

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5421274号
(P5421274)

(45) 発行日 平成26年2月19日 (2014. 2. 19)

(24) 登録日 平成25年11月29日 (2013. 11. 29)

(51) Int. Cl.	F I
HO 4W 12/06 (2009. 01)	HO 4W 12/06
HO 4W 36/14 (2009. 01)	HO 4W 36/14
HO 4W 88/06 (2009. 01)	HO 4W 88/06

請求項の数 15 (全 39 頁)

(21) 出願番号	特願2010-529860 (P2010-529860)	(73) 特許権者	502032105
(86) (22) 出願日	平成20年10月15日 (2008. 10. 15)		エルジー エレクトロニクス インコーポ レイティド
(65) 公表番号	特表2011-501554 (P2011-501554A)		大韓民国ソウル、ヨンドゥンポーク、ヨイ ーデロ、1 2 8
(43) 公表日	平成23年1月6日 (2011. 1. 6)	(74) 代理人	100078282
(86) 国際出願番号	PCT/KR2008/006074		弁理士 山本 秀策
(87) 国際公開番号	W02009/051400	(74) 代理人	100113413
(87) 国際公開日	平成21年4月23日 (2009. 4. 23)		弁理士 森下 夏樹
審査請求日	平成23年10月12日 (2011. 10. 12)	(72) 発明者	ハン, ジェン ベク
(31) 優先権主張番号	60/980, 458		大韓民国 4 3 1 - 0 8 0 キョンギード , アニョンシ, ドンガンク, ホ ゲ 1 (イル)ードン, エルジー イン スティテュート
(32) 優先日	平成19年10月17日 (2007. 10. 17)		
(33) 優先権主張国	米国 (US)		
(31) 優先権主張番号	10-2007-0139698		
(32) 優先日	平成19年12月28日 (2007. 12. 28)		
(33) 優先権主張国	韓国 (KR)		

最終頁に続く

(54) 【発明の名称】 異種無線アクセスネットワーク間におけるハンドオーバー方法

(57) 【特許請求の範囲】

【請求項 1】

マルチモード移動局 (MS) により異種無線アクセスネットワーク間におけるハンドオーバーを行う方法であって、

前記方法は、

前記マルチモードMSが接続している現在接続ネットワークとともに一つ以上の候補ターゲット接続ネットワークに関する情報を獲得することと、

候補ターゲット接続ネットワークの各々のネットワークタイプを決定することと、

前記現在接続ネットワークから受信された信号レベルが第1臨界値未満である場合に、前記候補ターゲット接続ネットワークのうち、選択されたターゲット接続ネットワークに直接または間接的に事前認証要請メッセージを伝送することと、

前記選択されたターゲット接続ネットワークから、前記事前認証要請メッセージに応答して、直接または間接的に事前認証結果情報を受信することと、

前記現在接続ネットワークから受信された信号レベルが第2臨界値未満である場合に、前記事前認証結果情報を用いて追加的な認証手順無しで前記選択されたターゲット接続ネットワークにハンドオーバーを行うことであって、前記第1臨界値は、前記第2臨界値よりも高く設定される、ことと

を含み、

前記事前認証結果情報は、第1タイプターゲットネットワークの場合に、HSS (Home Subscriber Server) から抽出された前記マルチモードMSに対

10

20

するセキュリティ情報を含み、前記事前認証結果情報は、第2タイプターゲットネットワークの場合に、前記HSSから抽出された前記マルチモードMSに対する前記セキュリティ情報を省略し、

前記現在接続ネットワークの識別子(ID)及び前記現在接続ネットワークの認証サーバのIDは、前記事前認証要請メッセージ及び前記事前認証結果情報から除外され、

前記マルチモードMSのIDは、前記方法を行うときに露出されず、前記マルチモードMSのIDは、IMSI(International Mobile Subscriber Identity)、TMSI(Temporary Mobile Subscriber Identity)またはMAC(Media Access Control)アドレスを含む、方法。

10

【請求項2】

前記情報を獲得すること、前記事前認証要請メッセージを送信すること、前記事前認証結果情報を受信すること、及び前記ハンドオーバーを行うことのうちの少なくとも一つは、MIH(Media Independent Handover)プリミティブを用いて行われる、請求項1に記載の方法。

【請求項3】

前記事前認証要請メッセージを送信することは、MIH事前認証要請プリミティブを用いて行われ、

前記MIH事前認証要請プリミティブは、

前記選択されたターゲット接続ネットワークのID、前記選択されたターゲット接続ネットワークの認証サーバのID、前記マルチモードMSのID及び事前認証要請指示子のうちの少なくとも一つを含む、請求項2に記載の方法。

20

【請求項4】

前記事前認証結果情報を受信することは、MIH事前認証応答プリミティブを用いて行われ、

前記MIH事前認証応答プリミティブは、

前記現在接続ネットワークのID、前記現在接続ネットワークの認証サーバのID、前記選択されたターゲット接続ネットワークのID、前記選択されたターゲット接続ネットワークの認証サーバのID、前記選択されたターゲット接続ネットワークのHSS(Home Subscriber Server)のID、事前認証結果状態ID及び事前認証結果伝達状態IDのうちの少なくとも一つを含む、請求項2に記載の方法。

30

【請求項5】

前記事前認証要請メッセージの伝送及び前記事前認証結果情報の受信が間接的に行われる場合、前記事前認証要請メッセージの伝送及び前記事前認証結果情報の受信は、前記現在接続ネットワークを通じて行われる、請求項1に記載の方法。

【請求項6】

前記事前認証要請メッセージの伝送及び前記事前認証結果情報の受信は、前記マルチモードMSのMIHエンティティにより行われ、

前記方法は、

前記MIHエンティティが前記事前認証要請メッセージを送信する前に、前記マルチモードMSのMIHエンティティにより、前記マルチモードMSのMIHユーザエンティティから前記事前認証要請メッセージを受信することと、

40

前記MIHエンティティが前記事前認証結果情報を受信した後に、前記MIHエンティティにより、前記事前認証結果情報を前記MIHユーザエンティティに通報することとをさらに含む、請求項1に記載の方法。

【請求項7】

前記事前認証結果情報を前記MIHユーザエンティティに通報することは、MIH事前認証確認プリミティブを用いて行われ、

前記MIH事前認証確認プリミティブは、

前記選択されたターゲット接続ネットワークのID、前記選択されたターゲット接続ネ

50

ットワークの認証サーバのID、事前認証結果状態ID及び事前認証結果伝達状態IDのうちの少なくとも一つを含む、請求項6に記載の方法。

【請求項8】

特定接続ネットワークにより異種無線アクセスネットワーク間のハンドオーバーを支援する方法であって、マルチモード移動局(MS)がターゲット接続ネットワークとして前記特定接続ネットワークに対して前記ハンドオーバーを行い、

前記方法は、

前記マルチモードMSから事前認証要請メッセージを受信することであって、前記事前認証要請メッセージは、現在接続ネットワークから前記マルチモードMSにより受信された信号レベルが第1臨界値未満である場合に、前記マルチモードMSから伝送される、ことと、

10

前記事前認証要請メッセージに応答して、事前認証結果情報を前記マルチモードMSに伝送することと、

前記事前認証結果情報を用いて前記マルチモードMSが前記ターゲット接続ネットワークへのハンドオーバーを行うことを、追加的な認証手順無しで支援することであって、前記マルチモードMSは、前記現在接続ネットワークから前記マルチモードMSにより受信された信号レベルが第2臨界値未満である場合に、ハンドオーバーを行い、前記第1臨界値は、前記第2臨界値よりも高く設定される、こととを含む、

前記事前認証結果情報は、第1タイプターゲットネットワークの場合に、HSS(Ho me Subscriber Server)から抽出された前記マルチモードMSに対するセキュリティ情報を含み、前記事前認証結果情報は、第2タイプターゲットネットワークの場合に、前記HSSから抽出された前記マルチモードMSに対する前記セキュリティ情報を省略し、

20

前記現在接続ネットワークの識別子(ID)及び前記現在接続ネットワークの認証サーバのIDは、前記事前認証要請メッセージ及び前記事前認証結果情報から除外され、

前記マルチモードMSのIDは、前記方法を行うときに露出されず、前記マルチモードMSのIDは、IMSI(International Mobile Subscriber Identity)、TMSI(Temporary Mobile Subscriber Identity)またはMAC(Media Access Control)アドレスを含む、方法。

30

【請求項9】

前記事前認証要請メッセージを受信すること、及び前記事前認証結果情報を伝送することのうちの少なくとも一つは、MIH(Media Independent Hand over)プリミティブを用いて行われる、請求項8に記載の方法。

【請求項10】

前記事前認証要請メッセージの受信及び前記事前認証結果情報の伝送は、前記特定接続ネットワークのMIHエンティティにより行われ、

前記方法は、

前記特定接続ネットワークのMIHエンティティが前記事前認証要請メッセージを受信した後に、前記事前認証要請メッセージを前記特定接続ネットワークのセキュリティエンティティを通じて前記特定接続ネットワークの認証サーバに伝送することと、

40

前記MIHエンティティが前記事前認証結果情報を伝送する前に、前記事前認証結果情報を前記セキュリティエンティティから受信することとをさらに含む、請求項9に記載の方法。

【請求項11】

特定接続ネットワークにより異種無線アクセスネットワーク間のハンドオーバーを支援する方法であって、マルチモード移動局(MS)が前記特定接続ネットワークと異なるターゲット接続ネットワークに対して前記ハンドオーバーを行い、

前記方法は、

50

前記マルチモードMSから事前認証要請メッセージを受信することであって、前記事前認証要請メッセージは、前記特定接続ネットワークから前記マルチモードMSにより受信された信号レベルが第1臨界値未満である場合に、前記マルチモードMSから伝送される、ことと、

前記事前認証要請メッセージに応答して、事前認証結果情報を前記ターゲット接続ネットワークに伝送することと、

前記ターゲット接続ネットワークから、前記事前認証結果情報に応答して、応答メッセージを受信することと、

事前認証応答メッセージを前記マルチモードMSに伝送することであって、前記事前認証応答メッセージは、前記事前認証結果情報及び前記ターゲット接続ネットワークの応答メッセージに関する情報を含む、ことと、

10

前記事前認証結果情報を用いて前記マルチモードMSが前記ターゲット接続ネットワークへのハンドオーバーを行うことを、追加的な認証手順無しで支援することであって、前記マルチモードMSは、前記特定接続ネットワークから前記マルチモードMSにより受信された信号レベルが第2臨界値未満である場合に、ハンドオーバーを行い、前記第1臨界値は、前記第2臨界値よりも高く設定される、こととを含む、

前記事前認証結果情報は、第1タイプターゲットネットワークの場合に、HSS (Home Subscriber Server) から抽出された前記マルチモードMSに対するセキュリティ情報を含む、前記事前認証結果情報は、第2タイプターゲットネットワークの場合に、前記HSSから抽出された前記マルチモードMSに対する前記セキュリティ情報を省略し、

20

前記特定接続ネットワークの識別子(ID)及び前記特定接続ネットワークの認証サーバのIDは、前記事前認証要請メッセージ及び前記事前認証結果情報から除外され、

前記マルチモードMSのIDは、前記方法を行うときに露出されず、前記マルチモードMSのIDは、IMSI (International Mobile Subscriber Identity)、TMSI (Temporary Mobile Subscriber Identity) またはMAC (Media Access Control) アドレスを含む、方法。

【請求項12】

30

前記事前認証要請メッセージを受信すること、前記事前認証結果情報を伝送すること、前記応答メッセージを受信すること、及び前記事前認証応答メッセージを伝送することのうちの少なくとも一つは、MIH (Media Independent Handover) プリミティブを用いて行われる、請求項11に記載の方法。

【請求項13】

前記事前認証要請メッセージを受信すること、前記事前認証結果情報を伝送すること、前記応答メッセージを受信すること、及び前記事前認証応答メッセージを伝送することは、前記特定接続ネットワークのMIHエンティティにおいて行われ、

前記方法は、

前記特定接続ネットワークのMIHエンティティが前記事前認証要請メッセージを受信した後に、前記事前認証要請メッセージを前記特定接続ネットワークのセキュリティエンティティを通じて前記ターゲット接続ネットワークの認証サーバに伝送することと、

40

前記MIHエンティティが前記事前認証結果情報を前記ターゲット接続ネットワークに伝送する前に、前記事前認証結果情報を前記セキュリティエンティティから受信することと

をさらに含む、請求項12に記載の方法。

【請求項14】

前記特定接続ネットワークのMIHエンティティは、MIH事前認証指示プリミティブを用いて、前記事前認証要請メッセージを前記セキュリティエンティティに伝送し、前記事前認証結果情報を受信することは、MIH事前認証結果要請プリミティブを用いて行わ

50

れ、

前記M I H事前認証指示プリミティブは、

前記ターゲット接続ネットワークのI D、前記ターゲット接続ネットワークの認証サーバのI D、前記マルチモードM SのI D及び事前認証要請指示子のうちの少なくとも一つを含み、

前記M I H事前認証結果伝達要請プリミティブは、

前記特定接続ネットワークのI D、前記特定接続ネットワークの認証サーバのI D、前記ターゲット接続ネットワークのI D、前記ターゲット接続ネットワークの認証サーバのI D、事前認証結果状態情報、前記マルチモードM SのI D、再認証用I D及び前記ターゲット接続ネットワークの認証手段により用いられるセキュリティコンテキストのうちの少なくとも一つを含む、請求項13に記載の方法。

10

【請求項15】

前記応答メッセージを受信することは、M I H事前認証結果伝達応答プリミティブを用いて行われ、

前記M I H事前認証結果伝達応答プリミティブは、

前記ターゲット接続ネットワークのI D、前記ターゲット接続ネットワークの認証サーバのI D、前記ターゲット接続ネットワークH S S (Home Subscriber Server)のI D、前記マルチモードM SのI D、再認証用I D、前記ターゲット接続ネットワークの認証手段により用いられるセキュリティコンテキストのうち獲得されなかった情報リスト及び事前認証結果伝達状態指示子のうちの少なくとも一つを含む、請求項13に記載の方法。

20

【発明の詳細な説明】

【技術分野】

【0001】

本発明は異種無線アクセスネットワーク間におけるハンドオーバー方法に関し、より具体的には、事前認証手順を用いて異種無線アクセスネットワーク間におけるハンドオーバーを効率的行う方法に関する。

【背景技術】

【0002】

通信中の移動端末(Mobile Terminal)が一つの無線アクセスネットワークから他の無線アクセスネットワークへと移動することでアクセスポイントが変わる場合、ハンドオーバー(Handover)動作によってサービス連続性が損なわれることがある。アクセスポイントの変更とは、管理ドメイン(Administrative domain)の変更やサブネットの変更のことをいう。特に、異種無線アクセスネットワーク間におけるハンドオーバーでは、新しい認証手順を伴うこととなり、このような認証手順の実行に起因する遅延は、ハンドオーバー手順の終了を遅らせ、現在サービス中のマルチメディアセッションに影響を与える結果を招く。

