NTMobileを利用したプライベートアドレス型WoTサーバに関する研究

183426006　黒宮　魁人
渡邊研究室

1. 序論

モノがインターネットに繋がるIoT（Internet of Things）が普及しつつある中，様々なフレームワークが乱立しサイロ化することが懸念されている．そこで，プラットフォームに依存しないWebの技術を利用することにより，IoTやアプリケーションを連携するWoT（Web of Things）がWorld Wide Web Consortiumによって提唱されている．しかしながら，WoTを支えるサーバはインターネットのグローバル空間に設置する必要があるため，サーバは常にDDoS攻撃を始めとした脅威に晒される．2016年にマルウェアであるMiraiがIoT機器に爆発的に感染したことにより，IoT機器の脆弱性が明るみになり，今に至るまで新種のマルウェアの開発と対策が繰り返されている．そのため，本稿ではNTMobile（Network Traversal with Mobility）を利用して，Webサーバをプライベート空間に設置し，異なるプライベートアドレス空間どうしで直接WoTの通信を実現する方法を提案する．これによって，WoTを構成する全てのモノをプライベートアドレス空間に設置することができ，外部からの攻撃から保護することができる．この方式であればセキュリティが脆弱なIoT機器であっても，マルウェアなどの脅威から保護できる．検証作業としてRaspberryPiをRC Tankに拡張したもの（以降，RasPiTank）に制御用のWebサーバを構築し，提案手法の形式にて画像通信と制御が可能であることを確認した．

2. NAT越え手法に関する既存研究

NAT越えの既存研究として，ICE (Interactive Connectivity Establishment) と OpenVPN (Open Virtual-Private-Network) について紹介する．ICEは，NAT越え技術であるSTUN (Session Traversal Utilities for NATs) とTURN (Traversal Using Relay around NAT) を組み合わせてNAT越えを実現する技術である．処理の流れとしては，1. 通信する両端末が通信経路及びに通信相手の端末とのアドレス候補（以降，Candidate）を収集する．2. Signaling Server等を利用してお互いのCandidateを交換する．3. 交換したCandidateの優先度が高いものからSTUN/TURNによる接続を確認する．4. 通信可能な経路を見つければICEを利用したコネクションを確立する．しかし，ICEはライブラリでの提供となるため，既存のシステムに対しての適用が難しい．

OpenVPNは，例えば，公衆の無線LANから自宅のパソコンをリモートコントロールする時などに利用される．このとき，セキュリティが考慮されていない公衆の無線LANであれば自宅のPCに対してポートフォワーディングをして接続していることが分かってしまうため，自宅のPCがパスワード解析攻撃の対象になる可能性がある．OpenVPNを利用するとトンネリング通信が行われるため，第三者からはパケット盗聴の被害を防ぐことができる．また，基本的にOpenVPNを利用する端末同士は相互認証しているため，第三者によって改竄されたパケットは不正なものとして破棄される．しかし，OpenVPNにてNAT越えを行うには，デカプセル処理や中継処理を行うOpenVPNのサーバをNAT配下に設置する必要があるが，このサーバにアクセスするために1194番ポート（デフォルト）に対してポートフォワーディングとファイアウォールの設定を行う必要がある．他にもサーバを確実に中継するためスループットが低下するという課題も存在する．

