FMIPv6における高速認証方式の提案と検証

山下 裕[†] 田中康之[†] 木村 徹[††,☆]
小野夏子[††,☆☆] 寺岡文男[†]

本論文では，FMIPv6において移動ノードとアクセスルータ間で高速に認証を行う方式の提案と検討を行う．FMIPv6はMobile IPv6を拡張し，移動探知とパケットのフォワーディングを行うことで高速移動時の遅延やパケット損失を削減するモビリティサポートプロトコルである．FMIPv6では，移動ノードとそのアクセスルータ（デフォルトルータ）との間，また移動前のアクセスルータと移動後のアクセスルータとの間で，制御パケットのやりとりを必要とする．そのため攻撃者のなりすましを防ぐ認証機構が不可欠である．そこで本論文では，認証機構としてIPsecと，鍵交換プロトコルであるIKEを利用したうえで，IPsec SAパラメータを移動前のアクセスルータから移動後のアクセスルータへFMIPv6自体の制御シーケンスを利用して転送することで，高速に認証が可能な方式を提案する．そして試験的な実装によりその動作を確認し，処理時間がわずかで済むことを示した．

Proposal and Verification of the Fast Authentication Method for FMIPv6

Yutaka Yamashita,[†] Yasuyuki Tanaka,[†] Toru Kimura,[††,☆]
Natsuko Ono[††,☆☆] and Fumio Teraoka[†]

In this paper, we propose and verify the method that achieves fast authentication between the mobile node and the access router with FMIPv6 protocol. FMIPv6 enhances Mobile IP. It detects movement of mobile nodes and forwards packets. Since it needs exchage of the control packets between the mobile node and the access router (default router) and between the previous access router and the new access router, the authentication mechanism that prevents attacker's disguise is indispensable. This paper proposes a fast authentication method using existing authentication protocols such as IPsec and IKE. This method transfers the parameters of the IPsec SAs from the previous access router to the new access router in the FMIPv6 sequence. We implemented a prototype and found that our method required negligible overhead.

1. はじめに

近年，無線によるネットワーク接続環境が充実してきたことにより，気軽にネットワークに接続し，インターネット通信を行うことが可能となっている．またコンピュータが小型化，高速化した影響もあって，コンピュータを容易に持ち歩くことも可能となっている．このように，様々な場所でインターネットに接続できる環境下で，VoIP（Voice over IP）アプリケーションや，モバイル端末にリアルタイム動画配信を行うアプリケーションを実現するためには，移動しても途切れることなくインターネット通信を行うことが必要となる．これを実現するためには，ノードが移動しても移動前に確立したセッションを維持し，通信を継続できる必要がある．次世代のIPプロトコルであるIPv6上で通信の継続を実現するプロトコルとしては，現在，Mobility Support in IPv6（MIPv6）[1]がRFCとして規定されている．しかしMIPv6では移動体が高速にサブネット間を移動する場合，ネットワーク移動時のアドレス解決と位置登録によって生じる遅延によりパケット損失が生じてしまう．Fast Handovers for Mobile IPv6（FMIPv6）[2]は，Mobile IPv6を拡張し移動探知とIPトンネルの生成を行うことでこの問

† 慶應義塾大学大学院理工学研究科
Graduate School of Science and Technology, Keio University
†† 日本テレコム株式会社研究開発本部情報通信研究所
Information and Communication Laboratories R&D Division Japan Telecom Co., Ltd.
☆ 現在，日本放送協会放送技術研究所ネットワークシステム
Presently with NHK Science & Technical Research Laboratories
☆☆ 現在，BBモバイル株式会社研究開発センター
Presently with R&D Center, BB Mobile Corp.

題を解決する．その際 FMIPv6 では，移動ノードとそのアクセスルータ（デフォルトルータ）との間，また移動前のアクセスルータと移動後のアクセスルータとの間で，制御パケットの交換を必要とする．そのため，制御パケットを保護し攻撃者のなりすましを防ぐ認証機構が不可欠である．しかし現段階では具体的な方法は提案されていない．

認証機構として IP 層でのセキュリティプロトコルである IPsec [3] と，鍵交換プロトコルである IKE [4] を使用するためには，認証を行うノード間で SA（Security Association）と呼ばれる論理的なコネクションを確立しておく必要がある．そして SA を確立するには，ノード間で暗号鍵や利用する暗号アルゴリズムの種類など，共通のパラメータを折衝しておく必要がある．このとき，アクセスルータ間の場合であれば，あらかじめ相手を把握可能で，事前に共通のパラメータを保持することは容易である．しかし次々に移動し，通信を行う相手が変わる移動ノードとアクセスルータの間では，事前に共通のパラメータを保持しておくことは困難である．そのため実際に IPsec を使用するには，移動のたびに共通パラメータの折衝を行わなければならない．その折衝にかかる待ち時間によって，移動を高速に行えないという問題が存在する．