30

【0003】

一方、異種ネットワーク間におけるハンドオーバーについては、現在、IEEE 802.21標準で活発に議論されている。MIH(Media Independent Handover)に対するIEEE 802.21標準の範囲は、リンク層に知能性を提供し、かつ、異種(Heterogeneous)ネットワーク間におけるハンドオーバーを最適化するために関連のネットワーク情報を上位層に伝達する規格を確立するためのものである。これは、3GPP/3GPP2により明示されたリンクだけでなく、IEEE 802シリーズ(以下、“802シリーズ”とも略す。)の有無線ネットワークを含む。すなわち、IEEE 802.21標準は、異種ネットワーク間におけるハンドオーバー(以下、“Inter-RATハンドオーバー”とも略す。)を支援することによってユーザの便宜を向上させることを目的とし、端末とネットワークにおいて使用可能な情報の協力的な使用を支援する。このために、移動端末、基地局のようなネットワークのアクセスポイント(Access Point)は、多重モード(Multi-Moda

40

50

1)を提供しなければならないが、これは、複数の無線標準を支援し、同時に一つ以上の無線インターフェース上の連結を許容するということを意味する。

【0004】

IEEE 802.21標準により定義されるMIH機能(Function)は、論理的な個体としてハンドオーバー決定をする役目を果たす。このMIH機能は、移動端末とネットワークの両方に設けられ、移動端末とネットワークが、移動端末周囲の接続ネットワーク(Access Network)に対する設定や状態に関する情報を交換できるようにする。このようなMIH機能は、場合によって、他の機能を実行するエンティティ(Entity)との区別のために“MIHエンティティ”と呼ばれることもできる。

【0005】

図1は、マルチモード移動端末、802シリーズネットワーク及び3GPP/3GPP2ネットワークのプロトコル層の構成図である。

【0006】

マルチモード移動端末101は、通信モード別インターフェースを含むことができ、図1は、3GPP/3GPP2インターフェース104及び802シリーズインターフェース105を含むものを示している。また、これらのインターフェースは、物理層(PHY: Physical Layer)と媒体接近制御層(MAC: Medium Access Control Layer)とに区分することができる。なお、図1は、802シリーズネットワーク102及び3GPP/3GPP2ネットワーク103がそれぞれ、インターフェース106及び107を含んでいるものを示している。

【0007】

一方、MIH機能108、109、110として表されるMIH層は、IP層を含む上位層の下に位置し、802シリーズインターフェース間におけるハンドオーバーだけでなく、IEEE802シリーズインターフェース及び3GPP/3GPP2により定義されたインターフェース相互間におけるハンドオーバーも定義する。すなわち、MIHは、他のネットワークについての情報を第2層(例えば、MAC層)から獲得し、異種ネットワーク間におけるハンドオーバー処理過程を容易にする。

【0008】

また、図1は、移動端末101、802シリーズネットワーク102及び3GPP/3GPP2ネットワーク103の上位層機能111、112、113を示しており、これら上位層機能111、112、113を、MIHの観点でMIHユーザ(MIH user)またはMIHユーザエンティティと呼ぶことができる。

【0009】

図2は、MIHベースのマルチモード移動端末による異種無線アクセスネットワーク間におけるハンドオーバー手順を示す。

【0010】

図2では、現在接続ネットワークのマルチモード移動端末201が、ネットワークX(202)によりサービスを受ける中に、ターゲット接続ネットワークのネットワークY(203)にハンドオーバーを行う過程を説明している。また、移動端末201において、MAC1(201c)はネットワークX(202)と、MAC2(201d)はネットワークY(203)とそれぞれ第2層通信を行うエンティティとする。

【0011】

まず、ネットワークX(202)と連結を維持しながら通信中にあるマルチモード移動端末201は、ネットワークX(202)から隣のネットワーク(例えば、ネットワークY(203))情報を獲得する(S201)。この時、MIH機能で定義する情報サービスを通じて認証方法、暗号化アルゴリズムなどを含む第2層のセキュリティと関連した情報を獲得することができる。その後、移動端末201は、スキニングを通じて隣のネットワークから信号を受信し、ネットワーク発見及び選択手順を行う(S202)。

【0012】

一方、サービングネットワークX(202)から受信する信号レベルが一定レベル以下

10

20

30

40

50

に落ちる場合、移動端末201のインターフェースMAC1(201c)は、これを、上位層MIH(201b)にローカルイベントトリガーを通じて報告し、遠隔イベントトリガーを通じてネットワークX(202)のMIH(202b)に知らせる(S203)。これにより、ネットワークX(202)のMIH(202b)は、ハンドオーバーするネットワークY(203)のMIH(203b)にIP情報を要請し(S204)、これを受信したネットワークY(203)は、IP情報をネットワークX(202)を介して移動端末201に伝達する(S205)。このようにしてネットワークY(203)のIP情報を受信した移動端末201は、これに基づいて、該当のネットワークへのハンドオーバー時に使用するIPアドレスをあらかじめ獲得することができる。

【0013】

10

その後、移動端末201のMIH(201b)は、ネットワークY(203)へのハンドオーバーのために、該当のインターフェースのMAC(すなわち、MAC2(201d))に第2層ハンドオーバーのための手順を行うように命令する(S206)。続いて、移動端末201は、ネットワークY(203)と認証及びセキュリティ連携手順を含むネットワーク初期登録手順を行うことによってネットワークY(203)への第2層ハンドオーバー手順を行う(S207及びS208)。

【0014】

移動端末201がネットワークY(203)との第2層ハンドオーバー(ネットワーク登録手順)を完了すると、移動端末201のMAC2(201d)は、第3層ハンドオーバー実行のために、それを上位層201aに報告する(S209)。すると、移動端末201は、新しいネットワーク(ネットワークY; 203)から獲得したCoA(Care-of-Address)をホームエージェント(Home Agent)に登録する手順を含む第3層ハンドオーバーを行い、ハンドオーバーが完了すると、新しいネットワークと通信を再開する(S210)。その後、移動端末201は、以前ネットワーク(ネットワークX; 202)との連結を解除する(S211)。

20

【0015】

このように、従来技術として明示されたIEEE 802.21で定義するマルチモード移動端末のInter-RATハンドオーバーは、移動端末が新しいネットワークと第2層ハンドオーバーを行う過程において、認証及び暗号化キー獲得手順を新しく行うように定義している。これは、ユーザのサービスに少なからず遅延を招くと予想され、データ損失につながる可能性もある。

30

【発明の概要】

【発明が解決しようとする課題】

【0016】

上述したような問題を解決するために、本発明は、マルチモード端末がInter-RATハンドオーバーを行う場合に、ハンドオーバーするターゲットアクセスポイントとリンク層ハンドオーバー手順を行う前にあらかじめ認証を行うことによって、現在受けているサービス品質に最小限の影響を与える事前認証方法を提供し、これを用いて効率的にハンドオーバーを行う方法を提供することを目的とする。

【0017】

40

本発明の他の目的は、異種ネットワーク間における異なる認証タイプ及び異なる認証性能などを考慮して上記の事前認証手順をMIHに基づいて行う方法を提供することにある。そのために、特定手順で必要な様々なMIHプリミティブを定義することによって、本発明で提案する事前認証方法を容易に行う。

【課題を解決するための手段】

【0018】

上記課題を解決するための本発明の一様態では、マルチモード移動端末が、異種無線アクセスネットワーク間におけるハンドオーバーを行う方法を提供する。この方法は、マルチモード移動端末が接続している現在接続ネットワークの他に、一つ以上の候補ターゲット接続ネットワークに関する情報を獲得するステップと、候補ターゲット接続ネットワー

50

クのうち、選択されたターゲット接続ネットワークに直接または間接的に事前認証要請メッセージを送信するステップと、ターゲット接続ネットワークから直接または間接的に事前認証要請メッセージ伝送について行われた事前認証結果情報を受信するステップと、事前認証結果情報を用いて追加的な認証手順無しでターゲット接続ネットワークにハンドオーバーを行うステップと、を含む。

【0019】

ここで、一つ以上の候補ターゲット接続ネットワークに関する情報の獲得、事前認証要請メッセージの伝送及び事前認証結果情報の受信のうち一つ以上は、MIH (Media Independent Handover) プリミティブ (Primitive) により行うことができる。

10

【0020】

特に、事前認証要請メッセージの伝送を、MIH事前認証要請プリミティブを用いて行う場合、MIH事前認証要請プリミティブは、現在接続ネットワークの識別子、現在接続ネットワーク認証サーバの識別子、ターゲット接続ネットワークの識別子、ターゲット接続ネットワーク認証サーバの識別子、マルチモード移動端末の識別子及び事前認証要請指示子のうち一つ以上を含むことができる。

【0021】

また、事前認証結果情報の受信を、MIH事前認証応答プリミティブを用いて行う場合、MIH事前認証応答プリミティブは、現在接続ネットワークの識別子、現在接続ネットワーク認証サーバの識別子、ターゲット接続ネットワークの識別子、ターゲット接続ネットワーク認証サーバの識別子、ターゲット接続ネットワークHSS (Home Subscriber Server) 識別子、事前認証結果状態識別子及び事前認証結果伝送状態識別子のうち一つ以上を含むことができる。

20

【0022】

具体的なパラメータの選択は、事前認証要請プリミティブ及び／またはMIH事前認証応答プリミティブが、現在接続ネットワークを介してターゲット接続ネットワークに伝達されるか、ターゲット接続ネットワークに直接伝達されるか、ターゲット接続ネットワークがどのタイプの接続ネットワークであるか等によって決定されることができる。

【0023】

また、事前認証要請メッセージの伝送及び事前認証結果情報の受信が間接的に行われる場合、事前認証要請メッセージ及び事前認証結果情報は、現在接続ネットワークを介して伝送及び受信されることができる。

30

【0024】

特に、事前認証要請メッセージの伝送及び事前認証結果情報の受信を、マルチモード移動端末のMIHエンティティ (entity) により行うことができ、この場合、異種無線アクセスネットワーク間におけるハンドオーバー方法は、マルチモード移動端末のMIHエンティティが事前認証要請メッセージを送信する前に、マルチモード移動端末のMIHエンティティが、マルチモード移動端末のMIHユーザ (MIH user) エンティティから事前認証要請メッセージを受信するステップと、マルチモード移動端末のMIHエンティティが事前認証結果情報を受信した後、マルチモード移動端末のMIHエンティティが、受信した事前認証結果情報をマルチモード移動端末のMIHユーザエンティティに通報するステップと、をさらに含むことができる。

40

【0025】

また、この場合、事前認証結果情報をマルチモード移動端末のMIHユーザエンティティに通報することは、MIH事前認証確認プリミティブを用いて行うことができ、MIH事前認証確認プリミティブは、現在接続ネットワークの識別子、現在接続ネットワーク認証サーバの識別子、ターゲット接続ネットワークの識別子、ターゲット接続ネットワーク認証サーバの識別子、事前認証結果状態識別子及び事前認証結果伝送状態識別子のうち一つ以上を含むことができる。

【0026】

50

一方、本発明の他の様態では、特定接続ネットワークにより、マルチモード移動端末が、特定接続ネットワークをターゲット接続ネットワークとして異種無線アクセスネットワーク間におけるハンドオーバーを行うことを支援する方法を提供する。この方法は、マルチモード移動端末から事前認証要請メッセージを受信するステップと、事前認証要請メッセージ受信について行われた事前認証結果情報を、マルチモード移動端末に伝送するステップと、事前認証結果情報を用いてマルチモード移動端末が特定接続ネットワークをターゲット接続ネットワークとしてハンドオーバーを行うことを、追加的な認証手順無しで支援するステップと、を含む。

【0027】

好適には、事前認証要請メッセージの受信及び事前認証結果情報の伝送のうち一つ以上は、MIH (Media Independent Handover) プリミティブ (Primitive) を用いて行う。

10

【0028】

さらに好適には、事前認証要請メッセージの受信及び事前認証結果情報の伝送を、特定接続ネットワークのMIHエンティティ (Entity) により行うことができ、この場合、異種無線アクセスネットワーク間におけるハンドオーバー支援方法は、特定接続ネットワークのMIHエンティティが事前認証要請メッセージを受信した後、事前認証要請メッセージに関する情報を特定接続ネットワークのセキュリティエンティティ (Security Entity) を介して特定接続ネットワークの認証サーバ (AAA Server) に伝達するステップと、特定接続ネットワークのMIHエンティティが事前認証結果情報を伝送する前に、事前認証結果情報を特定接続ネットワークのセキュリティエンティティ (Security Entity) から受信するステップと、をさらに含むことができる。

20

【0029】

一方、本発明のさらに他の様態では、特定接続ネットワークにより、マルチモード移動端末が特定接続ネットワークと異なるターゲット接続ネットワークに異種無線アクセスネットワーク間におけるハンドオーバーを行うことを支援する方法を提供する。この方法は、マルチモード移動端末から事前認証要請メッセージを受信するステップと、事前認証要請メッセージ受信について行われた事前認証結果情報を、ターゲット接続ネットワークに伝送するステップと、ターゲット接続ネットワークから事前認証結果情報伝送に対する応答メッセージを受信するステップと、事前認証結果情報及びターゲット接続ネットワークの応答メッセージに関する情報を含む事前認証応答メッセージを、マルチモード移動端末に伝送するステップと、を含む。

30

【0030】

好適には、事前認証要請メッセージの受信、事前認証結果情報の伝送、事前認証結果情報伝送に対する応答メッセージ受信及び事前認証応答メッセージの伝送のうち一つ以上は、MIH (Media Independent Handover) プリミティブ (Primitive) を用いて行うことが好ましい。

【0031】

更に好適には、事前認証要請メッセージの受信、事前認証結果情報の伝送、事前認証結果情報伝送に対する応答メッセージ受信及び事前認証応答メッセージの伝送を、特定接続ネットワークのMIHエンティティ (Entity) により行うことができ、この場合、異種無線アクセスネットワーク間におけるハンドオーバー支援方法は、特定接続ネットワークのMIHエンティティがマルチモード移動端末から事前認証要請メッセージを受信した後、事前認証要請メッセージに関する情報を、特定接続ネットワークのセキュリティエンティティ (Security Entity) を介してターゲット接続ネットワークの認証サーバ (AAA Server) に伝達するステップと、特定接続ネットワークのMIHエンティティが事前認証結果情報をターゲット接続ネットワークに伝送する前に、事前認証結果情報を特定接続ネットワークのセキュリティエンティティから受信するステップと、をさらに含むことができる。

40

50

【0032】

また、特定接続ネットワークのM I Hエンティティが事前認証要請メッセージに関する情報を特定接続ネットワークのセキュリティエンティティに伝達することは、M I H事前認証指示プリミティブを用いて行うことができ、この時、M I H事前認証指示プリミティブは、特定接続ネットワークの識別子、特定接続ネットワーク認証サーバの識別子、ターゲット接続ネットワークの識別子、ターゲット接続ネットワーク認証サーバの識別子、マルチモード移動端末の識別子及び事前認証要請指示子のうち一つ以上を含むことができる。

