電気学会論文誌 C（電子・情報・システム部門誌）
IEEJ Transactions on Electronics, Information and Systems
Vol.137 No.12 pp.1571–1579　DOI: 10.1541/ieejeiss.137.1571

論　文

NTMobileにおける通信制御機能の提案と実装

非会員　金松　友哉*　非会員　大久保陽平**　非会員　山田　貴之**
非会員　鈴木　秀和**a)　非会員　内藤　克浩***　非会員　渡邊　晃**

A Proposal and Implementation of Communication Control Function for NTMobile

Yuya Kanematsu*, Non-member, Yohei Okubo**, Non-member, Takayuki Yamada**, Non-member,
Hidekazu Suzuki**a), Non-member, Katsuhiro Naito***, Non-member, Akira Watanabe**, Non-member

（2017年4月5日受付，2017年8月24日再受付）

NTMobile (Network Traversal with Mobility) has been proposed to achieve end-to-end encryption communication supporting IP mobility in environments where IPv4/IPv6 networks coexist. However, since NTMobile unconditionally establishes an encrypted UDP tunnel between NTMobile-ready nodes (NTM nodes), a malicious NTM node can attack a target NTM node through the encrypted UDP tunnel without being detected by a firewall. Moreover, since communication with a general server always passes through a relay server, the route becomes redundant even when IP mobility is not needed, and the communication delay increases. In order to solve these problems, this paper proposes an access control function using the name of the correspondent node and a "Route option" which can select whether the relay server is used or not. As a result of implemention of the prototype system and evaluation of its performance, it was confirmed that the increase of the start-up time and that of the overhead at the beginning of the communication were quite small, and there was little influence on practical use.

キーワード：仮想オーバレイネットワーク，IPv4/IPv6 混在環境，移動透過性，アクセス制御，経路選択
Keywords: Virtual Overlay Network, IPv4/IPv6 Networks, IP Mobility, Access Control, Route Selection

1. はじめに

スマートフォンなどのモバイル端末の急激な普及により，モバイルトラフィックが増加の一途を辿っている[(1)]。そのため，通信を 3G や LTE などのセルラー網から無線 LAN を経由した固定網へトラフィックを分散させるデータオフロードの取り組みが盛んになってきた。しかし，TCP/IP ネットワークでは通信回線やネットワークを切り替えると通信識別子である IP アドレスが変化するため，それまで行っていた通信が断絶してしまう課題がある。この課題を解決するために，様々な移動透過性技術が提案されている[(2)]。

一方，今日のインターネットは IPv4 グローバルアドレスの枯渇問題に伴い，NAT（Network Address Translation）を導入してプライベートネットワークを構築したり，IPv6 への移行が進められている。このような IPv4/IPv6 混在環境において移動透過性技術を実現する技術として，筆者らは NTMobile（Network Traversal with Mobility）を提案している[(3)~(5)]。

NTMobile ではネットワークの移動によって変化しない仮想 IPv4/IPv6 アドレスを端末に割り当て，通信開始時に端末間で暗号化された UDP トンネルを構築する。その後，アプリケーションは通信相手の仮想 IP アドレスを用いて通信を行うことにより，ネットワークの移動による実 IP アドレスの変化を隠蔽して通信を継続する。仮想 IP アドレスが送信元および宛先として指定された IP パケットは，構築された UDP トンネルを利用して伝送される。これにより IPv4 ネットワーク間に NAT が存在したり，IPv6 ネットワークが混在した環境においても，端末間で仮想的なエンドツーエンド通信を実現している。通信相手が NTMobile

a) Correspondence to: Hidekazu Suzuki. E-mail: hsuzuki@meijo-u.ac.jp
* 名城大学理工学部
Faculty of Science and Technology, Meijo University
Graduate School of Science and Technology, Meijo University
** 名城大学大学院理工学研究科
〒 468-8502　愛知県名古屋市天白区塩釜口 1-501
Graduate School of Science and Technology, Meijo University
1-501, Shiogamaguchi, Tenpaku-ku, Aichi 468-8502, Japan
*** 愛知工業大学情報科学部
〒 470-0392　愛知県豊田市八草町八千草 1247
Faculty of Information Science, Aichi Institute of Technology
1247, Yachigusa, Yakusa, Toyota, Aichi 470-0392, Japan

を実装していない一般のサーバである場合，端末は中継装置との間に UDP トンネルを構築し，仮想 IP パケットを送信する。中継装置は端末から受信したパケットをデカプセル化し，送信元/宛先仮想 IP アドレスを実 IP アドレスに変換して一般サーバへ転送する。そのため，通信開始側端末がネットワークを切り替えて IP アドレスが変化しても，一般サーバとの通信を継続することができる。

しかし，NTMobile では DNS による名前解決を検知すると，どのような通信相手であっても無条件で UDP トンネルを構築する。そのため，NTMobile を実装した端末間で UDP トンネルが構築されると，グローバルネットワーク側からプライベートネットワーク側へ自由に通信を開始できるため，悪意のあるユーザから暗号化された UDP トンネルを通じて攻撃を受ける可能性がある。また，セッションを維持する必要が無い Web サイトの閲覧や，常時トラフィックが発生せず移動透過性を必要としないサービスを提供する一般サーバと通信する場合であっても，NTMobile を実装した端末は必ず中継装置との間に UDP トンネルを構築して通信を行う。そのため，無駄に冗長な経路で通信を行うため，通信遅延の増加やスループットの低下，中継装置に不要なトラフィックを処理させることに伴う処理負荷の増加などの課題がある。

上記の課題を解決するため，本論文では通信開始時に通信相手の FQDN（Fully Qualified Domain Name）と中継装置の利用有無の情報から UDP トンネル構築の可否を判断する通信制御機能を提案する。端末に ACL（Access Control List）を導入し，通信相手の FQDN に基づいて UDP トンネルを構築するか否かを判断する。さらに，中継装置の利用有無の情報に基づいて，NTMobile を利用した移動透過性サポートの通信か，NTMobile を利用しない通常の通信かを動的に切り替える。提案方式を実装して ACL に基づくフィルタリング処理のオーバヘッド時間を計測することにより，実用上問題ないことを確認する。

