ホームネットワークにおける OpenFlow を用いたトラフィック監視によるセキュリティ向上

Improving Security by Monitoring Traffic Using OpenFlow in 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，今後あらゆるもの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が混在することになる．ホームネットワークは情報家電などの普及も加わり，その形態が多様化していくと考えられる．

しかし，IoT の登場で利便性が高まる一方で，これまでのネットワークに接続されていないモノが接続されることにより，セキュリティ上のリスクが高まっている [1]．IoT はセキュリティを考慮せずに開発されたものが多く，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く，特に不正アクセスが多発している．これらが各種端末やネットワークごとに顕在した場合，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．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それらに搭載される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，どの端末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．

2　関連研究

村上らは，OpenFlow を用いてホームネットワーク内に，動的な認証システムを構築し，不正アクセスによる被害を軽減する手法を提案した [2]．認証時に頻繁に利用される情報を用いることで，ネットワークに接続する端末を制限すると共に，万が一認証が突破された場合でも不正アクセスが検出できるシステムを構築した．しかし，1 度攻撃者に認証を突破された場合，不正アクセスを検出するまでに時間がかかると考えられ，ホームネットワーク内に不正アクセスが拡大してしまう問題点がある．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．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．同じホームネットワークに他の多くの機器が何の制限もなく接続されているという事実を利用して，個人情報の漏洩やサービスの操作など，悪意ある活動を行う可能性がある [4]．

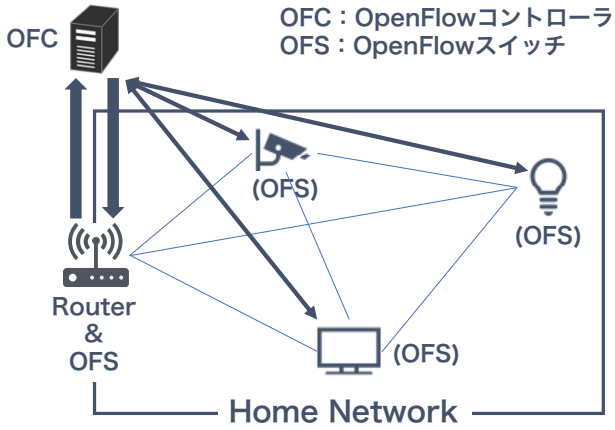

図 1　提案手法のアーキテクチャ

3　提案手法

前述の問題点を受けて，不正アクセス拡大を防ぐことを考慮し，ホームネットワーク内においての検知も必要である．本提案手法では，OpenFlow を利用することで，既存 IoT 機器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．また，動的に接続を管理することで，不正通信による被害を軽減する．

3.1　想定環境

本提案手法のアーキテクチャを図 1 に示す．ホームネットワークにおける閉じたデバイス間の通信，ルーター・デバイス間の通信を想定する．また，デバイス数は一般的に利用されているルーターの推奨接続台数である 10~15 台を想定する．

3.2 概要

OpenFlow を用いて，トラフィック監視を行うことで，ホームネットワーク内で行われる通信を制限する．既存 IoT 機器に OpenFlow スイッチの機能を導入することは困難であると考え，OpenFlow スイッチの機能を持った仮想デバイスを既存 IoT 機器の前に用意する．通信が行われる際に，仮想デバイスを通して，OpenFlow コントローラに接続し，トラフィック情報から通信の許可を判断する．

3.3 動作手順

本提案手法の動作手順のシーケンス図を図 2 に示し，詳細を以下に述べる．

1. 仮想デバイス (OFS) と OpenFlow コントローラは双方に対して，Echo Request/Reply メッセージを定期的に送信
2. 接続要求機器は仮想デバイス (OFS) に通信
3. 仮想デバイス (OFS) は OpenFlow コントローラに対して，Packet In メッセージを送信
4. OpenFlow コントローラはトラフィック情報を調査
5. 正当な通信の場合，OpenFlow コントローラは仮想デバイス (OFS) に対して，許可メッセージとして，Flow Mod メッセージを送信
   不正な通信の場合, OpenFlow コントローラは仮想デバイス (OFS) に対して，不許可メッセージとして，Flow Mod メッセージを送信
6. OpenFlow コントローラは送信元機器に対して，Packet Out メッセージを送信

3.4 トラフィック情報

本提案手法で通信の許可を判断するトラフィック情報として，以下の 3 点を用いる．

- パケットヘッダー
- パケットの長さ
- 周期性

4 評価

4.1 評価項目

本研究では，セキュリティと負荷を評価する．そのため，セキュリティ面では，正当なアクセスは通信が許可されるか，不正なアクセスは通信が許可されないかを実証する．また，負荷面では，ネットワークに与える影響を測定したいため，スループットを評価する．

4.2 評価シナリオ

評価シナリオとしては，IoT 機器が 1 対 1，1 対 N，N 対 N($2 \leqq N \leqq 15$) で通信を行っている状況を想定し，各状況において評価を行う．

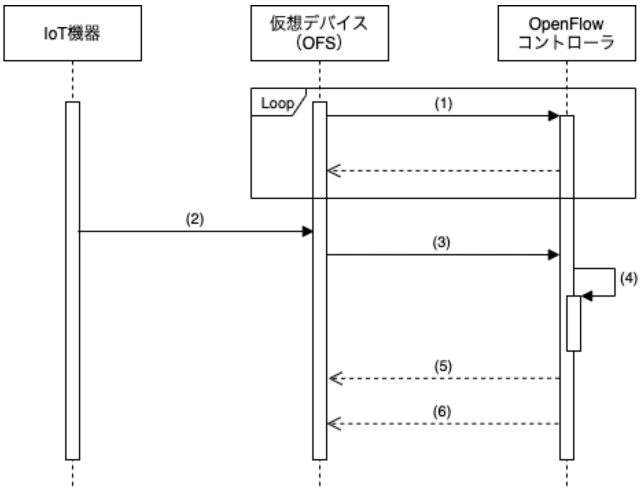

図 2　動作手順のシーケンス図

5 まとめ・今後の課題

本稿では，ホームネットワークの形態の多様化からセキュリティ上の課題として，近年，増加傾向が見られる不正アクセスに着目した．また，今後のスマートホームデバイスは，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．そこで本研究ではその対策として，OpenFlow を用いてホームネットワーク内で動的なトラフィック監視を行い，デバイス間通信における不正アクセスによる被害を軽減する手法を提案した．本提案手法では，デバイスの前に 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．

今後の課題としては，トラフィック情報の監視において，何を正当とし，何を不正とするのかの閾値と，具体的な検知手法を検討する必要がある．また，本提案手法の評価において，セキュリティ面の評価が重要であると考える．評価として，正当アクセスと不正アクセスをどれほど正確に判別できるか定性的な評価を行い，セキュリティの観点からの本提案方式の有用性を示したい．

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] 村上萌, 中村嘉隆, 高橋修, "OpenFlow を用いたホームネットワークへの接続端末制御による不正アクセス防御手法の提案", 研究報告コンピュータセキュリティ (CSEC), Vol.2016-CSEC-72, No.29, pp.1-6, 2016.

[3] C. Vallati, A. Virdis, E. Mingozzi and G. Stea, "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, M. Henze, S. Hack, M. Schuba, and K. Wehrle, "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.