ホームネットワークにおける SDN による仮想デバイスを用いたセキュリティプラットフォームの検討

A Study of SDN-based Security Platform for Home Networks

塚﨑 拓真 / Takuma Tsukasaki

1　はじめに

近年，IoT(Internet of Things) が注目を集めるようになり，今後あらゆるモノがネットワークに接続され，利用されることが予想される．それに伴い，ネットワーク内には様々な端末や機器 (まとめて，デバイス) が混在することになり，ホームネットワークの形態は多様化していくと考えられる．

しかし，IoT の発展で利便性が高まる一方で，これまでネットワークに接続されていなかったモノが接続されることにより，セキュリティ上のリスクも高まっている [1]．IoT デバイスは十分なセキュリティを考慮せずに開発されたものが多いため，悪意のある攻撃者によるサイバー攻撃の標的になりやすい．セキュリティ上の脅威が各種デバイスに顕在した場合，個別に対処するとコストや時間がかかってしまうため，脅威に対し一括に対処する必要がある．しかし，ホームネットワーク内には異なる規格のハードウェアや様々なアプリケーションが混在しているため，それら全てに対応したシステムの構築や更新を続けるのは困難である．そのため，ホームネットワーク内で通信するのであれば，どのデバイスも必ず利用するネットワークを利用したシステムを構築することが望ましい．本研究では，SDN を用いて，ホームネットワークに適した形での不正な通信の検知を検討する．

2　関連研究

今野らは，セキュリティ対策を施し，仮想的に作成した論理デバイスを利用し，実際の IoT デバイスの通信を中継することで，セキュアな通信環境を提供するプラットフォームを提案した [2]．これにより，IoT デバイスのリソース量に依存しないセキュリティ対策の実現が可能となる．しかし，クラウドサーバ宛て，ローカルネットワーク上のサーバ宛ての 2 パターンを前提としている．現在のスマートホームデバイスは，クラウド上のシステムと連携することで，デバイス間の連携を可能にしているが，今後はホームネットワーク内で閉じたデバイス間の通信によって連携を行う形になることが想定される [3]．デバイス間で直接通信を行う場合，各デバイスでどういったデバイスとの通信を受け入れるか，アクセス制御を行う必要がある．

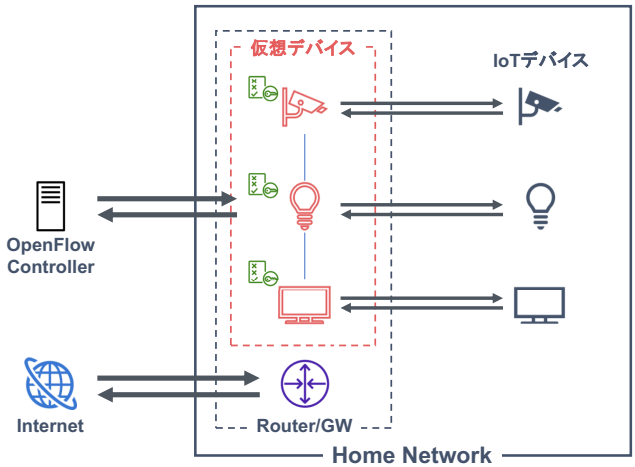

図 1: 提案システムの構成

しかし，全てのデバイスがアクセス制御に対応しているとは限らず，デバイスの計算能力の制限によって実現できるアクセス制御に制限があったり，デバイスのソフトウェア自体の脆弱性によってアクセス制御が機能しない場合が考えられる [4]．

3　提案システム

3.1　概要

前述の問題点を受けて，IoT デバイス間通信における不正な通信の検知も必要である．提案システムでは，SDN の代表的なプロトコルである OpenFlow を利用することで，既存 IoT デバイスや異なる規格などに対応でき，ホームネットワークに適した形で不正な通信の検知を実現する．仮想デバイスというセキュリティ対策を適用可能なデバイスを，ゲートウェイ上に仮想的に作成する．ここに IoT デバイスがリソースの都合上適用できないセキュリティ対策をオフロードし，この仮想デバイスが IoT デバイスの通信を中継し，仮想デバイス間通信も可能にすることで，本来 IoT デバイスに適用したいセキュリティ対策を実現する．今回はセキュリティ対策として，ホームネットワーク内通信のトラフィック情報は既知であることを考慮し，フローの検証を OpenFlow コントローラ (OFC) で行う．