以降，2 章で NTMobile の概要と課題を述べ，3 章で提案方式を示す。4 章で提案方式の実装と評価について説明し，5 章でまとめる。

2. NTMobile

〈2·1〉 概　　要　Fig. 1 に NTMobile の概要を示す。NTMobile システムは下記 3 種類の主要装置により構成される。

- NTM 端末：NTMobile を実装した端末。本論文では通信開始側 NTM 端末を MN（Mobile Node），通信相手側 NTM 端末を CN（Correspondent Node）と表記する。
- DC（Direction Coordinator）：NTM 端末のアドレス管理や仮想 IP アドレスの配布，トンネル構築処理の指示を行うサーバ。DNS サーバの機能も有しており，ドメイン単位で NTM 端末の情報を分散管理する。
- RS（Relay Server）：IPv4-IPv6 間のように NTM 端末がエンドツーエンドで通信できない場合に通信を中継するサーバ。この他，NTM 端末が NTMobile の機能を実装していない一般サーバ（以後，GS：General Server と表記）と通信する場合にも利用される。

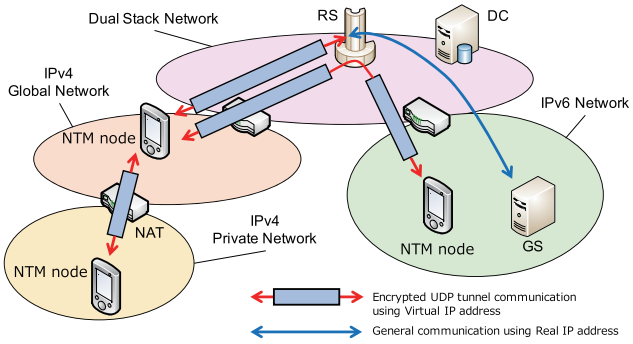


Fig. 1.　Overview of NTMobile.

NTM 端末は起動時に自身の FQDN と実 IP アドレスを DC に登録すると，DC は NTM 端末に仮想 IPv4/IPv6 アドレスを配付する。NTM 端末は NAT 配下のプライベートネットワークに存在する場合，DC との間で定期的に UDP による Keep Alive を実行し，DC からの制御メッセージを常時受信できる状態を維持する †。

NTM 端末が接続先ネットワークを切り替えた場合，実 IP アドレスが変化するため，DC に新しい実 IP アドレスを通知し，仮想 IP アドレスとのマッピング情報を更新する。これにより，NTM 端末の FQDN から現在割り当てられている実 IP アドレスおよび配付された仮想 IP アドレスの関係を検索することができる。

NTM 端末は一般的な通信と同様に，最初に DNS の仕組みにより通信相手端末の名前解決を行う。このとき，NTM 端末は DNS サーバへ送信する名前解決メッセージをトリガとして，下記に示すトンネル構築処理を実行する。

〈2·2〉 トンネル構築処理　NTMobile では UDP を用いた制御メッセージを NTM 端末，DC や RS 間で交換することにより，暗号化された UDP トンネルを構築する。暗号化された UDP トンネルとは，後述する仮想 IP アドレス宛の IP パケットを UDP/IP でカプセル化し，AES（Advanced Encryption Standard）による暗号化と MAC（Message Authentication Code）[7] が付与されたセキュアな通信路を意味している。以降，端末 N の FQDN を $FQDN_N$，端末 N のアドレス情報を管理している DC を DC_N と表記する。なお，通信の暗号化および認証に必要となる暗号鍵は端末間で交換されるが [8][9]，本論文では説明を省略する。

MN は A/AAAA レコードの問合せを検出すると，通信相手端末 N の $FQDN_N$ を記載した Direction Request を自身のアドレス情報が登録されている DC_{MN} へ送信して，ト

† UDP Keep Alive によるネットワークの輻輳を避けるため，オプションとして TCP Keep Alive を行う NS（Notification Server）が文献 (6) に定義されている。提案方式は TCP/UDP どちらの Keep Alive を利用しても適用可能であるため，本論文では仕様が簡素な UDP Keep Alive を利用した仕様に基づいて述べる。

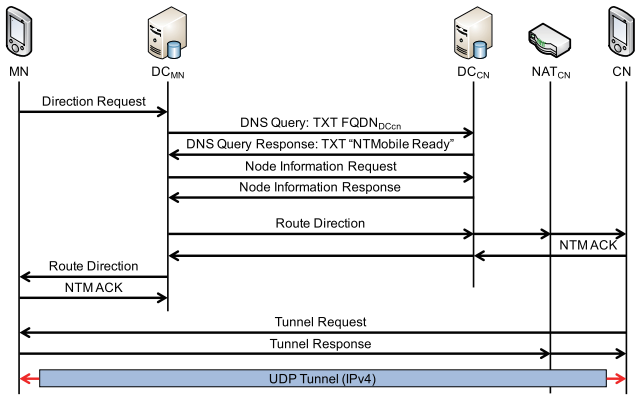


Fig. 2. Tunnel establishment sequence for CN.

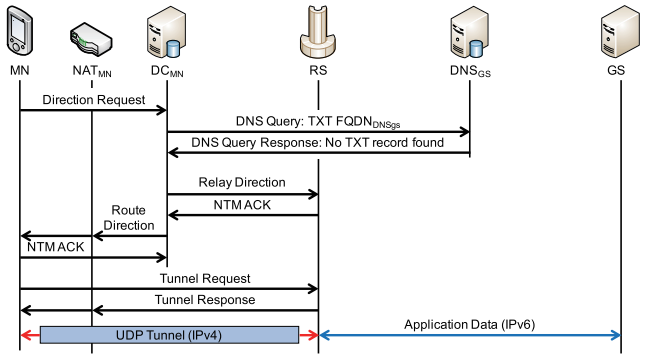


Fig. 3. Tunnel establishment sequence for GS.