【0033】

また、特定接続ネットワークのM I Hエンティティが事前認証結果情報を特定接続ネットワークのセキュリティエンティティから受信することは、M I H事前認証結果伝達要請プリミティブを用いて行うことができ、この時、M I H事前認証結果伝達要請プリミティブは、特定接続ネットワークの識別子、特定接続ネットワーク認証サーバの識別子、ターゲット接続ネットワークの識別子、ターゲット接続ネットワーク認証サーバの識別子、事前認証結果状態情報、マルチモード移動端末の識別子、再認証用I D及びターゲット接続ネットワークの認証手段により用いられるセキュリティコンテキストのうち一つ以上を含むことができる。

【0034】

なお、特定接続ネットワークのM I Hエンティティがターゲット接続ネットワークから事前認証結果情報伝送に対する応答メッセージを受信することは、M I H事前認証結果伝達応答プリミティブを用いて行うことができ、この時、M I H事前認証結果伝達応答プリミティブは、ターゲット接続ネットワークの識別子、ターゲット接続ネットワーク認証サーバの識別子、ターゲット接続ネットワークH S S (Home Subscriber Server) の識別子、マルチモード移動端末の識別子、再認証用I D、ターゲット接続ネットワークの認証手段により用いられるセキュリティコンテキストのうち獲得されなかった情報リスト、及び事前認証結果伝達状態指示子のうち一つ以上を含むことができる。

本願明細書は、例えば、以下の項目も提供する。

(項目1)

マルチモード移動端末が異種無線アクセスネットワーク間におけるハンドオーバーを行う方法であって、

前記マルチモード移動端末が接続している現在接続ネットワーク以外に一つ以上の候補ターゲット接続ネットワークに関する情報を獲得し、

前記候補ターゲット接続ネットワークのうち、選択されたターゲット接続ネットワークに直接または間接的に事前認証要請メッセージを送信し、

前記ターゲット接続ネットワークから直接または間接的に前記事前認証要請メッセージ伝送について行われた事前認証結果情報を受信し、

前記事前認証結果情報を用いて追加的な認証手順無しで前記ターゲット接続ネットワークにハンドオーバーを行うこと、

を含む、異種無線アクセスネットワーク間におけるハンドオーバー方法。

(項目2)

前記一つ以上の候補ターゲット接続ネットワークに関する情報の獲得、前記事前認証要請メッセージの伝送及び前記事前認証結果情報の受信のうち一つ以上は、M I H (Media Independent Handover) プリミティブ (Primitive) により行う、項目1に記載の異種無線アクセスネットワーク間におけるハンドオーバー方法。

(項目3)

前記事前認証要請メッセージの伝送は、M I H事前認証要請プリミティブを用いて行い、

前記M I H事前認証要請プリミティブは、

10

20

30

40

50

前記現在接続ネットワークの識別子、前記現在接続ネットワーク認証サーバの識別子、前記ターゲット接続ネットワークの識別子、前記ターゲット接続ネットワーク認証サーバの識別子、前記マルチモード移動端末の識別子及び事前認証要請指示子のうち一つ以上を含む、項目 2 に記載の異種無線アクセスネットワーク間におけるハンドオーバー方法。

(項目 4)

前記事前認証結果情報の受信は、M I H 事前認証応答プリミティブを用いて行い、

前記 M I H 事前認証応答プリミティブは、

前記現在接続ネットワークの識別子、前記現在接続ネットワーク認証サーバの識別子、前記ターゲット接続ネットワークの識別子、前記ターゲット接続ネットワーク認証サーバの識別子、前記ターゲット接続ネットワーク H S S (Home Subscriber S e r v e r) 識別子、事前認証結果状態識別子及び事前認証結果伝送状態識別子のうち一つ以上を含む、項目 2 に記載の異種無線アクセスネットワーク間におけるハンドオーバー方法。

(項目 5)

前記事前認証要請メッセージの伝送及び前記事前認証結果情報の受信が間接的に行われる場合、前記事前認証要請メッセージ及び前記事前認証結果情報は、前記現在接続ネットワークを通じて行われる、項目 1 に記載の異種無線アクセスネットワーク間におけるハンドオーバー方法。

(項目 6)

前記事前認証要請メッセージの伝送及び前記事前認証結果情報の受信は、前記マルチモード移動端末の M I H エンティティ (e n t i t y) により行われ、

前記異種無線アクセスネットワーク間におけるハンドオーバー方法は、

前記マルチモード移動端末の M I H エンティティが前記事前認証要請メッセージを送信する前に、前記マルチモード移動端末の M I H エンティティが前記マルチモード移動端末の M I H ユーザ (M I H u s e r) エンティティから前記事前認証要請メッセージを受信し、

前記マルチモード移動端末の M I H エンティティが前記事前認証結果情報を受信した後、前記マルチモード移動端末の M I H エンティティが、受信した前記事前認証結果情報を前記マルチモード移動端末の M I H ユーザエンティティに通報すること、

をさらに含む、項目 1 に記載の異種無線アクセスネットワーク間におけるハンドオーバー方法。

(項目 7)

前記事前認証結果情報を前記マルチモード移動端末の M I H ユーザエンティティに通報することは、M I H 事前認証確認プリミティブを用いて行い、

前記 M I H 事前認証確認プリミティブは、

前記現在接続ネットワークの識別子、前記現在接続ネットワーク認証サーバの識別子、前記ターゲット接続ネットワークの識別子、前記ターゲット接続ネットワーク認証サーバの識別子、事前認証結果状態識別子及び事前認証結果伝送状態識別子のうち一つ以上を含む、項目 6 に記載の異種無線アクセスネットワーク間におけるハンドオーバー方法。

(項目 8)

特定接続ネットワークが、マルチモード移動端末が前記特定接続ネットワークをターゲット接続ネットワークとして異種無線アクセスネットワーク間におけるハンドオーバーを行うことを支援する方法であって、

前記マルチモード移動端末から事前認証要請メッセージを受信し、

前記事前認証要請メッセージ受信について行われた事前認証結果情報を前記マルチモード移動端末に伝送し、

前記事前認証結果情報を用いて前記マルチモード移動端末が前記特定接続ネットワークを前記ターゲット接続ネットワークとしてハンドオーバーを行うことを、追加的な認証手順無しで支援すること、

を含む、異種無線アクセスネットワーク間におけるハンドオーバー支援方法。

10

20

30

40

50

(項目 9)

前記事前認証要請メッセージの受信及び前記事前認証結果情報の伝送のうち一つ以上は、MIH (Media Independent Handover) プリミティブ (Primitive) を用いて行う、項目 8 に記載の異種無線アクセスネットワーク間におけるハンドオーバー支援方法。

(項目 10)

前記事前認証要請メッセージの受信及び前記事前認証結果情報の伝送は、前記特定接続ネットワークのMIHエンティティ (Entity) により行われ、

前記異種無線アクセスネットワーク間におけるハンドオーバー支援方法は、

前記特定接続ネットワークのMIHエンティティが前記事前認証要請メッセージを受信した後、前記事前認証要請メッセージに関する情報を前記特定接続ネットワークのセキュリティエンティティ (Security Entity) を通じて前記特定接続ネットワークの認証サーバ (AAA Server) に伝達し、

前記特定接続ネットワークのMIHエンティティが前記事前認証結果情報を伝送する前に、前記事前認証結果情報を前記特定接続ネットワークのセキュリティエンティティ (Security Entity) から受信すること、

をさらに含む、項目 9 に記載の異種無線アクセスネットワーク間におけるハンドオーバー支援方法。

(項目 11)

特定接続ネットワークが、マルチモード移動端末が前記特定接続ネットワークと異なるターゲット接続ネットワークに異種無線アクセスネットワーク間におけるハンドオーバーを行うことを支援する方法であって、

前記マルチモード移動端末から事前認証要請メッセージを受信し、

前記事前認証要請メッセージ受信について行われた事前認証結果情報を前記ターゲット接続ネットワークに伝達し、

前記ターゲット接続ネットワークから前記事前認証結果情報伝送に対する応答メッセージを受信し、

前記事前認証結果情報及び前記ターゲット接続ネットワークの応答メッセージに関する情報を含む事前認証応答メッセージを前記マルチモード移動端末に伝送すること、

を含む、異種無線アクセスネットワーク間におけるハンドオーバー支援方法。

(項目 12)

前記事前認証要請メッセージの受信、前記事前認証結果情報の伝送、前記事前認証結果情報伝送に対する応答メッセージ受信及び前記事前認証応答メッセージの伝送のうち一つ以上は、MIH (Media Independent Handover) プリミティブ (Primitive) を用いて行う、項目 11 に記載の異種無線アクセスネットワーク間におけるハンドオーバー支援方法。

(項目 13)

前記事前認証要請メッセージの受信、前記事前認証結果情報の伝送、前記事前認証結果情報伝送に対する応答メッセージ受信及び前記事前認証応答メッセージの伝送は、前記特定接続ネットワークのMIHエンティティ (Entity) により行われ、

前記異種無線アクセスネットワーク間におけるハンドオーバー支援方法は、

前記特定接続ネットワークのMIHエンティティが前記マルチモード移動端末から事前認証要請メッセージを受信した後、前記事前認証要請メッセージに関する情報を前記特定接続ネットワークのセキュリティエンティティ (Security Entity) を通じて前記ターゲット接続ネットワークの認証サーバ (AAA Server) に伝達し、

前記特定接続ネットワークのMIHエンティティが前記事前認証結果情報を前記ターゲット接続ネットワークに伝送する前に、前記事前認証結果情報を前記特定接続ネットワークのセキュリティエンティティから受信すること、

をさらに含む、項目 12 に記載の異種無線アクセスネットワーク間におけるハンドオーバー支援方法。

10

20

30

40

50

(項目 1 4)

前記特定接続ネットワークの M I H エンティティが前記事前認証要請メッセージに関する情報を前記特定接続ネットワークのセキュリティエンティティに伝達することは、M I H 事前認証指示プリミティブを用いて行い、

前記 M I H 事前認証指示プリミティブは、

前記特定接続ネットワークの識別子、前記特定接続ネットワーク認証サーバの識別子、前記ターゲット接続ネットワークの識別子、前記ターゲット接続ネットワーク認証サーバの識別子、前記マルチモード移動端末の識別子及び事前認証要請指示子のうち一つ以上を含む、項目 1 3 に記載の異種無線アクセスネットワーク間におけるハンドオーバー支援方法。

10

(項目 1 5)

前記特定接続ネットワークの M I H エンティティが前記事前認証結果情報を前記特定接続ネットワークのセキュリティエンティティから受信することは、M I H 事前認証結果伝達要請プリミティブを用いて行い、

前記 M I H 事前認証結果伝達要請プリミティブは、

前記特定接続ネットワークの識別子、前記特定接続ネットワーク認証サーバの識別子、前記ターゲット接続ネットワークの識別子、前記ターゲット接続ネットワーク認証サーバの識別子、事前認証結果状態情報、前記マルチモード移動端末の識別子、再認証用 I D 及び前記ターゲット接続ネットワークの認証手段により用いられるセキュリティコンテキストのうち一つ以上を含む、項目 1 3 に記載の異種無線アクセスネットワーク間におけるハンドオーバー支援方法。

20

(項目 1 6)

前記特定接続ネットワークの M I H エンティティが前記ターゲット接続ネットワークから前記事前認証結果情報伝送に対する応答メッセージを受信することは、M I H 事前認証結果伝達応答プリミティブを用いて行い、

前記 M I H 事前認証結果伝達応答プリミティブは、

前記ターゲット接続ネットワークの識別子、前記ターゲット接続ネットワーク認証サーバの識別子、前記ターゲット接続ネットワーク H S S (H o m e S u b s c r i b e r S e r v e r) の識別子、前記マルチモード移動端末の識別子、再認証用 I D、前記ターゲット接続ネットワークの認証手段により用いられるセキュリティコンテキストのうち獲得されなかった情報リスト及び事前認証結果伝達状態指示子のうち一つ以上を含む、項目 1 3 に記載の異種無線アクセスネットワーク間におけるハンドオーバー支援方法。

30

【発明の効果】**【0035】**

本発明の各実施形態によると、マルチモード端末が I n t e r - R A T ハンドオーバーを行う場合に、ハンドオーバーするターゲットアクセスポイントとリンク層ハンドオーバー手順を行う前にあらかじめ認証を行うことによって、現在受けているサービス品質に最小限の影響を与える事前認証方法及びこれを用いた効率的なハンドオーバー方法を提供することができる。

40

【図面の簡単な説明】**【0036】**

【図 1】マルチモード移動端末、802 シリーズネットワーク及び 3 G P P / 3 G P P 2 ネットワークのプロトコル層の構成図である。

【図 2】M I H ベースのマルチモード移動端末による異種無線アクセスネットワーク間におけるハンドオーバー手順を示す図である。

【図 3】本発明の一実施形態によって、I E E E 802.16 ネットワークによりサービスを受けるマルチモード移動端末が、現在接続ネットワークを介して事前認証を行った後、他の I E E E 802 シリーズネットワークに i n t e r - R A T ハンドオーバーを行う過程を示す図である。

50

【図4】本発明の他の実施形態によって、I E E E 802.16ネットワークによりサービスを受けるマルチモード移動端末が、現在接続ネットワークの関与無しに直接ターゲットネットワークと事前認証を行った後、I E E E 802シリーズネットワークにinter-RATハンドオーバーを行う過程を示す図である。

【図5】本発明のさらに他の実施形態によって、移動端末がI E E E 802シリーズネットワークから3GPPネットワークにハンドオーバーする場合、事前認証を行う方法を示す図である。

【図6】本発明のさらに他の実施形態によって、移動端末がI E E E 802シリーズネットワークから3GPPネットワークにハンドオーバーする場合、事前認証を行う方法を示す図である。

【発明を実施するための形態】

【0037】

以下、本発明の好適な実施形態を、添付の図面を参照しつつ詳細に説明する。添付の図面と共に以下に開示される詳細な説明は、本発明の例示的な実施形態を説明するためのもので、本発明が実施されうる唯一の実施形態を表すためのものではない。以下の詳細な説明は、本発明の完全な理解を提供するために具体的細部事項を含む。しかし、このような具体的細部事項なしにも本発明を実施できるということが当業者には理解できる。例えば、以下の詳細な説明は、現在接続ネットワークがI E E E 802.16システムであり、且つ、ターゲット接続ネットワークが他の任意の802シリーズシステムであるまたは3GPP/3GPP2システムである場合を取り上げて重点的に説明するが、任意の他の異種ネットワーク間におけるハンドオーバーにも、以下に説明する事前認証方法及びこれを用いたハンドオーバー方法を同一原理に基づいて適用することができる。

【0038】

一方、場合によっては、本発明の概念が曖昧になるのを避けるために、公知の構造及び装置は省略されたり、各構造及び装置の核心機能を中心にしたブロック図の形式で図示されることができる。また、本明細書全体にわたって同一の構成要素には同一の図面符号を付して説明する。

