様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月　 ６ 日現在

機関番号：１７１０２
研究種目：挑戦的研究（萌芽）
研究期間：2019～2021
課題番号：１９Ｋ２２８４８

研究課題名（和文）デバイスの消耗を活用した動作時限付きシステムアーキテクチャの研究

研究課題名（英文）Limited-use system architecture by using wear-out devices

研究代表者
小野　貴継（Ono, Takatsugu）

九州大学・システムＬＳＩ研究センター・准教授

研究者番号：８０７５６２３９

交付決定額（研究期間全体）：（直接経費）　　4,800,000円

研究成果の概要（和文）：IoT 機器が正しく管理されない場合，インターネットに接続された状態が継続し，マルウェアやウィルスに感染する可能性がある．そこで本研究ではIoT 機器に対して利用可能な期間（ライフサイクル）を定める手法を提案した．攻撃者によって改ざんが困難なライフサイクルを実現するために，物理的に破壊されるウェアアウトデバイスを用いた．ウェアアウトデバイスの検討およびパラメータの決定方法について明らかにし，シミュレーションにより有効性を確認した．

研究成果の学術的意義や社会的意義
太陽光発電などにより電源を永続的に供給されるIoT機器の増加に伴い，適切に管理されていないIoT機器が長期間インターネットに接続されることが増えると予想される．セキュリティに関する脆弱性があるとそれが放置されることになり，将来的に大きな問題となることが予想される．本研究は改ざん困難なライフサイクルを定めるものであり，今後のIoT機器の安全な利用手法を示したという点でその意義は大きい．また，ライフサイクルを定めることは，ユーザが購入後に利用可能な期間が予め決められることを意味する．したがって，産業界では積極的な研究開発をためらうものであり学術界からの技術提案には社会的意義があると考えられる．

研究成果の概要（英文）：If IoT devices are not managed properly, they may remain connected to the Internet and be infected with malware or viruses. This study proposes a method to define IoT devices' period of availability (lifecycle). In order to realize a life cycle that is difficult to be tampered with by an attacker, we used a wear-out device that can be physically destroyed. We investigated the wear-out device and its parameters and confirmed its effectiveness through simulations.

研究分野：コンピュータアーキテクチャ

キーワード：コンピュータアーキテクチャ　IoTシステム　ハードウェアセキュリティ

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

センサやコンピューティングリソースなど，様々な機器がインターネットに接続される IoT 機器の普及が進んでいる．太陽光発電により動作するセンサなどは電源配線が不要であり設置の自由度が高いことからますます利用が拡大してくものと推測される．このようなセンサは一度設置すると物理的に故障するか利用者が回収するまで長期間にわたりデータを得ることが可能になる．IoT 機器から得られる情報をデータセンタに集約し，蓄積/処理の後，必要に応じて IoT 機器を制御するような IoT システムの開発が進められている．

このような IoT システムにおいて，すべての IoT 機器が正しく管理され続けるとは限らないという問題がある．適切に管理されない IoT 機器が長期間インターネットに接続される場合，セキュリティの問題が生じる可能性がある．なぜなら，通信状況や管理者の交代などが原因で，ソフトウェアやファームウェアが正しく更新され続けるとは限らず，セキュリティ関連の脆弱性が多数の IoT 機器で長期間放置される可能性があるためである．

２．研究の目的

このような背景のもと，IoT 機器に対して利用可能な期間(ライフサイクル)を定めることを考える．ライフサイクルの間は IoT 機器はインターネットに接続され，利用できるが，ライフサイクルを経過した場合はインターネットから遮断される．ライフサイクル経過後，利用者は新しい IoT 機器を導入することが求められるが，セキュリティの問題が生じることはない．利用者が意図したとおりに IoT 機器自ら特定の機能（ここではインターネット通信）を無効化する技術の確立を目指す．

