4M-08

センサデバイスの自己適応による効率的なデータ送信手法の提案

星野　隆太†　　岸　知二‡

早稲田大学創造理工学部経営システム工学科†‡

1.研究背景.

IoT(Internet of Things)は，家電などのモノがインターネットを介して接続されることで，さまざまな情報をリアルタイムに活用するという考え方である．IoT デバイスではハードウェアの制約から，大きなデータを扱うことができない．そうした中，MQTT(Message Queue Telemetry Transport)プロトコルは，ヘッダサイズが非常に軽量なことから，IoT 向けのプロトコルとして注目されている．一方 IoT デバイスのセキュリティ問題も重要な課題の一つとして挙げられている．そのためセキュリティを考慮したプロトコルである TLS(Transport Layer Security)が注目されている．TLS では証明書の交換を頻繁に行うとセキュリティは高まるが，大きなパケットサイズを要する再ネゴシエーションの回数が増えるというトレードオフの問題がある．そのため資源の乏しい IoT デバイスでは，この問題を解決する必要がある．

2.関連研究.

Singh ら[1]は MQTT 通信のセキュリティに関する研究をしている．この研究では，メッセージのトピックを暗号鍵にすることで，MQTT プロトコル自体をセキュアにする sMQTT を提案している．提案手法は従来手法と比較してパケットサイズが小さく，処理も短い結果を示した．また，セキュリティと通信のオーバーヘッドには正の相関があることが示されている．

田中ら[2][3]は，トレードオフの関係がある特性に，自己適応を用いることによる振る舞い改善の効果に関する研究をしている．[2]では，組み込みシステムにおける自己適応ソフトウェアのモデリング手法を提案している．自己適応ソフトウェアとは，周囲の状況に応じて振る舞いを変えることができるソフトウェアである．[3]では，DFEAM(動的フィーチャ指向消費電力適応型モデリング)により，消費電力と QoS のトレードオフに対して振る舞いを改善する手法を提案している．ソフトウェアの振る舞いバリエーションの探索には，フィーチャの重み付けを用いている．結果として消費電力の多いバリエーションほど QoS 値が高いという傾向が示されている．

A Method of Effective Connection for IoT Devices by Self-Adaptive

†Ryuta HOSHINO, WASEDA University

‡Tomoji KISHI, WASEDA University

3.研究目的.

本研究では MQTT によりデータ通信を行うセンサデバイスに自己適応機能を加えることで，パケットサイズを増加させることなく，セキュリティを高めることを目指す．具体的にはスマートホームに設置されることを想定したセンサデバイスの，データ計測頻度と，TLS のオーバーヘッドを含む再ネゴシエーションの頻度を，センサデータの変化傾向をもとにコントロールすることで，状況に応じて振る舞いを変化させる．

4.提案手法.

本研究では，センサデバイスが取得したセンサデータの変化値をもとに，状況ごとに適したバリエーションを選択させることで目的を達成する．具体的には，”センサデータの変化が小さい状況においてデータの計測頻度を低下させ，TLS 認証に割り当てるパケットサイズを増加させセキュリティを高めるバリエーション”と”センサデータの変化が大きい状況において TLS 認証に割り当てるパケットサイズを減らすことでデータの計測頻度を増加させるバリエーション”を用いる．

対象とするセンサデバイスは，処理能力の小さなコンピュータによって，センサを制御しデータを送信するデバイスを想定している．そのため前提として，デバイスの通信は MQTT プロトコルに TLS を付与して行う．

5.実装.

5.1.センサデバイス.

提案手法を評価するために，上述した自己適応機能を備えたセンサデバイスを実装する．具体的にはスマートホームの機能として，部屋の照度データをリアルタイムにネットワークに送信するセンサデバイスを想定している．センサデバイスは， CdS 照度センサを含む電子回路，マイコンボードの一種である Arduino Uno，Wi-Fi モジュールの ESP-WROOM-02 によって構成される．

5.2.MQTT.

本研究では，オープンソース MQTT ブローカーである Mosquitto を導入する．本研究では後述する TLS 接続を行うため 8883 番ポートを用いて接続する．

5.3.TLS.

デバイスとブローカーの通信をセキュアに行うため， TLS 通信を実装する．実装にはオープンソース

ライブラリである OpenSSL を用いて，鍵長 2,048bit のサーバ証明書と，各種秘密鍵ファイルを生成する．

5.4.自己適応機能.

