

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4468449号
(P4468449)

(45) 発行日 平成22年5月26日(2010.5.26)

(24) 登録日 平成22年3月5日(2010.3.5)

(51) Int.Cl.

F I

H O 4 W 84/12 (2009.01)

H O 4 L 12/28 3 1 0

H O 4 W 88/08 (2009.01)

請求項の数 13 (全 19 頁)

(21) 出願番号	特願2007-528619 (P2007-528619)	(73) 特許権者	392026693
(86) (22) 出願日	平成16年8月26日(2004.8.26)		株式会社エヌ・ティ・ティ・ドコモ
(65) 公表番号	特表2008-511223 (P2008-511223A)		東京都千代田区永田町二丁目11番1号
(43) 公表日	平成20年4月10日(2008.4.10)	(74) 代理人	100099623
(86) 国際出願番号	PCT/EP2004/051918		弁理士 奥山 尚一
(87) 国際公開番号	W02006/021236	(74) 代理人	100096769
(87) 国際公開日	平成18年3月2日(2006.3.2)		弁理士 有原 幸一
審査請求日	平成19年4月25日(2007.4.25)	(74) 代理人	100107319
			弁理士 松島 鉄男
		(72) 発明者	ブラサド, アナン・アール
			ドイツ連邦共和国, 80689 ミュンヘン, ゴットハルトシュトラッセ 101
		審査官	岩田 玲彦

最終頁に続く

(54) 【発明の名称】 セキュアハンドオーバをサポートする方法および装置

(57) 【特許請求の範囲】

【請求項1】

あるネットワーク内のあるモバイル端末による第1のネットワークエレメントから別のネットワークエレメントへのセキュアハンドオーバをサポートする方法であって、

前記ネットワークは、あるネットワークエレメントと通信セッションを確立するために必要な鍵を含むセキュリティ関連の情報を有するセキュリティサーバを含むものであり、

前記第1のネットワークエレメントが前記ネットワークへと追加されることに応じて、ネットワークトポロジを認識している管理マシン又は前記セキュリティサーバにより、前記第1のネットワークエレメントに対して、前記ネットワークのトポロジに基づいて、前記第1のネットワークエレメントからのハンドオーバ先の候補となることが期待される候補ネットワークエレメントを自動的に決定するステップと、

セキュリティアソシエーションに基づくハンドオーバをサポートするために前記候補ネットワークエレメントと前記第1のネットワークエレメントとの間にセキュリティアソシエーションを生成するステップであって、セキュリティサーバにより、候補エレメントと前記第1のネットワークエレメントとのペア毎に複数のセキュリティアソシエーションを生成するステップと、前記複数のセキュリティアソシエーションを前記セキュリティサーバから前記第1のネットワークエレメントへと送信するステップとを含むステップと、

前記第1のネットワークエレメントのエリア内に位置する1つ以上のモバイルステーションと前記候補ネットワークエレメントとの間にセキュリティアソシエーションを生成するステップと、

10

20

前記第1のネットワークエレメントによるサービスを受けるモバイル端末を決定し、前記第1のネットワークエレメントによるサービスを受ける前記モバイル端末に対して、前記モバイル端末による前記第1のネットワークエレメントから前記候補ネットワークエレメントのうちの1つへの高速なハンドオーバを可能にするために、前記モバイル端末と前記第1のネットワークエレメントとの間にそれぞれ生成された前記セキュリティアソシエーションを前記候補ネットワークエレメントへと転送するステップと

を含む方法。

【請求項2】

前記第1のネットワークエレメントと候補エレメントの各々からなるあるペアに対するセキュリティアソシエーションは、

前記候補ネットワークエレメントと通信するために前記候補ネットワークエレメントに関連付けられた鍵とする材料と、

前記第1のネットワークエレメントと通信するために前記第1のネットワークエレメントに関連付けられており、前記候補ネットワークエレメントと通信するために必要な前記候補ネットワークエレメントの鍵とする材料により暗号化された鍵とする材料と

を含み、

前記候補エレメントによる復号化の後に前記第1のネットワークエレメントと前記候補ネットワークエレメントとの間の直接的なセキュア通信を可能にするために、前記暗号化された鍵とする材料を前記候補エレメントへと送信する請求項1に記載の方法。

【請求項3】

新たなモバイルステーションによる前記第1のネットワークエレメントのエリアへの進入、または前記ネットワーク内のあるネットワークエレメントの追加、削除または移動のうちの少なくとも1つに基づいて、生成された前記セキュリティアソシエーションを更新するステップをさらに含む請求項1または2に記載の方法。

【請求項4】

起点となるネットワークエレメントと前記候補エレメントとの間のセキュリティアソシエーションを更新するために反復して実行される請求項1～3のいずれか一項に記載の方法。

【請求項5】

前記候補エレメントの決定は、前記候補エレメントのマルチホップ構造を取得するために、前記第1のネットワークエレメントの近隣のエレメントのほかにエレメントの選択を含むものであり、

ホップ数はネットワークポリシーにより決定されるものであり、

候補エレメントまたはホップ数のうちのいずれかまたは両方の決定は、ある候補エレメントへとハンドオーバを行う第1のネットワークエレメントの実能力的な能力または可能性に影響を与える環境的な影響に基づいて行われるものである、

請求項1～4のいずれか一項に記載の方法。

【請求項6】

候補エレメントの決定は、どのネットワークエレメントがハンドオーバの候補として用いる意味がないかを表す地理的な情報に基づくものである、請求項1～5のいずれか一項に記載の方法。

【請求項7】

前記地理的な情報は、ロケーションに関する情報に基づいて決定され、ある候補エレメントに対してハンドオーバが実行される確率または可能性に影響を与える環境的な影響を考慮するものである、請求項6に記載の方法。

【請求項8】

移動に基づいた、候補エレメントの再決定を可能にするために、前記第1のネットワークエレメントまたはその他のネットワークエレメントの移動について候補エレメントの決定を行うユニットへと通知するステップと、

前記移動が近傍グラフの再生成を行うために十分に有意であるかどうかを決定するステ

10

20

30

40

50

ップとを含み、

前記第1のネットワークエレメントの近隣にある一連のエレメントが移動により変化した場合に前記移動が十分に有意であると判断されるものである、

請求項1～7のいずれか一項に記載の方法。

【請求項9】

前記第1のネットワークエレメントと1つ以上の前記候補ネットワークエレメントとの間でコンテキストパラメータを送信するステップをさらに含む請求項1～8のいずれか一項に記載の方法。

【請求項10】

あるネットワーク内のあるモバイル端末による第1のネットワークエレメントから別のネットワークエレメントへのセキュアハンドオーバをサポートする装置であって、

前記ネットワークは、ネットワークエレメントと通信セッションを確立するために必要な鍵を含むセキュリティ関連の情報を有するセキュリティサーバを含み、

ネットワークトポロジを認識し、前記第1のネットワークエレメントが前記ネットワークへと追加されることに応じて、前記第1のネットワークエレメントに対して、前記ネットワークのトポロジに基づいて、前記第1のネットワークエレメントからのハンドオーバ先の候補ネットワークエレメントを自動的に決定する管理マシン又は前記セキュリティサーバと、