ンネル構築指示を要求する。DC_{MN} は受信した Direction Request から $FQDN_N$ を取得し，NS レコードを問合せることでその名前を管理している DNS サーバを発見する。次に，その DNS サーバに対して TXT レコードを問合せ，その応答内容から DC なのか一般の DNS サーバなのかを判断する。これは通信相手端末 N が NTM 端末，GS のどちらの端末であるかを判断することと同義である。

これ以降，通信相手端末 N の違いによりトンネル構築シーケンスが異なるため，通信相手端末 N が NTM 端末，GS の場合について分けて説明する。

〈2·2·1〉 通信相手端末が NTM 端末の場合 Fig. 2 にグローバル IPv4 ネットワークに接続した MN がプライベート IPv4 ネットワークに存在する CN に対して通信を開始する際のトンネル構築シーケンスを示す。DC_{MN} は CN のアドレス情報[†] を取得するため，$FQDN_{CN}$ を記載した Node Information Request を DC_{CN} へ送信する。DC_{CN} は通知された $FQDN_{CN}$ を用いて自身のデータベースを検索し，取得した CN のアドレス情報を Node Information Response により返信する。これにより，DC_{MN} は自身で管理している MN のアドレス情報と受信した CN のアドレス情報から，どの経路で UDP トンネルを構築すればよいかを決定する。

Fig. 2 の場合，NAT 配下に存在する CN から MN に対してトンネル構築を行うため，DC_{MN} は通信相手のアドレス情報が記載された Route Direction により，CN に対してトンネル構築を指示する。なお，CN は NAT 配下に存在するため，CN と Keep Alive をしている DC_{CN} を経由して転送される。Route Direction を受信した CN はトンネル構築指示を受けた旨を NTM ACK により DC_{MN} へ応答し，DC_{MN} は MN に対しても Route Direction を送信し，CN からのトンネル構築処理を受け付けるよう指示する。CN は MN との間で Tunnel Request/Response を交換することにより，エンドツーエンドの UDP トンネルが構築される。

UDP トンネルが構築された後，MN は $FQDN_{CN}$ の名前解決の結果として CN の仮想 IPv4/IPv6 アドレスをアプリケーション側へ回答し，トンネル構築処理を完了する。

[†] CN の実 IP アドレス，仮想 IP アドレスの他，NAT のグローバル IP アドレスなどを含む。

以上により，MN のアプリケーションは CN 宛に送信するデータを CN の仮想 IP アドレス宛に送信することになる[††]。この仮想 IP アドレス宛の IP パケットは構築した暗号化 UDP トンネルを用いて CN まで転送され，CN においてデカプセル化された後，CN のアプリケーションまでデータが届けられる。

〈2·2·2〉 通信相手端末が GS の場合 Fig. 3 にプライベート IPv4 ネットワークに接続した MN が IPv6 ネットワークに存在する GS に対して通信を開始する際のトンネル構築シーケンスを示す。DC_{MN} は RS へ Relay Direction を送信し，MN からのトンネル構築処理を受け付けるよう指示する。RS からの応答を受信した後，DC_{MN} は MN へ Route Direction を送信し，RS に対してトンネル構築を指示する。このとき，DC_{MN} は自身で管理している未割当の仮想 IPv6 アドレスを GS の仮想 IPv6 アドレスとして MN と RS に通知する。

MN は RS との間で Tunnel Request/Response を交換することにより，MN と RS 間に UDP トンネルが構築される。UDP トンネルが構築された後，MN は $FQDN_{GS}$ の名前解決の結果として DC_{MN} から通知された仮想 IPv6 アドレスをアプリケーション側へ回答し，トンネル構築処理を完了する。

以上により，MN のアプリケーションは GS 宛に送信するデータを上記仮想 IPv6 アドレス宛に送信することになる。この仮想 IPv6 アドレス宛の IP パケットは構築した UDP トンネルを用いて RS まで転送され，RS においてデカプセル化される。さらに仮想 IPv6 パケットの送信元 IPv6 アドレスを NPTv6（IPv6-to-IPv6 Network Prefix Translation）[10] により RS の実 IPv6 アドレスに変換し，宛先 IPv6 アドレスを仮想 IPv6 アドレスから GS の実 IPv6 アドレスに変換してから，GS へパケットが転送される[†††]。

[††] アプリケーションが A レコードおよび AAAA レコードの応答して仮想 IPv4/IPv6 アドレスの両方を取得した場合，アプリケーションが IPv6 対応であれば優先的に仮想 IPv6 アドレスを用いて通信する。IPv6 非対応の場合，あるいはアプリケーションが IPv4 を使用する設計になっている場合は仮想 IPv4 アドレスを使用することになる。

[†††] GS が IPv4 ネットワークに存在する場合は，送信元 IPv4 アドレスとポート番号は NAT により RS の実 IPv4 アドレスと未使用のポート番号に変換される。

〈2·3〉 NTMobile における課題 NTMobile を導入することにより，端末はネットワークの違いや移動に伴う IP アドレスの変化を意識することなく，暗号化通信および移動透過性を実現することができる。しかし，以下に示すセキュリティ面および利便性に関して解決すべき 2 つの課題が残されている。

（1） NTM 端末は DNS 名前解決パケットを検知すると，無条件で通信相手側 NTM 端末との間に UDP トンネルを構築する。そのため，NTMobile を実装した悪意のある攻撃者はターゲットとなる NTM 端末の名前解決を行って暗号化 UDP トンネルを構築することにより，ネットワーク上のファイアウォールに検出されることなく攻撃を実行することができる。さらに，NTMobile により IPv4/IPv6 の違いや NAT の存在に関係なく通信できるため，NTM 端末はどのネットワークに存在しても常に攻撃を受ける可能性がある。

（2） NTM 端末は GS と通信する場合，必ず RS を中継する仕様になっている。しかし，GS がセッションを維持する必要がなく，通信が切断された際に再接続してもアプリケーションに影響がないサービス † を提供する場合，あるいは NTM 端末がデスクトップ PC のように移動することがない場合，移動透過性は必要ない。このような場合，NTM 端末は RS を経由して通信するメリットはなく，RS におけるトラフィックの集中を助長し，スループットの低下や通信遅延の増加が生じる。

3. 提案方式

〈3·1〉 概　　要 〈2·3〉の課題を解決するために，本論文では NTM 端末に通信相手端末に応じてトンネル構築を行うか否かを判断するアクセス制御機能と，ユーザが通信相手端末に応じて RS の利用有無を選択できる機能を通信制御機能として NTMobile に追加する。

Fig. 4 に提案方式における追加機能を示す。従来方式では DNS 名前解決処理をトリガーにトンネル構築処理を無条件で実施していたのに対し，提案方式では MN 側におけるトンネル構築処理を実行する前と，CN 側におけるトンネル構築処理の途中でアクセス制御を行う。この時点においては通信相手端末の IP アドレスを解決できていないため，通信相手端末を識別する情報としては FQDN しかない。そこで，NTM 端末に通信相手端末の FQDN と通信可否などのルールを記載した ACL（Access Control List）を実装し，ACL のルールに基づいてトンネル構築処理を行うか否かを決定する。また，ACL のルールに RS を経由しない設定を行うことにより，通信相手端末が GS の場合に NTMobile を利用しない通常の直接通信に切り替えることを実現する。

