

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5166525号
(P5166525)

(45) 発行日 平成25年3月21日 (2013. 3. 21)

(24) 登録日 平成24年12月28日 (2012. 12. 28)

(51) Int. Cl. F I
HO 4 W 12/08 (2009. 01) HO 4 W 12/08
HO 4 W 8/26 (2009. 01) HO 4 W 8/26

請求項の数 18 (全 35 頁)

(21) 出願番号	特願2010-512576 (P2010-512576)	(73) 特許権者	000005821
(86) (22) 出願日	平成20年6月12日 (2008. 6. 12)		パナソニック株式会社
(65) 公表番号	特表2010-530680 (P2010-530680A)		大阪府門真市大字門真1006番地
(43) 公表日	平成22年9月9日 (2010. 9. 9)	(74) 代理人	100093067
(86) 国際出願番号	PCT/EP2008/004731		弁理士 二瓶 正敬
(87) 国際公開番号	W02008/155066	(72) 発明者	バッハマン イェンス
(87) 国際公開日	平成20年12月24日 (2008. 12. 24)		ドイツ連邦共和国 63225 ランゲン
審査請求日	平成23年5月25日 (2011. 5. 25)		モンツァシュトラーク 4c パナソニ
(31) 優先権主張番号	07011972.2		ック アールアンドディー センター ジ
(32) 優先日	平成19年6月19日 (2007. 6. 19)		ャーマニー ゲゼルシャフトミットベシユ
(33) 優先権主張国	欧州特許庁 (EP)		レンクテルハフツング内
(31) 優先権主張番号	08008131.8		
(32) 優先日	平成20年4月28日 (2008. 4. 28)		
(33) 優先権主張国	欧州特許庁 (EP)		

最終頁に続く

(54) 【発明の名称】 モバイルノードのためのアクセスネットワーク-コアネットワーク間信頼関係検出

(57) 【特許請求の範囲】

【請求項 1】

アクセスネットワークに接続するユーザ装置が、ゲートウェイと前記ユーザ装置の packets・データ・ネットワーク・ゲートウェイ (PDN-GW) とを含むコアネットワークと前記アクセスネットワークとの間の信頼関係を判定する方法であって、

前記アクセスネットワークに接続すると同時に、前記アクセスネットワークから前記ユーザ装置に通知された IP アドレス / IP プレフィックスを前記ユーザ装置が受信するステップと、

前記ゲートウェイによって割り当てられたリモート IP アドレスを前記ユーザ装置が受信するステップと、

前記ユーザ装置と前記ゲートウェイとの間で行われるセキュリティトンネル確立手順のメッセージであって、前記ユーザ装置の前記 IP アドレス / IP プレフィックスの情報を含む前記メッセージを交換するステップと、

前記セキュリティトンネル確立手順の後に、前記ユーザ装置において、前記アクセスネットワークが前記コアネットワークにより信頼されるものであるか否かを、前記 packets・データ・ネットワーク・ゲートウェイから前記ユーザ装置に送信されたバインディングアクノレッジ (B ACK) の宛先アドレスに基づいて判定するステップとを、

備える方法。

【請求項 2】

前記バインディングアクノレッジの宛先アドレスが前記 IP アドレス / IP プレフィッ

10

20

クスである場合、前記ユーザ装置は前記アクセスネットワークが前記コアネットワークにより信頼されるものであると判定し、

前記バインディングアクノレッジの宛先アドレスが前記リモート I P アドレスである場合、前記ユーザ装置は前記アクセスネットワークが前記コアネットワークにより信頼されるものでないと判定する請求項 1 に記載の方法。

【請求項 3】

前記ゲートウェイは発展型パケット・データ・ゲートウェイ (e P D G) である請求項 1 に記載の方法。

【請求項 4】

前記 I P アドレス / I P プレフィックスは、前記セキュリティトンネル確立手順の前記メッセージの 1 つで、前記ユーザ装置から前記発展型パケット・データ・ゲートウェイへ伝達される請求項 3 に記載の方法。

【請求項 5】

前記発展型パケット・データ・ゲートウェイから前記パケット・データ・ネットワーク・ゲートウェイへ転送されるモビリティメッセージは、前記 I P アドレス / I P プレフィックスを含み、前記パケット・データ・ネットワーク・ゲートウェイは、前記モビリティメッセージで受信される前記 I P アドレス / I P プレフィックスが既に前記パケット・データ・ネットワーク・ゲートウェイによって前記アクセスネットワークを介して前記ユーザ装置に割り当てられているホーム I P アドレス / I P プレフィックスと同一であるかどうかを判定し、

同一であると判定される場合には、前記バインディングアクノレッジの宛先アドレスに前記 I P アドレス / I P プレフィックスが設定されて送信され、同一でないと判定される場合には、前記バインディングアクノレッジの宛先アドレスに前記リモート I P アドレスが設定されて送信される請求項 4 に記載の方法。

【請求項 6】

アクセスネットワークに接続され、ゲートウェイと前記ユーザ装置のパケット・データ・ネットワーク・ゲートウェイ (P D N - G W) とを含むコアネットワークと前記アクセスネットワークとの間の信頼関係を判定するユーザ装置であって、

前記アクセスネットワークによって前記ユーザ装置に割り当てられた I P アドレス / I P プレフィックスを受信する受信部を備え、

前記ゲートウェイによって割り当てられたリモート I P アドレスを前記ユーザ装置が受信する前記受信部と、

前記ユーザ装置と前記ゲートウェイとの間で行われるセキュリティトンネル確立手順のメッセージであって、前記 I P アドレス / I P プレフィックスの情報を含むメッセージを交換する前記受信部及び送信部と、

前記セキュリティトンネル確立手順の後に、前記アクセスネットワークが前記コアネットワークにより信頼されるものであるか否かを、前記パケット・データ・ネットワーク・ゲートウェイから前記ユーザ装置に送信されたバインディングアクノレッジ (B A C K) の宛先アドレスに基づいて判定するプロセッサとを、

備えるユーザ装置。

【請求項 7】

アクセスネットワークに接続されたユーザ装置が、第 1 のゲートウェイと第 2 のゲートウェイとを含むコアネットワークと前記アクセスネットワークとの間の信頼関係を検出するための方法であって、

前記ユーザ装置が前記第 2 のゲートウェイを介して前記第 1 のゲートウェイへメッセージを送信するステップと、

前記ユーザ装置が信頼できるアクセスネットワークにいるのか、あるいは、信頼できないアクセスネットワークにいるのかを判断するステップと、

前記ユーザ装置が信頼できないアクセスネットワークにいる場合に、前記第 2 のゲートウェイと前記ユーザ装置との間を経由する前記第 1 のゲートウェイと前記ユーザ装置との

10

20

30

40

50

間の第1のトンネルを介して、前記第1のゲートウェイが前記ユーザ装置へ前記ユーザ装置のリモートIPアドレスを宛先アドレスとするメッセージを送信するステップと、

前記ユーザ装置が信頼できるアクセスネットワークにいる場合に、前記第1のゲートウェイと前記ユーザ装置との間の第2のトンネルを介して、前記第1のゲートウェイが前記ユーザ装置へ前記ユーザ装置のローカルIPアドレス／プレフィックスを宛先アドレスとするメッセージを送信するステップとを、

備える方法。

【請求項8】

前記第1のゲートウェイはパケット・データ・ネットワーク・ゲートウェイ(PDN-GW)であり、前記第2のゲートウェイは発展型パケット・データ・ゲートウェイ(ePDG)である請求項7に記載の方法。

10

【請求項9】

前記判断するステップは、前記第1のゲートウェイによって行われる、あるいは、認証、認可、アカウントिंगサーバによって行われる請求項7又は8に記載の方法。

【請求項10】

前記ユーザ装置が前記第1のゲートウェイへ送信するステップにおける前記メッセージはバインディングアップデートであり、前記バインディングアップデートは、トンネリングされる、あるいは、他のメッセージに含まれる請求項7から9のいずれか1つに記載の方法。

20

【請求項11】

前記第1のゲートウェイが前記ユーザ装置へ送信するステップにおける前記メッセージはバインディングアクノレッジ(BACK)である請求項7から10のいずれか1つに記載の方法。

【請求項12】

前記ユーザ装置が前記バインディングアクノレッジを受信するステップと、

前記バインディングアクノレッジの宛先アドレスにローカルIPアドレス／プレフィックスが使用される場合に、前記ユーザ装置が信頼できるネットワークにいると判定するステップと、

前記バインディングアクノレッジの宛先アドレスにリモートIPアドレスが使用される場合に、前記ユーザ装置が信頼できないネットワークにいると判定するステップとを、

30

さらに備える請求項11に記載の方法。

【請求項13】

アクセスネットワークに接続されたユーザ装置のために、コアネットワークと前記アクセスネットワークとの間の信頼関係が検出される、前記コアネットワークにおけるゲートウェイであって、