セキュリティアソシエーションに基づくハンドオーバをサポートするために、前記候補ネットワークエレメントと前記第1のネットワークエレメントとの間にセキュリティアソシエーションを生成するモジュールであって、候補エレメントと前記第1のネットワークエレメントとのペア毎に複数のセキュリティアソシエーションを生成するモジュールと、前記複数のセキュリティアソシエーションを前記セキュリティサーバから前記第1のネットワークエレメントへと送信するモジュールとを備えるモジュールと、

前記第1のネットワークエレメントのエリア内に位置する1つ以上のモバイルステーションと前記候補ネットワークエレメントとの間にセキュリティアソシエーションを生成するモジュールと、

前記第1のネットワークエレメントによるサービスを受けるモバイル端末を決定し、前記第1のネットワークエレメントによるサービスを受ける前記モバイル端末に対して、前記モバイル端末による前記第1のネットワークエレメントから前記候補ネットワークエレメントの1つへの高速なハンドオーバを可能にするために、前記モバイル端末と前記第1のネットワークエレメントとの間にそれぞれ生成された前記セキュリティアソシエーションを前記候補ネットワークエレメントへと転送するモジュールと

を備える装置。

【請求項11】

前記第1のネットワークエレメントと候補エレメントの各々からなるペアに対するセキュリティアソシエーションは、

前記候補ネットワークエレメントと通信するために前記候補ネットワークエレメントに関連付けられた鍵とする材料と、

前記第1のネットワークエレメントと通信するために前記第1のネットワークエレメントに関連付けられており、前記候補ネットワークエレメントと通信するために必要な前記候補ネットワークエレメントの鍵とする材料により暗号化された鍵とする材料と

を含み、

前記候補エレメントによる復号化の後に前記第1のネットワークエレメントと前記候補ネットワークエレメントとの間の直接的なセキュア通信を可能にするために、前記暗号化された鍵とする材料を前記候補エレメントへと送信するモジュールを備える請求項10に記載の装置。

【請求項12】

請求項3～9のいずれか一項に記載のステップを実行するモジュールをさらに備える請求項10または11に記載の装置。

【請求項 13】

コンピュータ上で、請求項 1～9 のいずれか一項に記載の方法を実行するコンピュータプログラム命令を含むコンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明はセキュアハンドオーバのための方法および装置に関し、具体的には、ネットワークプロトコルに基づいたハンドオーバの候補の選択と、これら候補との信頼関係の生成とに関する。

【背景技術】

10

【0002】

今日、ますます多くの通信リンクがワイヤレスネットワークを通して実装されている。このようなワイヤレスネットワークは、一般的にいわゆるセルラーネットワークとも呼ばれる携帯電話通信ネットワーク、無線 LAN のようなワイヤレスコンピュータネットワーク、または、多種多様なネットワークテクノロジーおよび対応する端末を含むハイブリッドネットワークを含んでいる。

【0003】

ワイヤレスネットワークの一般的な特性は、通常、ワイヤレスネットワークがセルによって組織化されること、すなわち、ある端末が、その端末を取り囲むある特定の範囲または領域に対して機能するいわゆるアクセスポイントを介してネットワークにアクセスできることにある。したがって、同一のセルには存在していない個々の端末間の通信は、アクセスポイントから情報を受信することと、その情報の所定の受信先である端末装置の近隣にある別のアクセスポイントに向けてその情報を配信することとを行うバックボーンネットワークを通して実現されるか、または、アクセスポイントが、受信する所定の端末が位置する範囲に達するまで、その情報をアクセスポイントからアクセスポイントへ送信することによって実現される。

20

【0004】

このようなタイプのネットワークの大きな利点は、端末装置（携帯電話機、PDA、ポータブルコンピュータなど）のユーザが、ネットワークを介して別のユーザとの通信リンクを維持しながら移動できるということである。しかし、これらのタイプのネットワークに生じる問題の 1 つは、ユーザがあるセルの範囲を離脱することがあるために、ユーザおよびそのユーザの端末がアクセスポイントまたは基地局の範囲を離脱してもなお通信リンクを維持する仕組みが必要ということである。

30

【0005】

あるセルの範囲を離脱しても通信を維持するために、端末は、移動した後のユーザのロケーションをカバーする範囲を有する別のセルを介して、アクセスを行い、通信リンクを維持しなければならない。このような手順は、一般的に「ハンドオーバ」と呼ばれている。従来の手順に基づいてハンドオーバを行うためには、新たなアクセスポイントまたは基地局に関してモバイル端末の認証および承認を行う必要がある。これについては、図 1 を参照して概略的に説明する。

40

【0006】

図 1 は、モバイル端末と通信可能なある範囲 100 を有する第 1 のアクセスポイント AP1 と、この範囲内に位置しており、別のアクセスポイント AP2 のサービス範囲 110 へ移動するモバイル端末 MT1 とを示している。ネットワークへの不正アクセスを防止し、アクセスの適切な制御とネットワークによって提供されるサービスの課金および構築とを確保するために、課金のみならず何らかの認証および承認を行わなければならない。一般的にこの種のタスクは、図 1 に示されている認証 (authentication)、承認 (authorization) および課金 (accounting) (AAA) サーバによって実行される。AAA サーバは、端末がネットワークにアクセスしようとするときに、認証および承認のチェックを行い、通信セッションのための鍵の生成および配信

50

、提供サービスの課金などの一般的なセキュリティ環境を受け持つ。

【0007】

モバイル端末MT1が、例えば、アクセスポイントAP1を介してネットワークにアクセスするとき、AP1は、最初にモバイル端末MT1を特定、認証し、次に通信セッションで使用する暗号鍵のような何らかのセキュリティ環境について取り決めるためにAAAサーバと通信する。その後、モバイル端末MT1がアクセスポイントAP2の範囲110へ移動する場合、認証および承認を実行するためにアクセスポイントAP2を介してAAAサーバと通信することにより、新たなアクセスポイントAP2に関して同じ認証および承認の手順を実行しなければならない。

【0008】

この手順には時間がかかるが、その理由は、セキュアハンドオーバー毎にAAAサーバが通信して、最初に認証をチェックし、次に新たなセル内の新たな（「セキュリティコンテキスト」または「セキュリティアソシエーション」とも呼ばれる）セキュリティ環境を取り決めることにより、新たなセキュリティ環境を生成する必要があるからである。

【0009】

前記に鑑みて、本発明の目的は、セキュアハンドオーバーを実行するためのさらに効率的な技術を提供することである。

【発明の開示】

【0010】

本発明の一態様によれば、モバイル装置がハンドオーバー可能な近隣のネットワークエレメント間での信頼関係の生成を利用するセキュアハンドオーバーをサポートする方法が提供される。アクセスポイントのような近隣のネットワークエレメント間でこのような信頼関係が生成されると、AAAサーバとの通信を通してモバイル装置を再認証する必要性を回避することにより、さらに速くさらに効率的な方法でハンドオーバーを行うことができる。

【0011】

一態様によれば、本方法は、ハンドオーバーが実行可能な近隣のネットワークエレメント（アクセスポイント）の特定を含むデータセットである近傍グラフ（neighbour graph）と、AAAサーバと再度通信することなく、近隣のネットワークエレメント間で直接的なハンドオーバーを可能にするセキュリティコンテキスト、セキュリティアソシエーションまたはセキュリティ情報との生成を含む。

【0012】

一実施形態によれば、近傍グラフは、ハンドオーバー可能なアクセスポイントのIDのリストまたは集合と、近隣のアクセスポイントまたは基地局との間の通信のための一連の鍵とを保持する。このような鍵は、例えば、暗号鍵、インテグリティチェック鍵であり、さらに、暗号化アルゴリズムの識別情報、または認証アルゴリズムの識別情報のパケットを含むことができる。

