

ECHONET Lite 機器のセキュア遠隔制御システムの提案

田中 久順^{†1} 山田 貴之^{†2} 大久保 陽平^{†2} 鈴木 秀和^{†2} 内藤 克浩^{†3} 渡邊 晃^{†2}
^{†1} 名城大学理工学部 ^{†2} 名城大学大学院理工学研究科 ^{†3} 愛知工業大学情報科学部

1 はじめに

近年, ECHONET Lite 等を始めとする宅外から遠隔制御できる家電製品が普及している. その多くは, インターネット上にメーカーが遠隔制御サーバを設置し, 操作端末からの制御命令を経由させることで, 宅内家電の遠隔制御を実現している [1]. しかし, サーバ上に操作ログが残ることによるプライバシーの課題や, メーカーのサポート終了により遠隔制御ができなくなるなどの課題がある. 本稿では, NAT 越えとエンドツーエンド接続性を実現できる NTMobile (Network Traversal with Mobility) [2] を利用することにより, 遠隔制御サーバを経由することなく宅外から宅内にある ECHONET Lite 機器を安全に遠隔制御するシステムを提案する.

2 NTMobile

NTMobile は仮想 IP アドレスとトンネル通信により, NAT 越えと移動透過性を実現する技術である. 通信開始時には経路制御サーバである DC (Direction Coordinator) による経路指示に従い, NTMobile 対応端末間に UDP トンネルを構築する. 端末間は仮想 IP アドレスで通信相手を認識し, 仮想 IP アドレス宛での IP パケットを生成する. この IP パケットは暗号化および実 IP アドレスを利用した UDP/IP ヘッダでカプセル化され, 構築したトンネルを用いて, 直接通信相手へ送信される. これにより, アプリケーションは通信経路上に存在する NAT やネットワークの移動等の影響を受けることなく, 安全にエンドツーエンド通信を行うことができる.

3 提案方式

3.1 概要

家電制御プロトコルの一種である ECHONET Lite に対応した機器を対象に, NTMobile を用いて宅外から遠隔操作を行う. 図 1 に UDP トンネル構築後の提案システムの概要を示す. 以後, NTMobile と ECHONET Lite 機器制御アプリケーションを搭載した操作端末を MN

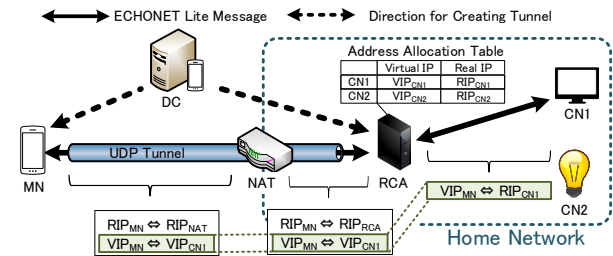


図 1 提案システムの概要図

(Mobile Node), 操作対象となる宅内の ECHONET Lite 対応家電機器を CN (Correspondent Node) とする. また, MN と CN の通信を中継する機器として, 新たに RCA (Remote Control Agent) を宅内に設置する. RCA には NTMobile を実装し, CN に対応付けるための仮想 IP アドレスを複数プールさせる. MN は NTMobile を利用して RCA との間にトンネルを構築し, ECHONET Lite 機器を制御するメッセージを RCA を経由することにより, 宅内に設置されている市販の ECHONET Lite 機器の遠隔制御を実現する.

3.2 通信シーケンス

NTMobile におけるトンネル構築処理は DNS を利用した通信相手の名前解決処理をトリガに実行される. これに対して ECHONET Lite では機器探索のためにマルチキャストパケットが送信される. そこで提案方式では, MN がこの探索パケットの送信を検知した際に, NTMobile によるトンネル構築処理および宅内の CN の探索処理を実行するよう, NTMobile を拡張する.

図 2 に機器探索通信の流れを示す. MN は ECHONET Lite 機器探索メッセージを検知すると, NTMobile のシグナリング処理を開始し, 予め決められた RCA との間で暗号化されたエンドツーエンドの UDP トンネルを構築する. その後, MN は機器探索パケットの代理送信を要求するために, 新たに定義する NTMobile の制御メッセージ Multicast Request を RCA に送信する. Multicast Request には宛先マルチキャストアドレス, 宛先ポート番号, 送信元 IP アドレス (MN の仮想 IP アドレス VIP_{MN}), 送信元ポート番号, 制御メッセージが格納されている. RCA は受信した Multicast Request を基に探索パケットを生成し, MN の代理で送信することにより, 宅内にある CN を探索する.