前記ユーザ装置からメッセージを受信する受信手段と、

前記ユーザ装置が信頼できるアクセスネットワークにいるのか、あるいは、信頼できないアクセスネットワークにいるのかを判断する判断手段と、

前記ユーザ装置が信頼できないアクセスネットワークにいる場合に、他のゲートウェイと前記ユーザ装置との間を経由する前記ゲートウェイと前記ユーザ装置との間の第1のトンネルを介して、前記ユーザ装置へ前記ユーザ装置のリモートIPアドレスを宛先アドレスとするメッセージを送信する送信手段とを備え、

40

前記送信手段は、前記ユーザ装置が信頼できるアクセスネットワークにいる場合に、前記ゲートウェイと前記ユーザ装置との間の第2のトンネルを介して、前記ユーザ装置へ前記ユーザ装置のローカルIPアドレス／プレフィックスを宛先アドレスとするメッセージを送信する

備えるゲートウェイ。

【請求項14】

前記ゲートウェイはパケット・データ・ネットワーク・ゲートウェイ(PDN-GW)である請求項13に記載のゲートウェイ。

50

【請求項 15】

アクセスネットワークに接続され、第1のゲートウェイと第2のゲートウェイを含むコアネットワークと前記アクセスネットワークとの間の信頼関係を検出できるユーザ装置であって、

前記第2のゲートウェイを介して前記コアネットワークへメッセージを送信する送信手段と、

前記ユーザ装置が信頼できないアクセスネットワークにいる場合に、前記第2のゲートウェイと前記ユーザ装置との間を経由する前記第1のゲートウェイと前記ユーザ装置との間の第1のトンネルを介して、前記第1のゲートウェイから前記ユーザ装置のリモートIPアドレスを宛先アドレスとするメッセージを受信する受信手段とを備え、

前記受信手段は、前記ユーザ装置が信頼できるアクセスネットワークにいる場合に、前記第1のゲートウェイと前記ユーザ装置との間の第2のトンネルを介して、前記第1のゲートウェイから前記ユーザ装置のローカルIPアドレス／プレフィックスを宛先アドレスとするメッセージを受信する

備えるユーザ装置。

【請求項 16】

ネットワークのコアネットワークにおけるゲートウェイのプロセッサによって実行されたときに、ユーザ装置のために前記コアネットワークとアクセスネットワークとの間の信頼関係を前記ゲートウェイに検出させる命令を格納するコンピュータ読み取り可能媒体であって、前記命令は、前記ゲートウェイに、

前記ユーザ装置からメッセージを受信させ、

前記ユーザ装置が信頼できるアクセスネットワークにいるのか、あるいは、信頼できないアクセスネットワークにいるのかを判断させ、

前記ユーザ装置が信頼できないアクセスネットワークにいる場合に、他のゲートウェイと前記ユーザ装置との間を経由する前記ゲートウェイと前記ユーザ装置との間の第1のトンネルを介して、前記ユーザ装置へ前記ユーザ装置のリモートIPアドレスを宛先アドレスとするメッセージを送信させ、

前記ユーザ装置が信頼できるアクセスネットワークにいる場合に、前記ゲートウェイと前記ユーザ装置との間の第2のトンネルを介して、前記ユーザ装置へ前記ユーザ装置のローカルIPアドレス／プレフィックスを宛先アドレスとするメッセージを送信させることによって、前記信頼関係を検出させるコンピュータ読み取り可能媒体。

【請求項 17】

ネットワークのアクセスネットワークに接続されたユーザ装置のプロセッサによって実行されたときに、前記アクセスネットワークと第1及び第2のゲートウェイを含むコアネットワークとの間の信頼関係を前記ユーザ装置に検出させる命令を格納するコンピュータ読み取り可能媒体であって、前記命令は、前記ユーザ装置に、

前記第2のゲートウェイを介して前記コアネットワークへメッセージを送信させ、

前記ユーザ装置が信頼できないアクセスネットワークにいる場合に、前記ユーザ装置と前記第2のゲートウェイとの間を経由する前記第1のゲートウェイへの第1のトンネルを介して、前記第1のゲートウェイから前記ユーザ装置のリモートIPアドレスを宛先アドレスとするメッセージを受信させ、

前記ユーザ装置が信頼できるアクセスネットワークにいる場合に、前記第1のゲートウェイへの第2のトンネルを介して、前記第1のゲートウェイから前記ユーザ装置のローカルIPアドレス／プレフィックスを宛先アドレスとするメッセージを受信させることによって、前記信頼関係を検出させるコンピュータ読み取り可能媒体。

【請求項 18】

請求項17に記載のコンピュータ読み取り可能媒体であって、ネットワークのアクセスネットワークにおけるユーザ装置のプロセッサによって実行されたときに、請求項10から12に記載の方法のステップを前記ユーザ装置に実行させることによって、前記アクセスネットワークと第1及び第2のゲートウェイを含むコアネットワークとの間の信頼関係

10

20

30

40

50

を検出させる命令を格納するコンピュータ読み取り可能媒体。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、概して移動体通信に関し、特に、非3GPPアクセスネットワークへのハンドオーバー後又は初期接続後のモビリティシグナリングに関する。

【0002】

本発明は、モバイルネットワークにおけるコアネットワークと非3GPPアクセスネットワークとの間の信頼関係検出の方法に関する。

【背景技術】

10

【0003】

3GPPでは、システムアーキテクチャの発展が標準規格に規定されている(3GPP TS 23.401及び3GPP TS 23.402)。発展の1つの側面としては、3GPP(3rd Generation Partnership Project)アクセス(例えば、GERAN(GSM/Edge Radio Access Network)、UTRAN(UMTS Terrestrial Radio Access Network)、E-UTRAN(Evolved-UTRAN))と、非3GPPアクセス(例えば、WLAN(Wireless Local Area Network)、WiMAX(Worldwide Interoperability for Microwave Access)、3GPP2(3rd Generation Partnership Project 2)等)と、さらにそれらの間のモビリティとをサポートすることが挙げられる。3GPPアクセスと非3GPPアクセスとの間のモビリティアンカーは、3GPPコアネットワークのゲートウェイである。このゲートウェイは、外部のパケット・データ・ネットワーク(PDN)とのインターフェースも提供し、PDN-GWと呼ばれる。3GPPアクセスと非3GPPアクセスとの間のモビリティは、モバイルIPに基づいており、それにより、そのプロトコルとして、クライアントモバイルIP(D. Johnson, C. Perkins, J. Arkko, “Mobility Support in IPv6” RFC 3775, 2004年6月; H. Soliman, “Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)” draft-ietf-mip6-nemo-v4traversal-04.txt, 2007年3月)及びプロキシモバイルIP(S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, “Proxy Mobile IPv6” draft-ietf-netlmm-proxymip6-00.txt, 2007年4月)のいずれを使用してもよい。非3GPPアクセスは、信頼できるアクセスと信頼できないアクセスとに分けられる。信頼できないアクセスは、信頼できないアクセスにいるユーザ装置(UE)は、オペレータのサービスにアクセスできるようになる前に、発展型(evolved)パケット・データ・ゲートウェイ(ePDG)への(IPsec(インターネット・プロトコル・セキュリティ)に基づいた)安全なトンネルをまず必要とすることを、前提とする。ePDGは、インターワーキングWLANに使用されるPDGと類似のものである(TS 23.234に記載されている)。一方、信頼できるアクセスからは、この安全なトンネルは必要ない。非3GPPアクセスが信頼できるものであるか否かは、オペレータの判断であり、オペレータによって異なる場合がある。

20

30

40

【0004】

同一の非3GPPアクセス内又は異なる非3GPPアクセス間のモビリティに対して、3GPPアクセスと非3GPPアクセスとの間のモビリティに対して使用されるものと類似のメカニズム、すなわち、クライアント又はプロキシモバイルIP(インターネットプロトコル)が使用することができる。

【0005】

50

上記したように、2種類の非3GPPアクセス、すなわち、信頼できない非3GPPアクセスと信頼できる非3GPPアクセスが定義されており、非3GPPアクセスが信頼できるものであるか否かは、3GPPオペレータに委ねられている。また、1つの非3GPPアクセスが、オペレータAの、あるUEにとっては信頼できるアクセスであり、オペレータAの別のUEにとっては信頼できないアクセスである、という場合もある。

【0006】

UEが信頼できない非3GPPアクセスへ移動又は初期接続する場合(図1)、UEは、まず、ePDGを発見して、ePDGとの間にIPsec鍵交換IKEv2/IPsecトンネルを確立しなければならない。そして、UEは、ePDG/IPsecトンネルを介して、発展型パケットコアEPC(PDN-GW)に接続することができる。一方、UEは、信頼できる非3GPPアクセスへ移動又は初期接続する場合(図2)には、EPC(PDN-GW)に直接接続することができる。

