

ワイヤレスネットワークシステムにおける シームレスユーザ認証方法に関する考察

朴 美 娘[†] 岡 崎 直 宣^{††} 馬 場 義 昌[†]

ユビキタスネットワークを確立する際のアクセス網として高速無線 LAN が注目を集めている。しかし、WLAN には個人のプライバシーを十分保護し安全な情報交換を保証できるセキュリティ・ソリューションが非常に重要な課題となっており、より強力なセキュリティ機能と厳密な認証方式が求められている。また、つねに移動する WLAN 環境で高品質のアプリケーションを提供するために、ハンドオフ遅延やパケットロスの性能を改善できるシームレス高速ユーザ認証方式が求められている。本研究では、よりシームレスなサービスを提供するために IP レイヤハンドオフ遅延を改善できるユーザ認証方式について検討する。そこで、WLAN におけるユーザーローミングを支援するために Mobile IPv6 を導入し、Mobile IPv6 環境下で頻繁に移動する端末の高速ハンドオフを可能とした拡張プロトコルの FMIPv6 を適用する。また、認証処理の高速化のため移動端末ユーザがサービス加入時に認証サーバ (AS: Authentication Server) との共有鍵を事前に配布する事前共有鍵に基づいた WLAN ユーザ認証フレームワークを提案する。さらに、WLAN システムの大規模化にともなう認証サーバへのトラフィック集中を分散し、移動端末のスケーラビリティ問題を解決するためにアクセスルータ (AR: Access Router) を導入する。さらに、つねに移動する移動端末の認証情報は AR で管理できるように分離し、FMIPv6 による AR 間の IP トンネルを用いて認証情報を転送し、事前認証を行うことにより遅延の少ない新しい AP へのセキュア・アソシエーション確立が高速にできるシームレスユーザ認証プロトコルを提案する。

A Study of a Seamless User Authentication Protocol on Wireless LAN Systems

MIRANG PARK,[†] NAONOBU OKAZAKI^{††} and YOSHIMASA BABA[†]

Rapid deployment of wireless technology has led to rapid growth of high-speed wireless LAN (WLAN). For constructing a ubiquitous network, the high-speed WLAN attracts attention as an infrastructure for global access. However, some issues are impeding further adoption of the technology, in particular, security problems including user authentication, message compromising, connection hijacking and handoff problems of moving users. In this paper, we discuss a seamless user authentication method of mobile terminals in WLAN. To achieve a fast IP layer handoff between Access Points (APs) and mobile terminals and sharing of a session key between users, we propose a seamless pre-authentication and key distribution protocol based on cached Pre-Shared Keys and FMIPv6 messages.

1. はじめに

現在、ユビキタスネットワークを確立する際のアクセス網として飛躍的な発展を続けている高速無線 LAN (WLAN) が注目を集めている。しかし、WLAN には人間がネットワークを意識しないような環境で情報を送受、蓄積し、必要なときにそれらの情報を利

用できるという特性上、個人のプライバシーを十分保護し、安全な情報交換を保証できるセキュリティのソリューションが非常に重要な課題となる¹⁾。そこで、無線 LAN 規格の拡張検討および標準化作業を行っている IEEE 802.11 委員会では無線 LAN におけるセキュリティ問題を議論するためにタスクグループ i (TG*i*) を設置した。ここでは、主に無線区間のデータ暗号化方式 WEP (Wired Equivalent Privacy) の強化策と、IEEE 802.1X/EAP (Extensible Authentication Protocol)^{2),3)} に基づいたモバイル端末 (MS: Mobile Station) の様々な認証方式^{4)~6)} について議論し、規格として IEEE 802.11i⁷⁾ を策定した。しかし、IEEE

[†] 三菱電機株式会社情報技術総合研究所
Information Technology R&D Center, Mitsubishi Electric Corporation

^{††} 宮崎大学工学部
Faculty of Engineering, University of Miyazaki

802.1X を WLAN に適用する際のセキュリティホールが報告⁸⁾されており、より強力なセキュリティ機能と厳密な認証方式が求められている⁹⁾。また、文献 10) では IEEE 802.11i におけるセキュリティ脅威問題を解決するための解析も行っている。

一方、移動通信ネットワークではつねに移動するモバイル端末ユーザのローミング問題も重要な課題となっている。たとえば、WLAN における MS があるアクセスポイント (AP: Access Point) から他の AP に移動する場合、MS は新しい AP に再接続するためにハンドオフが必要である。すなわち、AP との 802.11 無線リンク接続のための処理、新しい AP での MS の認証のための再認証処理、さらに IP サブネットが変わったときの IP connectivity のための IP レイヤの処理が必要になる。したがって、多くのメッセージ交換による遅延が生じ、通信の中断が起きる可能性があり、シームレスサービスを提供できない問題がある。このような通信の中断の問題は、ボイスオーバー IP (VoIP) やストリーミングのような滑らかな動作およびサービス品質 (QoS) を保証しなければならないリアルタイムアプリケーションにとっては大きな問題となる。したがって、WLAN 環境で高品質のアプリケーションを提供するために、ハンドオフ遅延やパケットロスの性能を改善できるシームレス高速ユーザ認証方式が求められている。

現在 WLAN ローミング問題に関して IEEE 802.11r¹¹⁾ で仕様検討を行っている。ここでは、MS の移動を同一の拡張サービスセット (ESS: Extended Service Set) 内だけに限定しており、移動前 AP と移動後 AP の通信範囲が重なっている場合を対象とするので物理・MAC レイヤ接続にともなう 802.11 ハンドオフ遅延はほとんど影響がない。したがって、MS 再認証処理の遅延を改善するために認証時間の短縮やプロトコルの高速化のアプローチを行っている。

一方、WLAN ハンドオフ処理において時間が一番長くなるのは、IP connectivity 処理のための IP レイヤハンドオフになる¹²⁾。本研究では、よりシームレスなサービスを提供するために IP レイヤハンドオフ遅延を改善できるユーザ認証方式について検討する。そこで、WLAN におけるユーザローミングを支援するために Mobile IPv6 を導入し、Mobile IPv6 環境下で頻繁に移動する端末の高速ハンドオフを可能とした拡張プロトコルの FMIPv6¹⁴⁾ を適用する。また MS 認証処理の高速化のため、MS がサービス加入時に認証サーバ (AS: Authentication Server) との共有鍵を事前に配布する事前共有鍵に基づいた認証方式を導入する。

さらに、WLAN システムの大規模化にともなう認証サーバへのトラフィック集中を分散し、移動端末のスケーラビリティ問題を解決するために、AS が AP をスケーラブルな方法で扱うことができる認証方式の確立について検討する。そこで、AP を管理するためのアクセスルータ (AR: Access Router) を導入し、AR だけで AS にアクセス可能とする WLAN ユーザ認証フレームワークを提案する。さらに、つねに移動する MS の認証情報は AR で管理できるように分離し、FMIPv6 による AR 間の IP トンネルを用いて認証情報を転送し、事前認証を行うことにより遅延の少ない新しい AP へのセキュア・アソシエーション確立を高速に行うことができるシームレスユーザ認証プロトコルを提案する。

以下、2 章で現在 WLAN でのユーザ認証に主に使われている IEEE 802.11i の概要と課題について述べた後、3 章で FMIPv6 による移動端末の事前認証とシームレスユーザ認証プロトコルを提案する。そして、4 章で提案方式の評価を行い、最後に 5 章でまとめる。

