

スマートホームにおける SDN を用いたトラフィック監視による不正アクセス防御手法の検討

A Study on Unauthorized Access Protection Method by Traffic Monitoring Using SDN in Smart Home

塚崎 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. 現在, IoT 機器が様々なところに置かれるようになり, 以前のパソコンやスマートフォンに限らず, 現在ではテレビやゲーム機, Web カメラ, 冷蔵庫などの家電などがインターネットに繋がり, 情報を通信するようになっている. 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. 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に対応したソフトウェアとして構築するのではなく, 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]. 本提案方式では, 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 度入られてしまったら, 攻撃されてしまう. 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

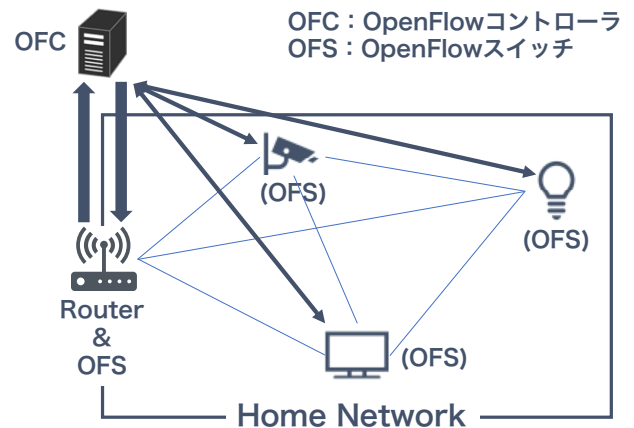


図1 提案手法のアーキテクチャ

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]. また, 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, マルウェアをインストールする. カメラに搭載されたマルウェアは, ローカルネットワーク上で他の潜在的に脆弱なデバイスをスキャンし, 例えばよく知られたセキュリティ上の欠陥を利用してそれらのデバイスにアクセスし, 同じまたは異なるマルウェアのコピーをさらにインストールしようとする. 感染した機器がマルウェアの支配下に置かれると, 個人情報の漏洩など, スマートホームネットワーク自体に被害を及ぼすだけでなく, DDoS 攻撃への加担やサービスの操作など, 他の悪意ある活動を行う可能性がある [4].

3 提案手法

前述の問題点を受けて, 関連研究は, 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としていた. しかし, デバイス間通信が想定され, 感染拡大を防ぐことを考慮し, ホームネットワーク内における検知も必要である. OpenFlow を利用することで, 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. 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

閉ざされたホームネットワークにおいて、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を以下に述べる。

1. 接続要求機器は仮想デバイス (OFS) に通信する
2. 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
3. OpenFlow コントローラはトラフィック情報を調査
4. 正当な通信の場合，OpenFlow コントローラは送信元機器に対して，許可メッセージとして，Flow Mod メッセージを送信
5. 不正な通信の場合，OpenFlow コントローラは送信元機器に対して，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実証したい。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，

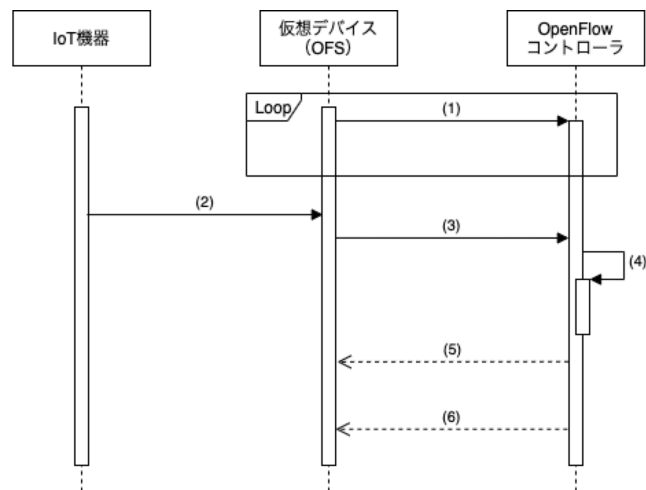


図 2 動作手順のシーケンス図

5 まとめ・今後の課題

本稿では，ホームネットワークの携帯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，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。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において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を決めたい。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。そのため，どのようにセキュリティを評価するのかを考えたい。

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.1-6，2016/2.
- [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.