10

【0007】

問題は、UEが、非3GPPアクセスへの初期接続の間又はハンドオーバーの後(図3)、そのアクセスが信頼できるものなのかあるいは信頼できないものなのかを把握しておらず、また、

— ePDGへのトンネルを確立して初めて、BUメッセージをPDN-GWへ送信できるのか、あるいは、

— BUメッセージをPDN-GWへ直接送信できるのか
を把握していないことである。

20

【0008】

上記のように、(ハンドオーバー後又は初期接続において)非3GPPアクセスネットワークとの接続確立を開始するUEは、その非3GPPアクセスネットワークが信頼できるものなのかあるいは信頼できないものなのかを把握していない場合がある。

【0009】

UEが非3GPPアクセスネットワークの信頼関係を検出できる方法に関しては、いくつかの解決策が考えられる。以下に、その解決策のうちのいくつかを説明し、それらの解決策において起こりうる問題に着目する。

1. いくつかの無線アクセス技術(Radio Access Technologies(RATs))をデフォルトで信頼できるもの(WiMAX)とし、その他をデフォルトで信頼できないもの(WLAN 802.11)とする。この解決策の問題は、無線アクセス技術が信頼できるものであるか否かはオペレータの判断になる可能性があるので、正しくないこともあり得る、ということである。また、非3GPPアクセスがUEにとって信頼できるものであるか否かは、このUEの機能に依存する場合がある。例えば、UEが特定のセキュリティ手段をサポートしている場合には、信頼できるものとなる。

30

2. 信頼できる非3GPPアクセスからのネットワークプレフィックスのリストを用いて、UEを事前に設定する。ここでの問題は、例えば、オペレータが多数の小規模な非3GPPアクセス・ホットスポット・オペレータとの間に信頼関係を持っている場合には、このリストが極めて大きくなる可能性があることである。また、新しい非3GPPアクセスネットワークが絶えず加わり得るので、リストを最新の状態に保たなければならない。これは、更新されなければならないUEが多数ある場合には、困難又はかなり非効率となる。

40

3. AAA(Authentication(認証)、Authorization(認可)、Accounting(アカウントिंग))手順の間に、例えば、EAP(拡張認証プロトコル)拡張機能によって、UEに通知してもよい。この解決策は、ローカルの非3GPPアクセスAAAプロトコル及びインフラストラクチャからのサポートを必要とするが、これが常にサポートされていることを前提とすることはできない。

4. 下位層の(例えば、L2の)情報によって、UEに通知する。ここでも、問題は、非3GPPアクセスネットワーク、すなわち、下位層からの(例えば、IEEE 802.11u又はIEEE 802.21によって何らかの手段で提供される)サポートを必要

50

とすることである。

5. UEがPDN-GWへの接続の確立を試行する、すなわち、バインディングアップデート (Binding Update) をPDN-GWのアドレスへ (又はPDN-GW及びePDGへ並行して) 直接送信する。PDN-GWへのその確立が失敗した (PDN-GWが信頼できない非3GPPアクセスから到達可能でないため) 場合には、UEは、信頼できない非3GPPアクセスにいて、ePDGを使用しなければならない、ということ把握する。問題は、UEが、PDN-GWへの到達を何度か試行しなければ、PDN-GWが到達可能ではないと確実に結論付けることができないので、その手順が非常に遅いことである。

6. UEが必ず、最初にePDGを使用する、すなわち、ePDGへのトンネルを確立する。そして、非3GPPアクセスが信頼できるものである場合には、UEは、PDN-GWへ直接接続するよう通知される。この解決策の問題は、最初に多くのリソースを消費することである。全てのパケットが2重にトンネリングされて (IPsec+MIPトンネル) ePDGを介してルーティングされるからである。したがって、あまり効率的ではない。

7. 信頼できる非3GPPアクセスにいるのかあるいは信頼できない非3GPPアクセスにいるのか、UEがDHCPサーバに問い合わせをしてもよい (R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)" RFC 3315, 2003年7月)。ここで、UEは、最初は非3GPPアクセスに接続し、L2アクセスが確立される。その後、UEは、DHCPサーバに信頼関係 (例えばNAIの形式のUEのID、及び/又は、ユーザのホームオペレータ識別子を含む) について要求する。非3GPPアクセスがユーザのホームオペレータとユーザにとって信頼できるものである場合には、DHCPサーバは、信頼関係についてユーザに通知する。DHCPサーバは、さらに、PDN-GWのIPアドレスを返してもよい。非3GPPアクセスがユーザのホームオペレータとユーザにとって信頼できないものである場合には、DHCPサーバは、信頼関係についてユーザに通知する。DHCPサーバは、さらに、ePDGのIPアドレスを返してもよい。ここでの問題は、この解決策が、ローカルDHCPサーバへの事前設定入力又はAAAインフラストラクチャによるサポートを必要とするので、DHCPサーバは、UEのアクセス認証の際、UEのための情報で更新される。しかしながら、これが利用可能でない場合には、DHCPは有効なIPアドレスを返すことができない。この場合、UEは、デフォルトでePDGを使用してもよい。しかしながら、このプロセスは遅い可能性がある。

8. 信頼できる非3GPPアクセスにいるのかあるいは信頼できない非3GPPアクセスにいるのか、UEがDNSサーバに問い合わせをしてもよい。ここで、UEは、最初は非3GPPアクセスに接続し、L2及びL3アクセスを確立する。その後、UEは、例えばサービス又はPDN用に、UE又はオペレータ固有のFQDN (Fully Qualified Domain Name; フルドメイン名) を、例えば次のように構成してもよい。

FQDN=<pdn>.<non-3gpp>.<hplmn>.3gppnetwork.org

FQDN= <pdn>.<user id>.<non-3gpp>.<hplmn>.3gppnetwork.org

【0010】

ここで、hplmn部は、ユーザのホームオペレータの識別子、例えば、MNCコード (Mobile Network Code) 及びMCC (Mobile Country Code) コードである。non-3GPP部は、非3GPPネットワークについてのある情報、例えば、広告されたネットワークアクセス識別子又は広告されたIPプレフィックスである。user id部は、ユーザの識別子、例えば、NAI (Network Access Identifier) である。UEは、この固有のFQDNについてDNS (Domain Name Server) に問合せをする。DNS要求は、再

10

20

30

40

50

帰的に解決される。前のDNSサーバによって解決できない場合には、最終的にはUEのホームオペレータのDNSサーバによって解決される。非3GPPアクセスが信頼できないものである場合には、DNSサーバは、IPアドレスと共にePDGを提供する。そして、UEはePDGへのトンネルを確立して、そのトンネルを介してBUをPDN-GWへ送信しなければならない。非3GPPアクセスが信頼できるものである場合には、DNSサーバは、IPアドレスと共にPDN-GWを提供する。そして、UEは、BUをPDN-GWへ直接送信しなければならない。ここで考えられる問題は、この解決方法が非常に遅いことである。

【発明の概要】

【0011】

本発明は、上記の状況を考慮してなされたものであり、非3GPPアクセスネットワークへのハンドオーバー後又は初期接続後のモビリティシグナリングをより効率的にすることを目的とする。本発明のより詳細な目的は、UEが接続したアクセスネットワークが信頼できるものであるか否かを容易に判定するための方法を提供することである。

【0012】

その目的は、独立クレームの主題によって解決される。本発明の有利な実施の形態は、従属クレームの主題である。

【0013】

本発明の種々の実施の形態によれば、ネットワークベースのモビリティ方式がユーザ装置(UE)によって使用され、信頼できないアクセスネットワークはUEによって使用されるネットワークベースのモビリティ方式をサポートしていないことを前提としている。したがって、UEは、ローカル・モビリティ・アンカー(UEに対応するコアネットワークにおけるパケット・データ・ネットワーク・ゲートウェイ(PDN-GW))との間で、発展型パケット・データ・ゲートウェイ(ePDG)(信頼できないアクセスネットワークへの接続性を提供する)を介して、そのネットワークベースのモビリティ方式を実現しなければならない。その際、UEはePDGとの間でセキュリティトンネルを確立しなければならない。ユーザデータは、その後、そのトンネルを介してUEとPDN-GWとの間で交換される。これが機能するためには、UEは、PDN-GWにおいて割り当てられたホームIPアドレスを通信に使用しなければならない。上記の場合にのみ、他のエンティティとのセッション通信に上記のホームIPアドレスを使用すると、ユーザデータは、実際にPDN-GWによって受信されてePDGに転送され、そこからさらにセキュリティトンネルを介してUEへ転送される。したがって、UEが別のアクセスへ移動しても、ネットワークベースのモビリティも正しく機能し、セッションは中断されない。PDN-GWにおいて割り当てられたホームIPアドレスを新しいアクセスネットワークにおいても使用することができるからである。