【0039】

上述の通り、本発明は、マルチモード端末がinter-RATハンドオーバーを行う場合に、ハンドオーバーするターゲットアクセスポイントとリンク層ハンドオーバー手順を行う前にあらかじめ認証を行うことによって、現在受けているサービス品質に最小限の影響を与えるようにするためのMIHベースの事前認証方法に関する。単一管理ドメインを考慮する単一(Homogeneous)環境では、認証サーバ無しにハンドオーバーを支援することができる。ただし、複数の管理ドメインにより運用される異種(Heterogeneous)環境では、認証サーバが認証子(Authenticator)タイプと性能(Capability)によって異なる認証結果を生成するから、このような場合のための柔軟で効率的なセキュリティメカニズムの定義が必要とされる。例えば、EAPベース認証を採択するI E E E 802.11ネットワークとI E E E 802.16ネットワークとの間にハンドオーバーが発生する時、単一のサービスプロバイダにより両接続ネットワークが運用される場合には何ら問題もない。しかし、複数のサービスプロバイダにより異種無線アクセスネットワークが運用される場合は、認証サーバを介さないハンドオーバーメカニズムは存在せず、これについての解決策が提供されなければならない。

【0040】

本発明では、EAPを認証フレームワークとして採択するI E E E 802.16無線アクセスネットワークのマルチモード移動端末が、類似のEAPベース認証フレームワークを用いる無線RANのようなその他のI E E E 802シリーズの無線アクセスネットワークへとハンドオーバーしたり、EAPを基本的な認証フレームワークとして採択しない非I E E Eシリーズ無線アクセスネットワーク(例えば、3GPPネットワーク)へとハンドオーバーしたりする場合、端末がターゲットネットワークアクセスポイントにリンク

10

20

30

40

50

層ハンドオーバーを行う前に事前認証を行い、通信のためのキーイング情報（Keying Material）を設定する方法を提案する。これにより、マルチモード移動端末がInter-RATハンドオーバーを行う時、該当の端末に対して時間がかかる認証手順を新しいアクセスポイントに接続する前にあらかじめ行うことで通信のための速いセキュリティ連携を設定し、サービス品質の低下を減少させることができる。以下、本発明についての説明では、ハンドオーバーの始点となる接続ネットワークをIEEE 802.16ネットワークとするが、IEEE 802.16ネットワークに限定されず、いずれのIEEE 802シリーズのネットワーク（例えば、802.11）としても良い。

【0041】

本発明で提案する方法は、IEEE 802.21標準に適用されるのに適している。すなわち、現在まではIEEE 802.21標準にセキュリティ関連内容が言及されておらず、これを改善するための技術といえよう。ただし、以下に説明するMIHベース事前認証方法及びこれを用いたinter-RATハンドオーバー方法は、IEEE 802.21に限定されず、他の任意の標準でも適用されうるということは勿論である。

【0042】

本発明で提案する事前認証（Preauthentication）の基本概念は、端末が現在接続しているアクセスポイントだけでなく、隣接のアクセスポイントにも認証を要請し、あらかじめ一つ以上のアクセスポイントから認証を受けておくものである。すなわち、本発明で述べる事前認証は、従来の概念を拡張して、Inter-RATハンドオーバーが発生する場合、現在接続ネットワークではなく隣接のターゲット接続ネットワークからあらかじめ認証を受けることを意味する。これにより、事前認証の最終ステップにおいてターゲット接続ネットワーク認証子は、該当の移動端末と関連したキーイング情報を獲得でき、端末も、ハンドオーバー可能性のあるターゲット接続ネットワークからあらかじめ認証を受けると同時に、キーイング情報を獲得することとなる。

【0043】

本発明は、ハンドオーバー性能の向上のために、セキュリティメカニズムの最適化が異なる接続技術において普遍的な形態で提供されなければならないという点を目標とし、このため、上述のMIHの使用を考慮する。

【0044】

本発明における事前認証方法は、単一のサービスプロバイダ（管理ドメイン）により運用されるネットワーク間におけるInter-RATハンドオーバーを扱うのではなく、それぞれ異なるサービスプロバイダ（管理ドメイン）により運用されるネットワーク間におけるInter-RATハンドオーバーを扱う。すなわち、サービング認証子及びハンドオーバーが予想されるターゲット認証子は、異なるサービスプロバイダネットワークの相異なる接続技術に基づくと仮定する。このような状況で、本発明による事前認証の使用は、端末がターゲットアクセスポイントに接続するに先立ってあらかじめ認証を受け、通信のためのセキュリティキーを設定できるようにする。事前認証手順は、MIH機能の使用を仮定するので、接続技術にかかわらずに様々なシナリオに適用可能である。

【0045】

本発明では、マルチモード移動端末のMIHを通じて、異なる管理ドメインにより運用される異なるネットワーク間におけるInter-RATハンドオーバー時に事前認証手順を行うことによって、従来技術において初めから認証を新しく行うことから生じる負荷と遅延を低減し、速いハンドオーバー手順を可能にすることによって、実際サービス連続性のき損や、サービス品質の低下を減少させる方法を定義する。また、これは、Inter-RATハンドオーバー時にターゲットネットワークで用いられる通信のためのキーイング情報を、リンク層ハンドオーバーが完了する以前に、ターゲットネットワークの認証子及び移動端末に伝達する方法を含む。

【0046】

本発明は、上述の通り、IEEE 802.21標準に適用されるのに適している。すなわち、IEEE 802.21標準では、媒体独立ハンドオーバーのための認証及びセ

10

20

30

40

50

セキュリティ連携設定方法については述べていないので、本発明で述べられているように、I E E E 802.21 M I Hを通じて事前認証を行うことによって、異なるネットワーク間におけるI n t e r-R A Tハンドオーバーがされる場合に、サービス品質に影響を大きく与えないながらも、途切れないサービスの提供を可能にする。本発明は、同一のサービスプロバイダが運用するネットワーク間におけるI n t e r-R A Tハンドオーバーシナリオに適用するよりは、異なるサービスプロバイダが運用するネットワーク間におけるI n t e r-R A Tシナリオに適用することを目的とする。ただし、本発明で提案する内容は、I E E E 802.21以外の標準に適用される場合であっても同一効果を奏することができるということは、上述したとおりである。

【0047】

10

上述のように、本発明で提案する事前認証方法は、隣接ネットワーク探索や隣接ネットワーク相互間のローミング協約のような情報を得るためにI E E E 802.21情報サービスを使用することを基本前提とする。すなわち、移動端末は、自身の隣にどのような候補ネットワークがあるかを、I E E E 802.21情報サーバから獲得することができる。情報サーバから獲得した情報に基づいて、移動端末は、ターゲットアクセスポイントに接続する前に事前認証を完了し、キーイング情報をあらかじめ設定できるので、ハンドオーバー時に発生する遅延を低減することができる。

【0048】

I E E E 802.21標準には、I n t e r-R A Tのための媒体独立ハンドオーバー時に、認証及びキー交換方法などを含むセキュリティへの考慮がされることが好ましい。すなわち、ネットワークに深刻な負荷を招かずに、I n t e r-R A Tハンドオーバーを行う移動端末へ途切れないサービスを提供するための方法が要求される。

20

【0049】

以下では、先ず、本発明の一様態として、移動端末の立場で事前認証を行う方法及びそれを用いたハンドオーバー方法、サービングネットワーク及び／またはターゲットネットワークの立場で移動端末のi n t e r-R A Tハンドオーバーを支援する方法を行うために、本発明が提案する種々のM I Hプリミティブについて説明する。ただし、以下に説明する本発明に係るM I Hプリミティブは、当業者が本発明を容易に実施できるように具体的な細部事項を含むが、各プリミティブの名称、含む具体的な情報のうち選択的な事項については、以下の説明とは別に定義して実施することもできる。

30

【0050】

本発明では、移動端末がハンドオーバーしようとする一つ以上の隣接候補接続ネットワークのタイプやその他の関連情報を、I E E E 802.21標準で提供する次のようなプリミティブを用いて獲得することを考慮する。

【0051】

【表 1】

プリミティブ	説明
MIH_Information.Request	1) IEEE 802. 21 標準に定義されている遠隔 MIH プリミティブであり、移動端末の MIH から現在のサービングネットワークの MIH に伝達される。移動端末がハンドオーバーしようとするネットワークに関する情報を要請する時に使用され、該当のネットワークで支援する認証方式を把握するために用いることができる。 2) プリミティブ構成 <pre> MIH_Information.Request { InfoQueryFilter: 情報要請ネットワークのタイプ (例: 802、GSM、CDMA 等) InfoQueryParameters: 情報要請の具体的なパラメータ (例: リンク層情報、上位層情報、セキュリティ関連情報など) }</pre>
MIH_Information.Response	1) MIH_info.Request プリミティブに対する応答であり、MIH により使用され、ネットワークに関する情報を移動端末に提供する目的で使用される。使用可能なネットワークのリスト、地理的な位置情報、伝送技術情報、ネットワークプロバイダの識別子、ネットワークプロバイダ名、IP バージョン、ローミングパートナーリスト、サービスレベルリスト、隣接ネットワーク情報、リンク層セキュリティ情報、リンク層サービス品質パラメータ、ルーター情報などが含まれることができる。 2) サービングネットワークの隣接ネットワーク情報提供は、移動端末から MIH_Information.Request を受信し、これに対する応答として MIH_Information.Response を伝達することによってなることができ、また、サービングネットワークが MIH_Information.Response を放送の形態で周期的に移動端末に伝達することによって移動端末がサービングネットワークと正常に通信している状況下においても隣接網に関する情報を得ることができる。 3) プリミティブ構成 <pre> MIH_Information.Reseponse { InfoQueryFilter: ネットワークのタイプ (例: 802、GSM、CDMA 等) MIH_REPORT: 情報の具体的なパラメータ (例: Neighbor Information, Link Layer Security Supported, Link QoS Parameters 等) Status: 情報伝達状態 (例: Success, Fail) }</pre>

10

20

30

【0052】

すなわち、現在ネットワークと連結を維持しつつ通信中の移動端末は、隣接ネットワークに関する情報を獲得するために、MIH機能において定義する表1のようなMIH_Information.Request/Responseプリミティブを通じて、認証方法及び暗号化アルゴリズムなど、周辺接続ネットワークの第2層セキュリティ関連情報を把握できる。

【0053】

一方、本発明では、次のようなMIHプリミティブを規定して使用することによって、ハンドオーバーが予想される他のサービスプロバイダにより運用されるターゲット無線アクセスネットワークに事前認証を要請し、その結果として事前認証に成功した場合、該当のネットワークで使用するキーイング情報を獲得することを提案する。

【0054】

40

【表 2】

【表 2】

プリミティブ	説明
MIH_MN_Preauth. Request	1) 移動端末の MIH User (Security Entity) が MIH Function に伝達するプリミティブであり、ターゲット接続ネットワーク認証サーバに事前認証を要請するために使用される。このプリミティブを受信した MIH Function は、プリミティブ中のパラメータを含み、現在ネットワークの Authenticator MIH Function に遠隔メッセージの MIH_MN_Preauth. Request を生成して伝達する。 2) プリミティブ構成 <pre> MIH_MN_Preauth. Request { Current Link Identifier: 現在接続ネットワークの識別子 Current Authentication Server Identifier: 現在接続ネットワーク認証サーバの識別子 Target Link Identifier: ターゲット接続ネットワークの識別子 Target Authentication Server Identifier: ターゲット接続ネットワーク認証サーバの識別子 Mobile Terminal Identifier: 移動端末の識別子 (例: MAC アドレス、IMSI 等) Preauthentication Request Indication }</pre>
MIH_MN_Preauth. Indication	1) 移動端末から受信した MIH_MN_Preauth. Request メッセージが受信されたことを現在ネットワーク Authenticator の MIH Function が MIH User に通報するために知らせるプリミティブである。これを受信した MIH User は、ネットワークを通じて事前認証要請を伝達するために現在ネットワークの AAA サーバに事前認証要請メッセージ (Preauth Request) を伝達し、これは、ターゲットネットワークの AAA サーバに伝達される。 2) プリミティブ構成 <pre> MIH_MN_Preauth. Indication { Current Link Identifier: 現在接続ネットワークの識別子 Current Authentication Server Identifier: 現在接続ネットワーク認証サーバの識別子 Target Link Identifier: ターゲット接続ネットワークの識別子 Target Authentication Server Identifier: ターゲット接続ネットワーク認証サーバの識別子 Mobile Terminal Identifier: 移動端末の識別子 (例: MAC アドレス、IMSI 等) Preauthentication Request Indication }</pre>

10

20

30

【 0 0 5 5 】

【表 3】

【表 3】

プリミティブ	説明
MIH_MN_Preauth. Response	1) 移動端末が要請した事前認証手順についてターゲット接続ネットワークの認証サーバからの事前認証結果を知らせるために現在ネットワークの Authenticator の MIH user が MIH Function に伝達するプリミティブであり、これを受信した MIH Function はプリミティブ中のパラメータを含み、移動端末の MIH Function に遠隔メッセージの MIH_MN_Preauth. Response を生成して伝達する。さらに、このプリミティブにはネットワーク固有のセキュリティ関連コンテキストが含まれることができる。 2) プリミティブ構成 <pre> MIH_MN_Preauth. Response { Current Link Identifier: 現在接続ネットワークの識別子 Current Authentication Server Identifier: 現在接続ネットワーク認証サーバの識別子 Target Link Identifier: ターゲット接続ネットワークの識別子 Target Authentication Server Identifier: ターゲット接続ネットワーク認証サーバの識別子 Target HSS Identifier: ターゲット接続ネットワーク HSS の識別子 Preauthentication Result Indication (例: Success, Failure) Protected Pseudonym (例: TMSI, Reauthentication ID) }</pre>
MIH_MN_Preauth. Confirmation	1) 遠隔に MIH_MN_Preauth. Response を受信したことを、移動端末の MIH Function が MIH User に通報するために使用されるプリミティブである。MIH_MN_Preauth. Response に含まれたパラメータがそのまま含まれ、移動端末の MIH User にターゲット接続ネットワークの認証サーバから認証の成否についての結果を提供するための目的で使用される。ネットワーク固有のセキュリティ関連コンテキストが含まれることができる。 2) プリミティブ構成 <pre> MIH_MN_Preauth. Confirmation { Current Link Identifier: 現在接続ネットワークの識別子 Current Authentication Server Identifier: 現在接続ネットワーク認証サーバの識別子 Target Link Identifier: ターゲット接続ネットワークの識別子 Target Authentication Server Identifier: ターゲット接続ネットワーク認証サーバの識別子 Preauthentication Result Indication (例: Success, Failure) Protected Pseudonym (例: TMSI, Reauthentication ID) }</pre>

【0056】

すなわち、移動端末は、異なる管理ドメインにより運用されるターゲットネットワーク認証サーバに事前認証を要請するために、表 2 の MIH_MN_Preauth. Request / Indication プリミティブを使用することができ、これらのプリミティブは、最終的に、ターゲット接続ネットワークの認証サーバ (AAA server) に伝達され、端末に対する事前認証が行われる。具体的に、移動端末に対する事前認証手順は、IETF プロトコルを通じてなされることができる。また、具体的な各パラメータの活用は、以下、本発明の各実施形態を段階的に説明しながら共に説明する。