【0013】

このような近傍グラフにより、ハンドオーバーのターゲットとなる近隣のネットワークエレメントへの高速なハンドオーバーを可能にするために必要な情報が提供される。

【0014】

一実施形態によれば、近傍グラフの生成は、近隣にあるハンドオーバーの候補ネットワークエレメントの選択または特定を含む。このような特定または選択を行うため、例えば、ネットワークポロジを表現したものを保持する管理マシンに記憶されたネットワークポロジを参照することができる。

【0015】

一実施形態によれば、セキュアハンドオーバーをサポートする方法は、ハンドオーバーを開始する起点となるネットワークエレメントから候補エレメントに向けて、近傍グラフに含まれている近隣のエレメントに関して生成されたセキュリティコンテキストを送信するステップを含む。

【0016】

一実施形態によれば、ハンドオーバーの候補および対応するセキュリティコンテキストを含んだ近傍グラフに関する情報は、あるネットワークエレメントがA A Aサーバにログオンするときに、「ピギーバック」としてそのネットワークエレメントに向けて送信することができる。すなわち、これは、近傍グラフを配信するためにネットワーク内でさらなるトラフィックを必要としないということを意味する。しかし、この手順を実施するためには、ネットワーク情報および関連する近傍グラフの情報がA A Aサーバで利用可能でなければならない。

【0017】

一実施形態によれば、本発明に係る方法は、ハンドオーバーが行われる近隣のエレメントを通して、あるアクセスポイントからのコンテキストパラメータの送信を可能にする。これは、A A Aサーバの仲介により全ての情報をリダイレクトすることなく、関連する近隣のアクセスポイント間で削減されたセキュアチャネルを直接使用することにより、ハンドオーバー中のサービスの品質を改善できる。さらに、（ロケーション、使用するサービス、サービス構成またはその他のパラメータといったユーザの状況または通信自体の状況に関連する任意のパラメータである）コンテキストパラメータの送信は、通信セッションが今までのアクセスポイントで行われていたのと同じやり方で新たなアクセスポイントにおいて継続できるように、サービスのハンドオーバーが関連する全てのコンテキスト情報を転送することによりシームレスな方式で実行できることを確保することによってハンドオーバーの品質を改善することができる。

【発明を実施するための最良の形態】

【0018】

図2は、本発明の実施形態に関して使用されるネットワークの構成を概略的に示している。図1と同様に、セキュリティタスクを担当するA A Aサーバが示されている。いくつかのアクセスポイントA P 1～A P 7は、それぞれのサービス範囲とともに示されている。さらに、例えば、ネットワークエレメントのリストを保持することや、ネットワークエレメントのアクセスおよび取り外しを管理することなどにより、ネットワークを一般的に管理するタスクを有する管理マシンMMが示されている。管理マシンは、ネットワークポロジを認識しており、すなわち、ネットワークエレメントのロケーションと、ネットワークエレメントによってカバーされる範囲とを認識している。一般的に、ネットワークエレメントに関する情報はセキュリティと関連があるため、管理マシンは、鍵またはその他のセキュリティに関する手段のうちのいずれかまたは両方により、その管理マシンへのアクセスを制限することによって保護されているセキュアロケーションである。

【0019】

A A Aサーバは、鍵、同一性などのセキュリティに関連する情報をネットワークエレメントごとに有している（または要求時に生成する）。ネットワークエレメントのスイッチがオンになると、そのネットワークエレメントはA A Aサーバにログオンしなければならない。A A Aサーバはネットワークエレメントのリストを保持し、エレメントが信頼されているか否か、または、ログオンしているか否か、さらにはそれらの共有鍵およびセキュリティアソシエーション（S A）を把握している。セキュリティアソシエーションは、本明細書においては、ネットワークエレメントとの通信セッションを確立するために必要なあらゆるセキュリティに関する情報を意味する。このセキュリティアソシエーションは、暗号鍵、インテグリティチェック鍵を含み、さらには暗号化アルゴリズムの識別情報または認証アルゴリズムに関する識別情報のパケットを含む。

【0020】

本実施形態において、A A Aサーバおよび管理マシンは、セキュア通信チャネルを有するか、または確立できるものとする。セキュア通信チャネルは、A A Aサーバおよび管理マシンの適切な構成によりネットワーク展開の間に確立される。

【0021】

以下、図2のシステムを用いて、本発明の一実施形態に基づくセキュアハンドオーバーを可能にする方法がどのように行われるかを説明する。

【0022】

管理マシンMMはネットワークのトポロジを認識しているため、管理マシンは、ネットワークエレメントごとにそのネットワークエレメントの近隣にあるネットワークエレメントを認識しており、または、少なくともあるネットワークエレメントの近隣のエレメントを見つけ出す能力を備えている。図3に示されているような一実施形態によれば、ステップ300において、管理マシンは、あるネットワークエレメントに関して、このネットワークエレメントからハンドオーバーする先の候補がどれであるかを決定する。一般的に、このような候補は近隣のエレメントであり、すなわち、これらのネットワークエレメントのサービス範囲はそのネットワークエレメントと隣接しているか、または重なっている。次に、ステップ310において、ハンドオーバーの起点となるあるネットワークエレメントと候補との間にセキュリティアソシエーションが生成される。

10

【0023】

図2に示されているネットワーク構成の場合、これは、起点となるエレメントであるネットワークエレメントAP3に関して、ネットワークエレメントAP1、AP2、AP4およびAP6が一連の候補に含まれることを意味する。次に、AP3とAP1、AP2、AP4およびAP6との間にセキュリティアソシエーションが生成される。すなわち、これは、セキュリティアソシエーションが生成された後、AP3から候補であるAP1とAP2とAP4とAP6とのうちのいずれかへのハンドオーバーが可能になり、モバイル装置を候補のうちのいずれかへハンドオーバーするときAP3と候補との間で生成されたセキュリティアソシエーションが使用できるので、AAAサーバでモバイル装置を再認証することなくハンドオーバーを実行できることを意味する。

20

【0024】

あるネットワークエレメントに関するハンドオーバーの一連の候補は、そのネットワークエレメントと候補との間の対応するセキュリティアソシエーションとともに「近傍グラフ」と呼ばれる。AP3に関して説明したこのような近傍グラフは、前記のようなやり方で全てのネットワークエレメントに関して実行することができ、その結果、いずれかのネットワークエレメントから別のネットワークエレメントへのさらに高速かつ効率的なハンドオーバーが可能になる。

【0025】

次に、さらなる実施形態に基づいた、近傍グラフを生成することによりセキュアハンドオーバーを可能にする方法について図4を参照して説明する。本実施形態では、最初にステップ400において、ネットワークエレメントは、例えば、電源を入れること、またはネットワークへ新たに追加されることにより「ウェイクアップ」し、次にAAAサーバへログオンする。図2と同様に、本実施形態においても、AAAサーバと管理マシンMMとの間にセキュアチャネルと「信頼関係」が存在する。これらに基づいて、ネットワークエレメントは、管理マシンと通信するためにAAAサーバからトークンを受信する（ステップ410）。AAAサーバは、さらにトークンを管理マシンへ送信する（ステップ420）。