【0014】

一般に、ユーザ装置は、新しいアクセスネットワークに接続するとき、始めに、そのアクセスネットワークからIPアドレス/プレフィックスを入手する。アクセスネットワークは、信頼できるネットワークである場合には、UEのネットワークベースのモビリティ方式をサポートしており、アクセスネットワークのアクセスポイントは、UEのモビリティに対応するローカル・モビリティ・アンカー(PDN-GW)に対するプロキシ・モビリティ・エージェントとして機能する。アクセスポイントは、UEのローカル・モビリティ・アンカーとコンタクトを取って、ローカル・モビリティ・アンカーからUEのホームIPアドレス/プレフィックスを受信することができ、その後、ユーザのホームIPアドレス/プレフィックスをUEへ伝送する。ホームIPプレフィックスを受信すると、UEは、そのホームIPプレフィックスを使用してホームIPアドレスを生成するものとする。UEは、そのホームIPアドレスを他のエンティティとのセッション通信に使用することができる。

【0015】

アクセスネットワークが信頼できないネットワークである場合には、UEのネットワー

10

20

30

40

50

クベースのモビリティ方式をサポートしていない。したがって、アクセスネットワークのアクセスポイントがローカル・モビリティ・アンカー（PDN-GW）に到達することはできない。その結果、アクセスネットワークにおいてローカルに割り当てられるIPアドレス／プレフィックスが、アクセスポイントによって生成されてUEに送信される。この場合、UEがローカル・モビリティ・アンカー（PDN-GW）とコンタクトを取るためのプロキシ・モビリティ・エージェントとしてePDGを使用し、それによってネットワークベースのモビリティを信頼できないアクセスネットワークにおいて実現することが必要になるであろう。この場合、UEは、PDN-GWにおいて割り当てられたUEのホームIPアドレス／プレフィックスを受信するために、ePDGへのセキュリティトンネルを確立し、ePDGがPDN-GWとコンタクトを取らなければならない。ePDGは、受信したホームIPアドレス／プレフィックスをUEへ転送する。IPプレフィックスの場合は、UEは、そのホームIPプレフィックスを使用して、他のエンティティとのセッション通信用のIPアドレスを生成する。したがって、この場合も、UEは、アクセスを変更するときに、セッションの連続性を維持することができる。逆に、UEがローカルに割り当てられたIPアドレス／プレフィックスをセッションに使用した場合（例えば、UEが信頼できないアクセスネットワークを信頼できるものと誤って想定し、IPアドレス／プレフィックスがUEのローカル・モビリティ・アンカーにおいて割り当てられたとき）には、UEがそのアクセスネットワークを離れるとすぐに、セッションは中断されてしまうであろう。

10

【0016】

20

UEから見て、上記の差異はトランスペアレントである。すなわち、UEは、受信したIPアドレス／プレフィックスが、PDN-GWにおいて割り当てられたもの（UEのホームIPアドレス／プレフィックス）なのか、あるいは、アクセスネットワークにおいてローカルに割り当てられたものなのかを把握していない。

【0017】

したがって、UEは、アクセスネットワークが信頼できるものなのか、つまり、受信したIPアドレス／プレフィックスをセッションの確立に使用することができるのか、あるいは、信頼できないものなのか、つまり、受信したIPアドレス／プレフィックスをセッションの確立に使用できず、その代わりにePDGを介してPDN-GWとの間でネットワークベースのモビリティを実現しなければならないのか、を判定しなければならない。

30

【0018】

しかしながら、ネットワークベースのモビリティ方式を使用するときのハンドオーバーの場合には、アクセスが信頼できるものであるか否かの検出は、前のアクセスネットワークにおいて受信したIPアドレス／プレフィックスを新しいアクセスネットワークにおいて受信したIPプレフィックスと比較することによって達成できる。より詳細には、UEが前のアクセスネットワークから新しいアクセスネットワークへハンドオーバーを行う場合、UEは、前のアクセスネットワークにおいては、UEのホームIPアドレスでありPDN-GW（UEのローカル・モビリティ・アンカー）において割り当てられたホームIPプレフィックスに基づくIPアドレスをセッション通信に使用していた。UEは、新しいアクセスネットワークへ移動すると、新しいアクセスネットワークからIPアドレス／プレフィックスを受信する。そのIPアドレス／プレフィックスは、PDN-GWにおいて割り当てられたホームIPアドレス／プレフィックス、及び、新しいアクセスネットワークにおいてローカルに割り当てられたIPアドレス／プレフィックスのどちらでもよい。前のアクセスネットワークで使用していた前のIPアドレス／プレフィックスを、新しいアクセスネットワークから受信した新しいIPアドレス／プレフィックスと比較することによって、UEは、受信した新しいIPアドレス／プレフィックスがUEのローカル・モビリティ・アンカーにおいて割り当てられたものであるか否かを推測することができ、それにより、アクセスネットワークが信頼できるものであるか否かを判定することができる。

40

【0019】

50

新しいアクセスネットワークとコアネットワークとの間の信頼関係を判定する上記の簡単な方法は、UEが新しいアクセスネットワークに初期接続することを前提とするときにはそれほど簡単ではない。この場合、前のIPアドレス／プレフィックスについての情報は何も得られない。UEによってそれ以前に確立されたセッションがないからである。したがって、UEは、受信したIPアドレス／プレフィックスがPDN-GWにおいて割り当てられたホームIPアドレス／プレフィックスなのか、あるいは、アクセスネットワークにおいてローカルに割り当てられたものなのかを把握することができない。

【0020】

本発明は、アクセスネットワークが信頼できるネットワークであるか否かを、この場合及び他の場合にUEが判定する簡単で効率的な方法を提供する。

10

【0021】

上記で使用した「IPアドレス／プレフィックス」という用語は、IPアドレス及びIPプレフィックスのいずれも使用できることを意味している。UEは、IPプレフィックスを入手すると、IPプレフィックスからIPアドレスを生成する。さらに、このIPアドレスは、その後、通信セッションに適用することができる。しかしながら、UEが、IPプレフィックスではなくIPアドレスを直接入手することも可能である。この場合、UEは、信頼できないアクセスネットワークに接続すると同時にローカルに割り当てられたIPアドレスを受信するか、あるいは、信頼できるアクセスネットワークから、PDN-GWにおいて割り当てられたホームIPアドレスを入手する。UEがIPプレフィックスからIPアドレスを生成する必要があるのか、あるいは、UEがIPアドレスを直接入手するのかは、発明が機能するためにはそれほど重要なことではない。当業者には、その違いと、後で説明する発明の種々の実施の形態の含意とが分かる。以下において、「IPアドレス」という用語又は「IPプレフィックス」という用語が使用されるときは、それぞれ、その代わりに「IPプレフィックス」又は「IPアドレス」をやはり使用することができる。このことは、当業者には明らかである。

20

【0022】

また、記載されている実施の形態の大半は、ネットワークベースのモビリティを前提としているが、本発明は、ネットワークベースのモビリティ方式に限定されず、クライアントベースのモビリティ方式に適用してもよい。

【0023】

30

例えば、クライアントベースのモビリティを使用するときは、UEは、新しいアクセスネットワークに接続するときに、前のアクセスネットワークからのハンドオーバー後の、あるいは、初期接続後のIPアドレスも入手する。このIPアドレスは、新しいアクセスネットワークにおいてローカルに割り当てられるものである。クライアントベースのモビリティを実現するために、UEは、その新しいIPアドレス（MIPを使用しているときは、気付アドレス）をコアネットワークのホームエージェントに登録しなければならない。これにより、ホームエージェントは、新しいアクセスネットワークにおけるUEとデータを交換することができる。

【0024】

しかしながら、アクセスネットワークがコアネットワークにより信頼されないものである場合には、ホームエージェントは、UEによる登録の試行を受け付けまいであろう。この場合、UEは、割り当てられたIPアドレスを使用してePDGとコンタクトを取って、新しいIPアドレスをePDGに要求しなければならない。その後、ePDGにおいて割り当てられた、新しく割り当てられたIPアドレスは、コアネットワークにおけるUEのホームエージェントにおいて正常に登録することができる。この新しいIPアドレスは、ePDGにおいて割り当てられるものであり、ePDGは、コアネットワークの一部なので、UEのホームエージェントにより信頼されるものだからである。UEは、ePDGへのセキュリティトンネルの確立も行わなければならないであろう。その結果、UEのホームエージェントを介して、また、信頼できないアクセスネットワークに接続しているUEへePDGを介して、データが交換される。

40

50

【0025】

アクセスネットワークがコアネットワークにより信頼されるものである場合には、UEのホームエージェントによる登録の試行は成功し、UEは、最初に受信したIPアドレスを使用して、通常、クライアントベースのモビリティの場合に行うのと同じように、通信セッションを開始することができる。

【0026】

今述べたように、UEは、最初に受信したIPアドレスを通信に使用できるか否かを把握するために、接続したアクセスネットワークがコアネットワークにより信頼されるものであるか否かを把握しなければならない。