2. 既存技術と課題

2.1 IEEE 802.11i

現在 WLAN でデータ暗号に使用されている WEP 暗号アルゴリズムにおける WEP キーは AP ごとに定められているので、その AP につながっている MS だけでは秘匿性がない。したがって、WLAN でデータの秘匿性を守るために認証と鍵共有メカニズムは分離する必要がある。IEEE 802.11 のタスクグループ i (TGi) では、WEP の強化策として IEEE 802.1X/EAP^{2),3)} に基づいたモバイル端末認証方式について議論し、規格として IEEE 802.11i⁷⁾ を規定している。IEEE 802.11i では、WEP に加えて RSNA (Robust Security Network Association) を定義している。ここでは、データの暗号化と安全性を保証するために WEP キーを動的に変更できる TKIP (Temporal Key Integrity Protocol) と AES を利用する CCMP (Counter mode with CBC-MAC Protocol) を策定した。さらに、AP が RADIUS のような AS と連携しながら MS の認証を行い、MS と AP 間のデータ暗号化のための暗号鍵を確立するための手順を図 1 のように定義している。以下、各手順について述べる。

【Step1】MS⇔AP 間の 802.11 無線リンク接続フェーズ

MS が無線リンク接続可能な AP を発見し、802.11 無線リンク接続を行う。接続にあたっては、認証要求

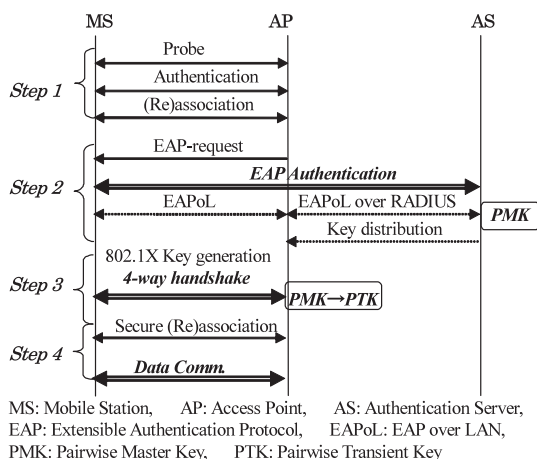


図1 IEEE 802.11iにおける認証・鍵共有手順

Fig.1 IEEE 802.11i RSNA establishment procedures.

パケットに対してつねに認証許可を行う 802.11 オープンシステム認証 (null 認証) を行う。ここで、MS と AP は後ほど使う認証方法と暗号化アルゴリズムのネゴシエーションを行う。

【Step2】MS⇔AS 間の 802.1X /EAP 認証フェーズ

IEEE 802.1X²⁾ により MS と AS 間で相互認証を行う。ここでは認証方式に依存しない拡張認証プロトコル EAP³⁾ を利用することを規定している。認証が成功すると MS と AS 間で共通のマスタ鍵 (PMK: Pairwise Master Key) が生成され、AS はその鍵を AP に配布する。しかし、この PMK は AP と MS の組に固有のものであるため、MS が AP を移動する場合は再度 802.1X 認証を実施する必要がある。

【Step3】MS⇔AP 間の鍵生成フェーズ

認証が成功すると 4 ウェイハンドシェイクと呼ばれるプロトコルにより、データの秘匿、完全性のための新たなセッション鍵 (PTK: Pairwise Transient Key) を生成する。PTK は MS と AP 間で共有されていた PMK および MS と AP が互いに交換する乱数 (ノンス) を用いて生成される。なお、マルチキャストアプリケーションに適用するためのグループ鍵 (GTK: Group Transient Key) が生成される場合もある。

【Step4】MS⇔AP 間のデータ暗号通信開始

AP と新しい共有鍵を確立した MS は DHCP などによって IP アドレスを取得する。そして、PTK を用いて AP と MS 間のデータ暗号化を行う。暗号化通信プロトコルとしては、TKIP や CCMP を用いる。

□

2.2 WLAN システムにおける IEEE 802.11i の課題

上記の IEEE 802.11i を WLAN システムに適用す

る際には、いくつかの課題をかかえているのが現状である。ここでは、セキュリティ問題、ハンドオフ遅延問題、スケーラビリティ問題について考察する。

(1) セキュリティ脅威問題

IEEE 802.11i では従来の WLAN のセキュリティ脅威問題を解決するために 802.1X/EAP をもとに鍵交換のための 4 ウェイハンドシェイクプロトコルを追加して策定したものの、DoS (Denial of Service) 攻撃をはじめとする多くのセキュリティ問題があることが指摘されている¹⁰⁾。すなわち、MS と AP 間の相互認証で用いる IEEE 802.1X プロトコルにはセキュリティホールがあり、攻撃者が MS と AP 間のセッションを乗っ取ることができるという脅威問題が報告されている⁸⁾。また、IEEE 802.11 ならびに IEEE 802.1X 管理フレームパケットや制御フレームパケットが暗号化されないので、攻撃者がこれらのパケットを変更できるとともに DoS 攻撃が可能であることが知られている⁸⁾。したがって、Security Rollback 攻撃や 4 ウェイハンドシェイクに対する攻撃など IEEE 802.11i 固有のセキュリティ脅威問題を解決できるより安全な WLAN ユーザ認証方式が求められている。

(2) ハンドオフ問題

WLAN で移動端末 MS が異なる拡張サービスセット (ESS: Extended Service Set) 間を移動する場合はもちろん、同一の ESS 内に位置する AP 間を移動する場合、すなわち異なる基本サービスセット (BSS: Basic Service Set) 間を移動する場合のハンドオフ遅延問題¹¹⁾の解決も重要な課題となっている。したがって、MS が IEEE 802.11i で動作する場合は、次のような多くのハンドオフ処理による遅延が生じ、通信の中断が起きる可能性があり、シームレスサービスを提供できない問題があるので、これらを解決できる認証方式が求められている。

①802.11 ハンドオフ遅延

MS は新しい有効な AP を探すために 802.11 のスキャンを行い、その中で選んだ AP への物理・MAC レイヤに接続するための追加要求を出す。また、その AP への認証要求と論理的な再接続 (re-association) 要求を出さなければならないので、これらによる遅延が生じる。

②再認証処理遅延

MS がある AP で 802.11i セキュア・アソシエーションを確立したとしても、移動先の AP に新しいセキュア・アソシエーションを確立するために認証サーバへの 802.1X/EAP 認証手続きを再度行わなければならない。したがって、これらの認証処理による遅延が生

じる。

③IP レイヤハンドオフ遅延

MS は移動先での有効な IP アドレスの取得のための DAD (Duplicate Address Detection) 処理を行わなければならない。したがって、IP レイヤにおける IP connectivity を提供するため IP レイヤのハンドオフ遅延が生じる。現在、WLAN システムにおけるハンドオフで IP レイヤハンドオフ遅延時間が一番長くなっており¹²⁾、大きな課題である。

(3) スケーラビリティ問題

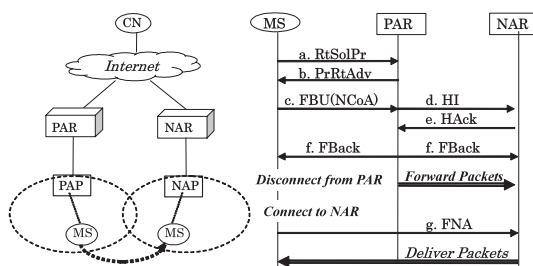
WLAN システムの固有の性質はモビリティであるので、利用するユーザ数や移動するユーザの変化においてスケーラビリティが要求される。したがって、IEEE 802.11i を適用する WLAN が高モビリティを支援するために、認証サーバが AP をスケーラブルな方法で扱うことができる認証方式を確立する必要がある。

2.3 FMIPv6 の概要

本研究では、上記ハンドオフ問題において遅延時間が一番長くなる IP レイヤにおける IP connectivity を迅速に提供するため、WLAN に Mobile IP を導入する。さらに、Mobile IP ハンドオフ遅延を改善するために Mobile IPv6 環境下で高速ハンドオフを可能としている FMIPv6¹⁴⁾ を適用する。

