークのセキュリティ）多数の IoT 機器がネットワーク化されたとき IoT ネットワークが不正動作や不正侵入なく正常動作することを担保する（クラウド側のセキュリティの担保)。

本研究開発では、上記①～③のセキュリティを担保するため以下のような研究開発を実施した。

２．研究開発内容及び成果

2.1 ①（IoT 部品のセキュリティ）の研究開発
研究開発項目①では、IoT 部品すなわち集積回路の「設計工程」に着目し、論理レベルの集積回路の設計データからいかにハードウェアトロイを検出するかを考えた。特にハードウェアトロイ検出に機械学習を活用し、膨大な既知のハードウェアトロイを学習した上で、未知のハードウェアトロイの検出を目指した。
機械学習によるハードウェアトロイ検出では「ハードウェアトロイ回路の特徴量として何を学習するか」が最大のポイントとなる。膨大な試行実験を通し、11 個の特徴量集合がハードウェアトロイ検出に有効であることを見出した。例えば、(a)対象信号線の入力側 4 段手前に接続される論理ゲートの入力数や、(b)対象信号線の入力側 4 段手前に接続されるフリップフロップの数、(c)対象信号線から出力側で最も近いフリップフロップの段数がハードウェアトロイ回路を識別するための有効な特徴量となる。
続いて、機械学習による学習器として、サポートベクタマシンやランダムフォレスト等があるが、これらの学習器に対して、上述の 11 個の最適特徴量を用いて網羅的に機械学習を行い、学習結果を得た結果、ランダムフォレストが多数の独立した「決定木」の識別結果を基本に、複数の識別結果から一つの結果を見出すものであり、ハードウェアトロイの検出には最適であると判断した。
以上の議論に基づき、実際に 11 個の特徴量とランダムフォレスト識別器を用い、未知ハードウェアトロイを含む回路設計データ中の信号線を識別した。ここでは、Trust-HUB ベンチマーク回路設計データ（トロイあり）と、トロイなしの回路設計データを用いた。回路設計データ中の各信号線について、その信号線がトロイか非トロイかを識別する。未知ハードウェアトロイの検出には、交差検証により、ある回路設計データ A に注目したとき、(1) A を未

知回路設計データ（トロイ信号線と非トロイ信号線が未知であるもの）とみなし、A 以外の回路設計データを学習データ（トロイ信号線と非トロイ信号線が既知であるもの）として識別器が学習する、(2) 学習した識別器を用いて、未知回路設計データ A 中の各信号線のハードウェアトロイの有無を識別するものとした。その結果、正解率（Accuracy）99.2%と高い確率でトロイ信号の識別に成功した。

2.2 ②・③（IoT 機器・IoT ネットワークのセキュリティ）の研究開発

研究開発項目②・③では、まず『エッジ監視』において、IoT 機器の消費電力波形等の『サイドチャネル情報』に着目する。サイドチャネル情報は、メインチャネル情報に比較してデータ量が小さく解析が容易となる。その一方、不正動作が発現すると、IoT 機器の種別や種類によらず発熱量や消費電力波形に何らかの「不正動作のパターン」が現れることが期待できる。そこで第一に、『エッジ監視』では IoT 機器のサイドチャネルに現れる不正動作パターンを検出し、IoT 機器の監視ポート・タイミングを絞り込むこととする。

次に『クラウド監視』では、IoT 機器のメインチャネル情報・エッジ監視結果をクラウド側に集約し、サーバ計算機により、サイドチャネル情報で絞り込まれた範囲のメインチャネル情報を詳細に、それ以外を簡略・高速に解析する（『大局的混合解析』）。その結果、メインチャネル情報を丸ごと解析する従来技術に比較し検出精度を落とすことなく、不正動作検出が可能となると見込む。

本研究開発では、脅威モデルとして IoT 機器に組み込まれた「マイクロコントローラ」を対象に、マイクロコントローラ中に挿入された悪意ある機能（ハードウェア・ソフトウェア）によって、不正動作が引き起こされるものと想定する。さらに複数のマイクロコントローラがネットワークを構成し、全体として IoT ネットワークを構成するものとする(図 1)。