【0057】

一方、表 3 に示す MIH_MN_Preauth. Response / Confirmation プリミティブは、ターゲット接続ネットワークの認証サーバにより伝達された特定端末に対する事前認証結果を、現在接続ネットワークの認証子が端末に伝達するために使用するプリミティブである。すなわち、端末の事前認証要請は、現在ネットワークの

認証子、認証サーバを通じて他のサービスプロバイダのターゲット認証サーバに伝達されたり、直接、ターゲット接続ネットワークの認証子を通じて他のサービスプロバイダの認証サーバに伝達される。ターゲットネットワーク認証サーバはその要請を受け、事前認証を行い、その結果をサービング接続ネットワークの認証サーバに伝達する。これは、最終的に、サービングネットワーク認証サーバにより現在接続ネットワークの認証子を介してまたは直接、移動端末に伝達される。

【0058】

一方、本発明では、特定端末に対する事前認証結果及びこれによって生成されたキーイング情報をネットワーク観点で伝達するためのMIHプリミティブとして下記のようなプリミティブをさらに提案する。

【0059】

【表4】

プリミティブ	説明
MIH_Net_Preauth_Result_Transfer.Request	1) 現在ネットワークの Authenticator の MIH User が MIH-Function に伝達するプリミティブであり、移動端末がハンドオーバーするターゲットネットワークの Authenticator に特定移動端末に対する認証の結果及び Keying Material を伝達するために使用する。これを受信した MIH Function は、ターゲットネットワークの Authenticator にこれを知らせるための遠隔 MIH プロトコルメッセージである MIH_Net_Preauth_Result_Transfer.Request を生成して伝達する。 2) プリミティブ構成 <pre>MIH_Net_Preauth_Result_Transfer.Request{ Current Link Identifier:現在接続ネットワークの識別子 Current Authentication Server Identifier:現在接続ネットワーク認証サーバの識別子 Target Authentication Server Identifier:ターゲット接続ネットワーク認証サーバの識別子 Preauthentication Result Status(例:Success, Failure) Mobile Terminal Identifier:移動端末の識別子(例:MAC アドレス、IMSI 等) Protected Pseudonym(例:TMSI, Reauthentication ID) Keying Material:ターゲットネットワークの Authenticator により使用されるセキュリティコンテキストであり、移動端末とネットワークとの間に Security Association を設定するために使用されることができる。 }</pre>
MIH_Net_Preauth_Result_Transfer.Indication	1) 現在ネットワークの Authenticator の MIH から MIH_Net_Preauth_Result_Transfer.Request を受信したことを、ターゲットネットワークの Authenticator の MIH Function が MIH User に伝達するために使用するプリミティブである。これを受信した MIH User は、事前認証の結果を知らせるために使用するプリミティブである MIH_Net_Preauth_Result_Transfer.Response を生成して MIH Function に伝達する。 2) プリミティブ構成 <pre>MIH_Net_Preauth_Result_Transfer.Indication{ Target Authentication Server Identifier:ターゲット接続ネットワーク認証サーバの識別子 Target HSS Identifier:ターゲット接続ネットワーク HSS の識別子 Preauthentication Result Status(例:Success, Failure) Mobile Terminal Identifier:移動端末の識別子(例:MAC アドレス、IMSI 等) Protected Pseudonym(例:TMSI, Reauthentication ID) Keying Material:ターゲットネットワークの Authenticator により使用されるセキュリティコンテキストであり、移動端末とネットワークとの間に Security Association を設定するために使用されることができる。 }</pre>

【0060】

【表 5】

【表 5】

プリミティブ	説明
MIH_Net_Preauth_Result_Transfer. Response	1) 特定移動端末に対する事前認証結果及び関連 Keying Material の伝達が正常にされたか否かを通報するためにターゲットネットワークの Authenticator の MIH User が MIH Function に伝達するプリミティブである。このプリミティブを通じて伝達されるパラメータには事前認証結果及び関連 Keying material の伝達要請に対する結果(Status)及び正常に受信できなかった Keying material のリストが含まれる。これを受信した MIH Function は、遠隔でサービングネットワークの Authenticator の MIH に知らせるための MIH_Net_Preauth_Result_Transfer. Response を生成して伝達する。 2) プリミティブ構成 <pre> MIH_NET_Preauth_Result_Transfer. Response { Target Link Identifier: ターゲット接続ネットワークの識別子 Target Authentication Server Identifier: ターゲット接続ネットワーク認証サーバの識別子 Target HSS Identifier: ターゲット接続ネットワーク HSS の識別子 Mobile Terminal Identifier: 移動端末の識別子(例:MAC アドレス、IMSI 等) Protected Pseudonym(例:TMSI, Reauthentication ID) List of Not Acquired Keying Materials Preauthentication Result Transfer Status(例 :Success, Failure) }</pre>
MIH_Net_Preauth_Result_Transfer. Confirmation	1) MIH_NET_Preauth_Result_Transfer. Response を受信したサービングネットワークの Authenticator の MIH は、その結果を MIH User に 通 報 す る た め に MIH_Net_Preauth_Result_Transfer. Confirmation プリミティブを生成して伝達する。このプリミティブに含まれるパラメータは次の通りである。 2) プリミティブ構成 <pre> MIH_Net_Preauth_Result_Transfer. Confirmation { Target Link Identifier: ターゲット接続ネットワークの識別子 Mobile Terminal Identifier: 移動端末の識別子(例:MAC アドレス、IMSI 等) List of Not Acquired Keying Materials Preauthentication Result Transfer Status(例 :Success, Failure)} }</pre>

10

20

30

【0061】

特に、表 4 は、特定端末に対する事前認証の結果及びこれによって生成されたキーイング情報の伝達のために用いられるプリミティブを示しており、表 5 は、表 4 のプリミティブを通じて、ターゲットネットワークの認証子が、該当の移動端末に対する事前認証結果及びキーイング情報の伝達がなされたか否かに対する結果を、現接続ネットワークの認証子に知らせるために用いられるプリミティブを示している。

40

【0062】

一方、本発明によって提案される方法を行うにあたり、より好ましい実施形態では下記のような条件を満たすように設定することを提案する。

【0063】

1) 3GPP/3GPP2 のような無線アクセス技術において移動端末及びネットワークにより長期間共有されるセキュリティクレデンシャル (Security Credential) は、マルチモード移動端末の SIM カードまたは UICC カードに保存されることが好ましい。

【0064】

2) サービングネットワークとターゲットネットワークとの間に交換される事前認証

50

関連シグナリングまたはキーイング情報に対する保護が提供されることが好ましい。

【0065】

3) IEEE 802.16 ネットワークは、3GPP ネットワークまたはその他の異種ネットワークとの連動のためにローミング協約を結んでいることが好ましい。

【0066】

4) ユーザ識別子（例えば、IMSI、TMSI、MAC アドレス）保護のために、これらの識別子が露出されないことが好ましい。

【0067】

上述の通り、サービング接続ネットワークの移動端末は、ターゲット接続ネットワークにハンドオーバーを行う前に、MIH 情報サービスを用いて、サービング接続ネットワークを通じてターゲット接続ネットワークと事前認証を行ったり、ターゲット接続ネットワークを通じて直接事前認証を行ったりし、一つ以上の接続ネットワークと事前認証を行うことができる。各接続ネットワークは、異なるAAA (Authentication, Authorization and Accounting) サーバを運用し、認証のためのEAPサーバ機能はAAAサーバに含まれ、認証子及び認証サーバ間の通信はRADIUS (Remote Authentication Dial In User Service) またはRADIUSを改善したDiameterのようなAAAプロトコルを通じて具現されることができる。

【0068】

ターゲット認証子がIEEE 802.16、IEEE 802.11 ネットワークのようにリンク層のキーを生成するためにEAPベースMSK (Master Session Key) を使用する場合、事前認証手順は、ターゲット認証子のためのMSKを生成することによって端末とネットワーク（基地局またはアクセスポイント (Access Point)）との間にセキュリティ連携 (Security Association) を設定可能にする。

【0069】

本発明では、移動端末、サービング認証子、ターゲット認証子及び認証サーバ間に事前認証がなされる方法を、2形態に区分して提案する。これは、サービング認証子が事前認証シグナリングにどのように関与しているかによって区分される。すなわち、本発明では、下記の直接事前認証方式及び間接事前認証方式を、本発明の各実施形態として提案する。

【0070】

先ず、直接事前認証では、事前認証シグナリングがサービング認証子に透明なようにして移動端末とターゲット認証子との間に交換され、このシグナリングは、ターゲット認証子を通じてターゲット認証サーバに伝達される方式である。一方、間接事前認証では、事前認証シグナリングにサービング認証子が関与し、これは、セキュリティ上、ターゲット認証子及び移動端末間のIP通信が許容されない場合に必要な技術として提案する。すなわち、間接事前認証シグナリングは、移動端末及びサービング認証子間のシグナリングと、サービング認証子及びターゲット認証子間のシグナリングとに区分することができ、サービング認証子及びターゲット認証子間のシグナリングには、サービング接続ネットワークの認証サーバ及びターゲット接続ネットワーク認証サーバが含まれる。

【0071】

以下、上述した2通りの実施形態のうち、間接事前認証を用いる実施形態について、図面を参照しつつより詳細に説明する。

【0072】

図3は、本発明の一実施形態によってIEEE 802.16 ネットワークによりサービスを受けるマルチモード移動端末が、現在接続ネットワークを通じて事前認証を行った後、他のIEEE 802 シリーズネットワークにinter-RAT ハンドオーバーを行う過程を説明するための図である。

【0073】

図3に示す実施形態では、移動端末の事前認証要請を、現在接続ネットワークの認証子が現在接続ネットワークの認証サーバを通じてターゲット接続ネットワークの認証サーバに伝達し、この要請を受けたターゲットネットワーク認証サーバは、該当の端末に対する事前認証を行った後、その結果を現在接続ネットワーク認証子を通じてターゲット接続ネットワーク認証子に伝達する方式を提案する。その後、ターゲットネットワーク認証子は、受信した事前認証結果に対する応答を現在接続ネットワークの認証子に通報する。その後、現在接続ネットワーク認証子は、ターゲットネットワークで使用するキーイング情報を事前認証の結果として移動端末に伝達する方式である。

【0074】

本実施形態では、基本的に、認証サーバがMIH機能を支援しない状況を仮定する。その理由は、現在IETFにより定義されたAAAフレームワーク(Framework)を修正してMIH機能を追加することは容易でないためである。ただし、本発明は、各認証サーバがMIH機能を支援して直接該当のMIHプリミティブを交換する概念を排除しない。

【0075】

事前認証が行われる2形態のうち、図3は、サービングネットワークの認証子を通じて事前認証要請を伝達する場合であり、この場合、表2及び表3に定義されたMIHプリミティブの使用において選択的なパラメータの使用が可能である。すなわち、表2に提示されたプリミティブにおいて、表2で提示した全てのパラメータを含むのではなく、それらのうち、現在接続ネットワーク識別子(Current Link Identifier)、現在認証サーバ識別子(Current Authentication Server Identifier)などのパラメータは含まなくても良い。同様に、表3に提示されたプリミティブにおいても、これら2種のパラメータは含まなくても良い。

【0076】

このような内容に基づき、図3に示す各手順について具体的に説明すると、下記の通りである。

【0077】

(1) 先ず、ステップ(1)では、マルチモード移動端末301が、IEEE 802.16ネットワークに接続し、EAPベースの認証によるマスターセッションキー(Master Session Key)及びAK(Alternate Key)共有、3-Way HandshakeによるTEK(Traffic encryption key)の共有などの過程を示している。IEEE 802.16ネットワークではなく他のIEEE 802シリーズネットワークである場合、EAPベースの類似な形態の初期認証手順がなされることができる。

【0078】

(2) このように、IEEE 802.16ネットワークと連結を維持しながら通信中のマルチモード移動端末301は、情報サーバ306から一つ以上の隣の候補ネットワークに関する情報を獲得する(ステップ(2))。これは、上述の通り、MIHで定義する情報サービスを通じて行うことができる。例えば、表1に示すようなMIH_Information.Request/ResponseプリミティブのようなMIH情報要請/応答プリミティブを通じて行うことができる。このようなプリミティブを用いて、移動端末は、隣接ネットワークの認証方法/暗号化アルゴリズムのようなリンク層セキュリティ関連パラメータを受信することができる。例えば、現在の管理ドメインにより運用されるIEEE 802.16ネットワーク302のMIHは、ハンドオーバーが予想される802シリーズネットワーク305のMIHにIP情報を要請し、これを移動端末301に伝達できる。IPアドレスは、移動端末のハンドオーバー時に用いることができる。

【0079】

(3) その後、移動端末301は、スキャンングを通じて隣接ネットワークから信号を受信し、ネットワーク探索/選択手順を行う(ステップ(3))。本実施形態では、このステップ(3)の結果として、802シリーズのネットワーク305が潜在的なハンドオ

ーバーターゲットネットワークとして他の管理ドメインにより運用されると仮定する。802シリーズのネットワークは、IEEE 802.16、IEEE 802.11などのネットワークを含むと仮定する。

【0080】

(4) その後、マルチモード移動端末301が、IEEE 802.16ネットワークから受信する信号レベルが一定レベル以下に落ちたことを認識すると、表2で提案したMIH_MN_Preauth_RequestプリミティブのようなMIH事前認証要請プリミティブを移動端末のMIHエンティティに伝送し、事前認証手順を行うことを指令することができる(ステップ(4))。ここで、MIH事前認証要請プリミティブは、表2に表すMIH_MN_Preauth_Requestプリミティブのように、現在接続ネットワーク302の識別子、現在接続ネットワーク認証サーバ303の識別子、ターゲット接続ネットワーク305の識別子、ターゲット接続ネットワーク認証サーバ304の識別子、マルチモード移動端末301の識別子及び事前認証要請指示子などを含むことができる。

10

【0081】

このように、移動端末301のMIHユーザ、すなわち、MIH上位層は、移動端末301のMIHに、ターゲットネットワークである802シリーズネットワーク認証サーバ304へ事前認証手順の要請を伝達することを要請することができる。これは、802.16ネットワーク認証子302と認証サーバ303を通してターゲットネットワークである802シリーズネットワークの認証サーバ304に伝達されることができる。本実施形態は、EAP機能を含むAAAサーバがMIHを支援しない場合を提示しているが、これに本発明が限定されるわけではない。

20

【0082】

なお、本実施形態のステップ(4)において、事前認証手順の開始は第2層ハンドオーバー実行前に行うと仮定しているが、上述のように、現在接続ネットワークからの受信信号レベルが所定の臨界値以下であるか否かを判断する時に用いられる所定の臨界値は、第2層ハンドオーバー開始を判定するために用いられる臨界値よりも高いレベルに設定することが好ましい。ただし、本発明は、実質的なハンドオーバー手順開始以前に事前認証が行える限り、上述の方法に限定されず、種々の説明を通じて具現されることができる。