本論文で提案する方式では，移動ノード（MN）が移動前に，その時点でのアクセスルータ（PAR）との間で確立している既存の SA を利用することで，MN と移動後のアクセスルータ（NAR）との間の SA を確立する．具体的には PAR から NAR に，MN と PAR 間で使用された SA パラメータを転送させ，そのパラメータを使用して MN と NAR 間の SA を確立する．これによって MN の移動後も，高速に MN と NAR 間で IPsec を利用したメッセージの送信元認証が可能となる．また，その SA 確立の際には FMIPv6 自体の制御シーケンスを利用することで，処理を高速に行う．本論文では，提案方式の検証を目的とし，SA パラメータの引き継ぎと FMIPv6 の制御シーケンスを利用した SA 確立の可否と優位性を検討した．

2. FMIPv6 の概要

MIPv6 では，比較的広域におけるあまり頻繁でない移動（マクロモビリティ）における通信の継続を目的としているため，高速道路上や電車内などで移動ノードが高速に次々とサブネット間を移動するような場合（マイクロモビリティ）では，以下にあげる 2 つの問題が生じる．1 つは，移動ノードの移動が頻繁に生じると，そのたびに位置登録のために制御パケットが必要

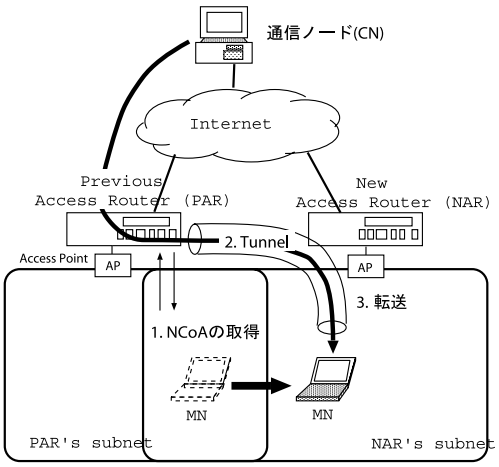


図 1 FMIPv6 ハンドオーバの例
Fig. 1 An example of the FMIPv6 handover.

となり，ネットワークの帯域を消費してしまう問題である．もう 1 つは，ネットワーク移動時の位置登録によって生じるハンドオーバの遅延によってパケットが損失する問題である．FMIPv6 は，データリンク層情報の利用と，トンネリングによって，ハンドオーバの遅延を短縮する高速ハンドオーバプロトコルである．**図 1** に代表的な動作モードである predictive モード時の FMIPv6 におけるハンドオーバのモデルを示す．

FMIPv6 では，図 1 に示したように，MN が Previous Access Router（PAR）から New Access Router（NAR）に移動する前に，移動後に使用する care-of address（NCoA）を取得し（1），PAR と MN 間でトンネルを生成することで（2），移動前に使用していた care-of address（PCoA）宛のパケットを移動後の MN に転送する（3）．移動後の MN に向けて転送されたパケットは，移動が完了するまで NAR でバッファリングされる．こうして本来は移動先で NCoA の設定にかかる時間による遅延と，位置登録である Binding Update が完了するまでにかかる時間による遅延が原因のパケット損失を削減する．

FMIPv6 のメッセージシーケンスは，まず MN はリンク層情報を利用して新しい基地局（AP）を検知すると，Router Solicitation for Proxy Advertisement（RtSolPr）を PAR に送信しその AP についての情報をリクエストする．すると PAR は MN に Proxy Router Advertisement（PrRtAdv）を送信し，その AP に対応した NAR についての情報（ネットワークプレフィックス，IP アドレスや MAC アドレス）を伝える．PrRtAdv の情報によって MN はハンドオーバ前に NCoA を生成することが可能となる．PrRtAdv

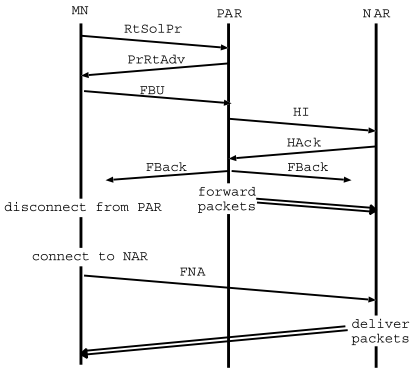


図 2 predictive モードのメッセージシーケンス
Fig. 2 Message sequence of predictive mode.

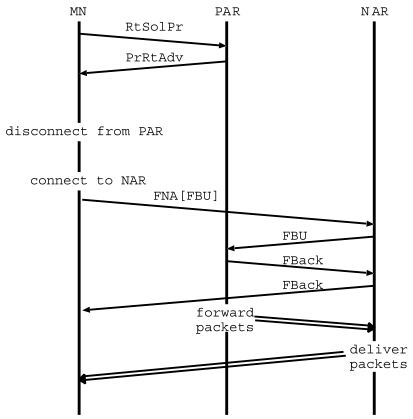


図 3 reactive モードのメッセージシーケンス
Fig. 3 Message sequence of reactive mode.