【0027】

発明の種々の実施の形態のベースとなる発明の趣旨は、アクセスネットワークが信頼できるものなのか、あるいは、信頼できないものなのかを判定するのに必要な情報を、コアネットワークの一部又はユーザ装置自身である1つの特定のエンティティに与えるために、セキュリティトンネル確立の手順を使用することである。

【0028】

セキュリティトンネル確立手順のメッセージを用いて、上記の判定を行うエンティティに必要な情報を与える。必要な情報は、アクセスネットワークに接続すると同時にそのアクセスネットワークによってユーザ装置に最初に割り当てられた第1のIPアドレス/プレフィックスを含んでもよい。必要な情報は、コアネットワークにおけるユーザ装置のホームエージェントにおいて割り当てられるIPアドレス/プレフィックスであるそのユーザ装置のホームIPアドレス/プレフィックスをさらに含んでもよい。

【0029】

アクセスネットワークの信頼関係を判定するエンティティによっては、必要な情報の一部、すなわち、第1のIPアドレス/プレフィックス又はホームIPアドレス/プレフィックスを既に把握している場合がある。したがって、そのエンティティは、足りない情報を保持している他のエンティティから残りの必要な情報を得なければならない。

【0030】

つまり、アクセスネットワークの信頼関係を判定するエンティティによっては、セキュリティトンネル確立手順のメッセージで、第1のIPアドレス/プレフィックス、又は、ホームIPアドレス/プレフィックス、又は、第1のIPアドレス/プレフィックス及びホームIPアドレス/プレフィックスを送信しなければならない場合がある。例えば、UEがアクセスネットワークの信頼関係を判定するエンティティである場合には、第1のIPアドレス/プレフィックスは、セキュリティトンネル確立手順のメッセージで伝達されない。UEは既に第1のIPアドレス/プレフィックスを把握しているからである。しかしながら、この場合、セキュリティトンネル確立手順のメッセージを使用して、ホームIPアドレス/プレフィックスをUEへ伝達しなければならない。

【0031】

したがって、ローカル・モビリティ・アンカー、つまり、PDN-GWがアクセスネットワークの信頼関係を判定するエンティティである場合には、セキュリティトンネル確立手順の際に、ホームIPアドレス/プレフィックスを交換する必要はない。ホームIPアドレス/プレフィックスは、概して、PDN-GWにとって既知だからである。しかしながら、第1のIPアドレス/プレフィックスをPDN-GWへ伝達しなければならない。これは、セキュリティトンネル確立手順のメッセージの1つを使用して行うことができる。

【0032】

ePDGがアクセスネットワークの信頼関係を判定する場合には、第1のIPアドレス/プレフィックス及びホームIPアドレス/プレフィックスをePDGに与えるべきである。ePDGは、第1のIPアドレス/プレフィックス及びホームIPアドレス/プレフィックスのいずれも把握していないからである。第1のIPアドレス/プレフィックス及びホームIPアドレス/プレフィックスは、セキュリティトンネル確立手順のメッセージ

10

20

30

40

50

を使用して、また、実際にはセキュリティトンネル確立手順の一部ではないが、セキュリティトンネル確立手順によってトリガされるメッセージも使用して、ePDGに与えることができる。

【0033】

この情報に基づいて、エンティティは、アクセスネットワークがコアネットワークにより信頼されるものであるか否かを判定してもよい。これは、第1のIPアドレス／プレフィックスをホームIPアドレス／プレフィックスと比較することによって行ってもよく、それらが一致する場合には、アクセスネットワークが信頼できるものであると推測することができる。この場合、アクセスネットワークはその信頼できるエンティティからIPアドレス／プレフィックスを取得して、その後、UEがアクセスネットワークに接続すると同時に、取得したこのIPアドレス／IPプレフィックスを第1のIPアドレス／プレフィックスとしてUEに与えている。

10

【0034】

逆に、対応するエンティティが、第1のIPアドレスとホームIPアドレスが一致しないと判定する場合には、UEがアクセスネットワークから受信したIPプレフィックスはローカルに割り当てられているので、UEは、このIPプレフィックスを通信セッション開始のために使用しないものとする。つまり、そのアクセスネットワークはコアネットワークにより信頼されないものである。したがって、信頼できないアクセスネットワークからコアネットワークへ橋渡しをするePDGを介して、コアネットワーク、すなわち、モバイルノードのローカル・モビリティ・アンカー（PDN-GW）と通信しなければならない。

20

【0035】

本発明の有利な実施の形態によれば、セキュリティトンネル確立手順が、ユーザ装置と、第1のゲートウェイと、コアネットワークの認証サーバとの間で行われる認証手順を備える。この場合、第1ゲートウェイは、ホームIPアドレス／IPプレフィックスを認証サーバからその認証手順のメッセージで受信する。これにより、判定全体を迅速化することができる。認証手順は、通常、始めに行われるので、第1のゲートウェイがホームIPアドレス／プレフィックスの情報をかなり早い時点で受信することになるからである。そして、第1のゲートウェイは、アクセスネットワークが信頼できるものであるか否かを判定することができる。あるいは、判定に対応するエンティティに、ホームIPアドレス／プレフィックスの情報を与えることができる。

30

【0036】

本発明の別の実施の形態においては、アクセスネットワークがコアネットワークにより信頼されるものであるか否かを第1のゲートウェイが判定する場合には、その判定の結果は、セキュリティトンネル確立手順のメッセージでユーザ装置へ伝達される。

【0037】

本発明の別の有利な実施の形態を次に参照すると、第1のゲートウェイは発展型パケット・データ・ゲートウェイであり、信頼できるエンティティはユーザ装置に対応するパケット・データ・ネットワーク・ゲートウェイである。ホームIPアドレス／プレフィックスは、パケット・データ・ネットワーク・ゲートウェイから、セキュリティトンネル確立手順のメッセージの1つを使用してユーザ装置へ、及び／又は、セキュリティトンネル確立手順によってトリガされる他のメッセージで発展型パケット・データ・ゲートウェイへ、伝達される。

40

【0038】

本発明の別の有利な実施の形態によれば、第1のIPアドレス／プレフィックスは、セキュリティトンネル確立手順のメッセージの1つでユーザ装置から発展型パケット・データ・ゲートウェイへ伝達される。これは、アクセスネットワークの、コアネットワークとの信頼関係をユーザ装置が判定しない場合に行われる。

【0039】

本発明の別の実施の形態においては、セキュリティトンネル確立手順は、発展型パケッ

50

ト・データ・ゲートウェイからパケット・データ・ネットワーク・ゲートウェイへのモビリティメッセージの送信をトリガし、モビリティメッセージはパケット・データ・ネットワーク・ゲートウェイをトリガしてホームIPアドレス／プレフィックスを発展型パケット・データ・ゲートウェイへ返すようにさせる。

【0040】

本発明の別の実施の形態を参照すると、パケット・データ・ネットワーク・ゲートウェイへ転送されるモビリティメッセージは、IPアドレス／プレフィックスを含み、パケット・データ・ネットワーク・ゲートウェイは、モビリティメッセージで受信されるそのIPアドレス／プレフィックスが既にパケット・データ・ネットワーク・ゲートウェイによってユーザ装置に割り当てられているかどうかを判定する。モビリティメッセージで受信されるそのIPアドレス／プレフィックスが、ユーザ装置がアクセスネットワークに接続すると同時にそのユーザ装置に割り当てられるIPアドレス／プレフィックスと同一であると判定される場合には、パケット・データ・ネットワーク・ゲートウェイは、その判定の結果の情報を発展型パケット・データ・ゲートウェイへ返す。ユーザ装置がアクセスネットワークに接続すると同時に、パケット・データ・ネットワーク・ゲートウェイによって、モビリティメッセージで受信されるそのIPアドレス／プレフィックスがユーザ装置に割り当てられなかったと判定される場合には、ホームIPアドレス／プレフィックスはパケット・データ・ネットワーク・ゲートウェイによって生成され、発展型パケット・データ・ゲートウェイへ送信される。

【0041】

本発明の別の有利な実施の形態によれば、第1のゲートウェイ及び信頼できるエンティティは、ユーザ装置に対応するパケット・データ・ネットワーク・ゲートウェイである。そして、ホームIPアドレス／プレフィックスは、セキュリティトンネル確立手順のメッセージの1つでパケット・データ・ネットワーク・ゲートウェイからユーザ装置へ伝達される。あるいは、第1のIPアドレス／プレフィックスは、セキュリティトンネル確立手順のメッセージの1つでユーザ装置からパケット・データ・ネットワーク・ゲートウェイへ伝達される。これは、どのエンティティが実際に信頼関係の判定を行うかによる。

