ISS-A-038

安価な IoT デバイスの通信路保全を可能とする MQTT エッジプロキシの設計と実装

遊亀　嘉生†　　高鶴　蒼史†　　利根川　寛太†　　藤野　貴之†
† 近畿大学工学部電子情報工学科

1. はじめに

IoT(Internet of Things)とはデバイスがインターネット上での通信を可能にする概念である. 近年, IoT デバイスの数は急増しており, 2020 年までに 500 億に達すると予想されている[1]. 安価な IoT デバイスはリソースに制約があり[2], TLS を動作させるといった重い演算は使用できない. そのため安価な IoT デバイスを起点とする通信はセキュリティが脆弱である場合が多い. 本稿では MQTT エッジプロキシにより, IoT デバイスからは透過的に通信を暗号化する手法を提案する.

2. MQTT プロトコル

MQTT(MQ Telemetry Transport)とはパブリッシュ/サブスクライブ型の仕組みを使用するメッセージングプロトコルである. MQTT は実装が容易であり, 軽量なプロトコルであることから制約が厳しいデバイス上でも実装することが可能である. Publisher, Subscriber をクライアント, Broker をサーバと呼ぶことがある. MQTT のメッセージはトピックと呼ばれる階層構造のメッセージ識別子を持つ.

3. セキュリティの問題

MQTT は標準ではデータの送受信を平文で行うため, 攻撃者によってデータのやり取りが盗聴され, 情報が漏洩する可能性がある. Broker はクライアントの認証機能を標準では提供せず, オプションでも簡易なパスワード認証しか提供しない. そのため, Broker に対して偽の Publisher を接続して本来権限のないメッセージを発行したり, 偽の Subscriber を接続して権限のないメッセージを盗み見たりすることができる.

4. 提案手法

本稿では, 以上のセキュリティ問題に対処するため, 図1に示す MQTT エッジプロキシを提案する. Proxy-Local Broker を①, Publisher(TLS)-Broker(TLS)を②とすると, MQTT エッジプロキシは, ①②と, ①②を繋ぐ部分で構成される. Publisher から送信されたメッセージをポート番号 1883 で待機しているエッジプロキシノードで受け取り, ①で Publisher と Broker の接続処理を行う. その後, ①②を繋ぐ部分でメッセージからトピックとペイロードを抽出し, TLS を付加したメッセージに作り直す. 作り直したメッセージを③で Broker(TLS)に送信する. これらの処理により, Publisher からは透過的に通信を暗号化する事が出来る.

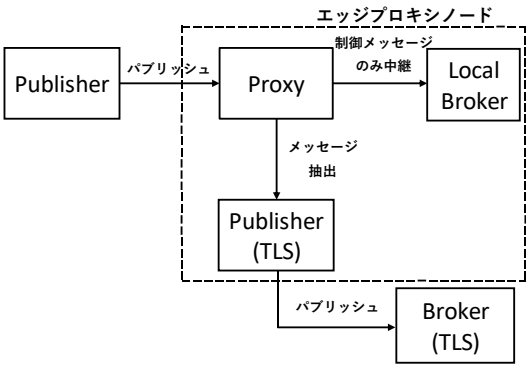

図1. MQTT エッジプロキシ

5. 実装結果

Raspberry Pi3 Model B 2 台とデスクトップ PC を用いて実装する. Raspberry Pi 間は無線で通信する. MQTT 実装のためオープンソースメッセージブローカである Eclipse Mosquitto[3] を使用する. Proxy と Publisher(TLS)は Java で実装し, Publisher(TLS)は Mosquitto のクライアントライブラリである Paho[4]を用いる. Publisher の平文メッセージを Proxy 上で抽出し, 新たに Publisher(TLS)でメッセージを発行して Broker(TLS)に送信出来ることを確認した.

```
Opening ipv6 listen socket on port 8883.
Opening ipv4 listen socket on port 8883.
New connection from 192.168.1.20 on port 8883.
New client connected from 192.168.1.20 as javasample (p2, c1, k60).
No will message specified.
Sending CONNACK to javasample (0, 0)
Received PUBLISH from javasample (d0, q0, r0, m0, 'mqtt', ... (12 bytes))
Received DISCONNECT from javasample
Client javasample disconnected.
```

図 1. Broker(TLS)の結果

6. 今後の課題

今後はさらに Proxy の機能を改良する予定である.

参考文献

[1] D. Evans, “The internet of things : How the next evolution of the internet is changing everything, ” pp. 1-11, 2011.

[2] C. Bormann, M. Ersue, and A. Keranen, “RFC 7228 Terminology for Constrained-Node Networks,” IETF, May2014.

[3] Eclipse Mosquitto. http://mosquitto.org/,(accessed 2020-02-02)

[4] Eclipse Paho – MQTT and MQTT-SN software. http://www.eclipse.org/paho/,(accessed 2020-02-02)