30

【0026】

管理マシンは、ネットワークエレメントのロケーションをチェックし、そのネットワークエレメントからハンドオーバーするための候補を決定する（ステップ430）。これは、前述の実施形態と同様に近隣のエレメントだけである。しかし、特定の実施形態によれば、候補には、直接的に近隣のものというわけではなく、「中間ネットワークエレメント」を介してのみ到達することができるネットワークエレメントがさらに含まれ、これは「マルチホップ」とも呼ばれている。この中間ネットワークエレメントは、ネットワークポリシーに依存し、可能であればその他のパラメータにも依存してハンドオーバーの候補を決定する場合に候補に含めることができる。

40

【0027】

なお、本明細書において「ホップ」または「マルチホップ」という用語は、以下では、直接的な近隣のネットワークエレメントの他に、あるネットワークエレメントへのハンド

50

オーバが中間ネットワークを介して実行できるように、「近隣の近隣」である別のネットワークエレメントが含まれる状況に関連するものであることを理解されたい。以下この状況をマルチホップと呼ぶことにする。さらに本明細書において、近傍グラフの生成は、起点となるネットワークエレメントに対して直接的に近隣のものではないネットワークエレメントを含むことも理解されたい。

【0028】

一実施形態によれば、ホップ数は固定することができる。しかし、特定の実施形態では、あるパラメータ、例えば、ユーザが期待する速度とネットワークのロケーションとに基づいてホップ数を決定できる。例えば、列車のレールの近くにあるネットワークエレメントは、高速で移動するユーザに対するものであることが多く、その結果、マルチホップ近傍グラフが有利である。ホップ数は、許容されているデータレートに依存する個々のネットワークエレメントのサービス範囲（セルサイズ）にもよることができる。

10

【0029】

あるネットワークエレメントからハンドオーバする候補エレメントが決定されると、この情報（「候補に関する情報」）は、ハンドオーバの起点となるネットワークエレメントに向けて送信される（ステップ440）。このようにして送信された候補に関する情報は、例えば、候補ネットワークエレメントのIDと、テクノロジーの有用性に依存した（例えば、移動していて固定的ではない場合に、GPSシステムから得られる）、候補ネットワークエレメントのロケーションと、それらの機能（例えば、利用可能なサービス、帯域幅およびその他のサービスに関連するパラメータ）と、起点となるネットワークエレメントからのホップ数とを含んでいる。この情報の中で最も重要なのは、候補エレメントのIDである。

20

【0030】

ハンドオーバの候補ネットワークエレメントに関して受信した情報に基づいて、起点となるネットワークエレメントは、この候補エレメントに関する情報をAAAサーバに向けて送信し、候補ネットワークエレメントとのセキュリティアソシエーションを生成するように要求する（ステップ450）。

【0031】

次にAAAサーバは、セキュリティアソシエーションを生成し（または、既に生成されているならば取得し）、それらをハンドオーバの起点となるネットワークエレメントへ送信する。本実施形態では、セキュリティアソシエーションとは、例えば、起点となるネットワークエレメントに関連するものであって、それぞれの候補エレメントに属する鍵によってそれぞれ暗号化される鍵のような暗号情報を意味する。したがって、例えば、AP3が起点となるネットワークエレメントである場合にAP3とAP4との間のセキュリティアソシエーションは、AP4に属するある鍵または複数の鍵によって暗号化されたAP3に属するセキュリティ関連の情報（鍵、暗号化アルゴリズム、および、例えばハッシュアルゴリズムのような認証アルゴリズム）である。その結果、このようにして暗号化された情報は、AP3とAP4との間の「セキュリティアソシエーション」を形成する。このようなセキュリティアソシエーションは、起点となるネットワークエレメントと候補エレメントとの間の全てのペアに関して生成される。

30

40

【0032】

一般的に、セキュリティアソシエーションは、（一般的にコンピュータであるが、ユーザまたはソフトウェアコンポーネントでもよい）2個以上のエンティティ間の関係であり、エンティティが通信するために暗号化のようなセキュリティサービスをどのように使用するかについて表現したものと考えることができる。

【0033】

次に、ネットワークエレメントは、（AAAサーバによって実行される）個々の候補ネットワークエレメントの鍵によって暗号化されたSAを候補ネットワークエレメントに向けて送信する（ステップ470）。これはマルチキャストでもユニキャスト（すなわち、全てのセキュリティアソシエーションは、一緒に単一の大きなセキュリティアソシエーシ

50

ョンメッセージとして各ネットワークエレメントへ送信されるが、時間がかかる)でもよい。各ネットワークエレメントは、そのS Aまたはその一部を復号化できる。これは、各候補エレメントが、起点となるネットワークエレメントのセキュリティ関連の情報(鍵とする材料(keying materials)、暗号化アルゴリズム、ハッシュアルゴリズムのような認証アルゴリズムなど)を認識することを意味し、逆もまた同様である。このことが今度は、A A Aサーバにおいてモバイル端末を再認証することなく、このようにして生成された「近傍グラフ」に基づいて起点となるネットワークエレメントから候補エレメントのいずれかに向けてセキュア(ダイレクト)ハンドオーバを実行することを可能にする。

【0034】

言い換えると、起点となるネットワークエレメントに関連付けられた鍵とする材料は、ある候補ネットワークエレメントの鍵とする材料により暗号化され、続いてその候補ネットワークエレメントへと転送される。候補ネットワークエレメントは、その候補ネットワークエレメント自体が有する復号化のための鍵とするエレメント(keying elements)を用いて、起点となるネットワークエレメントに関連付けられた鍵とする材料を復号化することができ、それにより、起点となるネットワークエレメントと通信するために必要な鍵とするエレメントまたはセキュリティ情報を受信する。さらに、起点となるネットワークエレメントは、候補エレメントの鍵とする材料を受信する。セキュリティ上の理由から、これら鍵とするエレメントは、起点となるネットワークエレメントへと送信される前に、前記起点となるネットワークエレメントの持つ鍵とする材料を用いて暗号化される。次に起点となるネットワークエレメントは、ネットワークにログオンしたときに提供された、起点となるそのネットワークエレメント自体の鍵とする材料を用いてそれらを復号化することができる。

【0035】

したがって、一実施形態によれば、起点となるネットワークエレメントへ送信されるメッセージは、以下のようになる。

$((C_{cand}(Key_{orig}); C_{orig}(Key_{cand}))_{i=1}, \dots, (C_{cand}(Key_{orig}); C_{orig}(Key_{cand}))_{i=n})$

【0036】

本明細書において、メッセージパート $((C_{cand}(Key_{orig}); C_{orig}(Key_{cand}))_{i=1})$ は、候補エレメント $i = 1$ の鍵とするエレメントを用いて暗号化アルゴリズム C_{cand} により暗号化された、起点となるネットワークエレメントの鍵とするエレメント Key_{orig} と、候補ネットワークエレメント $i = 1$ の鍵とする材料 Key_{cand} が、起点となるネットワークエレメントの鍵とする材料 C_{orig} を用いて暗号化されることを意味する。このようなメッセージパートが、起点となるネットワークエレメントと n 個の各候補エレメントとの間で構成されるペア毎に生成されて、起点となるネットワークエレメントへ送信されるため、メッセージ全体は、上述のようにこのようなメッセージエレメントを n 個含んでいる。

【0037】

鍵とする材料は、一般的に、セキュリティサーバ、または鍵とする材料およびその他のセキュリティ関連の情報の生成とメンテナンスのために設けられる、信頼できるユニットを使用して生成される。セキュリティサーバは、例えば、A A Aサーバである。