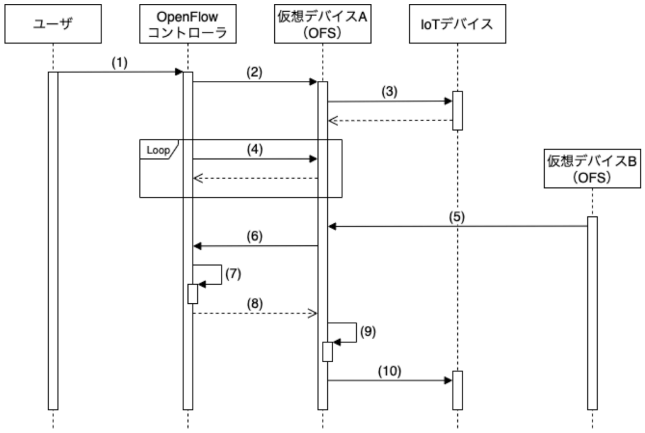

図 2: 提案システムの動作手順

3.2 システム構成

OpenFlow を用いて，トラフィックフロー制御を行うことで，ホームネットワーク内で行われる通信を制限する．提案システムの構成を図 1 に示す．構成要素としては，IoT デバイス，仮想デバイス，ルータ・ゲートウェイ，OFC から構成される．IoT デバイスは，センサをはじめとした，リソースを十分に持たず，デバイスに直接セキュリティ対策を適用できないデバイスと定義する．仮想デバイスは，IoT デバイスに要求されるセキュリティ対策を仮想的に実現したものである．IoT デバイスからの通信を中継し，セキュリティ対策を適用する．また，OpenFlow スイッチ (OFS) で構成し，仮想デバイス間通信を可能とする．OFS の機能を持った仮想デバイスをゲートウェイに配置し，OFC と通信を行うことでセキュリティ対策を実現する．

3.3 動作手順

提案システムの動作手順を図 2 に示し，詳細を以下に述べる．送信先の IoT デバイスの仮想デバイスを仮想デバイス A とし，送信元の IoT デバイスの仮想デバイスを仮想デバイス B とする．

1. ユーザは，OFC に仮想デバイス A 作成要求
2. OFC は，仮想デバイス A を作成
3. 仮想デバイス A は，IoT デバイスを確認
4. OFC と仮想デバイス A は互いに，Echo Request/Reply メッセージを定期的に送信
5. 仮想デバイス B は，仮想デバイス A に通信
6. 未知のフローだった場合，仮想デバイス A は，OFC に対して Packet In メッセージを送信
7. OFC は，トラフィック情報を調査
8. OFC は，仮想デバイス A に対して許可/不許可メッセージとして Flow Mod メッセージを送信
9. 仮想デバイス A は，フローを更新
10. OFC は，仮想デバイス A に対して Packet Out メッセージを送信

3.4 想定環境

ホームネットワークにおける閉じたデバイス間の通信，デバイス・クラウドサーバ通信，デバイス・ローカルサーバ通信を想定する．

4 評価

4.1 評価項目

本研究では，実用性と信頼性を評価する．実用性では，システムの負荷がネットワークに与える影響を測定したいため，遅延を評価する．信頼性では，IoT デバイスを用いたシステムの安心安全を確保するための機能として，IPA により IoT 高信頼化要件・機能要件が定義されている [5]. 本研究では，システムの稼働中の局面である予防，検知，回復の 3 つにおける高信頼化要件に対し，提案システムの有効性について考察する．

4.2 評価シナリオ

評価シナリオとしては，デバイス・クラウドサーバ通信，デバイス・ローカルサーバ通信を行っている状況を想定し，前述した関連研究との比較を行う．また，ルータ・ゲートウェイを経由したデバイス間通信の検証も行う．

5 まとめ・今後の課題

本研究では，ホームネットワークのセキュリティ上の課題として，十分なリソースを持たない IoT デバイスに起因するセキュリティ対策の困難さに着目した．また，今後のスマートホームデバイスはデバイス間通信によって連携を行う形になることが想定される．そこで本研究では，OpenFlow を用いてデバイス間通信における不正アクセスを軽減するシステムを提案した．本提案提案システムでは，ルータ・ゲートウェイに OpenFlow スイッチの機能を持った仮想デバイスを配置し，トラフィック情報を OpenFlow コントローラで管理することで不正アクセスを防ぐ．実用性・信頼性を検証し，提案システムの有用性を示す．今後は，トラフィックフロー調査によるセキュリティ対策の深堀りや評価シナリオの具体化を検討していく．

参考文献

[1] IoT 推進コンソーシアム, 総務省, 経済産業省, "IoT セキュリティガイドライン ver 1.0", 2016.

[2] 今野裕太, 佐藤健哉, "論理デバイスプロキシを利用した IoT セキュリティプラットフォームの提案", 2017 年度 情報処理学会関西支部支部大会 講演論文集, Vol. 2017, 2017.

[3] C. Vallati et al., "Mobile-Edge Computing Come Home Connecting things in future smart homes using LTE device-to-device communications", IEEE Consumer Electronics Magazine, Vol.5, No.4, pp.77-83, 2016.

[4] M. Serror et al., "Towards In-Network Security for Smart Homes", Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES 2018), No.18, pp.1-8, 2018.

[5] IPA 技術本部 ソフトウェア高信頼化センター (SEC), "「つながる世界の開発指針」の実践に向けた手引き", 2017.