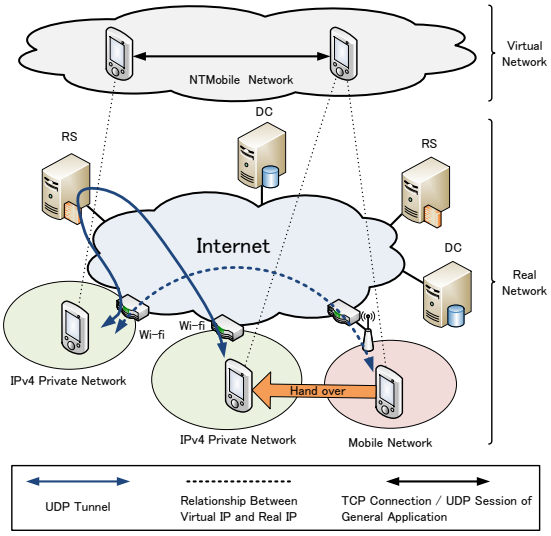

図 1: NTMobileの構成

3. 提案方式

3.1 NTMobile

NTMobileはNATの変更を必要とせずにNAT越え問題を解決し，IPv4/IPv6ネットワークが混在した環境においても，端末の通信接続性を実現する通信技術である．また移動透過性も有する．図1にNTMobileの構成を示す．NTMobileによる通信を利用するためには，NTMobileがインストールされた端末（以降，NTM端末）の他に，端末情報の管理や通信経路の指示，仮想IPアドレスの割り当てを行うDC（Direction Coordinator），NTM端末が直接通信が行えない場合に，パケットの中継を行うRS（Relay Server）が必要とされる．DCとRSはネットワークの規模に応じて，複数台設置することが可能である．これによって，各装置の負荷が分散できる．NTMobileでは，装置間ではTLS双方向による認証，端末は全て共通鍵で認証した通信を行っているため，MitM（Man-in-the-Middle）攻撃に耐性を持ち，リプレイ防御ウィンドウによるリプレイ攻撃の対策もされている．また，DDoS攻撃対策として，MAC (Message Authentication Code) 認証が実装されている．さらに，シーケンス番号と共通鍵を利用した簡易認証をパケット受信時に実行することで不正なパケットをより高速に破棄できる．現在，DCにNTMobileの通信グループの設定を行う検討がされており，これが実装されれ

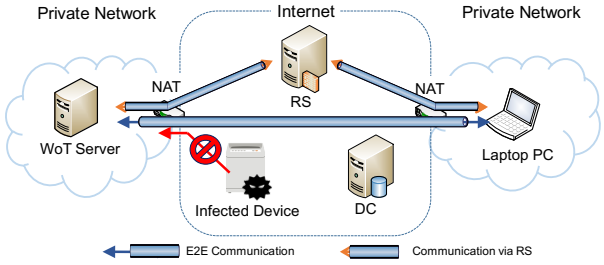

図 2: 提案システムの構成

ば，NTMobile 通信であっても，許可されていない端末には DC が通信経路の指示をしない．これによって，悪意のある攻撃の被害が小さくなると考えられる．

3.2 提案システムの構成

図 2 に提案システムの構成を示す．Web of Things を構成する Web サーバ（以降，WoT サーバ）を NAT 配下に設置し，NTMobile を利用して通信する．これによって，NAT やファイアウォールの変更せずにどのような環境からでも WoT サーバに通信が開始できる．NTMobile 通信でない端末は NAT によって WoT サーバのアドレスが隠蔽されるため，通信を開始することができない．そのため，大規模な DDoS 攻撃から WoT サーバを守ることができる．

4. 検証

4.1 検証の方法

RaspberryPi に市販されているキットを装着して，RaspberryPi の GPIO ポートの出力によって自走する RC タンクを作成した．検証では，この RasPiTank の中に WebIOPi を利用して WoT サーバを構築し，異なるプライベートネットワークに接続されたラップトップ PC のブラウザから，RasPiTank を制御した．

4.2 Web ページと Web サーバの作成

図 3 に，RasPiTank の外観と作成した Web ページのスクリーンショットを示す．図 3 の右側の Web ページのうち，青枠内の画像が RaspberryPi がカメラモジュールで取得した画像である．今回は，mjpg-streamer を利用して html ファイルに埋め込んでいる．赤枠内の部分が RasPiTank を制御するコントローラになる．これは WebIOPi をインポートした python ファイルに各ボタンに対応した処理を記述して html ファイルから呼び出した．