【0083】

(5) ステップ(5)では、表2のMIH_MN_Preauth_RequestプリミティブのようなMIH事前認証要請プリミティブを受信した移動端末301のMIHが、MIH遠隔プロトコルメッセージであるMIH_MN_Preauth_Requestプロトコルメッセージを生成し、これを、サービングネットワークであるIEEE 802.16ネットワーク認証子302のMIHに伝達することができる(ステップ(5))。このメッセージは、ステップ(4)におけるMIH事前認証要請プリミティブ中のパラメータを含むことができる。

30

【0084】

(6) その後、IEEE 802.16ネットワーク認証子302のMIHは、遠隔プロトコルメッセージ受信結果を認証子MIHユーザに知らせるために、表2に表すMIH_MN_Preauth_IndicationプリミティブのようなMIH事前認証指示プリミティブを生成した後に、これを、認証子302のMIHユーザに伝達することができる(ステップ(6))。ここで、MIH事前認証指示プリミティブは、表2に表すように、現在接続ネットワーク302の識別子、現在接続ネットワーク認証サーバ303の識別子、ターゲット接続ネットワーク305の識別子、ターゲット接続ネットワーク認証サーバ304の識別子、マルチモード移動端末301の識別子及び事前認証要請指示子などを含むことができる。

40

【0085】

(7) 一方、ステップ(7)では、ステップ(6)でMIH事前認証指示プリミティブを受信した認証子302のセキュリティを担当する個体が、事前認証を要請するメッセー

50

ジを、IEEE 802.16と関連しているAAAサーバ303を通じてターゲット802シリーズネットワーク305と関連しているAAAサーバ304に伝達する。

【0086】

(8)その後、IETFプロトコルを通じて移動端末301とターゲットネットワークのAAAサーバ304との間に事前認証手順が行われる(ステップ(8))。事前認証手順は、移動端末301、サービングネットワーク認証子302、サービングネットワーク認証サーバ303、そしてターゲットネットワーク認証サーバ304が関与し、その結果はサービングネットワーク認証子302のMIHユーザにも伝達される。本実施形態において、サービングネットワークで用いられる認証クレデンシャル(Credential)とターゲットネットワークで用いられる認証クレデンシャルとが同一でなくても良いが、この問題は、ステップ(2)のようにMIH情報サービスにより提供される情報を獲得することによって解決できるわけである。すなわち、移動端末301は、ターゲットネットワークで考慮するクレデンシャルについての内容をMIH情報要請/応答プリミティブなどから把握できるので、事前認証手順を行うことができる。

10

【0087】

(9)ターゲットIEEE 802シリーズAAAサーバ304は、事前認証手順の結果及びターゲットネットワークで使用するキーイング情報を含むメッセージ(Preauth Response)を生成し、これをIEEE 802.16ネットワークAAAサーバ303を通じてサービングネットワーク302のセキュリティを担当する個体(Security Entity)に伝達する。

20

【0088】

(10)その後、事前認証手順の結果及びターゲットネットワークで使用するキーイング情報を受信した現在ネットワーク認証子302のMIHユーザは、表4に表すMIH_Net_Preauth_Result_Transfer_RequestプリミティブのようなMIH事前認証結果伝達要請プリミティブを生成し、現在ネットワーク認証子302のMIHに伝達できる(ステップ(10))。このMIH事前認証結果伝達要請プリミティブは、表4に表す通り、現在接続ネットワーク302の識別子、現在接続ネットワーク認証サーバ303の識別子、ターゲット接続ネットワーク305の識別子、ターゲット接続ネットワーク認証サーバ304の識別子、事前認証結果状態情報(すなわち、事前認証の成否)、マルチモード移動端末301の識別子、保護されるセキュリティ情報及びターゲット接続ネットワークの認証手段により用いられるセキュリティコンテキストなどを含むことができる。

30

【0089】

(11)その後、ステップ(11)では、このようなMIH事前認証結果伝達要請プリミティブを受信した現在ネットワーク認証子302のMIHが、ターゲットネットワーク認証子305のMIHに、遠隔プロトコルメッセージであるMIH_Net_Preauth_Result_Transfer_Requestを生成して伝達できる(ステップ(11))。このメッセージは、ステップ(10)で言及したMIH事前認証結果伝達要請プリミティブにあるパラメータを含むことができる。

【0090】

40

(12)その後、上述したMIH事前認証結果伝達要請プリミティブメッセージを受信したターゲットネットワーク認証子305のMIHは、これをMIHユーザに知らせるために、表4に表すMIH_Net_Preauth_Result_Transfer_IndicationプリミティブのようなMIH事前認証結果伝達指示プリミティブを新しく生成した後、これをMIHユーザに伝達することができる(ステップ(12))。このプリミティブには、ステップ(11)におけるMIH事前認証結果伝達要請プリミティブに含まれたパラメータの一部及びターゲットネットワーク認証子305のMIHユーザのために必要な一部のパラメータが追加されることができ、これは、表4に表す通りである。

【0091】

50

(13) これにより、MIH事前認証結果伝達指示プリミティブを受信したターゲットネットワーク認証子305のMIHユーザは、サービングネットワーク認証子302から移動端末301に対する事前認証手順の結果及びターゲットネットワーク認証サーバ304が生成したキーイング情報の受信有無をターゲットネットワーク305のMIHに伝達するために、表5に表すMIH_Net_Preauth_Result_Transfer. ResponseプリミティブのようなMIH事前認証結果伝達応答プリミティブを生成してMIHに伝達することができる(ステップ(13))。MIH事前認証結果伝達応答プリミティブは、表5に表す通り、ターゲット接続ネットワーク305の識別子、ターゲット接続ネットワーク認証サーバ304の識別子、ターゲット接続ネットワークHSS(Home Subscriber Server)の識別子、マルチモード移動端末301の識別子、再認証用ID、獲得できなかったキーイング(Keying)情報及び事前認証結果伝達状態指示子などを含むことができる。ただし、パラメータのうちHSS識別子は本実施形態では省略可能である。

【0092】

(14) その後、上述したようなMIH事前認証結果伝達応答プリミティブを受信したターゲットネットワーク認証子305のMIHは、サービングネットワーク認証子302に伝達するための遠隔メッセージとして、遠隔MIHプリミティブであるMIH_Net_Preauth_Result_Transfer. Responseプリミティブを生成して伝送できる(ステップ(14))。このプリミティブは、ステップ(13)におけるMIH事前認証結果伝送応答プリミティブに含まれるパラメータを含むことができる。

【0093】

(15) その後、サービングネットワーク認証子302は、ステップ(14))で言及されたようなMIH事前認証結果応答プリミティブメッセージを受信した結果として、MIHユーザに、表5に表すMIH_Net_Preauth_Result_Transfer. ConfirmationプリミティブのようなMIH事前認証結果伝達確認プリミティブを生成して伝達することができる(ステップ(15))。

【0094】

(16) これにより、サービングネットワーク認証子302のMIHユーザは、ステップ(15)で言及されたように、MIH_Net_Preauth_Result_Transfer. Confirmationプリミティブを受信した後、これに対する応答として、表3に表すMIH_MN_Preauth. ResponseプリミティブのようなMIH事前認証応答プリミティブをサービングネットワーク認証子302のMIHに伝達できる(ステップ(16))。

【0095】

(17) その後、ステップ(16)で言及されたようなサービングネットワーク認証子302のMIHは、遠隔プロトコルメッセージのMIH_MN_Preauth. Responseプリミティブを、移動端末301のMIHに伝達することができる(ステップ(17))。この時、用いられるプリミティブは、ステップ(16)で言及されたMIH_MN_Preauth. Responseプリミティブに含まれたパラメータを含むことができる。

【0096】

(18) これにより、MIH_MN_Preauth. Responseプリミティブメッセージを受信した移動端末301のMIHは、移動端末301のMIHユーザにそれを知らせるために、表3に表すMIH_MN_Preauth. ConfirmationプリミティブのようなMIH事前認証確認プリミティブを生成して伝達することができる(ステップ(18))。

【0097】

(19) このようにして事前認証手順が完了した後に、新しいネットワークとのハンドオーバー、すなわち、リンク設定手順を開始する命令が上位管理個体から伝達され、この

10

20

30

40

50

時、上位管理個体は、全く新しい認証及びセキュリティキー設定などのような大きい負荷を招き、遅延につながる可能性のあるセキュリティ関連手順を省略できるということを通報する（ステップ（19））。

【0098】

（20）これを受信した移動端末301のMIHは、リンクを設定するようとの命令を該当のリンクに伝送する（ステップ（20））。

【0099】

（21）これにより、マルチモード移動端末301は、第2層（またはL2）ハンドオーバーを行うことができる（ステップ（21））。この場合、新しい認証手順は省略され、上述したステップ（4）～（18）手順で行われた事前認証手順の結果として、サービ
10
ングネットワークとターゲットネットワークのネットワーク個体（認証子、認証サーバ）相互間に交換された情報に基づいてターゲットネットワークへの登録時に初めから認証を新しく行い、キーを設定する過程を省略することができる。

【0100】

第2層ハンドオーバーを完了すると、移動端末301のMACは、ターゲットネットワークのアクセスポイントとセキュリティ連携を設定し、通信を準備することができる。

【0101】

図3と関連して上述した実施形態では、IEEE 802.16ネットワークでサービスを受けたマルチモード移動端末が、サービングネットワークの認証子を通じて事前認証要請を伝達し、802シリーズネットワークにハンドオーバーした場合のシナリオを示し
20
ている。ただし、上記実施形態のステップ（16）～（18）は、手順の最適化のために省略されても良い。

【0102】

一方、以下では、マルチモード移動端末がターゲットネットワーク認証子に直接事前認証要請を伝達し、ターゲットネットワーク認証サーバに事前認証手順を行わせる実施形態について説明する。

【0103】

図4は、本発明の他の実施形態によって、IEEE 802.16ネットワークによりサービスを受けるマルチモード移動端末が、現在接続ネットワークの関与無しに直接ターゲットネットワークと事前認証を行った後、IEEE 802シリーズネットワークにin
30
t e r - R A Tハンドオーバーを行う過程を説明するための図である。

【0104】

図4の手順は、図3と比較すると、マルチモード移動端末401が直接ターゲット接続ネットワークの認証子403及び認証サーバ404に事前認証を要請し、事前認証結果を受信し、現在接続ネットワークの認証子402及び認証サーバ403は、移動端末401とターゲット接続ネットワークの認証子403及び認証サーバ404との事前認証過程に関与せず単にこれらの間を中継（r e l a y）する点以外は、基本的には、図3の細部的な手順と同一に行われる。以下では、上述の通り、現在接続ネットワークの認証子及び
40
認証サーバが事前認証手順に関与せずに第2層の単純中継によって行われる場合を“直接事前認証”と称し、現在接続ネットワークの認証子及び認証サーバが事前認証手順に実質的に関与する、つまり第3層以上の関与を伴う場合を“間接事前認証”と称する。したがって、以下では、重複を避けるために、直接事前認証の場合を示す図4の実施形態による各ステップのうち、間接事前認証の場合を示す図3と相違する部分についてのみ重点的に説明するものとする。

【0105】

図4では、事前認証要請がターゲットネットワークの認証子405に直接伝達される。この場合には、事前認証の結果がターゲット接続ネットワーク認証サーバ404からターゲットネットワークの認証子403に伝達されるため、図3の場合とは違い、表4及び表5に定義されたプリミティブを用いなくて済む。以下では、各ステップ別に、図3の実施形態との差異点を中心に説明する。
50

【0106】

(1)～(4)マルチモード移動端末401は、図3で説明したステップ(1)～ステップ(4)と同様に、現在接続ネットワーク402に接続して通信をする中に、MIH情報要請／応答プリミティブなどを通じて情報サーバ406から一つ以上の候補接続ネットワークに関する情報を獲得でき、その後、現在接続ネットワーク402から受信した信号レベルが、所定臨界値（好ましくは、ハンドオーバー開始を判定するために用いられる臨界値よりも高いレベルの臨界値）以下になる場合、移動端末401の上位層は、MIHに事前認証手順開始を命令でき、この事前認証手順は、図3で説明した実施形態のようにMIH_MN_Preauth. Requestプリミティブを用いて行うことができる。

【0107】

(5) 上述したMIH_MN_Preauth. Requestプリミティブを受信した移動端末401のMIHは、MIH遠隔プロトコルメッセージであるMIH_MN_PreauthRequestプリミティブを生成し、ターゲットネットワークであるIEEE 802シリーズネットワーク認証子404のMIHに伝達することができる。すなわち、本実施形態では、図3の場合とは違い、MIH_MN_Preauth. Requestプリミティブが、移動端末401のMIHからサービングネットワークの認証子402及び認証サーバ403の関与無しにターゲットネットワーク認証子405のMIHに伝達されることができると仮定する。すなわち、サービングネットワークは、移動端末401とターゲットネットワークの認証子405との間のプリミティブ交換を単純中継する役割を果たす。

【0108】

この時、MIH_MN_Preauth. Requestプリミティブメッセージは、ステップ(4)で受信されたプリミティブ中のパラメータを含むとする。

【0109】

(6) その後、ターゲットネットワーク認証子405のMIHは、遠隔プロトコルメッセージの受信結果を認証子405のMIHユーザに知らせるために、表2に表すMIH_MN_Preauth. IndicationプリミティブのようなMIH事前認証指示プリミティブを生成した後、これを認証子405のMIHユーザに伝達する。ここで用いられるMIH事前認証指示プリミティブは、表2に表すように、現在接続ネットワーク402の識別子、現在接続ネットワーク認証サーバ403の識別子、ターゲット接続ネットワーク405の識別子、ターゲット接続ネットワーク認証サーバ404の識別子、マルチモード移動端末401の識別子及び事前認証要請指示子などを含むことができるが、本実施形態のように現在接続ネットワークの関与無しに直接ターゲット接続ネットワークにMIHプリミティブが伝達される場合、パラメータのうち、現在接続ネットワーク402の識別子及び現在接続ネットワーク認証サーバ403の識別子は省略しても良い。

【0110】

(7) その後、上述したMIH_MN_Preauth. Indicationプリミティブを受信した認証子405のセキュリティを担当する個体は、事前認証を要請するメッセージを、ターゲット802シリーズネットワークと関連しているAAAサーバ404に伝達する（ステップ(7)）。

【0111】

(8) その後、実質的な事前認証手順は、図3で説明した事前認証手順と基本的に同一に行うことができる。ただし、本実施形態における事前認証手順は、現在接続ネットワーク認証子402及び現在接続ネットワーク認証サーバ403の関与無しに移動端末401とターゲット接続ネットワーク認証子405及びターゲット接続ネットワーク認証サーバ404との間に行われる点で、図3と相違している。また、事前認証の結果は、図3では現在接続ネットワーク認証子のMIHユーザに伝達されたが、これと違い、本実施形態では、ターゲットネットワーク認証子405のMIHユーザに伝達されとする。