CN は探索パケットを受信後, MN の仮想 IP アドレ

A Proposal of Secure Remote Control System for ECHONET Lite Home Appliances Using NTMobile

Hisayoshi Tanaka^{†1}, Takayuki Yamada^{†2}, Yohei Okubo^{†2},

Hidekazu Suzuki^{†2}, Katsuhiko Naito^{†3} and Akira Watanabe^{†2}

^{†1} Faculty of Science and Technology, Meijo University

^{†2} Graduate School of Science and Technology, Meijo University

^{†3} Faculty of Information Science, Aichi Institute of Technology

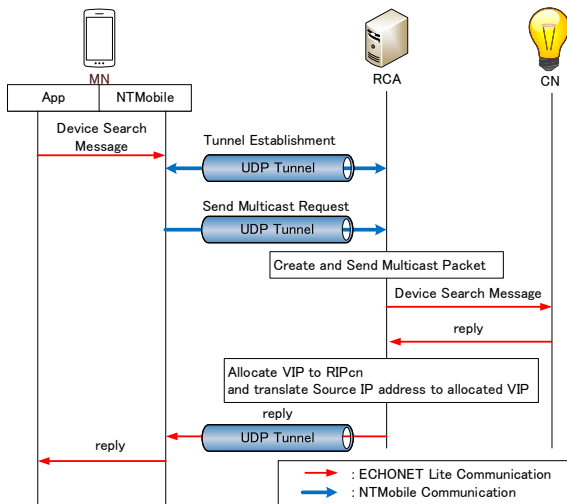


図2 ECHONET Lite 機器に対する探索シーケンス図

ス VIP_{MN} 宛に回答パケットを送信する。なお、仮想 IP アドレス宛のパケットが RCA に届くよう、事前に宅内のルータ等を設定しておく。回答パケット内には ECHONET Lite 通信で制御可能な家電機器の情報が含まれ、これを受信した RCA は UDP トンネルを用いて MN に転送する。この際、RCA は回答パケット内にある CN の実 IP アドレス RIP_{CN} と仮想 IP アドレスを対応付け、その対応関係をアドレス割当テーブルにて管理する。その後、RCA は回答パケット内にある RIP_{CN} を対応付けた仮想 IP アドレス VIP_{CN} に書き換え、パケットを MN へ送信する。

MN は入手した CN の仮想 IP アドレス VIP_{CN} を指定して制御を行う。機器探索時に構築した UDP トンネルを再利用して、ECHONET Lite 機器の制御メッセージを RCA に送信する。RCA は制御メッセージを受信した後、パケットの復号およびデカプセル化を行う。さらに宛先の VIP_{CN} を用いてアドレス割当テーブルを参照し、 RIP_{CN} 宛に制御メッセージを転送する。制御メッセージに対する CN からの応答は、再度 RCA を経由して上記と逆の処理手順により MN まで転送される。

以上により、メーカーが設置した遠隔制御サーバを中継することなく、宅外から ECHONET Lite 機器を安全に制御することができる。

4 実装

従来の NTMobile におけるデーモンプログラム及びカーネルモジュールを拡張し、MN と RCA のプロトタイプ実装を行った。

4.1 MN

Linux の Netfilter モジュールを利用したカーネルモジュールを拡張し、機器探索を行う際に送信するマルチキャストパケットの検知機能を実装した。この機能

は、自端末が送信した探索パケットの情報を、Netlink ソケットを利用してユーザ空間で動作するデーモンへ転送する。デーモンプログラムは事前に指定された RCA とトンネル構築を行えるように機能を拡張した。その後、探索パケットの情報を元に Multicast Request の生成および送信機能を実装した。

4.2 RCA

Multicast Request を受信して、探索パケットを生成し、宅内ネットワーク内にマルチキャストする機能をデーモンとして実装した。また、CN の実 IP アドレスをアドレス割当テーブルに登録する機能を実装した。カーネルモジュールには、CN からの応答パケットを Netfilter によりフックし、デーモンへ渡す機能を実装した。

5 評価

プロトタイプシステムの実装を進めた。現在、MN において、ECHONET Lite 機器探索パケットをトリガにトンネル構築を実行する機能、RCA では宅内ネットワークに機器探索パケットを送信する機能まで実装した。

従来手法では遠隔制御サーバが停止したり、サービスが終了した際、宅外からの制御ができなくなることに加え、複数の家庭において同様の問題が発生する。提案手法では、操作端末と RCA が直接通信を行うため、従来手法のような課題は発生しない。

また、従来手法では宅外からの制御は遠隔制御サーバを経由するため、制御端末が応答を受け取るまでに時間がかかる。提案手法では、遠隔制御サーバを経由することなく直接メッセージを送受信するため、従来手法より短時間で制御が可能となる。

以上より、ユーザの管理外となる機器やサービスの影響を受けず、かつ従来よりプライバシーや応答性の観点で優れていると言える。

6 まとめ

本稿では、NTMobile を用いた ECHONET Lite 対応家電の遠隔制御手法を提案した。提案手法により遠隔制御サーバを介さずに家電を遠隔操作することができる。また、従来システムよりセキュアかつメーカーのサポート状況に依存せず利用が可能となる。

謝辞

本研究は内藤科学技術研究助成金を受けて実施したものである。

参考文献

- [1] 江坂．他：東芝レビュー，Vol. 70，No. 6，pp. 23–26，2015.
- [2] 鈴木．他：情報処理学会論文誌，Vol. 54，No. 1，pp. 367–379，2013.