３．研究の方法

ライフサイクルマネジメントを実現するには，ソフトウェアとハードウェアの 2 つの方法が考えられる．ライフサイクルは攻撃者によって意図的に長く(または短く)することが可能であってはならない．ソフトウェアで実現した場合は，OS の脆弱性などを利用してライフサイクルを改ざんされる可能性がある．

そこで，本研究では，ウェアアウト技術を用いた OTP(one-time pad)を利用し，IoT 機器とサーバ間との通信を制限することを検討する．ウェアアウト技術，NEMS を用いた OTP の実装方法が先行研究によって提案されている [1]．しかしながら，IoT 機器を対象として NEMS を用いた OTP 方式が有効であるかは明らかになっていない．そこで，IoT 機器のライフサイクルマネジメントの観点から要件を整理し，NEMS を用いた OTP 方式が有効であるかを定量的に確認する．具体的的には IoT 機器内に実行しているクライアントからサーバへの通信を行う際，ウェアアウト技術での OTP 決定木から暗号鍵を求め，送信メッセージを暗号化し，サーバに送信する．サーバには IoT 機器からの情報を管理するブローカおよびブローカへの暗号通信を標準化するプロキシがある．1mm2 チップ内の決定木予想密度から OTP 決定木 の総数を見積もり，妥当な決定木パラメータで IoT 機器に適した使用可能な鍵数(通信回数) および OTP 決定木の消費エネルギーと回路面積を評価する．

４．研究成果

ウェアアウトデバイスを用いたライフサイクルマネジメント手法を開発した．本研究では主に，適切なデバイスの選択，ウェアアウトデバイスを用いた OTP 決定木の構成，通信可能回数に基づく OTP 決定木のパラメータ検討，シミュレーションによる検証を実施し，その有効性を確認した．

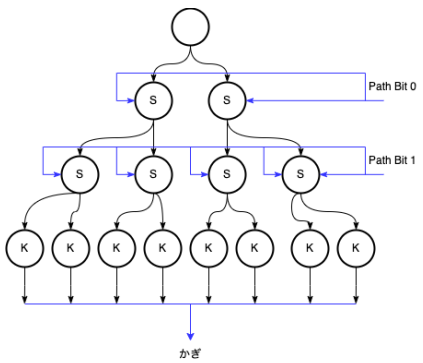

図１：決定木の構成例

デバイスの選択

一定の利用回数の後に故障することで不可逆的に利用できなくなるようにスイッチを実現する必要がある．これを実現するデバイスとして，MEMS (Micro Electromechanical System)，NEMS (Nano Electromechanical System)，PCM (Phase Change Memory) などが挙げられる．これらの技術は，いずれも CMOS の消費電力の問題を解決するために設計されているため，対象とする機器に低消費電力で動作が可能である．本研究で重視している特性は，ウェア アウトの上限値である．MEMS スイッチでは，6GHz で 10^7 のオーダーのスイッチングが可能である．さらに，現時点の

製造技術では，多くの故障要因を持っている．一方，NEMS スイッチは，過酷な環境に対する耐性を有するデバイスであり，10^9 オーダーで故障せずにスイッチング可能である．PCM はスイッチではなく，状態を記憶する新しい種類のメモリであるが，DRAM と比較して書き換え可能回数の上限が低いという問題がある．PCM は，10^7 から 10^9 までのオーダーで書き込み可能である

このように，MEMS のスイッチング周波数が低くなれば，ウェアアウトの限界が高くなり，ウェアアウトデバイスの安全性が損なわれることになる．PCM は CMOS と異なる製造プロセスを用いる必要がある．したがって，製造が難しく，コストが高いという課題がある．本研究では，NEMS スイッチを用いることした．しかしながら，NEMS スイッチには，エネルギーハーベスティング機器に対し，高いプルイン電圧を必要とする特性がある．現在の NEMS スイッチは，対象機器にはまだ適していなく，プルイン電圧を低減する技術や手法を今後の課題である．