を受信した MN は，Fast Binding Update（FBU）を PAR に送信し，生成した NCoA を伝える．FBU を受信した PAR は，NAR に Handover Initiate（HI）を送信し，FBU に含まれた NCoA が実際に使用可能かを問い合わせる．HI を受信した NAR は，その NCoA の利用の可否や代替アドレスを Handover Acknowledge（HAck）として送信する．HAck を受信した PAR は，FBU に対する応答として Fast Binding Acknowledgment（FBack）を MN に送信する．

FMIPv6 では，MN がハンドオーバするタイミングによって predictive モードと reactive モードの 2 つのメッセージシーケンスが存在する．それぞれを**図 2** と**図 3** に示す．

predictive モードとは，MN が移動前に FBack の受信をした場合である．その場合，NAR のリンクに接続次第，アドレス設定にかかる遅延なく NCoA の使用が可能である．MN は NAR に接続すると，Fast Neighbor Advertisement（FNA）を送信することで接続を通知し，トンネリングによって PAR から NAR に転送されバッファリングされていた PCoA 宛のパケットを受信する．reactive モードとは，MN が RtSolPr を送信できず，PrRtAdv を受信できなかった場合や，FBU を移動前に送信できなかった場合，また，FBack を移動前に受信できなかった場合である．その場合，MN は NAR のリンクに接続次第 FBU を送信する．このとき FBU は FNA によってカプセル化されて送信される．

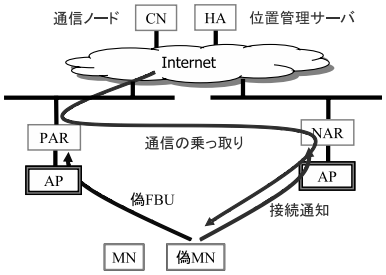


図 4 FBU の詐称
Fig. 4 Spoofing of FBU.

2.1 FMIPv6 のセキュリティ上の問題点

FMIPv6 での認証の必要性を考慮すると，まず MN と HA（Home Agent）間および MN と通信ノード（CN）間では，通常の MIPv6 と同様 Binding Update が正しい MN から送信されたものであるかを認証する必要がある．そして FMIPv6 特有である MN とアクセスルータ（AR）間の通信では，通信の乗っ取りや，不必要なトンネルの生成を防ぐために図 2 や図 3 でも示された FMIPv6 独自のメッセージを認証する必要がある．これらに対する認証方式として，MN と HA 間では IPsec と IKE を用い[5]，MN と CN 間では Return Routability[1] を用いることが規定されている．しかし，MN と AR 間では，FMIPv6 の仕様において，利用が可能であれば IPsec を利用すると規定されているだけであり，実際の IPsec の適用方法は規定されていない．MN と AR という通信相手が固定していない関係では，後述する IPsec の性質によって事実上認証は困難であり，MN と AR にはなりすましの危険性が存在する．

たとえば FBU が詐称された場合を考えると，**図 4** に示したように偽の MN が FBU を PAR に送信し，NAR において FNA を送信することで MN と CN で行われていた通信が乗っ取られてしまう．

3. IPsec と IKE

IPsec は暗号化や認証に使用するアルゴリズムを柔軟に選択することが可能な，強固なセキュリティプロ

トコルである．これを使用することによってデータの送信元の認証が可能である．しかし IPsec を利用するには，IPsec SA（Security Association）という単方向ごとの論理的なコネクションを確立する必要がある．そして IPsec SA を確立するには事前に通信を行う 2 者間で IPsec SA を識別するインデックス値（SPI 値）や暗号化やハッシュ化に使用するアルゴリズムの種類，それらのアルゴリズムで使用する秘密鍵など共通パラメータを折衝しておく必要がある．そのため不特定多数のノード間では適用が困難である．

IKE は 2 者間での IPsec SA パラメータの折衝を自動で行い，またそのパラメータのうちで，共有秘密鍵の更新（rekey）を自動で行うことを可能にするプロトコルである．しかし IKE ではまず ISAKMP SA と呼ばれる IPsec SA とは別の双方向の SA の確立が必要であり，事前の共通パラメータの設定が必要である．また IKE を用いて IPsec SA を確立するまでには 2 者間でまず ISAKMP SA を確立し，それを利用して IPsec SA を確立するため必要な手順が多く，処理時間が増加してしまう．

FMIPv6 の場合，MN は，ハンドオーバごとに接続する AP を次々と変更していく．それにともない AR も次々と変更していく．不特定多数の MN が全 AR との間で共通パラメータを保持するのは困難である．そのため IPsec の利用も困難である．IKE の利用についても，ハンドオーバごとに IPsec SA を確立するまでに多くのメッセージ手順を経る必要性があり，処理時間の関係で高速ハンドオーバの障害となる可能性がある．つまり通常の方法では，IPsec と IKE を FMIPv6 における MN と AR 間に適用することは困難である．