† 例えば，Google などの検索サービスやブログ等の WWW サーバや時刻同期を行う NTP（Network Time Protocol）サーバなど。

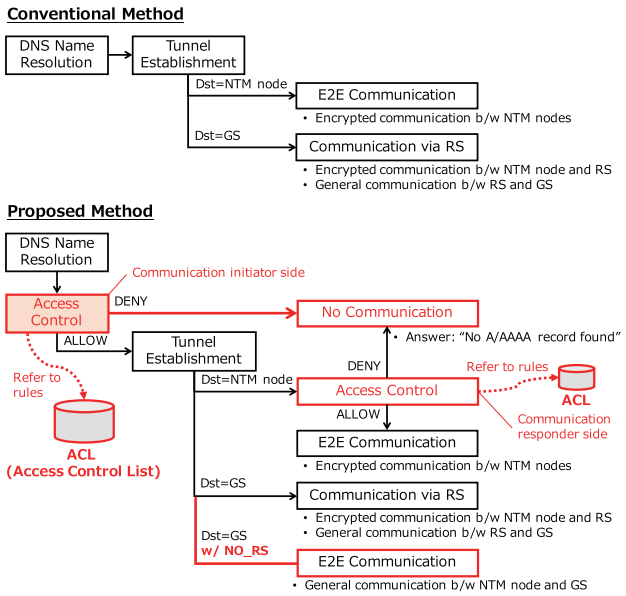


Fig. 4. Additional functions in the proposed method.

Black List

```
mallory.example.com  DENY
*.example.org        DENY
gs.example.com       ALLOW NO_RS

*                    ALLOW
```

White List

```
cn.example.com   ALLOW
*.example.org    ALLOW
gs.example.com   ALLOW NO_RS

*                DENY
```

Fig. 5. Example of Access Control List.

〈3·2〉 ACL に基づくアクセス制御 Fig. 5 に ACL の例を示す。ACL はブラックリスト方式およびホワイトリスト方式のどちらかに基づいてルールを記述する。FQDN の指定にはワイルドカード "*" を指定することも可能で，任意のサブドメインやホスト名を指定することができる。ブラックリスト方式では特定の端末との通信を拒否するルールを記述し，ルールの最後に " * ALLOW " を記述する。これにより，特定の端末以外との通信は全て許可する。一方，ホワイトリスト方式では特定の端末との通信のみを許可するルールを記述し，最後に " * DENY " を記述することにより，許可された端末以外との通信を全て拒否する。そのため，ユーザは用途や利便性に応じて，どちらかの方式に基づいて ACL を作成する。

NTM 端末に ACL を持たせ，FQDN によりフィルタリングすることによりアクセス制御を実現する。MN が DNS の名前解決パケットの送信を検知した際，通信相手端末の FQDN を取得し，ACL を検索する。$\mathrm{FQDN_N}$ に関するルールが ACL に存在し，通信が許可されていれば従来通りのトンネル構築処理を行う。一方，通信が拒否されている場合はトンネル構築処理を開始せず，A レコードおよび AAAA レコードが見つからない旨の DNS クエリ応答メッセージを作成してアプリケーションに返す。これにより，アプリケーションは通信相手端末の IP アドレスを取得することができないため，通信を開始することはできない。

MN と CN 間で通信する場合，MN 側だけでなく，CN 側でもアクセス制御を行う必要がある。そのため，CN に MN

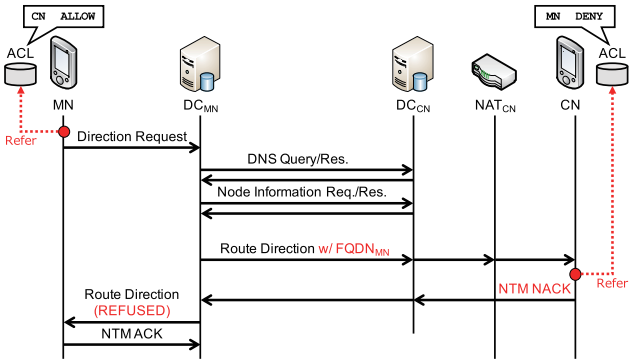


Fig. 6. Access control on CN in tunnel establishment sequence.

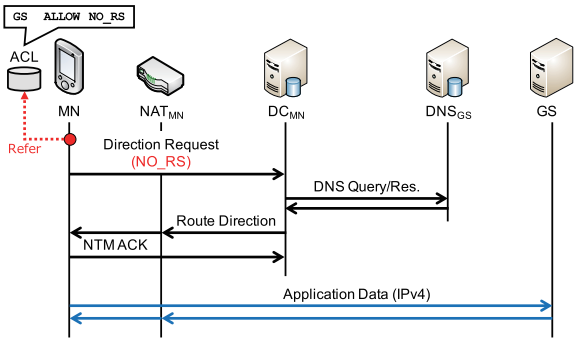


Fig. 7. Tunnel establishment sequence when RS is not relayed.

の FQDN を通知できるよう，Route Direction のメッセージフォーマットを拡張する。Fig. 6 に CN が MN との通信を拒否している場合のトンネル構築シーケンスを示す。CN が Route Direction を受信すると，FQDN$_{MN}$ を取得し，自身の ACL のルールと照合する。CN が MN との通信を拒否している場合は，NTM NACK を応答する。DC$_{MN}$ が NTM NACK を受信すると，CN 側でトンネル構築処理が拒否されたと判断し，MN 宛の Route Direction に REFUSED フラグを設定して送信する。このフラグが設定されている Route Direction を受信した MN はトンネル構築処理を終了し，A レコードおよび AAAA レコードが見つからない旨の DNS クエリ応答メッセージを作成してアプリケーションに返す。

なお，NTM 端末が ACL に基づくアクセス制御の機能を有効にしていない場合は，従来の NTMobile と同様の処理を行うため，NTM 端末のうちどちらか一方が通信を拒否する設定を行っていた場合のみ，通信が拒否される。

〈3·3〉 Route オプション GS との通信で RS を利用しない場合は，ACL における当該 GS に関するルールに “NO_RS” を指定するだけでよい。NTMobile では DC がトンネルをどの端末間で構築するかを決定するため，NTM 端末は RS を中継しない旨を DC に通知する必要がある。そこで，Direction Request のメッセージヘッダに Route オプションフラグ “NO_RS” を新たに定義する。

