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．

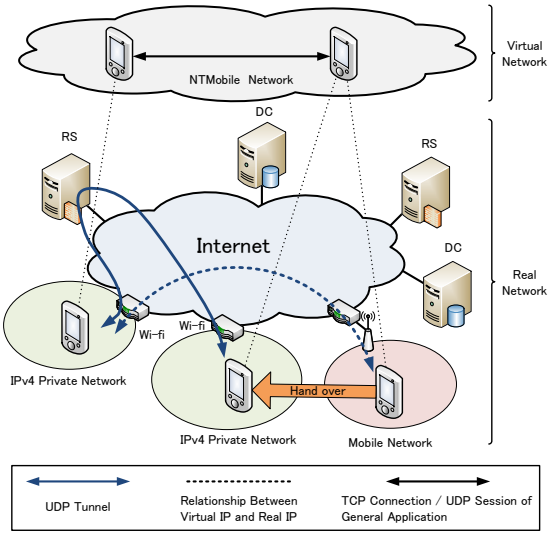


図 1: NTMobileの構成

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

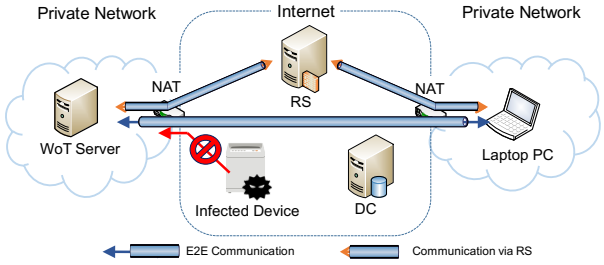


図 2: 提案システムの構成

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．

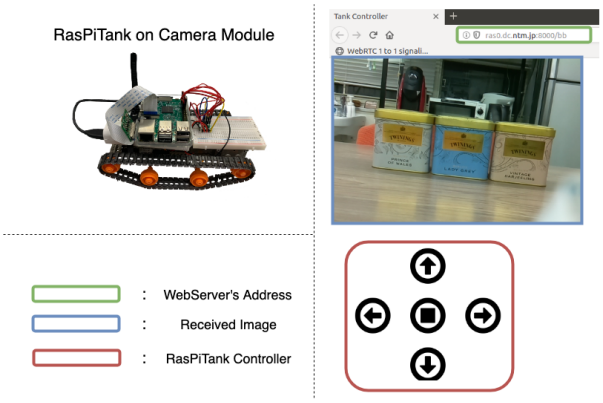


図 3: RasPiTank 外観と作成した Web ページ

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).

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

理工学研究科情報工学専攻

学籍番号:183426006

渡邊研究室:黒宮魁人

はじめに

- IoT (Internet of Things)が世界的に広がっている
  - 様々なIoTの通信規格が生まれている
  - しかし，複数のフレームワークが乱立するという課題がある

- WoT (Web of Things)はWebの技術を利用することで，プラットフォームに依存しない通信が可能[1]
  - サーバをグローバルネットワークに設置すると攻撃や不正アクセスのターゲットになる

[1] : World Wide Web Consortium. : https://www.w3.org/.

IoT機器による攻撃の事例

- 2016年にIoT機器に感染するMiraiが猛威を振るった
  - DNS提供会社が標的にされ，GitHubやTwitterといった大手のSNSサービスに通信障害が発生[2]
  - Miraiに感染したIoT機器は51万5000台以上であると推定されている[3]

何故，Miraiが爆発的な感染をしたのか

1. 23 番ポート，2323 番ポートでtelnetが動作するIoT 機器の存在
2. ID とパスワードがハードコーディングされたままのIoT機器の存在
3. IoT機器の初期パスワードを変更しないユーザの存在

2, 3番の条件に当てはまるIoT機器は，辞書攻撃のターゲットになる

結果，感染したIoT機器はUDP flood, DNS floodを実行してしまう

[2] :辻　宏郷：顕在化したIoT のセキュリティ脅威とその対策(2017). https://www.ipa.go.jp/files/000062277.pdf.
[3] : Shodan. https://www.shodan.io/report/aE9jvAXo

研究の目的

研究の目的

・セキュリティが脆弱なIoT機器であっても安全なWoTシステム構築を目指す
・WoTサーバをプライベートネットワークに設置することにより，WoTサーバのIPアドレスを隠蔽する．これによって外部からの攻撃から保護する

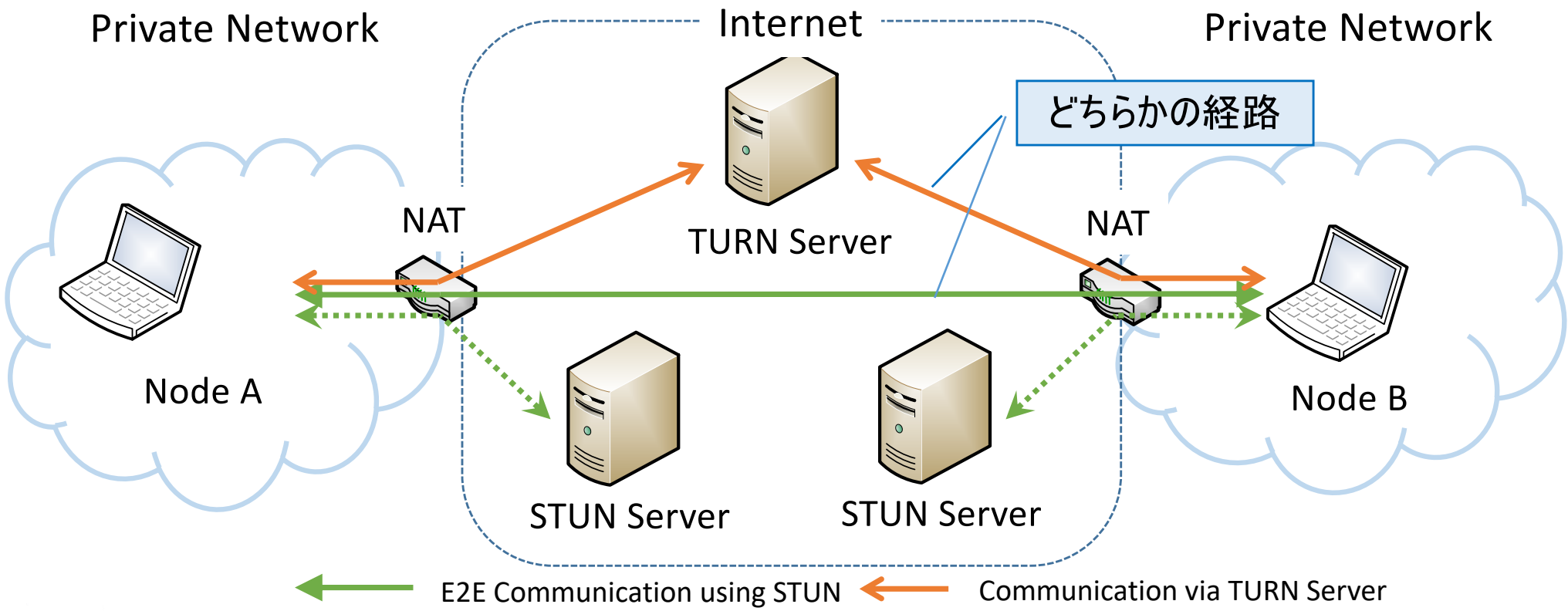
実現のために求められる要素

- どのような環境でもプライベートネットワークに通信開始ができる
- 高セキュリティで，安全な通信を提供できる

ICE (Interactive Connectivity Establishment)

- ICEはSTUN/TURNを組み合わせてNAT越えを提供[4]
  - STUN/TURNから得た経路の中から最良のものを選択
    - 可能な限り，NATやTURNサーバを経由しない経路