【0112】

(9) ターゲットネットワークの認証サーバ404は、事前認証手順の結果を含むメッ

10

20

30

40

50

セージ (Preauth Response) を生成し、これをターゲット IEEE シリーズネットワーク認証子 405 のセキュリティを担当する個体 (Security Entity) に伝達する。

【0113】

(10) その後、事前認証手順の結果及びターゲットネットワークで使用するキーイング情報を受信したターゲットネットワーク認証子 405 の M I H ユーザは、認証子 405 の M I H に、表 3 に表す M I H _ M N _ P r e a u t h . R e s p o n s e プリミティブのような M I H 事前認証応答プリミティブを生成した後、これを M I H に伝達することができる。

【0114】

(11) これにより、ターゲットネットワーク認証子 405 の M I H は、上述の通り、M I H _ M N _ P r e a u t h . R e s p o n s e プリミティブを受信した後、遠隔プロトコルメッセージである M I H _ M N _ P r e a u t h . R e s p o n s e プリミティブを生成し、これをサービングネットワークの認証子 402 の M I H に伝達する。このメッセージは、上述した M I H _ M N _ P r e a u t h . R e s p o n s e プリミティブのパラメータを含むとする。サービングネットワークの認証子 402 の M I H は、遠隔 M I H _ M N _ P r e a u t h . R e s p o n s e メッセージを受信した後、これを移動端末 401 の M I H に伝達する。

【0115】

(12) ~ (15) このように M I H _ M N _ P r e a u t h . R e s p o n s e プリミティブを受信したマルチモード移動端末 401 の M I H は、M I H ユーザにこれを知らせるために、表 3 に表す M I H _ M N _ P r e a u t h . C o n f i r m a t i o n プリミティブのような M I H 事前認証確認プリミティブを生成した後、これを M I H ユーザに伝達でき、このようにして事前認証手順が完了した後、新しいネットワークとのハンドオーバー、すなわち、リンク設定手順を開始するようとの命令が上位管理個体から伝達され、この時、全く新しい認証及びキー設定などのような大きい負荷を招き、遅延につながる可能性のあるセキュリティ関連手順が省略可能であるということを通報する。これにより、移動端末 401 は、より簡単にハンドオーバー手順を行うことができる。

【0116】

上述した実施形態は、IEEE 802.16 ネットワークでサービスを受けていたマルチモード移動端末が、ターゲットネットワークの認証子を通じて事前認証要請を伝達し、802 シリーズネットワークにハンドオーバーする場合のシナリオを示している。しかし、ステップ (10) ~ ステップ (12) は手順の最適化のために省略することができる。

【0117】

図 3 及び図 4 と関連して上述した 2 つの実施形態は両方とも、移動端末が E A P ベースの認証フレームワークを採択している接続ネットワーク間においてハンドオーバーする場合に関するものである。ただし、本発明による事前認証方法及びこれを用いたハンドオーバー方法は、移動端末が、IEEE 802 シリーズネットワークから上述したような E A P ベース認証フレームワークを採択していない非 IEEE 802 シリーズネットワーク、すなわち、3 G P P ネットワークにハンドオーバーする場合にも、同様に適用できる。

【0118】

図 5 及び図 6 は、本発明の更に他の実施形態によって、移動端末が IEEE 802 シリーズネットワークから 3 G P P ネットワークにハンドオーバーする場合、事前認証を行う方法を説明するための図である。

【0119】

図 5 及び図 6 に示す実施形態は、IEEE 802.16 ネットワークから 3 G P P ネットワークのような非 IEEE 802 シリーズネットワークに移動端末がハンドオーバーする場合、事前認証手順の過程を示している。すなわち、図 5 及び図 6 では、インターワーキングのために 3 G P P A A A サーバ 504, 604 が存在し、E A P ベースの認証

10

20

30

40

50

フレームワークを支援する時、EAP-AKAまたはSIMなどの認証方法を通じて事前認証を行う場合の例を取り上げている。

【0120】

各実施形態で基本的な事前認証方法及びこれを用いたハンドオーバー方法は、図3及び図4で上述した実施形態と同一である。したがって、図5及び図6の実施形態について段階的に説明する中で、図3及び図4に示す実施形態と異なる部分についてのみ具体的に説明する。

【0121】

図5は、図3に示す実施形態とように、移動端末501が現在接続ネットワーク502を通じてターゲットネットワーク506に事前認証を要請する実施形態を示す。

10

【0122】

先ず、マルチモード移動端末501がIEEE 802.16ネットワークに接続してEAPベース認証を行った後（ステップ（1））、IEEE 802.16ネットワーク502と連結を維持した状態で一つ以上の候補ネットワークに対する検索を行う（ステップ（2））。その後、上述した実施形態と同様にターゲットネットワークを選択し、情報サーバ507からターゲットネットワークに関する情報をMIH_information.Request/Responseプリミティブを通じて獲得できる（ステップ（3））。本実施形態では、このようなプリミティブを通じて他の管理ドメインにより運用される非802シリーズネットワークを潜在的なハンドオーバーターゲットネットワークとして決定したと仮定する。特に、図5では、非802シリーズのネットワークである3GPPネットワーク506をターゲットネットワークとして選択することを示している。

20

【0123】

一方、マルチモード移動端末501がIEEE 802.16ネットワークから受信する信号レベルが一定レベル（好ましくは、ハンドオーバー開始を判断できるようなレベル以上）以下に落ちたことを認識すると、移動端末501のMIHユーザは、MIH_MN_Preauth.Requestプリミティブを通じて移動端末501のMIHに、ターゲットネットワークである非802シリーズネットワーク認証サーバ503に事前認証手順の要請を伝達することを要請することができる（ステップ（4））。これは、802.16ネットワーク認証子502と認証サーバ503を経てターゲットネットワークの非802シリーズネットワークの認証サーバ504に伝達されることができる。本実施形態も、図3及び図4で説明した実施形態と同様に、EAP機能を含むAAAサーバ503がMIHを支援しない場合を仮定する。

30

【0124】

その後、MIH_MN_Preauth.Requestプリミティブを受信した移動端末501は、該当の情報をサービングネットワークのIEEE 802.16ネットワーク認証子502のMIH、MIHユーザを経て（ステップ（5）、（6））、ターゲットネットワークの3GPP AAAサーバ504に伝達し（ステップ（7））、各ステップで用いるプリミティブの例は、図5に示す通りである。

【0125】

このように、ターゲットネットワーク認証サーバ504が事前認証要請情報を受信すると、本実施形態による事前認証手順が行われる（ステップ（8））。本実施形態において事前認証手順は、移動端末501、サービングネットワーク認証子502、サービングネットワーク認証サーバ503、ターゲットネットワーク認証サーバ504、ターゲットネットワーク認証子506の他に、ターゲットネットワークのHSS（Home Subscriber Server）が関与することとなる。その結果は、サービングネットワーク認証子502のセキュリティを担当する層に伝達される（ステップ（9））。3GPPネットワークの認証サーバ504を含む事前認証手順は、HSSからユーザと関連したセキュリティコンテキストを抽出する手順も含むとする。

40

【0126】

ステップ（10）～ステップ（21）の手順は、図3と関連して上述した実施形態のス

50

テップ（１０）～（２１）の手順と同一に行うことができる。ただし、事前認証結果に基づく情報を含むＭＩＨ事前認証結果伝達要請／応答プリミティブにおいては、図３と関連して上述した実施形態でＨＳＳ識別子などの情報が省略可能であったのに対し、事前認証に参与したＨＳＳ識別子情報を含むように設定されると仮定する。この実施形態においても同様、ステップ（１６）～ステップ（１８）は手順の最適化のために省略しても良い。

【０１２７】

また、上述した実施形態において、各プリミティブの選択的な使用が可能である。ここでいうプリミティブは、`MIH_MN_Preauth.Request/Indication`プリミティブ及び`MIH_MN_Preauth.Response/Confirmation`を意味する。

10

【０１２８】

このように実質的な第２層ハンドオーバーを行う前に事前認証を行うことによって、`enter-RAT`ハンドオーバー過程で認証による遅延を低減させることができる。

【０１２９】

一方、図６は、図４に示す実施形態と同様に、移動端末６０１が現在接続ネットワーク６０２の関与無しに直接ターゲット接続ネットワーク６０６に事前認証を要請する実施形態に関する。

【０１３０】

先ず、マルチモード移動端末６０１は、現在サービングネットワークであるIEEE 802.16ネットワーク６０２に接続してEAPベース認証を行い（ステップ（１））、IEEE 802.16ネットワーク６０２と連結を維持した状態で一つ以上の候補ネットワークに対する検索を行う（ステップ（２））。その後、上述した各実施形態と同様に、ターゲットネットワークを選択し、情報サーバ６０７からターゲットネットワークに関する情報を`MIH_information.Request/Response`プリミティブを通じて獲得することができる（ステップ（３））。このようなプリミティブを通じて他の管理ドメインにより運用される非８０２シリーズネットワークを、ハンドオーバーのターゲットネットワークと仮定する。特に、図６では、非８０２シリーズのネットワークの３ＧＰＰネットワーク６０６が、ターゲットネットワークとして選択される。

20

【０１３１】

一方、マルチモード移動端末６０１がIEEE 802.16ネットワークから受信する信号レベルが、一定レベル（好ましくは、ハンドオーバー開始を判断すできるようなレベル以上）以下に落ちたことを認識すると、移動端末６０１のＭＩＨユーザは、`MIH_MN_Preauth.Request`プリミティブを通じて移動端末６０１のＭＩＨに、ターゲットネットワークの非８０２シリーズネットワーク認証サーバ６０３に事前認証手順の実行要請プリミティブを伝達することを要請できる（ステップ（４））。このような事前認証要請プリミティブは、図５と関連して上述した実施形態で８０２.16ネットワーク認証子６０２及び認証サーバ６０３の事前認証手順に対する関与の下にターゲットネットワークの非８０２シリーズネットワークの認証サーバ６０４に伝達されたのに対し、８０２.16ネットワーク認証子６０２及び認証サーバ６０３の単純中継を通じてターゲットネットワーク認証子６０６に伝達されるという特徴を有する（ステップ（５）、（６））。また、本実施形態で伝達される`MIH_MN_Preauth.Indication Primitive`は、ＭＩＨユーザのために必要なパラメータ（ＨＳＳ識別子など）をさらに含むことができる。

30

40

【０１３２】

その後、`MIH_MN_Preauth.Indication`プリミティブを受信した認証子６０６のセキュリティを担当する個体は、事前認証を要請するメッセージを、ターゲット３ＧＰＰネットワークと関係しているAAAサーバ６０４に伝達する。

【０１３３】

これにより、IETFプロトコルを通じて移動端末６０１とターゲットネットワークのAAAサーバ６０４との間に事前認証手順が行われる（ステップ（８））。事前認証手順

50

には、移動端末601、ターゲットネットワーク認証子606、ターゲットネットワーク認証サーバ604及びターゲットネットワークHSS(605)が関与することができる。その結果を、ターゲットネットワーク認証子606のMIHユーザに伝達することができる。3GPPネットワークの認証サーバ604を含む事前認証手順は、HSS(605)から、ユーザと関連したセキュリティコンテキストを抽出する手順も含む。

【0134】

ステップ(9)～ステップ(16)は、図4と関連して上述した実施形態と基本的に同一に行われる。ただし、本実施形態において事前認証結果を伝達するMIH事前認証応答プリミティブは、図4と関連して上述した実施形態と違い、ターゲットネットワークHSS(605)識別子も含むことができる。

10

【0135】

一方、この実施形態においても同様、ステップ(9)～ステップ(13)は手順の最適化のために省略可能である。

【0136】

このようにハンドオーバー実行前に事前認証手順を行うことによって、実際ハンドオーバー過程において認証による遅延を低減させることができる。

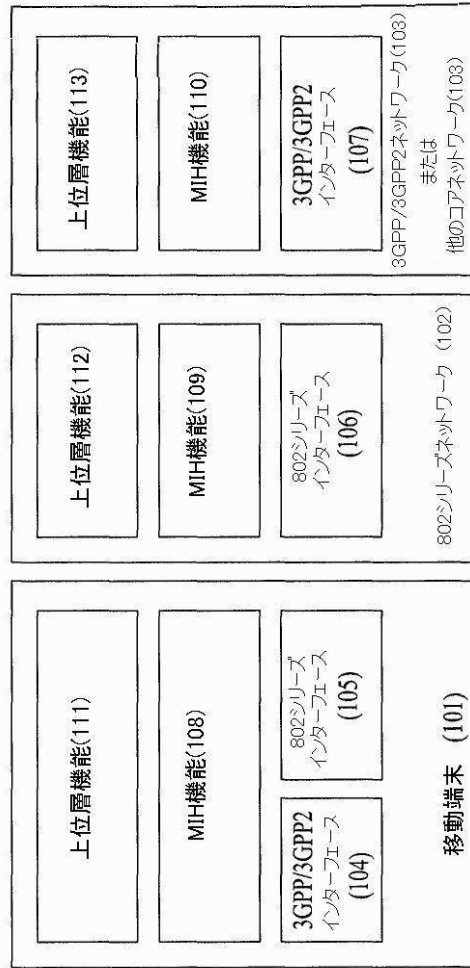
【0137】

上述したように、本発明の好ましい実施形態についての詳細な説明は、当業者が本発明を具現及び実施できるように提供された。以上では本発明の好ましい実施例に上げて本発明を説明してきたが、該当技術分野における熟練した当業者には、添付の特許請求の範囲に記載された本発明の思想及び領域を逸脱しない範囲内で、本発明を様々に修正及び変更できるということが理解できる。したがって、本発明は、ここに開示された実施形態に制限されるものではなく、ここに開示された原理及び特徴と一致する最も広い範囲の権利を受けるためのものであることは明らかである。