Fig. 7 に GS と通信する際に RS を利用しない場合のトンネル構築シーケンスを示す[†]。MN は “NO_RS” フラグを設定した Direction Request を送信し，DC$_{MN}$ が DNS$_{GS}$ に TXT レコードを問い合せる。DNS$_{GS}$ は NTMobile 非対応の一般 DNS サーバであるため，従来方式における DC$_{MN}$ は MN と RS の間にトンネルを構築しようとするが，提案方式では RS を中継しない旨の要求を受けているため，MN にトンネル構築処理を終了し，通常の DNS 処理を行うよう Route Direction で指示する。MN は通常の DNS 名前解決処理を実施して DNS$_{GS}$ から GS の実 IP アドレスを入手してアプリケーションに返す。これにより，MN は NTMobile を利用せず，直接 GS と通常の通信を行うことになる。

[†] MN と GS は共に IPv4 ネットワーク上に存在する場合の例である。

なお，通信相手端末が NTM 端末であり，ACL のルールに “NO_RS” が設定されていた場合，DC は Direction Request を受信しても下記の理由により Route オプションを無視し，従来通り RS を経由したトンネルを構築処理を行い，NTM 端末間を疎通させることを優先する。

- 異なるプライベート IPv4 ネットワーク間で通信する場合，NAT の種類によっては経路最適化 [11] を行うことができない。その場合はエンドツーエンド通信ではなく，必ず RS を中継しなければならない。
- IPv4 ネットワークと IPv6 ネットワークの間で通信する場合，必ず RS を中継しなければならない。

4. 実装と評価

〈4·1〉 実　装 NTMobile には NTM 端末を実現するために，カーネル実装モデル [5]，フレームワーク組込モデル [8]，VPN 利用モデル [12] が存在する。本論文ではフレームワーク組込モデルを利用して，Linux で動作する既存モジュールを拡張することにより提案方式を実装した。

フレームワーク組込モデルは，端末のアプリケーションに組み込むことにより，NTM 端末と同様の機能を実装することができる。以後，このアプリケーションを NTM アプリと呼称する。NTM アプリは起動時に DC へアドレス情報を登録したり，仮想 IP アドレスを割り当ててもらうなどの初期化処理を行う。そこで，この初期化時に今回追加したアクセス制御モジュールも初期化し，テキスト形式の設定ファイルとして定義したルールを読み込み，ハッシュテーブルとして実装した ACL に反映されるようにした。また，ユーザはフィルタリングルールを任意のタイミングで追加および削除して反映させることもできる。なお，ハッシュテーブルのサイズは既存のファイアウォール製品におけるホワイトリストやブラックリストの設定上限目安 [13]~[15] とほぼ同じ 512 とし，ハッシュ値が衝突した場合はチェイン法で処理するように設計した。

〈4·2〉 動作検証 プロトタイプ実装した NTM アプリを用いて，提案方式によるアクセス制御が正常に動作するか検証を行った。Fig. 8 に検証環境を，Table 1 に使用した PC の仕様を示す。大学研究室内に構築した 2 つの IPv4 プ

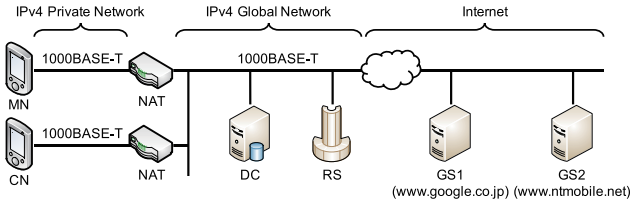


Fig. 8. Verification and measurement environment.

Table 1. Specification.

	MN, CN	DC, RS (Virtual Machine)
OS	Ubuntu 14.04	CentOS 6.8
Kernel	Linux 3.13	Linux 2.6.32
CPU	Intel Celeron N2820 2.16GHz	AMD Opteron 4180
Memory	4 GB	512 MB

Table 2. ACL used for operation verification.

Target FQDN	Action & Option
`*.google.co.jp`	`ALLOW NO_RS`
`*.google.com`	`ALLOW NO_RS`
`*.ucl.meijo-u.ac.jp`	`ALLOW`
`www.ntmobile.net`	`ALLOW`
`*`	`DENY`

ライベートネットワークおよびIPv4グローバルネットワークに，MNとCNおよびDCとRSをそれぞれ配置した†。MNとCNのアドレス情報は1台のDCで管理し，Googleおよび研究室管理のWWWサーバ（`www.ntmobile.net`）をそれぞれGS1，GS2として使用した。MNとCNのACLはホワイトリスト方式とし，Table 2に示す5つのフィルタリングルールを登録した。

以上の検証環境においてMNが各装置に通信開始した結果，通信相手端末がCNとGS2の場合はMNとCN間およびMNとRS間でNTMobileのトンネル構築処理が実行され，通信相手端末がGS1の場合はNTMobileのトンネル構築処理が行われず，MNは直接GS1との通信を開始した。また，本学のWWWサーバ（`www.meijo-u.ac.jp`）に対して通信を行った場合はIPアドレスを取得できず，通信できなかった。これらの結果より，提案方式における通信制御が正常に動作していることを確認した。

〈4·3〉 性能評価 提案方式の導入に伴い，通信開始時に行われるNTMobileのトンネル構築処理の度にACLに基づくフィルタリング処理が発生するため，アプリケーション通信に影響を及ぼす可能性が考えられる。そこで，提案方式が通信開始時に与える影響を明らかにするために，Fig. 8の環境において通信開始時におけるACLに基づくアクセス制御およびRouteオプションを用いた際のトンネル構築が終了するまでのオーバヘッド時間をそれぞれ計測した。また，MNにおける初期化処理についても計測した。さらに，比較のため従来方式の各処理についても同様の実験を行いオーバヘッド時間の測定を行った。オーバヘッド時間

† NTMobileに対応するこれら4台の装置のドメイン名には研究室のサブドメインである“`ucl.meijo-u.ac.jp`”が設定されている。

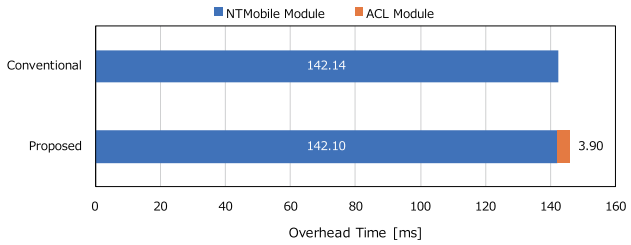


Fig. 9. Overhead of module initialization.