FMIPv6 は Mobile IPv6 環境下で頻繁に移動する端末の高速ハンドオフを可能とした拡張プロトコルである。ここでは、新しい接続ポイントでの IP connectivity を迅速に提供するために、ハンドオフイベントを予測するか、ハンドオフイベントに素早く応答するためにデータリンク層情報を利用する。また、移動端末が現在接続しているアクセスルータ (PAR: Previous Access Router) と移動先で接続するアクセスルータ (NAR: Next Access Router) 間のデータをトンネリングすることによって、ホームエージェントや通信ノード (CN: communication node) に移動先の Mobile IP 登録をする前に IP connectivity を提供でき、移動先の登録により生じる遅延とそれによるパケットロス問題を解決している。図 2 に FMIPv6 の代表的な predictive ハンドオフを WLAN と組み合わせた場合の動作を示す。ここでは、移動端末ノード MS が現在接続している AP (PAP) で新しい AP (NAP) のデータリンク層情報を検知するところから始まる。

- a. MS は PAR に NAP のデータリンク情報 (LLA: link layer address, AP-ID) を用いて近隣 AR を探すための代理ルータ要請 (Router Solicitation



MS: Mobile Station, PAR: Previous Access Router, NAR: New Access Router
PAP: Previous Access Point, NAP: New Access Point, CN: Communication Node

図 2 FMIPv6 における Predictive ハンドオフの動作
Fig. 2 Predictive fast handover for FMIPv6.

- for Proxy: RtSolPr) メッセージを送る。
- b. PAR は RtSolPr メッセージの NAP の情報に基づき、その NAP が接続されている AR (NAR) の IP レイヤ情報を含む代理ルータ広告 (Proxy Router Advertisement: PrRtAdv) メッセージを MS に送信する。
- c. MS はここで得られた NAR のネットワークプレフィックス情報を用いて移動後に用いる新しい気付けアドレス (New Care of Address: NCoA) を生成する。そして、PAR に NCoA を知らせる高速位置登録 (Fast Binding Update: FBU) メッセージを送信する。
- d. PAR は MS の移動中に移動前の気付けアドレス (Previous Care of Address: PCoA) に送られたパケットを移動後のアドレス (NCoA) に転送するためのトンネルを生成する。そして、PAR は MS が導出した NCoA が利用可能であるかを問い合わせるハンドオフ初期化 (Handover Initiate: HI) メッセージを NAR に送る。
- e. NAR は NCoA が利用可能かどうかを調べ、PAR に NCoA の利用可否と利用可能でなければ代替アドレスを送るハンドオフ応答 (Handover Acknowledgment: HAck) メッセージを送る。
- f. PAR は MS と NAR に高速位置登録応答メッセージ (FBack) を送り、NCoA 宛のパケットを NAR に転送する。
- g. MS は PAR から離れ NAR に接続すると、高速近隣広告 (Fast Neighbor Advertisement: FNA) メッセージを出す。そして、NAR にバッファリングされた NCoA 宛のパケットを転送してもらうことができる。 □

もし、MS がハンドオフイベントを予測できなかった場合 (reactive ハンドオフ) は、上記の step g において FBU を含む FNA の送信の後 PAR-NAR 間のトンネルを生成し、バッファリングしていた NCoA 宛の

パケットを転送する。このことにより, predictive ハンドオフの場合に比べると効果は低いものの, FMIPv6 を適用しない場合と比較して位置登録の迅速化によるハンドオフの高速化が図られている。

3. シームレス移動端末ユーザ認証プロトコル

3.1 WLAN システムの汎用ユーザ認証フレームワーク

本研究ではより安全で遅延の少ないシームレス WLAN サービスを提供するために, 図 3 に示すような移動端末ユーザ認証フレームワークを提案する。ここで, 各サービスプロバイダ (ISP) は, 所定の通信エリア内における MS に無線リンク接続サービスを提供する AP と, AP でリンク接続された MS のインターネット接続制御を行う AR およびアプリケーション提供時に MS を認証する AS で構成される。本認証フレームワークは, ISP ごとに MS を認証する AS を中心とした階層構造で構成されている。ここで, AP は従来の 802.11 プロトコルにおける 802.11 ハンドオフ遅延問題を改善するために, MS の物理・MAC レイヤにおけるアクセス制御機能を持つと仮定する。また, AR は従来の 802.11 プロトコルにおけるスケラビリティ問題および再認証処理遅延や IP レイヤハンドオフ遅延問題を改善するために導入するものであり, MS の移動を支援するためレイヤ 3 の Mobile IP など様々なデータ・管理機能を持つ。なお, 鍵管理サーバ KMS (Key Management Server) は従来の 802.11 の AS でのユーザ認証機能と鍵配布機能を分離するために導入するものであり, MS ユーザ間の暗号通信のためのセッション鍵を生成する機能を持つ。

本認証フレームワークでは, MS と AP または AR

の関係は MS の移動によってダイナミックに変更できるものとする。なお, IP レイヤハンドオフ遅延を削減するために, FMIPv6 による AR 間のデータトンネルを設定する。以下では, 同一 AR 配下の AP 間のハンドオフを intra-ESS ハンドオフ, 同一 ISP 内の異なる AR 配下にある AP 間のハンドオフを inter-ESS ハンドオフ, 異なる ISP の AR 配下の AP 間ハンドオフを inter-ISP ハンドオフとそれぞれ呼ぶ。

提案するフレームワークでは, 安全なシームレス WLAN サービスを提供するために, 下記のような認証機能を持つ。

(1) AP における MAC レイヤアクセス制御

MS が移動先の新しい AP に接続しようとした場合, AP に接続できる MS を制限するために, 無線リンク接続を要求する MS を認証する機能が必要である。

(2) AR における MS のモビリティ認証

AP での MS アクセス制御は同一リンク上に存在するすべての MS に共有されているため, AR においてつねに移動する MS は信頼できない。そこで, AR で MS のモビリティ認証を行う機能が必要である。

(3) AS における上位レイヤ認証

AP と AR での認証が成功すると, セッション鍵の取得のための AS など上位レイヤでの認証を行う機能が必要である。

3.2 Cache-PSK 認証方式

現在 EAP で主に使われている PKI ベース認証方式 (EAP-TLS, TTLS) は安全性の面では優れているが証明書確認のための処理時間が長くなり, MS の移動による AP への接続遅延が長い。そこで本研究では, 実現の容易性と既存のネットワークへの親和性を考慮し上記認証フレームワークにおける MS の認証・鍵

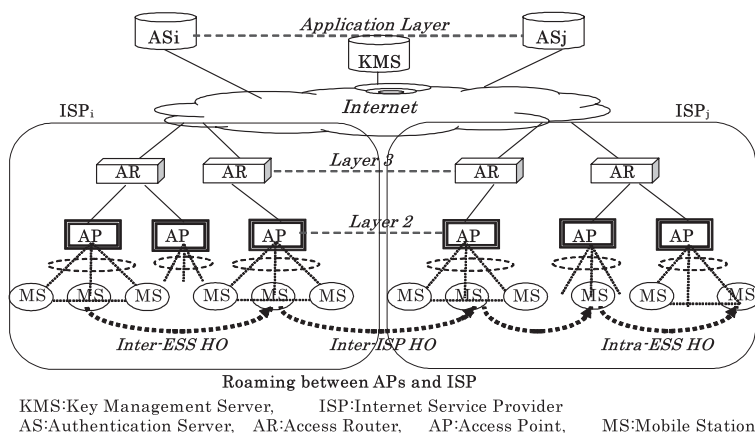


図 3 シームレス移動端末ユーザ認証フレームワーク

Fig. 3 Seamless mobile station authentication framework.