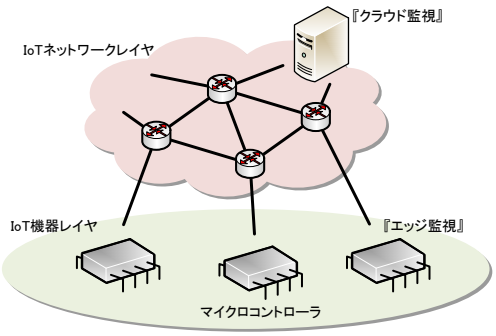

図 1：IoT 機器と IoT ネットワークモデル

本モデルに対して、以下の手順で異常動作検知を行った。

フェーズ 1『エッジ監視』：各 IoT 機器について以下の処理を実行する：

（１）**電力測定と波形整形**：測定機器を用いて対象となる IoT 機器の消費電力を計測し、ノイズを軽減するため、消費電力の測定波形を平滑化する。

（２）**通常/スリープモードの識別**：教師なし学習を用いて、消費電力波形を通常モードの区間とスリープモードの区間に識別する。

（３）**特徴量抽出**：通常モードと識別された区間に対し、その継続時間とその間の消費エネルギーを算出し、特徴量として抽出する。

（４）**外れ値検知**：抽出された特徴量に対し外れ値検知アルゴリズムを適用し、異常な区間を検出する。メインチャネル情報と検出された区間とから、悪意のある機能の候補を収集する(局所的混合解析)。

フェーズ 2『クラウド監視』：すべての IoT 機器からネットワーク側に収集された情報にもとづき以下の処理を実行する：

（５）**クラウド監視**：収集した悪意ある機能候補から実際に悪意ある機能を特定する(大局的混合解析)。

実験評価として、暗号化されたセンサ情報をネットワークによってクラウドに送信するマイクロコントローラ動作を想定した。その上で、間欠的に非暗号化センサ情報の送信を異常動作とした。上記手順によって、正しく異常動作の検知に成功した。

３．今後の研究開発成果の展開及び波及効果創出への取組

本研究開発では、IoT 機器の構成部品、機器そのもの、ネットワークの 3 階層にわたり、総合的に IoT セキュリティをとらえ、すべての階層について高いレベルでセキュリティの担保を確立したものである。本研究開発のシーズ技術について複数の産業界が高い関心を持ち、すでに一部では、プロトタイプを開発し社会実装を準備している。

４．むすび

本研究開発では、①IoT 部品のセキュリティ、②・③IoT 機器・ネットワークのセキュリティについて、世界に先駆けて研究開発を実施し、いくつかの実験例を通して、その有効性を確認した。

【誌上発表リスト】

[1] K. Hasegawa、M. Yanagisawa、and N. Togawa、"Empirical evaluation and optimization of hardware-Trojan classification for gate-level netlists based on multi-layer neural networks、" IEICE Transactions on Fundamentals、vol. 101-A、no. 12、pp. 2320-2326 (2018 年 12 月 1 日).

[2] K. Hasegawa, M. Yanagisawa, and N. Togawa, "Trojan-net feature extraction and its application to hardware-Trojan detection for gate-level netlists using random forest、" IEICE Transactions on Fundamentals, vol. 100-A, no. 12, pp. 2857-2868 (2017 年 12 月 1 日).

[3] K. Hasegawa, M. Yanagisawa, and N. Togawa、"A hardware-Trojan classification method using machine learning at gate-level netlists based on Trojan features, " IEICE Transactions on Fundamentals, vol. 100-A、no. 7、pp. 1427-1438 (2017 年 7 月 1 日).

【申請特許リスト】

[1] 戸川望、長谷川健人、検出方法及び検出装置、(申請国) 日本、2018 年 6 月 14 日.

【受賞リスト】

[1] D. Oku, M. Yanagisawa, and N. Togawa, IEEE ICCE-Berlin, Best Paper Award, 2017 年 9 月 7 日.

【本研究開発課題を掲載したウェブページ】

http://www.togawa.cs.waseda.ac.jp/research/secu.html#ht