【0038】

起点となるネットワークエレメントが享受する信頼のレベルに応じて、起点となるネットワークエレメントに向けて鍵とする材料 Key_{cand} だけを配信するために、起点となるネットワークエレメント自体によって上記メッセージの暗号化を行うことが許されている。次に、起点となるネットワークエレメントは、 $((C_{cand}(Key_{orig}))$ を取得するために、それ自体によって暗号化を行うが、別の実施形態によれば、暗号化はA A Aサーバのような別のユニットにおいて行われる。

【0039】

各候補エレメントが、起点となるネットワークエレメントとの通信を可能にするセキュ

リティアソシエーションを受信すると、起点となるネットワークエレメントについての近傍グラフができる。上述したやり方で全てのネットワークエレメントについて近傍グラフを生成することが好ましいことを理解されたい。

【0040】

セキュア近傍グラフを生成する上述の手順は、所定の間隔で反復することができる。これにより、新たなネットワークエレメントがネットワークに追加された場合に近傍グラフの更新を可能にする。

【0041】

代替的または付加的に、新たなネットワークエレメントがネットワークに追加された場合に近傍グラフを再生成することができる。この追加は、このような場合に近傍グラフの再生成をトリガするように構成された管理マシンによって通知される。これに対し、あるネットワークエレメントが、ネットワークパラメータとして設定されている所定の時間にわたってアイドル状態の場合、そのネットワークエレメントは近傍グラフから削除することができる。

【0042】

以下、ハンドオーバー先の対応する候補エレメントとの通信を可能にする近傍グラフを、そのターゲット、すなわち起点となるネットワークエレメントに向けて転送する方法のバリエーションに焦点を当てていくつかの実施形態について説明する。

【0043】

一実施形態によれば、AAAサーバは、ネットワーク構成に関する情報を有しており、新たなネットワークエレメントのログオン時に近傍グラフ（または、ハンドオーバー先の候補エレメントのリスト）をその新たなネットワークエレメントへ送信する。これにより管理マシンは必要ではなくなるが、AAAサーバがネットワークトポロジを認識するよう構成するべきであり、かつ、起点となるあるネットワークエレメントに対応するハンドオーバー先の候補エレメントを決定できるようさらに構成するべきであることを意味する。

【0044】

さらなる一実施形態によれば、ネットワークエレメントのログオン時にAAAサーバは管理サーバと通信し、候補エレメントをAAAサーバへ送信する。これは既に詳細に説明した実施形態と対応している。

【0045】

さらなる一実施形態によれば、AAAサーバはSA（セキュリティアソシエーション）に関する情報を有する各トークンを起点となるネットワークエレメントおよび管理マシンに向けて送信する。これは、AAAサーバと管理マシンとの間、および、AAAサーバと起点となるネットワークエレメントとの間にそれぞれ信頼関係が存在するという条件の下で可能である。トークンの配信は鍵とするエレメントで構成されており、その結果、管理マシンおよび起点となるネットワークは安全なやり方で直接通信できる。換言すれば、管理マシンと起点となるネットワークとの間に信頼関係が確立されている。次に、起点となるネットワークエレメントは、管理マシンと通信し、ハンドオーバー先の一連の候補エレメントを取得することができる。次に、既に詳細に説明したようなやり方で近傍グラフの生成が続く。

【0046】

一実施形態によれば、近傍グラフの生成は以下の通り行うことができる。ネットワークエレメントの要求時（例えば、ログオン時）に、管理マシンにより直接的に、またはAAAサーバにより候補エレメントのリストが決定される。次にAAAサーバは、一連の候補エレメントに基づいて、候補エレメント毎に、起点となるネットワークエレメントと各候補エレメントとの鍵とする材料を含むセキュリティアソシエーションを生成する。次に、それぞれのセキュリティアソシエーションは、AAAサーバから各候補エレメントへ直接送信され、それにより、候補エレメントと起点となるネットワークエレメントとの間の通信がそれぞれ可能になる。

【0047】

以下、ハンドオーバ先の候補エレメントを決定する方法について詳細に説明する。

【0048】

候補エレメントを決定するためには以下の情報が必要である。

1つ目は、ログオン時に使用するネットワークエレメントIDである。固定的なネットワークの場合はこれで十分である。固定的なネットワークの場合（ネットワークエレメントが移動しない場合）、近隣のネットワークエレメントをこの情報で十分に決定できるからである。

2つ目は、ネットワークエレメントのロケーションであり、ネットワークエレメントが移動可能であるときに必要となる。

【0049】

管理マシンがネットワークエレメントIDを受信すると、管理マシンはネットワーク構成に基づいて近隣のエレメントを決定する。このため、実施形態に応じて様々な方法を用いることができる。

【0050】

一実施形態によれば、管理マシンは、単純にネットワークエレメントのIDをチェックし、ネットワーク構成内のそのネットワークエレメントが維持するロケーションを見つける。次に、ネットワークエレメントは、ネットワークポリシーによって定められているホップ数に達するまで、近隣の全てのネットワークエレメントのIDを送信する。

【0051】

さらなる実施形態によれば、管理マシンは、上述のように近隣で利用できるネットワークエレメントをチェックする。しかし、本実施例では、信号を歪ませる壁またはその他のものが存在し、これによって、モバイル装置によるこのようなネットワークエレメントへのハンドオーバが不可能にならないかどうかを管理マシンがさらにチェックする。このような外部の影響に基づいて、管理マシンは、ハンドオーバのために特に用いることができるネットワークエレメントのIDを近傍グラフから決定する。本実施形態では、ネットワークポリシーに基づくホップ数も同様にチェックし、それに応じて候補エレメントを決定する。

【0052】

さらなる実施形態によれば、候補エレメントは上述した2つの方法のいずれかと同様に決定されるが、本実施形態では、ホップ数はモバイル端末またはネットワークエレメントの方向に依存する。建物内部への方向であれば、ユーザは歩行しており、ユーザの速度は2ホップ以上を必要としないので、1ホップの情報だけで十分と考えられる。しかし、モバイル端末またはネットワークエレメントが街路の方向であれば、ユーザは運転している可能性があり、したがって本実施形態では、候補エレメントは、マルチホップを含むように決定される。移動方向に代えて、または、移動方向の他に、さらにユーザまたはネットワークエレメントのロケーションに依存して、そして、このようなロケーションにおける環境の条件に基づいてホップ数を決定することができる。例えば、ロケーションが列車のレールに近いならば、ユーザは列車に乗車した後であり、おそらく、高速に移動するので、マルチホップが好ましく、候補エレメントにマルチホップを含めるべきである。ネットワークパラメータを定義するときに適切に選択できる環境状態に応じて、ホップ数に関する詳細を選択できる。

【0053】

さらなる実施形態によれば、ネットワークエレメントは、（例えば、GPSに基づいて）そのネットワークエレメント自体のロケーションを見つける能力を有しており、そのIDおよび座標を例えば管理マシンへ送信する。これは、特にトポロジが変化する状況、すなわち、（モバイル装置を携帯するユーザだけでなく）ネットワークエレメント自体が移動可能であるという状況で役に立つ。次に管理マシンは、起点となるネットワークエレメントのロケーションに基づいて近隣のネットワークエレメントのIDおよび座標を決定する。これは、ネットワークポリシーによって定められ、さらには移動の方向にも基づくホップ数に依存した候補の決定を含んでいる。