共有方法として、あらかじめ共有した鍵 (PSK: Pre-Shared Key) を用いて各エンティティ間の相互認証およびセッション鍵の導出を可能とする共通鍵ベース認証方式について検討する。しかし、従来の EAP-PSK 方式¹⁵⁾ (以下, pure-PSK 方式と呼ぶ) では, MS の認証が証明書ベース方式より速くなるという長所を持つが, システムの大規模化にともなう秘密情報 (鍵) の管理が容易ではないという短所を持つ。なお, 安全性の面では, 従来の 802.11i のセキュリティ脅威問題におけるいくつかの問題 (データの秘匿性, 相互認証および鍵の導出) は解決したものの, DoS 攻撃や再接続問題などは解決できていないのが現状である。

本研究では, 特に頻繁に移動するユーザに対して遅延の少ない高品質のサービスを提供することを目的としている。そこで, 上記認証フレームワークにおける前提条件として AR に共有鍵を事前に配布しておくものとする。このような AR への共有鍵の事前配布は, 鍵漏洩の問題において従来の認証サーバで管理することに比べると安全性の品質が低くなる可能性があると考えられる。しかし, AR は AP と比較して攻撃者が検出し難く, またネットワーク内部に設置され, その管理もより厳重であることを前提とすると, 一定の安全性は確保できると考える。なお, AR への鍵の配布は ISP の安全性を保証すべくシステム運用管理者自身が行うような環境を想定する。このような前提条件で, 下記の特徴を持つキャッシュベース事前共有鍵 (Cache-PSK) に基づく認証方式を導入する。

- KMS は MS を認証する事前共有鍵および MS ユーザ間の暗号通信のためのセッション鍵を生成する機能を持ち, 各 ISP の AS に配布する。
- MS がある ISP に加入すると AS は MS に事前共有鍵 (K_{MU}) を発行し AS で管理する。
- AS は配下の AR とセキュアな通信路を確保するために事前に秘密鍵 (K_{AR}) を共有しておく。
- AS で AP を認証する認証機能の一部を AR に分離するため, AP の識別子のアドレス情報 (AP_{ID}) を上位の AR に登録しておく。
- AS で MS の認証が成功すると, その MS の認証情報となる事前共有鍵 (K_{MU}) とユーザ識別子 (U_{ID}) を AR に保管 (cache) する。
- MS が異なる ISP の管理エリアに移動すると KMS は MS の事前共有鍵を更新する。

以下では, まず FMIPv6 による移動端末の事前認証方式について述べ, 図 3 の各ハンドオフの場合における詳細なプロトコルを提案する。

3.3 FMIPv6 による移動端末の事前認証方式

本論文ではつねに移動する MS のハンドオフ遅延を改善するために FMIPv6 を導入し, それに基づいた MS のシームレス認証手法を提案する。ここでは, 提案手法の概要について述べ, 詳細プロトコルについては次節で示す。

本論文で提案する FMIPv6 による事前認証方式 (図 4) の手順は以下になる。なお以下の番号は同図中の番号に対応している。

- (1) PAR AR_i 配下の PAP AP_i にて認証済みの MS MS が移動によって NAR AR_j 配下の NAP AP_j に接続しようとするとき, まず FMIPv6 を用いて AR_j の情報と移動先での IP アドレスを導出する。そして, MS は AR_i に接続している間に自分の認証情報を用いた AR_i へ事前認証要求メッセージ (PRE_AUTH_REQ) を出す。
- (2) AR_i では保管している MS の認証情報に基づき MS を事前認証し, MS に事前認証完了メッセージ (PRE_AUTH_ACK) を送る。また, AR 間の IP トンネルを用いて AR_i で保存している MS の認証情報を AR_j に転送する事前認証完了メッセージを送る。 AR_j は MS の認証情報を保存しておくとともに, AP_j に MS の事前認証完了メッセージを送ると AP_j は MS の識別子情報を保存しておく。
- (3) AR_i で事前認証完了メッセージを受け取った MS は移動によって AP_i から離れて AP_j に接続すると, AP_j とのセッション確立のためのネットワーク接続要求 ($CONN_REQ$) メッセージを出すことができる。
- (4) AP_j は MS の要求情報から MS が事前認証済みのユーザであることを確認し, AR_j にセッション鍵配布要求メッセージ (KEY_DIS_REQ) を

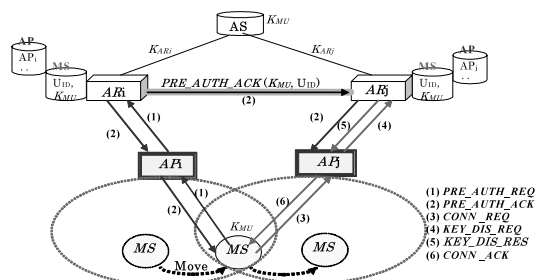


図 4 FMIPv6 による移動端末のシームレス認証手法

Fig. 4 Seamless user authentication method based on FMIPv6.

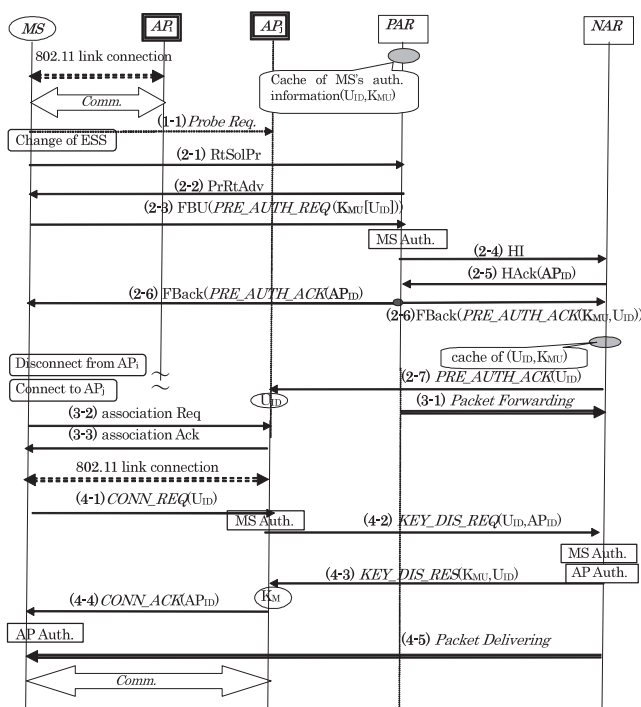


図 5 inter-ESS ハンドオフ認証プロトコル

Fig. 5 Seamless user authentication protocol in inter-ESS hand-off.

出す。

- (5) AR_j は保存している情報から MS と AP_j を確認し, MS の事前共有鍵を配布するメッセージ (KEY_DIS_RES) を AP_j に送る。
- (6) MS の事前共有鍵を取得した AP_j は MS にコネクション応答メッセージ ($CONN_ACK$) を出すことにより, MS と AP_j 間のセキュア・アソシエーションが確立されデータ暗号通信を開始することができる。□

3.4 FMIPv6 に基づくシームレス移動端末ユーザ認証プロトコル

本節では, 図 3 での inter-ESS ハンドオフ, inter-ISP ハンドオフ, intra-ESS ハンドオフのそれぞれの場合における, シームレス認証プロトコルを示す。

3.4.1 inter-ESS ハンドオフ認証プロトコル

ある LAN セグメントの AR PAR 配下の PAP AP_i において認証済みの MS MS が, 他の LAN セグメントの AR NAR 配下の NAP AP_j に移動する場合について考える。この場合の Cache-PSK に基づくシームレス認証プロトコルは図 5 のようになる。

【Step1】 $MS \leftrightarrow AP_j$: 無線リンク接続要求

(1-1) $MS \rightarrow AP_j$: $Probe_Req$;