【0042】

本発明の別の実施の形態は、アクセスネットワークに接続されたユーザ装置のために、コアネットワークとそのアクセスネットワークとの間の信頼関係を判定する方法を提供する。そのコアネットワークは、パケット・データ・ネットワーク・ゲートウェイを含む。開始メッセージは、ユーザ装置からパケット・データ・ネットワーク・ゲートウェイへ送信される。開始メッセージに応じて、パケット・データ・ネットワーク・ゲートウェイから応答を受信しない場合には、ユーザ装置は、アクセスネットワークがコアネットワークにより信頼されないものであると判定する。

【0043】

本発明の上記別の実施の形態によれば、その開始メッセージで、ユーザ装置とパケット・データ・ネットワーク・ゲートウェイとの間でセキュリティトンネル確立手順を開始する。

【0044】

また、本発明は、アクセスネットワークに接続され、第1のゲートウェイを含むコアネットワークとそのアクセスネットワークとの間の信頼関係が判定されるユーザ装置を提供する。ユーザ装置の受信部は、アクセスネットワークによってユーザ装置に割り当てられた第1のIPアドレス／プレフィックスを受信する。ユーザ装置の受信部と送信部とは、ユーザ装置と第1のゲートウェイとの間で行われるセキュリティトンネル確立手順のメッセージを交換する。そのメッセージは、第1のIPアドレス／プレフィックス及び／又はユーザ装置のホームIPアドレス／プレフィックスの情報を含む。ユーザ装置内のプロセッサは、アクセスネットワークがコアネットワークにより信頼されるものであるか否かを、その第1のIPアドレス／プレフィックスとホームIPアドレス／プレフィックスとに基づいて判定する。

【0045】

前記ユーザ装置が、本発明のこれまでに説明した実施の形態のステップを行う及び／又はそれらに關与する手段をさらに備えることは、当業者には明らかなはずである。

【0046】

さらに、本発明は、アクセスネットワークに接続されたユーザ装置のために、コアネットワークとそのアクセスネットワークとの間の信頼関係が判定される、そのコアネットワークにおけるゲートウェイを提供する。ゲートウェイの受信部と送信部とは、ユーザ装置とゲートウェイとの間で行われるセキュリティトンネル確立手順のメッセージを交換する。そのメッセージは、アクセスネットワークに接続すると同時にユーザ装置によって受信され、かつアクセスネットワークによってユーザ装置に割り当てられた第1のIPアドレス／プレフィックスの情報を含む。そのメッセージは、さらに、ユーザ装置のホームIPアドレス／プレフィックスの情報を含む。ゲートウェイ内のプロセッサは、アクセスネットワークがコアネットワークにより信頼されるものであるか否かを、その第1のIPアドレス／プレフィックスとホームIPアドレス／プレフィックスとに基づいて判定する。

10

【0047】

前記ゲートウェイが、本発明のこれまでに説明した実施の形態のステップを行う及び／又はそれらに關与する手段をさらに備えることは、当業者には明らかなはずである。

【0048】

第1の態様によれば、アクセスネットワークに接続されたユーザ装置のための、第1のゲートウェイと第2のゲートウェイとを含むコアネットワークとそのアクセスネットワークとの間の信頼関係検出のための方法と、ゲートウェイと、ユーザ装置と、ネットワークと、コンピュータ読み取り可能媒体とが提供される。その方法は、ユーザ装置が第2のゲートウェイを介してコアネットワークへメッセージを送信するステップを備える。その後、ユーザ装置が信頼できるアクセスネットワークにいるのか、あるいは、信頼できないアクセスネットワークにいるのかが判断される。第1のゲートウェイは、ユーザ装置が信頼できないアクセスネットワークにいる場合に、第2のゲートウェイとユーザ装置との間を経由する第1のゲートウェイとユーザ装置との間のトンネルを介して、ユーザ装置へメッセージを送信する。また、第1のゲートウェイは、ユーザ装置が信頼できるアクセスネットワークにいる場合に、第1のゲートウェイとユーザ装置との間のトンネルを介して、ユーザ装置へメッセージを送信する。

20

30

【0049】

第1の態様をさらに詳細に参照すると、第1のゲートウェイはパケット・データ・ネットワーク・ゲートウェイであり、第2のゲートウェイは発展型パケット・データ・ゲートウェイである。前記判断するステップは、第2のゲートウェイ、第1のゲートウェイ、又は認証、認可、アカウントティングサーバによって行われる。第1の態様によれば、前記送信するステップにおけるメッセージはバインディングアップデートであり、そのバインディングアップデートは、トンネリングされる、あるいは、他のメッセージに含まれる。さらに、ユーザ装置が信頼できるアクセスネットワークにいる場合に、第1のゲートウェイが、ユーザ装置の非3GPPアクセスネットワークにおけるインターネット・プロトコル・アドレス宛てにバインディングアクノレジメント(binding acknowledgement)メッセージを送信するステップが備えられている。第1の態様によれば、ユーザ装置が信頼できないアクセスネットワークにいる場合に、第1のゲートウェイが、ユーザ装置の第2のゲートウェイにおけるインターネット・プロトコル・アドレス宛てにバインディングアクノレジメントメッセージを送信するステップが備えられている。第1の態様においては、第2のゲートウェイにおけるインターネット・プロトコル・アドレスは、事前に設定、あるいは、動的に決定される。さらに、第1の態様は、ユーザ装置がバインディングアクノレジメントメッセージを受信するステップと、非3GPPアクセスネットワークにおけるインターネット・プロトコル・アドレスが使用される場合に、ユーザ装置が信頼できるネットワークにいると判定するステップと、第2のゲートウェイでのインターネット・プロトコル・アドレスが使用される場合に、ユーザ装置が信頼で

40

50

きないネットワークにいると判定するステップとをさらに備える。

【0050】

第1の態様によれば、ユーザ装置のために、コアネットワークとアクセスネットワークとの間の信頼関係が検出されるネットワークが提供される。そのコアネットワークは、第1のゲートウェイと第2のゲートウェイを含む。ユーザ装置は、第2のゲートウェイを介してコアネットワークへメッセージを送信する。コアネットワークは、ユーザ装置が信頼できるアクセスネットワークにいるのか、あるいは、信頼できないアクセスネットワークにいるのかを判断する。また、第1のゲートウェイは、ユーザ装置が信頼できないアクセスネットワークにいる場合に、第2のゲートウェイとユーザ装置との間を経由する第1のゲートウェイとユーザ装置との間の第1のトンネルを介して、ユーザ装置へメッセージを送信する。逆に、第1のゲートウェイは、ユーザ装置が信頼できるアクセスネットワークにいる場合に、第1のゲートウェイとユーザ装置との間の第2のトンネルを介して、ユーザ装置へメッセージを送信する。

10

【0051】

さらに、第1の態様は、アクセスネットワークに接続されたユーザ装置のために、コアネットワークとそのアクセスネットワークとの間の信頼関係が検出される、そのコアネットワークにおけるゲートウェイを提供する。ゲートウェイは、ユーザ装置からメッセージを受信する受信手段を備える。ゲートウェイにおける判断手段は、ユーザ装置が信頼できるアクセスネットワークにいるのか、あるいは、信頼できないアクセスネットワークにいるのかを判断する。ゲートウェイの送信手段は、ユーザ装置が信頼できないアクセスネットワークにいる場合に他のゲートウェイとユーザ装置との間を経由するゲートウェイとユーザ装置との間の第1のトンネルを介して、ユーザ装置へメッセージを送信する。ゲートウェイの送信手段は、ユーザ装置が信頼できるアクセスネットワークにいる場合に、ゲートウェイとユーザ装置との間の第2のトンネルを介して、ユーザ装置へメッセージを送信する。

20

【0052】

第1の態様は、別の選択肢として、アクセスネットワークに接続されたユーザ装置のために、コアネットワークとアクセスネットワークとの間の信頼関係が検出される、コアネットワークにおけるゲートウェイを提供する。ゲートウェイは、ユーザ装置からメッセージを受信する受信手段を備える。ゲートウェイにおける判断手段は、ユーザ装置が信頼できるアクセスネットワークにいるのか、あるいは、信頼できないアクセスネットワークにいるのかを判断する。ゲートウェイの通信手段は、ユーザ装置が信頼できないアクセスネットワークにいる場合に、他のゲートウェイとユーザ装置との間で、メッセージを搬送する。

30

【0053】

また、第1の態様は、アクセスネットワークに接続され、第1のゲートウェイと第2のゲートウェイを含むコアネットワークとそのアクセスネットワークとの間の信頼関係が検出されるユーザ装置を提供する。ユーザ装置は、第2のゲートウェイを介してコアネットワークへメッセージを送信する送信手段を備える。ユーザ装置の受信手段は、ユーザ装置が信頼できないアクセスネットワークにいる場合に第2のゲートウェイとユーザ装置との間を経由する第1のゲートウェイとユーザ装置との間の第1のトンネルを介して、第1のゲートウェイからメッセージを受信する。又は、その受信手段は、ユーザ装置が信頼できるアクセスネットワークにいる場合に、第1のゲートウェイとユーザ装置との間の第2のトンネルを介して、第1のゲートウェイからメッセージを受信する。