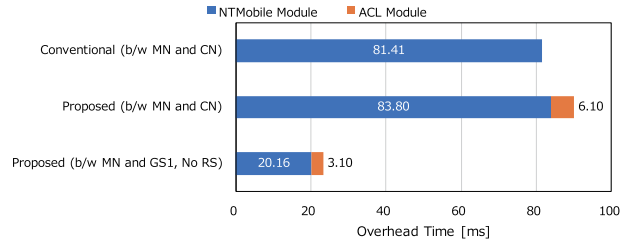


Fig. 10. Overhead of tunnel establishment process.

はNTMobileモジュールおよびACLモジュールにおける各処理の開始時と終了時の時刻を取得し，その差分を算出することにより求めた。なお，測定回数は10回であり，以下に示す結果はその平均値である。

〈4·3·1〉 端末起動時 Fig. 9に初期化処理に要した時間を示す。NTMobileモジュールの処理時間は，DCへのアドレス登録処理，仮想IPアドレスの配付処理などを含むものであり，従来方式と提案方式で変わりない。提案方式ではさらにACLモジュールの初期化処理が加わり，設定ファイルの読み込みからルールの設定までを含め，3.90 [ms]の処理時間を要した。従って，従来方式および提案方式における初期化処理は，それぞれ142.14 [ms]，146.00 [ms]であり，提案方式による増分は2.7%に過ぎない。

なお，登録するルール数に応じてACLモジュールの処理時間は増加する。今回の性能評価においてはルール1件当たりの平均登録時間が約0.71 [ms]だったため，ハッシュテーブルのハッシュ値が衝突しないと仮定すると，設定目安の上限にあたる500件のルールを追加する場合はおよそ350 [ms]程度のオーバヘッドになることが予想される。ただし，この処理はNTM端末起動時††に1回しか発生しないため，その後のアプリケーション利用時の通信には影響を及ぼさない。

〈4·3·2〉 通信開始時 Fig. 10にトンネル構築処理に要した時間を示す。MNとCN間の通信時に行うトンネル構築処理に着目すると，従来方式および提案方式のオーバヘッドはそれぞれ81.41 [ms]，89.90 [ms]であった。このうち，提案方式におけるACLに基づくアクセス制御処理のオーバヘッドは6.10 [ms]であった。文献(16)によると，ネットショップ利用者の47%がWebページの読み込み完了に期待する時間を2秒と回答しており，またページの描画に3秒を超えると40%のユーザが待つことを諦めてしま

†† フレームワーク組込モデルの場合は，NTMアプリ起動時に該当。

うことが報告されている。従って，従来の NTMobile に対して提案方式によるオーバヘッドは 10.4%程度増加するものの，通信開始時にのみ発生するオーバヘッドとしては極短時間であること，ならびに上記の調査結果を考慮すると，提案方式がアプリケーション通信に与える影響は極めて少なく，実用上問題ないと考えられる。

なお，ハッシュテーブルのハッシュ値が衝突しなければ，ルール数が増加しても上記オーバヘッドは変わらない。メモリ消費量は増加するが，ハッシュテーブルのサイズを拡大させることにより，衝突確率をさらに低下させることができるため，低いオーバヘッドを維持することができる。

また，Route オプションを用いて RS を経由しない通信経路とする場合，トンネル構築処理が終了するまでの処理時間は 23.26 [ms] であった。RS を経由しない場合，RS では Relay Direction 以降のトンネル構築処理や，その後の NTM 端末から受信したデカプセル化処理やアドレス変換処理を行わない為，従来方式と比較してトンネル構築処理時間が短縮されるだけでなく，RS の負荷および NTM 端末と GS 間の通信遅延の低下やスループットの向上などの効果が期待できる。

〈4･4〉 関連技術との比較　通信相手端末に応じて通信の可否を制御する関連技術として，ファイアウォールや IPsec [17] がある。〈2･3〉（1）の課題について，これらの技術による対策が可能かを考察する。

〈4･4･1〉 ファイアウォール　ファイアウォールは送信元/宛先の IP アドレスや FQDN，ポート番号などに基づいて IP パケットの通過や遮断を制御するソフトウェアである。例えば Linux に標準搭載されている iptables ではフィルタルールを指定する際に FQDN を利用できるが，ルールをカーネルモジュールに反映する際に名前解決が一度だけ行われ，最終的には FQDN に対応する IP アドレスがフィルタルールとして登録される。従って，実際の IP パケットをフィルタリングする際は，IP ヘッダに記載された IP アドレスをチェックすることになる。NTMobile では端末が移動することを想定しているため，端末が移動して IP アドレスが変化する度にルールを更新しなければならないが，ルールに追加した対象端末が移動したことを把握することは非常に困難である。

また，通常のファイアウォールは IP パケットのヘッダ部（IP および TCP/UDP ヘッダなど）を監視するため，DNS 問合せメッセージの中身を見て NTMobile のトンネル構築処理を行うか否かを判断することはできない。DNS 問合せメッセージの中身まで監視する方法として，DPI（Deep Packet Inspection）機能がある [18]。DPI 機能を用いれば，特定の通信相手端末に関する名前解決処理だけを遮断できると考えられる。DPI 機能は一般に高性能なルータなどに実装されるケースが多く，端末側にインストールされるパーソナルファイアウォールに必ずしも実装されているとは限らない。また，NTM 端末はネットワークを移動することを想定しているため，全ての移動先ネットワークのルータが DPI 機能を有していることは現実的でない。仮にそのようなルータが設置されていたとしても，管理者権限を持たない NTM 端末が移動先ネットワークに設置されているルータのフィルタリングルールを動的に設定することはできない。

上述の通り，端末が移動する状況下においてファイアウォールで特定の DNS 名前解決だけを遮断することは困難であるため，その後のトンネル構築を開始した際に MN から送信される Direction Request を遮断する方法が考えられる。Direction Request は通信相手 NTM 端末の違いに関わらず，必ず特定の DC に送信する。そのため，特定の NTM 端末に関するトンネル構築処理だけを DPI 機能無しのファイアウォールにより遮断することはできない。

一方，通信相手 NTM 端末と直接交換される Tunnel Request/Response を遮断することにより，特定の NTM 端末とのトンネル構築を遮断することは可能であると考えられる。ただし，提案方式の方が早期段階でトンネル構築処理を遮断することが可能なため，ネットワークに不要な制御メッセージを送信したり，DC などのサーバ群にも無駄な処理負荷は発生しないため，ファイアウォールで対処するより効率的である。さらに，通信相手が GS の場合，Tunnel Request/Response の交換相手が RS となるため，特定の GS との通信に関わるトンネル構築処理だけを限定して遮断することはできないため，ファイアウォールにより画一的な方法で制御することはできない。