MS が移動し始め現在接続されている AP AP_i 以

外の他の ESS 内の AP AP_j の無線リンクを検出すると, AP_j に 802.11 無線リンク接続を要求する (Probe request)。

【Step2】 $MS \leftrightarrow PAR$: PAR での事前認証

(2-1) $MS \rightarrow PAR$: $RtSolPr$ (LLA, AP-ID);

MS は自分が検知した AP_j のデータリンク層情報 (LLA, AP-ID) をもとに AP_j の管理 AR を探すために, FMIPv6 の代理ルータ要請メッセージを PAR に送信する。

(2-2) $PAR \rightarrow MS$: $PrRtAdv$ (NAR);

PAR は AP_j のデータリンク情報に基づき, その AP が接続されている AR (NAR) の情報を含む代理ルータ広告メッセージを MS に返す。

(2-3) $MS \rightarrow PAR$: $FBU(PRE_AUTH_REQ(K_{MU}[U_{ID}]))$;

MS はその情報に基づき移動後に用いる IP アドレス (NCoA) を導出し, それを PAR に伝えるための FBU を PAR に送る。このとき MS は FBU に事前共有鍵で暗号化した事前認証要求メッセージ情報を入れて送る。

(2-4) $PAR \rightarrow NAR$: HI (NCoA);

事前認証要求メッセージを受け取った PAR は自分が保管しているユーザ認証情報を用いて MS の事前認

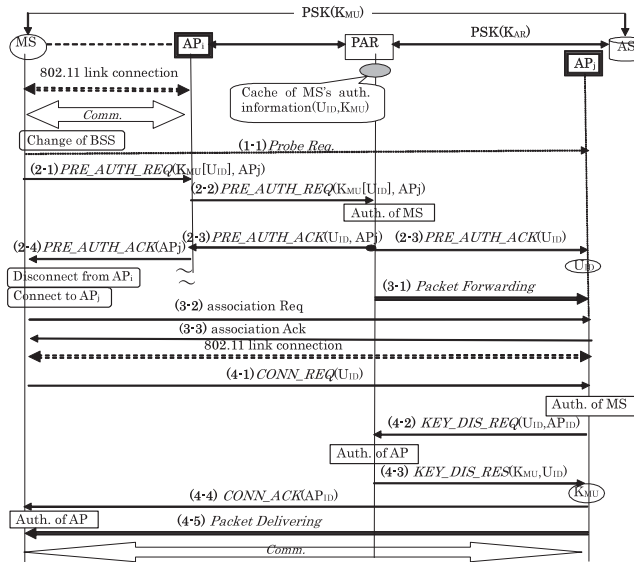


図 6 intra-ESS ハンドオフ認証プロトコル

Fig. 6 Seamless user authentication protocol in intra-ESS hand-off.

証を行う。事前認証が成功すると、PAR は NAR に MS の新しい IP アドレスが利用できるかどうか問い合わせるハンドオフ初期化メッセージを送る。

(2-5) NAR→PAR: HAck (AP_{ID});

NAR は NCoA が利用できるかどうかを調べ、PAR に NCoA の利用可否と利用可能な AP を知らせるハンドオフ応答メッセージを返す。

(2-6) PAR→NAR: FBack (PRE_AUTH_ACK (K_{MU}, U_{ID}));

PAR→MS: FBack (PRE_AUTH_ACK (AP_{ID}));

PAR は NAR に MS の事前認証応答のメッセージを含む FBU 応答メッセージを送り、ハンドオフの準備を行う。その事前認証応答メッセージには MS の認証情報も入れておき、NAR はその情報を保存しておく。なお、事前認証要求メッセージを送られてきた MS にも事前認証応答のメッセージを含む FBU 応答メッセージを送る。

(2-7) NAR→AP_j: PRE_AUTH_ACK (U_{ID});

NAR は自分の配下の AP_j に MS の事前認証応答メッセージを出す。AP_j は MS の事前認証情報を保存しておく。

【Step3】MS⇔NAR: NAR への接続

(3-1) PAR→NAR: Packet Forwarding;

PAR は MS 宛のパケットを NAR に転送する。

(3-2) MS→AP_j: association Req;

MS は AP_i から離れて AP_j に接続する。

(3-3) AP_j→MS: association Ack;

AP_j は MS を 802.11 認証し無線リンク接続を確立する。

【Step4】MS⇔AP_j: セキュア・セッション確立

(4-1) MS→AP_j: CONN_REQ (U_{ID});

AP_j に 802.11 無線リンク接続した MS は AP_j へのセキュア・セッション接続を要求する。

(4-2) AP_j→NAR: KEY_DIS_REQ (U_{ID}, AP_{ID});

AP_j は保存している事前認証済みユーザ情報に基づき MS を認証し、NAR へのセッション鍵配布要求メッセージを出す。

(4-3) NAR→AP_j: KEY_DIS_RES (K_{MU}, U_{ID});

NAR は保存している事前認証済みユーザ情報と配下管理 AP 情報に基づき MS と AP を確認し、AP_j に MS のセッション鍵情報 (K_{MU}) を配布する。

(4-4) AP_j→MS: CONN_ACK (AP_{ID});

AP_j は MS のセッション鍵情報を取得し、MS にセキュア・セッション接続応答メッセージを送る。

(4-5) NAR→MS: Packet delivering;

NAR は PAR から転送してもらった NCoA 宛のパケット情報を MS に転送し、MS は AP_j との暗号通信を開始することができる。 □

3.4.2 intra-ESS ハンドオフ認証プロトコル

ここでは AR PAR 配下の PAP AP_i において認証済みの MS MS が同一 AR 配下の NAP AP_j に移動する場合のシームレス事前認証手順を示す。以下、図 6 に基づきプロトコルの詳細を示す。

【Step1】 $MS \rightleftharpoons AP_j$: 無線リンク接続要求

(1-1) $MS \rightarrow AP_j$: *Probe_Req*;

AP_i と通信中の MS が移動し始め異なる BSS の AP_j の無線リンクを検出すると, AP_j に無線リンク接続を要求する.

【Step2】 $MS \rightleftharpoons PAR$: PAR での事前認証

(2-1) $MS \rightarrow AP_i$: *PRE_AUTH_REQ* (K_{MU} [U_{ID}], AP_j);

MS は検出した AP_j に接続するために, AP_j のデータリンク層情報を用いて AP_j へ移動する前の事前認証要求メッセージを出す.

(2-2) $AP_i \rightarrow PAR$: *PRE_AUTH_REQ* (K_{MU} [U_{ID}], AP_j);

AP_i は MS の事前認証要求メッセージ情報を PAR に転送する.

(2-3) $PAR \rightarrow AP_j$: *PRE_AUTH_ACK* (U_{ID});

$PAR \rightarrow AP_i$: *PRE_AUTH_ACK* (U_{ID});

PAR は保存されたユーザ認証情報を用いて MS の認証を行い, AP_j の情報を確認する. PAR は AP_j に MS の事前認証応答メッセージを送信し, AP_j はその MS の情報を保存しておく. また, 同時に事前認証要求メッセージを出した AP_i にも事前認証応答メッセージを送信する.

(2-4) $AP_i \rightarrow MS$: *PRE_AUTH_ACK* (AP_j);

AP_i は MS に AP_j への事前認証応答メッセージを送る.

【Step3】 $MS \rightleftharpoons AP_j$: AP_j への接続

(3-1) $PAR \rightarrow AP_j$: *Packet Forwarding*;

PAR は MS 宛のパケットを AP_j に転送する.

(3-2) $MS \rightarrow AP_j$: *association Req*;

MS は AP_i から離れて AP_j に接続する.

(3-3) $AP_j \rightarrow MS$: *association Ack*;

AP_j は MS を 802.11 認証し無線リンク接続を確立する.