10

20

30

40

50

【0054】

さらなる実施形態によれば、管理マシンがサイトサーベイ情報を有する場合に、改良された決定を行うことができる。サイトサーベイ情報は、例えば、ネットワークエレメントが所与のロケーションに位置するときに信号強度がどのようになるかについての情報を含んでいる。代替的または付加的には、地理的な情報に基づいて決定を行うことができる。地理的な情報は、例えば、ハンドオーバーの候補として使用する意味のないネットワークエレメントを示す情報を含んでいる。これは、この地理的な情報に基づいて決定でき、候補エレメントに対してハンドオーバーを行う確率または可能性に影響を与える環境的な影響を考慮するものである。例えば、列車のレールのロケーションと一致するために、ユーザが非常に高い確率で列車内にいることをユーザの位置情報が示す場合に、起点となるエレメントの近隣のエレメントではあるものの、レールが位置する、つまり列車とユーザが移動する地理的なエリアをカバーしない候補エレメントを含める意味はない。しかし、このような条件では、列車は高速に移動し、したがって、高速なハンドオーバーの手順が必要となるので、レールの方向にホップ数を増加させることが有益である。

10

【0055】

上記実施形態では、各ネットワークエレメントは、ロケーションの変化時に、その新たな座標を管理サーバへ送信することが好ましい。ロケーションが変化すると、新たな近傍グラフを生成することが好ましい。代替的に、ロケーションの変化に基づいて、候補エレメントを決定する管理マシンまたはユニットは、移動が有意（significant）であるため新たな近傍グラフを生成すべきかどうかをチェックするために有意性チェック（significance check）を行う。例えば、ロケーションの変化が、近隣の一連のネットワークエレメントが変化したことを意味するならば、一実施形態によれば、これは新たな近傍グラフを生成するために十分有意であるとみなされる。これに対し、移動が近隣の一連のエレメントに対して変化を生じさせない限り、一実施形態では、移動が有意ではなく、新たな近傍グラフを生成する必要がないことを決定できる。

20

【0056】

一実施形態によれば、本発明は、メッシュネットワーク、例えば固定的なワイヤレスメッシュネットワークに適用できる。これは、ワイヤレスメッシュネットワークにはトポロジの変化がないことを意味する。上述の方法は、ネットワークの安価な展開または拡張に使用できる。例えば、新たなネットワークエレメントがLANに追加されるとき、その新たなネットワークエレメントは、最初にネットワークアドミニストレータによりネットワークに追加される。その後、その新たなネットワークエレメントがネットワークにログオンするとき、上述したやり方で近傍グラフの（再）生成をトリガすることができる。ネットワークトポロジは時間的に変化しないので、ネットワークエレメントのロケーションの変化による近傍グラフの修正は不要である。

30

【0057】

トポロジの変化の影響を受けるワイヤレスメッシュネットワークの場合、状況は多少異なる。このような場合にはロケーションに関する情報が必要となるため、トポロジの変化によりシステムが少し複雑になる。ロケーションに関する情報は、例えば、GPSまたはその他の位置決め技術（positioning technology）を用いることにより見出すことができる。本実施形態では、ネットワークエレメントは、好ましくは管理マシン、または候補エレメントの決定を行うユニットに対し、そのネットワークエレメントが移動するたびにロケーションを通知する。このような一実施形態では、それぞれの移動は新たな近傍グラフを意味する。この場合、ネットワークエレメントは近傍グラフの要求とともにロケーションに関する情報を送信することができる。特定の一実施形態では、新たな近傍グラフの生成が必要となるほど移動が十分に有意であるかどうかをチェックするユニットを設けることができる。このユニットは、管理マシン、AAAサーバ、またはネットワークエレメント自体にも実装できる。

40

【0058】

上述の実施形態によれば、第1のネットワークエレメントとハンドオーバー先の候補エレ

50

メントとの間のセキュア通信を可能にする近傍グラフが生成される。一実施形態によれば、このようにして生成されたセキュア通信チャンネルは、ハンドオーバーが行われる近隣のネットワークエレメント（アクセスポイント）を介して、あるアクセスポイントからコンテキストパラメータを送信するために使用できる。これにより、AAAサーバの仲介によって全ての情報をリダイレクトせずに、関連する近隣のアクセスポイント間の短縮したセキュアチャンネルを直接使用することにより、ハンドオーバー中のサービスの品質を改善できる。さらに、（ロケーション、使用されるサービス、サービスの設定、またはその他のパラメータといったユーザの状況または通信自体の状況に関連付けられるいずれのパラメータでもよい）コンテキストパラメータの送信は、今までのアクセスポイントで行われていたやり方と同じやり方で新たなアクセスポイントにおいても通信セッションを継続できるようにするために、関連する全てのコンテキスト情報を転送することによりサービスのハンドオーバーをシームレスなやり方で実行できるようにすることによってハンドオーバーの質を改善できる。単なる一例ではあるが、転送されるコンテキスト情報は、帯域幅またはデータレートなどの、サービスまたは利用可能なサービスの品質に関する情報を含むことができ、したがって、ハンドオーバー後の通信セッションは、これらコンテキスト情報に基づいて適切なやり方で継続できる。

【0059】

本発明の一実施形態に基づくシステムとその有利な効果とについて図5を参照して説明する。図5の左側に、IEEE 802.11規格に準拠したワイヤレスLANシステムにおけるハンドオーバーの手順のメッセージシーケンスを示している。このメッセージシーケンスにおいて、今までのアクセスポイントAPに接続しており、今度は新たなアクセスポイントAPnewに対してハンドオーバーをしようとしているステーションSTAが示されている。最初に、図5の上方に示されているように、異なる3個のチャンネルを通してプローブ要求およびプローブ応答がステーションSTAにより送信される。規格自体によれば3個のチャンネルは必要とされないが、良好に実施をするために3個のチャンネルを使用するというところにここで注意すべきである。これは、ハンドオーバーのために適切または利用可能な新たなアクセスポイントを単に探すことを目的としている。このため、ステーションSTAは、現在進行中の通信のチャンネルとは異なる3個のチャンネルを通してこれらの要求を送信する。ハンドオーバーの準備ができている全てのアクセスポイントは、シーケンス図に示されているように対応する応答を送信する。

【0060】

次に新たなアクセスポイントが選択されると、IEEE 802.11規格に基づく用語であるオープンシステム認証が行われる。このオープンシステム認証とは、ステーションが新たなアクセスポイントとメッセージを交換することを意味するに過ぎない。このオープンシステム認証はまだセキュリティパラメータを含んでいないため、セキュア送信またはセキュリティチェックがこの認証に含まれているという意味で「真の認証」ではなく、それゆえ「オープンシステム認証」と呼ばれている。

【0061】

オープンシステム認証の後、リアソシエーションのプロセス、すなわちステーションSTAがそれ自体を新たなアクセスポイントと関連付けるプロセスが続く。このため最初に、ステーションから新たなアクセスポイントAPnewに向けてメッセージが送信される。次のステップで、今までのアクセスポイントと新たなアクセスポイントとの間で信頼関係を生成すべく認証手順を実行するために、今までのアクセスポイントはAAAサーバと通信する。次に、2個のアクセスポイントの間の信頼関係の確立を完了し、新たなアクセスポイントがモバイルステーションを引き継ぐことを最終的に認めるために、今までのアクセスポイントは新たなアクセスポイントに向けてメッセージを返却する。後述する後続の2つのステップを含むこの手順は、今までのアクセスポイントと新たなアクセスポイントとの間のいわゆるIAPP移動手順（IAPP move producer）である。IAPP（inter-access point protocol）の移動手順に基づくこれらメッセージの交換は、最初に、新たなアクセスポイントAPnewがモバイ