これに対して，提案方式では FQDN を用いてアクセス制御を行うため，端末の移動に伴うアドレスの変化に影響されず，ACL のルールを継続して利用することができる。

〈4･4･2〉 IPsec　IPsec は IP 層におけるセキュリティアーキテクチャで，暗号技術を用いて IP パケットの暗号化や改ざん検知などを実現することができる。IPsec では暗号化やパケット廃棄などの処理をどの IP パケットに対して適用するかを決定するために，SPD（Security Policy Database）が定義されている。SPD に格納されているセキュリティポリシーを検索する際は，IP パケットの送信元/宛先 IP アドレスとポート番号，プロトコルの情報が利用される。

一方，NTMobile では DNS 名前解決パケットに含まれている通信相手端末の FQDN をキーとして，トンネル構築を制御する必要がある。従って，IPsec の仕組みを〈2･3〉（1）の課題を解決するためには利用できない。

〈4･5〉 ACL 設定の負担　提案方式によるアクセス制御を実施する場合，ユーザは ACL を設定するために設定ファイルにルールを記述する必要がある。Table 3 に関連技術と提案方式の設定項目の比較を示す。提案方式における設定ファイルは通信相手端末の FQDN と通信可否を示すキーワード（`ALLOW/DENY`）のみで，必要に応じて Route オプションを追加するだけである。ポート番号やプロトコル，送受信方向などの設定が必要なファイアウォールや，暗号化や認証アルゴリズム，事前共有鍵などの設定が必要な IPsec/IKE と比較すると，提案方式は携帯電話会社が提供している迷惑メールフィルタのサービスにおける受信拒否

Table 3. Comparison of setting items.

Firewall	Spam mail filter	IPsec/IKE	ACL (Proposed)
• IP address/FQDN • Port number • Protocol • Direction (In/Out) • Action (Accept/Drop)	• Mail address • Action (Allow/Deny)	• IP address • Action (Allow/Drop) • Encapsulation type (Transport/Tunnel) • Security protocol (AH/ESP/Both) • Authentication algorithm • Encryption algorithm • Diffie-Hellman group • Pre-shared key etc.	• FQDN • Action (Allow/Deny) • Route Option

するメールアドレスを設定する内容および作業と類似している[(19)~(21)]。従って，ネットワークやセキュリティに関する専門知識がない一般ユーザにとっても内容を把握しやすく，設定における煩雑さや負担は大きな問題にはならないと考えられる。

なお，ユーザにわかりやすい ACL ルール設定インタフェースを用意することにより，さらにユーザの設定作業を容易にすることができる。

〈4·6〉 セキュリティに関する考察

〈4·6·1〉 制御メッセージに対する改ざん攻撃 Fig. 6 や Fig. 7 で示したように，提案方式では制御メッセージに新たなフラグを導入した。攻撃者が強制的に Route Direction に `REFUSED` フラグを設定したり，Direction Request に `NO_RS` フラグを設定するなどの改ざんを行うと，当該 NTM 端末のトンネル構築処理が妨害され通信できなくなったり，RS を経由できずに移動透過性を満たした通信を行えない可能性が考えられる。NTMobile では NTM 端末，DC，RS 間で暗号鍵を共有しており，制御メッセージは MAC による改ざん検知が可能である。従って，提案方式で追加したフラグを利用した攻撃は成功せず，トンネル構築処理の妨害は生じない。

〈4·6·2〉 FQDN の変更によるアクセス制御の回避

攻撃者は自身の FQDN を変更することにより，ターゲットとなる NTM 端末の ACL に基づくアクセス制御を回避することが考えられる。NTMobile では，NTM 端末の FQDN を DC で重複が無いように管理している。そのため，DC の管理者は短期間に頻繁に FQDN を更新する NTM 端末を異常行動端末として特定することができる。また，攻撃を受けたユーザは攻撃者と思われる FQDN を DC の管理者に通報することにより，DC の管理者は FQDN の変更履歴から攻撃者を特定し，当該 NTM 端末アドレス情報を無効にすることができる。これにより，攻撃者が NTMobile のトンネル構築処理をできないようにする対策が可能である。

5. ま と め

本論文では，NTMobile における通信制御機能として，通信相手端末の FQDN を用いたアクセス制御機能と，RS の利用有無を選択可能な Route オプションを導入することを提案した。これにより，従来の NTMobile で課題となっていた暗号化された UDP トンネルを利用した悪意ある攻撃者からの攻撃を防止することができ，また移動透過性を必要としない一般サーバとの通信時に RS を経由しない最適な通信を実現することができた。

提案方式を既存の NTMobile モジュールに実装し，通信開始時に与える影響を明らかにするための性能測定を実施した。その結果，提案方式を導入した場合の端末起動時および通信開始時に発生するオーバヘッド時間の増分は極めて小さく，実用上問題ないことを確認した。

本論文では NTMobile におけるトンネル構築の制御を実現できたが，トンネル構築後の通信を制御するまでには至っていない。今後は提案方式を拡張することにより，トンネル構築後の仮想 IP アドレスに基づく通信を制御できるよう，更なる安全性向上を検討する。また，企業内での NTMobile の利用も想定し，多数の社員端末に ACL を設定するのではなく，DC に提案方式を適用することによりネットワーク側で通信制御したり，部門などのグループ単位で通信制御を行う方式も検討する。