【Step4】 $MS \rightleftharpoons AP_j$: セキュア・セッション確立

(4-1) $MS \rightarrow AP_j$: *CONN_REQ* (U_{ID});

AP_i から離れて AP_j に接続した MS は AP_j へのセキュア・セッション接続を要求する.

(4-2) $AP_j \rightarrow PAR$: *KEY_DIS_REQ* (U_{ID} , AP_{ID});

AP_j は PAR からの事前認証応答情報を用いて MS 認証を行い, PAR にセッション鍵配布を要求する.

(4-3) $PAR \rightarrow AP_j$: *KEY_DIS_RES* (K_{MU} , U_{ID});

PAR は AP_j を認証した後 MS のセッション鍵情報を AP_j に配布する.

(4-4) $AP_j \rightarrow MS$: *CONN_ACK* (AP_{ID});

AP_j は MS のセッション鍵情報を格納しておき, MS

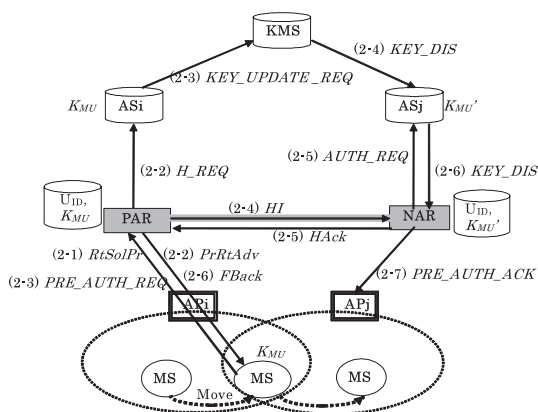


図 7 inter-ISP ハンドオフ認証プロトコル

Fig. 7 Seamless user authentication protocol in inter-ISP hand-off.

にセキュア・セッション応答確立メッセージを送る.

(4-5) $AP_j \rightarrow MS$: *Packet delivering*;

AP_j は PAR から転送してもらったパケット情報を MS に転送し, MS は AP_j を認証し, 暗号通信を開始する. □

3.4.3 inter-ISP ハンドオフ認証プロトコル

次に, ある ISP ISP_i の AR PAR 配下の AP AP_i において認証済みの MS が異なる ISP ISP_j の AR NAR 配下の AP AP_j に移動する場合の認証手順を図 7 に示す. ここでは, 3.4.1 項の Inter-ESS ハンドオフ認証プロトコルより変更になる Step2 を中心に述べる.

【Step1】 $MS \rightleftharpoons AP_j$: 無線リンク接続要求

【Step2】 $MS \rightleftharpoons KMS$: KMS で MS の事前共有鍵を更新

(2-1) $MS \rightarrow PAR$: *RtSolPr* (LLA , AP_{ID});

MS は自分が検出した AP_j の管理 AR を探すための代理ルータ要請メッセージを PAR に送信する.

(2-2) $PAR \rightarrow MS$: *PrRtAdv* (NAR);

$PAR \rightarrow AS_i$: *H_REQ* (U_{ID} , NAR);

PAR は AP_j が接続されている AR NAR の情報を含む代理ルータ広告メッセージを MS に返す. また, PAR はその NAR が自分の属する ISP の AR ではないことが分かると, AS_i に MS の NAR へのハンドオフ要求 (*H_REQ*) を出す.

(2-3) $MS \rightarrow PAR$: *FBU*(*PRE_AUTH_REQ* (K_{MU} [U_{ID}]);

$AS_i \rightarrow KMS$: *KEY_UPDATE_REQ* (U_{ID} , NAR);

MS は NCoA を導出し, それを伝えるための FBU を PAR に送る. また, この FBU には事前共有鍵で

暗号化した事前認証要求メッセージ情報も含む。

なお、 AS_i は MS を確認し KMS に MS の鍵更新要求メッセージ (KEY_UPDATE_REQ) を出す。

(2-4) $PAR \rightarrow NAR$: HI (U_{ID} , $NCoA$);

$KMS \rightarrow AS_j$: KEY_DIS (U_{ID} , K_{MU}');

PAR は自分が保管しているユーザ認証情報を用いて MS の事前認証を行い、認証が成功すると NAR に MS のハンドオフ初期化メッセージを送る。

なお、 KMS は NAR を管理する AS_j を検索し、 AS_j に MS の更新された事前共有鍵 (K_{MU}') を配布する。

(2-5) $NAR \rightarrow PAR$: HAcK (AP_{ID});

$NAR \rightarrow AS_j$: AUTH_REQ (U_{ID});

NAR は $NCoA$ が利用できるかどうかを調べ、 PAR に AP_j へのハンドオフ応答メッセージを返す。また、 AS_j に MS の認証要求メッセージ ($AUTH_REQ$) を出す。

(2-6) $PAR \rightarrow MS$: FBack (PRE_AUTH_ACK (AP_{ID}));

$AS_j \rightarrow NAR$: KEY_DIS (U_{ID} , K_{MU}');

PAR は MS に事前認証応答メッセージを含む FBU 応答メッセージを送る。

また、 AS_j は MS を認証し NAR に MS の更新された事前共有鍵を配布する。 NAR は MS の更新された認証情報 (U_{ID} , K_{MU}') を保存しておく。

(2-7) $NAR \rightarrow AP_j$: PRE_AUTH_ACK (U_{ID});

NAR は自分の配下の AP_j に MS の事前認証応答メッセージを出す。 AP_j は MS の認証情報を保存しておく。

【Step3】 $MS \leftrightarrow NAR$: NAR への接続

【Step4】 $MS \leftrightarrow AP_j$: セキュア・セッション確立

□

このように本提案認証フレームワークでは、 PAP に接続していた MS が異なる ISP の NAP に移動する際、 KMS で MS の事前共有鍵を更新し移動先の NAR に配布することにより、移動先 ISP で新たな加入手続きおよび認証を必要としないので、よりシームレスサービスを実現することができる。

4. 提案方式の評価

本章では、3.1 節で提案したシームレス移動端末認証フレームワークに基づき提案プロトコルの有効性について述べる。また、本論文で提案した方式の達成すべき安全性と達成程度について考察する。

4.1 提案方式の有効性

4.1.1 評価項目

3.4 節で提案した FMIPv6 に基づく移動端末の事前

認証方式は、従来の pure-PSK 方式における移動端末のハンドオフ遅延時間と鍵管理問題を解決するためのものとして、認証済みの無線端末ユーザ MS が同一 AR の配下で移動する場合や AR 間を移動する場合などに応じたプロトコルを含む。ここでは、2.1 節の IEEE 802.11i における pure-PSK 方式との比較を行うため、3.4.1 項で提案した AR が変わる場合 (inter-ESS ハンドオフ) のシームレス認証プロトコルを中心に評価を行う。このプロトコルは、FMIPv6 に基づき移動先のアクセスポイント (NAP) への無線接続要求を出し、移動する前に PAR で保存しているユーザ認証情報を用いた事前認証と NAP を管理する NAR への接続および移動先のアクセスポイントにセキュア・セッション確立を行う 4 つのステップからなる。

このうち、 NAP への無線接続要求と PAR での事前認証は現在のアクセスポイントに接続している状態で行うので遅延や通信の中断などデータ通信への影響も少ない。しかし、セッション確立は現在のアクセスポイントから離れて新しいアクセスポイントにリンク接続し、その NAP を管理する NAR での MS , AP 認証を行うので、その時間が長くなると接続遅延による通信中断が起きるので、データ通信の性能にも影響を及ぼす。そこで、ここでは遅延時間、すなわち再接続のための通信中断時間を評価項目として検討する。