ルステーションSTAを引き継ぐことを今までのアクセスポイントに向けて通知し、認証（IAPP移動手順中の第1番目から第4番目のメッセージ）を実行するという目的を有する。第5番目および第6番目のメッセージは、コンテキスト情報、例えばサービスと進行中の通信セッションの特性とに関連付けられたコンテキスト情報の転送のために使用できる。

【0062】

リアソシエーションが行われた後、EAP-TLSが最も標準的である認証が行われる。本明細書において、EAPは拡張認証プロトコル（`extensible authentication protocol`）の略語であり、TLSはトランスポートレイヤセキュリティの略語である。図における認証に関して示されているメッセージシーケンスは、IEEE 802.11i規格に基づいている。図からわかるように、この認証は多くのメッセージの交換を含んでおり、さらに、2段階のメッセージ交換、すなわちステーションSTAから新たなアクセスポイントAPnewへ、および新たなアクセスポイントAPnewからAAAサーバへの段階と、新たなアクセスポイントを経由してステーションSTAへ戻る段階とを含む。図5の左側のメッセージシーケンス図に示されているようにメッセージ全体がハンドオーバー遅延を生じ、オープンシステム認証からEAP-TLS認証へのメッセージは、新たなアクセスポイントAPnewにおけるステーションの再認証に関連した再認証による遅延を生じる。

【0063】

以下、本発明の一実施例に基づく方法およびシステムの有益な効果について、図5の右側のメッセージシーケンス図を参照しながら説明する。この図からわかるように、ここでのプローブ要求およびプローブ応答は、図5の左側の図と同じである。同様に、プローブ要求およびプローブ応答の後のオープンシステム認証も図5の左側と同じである。さらに、リアソシエーションに関連したシーケンスも左側のメッセージシーケンス図と原理的に同じである。しかしながら、本実施形態におけるコンテキストパラメータの送信（IAPP移動手順における最後の2つのメッセージ）は、例えば（複数の）鍵、および、おそらくは例えば暗号化アルゴリズムまたはハッシュアルゴリズムといった認証アルゴリズムのうちのいずれかまたは両方のようなその他のセキュリティ関連の情報といった、新たなアクセスポイントがステーションSTAと通信するために必要なセキュリティコンテキストの送信を含んでいる。

【0064】

図5の右側のメッセージシーケンス図の下部からわかるように、新たなアクセスポイントAPnewにおけるステーションSTAの実際の再認証は、左側の場合よりもかなり高速であって、2つの認証メッセージの交換だけを含んでいる。その理由は、本発明の実施形態によれば、ステーションSTAと新たなアクセスポイントとの間のセキュリティアソシエーションは、例えばIAPP手順に関連して既に説明したようなセキュリティコンテキストの転送により、実際のハンドオーバー前に既に生成され配信されているからである。したがって、新たなアクセスポイントでステーションSTAの認証を実行するために、一対の認証メッセージの交換（チャレンジとレスポンス）だけが必要となる。さらに、図5の右側の図からわかるように、関連するセキュリティ情報の全てが通信する相手に対して予め配信されているので、認証サーバAAAはこの認証手順に関与しない。図5の左右のメッセージシーケンス図の比較からわかるように、再認証による遅延と、それによるハンドオーバー遅延とは、図5の左側に示されている従来技術に比べると、本発明に基づく実施形態において大幅に短縮される。

【0065】

以下、本発明のさらなる実施形態に基づく有利な効果について図6を参照して説明する。図6の左側は、図5の右側のメッセージシーケンス図と同一のメッセージシーケンス図を示している。IAPP移動手順に関して、コンテキスト情報の転送のために使用される最後の2つのメッセージは、ステーションSTAが新たなアクセスポイントAPnewと通信できるように、セキュリティコンテキストの転送すなわち通信する相手間での関連し

た鍵の交換を含んでいることにここで注意すべきである。このセキュリティコンテキストまたはセキュリティアソシエーションがI A P P移動手順の間に転送されると、新たなアクセスポイントA P n e wにおけるS T Aの実際の認証は、A A Aサーバが関与することなく、図5の右側および図6の左側に示されているような迅速な方式で実行できる。

【0066】

右側には、本発明のさらなる実施形態に基づくメッセージシーケンス図が示されている。本実施形態では、セキュリティコンテキストパラメータまたはセキュリティアソシエーションの転送は既に行われていること、つまり、新たなアクセスポイントA P n e wは既にステーションS T Aとの通信を可能にする関連した鍵を既に認識していることを想定している。これは、上述の本発明の実施形態に関連して説明したようなセキュア近傍グラフの生成の結果である。

10

【0067】

このようなセキュア近傍グラフが生成され、セキュリティコンテキストが既に転送されていると、I A P P移動手順は、新たなアクセスポイントA P n e wがステーションS T Aとの通信セッションを引き継ぐことを今までのアクセスポイントA Pに通知するために、2つのメッセージの交換だけを含むことになる。特定の実施形態では、実際には、セキュリティアソシエーションが今までのアクセスポイントA Pと新たなアクセスポイントA P n e wとの間で既に生成されているので、これらの2つのメッセージは（順番にではなく）同時に交換可能である。すなわち、これは、2つのメッセージの交換はいかなるセキュリティチェックも伴う必要がなく、したがって、I A P P移動手順に含まれている2つのメッセージの交換は実際には同時に送信され、これにより、再認証に関連付けられた遅延をさらに低減するということを意味する。

20

【0068】

I A P P移動手順の後、新たなアクセスポイントA P n e wにおけるステーションS T Aの実際の認証は、図6の左側に示されている図を参照して既に説明したように実行できる。要約すると、図6の右側のメッセージシーケンス図を参照して説明した実施形態の場合、ハンドオーバー遅延の全体は、従来技術に基づくハンドオーバーの手順に比べるとさらに低減することができる。

【0069】

図5および図6を参照して説明した実施形態は、ハンドオーバーがワイヤレスL A Nにおいて実行される実施形態であることに注意すべきである。しかし、原理的に、固定的な有線ネットワークにおいても同じ手順を実行することができる。このような固定的な有線ネットワークにおいてアクセスポイント間に信頼関係があれば、ネットワーク内のアクセスポイント間にセキュリティアソシエーションが既に存在しているので、手順はA PとA Pとの通信に関連付けられた遅延を含まず、その結果、異なるアクセスポイント間で最初にセキュリティアソシエーションを生成する必要はない。それにもかかわらず、このような場合における近傍グラフの生成は、不要なセキュリティコンテキスト情報の配信を回避し、したがって、ネットワークの負荷を不必要に増加させないため有利である。しかし、図6の右側に示されているような実施形態では、リアソシエーション（I A P P移動手順）中の応答待ち時間は大幅に削減できるため、応答待ち時間は有線ネットワークにおける手順に比べて殆ど無視することができる。