ICEの課題：アプリケーション作成時にICEライブラリを組み込む必要があるため，既存システムへの適用が難しい．

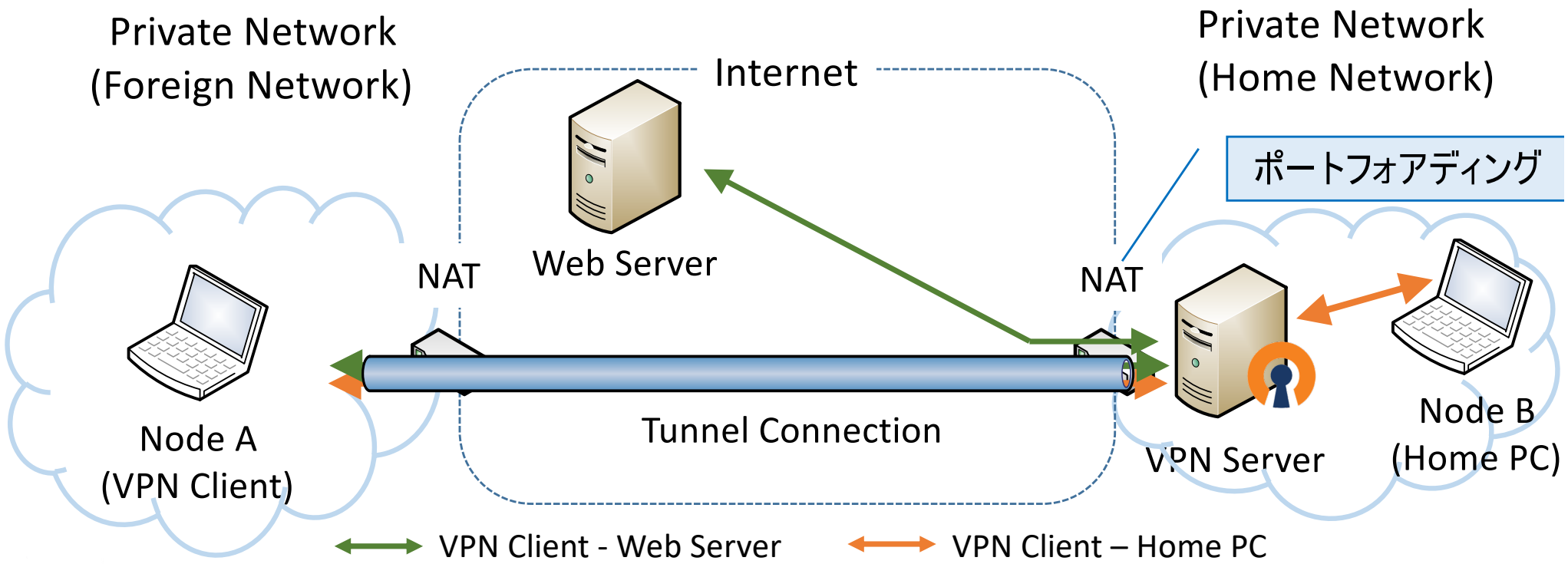


[4] : Interactive Connectivity Establishment (ICE): https://tools.ietf.org/html/rfc8445.

OpenVPN (Open Virtual Private Network)

- アプリケーションにユーザ空間でVPN通信を提供[5]
  - 仮想I/FのTUN/TAPを利用してトンネル通信を実現
- 出先のネットワークから自宅のPCに安全な接続が可能

OpenVPNの課題：・全ての通信経路がVPN Serverを中継する.
・NATとFirewallの設定を変更する場合がある.

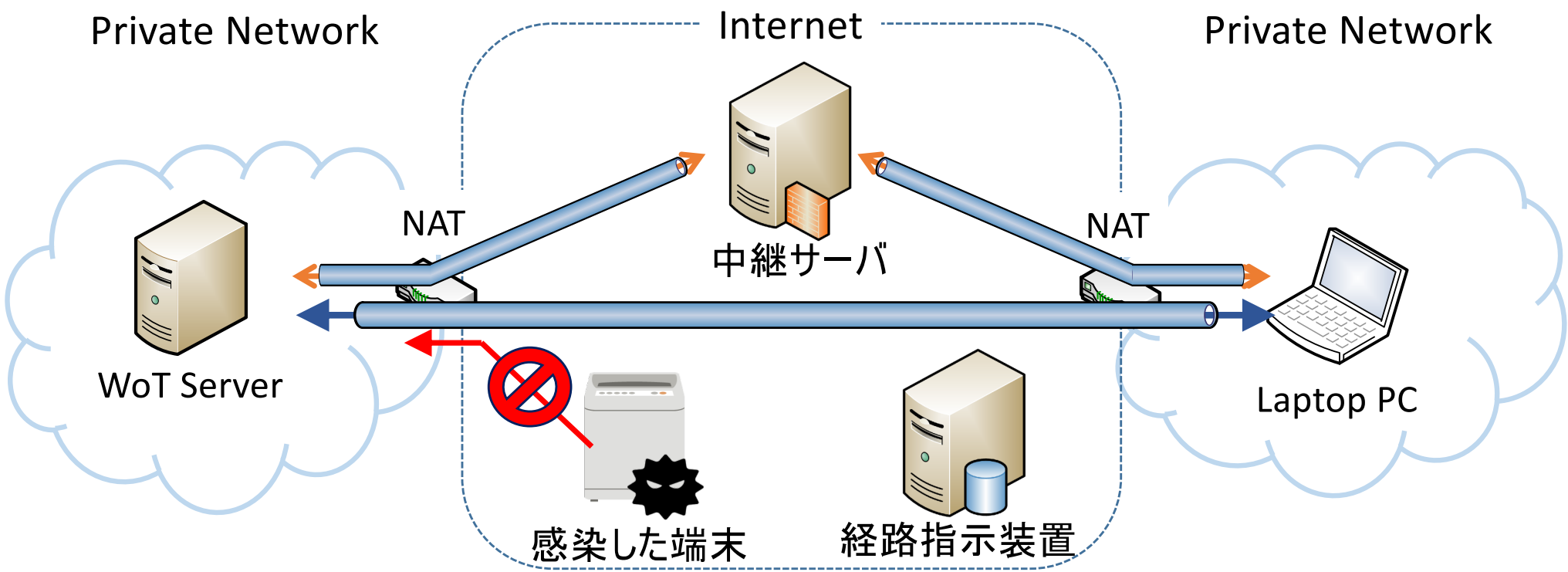


[5] : openvpn: VPN Software Solutions & Services For Business. https://openvpn.net/.

提案

提案方式

安全な通信を実現するために，NTMobileを利用してWoTサーバとクライアントを異なるプライベートネットワーク間で制御する



NTMobile (Network Traversal with Mobility)

- 移動透過性とNAT越え問題の解決を同時に実現[6][7]
- NTMobileは仮想IPアドレスを各端末に割り当てる
  - 移動透過性の実現
    - 実IPパケットによる仮想IPパケットのカプセル化
  - NAT越え問題の解決
    - DC (Direction Coordinator)が，通信経路の指示を行う
    - NATの設定を変更することなくNAT越え問題の解決が可能
- IPv4 / IPv6の相互通信が実現できる

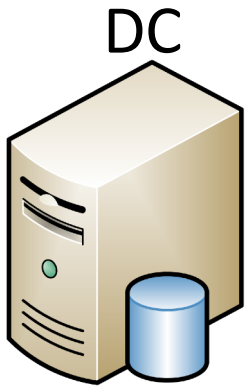
実IPアドレス ：ルータ等から割り当てられるIPアドレス

仮想IPアドレス ：NTMobileによって割り当てられるIPアドレス
IANAが規定している “198.18.0.0/15”の帯域を使用

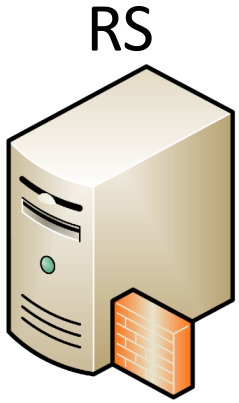
[6] : 鈴木秀和，上酔尾一真，水谷智大，西尾拓也，内藤克浩，渡邊　晃 : NTMobile における通信接続性の確立手法と実装，情報処理学会論文誌
[7] : 内藤克浩，上酔尾一真，水谷智大，西尾拓也，鈴木秀和，渡邊　晃 : NTMobile における移動透過性の実現と実装，情報処理学会論文誌