4. 提案方式

4.1 動作概要

本提案方式は，FMIPv6 において IPsec の利用が困難であるという問題を解決し，IPsec を用いた高速認証方式を実現するものである．これによって MN と AR のなりすましを防ぐことを可能とする．まず前提として，冒頭の MN と AR 間では，AAA（Authentication, Authorization, and Accounting）認証のような方法を利用することで共通パラメータを取得し，すでに SA（IPsec SA および ISAKMP SA）が確立しているものとする．また PAR と NAR 間は，IPsec による暗号化によって，盗聴などの危険性のない安全な経路とする．

動作概要としては**図 5** で示したように，MN と PAR 間および PAR と NAR 間ですでに確立済みの IPsec SA を利用し，その IPsec SA パラメータを PAR から NAR に転送する．また，その転送の際には FMIPv6 自体のメッセージシーケンスを利用する．そして転送したパラメータで MN と NAR 間の IPsec SA を確立する．これによって最小限の手順で IPsec SA を確立することが可能となる．

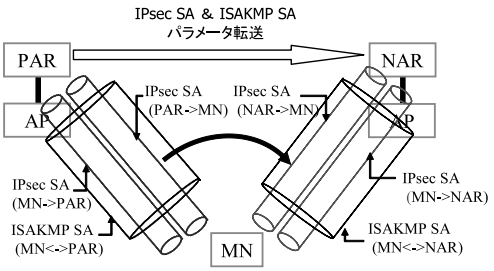


図 5 IPsec SA と ISAKMP SA パラメータの転送
Fig. 5 Transfer of the parameters of IPsec SA and ISAKMP SA.

また図 5 でも示したように，IPsec SA パラメータとともに ISAKMP SA パラメータも転送可能にする．これによって MN と NAR 間の ISAKMP SA を確立することが可能であり，ハンドオーバ後も即座に IKE を利用した IPsec SA の rekey が可能となる．

このとき，PAR から NAR に移動させるパラメータは**表 1** で示したものである．IPsec SA パラメータの中で，各パケットに付けられる順序番号であるシーケンス番号は移動させない．これは移動後のシーケンス番号を 0 に戻すことで，移動前後でのシーケンス番号の重複を避けるためである．

4.2 SPI 値の折衝

SPI 値とは IPsec SA パラメータの 1 つで，各 IPsec SA の識別に使われるインデックス値である．単純に MN と PAR 間で使用していた SPI 値を転送し，MN と NAR 間でも使用すると，**図 6** で示されるように，すでに NAR が同じ SPI 値を他の MN と使用している場合がある．IPsec SA は，SPI 値，宛先アドレス，使用 IPsec プロトコルの 3 つで識別されるため，提案方式では宛先アドレスと SPI 値がともに衝突しないように折衝を行う．実際には IPsec SA の受信側が SPI 値を決定し，送信側に伝えるようにする．

4.3 提案方式のメッセージとシーケンス

提案方式では，SPI 値が衝突しないように IPsec SA の受信側が値を設定する．そして既存の FMIPv6 メッセージを拡張し SA パラメータの転送を行う．またその FMIPv6 メッセージ自身も，IPsec が適用されるように IPsec SA を確立する．メッセージシーケンスと付加された内容，そして SA を確立するタイミン

表 1 移動させる SA パラメータ
Table 1 Security Association parameters to be migrated.

IPsec SA パラメータ	ISAKMP SA パラメータ
IPsec プロトコル（AH，ESP）	始動者クッキー
IPsec プロトコルモード（transport，tunnel）	応答者クッキー
ハード有効期間	認証方式（事前共有秘密鍵，公開鍵，デジタル署名）
ソフト有効期間	認証アルゴリズム
リプレイ防御機能の有無	暗号化アルゴリズム
リプレイウインドウのサイズ	SKEYID_d
シーケンスナンバーオーバフロー時の再利用の可否	SKEYID_e
認証アルゴリズム	SKEYID_a
認証用共有秘密鍵	有効期間タイプ
暗号アルゴリズム	有効期間
暗号化用共有秘密鍵	

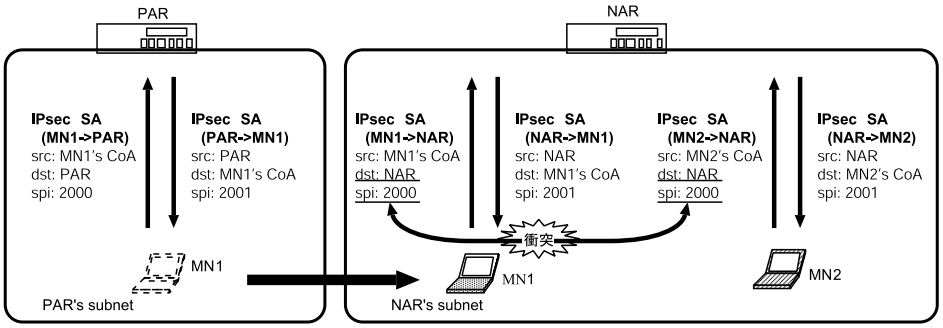


図 6 SPI 値の衝突
Fig. 6 Collision of the value of the SPI.