4.3 TUN 型 NTMobile を利用した接続の確認

TUN 型 NTMobile は，Linux の TUN サービスと，NTMobile の通信ライブラリを利用して作成されたアプリケーションである．TUN 型 NTMobile は TUN インターフェースに仮想 IP アドレスを割り当てて利用する．よって，NTMobile 通信を利用するアプリケーションが送信する仮想 IP アドレス宛の IP パケットは，全て TUN インターフェースにルーティングされる．TUN インターフェースに流れるパケットは全てユーザ空間の NTMobile の通信ライブラリがフックして実インタフェースに書き込むため，既存のプログラムの書き換えやカーネルの改造は一切行う必要がない．これにより，端末の全ての通信は TUN 型 NTMobile のアプリケーションを起動するだけで NTMobile 通信ができる．検証作業では Web サーバとクライアントに，TUN 型 NTMobile をインストールし，図 2 の環境で Web 通信ができることを確認をした．

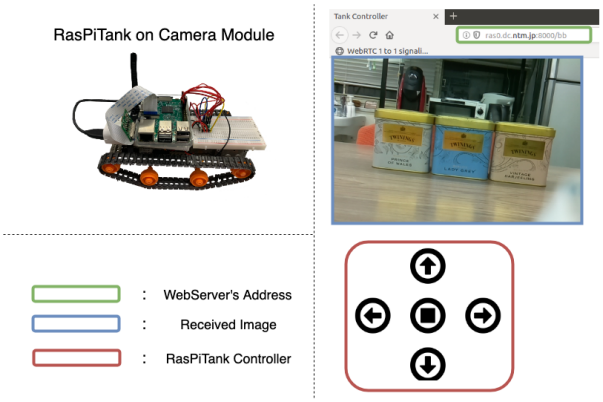

図 3: RasPiTank 外観と作成した Web ページ

表 1: 既存研究との比較

	ICE	OpenVPN	NTMobile
既存システムへの適用	×	○	○
NAT と Firewall の設定	○	△	○
対応する OS の種類	○	○	△
DDoS 攻撃への耐性	-	○	◎

5. 評価

表 1 に，提案方式と既存研究の比較結果を示す．既存システムに適用の項目では，ICE はアプリケーションに ICE のライブラリを組み込む必要があるため×とした．NAT と Firewall の設定であるが，OpenVPN は NAT とファイアウォールの設定を変更する必要がある場合があるため△とした．OS の自由度は，TUN 型 NTMobile が基本的に検証を Linux 行っているため，現段階では Windows や iOS にて動作しない．しかし，原理的には動作可能であるため，△の評価を与えている．DDoS 対策への耐性の項目は，ICE は組み込まれたアプリケーションに依存するため評価を行っていない．NTMobile は，DDoS 攻撃による不正なパケットを簡易認証によって，既存研究より高速に処理ができるため◎の評価を与えている．

RasPiTank を名城大学の多段 NAT 配下にある 2.4GHz 帯のルーターに接続した．Laptop PC は UQ Wi-MAX2+ に接続した．この環境で RS 経由の NTMobile 通信を利用してパケットを送信したところ，パケットは 84.559[msec] にて到達した．この値は 100 回送信した際の平均値である．この性能は NTMobile を使わない通信の約 76%であった．

6. 結論

本研究では，NTMobile を利用して WoT サーバをプライベートネットワークに設置する提案を行った．また，提案方式を検証するために，RaspberryPi に NTMobile と WebIOPi による WoT サーバを実装し，提案方式による通信の確認を行った．性能評価では，NTMobile を利用しない通信の約 76%の性能にて通信が行えることを確認した．

参考文献

[1] 鈴木 秀和，上酔尾 一真，水谷 智大，西尾 拓也，内藤 克浩，渡邊 晃: NTMobile における通信接続性の確立手法と実装, 情報処理学会論文誌, Vol. 54, No. 1, pp. 367–379 (2013).

[2] 内藤 克浩，上酔尾 一真，水谷 智大，西尾 拓也，鈴木 秀和，渡邊 晃: NTMobile における移動透過性の実現と実装, 情報処理学会論文誌, Vol. 54, No. 1, pp. 380–393 (2013).