NTMobileの装置群

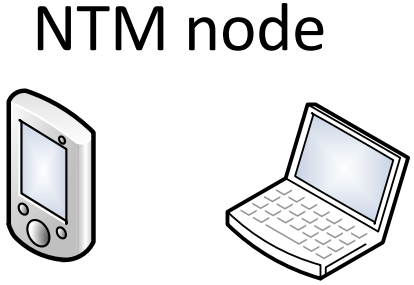
- DC（Direction Coordinator）
  - 仮想IPアドレスの配布
  - 通信経路の指示



- RS（Relay Server）
  - 必要に応じてパケットを中継
    - 両端末がNAT配下に存在する時
    - IPv4 / IPv6の相互通信



- NTM node
  - NTMobileの機能を持つ端末
  - LinuxとAndroidで動作を確認済み

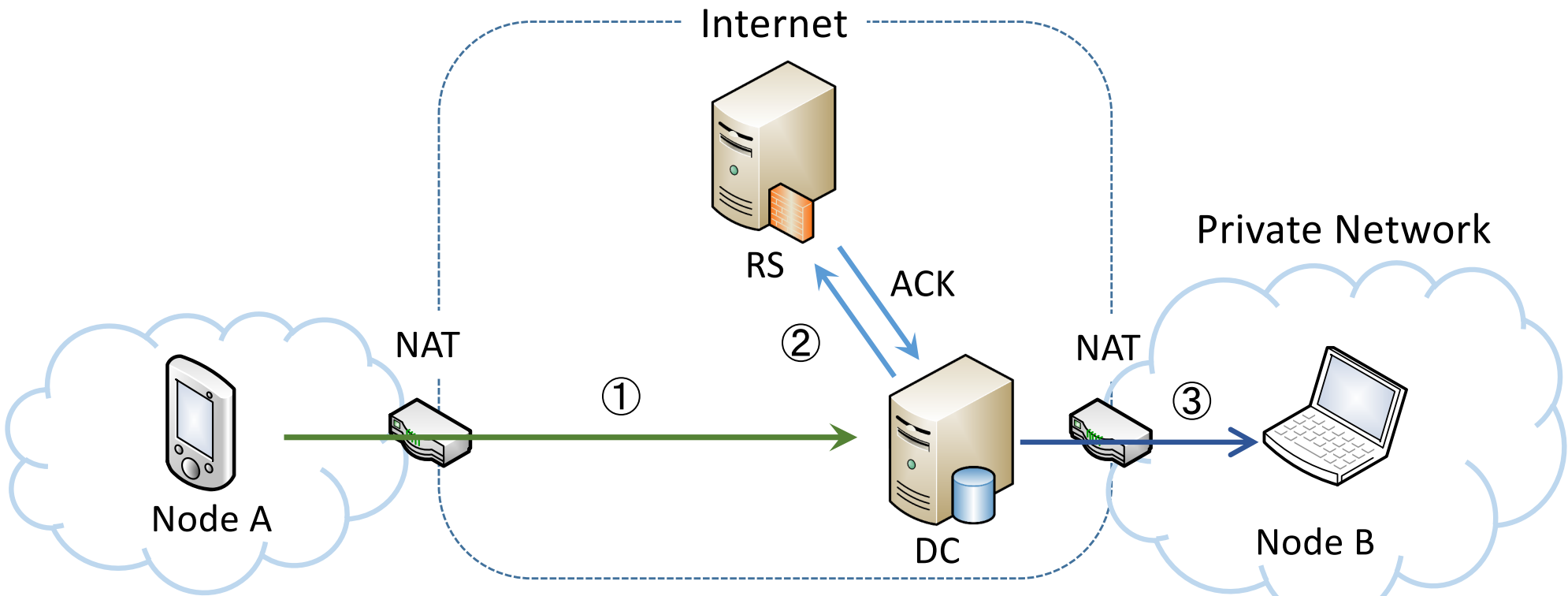


NTMobileのセキュリティ

- NTMobileで使用するDC, RSは分散配置可能
  - 1つのDCやRSに依存した通信ではない
- 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
  - これによってMitM(Man in the Middle) 攻撃に耐性
- Replay攻撃対策に，Anti-Replay Windowを実装
- DoS攻撃対策には簡易認証を利用
  - 不正パケットを約1/8の速度で破棄できる

NTMobileの動作概要

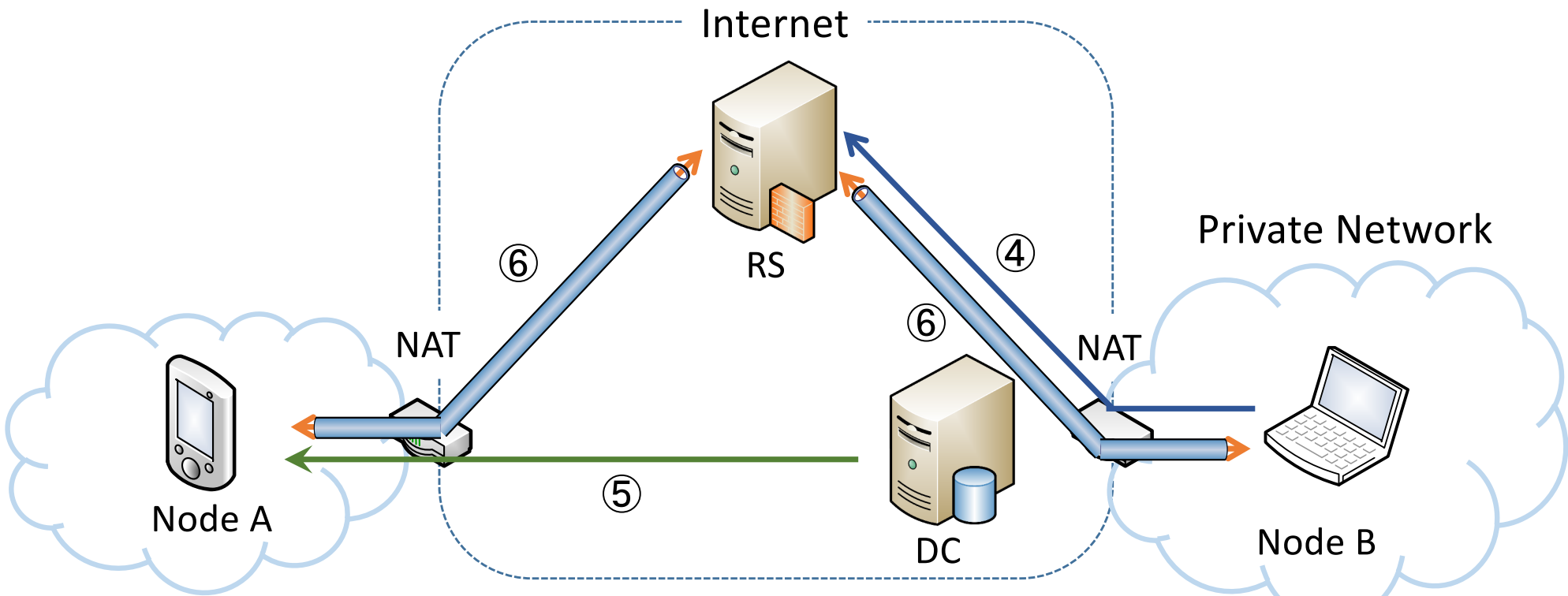
- NTMobileの動作概要を示す
  1. Initiator(Node A)がDCに通信経路の指示を要求
  2. DCがRSにNode AとNode Bの通信中継を依頼
  3. DCがNode BにRSのアドレスを通知