また、従来の pure-PSK 方式においては各ユーザの事前共有鍵を AS で管理するので、システムの規模が大きくなると鍵管理が容易ではなくなるという問題や、移動端末ユーザ認証のための通信トラフィックが AS に集中してしまうという問題があった。一方、提案手法では、認証済みユーザの秘密認証情報 (鍵) をユーザの移動管理を行う AR で保管するように分離することによって、この問題を解決しようとしている。そこで、ユーザ認証に要する通信トラフィックがどの程度改善されたのかについても検討する。

4.1.2 遅延時間

図 3 のネットワークモデルで、移動端末ユーザ MS の再認証にかかる時間 (再認証時間) について検討する。再認証時間には、認証・鍵共有プロトコルのメッセージ転送に必要な時間 (メッセージ転送時間) とともに、転送経路上のルータや AP におけるプロトコル処理時間 (D_P) が含まれる。さらに、メッセージ転送時間には、ルータ間の伝送路における伝送遅延時間 (D_L) と LAN セグメント上での伝送遅延時間 (D_S) がある。このうち、 D_P はルータや AP の性能に大きく依存し、また D_L と D_S はその帯域やデータトラフィックの状況によっても変化する。さらに、 D_L は

リンク間の距離によっても大きく異なる。しかしながら、ここでは、特にこのネットワークモデルで対象としているような広域にまたがるネットワークでは D_P や D_S は D_L に比べて十分小さいと仮定し、以下では D_L のみを考慮する。

図 1 における既存方式による MS の再認証時間は、MS が NAP に 802.11 接続し、AS への認証要求メッセージを出してから、認証が成功して NAP との新しいセッション鍵を生成し、それによる暗号通信開始のための IP 接続調整を行うまでの時間である。そこで、遅延時間は次のように与えられる。

$$D_{AS} = t_{s1} + t_{s2} + t_{s3} + t_{s4} \quad (1)$$

ここで、式 (1) の第 1 項はステップ 1 の MAC レイヤにおける 802.11 接続要求パケットに対する認証とその応答の転送時間を表し、第 2 項は AS への EAP 認証にかかる時間を表す。また、第 3, 4 項は新しい AP とのセッション鍵生成と、DHCP などによる IP connectivity 調整が終了するまでの時間を表す。これらの遅延時間は認証方式により多少異なってくるが、現在実用化されている一般的な IPv4 のルータおよび AP に対して、 t_{s1} は 24 ms～380 ms、 t_{s2} は 750 ms～1,200 ms、 t_{s3} は 10 ms～80 ms、さらに t_{s4} は 200 ms～3,500 ms かかることが報告されている¹²⁾。これらより、 D_{AS} は 1,000 ms～5,200 ms 程度と考えられる。

一方、図 5 の提案方式においては 802.11 接続要求と MS 認証は移動する前に行うので、遅延時間は次のようになる。

$$D_{AR} = t'_{s3} + t'_{s4} \quad (2)$$

式 (2) の第 1 項は MS が PAP から離れて移動先の NAR の NAP に 802.11 無線リンク接続を確立するための時間である。また、第 2 項は新しい AP とのセキュア・セッション確立のための時間で、セッション鍵配布要求・応答メッセージを転送する時間と、MS、AP、AR 上での認証処理の時間が含まれる。ここで、 t'_{s3} は従来方式における t_{s3} と同様に 10 ms～80 ms と考えられる。また、 t'_{s4} のセッション確立の遅延時間については筆者らの知るかぎり報告例はないが、上記と直接比較はできないものの、PC 上での EAP 認証処理については 10 ms 未満との報告¹⁶⁾がある。これらのことから、 D_{AR} は D_{AS} に比べ十分小さな値になると考えられる。ただし、資源の限定された MS 上の AP の認証処理は文献 16) に比べて大きくなると予想される。この部分は MS の性能に大きく依存すると考えられ、今後実装して確認する必要がある。

4.1.3 通信トラフィック

次に、ユーザ認証・鍵共有の手順に要する AS に対

する通信トラフィックに関して考察する。

提案方式においては、intra-ESS ハンドオフおよび inter-ESS ハンドオフの場合は AS で認証済みの移動端末ユーザ MS の認証情報を AR であらかじめ保管しているため、ハンドオフの際の再認証要求メッセージは AR へ出され、AS へのトラフィックは発生しない。したがって、ユーザ認証のトラフィックは inter-ISP ハンドオフの場合のみ発生し、

$$T = 2mnpq \quad (3)$$

となる。ここで、 n は AS が管理するユーザ数、 m は MS の単位時間あたりのハンドオフ数（ハンドオフ頻度）をそれぞれ表す。また、 p は intra-ESS ハンドオフの頻度に対する inter-ESS ハンドオフの頻度の割合を、 q は inter-ESS ハンドオフの頻度に対する inter-ISP ハンドオフの頻度の割合を、それぞれ表す ($0 < p, q$)。

一方、図 1 の従来方式では、intra-ESS ハンドオフ、inter-ESS ハンドオフ、および inter-ISP ハンドオフのすべてについて MS の認証要求・応答メッセージが発生し、それらが AS に集中する。したがって、AS のユーザ認証のトラフィックは

$$T' = 2mn(1 + p + pq) \quad (4)$$

である。

これより、式 (4) に対する式 (3) の比は

$$T/T' = pq/(1 + p + pq) \quad (5)$$

となる。一般に、inter-ESS ハンドオフの頻度は intra-ESS ハンドオフの頻度に対して、さらに、inter-ISP ハンドオフの頻度は inter-ESS ハンドオフの頻度に対して、それぞれ十分小さいと考えられる。そこで、 $p \ll 1$ 、 $q \ll 1$ と仮定すると、式 (5) は

$$T/T' = pq/(1 + p + pq) \approx pq \quad (6)$$

となる。

このことより、提案手法における AS に対する送受信パケット数は、従来方式に対して大きく削減されることが考えられる。

4.1.4 考察

従来の方式における移動端末の再認証によるハンドオフ問題を解決するために、本論文で提案した方式においては、AR で認証済みのユーザ認証情報を管理できる分散管理機能を導入し、FMIPv6 に基づいた AR での事前共有鍵による MS モビリティ認証を行い、迅速な再接続が可能になり遅延による通信中断の時間を短くすることができた。ただし、reactive ハンドオフの場合は、MS が NAR に接続した後 PAR-NAR 間のトンネルが生成され、それを用いてセッション認証情報を転送することで MS の認証が可能となる。こ

れにより、MS は移動先で改めて AS への認証の依頼をすることなく、その分ハンドオフの遅延が低減されたと考える。ただし、この場合には NAR に接続する前に事前認証を済ませる predictive ハンドオフの場合に比べて高速化の効果は少なくなる。したがって、FMIPv6 における MS の reactive ハンドオフがどれくらい発生するかによって、本方式の効率が異なってくると予想される。

また、ワイヤレスネットワークでは頻繁に移動する端末ユーザの変化に応じて、サーバが管理しなければならないユーザの情報量とサーバへのアクセスにともなうトラフィックの集中について考慮しなければならない。すなわち、ユーザが移動するたびに AS にアクセスするので AS に対するトラフィック負荷分散をさらに考慮しなければならない。提案システムにおいては、移動端末のスケーラビリティの問題を解決するために、認証サーバでのユーザ情報管理機能を AR に分離し保管することによりサーバの負荷分散を行った。

なお、本論文では、ISP 内のハンドオフに加え、ISP 間のハンドオフも想定しており、これを実現するためには事前に複数の ISP に加入しておく必要がある。すなわち、現状では本提案方式における ISP 間のハンドオフの適用は、ユーザが加入している複数の ISP 間に制限される。したがって、「いつでも世界中のどこでもコンピュータが使える」という真のユビキタスネットワークを実現するにあたっては、各ユーザが事前にすべての ISP に加入しておくという前提が必要になる。将来的には、認証情報や加入者情報などが一定のポリシーの下に共有され、1 つの ISP への加入で ISP 間のハンドオフが可能となるようなサービスが提供されるようになり、このような制約が緩和されるものと考えられる。