文 献

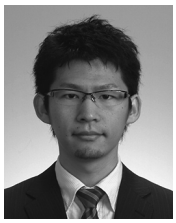
（1） Cisco Visual Networking Index: “Global Mobile Data Traffic Forecast Update, 2016-2021”, Cisco Systems (2017)
（2） 寺岡文男：「インターネットにおけるノード移動透過性プロトコル」，信学論 D，Vol.J87-D-I, No.3, pp.308–328 (2004)
（3） 鈴木秀和・上醉尾一真・水谷智大・西尾拓也・内藤克浩・渡邊 晃：「NTMobile における通信接続性の確立手法と実装」，情処学論，Vol.54, No.1, pp.367–379 (2013)
（4） 内藤克浩・上醉尾一真・西尾拓也・水谷智大・鈴木秀和・渡邊昇・森香津夫・小林英雄：「NTMobile における移動透過性の実現と実装」，情処学論，Vol.54, No.1, pp.380–393 (2013)
（5） 上醉尾一真・鈴木秀和・内藤克浩・渡邊 晃：「IPv4/IPv6 混在環境で移動透過性を実現する NTMobile の実装と評価」，情処学論，Vol.54, No.10, pp.2288–2299 (2013)
（6） 杉原史人・内藤克浩・鈴木秀和・渡邊 晃・森香津夫・小林英雄：「NTMobile における組み込み機器向けトラフィック削減手法の提案」，マルチメディア，分散協調とモバイルシンポジウム 2014 論文集，Vol.2014, pp.1313–1318 (2014)
（7） H. Krawczyk, M. Bellare, and R. Canetti: “HMAC: Keyed-Hashing for Message Authentication”, RFC 2104, IETF (1997)
（8） 納堂博史・杉原史人・鈴木秀和・内藤克浩・渡邊 晃：「NTMobile の実用化に向けた統合的枠組みの検討」，情処学研報，Vol.2015-MBL-77, No.20, pp.1–8 (2015)
（9） Y. Miyazaki, F. Sugihara, K. Naito, H. Suzuki, and A. Watanabe: “Certificate based key exchange scheme for encrypted communication in NTMobile networks”, Proc. of the 12th IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS 2015), No.RS8-5, pp.1–5 (2015)
（10） M. Wasserman and F. Baker: “IPv6-to-IPv6 Network Prefix Translation”, RFC 6296, IETF (2011)
（11） 納堂博史・鈴木秀和・内藤克浩・渡邊 晃：「NTMobile における自律的経路最適化の提案」，情処学論，Vol.54, No.1, pp.394–403 (2013)
（12） T. Yamada, H. Suzuki, K. Naito, and A. Watanabe: “IP Mobility Protocol Implementation Method Using VpnService for Android Devices”, Proc. of The 9th International Conference on Mobile Computing and Ubiquitous

Networking (ICMU 2016), Vol.2016, No.16, pp.1–2 (2016)
（13） NTT コミュニケーションズ：「Managed Firewall/Managed UTM – オブジェクト設定上限（目安）」，https://ecl.ntt.com/documents/tutorials/security/rsts/security/operation/managed_firewall_utm/8060_upper_limit_object.html
（14） マクニカネットワークス (株)：「Barracuda Email Security Gateway – よくあるご質問」，https://www.macnica.net/barracuda/faq.html/#024
（15） アライドテレシス (株)：「AR2050V/3050S/AR4050S リリースノート – サポートリミット一覧」，https://www.allied-telesis.co.jp/support/list/router/ar3050s_ar4050s/rel/5.4.6-0.1/613-002108_H/#SPC00218
（16） Akamai: “Akamai Reveals 2 Seconds As The New Threshold Of Acceptability For ECommerce Web Page Response Times”, https://www.akamai.com/us/en/about/news/press/2009-press/akamai-reveals-2-seconds-as-the-new-threshold-of-acceptability-for-ecommerce-web-page-response-times.jsp
（17） S. Kent and K. Seo: “Security Architecture for the Internet Protocol”, RFC 4301, IETF (2005)
（18） S. Dharmapurikar, P. Krishnamurthy, T.S. Sproull, and J.W. Lockwood: “Deep packet inspection using parallel bloom filters”, IEEE Micro, Vol.24, No.1, pp.52–61 (2004)
（19） NTT ドコモ：「指定受信/拒否設定」，https://www.nttdocomo.co.jp/info/spam_mail/spmode/domain/
（20） au：「迷惑メールフィルター設定」，https://www.au.com/support/service/mobile/trouble/forestalling/mail/
（21） SoftBank：「迷惑メールの個別設定をする」，http://www.softbank.jp/mobile/support/antispam/settings/indivisual/whiteblack/

金 松 友 哉（非会員） 1994 年生。2017 年 3 月名城大学理工学部情報工学科卒業。2017 年 4 月 NEC ネッツエスアイ (株) 入社。学士（工学）。情報処理学会会員。在学時代は主としてモバイルネットワークにおけるセキュリティに関する研究に従事。

大久保 陽 平（非会員） 1993 年生。2015 年 3 月名城大学理工学部情報工学科卒業。2017 年 3 月同大学大学院理工学研究科情報工学専攻修士課程修了。2017 年 4 月東海旅客鉄道 (株) に入社。修士（工学）。情報処理学会会員。在学時代は主としてモバイルネットワークにおけるハンドオーバに関する研究に従事。

山 田 貴 之（非会員） 1993 年生。2015 年 3 月名城大学理工学部情報工学科卒業。2017 年 3 月同大学大学院理工学研究科情報工学専攻修士課程修了。2017 年 4 月富士通 (株) に入社。修士（工学）。在学時代は主としてモビリティプロトコルに関する研究に従事。



鈴 木 秀 和（非会員） 1982 年生。2004 年 3 月名城大学理工学部情報科学科卒業。2009 年 3 月同大学大学院理工学研究科電気電子・情報・材料工学専攻博士後期課程修了。2008 年 4 月日本学術振興会特別研究員。2010 年 4 月名城大学理工学部助教。2015 年 4 月より同大学理工学部准教授および東北大学電気通信研究所共同研究員を兼任。博士（工学）。IEEE，ACM，WCTR，情報処理学会，電子情報通信学会各会員。主としてネットワークセキュリティ，モバイルネットワーク，ホームネットワーク等の研究に従事。

内 藤 克 浩（非会員） 1977 年生。1999 年 3 月慶應義塾大学理工学部電気工学科卒業。2004 年 3 月名古屋大学大学院工学研究科情報工学専攻博士課程後期課程修了。2004 年 4 月三重大学工学部電気電子工学科助手。2007 年 4 月同大学助教。2011 年 9 月カリフォルニア大学ロサンゼルス校客員研究員。2014 年 4 月愛知工業大学情報科学部准教授。2016 年情報処理学会・長尾真記念特別賞受賞。博士（工学）。IEEE，情報処理学会，電子情報通信学会各会員。主として無線ネットワーク，モバイルコンピューティングの研究に従事。

渡 邊 晃（非会員） 1951 年生。1974 年 3 月慶應義塾大学工学部電気工学科卒業。1976 年 3 月同大学大学院工学研究科修士課程修了。1976 年 4 月三菱電機株式会社に入社後，LAN システムの開発・設計に従事。1991 年 9 月同社情報技術総合研究所に移籍し，主としてルータ，ネットワークセキュリティ等の研究に従事。2002 年 4 月名城大学理工学部教授。博士（工学）。IEEE，情報処理学会，電子情報通信学会各会員。