前提として，Node AとNode Bは，KeepAliveをDCに送信している

NTMobileの動作概要

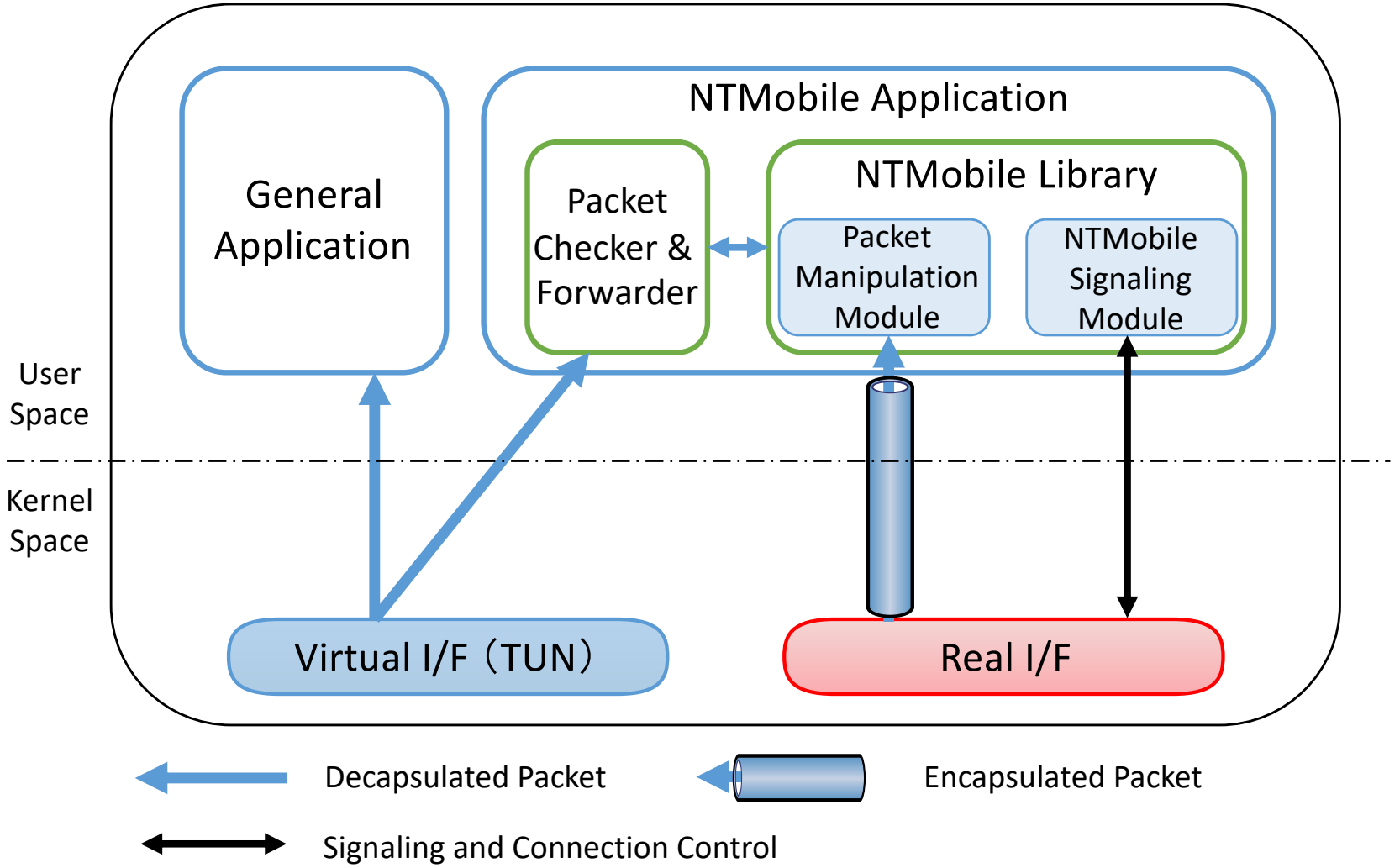
- NTMobileの動作概要を示す
  4. Node BがRSにHole Punchを送信
  5. DCがNode Aに通信経路の指示
  6. RSを経由した通信経路が構築



前提として，Node AとNode Bは，KeepAliveをDCに送信している

NTM Nodeのモジュール構成

- NTM nodeのモジュール構成は以下のとおりである



検証

検証内容

RaspberryPiのGPIOピンの出力によって自走するラジコン戦車を作成した（以降，RasPiTank）．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WoT サーバにアクセスし，RasPiTank を制御した．

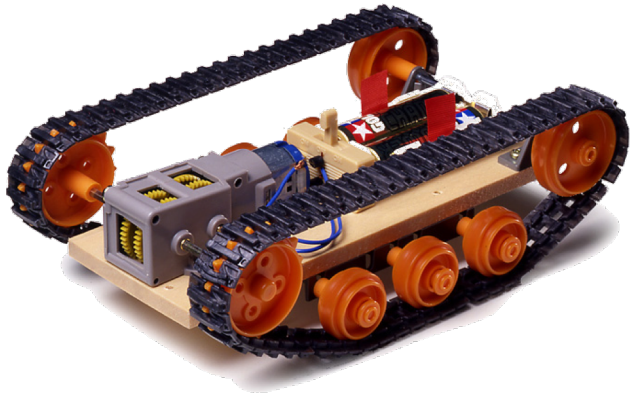
使用した諸元

	OS	CPU	Memory
Server	Raspbian 9.11	Cortex-A53 4 Core 1.2GHz	1GB
Client	Ubuntu16.04LTS	Intel Corei5-2520M 2.5GHz	2GB
DC on VPS	CentOS 6.9	Virtual CPU 1 Core 3.3GHz	512 MB
RS on VPS	CentOS 6.9	Virtual CPU 2 Core 3.1GHz	1536 MB

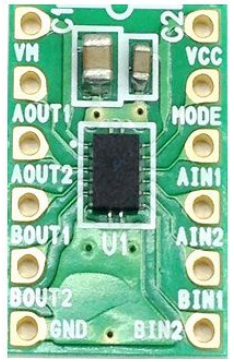
VPS : https://www.ablenet.jp/

検証に利用した機材（1 / 2）

- WoTサーバ（Raspberry Pi3に搭載）
  - WebIOPiにて構築（RaspberryPiのGPIOポートの制御）
- TAMIYAの楽しい工作シリーズ　タンク工作基本セット
  - モータ，単三電池ボックス，ギヤボックス，ホイール，キャタピラによって構成
- デュアルモータドライバ（型番：DRV8835）
  - GPIOピンの出力でモータを駆動させるために使用



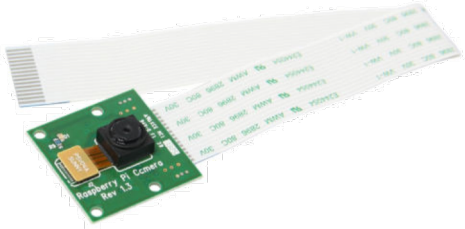
タンク工作基本セットの組み立てイメージ



DRV8835

検証に利用した機材（2 / 2）

- RaspberryPi Camera Module V1（Rev1.3）
  - RaspberryPiが映像をキャプチャするために使用
- モバイルバッテリー（型番：BSMPB5201P2WH）
  - BUFFALO製，5200mAhのものを使用
  - RaspberryPiに電源を供給するために使用