40

【図面の簡単な説明】

【0054】

添付の図面に示される本発明の種々の実施の形態のより詳細な後述の説明から、さらなる特徴と利点とが明らかになるであろう。

【図1】 3GPPから信頼できない非3GPPアクセスネットワークへ移動するUEを示す。

50

【図 2】 3 G P P から信頼できる非 3 G P P アクセスネットワークへ移動する U E を示す。

【図 3】 ホームネットワークの信頼関係検出のための上位のシグナリングフローを示す。

【図 4】 暗黙の B U 及び e P D G が関与する場合の例としてのシグナリングフローを示す。

【図 5】 独立した B U が関与し e P D G が関与しない場合の例としてのシグナリングフローを示す。

【図 6】 P M I P v 6 を使用する M N 用の初期接続手順のシグナリング図を示す。

【図 7】 モバイルノードが発展型 P D G との間で I K E セキュリティアソシエーションの交換を行う、本発明の実施の形態による例としてのシグナリングフローである。

【図 8】 モバイルノードが P D N - G W との間で I K E セキュリティアソシエーションの交換を行う、本発明の別の実施の形態による例としてのシグナリングフローである。

【図 9】 モバイルノードが P D N - G W との間で I K E セキュリティアソシエーションの交換を行い、P D N - G W がアクセスネットワークが信頼できるものなのかあるいは信頼できないものなのかを判断する、本発明のさらに別の実施の形態による例としてのシグナリングフローを示す。

【発明を実施するための形態】

【 0 0 5 5 】

以下の各節では、3 G P P コアネットワークと非 3 G P P アクセスネットワークとの間の信頼関係の検出を含む本発明の種々の実施の形態について説明し、その他の選択可能な構成を例示する。

【 0 0 5 6 】

例示的な目的でのみ、実施の形態の大半を、3 G P P 通信システムとの関連で概説しており、以下の各項で使用される用語は主に 3 G P P の用語に関連する。しかしながら、ここで使用される用語と 3 G P P のアーキテクチャに基づく実施の形態の説明とは、そのようなシステムに対する本発明の原理と思想の限定を意図するものではない。

【 0 0 5 7 】

また、上記背景技術の項で行った詳細な説明は、単に、以下に記載の概ね 3 G P P に特化した例である実施の形態をよりよく理解することを意図するものであって、上記移動体通信ネットワークにおいてここに具体的に記載されている通りに処理装置及び機能を実装することに本発明を限定するものと理解すべきではない。

【 0 0 5 8 】

第 1 の態様

第 1 の態様によれば、非 3 G P P アクセスへのハンドオーバを行った、あるいは、非 3 G P P アクセスに初期接続した U E が、その非 3 G P P アクセスがホームオペレータの観点から信頼できるものであるか否かを検出できるようにし、また、これに関して、ホームネットワークへの使用すべきトンネルを検出できるようにする方法が提供される。

【 0 0 5 9 】

信頼関係を検出するために、U E 1 0 は、モビリティに関するメッセージを e P D G 1 2 へ伝送し、e P D G 1 2 は、そのメッセージを P D N - G W 1 4 へ転送する。e P D G 1 2 又は P D N - G W 1 4 は、メッセージの処理中に、U E 1 0 が信頼できる非 3 G P P アクセスネットワーク 2 0 にいるのかあるいは信頼できない非 3 G P P アクセスネットワーク 1 8 にいるのかを判断又は判定してもよい。U E 1 0 が信頼できない非 3 G P P アクセスネットワーク 1 8 にいる場合には、P D N - G W 1 4 は、e P D G 1 2 を介してモビリティメッセージを U E 1 0 に返信する。一方、U E 1 0 が信頼できる非 3 G P P アクセスネットワーク 2 0 にいる場合には、P D N - G W 1 4 は、モビリティメッセージを U E 1 0 に直接返信する。

【 0 0 6 0 】

P D N - G W 1 4 からのモビリティメッセージの宛先に基づいて、U E 1 0 は、信頼できる非 3 G P P アクセス 2 0 なのかあるいは信頼できない非 3 G P P アクセス 1 8 なのか

10

20

30

40

50

を検出できる。

【0061】

非3GPPアクセスネットワークにいるUE10には、IPアドレスが割り当てられており、そのIPアドレスはUE10自身が把握しているものである。信頼できないアクセスネットワーク18においては、UE10に対してもう1つのアドレスが必要であり、そのアドレスはePDG12によって割り当てられて、UE10自身に知らされる。このアドレスは、リモートアドレスである。

【0062】

UE10は、宛先をPDN-GW14にして、バインディングアップデート（BU）をePDG12へトンネリングする。その後、ePDG12は、UE10が信頼できる非3GPPアクセスネットワーク20にいるのかあるいは信頼できない非3GPPアクセスネットワーク18にいるのかを判断又は判定し、BUをPDN-GW14へ送信してもよい。または、ePDG12はBUをPDN-GW14へ転送し、PDN-GW14が、UE10が信頼できる非3GPPアクセスネットワーク20にいるのかあるいは信頼できない非3GPPアクセスネットワーク18にいるのかを判断又は判定してもよい。UE10が信頼できる非3GPPアクセスネットワーク20にいる場合には、PDN-GW14は、BACK（Binding Acknowledgement）を、その非3GPPアクセスにおいてUEに割り当てられたIPアドレスへ送信する。UE10が信頼できない非3GPPアクセスネットワーク18にいる場合には、PDN-GW14は、BACKを、ePDGにおいてUEに割り当てられたIPアドレス（UEのリモートIPアドレス）へ送信する。BACKにおいて使用されている宛先アドレスに基づいて、UE10は、信頼できる非3GPPアクセス20なのかあるいは信頼できない非3GPPアクセス18なのかを検出できる。

【0063】

本発明との関連においては、タイプ2ルーティングヘッダ又はホームアドレスオプションを用いたメッセージの送信は、トンネリングされていると見なされるということが分かる。

【0064】

上記の方法の利点としては、UEごとの動的な信頼可否判断が可能になること、事前設定が不要で、下位層又は非3GPPのアクセスに対するサポートが必要ないこと、UEが信頼できる非3GPPアクセスにいる場合に初期の二重トンネリング（IPsec+MIPTonneリング）が回避されること、そしてそのアクセスが、UEが例えばDHCP/DNSを介して信頼／非信頼関係を検出する機構よりも高速であることが挙げられる。

【0065】

非3GPPアクセスとホームオペレータとの間の信頼関係を検出するために、図3に示す以下の上位レベルのシグナリング手順を行う。

31. UEは、非3GPPアクセスネットワークへのハンドオーバ、あるいは、非3GPPアクセスへの初期接続を行う。UEは、その非3GPPアクセスが信頼できるものであるか否かを把握していない。

32. UEは、非3GPPアクセス認証を行ってもよい。この場合、3GPPのAAAサーバも関与する。

33. UEは、バインディングアップデート（BU）を送信する。実際には、BUの最終的な宛先はPDN-GWであるが、まずePDGへ送信される。BUをePDGに受信させるため、BUは、UEからePDGへトンネリングされるか、あるいは、ePDGへ送信される他のメッセージ（例えば、図4IKEv2メッセージ）に含める。ePDGのIPアドレスは、例えばDHCP又はDNSを介して、あるいはエニーキャストで、事前に設定又は動的に決定してもよい。

34. ePDGは、バインディングアップデートにて伝達される非3GPPアクセスについての情報、及び／又は、AAAサーバから受信した情報、及び／又は、PDN-GWから受信した情報に基づいて、非3GPPアクセスとホームオペレータとの間の信頼関係を

10

20

30

40

50

判定してもよい。AAAサーバが判定に関与する（例えば、ePDGが、UEを認証する際あるいは別のシグナリング交換時に、AAAサーバに問合せをする）場合には、AAAサーバが、アクセス認証の際に伝達される非3GPPアクセスについての情報、及び／又は、バインディングアップデートにて伝達されてePDGにより提供される非3GPPアクセスについての情報（例えば、アクセスネットワーク識別子）、及び／又は、加入者データベース内の情報に基づいて、非3GPPアクセスとホームオペレータとの間の信頼関係を判定してもよい。AAAサーバは、ePDGへ通知を送信してもよい（例えば、PDN-GWが、UEを認証する際に、応答を送信する）。その通知により、UEが信頼できる非3GPPアクセスにいるのかあるいは信頼できない非3GPPアクセスにいるのかをePDGに通知してもよい。