自己適応機能は，Arduino のプログラムに実装される．具体的には取得したセンサデータの変化値を蓄積し，時間あたりの変化値に応じてバリエーションを選択する．本研究の提案手法によるバリエーションを表 1 に示す．また，これらのバリエーション間の遷移条件を状態遷移モデルで示したものが図 1 である．図 1 における dif は 1 バリエーション実行あたりのデータ変化の平均値を示す．

表 1．自己適応バリエーション

	A: 送信間隔	B: 切断間隔	Y:36sec あたり パケットサイズ
V1	3.6sec	36sec	398.0
V2	14.4sec	28.8sec	377.5
V3	1.8sec	72sec	379.0

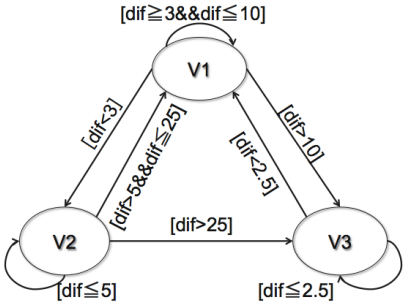

図 1．状態遷移モデル

このアプリケーションは送信間隔(A)36，切断間隔(B)3600 で動作することを想定しているが，これは IoT センサ[4]のデータ取得間隔が 36，TLS を用いた OpenVPN の再ネゴシエーション間隔が 3600 に設定されているためである．また実験時間を短縮するために時間スケールをそれぞれ 100 分の 1 に設定して実装したため，初期状態 V1 は A=3.6，B=36 となる．V2 は計測頻度を少なくして再ネゴシエーションを多く行うバリエーションであり，V1 と比較してわかりやすいように最も多く再ネゴシエーションを行うように設計されている．V3 は再ネゴシエーションを少なくしてデータを頻繁に計測するバリエーションであり，V1 と比較してわかりやすいように ESP-WROOM-02 に設定できる最長のセッション長を V3 の切断間隔に設定している．

6.評価実験.

6.1.実験目的および実験方法.

評価実験では，提案手法と比較手法を評価する．比較手法とは，提案手法における V1 のみを実行し続ける，自己適応しない場合の通信である．双方による通信をそれぞれ Wireshark により記録し，センサデータの変化値に応じたデータの送信回数，再ネゴシエーション回数を評価する．同時に各バリエーションが実行時間内に使用した，センサデータのパケットサイズと TLS 認証のパケットサイズの合計値を記録する．V2 および V3 は V1 よりも時間あたりパケットサイズが小さくなるように設計されているため，提案手法が V1 単一の動作時と比較して常に時間あたりパケットサイズが小さくなることを実験により確認する．

6.2.実験結果.

実験結果を図 2 に示す．

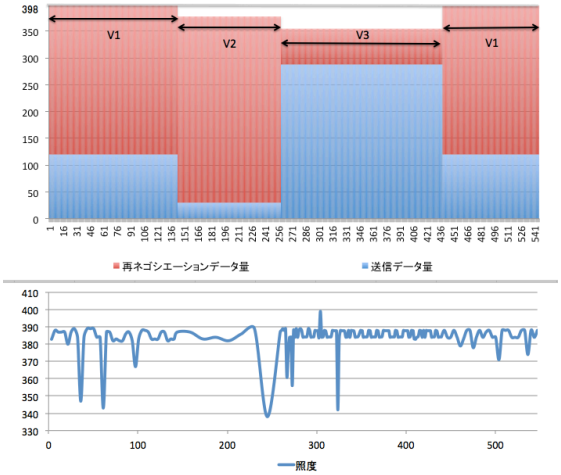

図 2．実験結果

V2 および V3 実行時の時間あたりパケットサイズは，いずれも V1 より小さい．このことから提案手法は比較手法より常にパケットサイズが小さい．V2 はデータ変化の少ない時間帯にデータの計測頻度を長くすることで，再ネゴシエーションの回数を増やすことができている．V3 はデータ変化の多い時間帯においてデータの計測頻度を多くすることができている．これらのことから，自己適応機能により状況に適したバリエーションの選択ができており，それぞれのバリエーションにおいて最大回数の再ネゴシエーションを行っている．

7.今後の課題.

今後の課題はバリエーションの選択の精度や応答率など自己適応機能の評価を行うことである．また，最もセキュリティレベルの低いバリエーションにおいて，72sec ごとに再ネゴシエーションを行ったが，これがセンサデバイスのセキュリティの観点から妥当であるかの評価を行い，各パラメータの設定を見直す必要がある．

参考文献.

[1] Meena Singh ら(2015) ”Secure MQTT for Internet of Things (IoT) “ , 2015 Fifth International Conference CSNT, pp.746-751.

[2] 田中 文也ら(2017)「モデル駆動開発による 消費電力自己適応型ソフトウェアの開発方法論」，組み込みシステムシンポジウム 2017，pp.23-30.

[3] 田中 文也ら(2018)「DFEAM:動的フィーチャ指向消費電力適応型モデリング」，組み込みシステムシンポジウム 2018，pp.75-82.

[4]レンジャーシステムズ株式会社 「IoT コネクティングサービス 」，<https://www.ranger-systems.co.jp/iot/>，（参照 2018-12-05）.