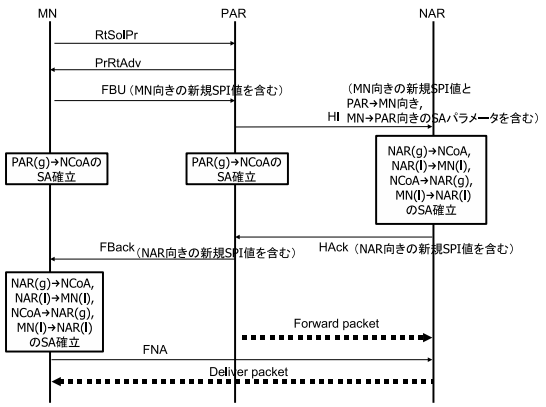


図 7 提案方式のシーケンス（predictive モード）
Fig. 7 Sequence of the proposed method (predictive mode).

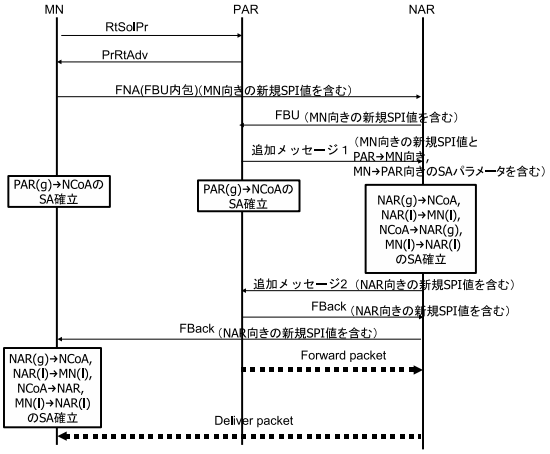


図 8 提案方式のシーケンス（reactive モード）
Fig. 8 Sequence of the proposed method (reactive mode).

グは，FMIPv6 のモードによって FMIPv6 に必要なメッセージの数やシーケンスが異なるため，モード別に**図 7** と**図 8** に示した．

predictive モードの場合 FNA は，FBU の後に PAR から NAR に転送されバッファリングされている PCoA 宛のパケットを，MN に送信開始するトリガの働きをする．そのため FNA にも認証が必要となる．そこで，MN が PAR から FBack メッセージを受信した時点で，MN と NAR との間で NCoA から NAR への向きの IPsec SA を確立する必要がある．そのため図 7 のようなシーケンスとなる．以下，ノード A からノード B 向きの IPsec SA を IPsec $SA_{A\to B}$ と表記する．またそのアドレスがリンクローカルアドレスの場合は A(l)，グローバルアドレスの場合は A(g) と表記す

る．RtSolPr と PrRtAdv は，リンクローカルアドレスを使用して通信を行う可能性があり，その他のメッセージではグローバルアドレスを使用して通信を行う．そのためすべてのメッセージの認証を可能とするために IPsec $SA_{MN(l)\rightarrow NAR(l)}$，IPsec $SA_{NCoA\rightarrow NAR(g)}$，IPsec $SA_{NAR(l)\rightarrow MN(l)}$，IPsec $SA_{NAR(g)\rightarrow NCoA}$ の 4 つと，さらに送信元アドレスが PAR(g) で宛先アドレスが NCoA である FBack のために，IPsec $SA_{PAR(g)\rightarrow NCoA}$ を確立する．MN の移動前に，これらの IPsec SA を MN と NAR において FMIPv6 メッセージ処理プロセス中に確立させる．これらの SA によって，NAR は MN からの FNA を認証することが可能となり，その後 MN がさらに別の AR のサブネットに移動する際も，その他の各 FMIPv6 メッセージの認証が IPsec によって可能となる．

reactive モードの場合，FNA は Neighbor Advertisement（NA）と同じ働きをする．そのため PCoA 宛のパケット転送のトリガは FNA にカプセル化された FBU であり，FBU が認証されればよい．そのため，図 8 のようなシーケンスとなる．predictive モードと異なる点として，MN は FBack を受信せずに NAR に接続すると，まず NAR に FNA を送信する．FNA は送信元アドレスが NCoA であり，宛先アドレスが NAR(g) であることから FNA に対応する IPsec SA は存在できず，NAR は FNA の認証はできない．しかし FNA によってカプセル化されていた FBU が，カプセル化を解除され NAR から PAR に転送される．そのとき，FBU は仕様上送信元アドレスが NCoA であり，送信先アドレスが PAR(g) であるが，Destination Options Header の Home Address Destination Option において PCoA を指定していることによって，受信する PAR は，確立済みの IPsec $SA_{PCoA\rightarrow PAR(g)}$ によって認証することができる[5]．また predictive モードで HI と HAck に追加して送信していた内容は，新規の追加メッセージとして送信する．