OTP 決定木の構成

OTP 暗号を行う際，送信メッセージ分の長さが必要であるランダム鍵を用意し，伝送するという手順が必要である．暗号鍵を安全に伝送する負担を緩和するために，決定木を設計し，OTP に必要な鍵を複数ブロックに分け，図 1 のように，木の葉に鍵候補として格納する．ここで、図 1 にある‘S’ はスイッチを表し，‘K’ は鍵候補を格納するシフトレジスタを表している．各鍵を取るためには経路情報，短い文字列をインデックスとして付ける．これらの ランダム鍵を安全に伝送するためには，

表 1：決定木のパラメータ

記述	決定木のパラメータ
NEMS の平均期待寿命	α
NEMS 寿命のばらつき	β
決定木の高さ	H
決定木の総数	N
OTP 決定木から取得すべき決定木数	k

- 短いパス（経路情報），文字列
- 複数のランダム鍵候補を格納している決定木

の 2 つの要素が必要となる．この決定木は NEMS スイッチを用いて構築されたデバイスである．OTP 鍵を 1 つの決定木に格納することは安全ではない．複数の決定木(複数のランダム鍵候補を持つ)を含むチップを OTP 暗号鍵のセットとして見なし，メッセージの送信や受信を行う前にあらかじめ受信側に配信すべきである．具体的にその複数決定木を 10 個としたとき，OTP 鍵を生成する際，同時に全ての決定木へアクセスし，取得できた鍵候補を足し合わせたものを OTP 鍵とする．

OTP 決定木を構成しているパラメータを表 1 に示す．これらのパラメータを用いて OTP 決定木から鍵を生成可能な確率のモデルを構築した．通信が必要な回数から各パラメータを算出することが可能になった．

シミュレーションによる検証

図 2 に評価の対象とした IoT システムの概略図を示す．MQTT のプロトコルを用いて，IoT 機器がサーバと接続し通信を行う状況を想定した．プロキシは OTP 暗号手法で通信している IoT 機器の暗号を復号化し，ブローカに送信し，ブローカからのメッセージを暗号化し，IoT 機器に送信するという役割がある．ただし，プロキシ側にも該当する IoT デバイスの OTP 決定木を持つ必要がある．プロキシに IoT 機器内の OTP 決定木を伝送するのに 2 つの方法が考えられる．

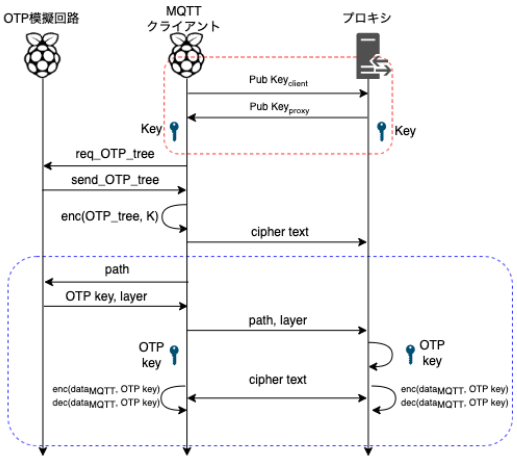

図 2：システムの全体図

- 方式 1：OTP 決定木チップを製造時，鍵情報が既に知っているため，製造者が鍵情報をフラッシュメモリに格納し，チップと共に伝送し，ユーザが手動でプロキシに登録する．または，フラッシュメモリに格納するのではなく，プロキシに登録し，チップとプロキシと共に伝送する方式である．
- 方式 2：IoT 機器内の OTP 決定木を全て探索し，OTP 暗号ではなく，例えば Diffie-Hellman 鍵交換アルゴリズムから生成された鍵で決定木の情報を暗号化し，プロキシに伝送する方式である．

方式 1 では，ネットワークを介さずに，伝送できるため，より安全である．また，NEMS を製造時に精密なウェアアウトが求められていないため，製造コストが低くなる利点がある．た