30

40

【0070】

本発明のさらなる実施形態について次に説明する。近傍グラフを生成する本実施形態によれば、2つのタイプのセキュリティアソシエーションが生成される。最初に、起点となるアクセスポイントと、この起点となるアクセスポイントの近傍における、おそらくハンドオーバー手順のターゲットである候補エレメントとの間でセキュリティアソシエーションが生成される。これらの候補アクセスポイントに関して、I A P P移動手順中の最初の4つのメッセージを参照することにより図5の右側および図6の左側と関連付けて説明したように、起点となるアクセスポイントとこれら候補エレメントとの間に信頼関係またはセキュリティアソシエーションが生成される。しかし、近傍グラフを完成させるため、さら

50

なるセキュリティアソシエーションまたはセキュリティコンテキストがさらに転送され、この転送されたその他のセキュリティアソシエーションは、モバイルステーション S T A と起点となるアクセスポイント A P との間のセキュリティアソシエーションに関連している。このセキュリティアソシエーションは、例えば、図 5 の右側および図 6 の左側の I A P P 移動手順中の第 5 番目および第 6 番目のメッセージによって転送される。

【0071】

特定の一実施形態によれば、起点となるアクセスポイントとしての役目を果たし、そのための近傍グラフが生成される特定のアクセスポイントは、起点となるアクセスポイントと候補エレメントとの間のセキュリティコンテキスト転送が実行されることに基づいて候補エレメントを決定するだけではなく、どちらのモバイルステーションがこの起点となるアクセスポイントによるサービスを受けているかをさらに決定する。この起点となるアクセスポイントのサービスエリアに位置し、サービスを受けているモバイルステーションに関して、これらモバイルステーションと起点となるアクセスポイントとの間のセキュリティアソシエーションが、上述のような高速ハンドオーバを可能にするために候補エレメントに向けてさらに転送される。本実施形態では、その結果、起点となるアクセスポイントは、起点となるアクセスポイントのサービスエリア内に位置する個々のモバイルステーションに基づいて、セキュリティコンテキストまたはセキュリティアソシエーションを近隣の候補エレメントへと転送する。

10

【0072】

特定の実施形態によれば、新たなモバイルステーションが起点となるアクセスポイントのエリアに入ると、このアクセスポイントは、この新たなモバイルステーションと起点となるアクセスポイントとの間で確立されたセキュリティアソシエーションを、近傍グラフに含まれる他の候補エレメントにも転送することにより近傍グラフを更新し、新たなモバイルステーションが起点となるアクセスポイントのエリアに入った後にこのモバイルステーションの起点となるアクセスポイントから候補エレメントのうちの 1 つへの高速なハンドオーバを可能にする。これは近傍グラフの更新と考えることができる。

20

【0073】

したがって、近傍グラフの更新は、モバイルステーションと起点となるアクセスポイントとの間のセキュリティアソシエーションの転送を含む。近傍グラフの更新は、モバイルステーションがある特定のアクセスポイントのサービスエリアに入ることによって開始でき、この特定のアクセスポイントは、この新たに入ったモバイルステーションの起点となるアクセスポイントとなるため、その近傍グラフを更新しなければならない。

30

【0074】

さらなる実施形態によれば、近傍グラフの更新は、ある特定のアクセスポイントがその特定のアクセスポイントのサービスエリアに位置するモバイルステーションをポーリングすることによりチェックを行うステータスポーリングの結果に依存する。このようなポーリングは、所定の時点または所定の間隔で実行することができる。

【0075】

さらなる実施形態によれば、近傍グラフの更新は、ある特定の起点となるアクセスポイントのサービスエリアから離脱するモバイルステーションにも基づいている。モバイルステーションが起点となるアクセスポイントのサービスエリアを離脱した後、この起点となるアクセスポイントは、その近傍グラフに含まれる候補エレメントに対し、このモバイルステーションが離脱したことと、たった今離脱したこのモバイルステーションに関連付けられたセキュリティアソシエーションをこれら候補エレメントが削除できることを通知することができる。このようにして、実際には、異なるアクセスポイントにおいてもはや使用できないセキュリティアソシエーションのオーバーフローまたは過剰な累積を回避できる。

40

【0076】

しかし、このような場合、近傍グラフは、モバイルステーションが進入したサービスエリアを有するアクセスポイントにおいて再生成または更新されることが好ましいというこ

50

とに注意すべきである。これにより、このモバイルステーションのセキュリティアソシエーションが、このモバイルステーションが新たなサービスエリア内に移動した後であっても実際にハンドオーバーする可能性のあるこのようなアクセスポイントから削除されることを避けることができる。

【0077】

特定の実施形態によれば、ある特定のアクセスポイント（または起点となるアクセスポイント）ごとに生成された近傍グラフは、このアクセスポイントのサービスエリアに位置するモバイルステーションの個々のパラメータまたは特性にも依存する。例えば、このアクセスポイントのサービスエリア内に、マルチホップ近傍グラフを要求する比較的高速で移動できる1台のモバイルステーションが位置している場合、この起点となるアクセスポイントの近傍グラフはマルチホップの候補エレメントを含むことができる。このモバイルステーションがこの起点となるアクセスポイントのサービスエリアを離脱すると、マルチホップ要求のために含まれていた候補エレメントは、この起点となるアクセスポイントの近傍グラフから削除することができる。

10

【0078】

特定の一実施形態によれば、ある特定の起点となるアクセスポイントの近傍グラフに含まれている個々の候補エレメントは、それら候補エレメントが近傍グラフに含まれる根拠となるモバイルステーションを特定できる対応する識別子を有する。上述の実施形態の場合と同様に、例えば、ある候補エレメントは、低速で移動する第1のモバイルステーションに起因し、かつ、高速で移動するモバイルステーションにも起因して近傍グラフに含まれている。この場合、その候補エレメントは、これら2台のモバイルステーションを特定する対応する識別子を2つ有する。高速で移動するモバイルステーションがサービスエリアを離脱しても、この候補エレメントは、別のモバイルステーションにも起因して含まれているために近傍グラフに含まれたままである。しかし、高速で移動するモバイルステーションだけに起因して近傍グラフに含まれる候補エレメント（例えば、起点となるアクセスポイントと直接的には近接していないマルチホップステーション）は、この高速で移動するモバイルステーションが起点となるアクセスポイントのサービスエリアを離脱すると、近傍グラフから削除することができる。

20

【0079】

以上、本発明について典型的な実施形態を用いて説明した。ここで記載した実施形態に基づく方法は、適切にプログラムされたコンピュータまたはコンピュータシステムによって実施できることは当業者には容易に理解されるであろう。

30

【0080】

上述の実施形態は単に例示を目的としており、当業者によって変更可能であることをさらに理解されたい。

【図面の簡単な説明】

【0081】

【図1】従来技術に基づくネットワーク構成を概略的に示す図である。

【図2】本発明の実施形態と併せて使用するネットワーク構成を概略的に示す図である。

【図3】本発明の実施形態を概略的に示すフローチャートである。

40

【図4】本発明のさらなる実施形態を概略的に示すフローチャートである。

【図5】従来技術と対比して本発明の実施形態によるメッセージシーケンスを概略的に示す図である。

【図6】本発明のさらなる実施形態によるメッセージシーケンスを概略的に示す図である。

フロントページの続き

- (56)参考文献 特開2004-222300 (JP, A)
特開2004-214869 (JP, A)
特開2004-166270 (JP, A)
特開2003-333639 (JP, A)

- (58)調査した分野(Int.Cl., DB名)
H04W 84/12
H04W 88/08