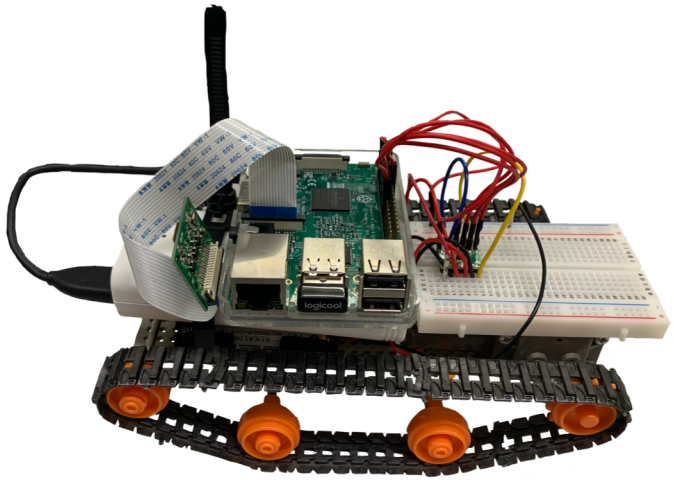


RaspberryPi Camera Module

モバイルバッテリー

WebIOPi

- RasppberryPi用のIoTフレームワーク
- WebIOPiはWebの技術を利用して，RaspberryPiのGPIOピンの操作を可能とする
- 本稿では，RasPiTankの制御に使用
  - RaspberryPiのGPIOピンの出力でモータを制御する