だし，製造者を信頼しなければならない立場になる．さらに，ユーザがプロキシに IoT 機器の OTP 決定木の情報を登録し間違える可能性がある． プロキシは複数 IoT 機器に対応できないため， 改ざん不可能な IoT 機器の識別(ID)も定めなければならない． 将来的にユーザが新しい IoT 機器を既存のネットワークに追加する場合，プロキシの再登録や再設定を行う必要があり，柔軟性を失う欠点がある．一方， 方式 2 では， 設定などがより簡単になるが， ネットワークでの伝送であるため， 確実に安全であるとは限らない． 加えて， OTP 決定木の鍵情報を伝送する際，決定木を探索する必要であり，NEMS に対し，精密なウェアアウトが求められ，製造コストが高くなる.さらに，プロキシの安全性も保証できず，伝送先(プロキシアドレス)が正しいとは限らない． 偽プロキシである可能性があり， 全ての鍵情報が盗まれかねない． したがって，認証方法も考える必要がある．本研究では，方式 2 でプロキシ側に IoT 機器の OTP 決定木を伝送するという前提で，鍵を探索する際，ウェアアウトしないように設定した．

本実験では，1㎜2 あたりのチップ面積を仮定して，OTP 決定木によって定義される通信可能な回数を得るためのパラメータを調査した．その結果を表 2 と表 3 に示す．例えば，1 時間に 1 回の通信を行う IoT 機器の場合，1 年間の連続動作では 8,760 回，5 年間では 43,950 回の通信が必要となる．8,760 回の通信は，表 2 から，$N = 256, H = 7$のときに実現可能であり，43,950 回の通信は表 3 から$N = 128, H = 7$のときに実現可能であることがわかる．

表 2：$\alpha = 100, \beta = 1, k = 80$における評価結果

決定木のパラメータ	平均通信回数	平均 k	平均デュプリケート数	$1mm^2$ 内の OTP 決定木総数	$1mm^2$ での通信可能回数
N = 128, H = 7	21	98	0	312	6552
N = 256, H = 7	57	145	0	156	8892
N = 128, H = 8	20	98	0	156	3120
N = 256, H = 8	56	144	0	78	4368

表 3：$\alpha = 1{,}000, \beta = 1, k = 80$における評価結果

決定木のパラメータ	平均通信回数	平均 k	平均デュプリケート数	$1mm^2$ 内の OTP 決定木総数	$1mm^2$ での通信可能回数
N = 128, H = 7	230	101	1.96	312	71, 760
N = 128, H = 8	236	101	1.03	156	36, 816

表 2，表 3 から，決定木には複数鍵候補があるにもかかわらず， OTP 鍵を生成し， 実際に通信できる回数が少ないことがわかる．セキュリティの観点からすれば，攻撃者は一部の OTP 決定木にある鍵情報を入手できたとしても， 今後の暗号化または復号化に使えるとは限らない． このことから， 仮に IoT 機器が攻撃者に乗っ取られ攻撃により OTP 決定木にアクセスしウェアアウトすると IoT 機器が利用できなくなる．したがって，IoT 機器は攻撃者に悪用されることを防ぐことが可能になる一方でユーザにとっては損失となる．本手法は攻撃そのものを防ぐものではなく，攻撃によりさらなる被害を防ぐために利用するものである．攻撃を防ぐための手段は別に用意する必要があることに注意しなければならない．

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計2件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 山方大輔，川上哲志，谷本輝夫，井上弘士，小野貴継
２．発表標題 プロセッサへの実装に向けたORAMにおけるポジションマップ削減手法の検討
３．学会等名 Symposium on Cryptography and Information Security (SCIS)
４．発表年 2021年

１．発表者名 Sandeep Kumar, Diksha Moolchandani, Takatsugu Ono and Smruti Sarangi
２．発表標題 F-LaaS: A Control-Flow-Attack Immune License-as-a-Service Model
３．学会等名 IEEE International Conference on Services Computing（国際学会）
４．発表年 2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関