5. 実装と評価

5.1 実　　装

実装環境として，オペレーティングシステムは FreeBSD 5.1 Release を使用し，IKE デーモンは racoon[6] を用いた．今回は提案方式の検証を目的とするため，SA パラメータを含んだ FMIPv6 メッセージのシーケンスをエミュレートし，SA パラメータの転送と，そのパラメータによる IPsec SA の確立を行うデーモンを実装した．それによって SA パラメータ転送とそれによる IPsec SA 確立可否の確認を行った．

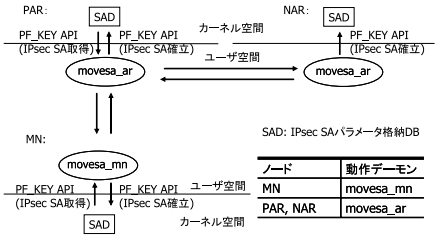


図 9 実装における各デーモンの動作
Fig. 9 Behavior of the daemons.

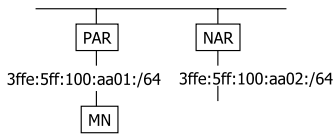


図 10 実験ネットワーク環境
Fig. 10 Experimental network environment.

表 2 実験ネットワーク環境（RTT）
Table 2 Experimental network environment (RTT).

場所	RTT（msec）
MN と PAR 間	0.32
MN と NAR 間	0.32
PAR と NAR 間	0.34

また同時にそのメッセージ自身に対しても IPsec が適用されていることも確認した．

実際に実装した各ホスト別のデーモンの動作モデルを**図 9** に示した．MN と AR，また AR どうしでは UDP を使用してメッセージの交換を行う．そしてカーネルとは PF_KEY API[7] を用いて，SA パラメータの取得や設定を行う．

評価を行った計算機環境としては MN，PAR，NAR すべてのマシンは，CPU が VIA C3 800 MHz，メモリが 500 MB で共通である．またネットワーク環境は**図 10** に示した．帯域はすべて 100 Mbps であり，各マシン間の RTT は**表 2** に示した．

5.2 セキュリティについての考察

IPsec SA のパラメータを引き継ぐ際のセキュリティ上の問題を考える．PAR と NAR 間で IPsec SA パラメータの送受信を行うことについては，PAR と NAR 間は IPsec によって暗号化された安全な経路が確立していることを前提としているため，方式上の問題は存在しない．次に，IPsec SA パラメータを移動後も使い続けることについては，そこに含まれる共有秘密鍵を使い続けることになり，共有秘密鍵の解読の可能性を高めてしまう問題が存在する．しかし提案方式では IPsec SA パラメータの有効期間の残りも同時に引き継ぐ．これによって最初に設定された有効期間が経過

表 3 提案方式による IPsec SA 確立の処理時間
Table 3 Processing time in establishing IPsec SAs with the proposed method.

ノード	処理時間（msec）
MN	6.9
NAR	1.4

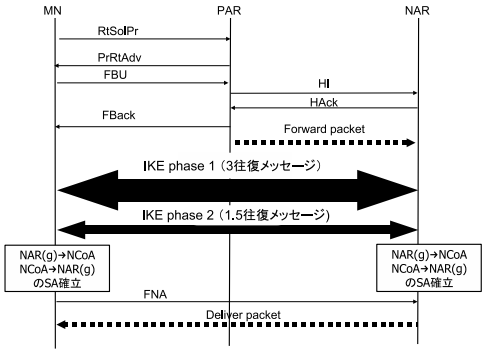


図 11 IKE 使用時の動作シーケンス（predictive モード）
Fig. 11 Sequence of IKE and FMIP messages (predictive mode).

表 4 IKE 使用時の IPsec SA 確立の処理時間
Table 4 Processing time in establishing IPsec SAs with IKE.