RasPiTank

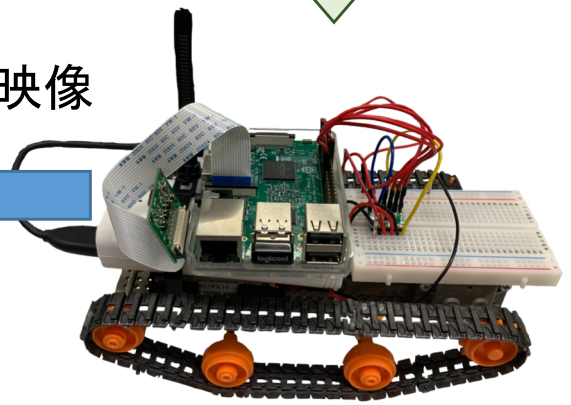
Browser

作成したWebページ

ブラウザのスクリーンショット

1: NTMobileのFQDNを指定して通信の開始

2: カメラが撮影した映像



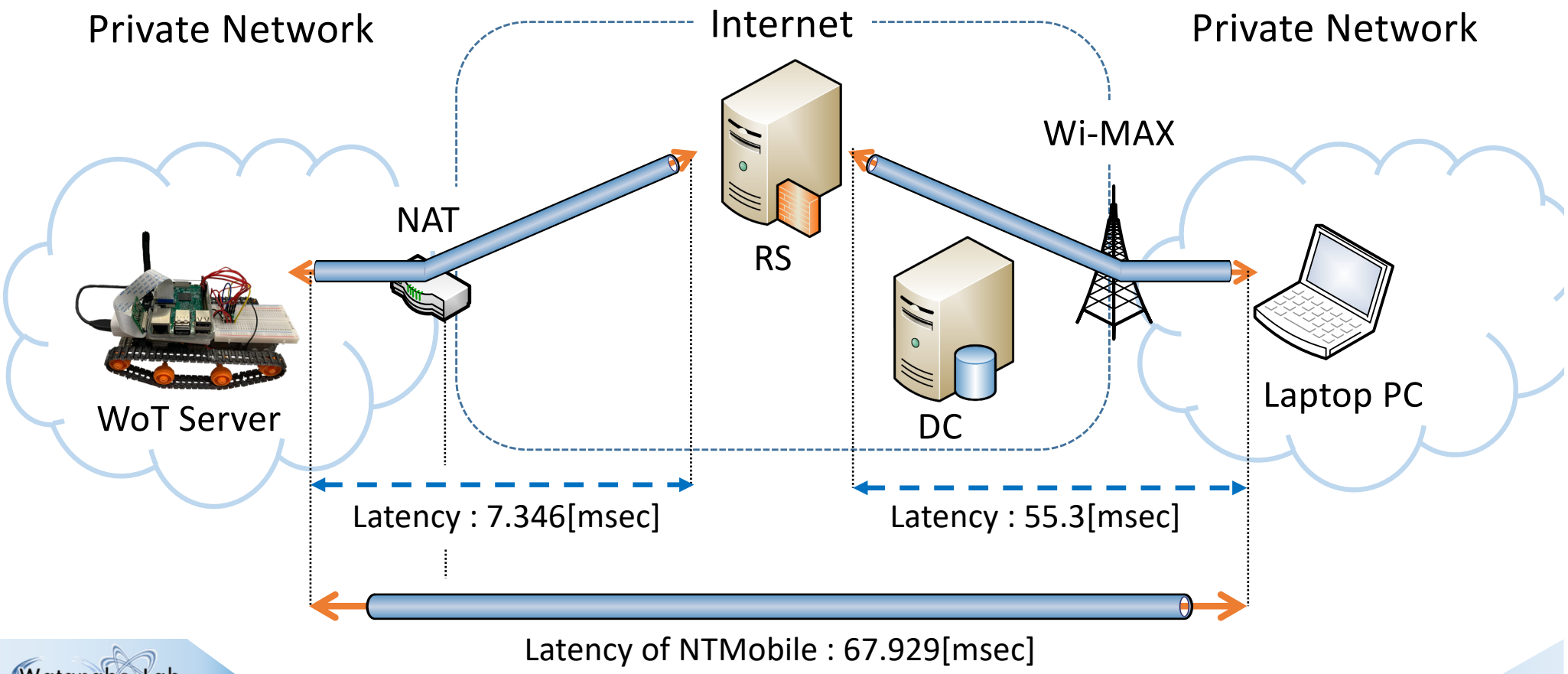
RasPiTank

3 : ブラウザからGPIOピンの制御

WebIOPiにて，GPIOピンの出力をモータドライバに送信

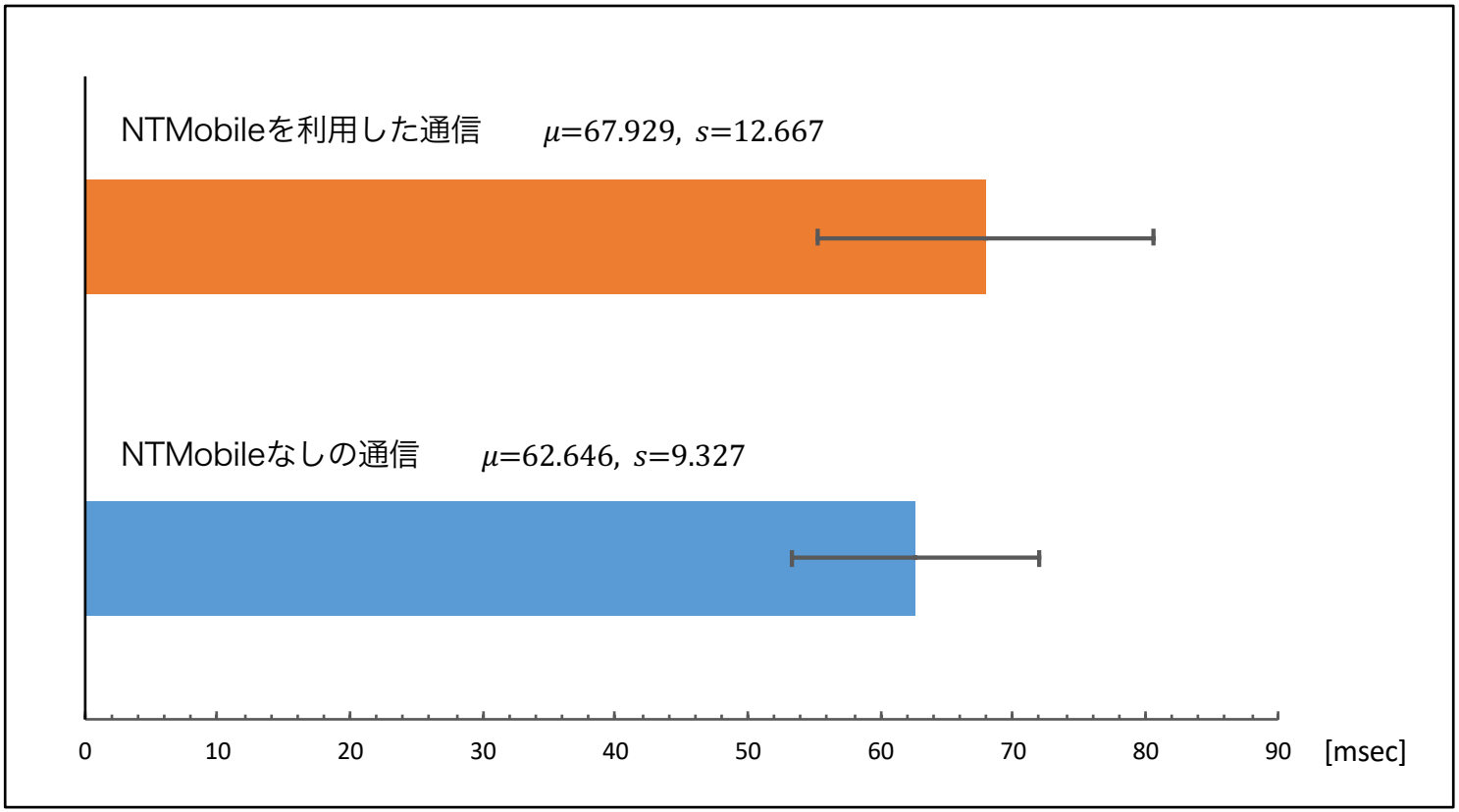
性能の評価

- NTMobileによって通信遅延がどの程度発生するのか測定
  - RasPiTank制御パケットはNTMobileを利用しないと測定できない
    - 代わりにPingのRTTを使用(100回平均)
    - NTMobileを利用しない通信は両端末からRSまでのRTTを合算した値を利用



性能評価

- 性能評価を行った結果を示す
  - NTMobileを利用した通信は $\mu = 67.929,\ s = 12.667$
  - NTMobileなしの通信で $\mu = 62.646,\ s = 9.327$

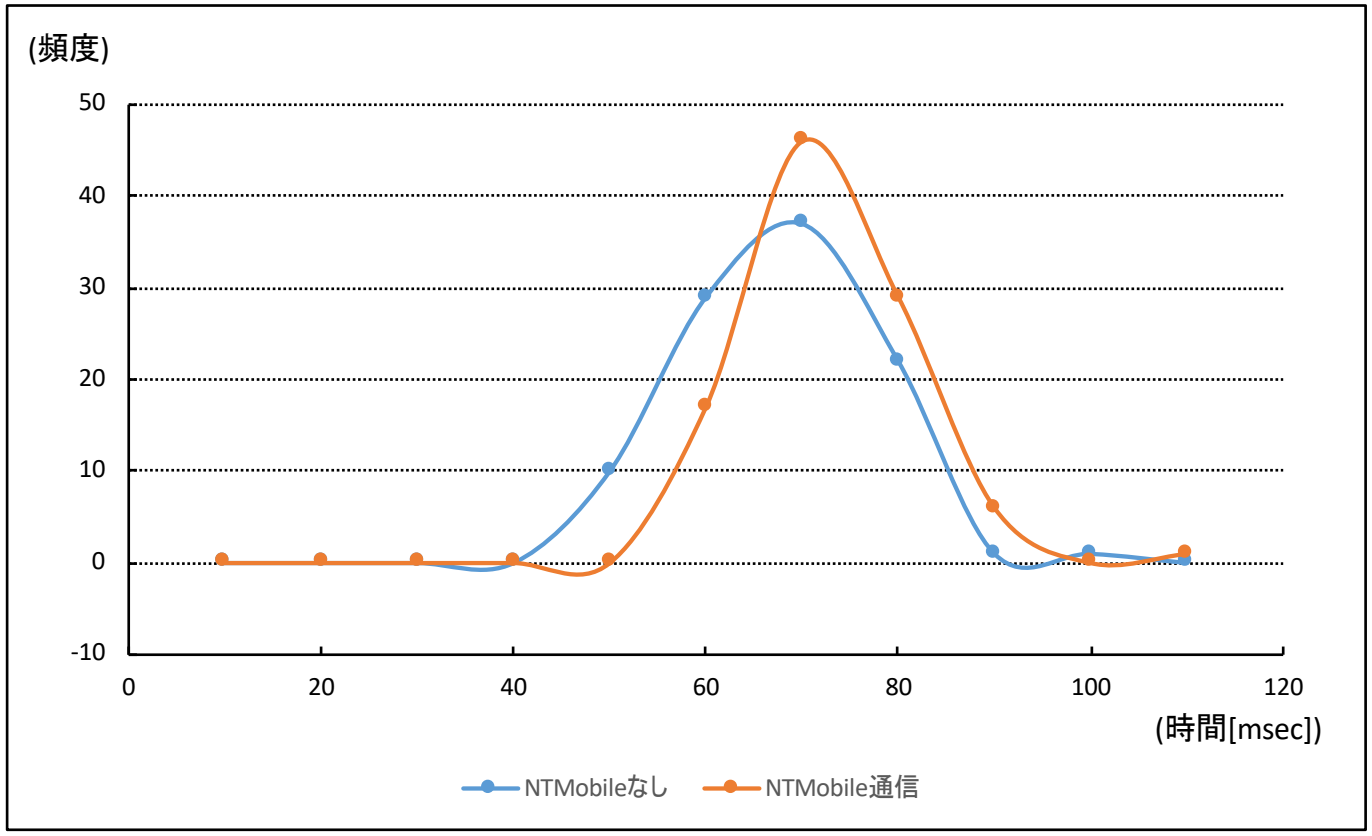


$z_n = \frac{x_n - \mu}{s}$ にて標準化を行い，　z_n が5より大きいものを外れ値として処理

測定結果のヒストグラム

- 二群間の比較をウェルチのt検定にて行った $\alpha = 0.05$
  - 対応のない，不等分散な正規分布であるため

F検定を2群間に行ったところ，$P(F \leq f) = 0.00129$ より帰無仮説は棄却



$t = 3.551, df = 182, p < 0.05$ で，帰無仮説が棄却された

測定結果に関する考察

- 検定結果から，性能が異なることが示された
  - NTMobileを利用すると性能は92%程度となる
    - RSの設置場所次第で，更に性能の低下が考えられる
    - RSが複数の通信を処理すると性能が低下する可能性もある

    → NTMobileの経路最適化を利用（RSを経由しない通信が可能）[8]
  - NTMobileを利用した通信の標準偏差が大きい
    - NTMobileがパケットを処理する時間のばらつき
    - RSがパケットを中継する時間のばらつき

リアルタイム性が必須とされるシステムでなければ，安全なWoTシステムの構築が可能

[8]：納堂博士，鈴木秀和，内藤克浩，渡邊　晃：エンドツーエンド通信をアプリケーションレベルで可能にする通信ライブラリの実現と評価，情報処理学会論文誌

関連技術との比較

- 関連技術との比較を行った

	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	×	○	○**

* Linux, Android以外にも原理的には実現が可能であるため，
将来的には，様々な環境でNTMobileを運用することが可能である

** 簡易認証によって関連技術より高速に不正パケットを廃棄できる

- IP Mobilityを意識した技術であるため，移動通信に応用が可能

以上から，関連技術と比較しても有用性はあると考えられる

まとめ

- NTMobileを利用してWoTサーバをプライベート空間に設置する方式について提案した
- 検証作業では，WebIOPiを利用したRaspiTankの制御を行った
  - RSを経由した通信で67.929[msec]にてパケットが到達
  - この値はNTMobileなしの通信の92%程度の性能

- 研究業績
  - 国際発表 : ICMU2018, ICCE2020
  - 国内発表 : DICOMO2018など6件
  - 展示会 : Interop2019など2件
  - 外部助成 :公益財団法人中部電気利用基礎研究振興財団
    （平成30年度国際交流援助海外渡航費助成）

アブストラクトの測定結果との差の考察

- アブストラクト執筆時
  - NTMobile利用時の通信の性能が約76%になると報告
- 今回の発表で提示した値
  - NTMobile利用時の通信の性能が約92%になると報告