20

【図 1】

FIG. 1



【図 2】

FIG. 2

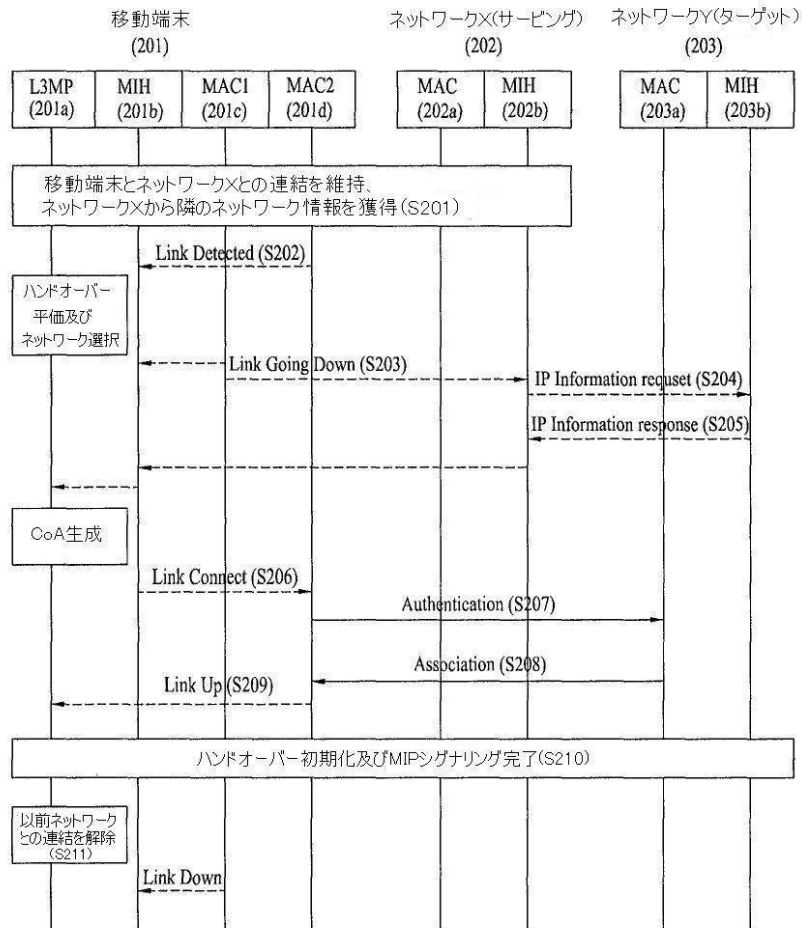
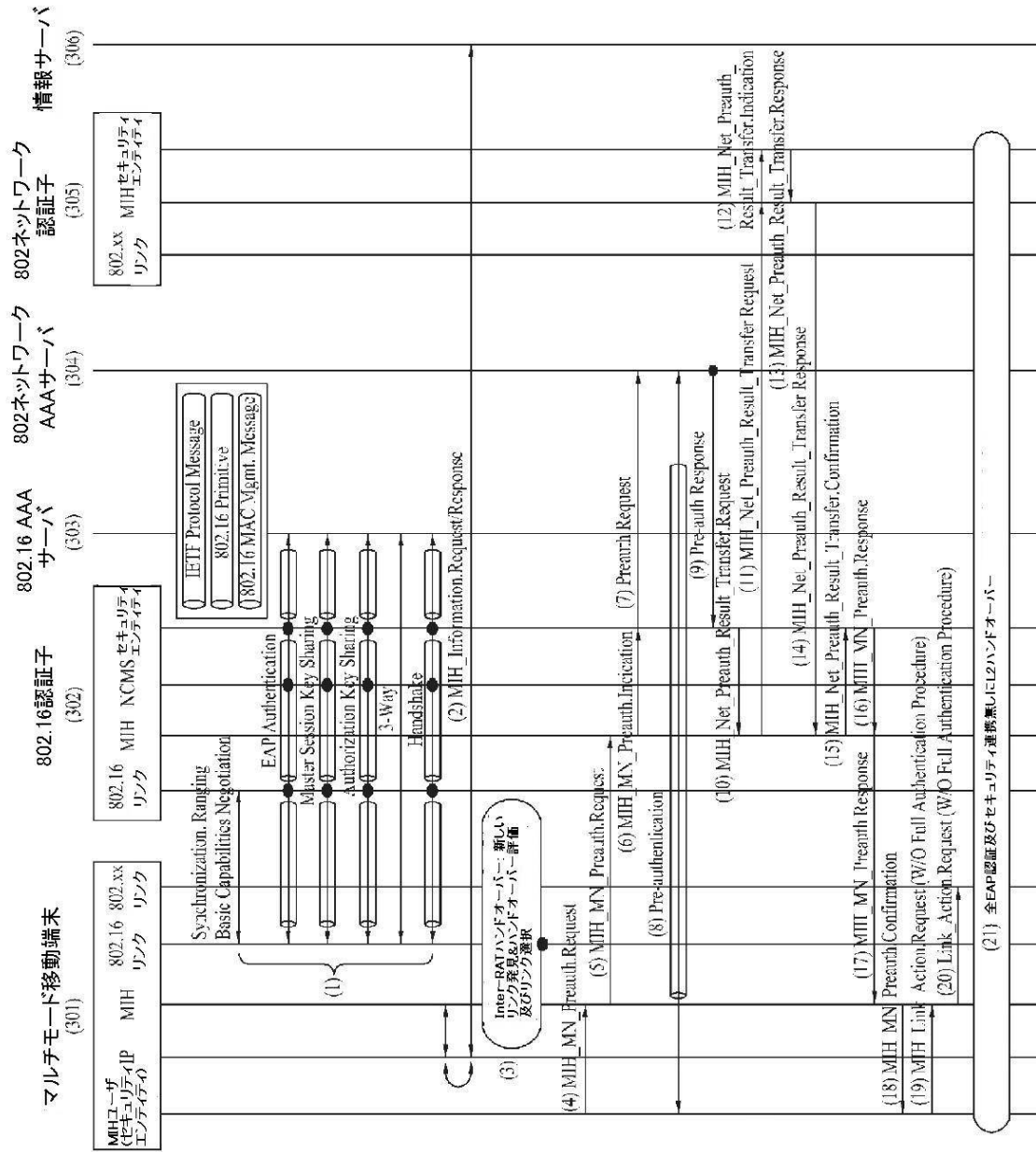


FIG. 3

【図 3】



【図 4】

FIG. 4

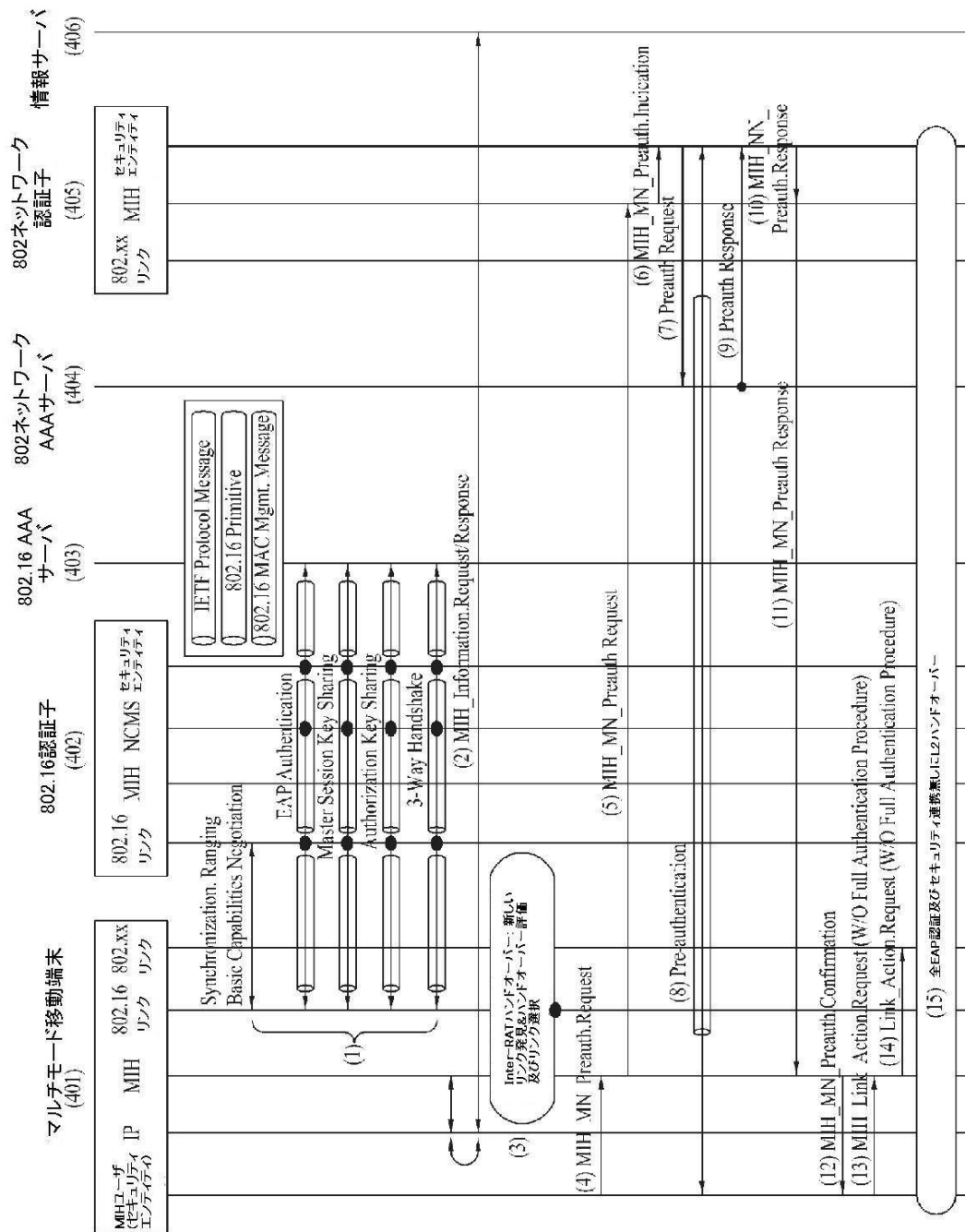
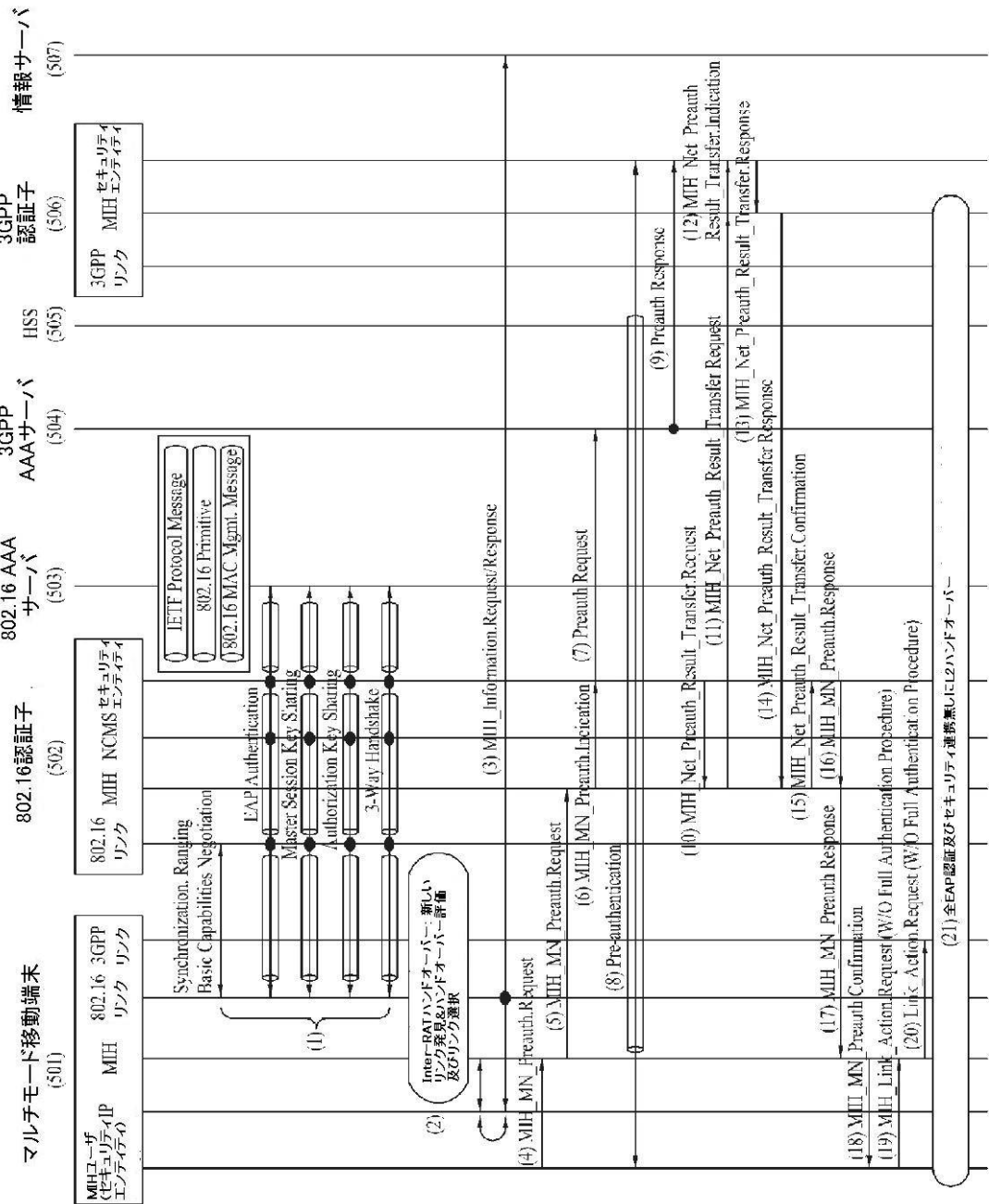


FIG. 5

【図 5】



フロントページの続き

- (31)優先権主張番号 10-2008-0041049
 (32)優先日 平成20年5月1日(2008.5.1)
 (33)優先権主張国 韓国(KR)

前置審査

- (72)発明者 ヨン, エ ラン
 大韓民国 431-080 キョンギード, アニャンーシ, ドンガンーク, ホゲ 1 (イル)
)ードン, エルジー インスティテュート
 (72)発明者 ハ, スン ウン
 大韓民国 431-080 キョンギード, アニャンーシ, ドンガンーク, ホゲ 1 (イル)
)ードン, エルジー インスティテュート
 (72)発明者 パク, ジ ウォン
 大韓民国 431-080 キョンギード, アニャンーシ, ドンガンーク, ホゲ 1 (イル)
)ードン, エルジー インスティテュート

審査官 深津 始

- (56)参考文献 国際公開第2007/007914 (WO, A2)
 特表2008-517516 (JP, A)
 国際公開第2006/083039 (WO, A1)
 特表2008-503108 (JP, A)
 国際公開第2006/135082 (WO, A1)
 特表2008-512892 (JP, A)
 Subir Das, Marc Meylemans, "Technical Requirements document for MIH Security", 2007年 9月 27日, pages 1-11, URL, http://www.ieee802.org/21/doctree/Security_SG/21-07-0302-02-0sec-MIH_Security_Technical_Requirements_Skeleton.doc
 Subir Das, Marc Meylemans, Shubhranshu Singh, Ajay Rajkumar, "An Architecture for Security Optimization During Handovers", 2007年 9月, pages 1-9, URL, <https://mentor.ieee.org/802.21/dcn/07/21-07-0301-01-0sec-security-architecture.ppt>
 Subir Das, Yoshihiro Ohba, "An Architecture for Security Optimization During Handovers", 2007年 9月, pages 1-7, URL, http://www.ieee802.org/21/doctree/Security_SG/21-07-0301-00-0sec-Security_Architecture.ppt
 A. Dutta, V. Fajardo, R. Lopez, Y. Ohba, K. Taniuchi, H. Schulzrinne, "Media-Independent Pre-Authentication (MPA) Implementation Results draft-ohba-mobopts-mpa-implementation-04", 2008年 1月 9日, pages 1-33, URL, <http://tools.ietf.org/pdf/draft-ohba-mobopts-mpa-implementation-04.pdf>

(58)調査した分野(Int.Cl., DB名)

H04W	4/00	—H04W	99/00
H04B	7/24	—H04B	7/26