4.2 提案方式の安全性

次に、本論文で提案した方式の達成すべき安全性と達成程度について考察する。本論文では WLAN システムにおける移動端末のユーザ認証と高速ハンドオフを可能にするために、FMIPv6 に基づいたシームレスユーザ認証方式を提案した。したがって、提案方式において達成すべき安全性としては、AR 間のトンネルに転送される認証情報メッセージの暗号化による保護と 802.11i におけるセキュリティ脅威問題の解決が考えられる。

802.11i におけるセキュリティ脅威問題に関しては、2.2 節でも述べたように DoS 攻撃をはじめ不正 AP の検出問題、認証プロトコルで用いる制御・管理フレームパケットの暗号化および安全な鍵配布問題などがあ

る。それに対して提案方式においては、AR を導入して AP を管理し、KMS から AS と AR 間の事前共有鍵を配布しそれを用いて通信パケットを暗号化しているため、IEEE 802.11i のセキュリティ脅威問題となる不正 AP を検出することおよび認証パケットを保護することができる。しかし、管理フレームパケットを認証する機構は持たないため、従来の IEEE 802.11i における DoS 攻撃については同様の課題がある。なお、AR への共有鍵の事前配布は、鍵漏洩の問題において従来の認証サーバで管理することに比べると安全性の品質が低くなる可能性があると考えられる。しかしながら、AR は AP と比較して攻撃者が検出し難く、またネットワーク内部に設置され、その管理もより厳重であることを前提とすると、一定の安全性は確保できると考える。ここで、AR への鍵の配布はシステム運用管理者自身が行うべきであろう。

一方、AR 間のトンネルに転送される認証情報メッセージの暗号化については、FMIPv6 仕様¹⁴⁾ に基づき IPsec を用いて解決できると考える。すなわち、提案方式によると MS が移動前に PAR で保管しているユーザの認証情報を用いて事前認証を行うとともに、PAR から PAR-NAR 間のトンネルを用いてセッション認証情報を転送している。このような AR 間の認証メッセージは IPsec によって安全に転送できる。

5. ま と め

本研究では、ワイヤレスネットワーク上でモバイル端末を用いて移動するユーザのシームレス認証方式について検討した。特に、ワイヤレスネットワーク固有の問題となるモビリティとスケーラビリティ問題を考慮した認証方式について検討した。そこで、従来の pure-PSK 方式における移動端末の再認証によるハンドオフ問題と移動端末のスケーラビリティの問題を解決するために、AR で認証済みのユーザ認証情報を管理できる分散管理機能を導入した認証フレームワークを提案し、そのうえで FMIPv6 に基づいた Cache-PSK による事前認証方式を提案した。また、提案方式の有効性を示すためにプロトコルの分析による定量的な評価について検討を行った。今後は、提案方式の実用化レベルの確認のため、提案プロトコルの実装および実際のネットワーク上での有効性の検証法について検討していく予定である。なお、DoS 攻撃に関する対策や、提案方式のより詳細なセキュリティレベルの評価についても検討していく予定である。

参 考 文 献

- 1) Arbaugh, W.A., Shankar, N. and Wang, J.: Your 802.11 Wireless Network has No Clothes, *Proc. 1st IEEE International Conference on wireless LANs and Home Networks* (Dec.2001).
- 2) Institute of Electrical and Electronics Engineers: Local and Metropolitan Area Networks: Port-Based Network Access Control, IEEE standard 802.1X-2004 (Dec. 2004).
- 3) Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J. and Levkowetz, H.: Extensible Authentication Protocol (EAP), RFC 3748 (June 2004).
- 4) Aboba, B. and Simon, D.: PPP EAP TLS Authentication Protocol, RFC 2716 (Oct. 1999).
- 5) Funk, P. and Blake-Wilson, S.: EAP Tunneled TLS Authentication Protocol, Internet-Draft, draft-ietf-pppext-eap-ttls-01.txt (Feb. 2002).
- 6) Palekar, A., Simon, D., Salowey, J., Zhou, H., Zorn, G. and Josefsson, S.: Protected EAP Protocol (PEAP) Version 2, Internet-Draft, draft-Josefsson-pppext-eap-tls-v0.txt (Oct. 2004).
- 7) Institute of Electrical and Electronics Engineers: Supplement to Standard for Telecommunications and Information Exchange between Systems —LAN/MAN Specific Requirements-Part11: Wireless Medium Access Control (MAC) and physical layer (PHY) Specification: Specification for Enhanced Security, IEEE Standard 802.11i-2004 (Dec. 2004).
- 8) Arbaugh, W.A., Shankar, N. and Wan, Y.C.J.: An Initial Security Analysis of the IEEE 802.1X Standard, Univ. of Maryland Technical Report (2002).
- 9) Stanley, D.: EAP Method Requirements for Wireless LANs, RFC4017 (March 2005).
- 10) He, C. and Mitchell, J.C.: Security Analysis and Improvements for IEEE 802.11i, *11th Annual Network and Distributed System Security Symposium (NDSS'05)* (Feb. 2005).
- 11) Spilman, J., et al.: Test Methodology for Measuring BSS Transition Time, IEEE 802.11WG, document 802.11-04/0748r1 (2005).
- 12) Alimian, A. and Aboba, B.: Analysis of Roaming Technique, IEEE 802.11WG, document 802.11-04/0377r1 (2004).
- 13) Aboba, B., Simon, D, Arkko, J., Eronen, P. and Levkowetz, Ed. H.: Extensible Authentication Protocol (EAP) Key Management Framework, Internet-Draft, draft-ietf-eap-keying-05.txt (Feb. 2005).
- 14) Koodli, R.: Fast Handover for Mobile IPv6, RFC4068 (July 2005).
- 15) Bersani, F. and Tschofenig, H.: The EAP-PSK Protocol: a Pre-Shared Key EAP Method, Internet-Draft, draft-bersani-eap-psk-09.txt (Aug. 2005).
- 16) 海沼義彦, 小野夏子, 木村 徹, 張 亮, 林 秀樹, 寺岡文男: FMIPv6 における PANA を用いた高速認証方式の設計と実装及び評価, IPSJ Symposium Series, Vol.2005, No.6, pp.101-104 (2005).

(平成 17 年 12 月 2 日受付)

(平成 18 年 5 月 9 日採録)

**朴 美娘** (正会員)

1983 年漢陽大学工学部電子工学科卒業。同年漢陽大学工学部助手。1993 年東北大学大学院工学研究科情報工学専攻博士後期課程修了。同年東北大学電気通信研究所助手。1994 年三菱電機株式会社入社。現在、同社情報技術総合研究所勤務。通信プロトコル設計, ネットワークセキュリティ, 移動通信ネットワーク等の研究に従事。博士 (工学)。電子情報通信学会会員。

**岡崎 直宣** (正会員)

1986 年東北大学工学部通信工学科卒業。1991 年東北大学大学院工学研究科電気および通信工学専攻博士後期課程修了。同年三菱電機株式会社入社。2002 年より宮崎大学工学部助教授。通信プロトコル設計, ネットワーク管理, ネットワークセキュリティ, モバイルネットワーク等の研究に従事。博士 (工学)。電子情報通信学会, 電気学会, IEEE 各会員。

**馬場 義昌**

1984 年慶應義塾大学工学部計測工学科卒業。1986 年慶應義塾大学院修士課程修了。同年三菱電機 (株) 入社。以来, LAN, インターネット, ネットワークセキュリティ, 光ネットワーク制御等の研究開発に従事。現在、同社情報技術総合研究所に勤務。