考えられる要因

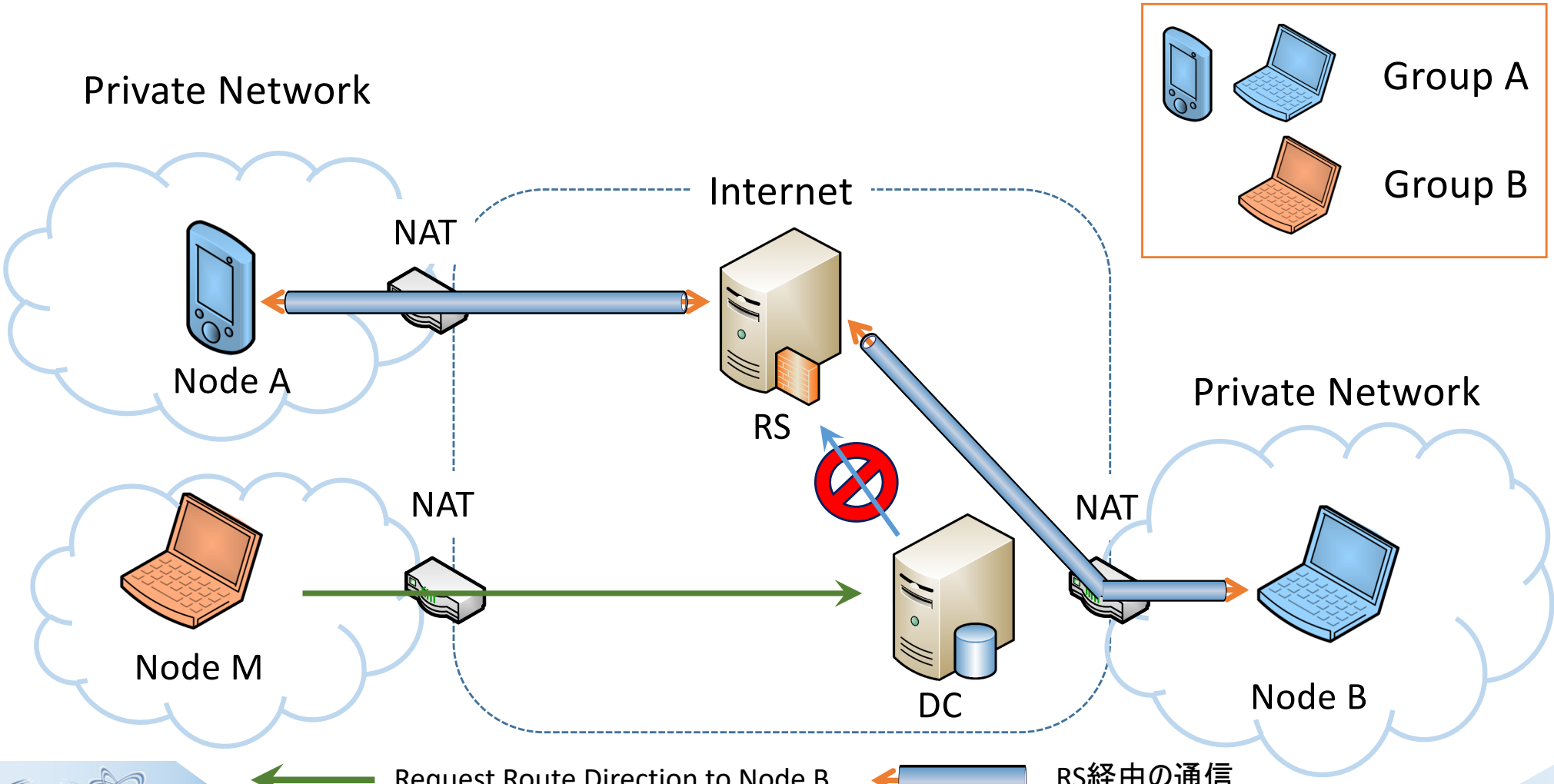
- アブストラクト執筆時に出した処理は，pingコマンド実行時の平均時間をそのまま利用している
  - 外れ値を除いていないためRTTが3000msec超えのパケットも計算
- 測定時間の差
  - アブストラクト執筆時は0:00から1:00の間，今回の発表では17:00から18:00にかけて測定している
    - アブストラクト執筆時の値はWiMAXの帯域が逼迫しやすく，不安定であることが要因の一つ？

他に行った研究

- Android向けのNTMobileに移動処理機能を実装
  - NTMobileのライブラリがOS共通でネットワークの変化を検出できなかった
    - Connectivity Managerを継承したレシーバを作成し，それをトリガとして，NTMobileの移動処理を実行させた
    - ネットワークを切り替えてもそのまま通信が維持できるようになった
- 統合生活支援システム（TLIFES）をRaspberry Piに構築して，NTMobileによる通信を確認
  - TLIFESは，ユーザの個人情報や位置情報を蓄積する
    - 不正アクセスにより，流失してしまう危険性があった
  - 各家庭ごとにTLIFESを実装したRaspberry Piを設置することで，インターネットからの攻撃から個人情報を保護する

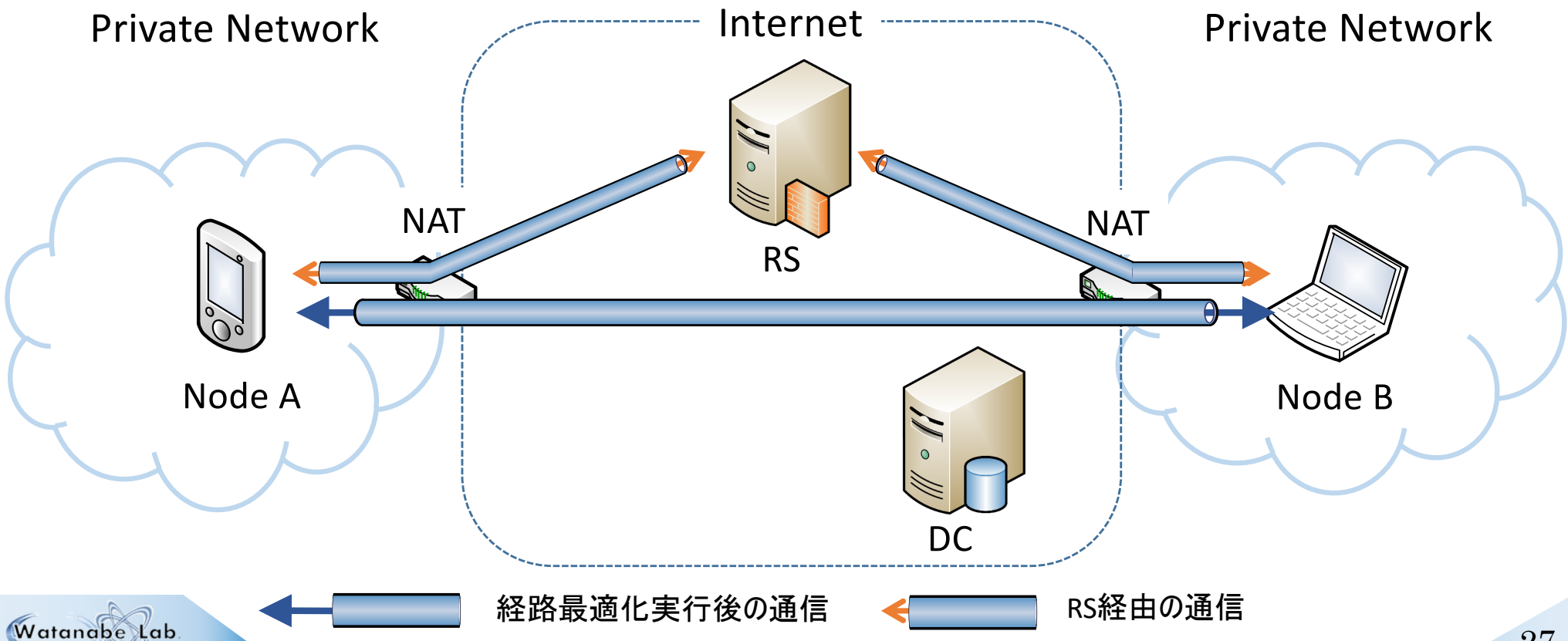
NTMobileのグルーピング

- NTMobileはグルーピング機能があり，特定のグループのみの通信を許可することが可能



経路最適化について

- NTMobileは経路最適化のオプションがある
- 経路最適化が成功するとE2Eの直接通信が可能
  - 経路最適化が失敗しても，確実にRS経由で通信ができる