ノード	処理時間（msec）
MN と NAR ともに	1,127

すると，その IPsec SA は無効になる．これによって解読の危険性に対し最低限の安全性は確保している．

5.3 性能評価

predictive モードにおいて，MN と NAR との間でメッセージの認証を可能にすることで必要になった時間を，提案方式（メッセージシーケンスは図 7）を用いた場合（**表 3**）と既存の方式として IKE をそのまま用いた方式（メッセージシーケンスは**図 11**）の場合（**表 4**）とで比較した．

その結果，提案方式によって FMIPv6 シーケンス上で増加する処理時間（メッセージ内容の増加および SA の確立処理によって増える時間）は，IKE を用いた方式における MN の移動ごとに必要となる折衝の時間（IKE phase 1 と phase 2 に必要な時間）と比較して，大幅に少ないことが分かり，高速性が確認された．提案方式によるもの（表 3）において，MN と NAR で処理時間が異なるのは，MN においては RtSolPr 送信開始から FBack を受信し NAR との IPsec SA を確立するまでの間に提案方式によって増えた処理時間であり，NAR においては HI の受信完了から HAck の送信完了までの間に提案方式によって増えた処理時間を示しているためである．IKE を用いた方式では，

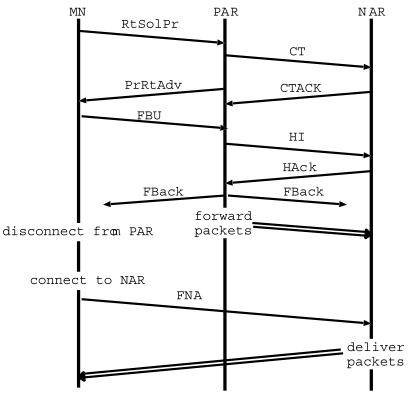


図 12 SAFMIP の動作シーケンス（predictive モード）
Fig. 12 Sequence of Security Association for FMIP messages (predictive mode).

確立させる SA それぞれにおいて phase 1 で 3 往復メッセージ，phase 2 で 1.5 往復メッセージという多くのメッセージが必要となることに加え，phase 1 における Diffie-Hellman 鍵交換が処理時間を大きなものとしている．

つまり IKE を用いた方式では，MN が移動するたびに SA 確立に多大の処理時間が必要となり，高速移動の阻害要因となる可能性が高いが，提案方式ではそのようなことにはならないと考えられる．

6. 関連研究

Security Association for FMIP Messages[8]（以下 SAFMIP と表記する）は，2004 年の 3 月に IETF で発表された方式である．MN と AR 間で IPsec による認証を行うために，FMIPv6 のメッセージシーケンス上で ISAKMP SA および IPsec SA を確立させるなどの点で提案方式と目的と手法が類似している．

提案方式との主な相違は，SAFMIP では Context Transfer Protocol[9] を利用して SA パラメータ転送用の新たなメッセージである Context Transfer（CT）と Context Transfer Acknowledgment（CTACK）を定義しそれだけを使用している点，また PAR が FBU の到達前に NAR になりうるすべての AR に対して CT メッセージを送信し，必要なパラメータを転送する点，IPsec SA パラメータ中の SPI 値の折衝は行わない点があげられる．SAFMIP におけるメッセージシーケンスを**図 12** に示す．

相違点による SAFMIP の利点としては，FMIPv6 のシーケンス初期に SA を確立可能で，predictive モード，reactive モードに限らず同じメッセージシーケンスである点があげられる．欠点としては，利点であげた要素を可能にするため，NAR になりうる全 AR に

CT メッセージを送信することによってトラフィックが増大する点，そして FBU によって NAR が決定され，HAck によって NCoA が決定されるという FMIPv6 の仕様から外れるため，NAR による NCoA の決定方法をあらかじめ規定しておく必要がある点，MN から NAR の向きの SPI 値を NAR がすでに使用中の場合，値の衝突が生じる危険性が存在する点があげられる．概して提案方式が FMIPv6 の仕様に準拠することを重視しているのに対し，SAFMIP では SA を確立するまでの手順の簡潔性を重視しているといえる．

7. ま と め

本論文では，FMIPv6 における移動ノードとアクセスルータ間での認証に対し，IPsec を用いて認証可能な方式を提案した．この方式では既存の IPsec SA を利用することで新たな IPsec SA を確立する．そのため FMIPv6 において移動ノードがハンドオーバを繰り返しても高速に移動ノードとアクセスルータ間で IPsec による認証が可能となる．

本論文では，提案方式によって実際に既存の IPsec SA パラメータを利用し新たな IPsec SA を確立することが可能であるかを検証し，さらに必要となる処理時間の検討を行った．そしてその通信をモニタし，IKE を通常利用した場合と処理時間を比較することで提案方式の妥当性と高速性を示した．

今後の課題は，実際に FMIPv6 に提案方式を適用することである．さらに本論文では SA のみに注目しており，セキュリティポリシについては考慮していない．今回はすべてのノードが共通のセキュリティポリシを用いるという前提としたが，実際には SA とともにセキュリティポシリも動的に設定する方式が必要である．

参 考 文 献

1) Johnson, D.B., Perkins, C.E. and Arkko, J.: Mobility Support in IPv6, RFC 3775 (2004).
2) Koodli, R.: Fast handovers for Mobile IPv6, RFC 4068 (2005).
3) Kent, S. and Atkinson, R.: Security Architecture for the Internet Protocol, RFC 2401 (1998).
4) Harkins, D. and Carrel, D.: The Internet Key Exchange (IKE), RFC 2409 (1998).
5) Arkko, J., Devarapalli, V. and Dupont, F.: Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents, RFC 3776 (2004).
6) KAME Project: racoon. http://www.kame.net/racoon/
7) McDonald, D.L., Metz, C. and Phan, B.G.: PF_KEY Key Management API, Version 2, RFC 2367 (1998).
8) Ogawa, T., Ohnishi, H. and Yoshitake, H.: Security Association for FMIP Messages, Internet draft, IETF (2004). (work in progress).
9) Koodli, R., Loughney, J., Nakhjiri, M.F. and Perkins, C.E.: Context Transfer Protocol, Internet draft, IETF (2004). (work in progress).

付 録

A.1 略 号 一 覧

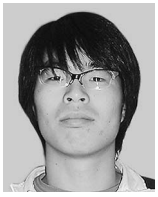
- MIP6: Mobility Support in IPv6（Mobile IPv6）
- FMIPv6: Fast Handovers for Mobile IPv6
- IPsec: Security Architecture for the Internet Protocol
- IKE: Internet Key Exchange
- SA: Security Association
- MN: Mobile Node
  移動ノード
- AR: Access Router
  MN が接続するルータ
- PAR: Previous Access Router
  MN が移動前に接続していたアクセスルータ
- NAR: Next Access Router
  MN が移動後に接続するアクセルルータ
- CoA: Care-of Address
- PCoA: Previous Care-of Address
  MN が移動前に使用していた CoA
- NCoA: Next Care-of Address
  MN が移動後に使用する CoA
- AP: Access Point
  無線基地局
- RtSolPr: Router Solicitation for Proxy Advertisement
- PrRtAdv: Proxy Router Advertisement
- FBU: Fast Binding Update
- HI: Handover Initiate
- HAck: Handover Acknowledge
- FBack: Fast Binding Acknowledgement
- FNA: Fast Neighbor Advertisement
- HA: Home Agent
  位置管理ノード
- CN: Correspondent Node
  通信ノード

- SPI: Security Parameter Index
  IPsec SA を識別するインデックス
- AAA: Authentication, Authorization, and Accounting
- NA: Neighbor Advertisement
- CT: Context Transfer
- CTACK: Context Transfer Acknowledgement

(平成 17 年 2 月 1 日受付)
(平成 17 年 7 月 4 日採録)

山下　裕

1980 年生．2004 年慶應義塾大学理工学部情報工学科卒業．現在，同大学大学院理工学研究科前期博士課程に在学中．移動体通信を考慮した認証方式や鍵交換に興味を持ち，主な研究テーマとしている．



田中　康之

1980 年生．2003 年慶應義塾大学理工学部情報工学科卒業．2005 年同大学大学院理工学研究科前期博士課程修了．エンドホストにおけるルーティング機構に興味を持つ．

木村　徹

1996 年京都工芸繊維大学工芸学部電子情報工学科卒業．同年日本テレコム（株）入社．1998 年東京大学工学部委託研究員．1999 年日本テレコム（株）情報通信研究所に配属．ネットワークセキュリティおよび次世代移動通信における IP モビリティの研究に従事．2004 年 NHK 放送技術研究所．通信ネットワーク利用放送の研究に従事．電子情報通信学会所属．

小野　夏子

1999 年早稲田大学理工学部情報学科卒業．2001 年同大学大学院理工学研究科博士前期課程修了．同年日本テレコム（株）入社．2004 年 BB モバイル（株）出向，現在に至る．次世代移動通信における IP モビリティの研究に従事．電子情報通信学会所属．

寺岡　文男（正会員）

慶應義塾大学理工学部情報工学科教授．1959 年生．1984 年慶應義塾大学大学院工学研究科電気工学専攻修士課程修了．同年キヤノン株式会社入社．1988 年株式会社ソニーコンピュータサイエンス研究所入社．2001 年 4 月から現職．博士（工学）．1991 年日本ソフトウェア科学会高橋奨励賞受賞．1993 年元岡記念賞受賞．2001 年情報処理学会平成 12 年度論文賞受賞．コンピュータネットワーク，オペレーティングシステム，分散システム等の研究に従事．特に移動透過性を保証するプロトコル VIP（Virtual IP）の開発を通して IETF の Mobile IP 分科会の活動に貢献．2000 年 5 月から 2002 年 5 月まで情報処理学会理事．2005 年 4 月から日本ソフトウェア科学会理事．著書に『ワイヤレス LAN アーキテクチャ』(共著，共立出版)，『Wireless IP and Building the Mobile Internet』(共著，Artech House Publishers)．監訳に『詳細 Mobile IP』(共監訳，プレンティスホール出版)．ACM，IEEE，日本ソフトウェア科学会，電子情報通信学会各会員．