DRV8835の挙動とRaspiTankの外観

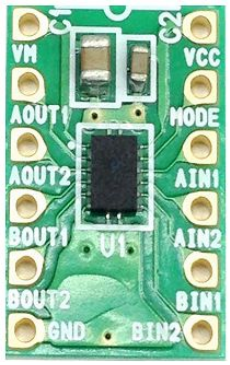
- DRV8835の挙動を左に，RasPiTankの外観を右に示す

DRV8835のピンの名称と機能

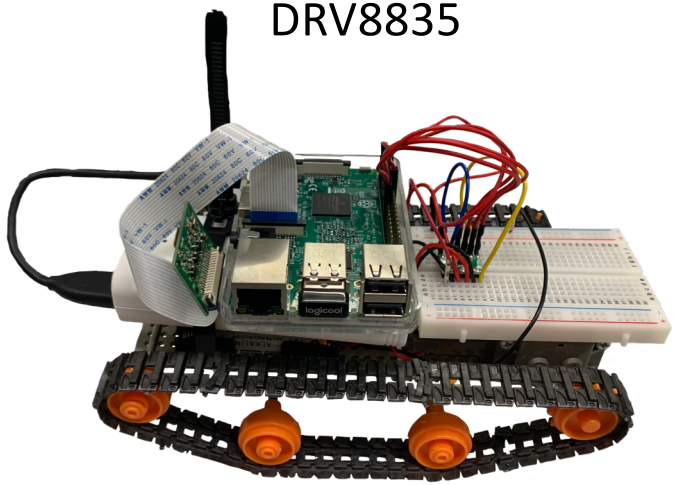
ピン	名称	機能	ピン	名称	機能
1	VMM	モータ電源	12	VCC	ロジック電源
2	AOUT1	A出力1	11	MODE	モード設定
3	AOUT2	A出力2	10	AIN1	A入力1
4	BOUT1	B出力1	9	AIN2	A入力2
5	BOUT2	B出力2	8	BIN1	B入力1
6	GND	グラウンド	7	BIN2	B入力2

DRV8835における入力と出力の対応

Mode	xIN1	xIN2	xOUT1	xOUT2	機能
0	0	0	Z	Z	Coast（空転）
0	0	1	L	H	Reverse（後転）
0	1	0	H	L	Forward（前転）
0	1	1	L	L	Brake（停止）



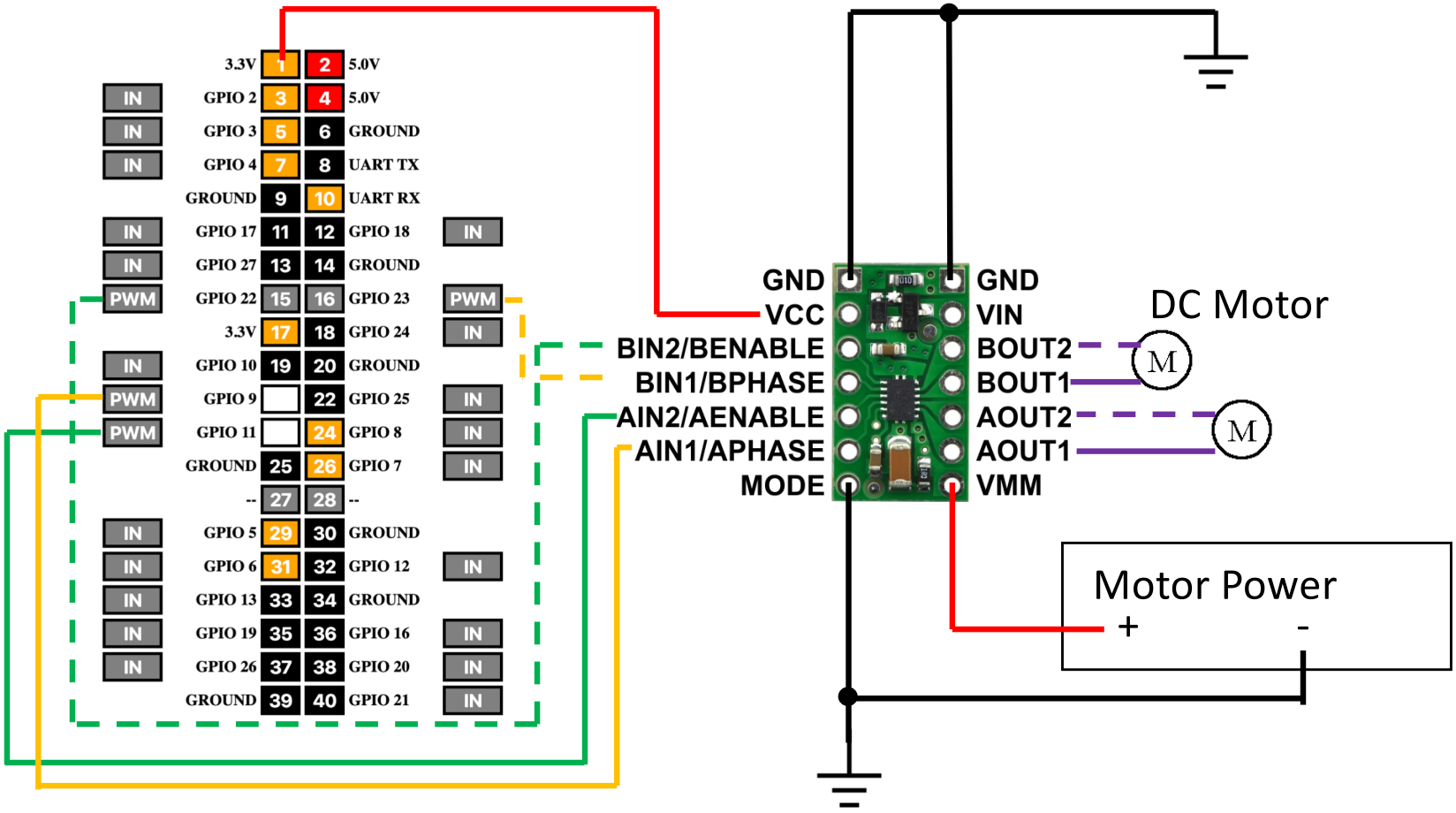
DRV8835



RasPiTankの外観

RasPiTankの設計

- タンク工作基本セットとデュアルモータドライバを左図のように配線した



RaspberryPi3とデュアルモータドライバの配線

IPv6環境に提案環境を構築するための検討

- IPv6環境においては，ND Proxy機能を利用する
  - ND Proxyを利用することでルータを介して通信が可能
    - ステートフルパケットインスペクション（IPv6ファイアウォール）
    - IPv6パケットフィルタリング機能

しかし，この環境を構築するためには

- ND Proxy機能を持つルータを準備する必要がある

NTMobileの経路最適化

- NATが以下の条件を満たせば経路最適化が可能

フィルタリング特性

外部端末からNAT宛てのパケットを受信したときのフィルタリングの方法を指す．

マッピング生成規則

NAT配下の端末からのパケットがNATを通過した際に，NATに生成されるマッピング生成規則のことを指す．

		フィルタリング特性		
		外部端末によらず通過	アドレス整合性をチェック	アドレス/ポート整合性をチェック
マッピング生成規則	外部端末によらず同一	Success	Success	Success
	アドレス単位	Failure		
	アドレス/ポート単位			