10

35. ePDGが信頼関係の判定に関与する場合には、ePDGは、BUを修正、あるいは、新規のBUを生成して、そのBUをPDN-GWへ送信してもよい。例えば、UEが信頼できる非3GPPアクセスにいとePDGが判定した場合には、ePDGは、気付アドレス=UEの非3GPPのローカルIPアドレスとしてBUをPDN-GWへ送信し、一方、UEが信頼できない非3GPPアクセスにいとePDGが判定した場合には、ePDGは、気付アドレス=UEのリモートIPアドレスとしてBUをPDN-GWへ送信してもよい。ePDGが信頼関係の判定に関与しない場合には、ePDGは、BUを処理せずにPDN-GWへ転送してもよい。

36. PDN-GWは、バインディングアップデートにて伝達される非3GPPアクセスについての情報、及び／又は、AAAサーバから受信した情報に基づいて、非3GPPアクセスとホームオペレータとの間の信頼関係を判定してもよい。

20

37.

a. UE10が信頼できない非3GPPアクセスにいる場合には、PDN-GWは、バインディングアクトレジット(BACK)をUEのリモートIPアドレスへ送信する。すなわち、BACKは、まずePDGによって受信され、ePDGからUEへトンネリングされる。BACKにおいて使用されている宛先IPアドレスに基づいて、UEは、信頼できない非3GPPアクセスネットワークに置かれていること、及び、PDN-GWへのトラフィックは全てePDGを介してトンネリングしなければならないことを検出できる。

b. UE10が信頼できる非3GPPアクセスにいる場合には、PDN-GWは、バインディングアクトレジット(BACK)をUEの非3GPPのローカルIPアドレスへ送信する。すなわち、BACKは、ePDGを介することなくUEへ直接送信される。BACKにおいて使用されている宛先IPアドレスに基づいて、UEは、信頼できる非3GPPアクセスネットワークに置かれていること、及び、トラフィックは全てPDN-GWへ直接送信可能であることを検出できる。

30

【0066】

この項では、例となるシグナリングフローを示す(図4参照)。このフローにおいては、BUは、独立したメッセージで送信されるのではなく、IKEv2のメッセージに含まれる。ePDGは、この暗黙のBUを検出することができ、以下にさらに詳細に述べるように、適切な措置を開始する。

41. 非3GPPアクセスネットワークへのハンドオーバー後、あるいは、非3GPPアクセスネットワークへの初期接続後、UEは、ePDGとの間でIKEv2トンネルの確立を開始する。すなわち、UEは、IKE_SA_INITメッセージをePDGへ送信し、ePDGは、IKE_SA_INITメッセージで応答する。その後、Diffie-Hellman交換が完了し、以後、全てのメッセージは、暗号化されてインテグリティが保護される。ePDGのIPアドレスは、例えばDHCP又はDNSを介して、あるいはユニキャストで、事前に設定又は動的に決定してもよい。

40

42. UEは、まず、IKE_AUTH交換を行って自身の認証を行う。UEは、さらに、リモートIPアドレスがまだ割り当てられていない場合には、設定ペイロードにおいてリモートIPアドレスを要求してもよい。

その認証は、例えば、EAPに基づいて、あるいは、メッセージ交換の数を低減するた

50

めに、EAP再認証拡張機能（ERX）のような拡張機能に基づいて行うことができる。ERXでは、UEは、再認証インテグリティ鍵を使用して認証を行うので、ここでは従来の認証が要求される。IKE_AUTHメッセージにおいては、UEがバインディングアップデートをPDN-GWとの間で行うことを希望する旨を追加フラグで示してもよい。また、例えば、競合状態を回避するために、BUのシーケンス番号が含まれなければならない（タイムスタンプも含めてもよい）。

より高速に（ERXを使用せずに）認証を行い暗黙のBUを送信する他の可能性としては、BUを（完全に又は部分的に）IKE_AUTHメッセージのIDフィールドに含めることである。IDメッセージは、可変長のフィールドであり、インシエータの識別に使用される。この場合、インシエータは、例えばBUに含まれているMN-NAIにより識別される。BUの認証は、モバイルIPv6用の認証プロトコルで行うことができる。すなわち、MN-AAAセキュリティアソシエーションを使用する。

43. ePDGはAAAサーバとコンタクトを取り、例えば、ERXを使用して、あるいは、MIP6の認証プロトコルによる機構を使用して、UEの認証を行う。

44. ePDGは、UEの認証を行った後、UEが信頼できる非3GPPアクセスにいるのかあるいは信頼できない非3GPPアクセスにいるのかを判定することができる（例えば、IKEv2メッセージにおけるUEの送信元IPアドレス、AAAサーバからの情報、又はIKE_AUTHメッセージにおけるアクセスネットワーク識別子に基づいて）。

45.

a. UEが信頼できない非3GPPアクセスネットワークにいる場合には、ePDGは、リモートIPアドレスをUEに割り当ててもよく、CoA=UEのリモートIPアドレスとしてBUをPDN-GWへ送信する。

BUフラグ付きのERXが使用された場合には、ePDGは、プロキシバインディングアップデート（Proxy Binding Update）をPDN-GWへ送信し、代替気付アドレスモビリティオプションを使用して、代替気付アドレスオプションをUEのリモートIPアドレスに設定してもよい。

含まれている、MIP6の認証プロトコル付きのBUが使用された場合には、ePDGは、BUを送信し、そのインテグリティを、UEから送信された通りに保護することができる。ePDGは、認証の際、MN-HAセキュリティアソシエーションの鍵を受信しているからである。しかしながら、UEのIPアドレスの偽造を防ぐために、この場合も、ePDGは、代替気付アドレスオプションを使用して、代替気付アドレスオプションをUEのリモートIPアドレスに設定してもよい。

b. UEが信頼できる非3GPPアクセスネットワークにいる場合には、ePDGは、CoA=UEの非3GPPのローカルIPアドレスとしてBUをPDN-GWへ送信する。ここで、ePDGは、リモートIPアドレスを割り当てることはできない。

BUフラグ付きのERXが使用された場合には、ePDGは、プロキシバインディングアップデートをPDN-GWへ送信し、代替気付アドレスモビリティオプションを使用して、代替気付アドレスオプションをUEの非3GPPのローカルIPアドレスに設定してもよい。

含まれている、MIP6の認証プロトコル付きのBUが使用された場合には、ePDGは、BUを送信し、そのインテグリティを、UEから送信された通りに保護することができる。ePDGは、認証の際、MN-HAセキュリティアソシエーションの鍵を受信しているからである。しかしながら、UEのIPアドレスの偽造を防ぐために、この場合も、ePDGは、代替気付アドレスオプションを使用して、代替気付アドレスオプションをUEの非3GPPのローカルIPアドレスに設定してもよい。

46.

a. UEが信頼できない非3GPPアクセスネットワークにいる場合には、ePDGは、IKE_AUTHメッセージにおいて、認証の成功をUEに通知する。ePDGは、さらに、設定ペイロードにおいて、リモートIPアドレスをUEに通知してもよい。

b. UEが信頼できる非3GPPアクセスネットワークにいる場合には、ePDGは、I

10

20

30

40

50

KE__AUTHメッセージにおいて、認証が失敗したことをUEに通知してもよい。
47.

a. UEが信頼できない非3GPPアクセスネットワークにいる場合には、PDN-GWは、バインディングアクノレッジ(BACK)をUEのリモートIPアドレスへ送信する。すなわち、BACKは、まずePDGによって受信され、ePDGからUEへトンネリングされる。MIP6の認証プロトコルを使用してBUの認証を行った場合には、BACKの認証にもMIP6の認証プロトコルが使用される。BACKにおいて使用されている宛先IPアドレスに基づいて、UEは、信頼できない非3GPPアクセスネットワークに置かれていること、及び、PDN-GWへのトラフィックは全てePDGを介してトンネリングしなければならないことを検出できる。

10

b. UEが信頼できる非3GPPアクセスネットワークにいる場合には、PDN-GWは、バインディングアクノレッジ(BACK)をUEの非3GPPのローカルIPアドレスへ送信する。すなわち、BACKは、UE-ePDG間のトンネルを介することなくUEへ直接送信される。MIP6の認証プロトコルを使用してBUの認証を行った場合には、BACKの認証にもMIP6の認証プロトコルが使用される。BACKにおいて使用されている宛先IPアドレスに基づいて、UEは、信頼できる非3GPPアクセスネットワークに置かれていること、及び、トラフィックは全てPDN-GWへ直接送信可能であることを検出できる。

【0067】

この項では、例となるシグナリングフローを示す(図5参照)。このフローにおいて、BUは、独立したメッセージで送信されるが、大幅な遅延は伴わない。さらに、信頼可否の判定は、ePDGにとってトランスペアレントに行うことができる。

20

51. UEは、ePDGとの間でIKEv2トンネルの確立を開始する。すなわち、UEは、IKE__SA__INITメッセージをePDGへ送信し、ePDGは、IKE__SA__INITメッセージで応答する。その後、Diffie-Hellman交換が完了し、以後、全てのメッセージは、暗号化されてインテグリティが保護される。ePDGのIPアドレスは、例えばDHCP又はDNSを介して、あるいはエニーキャストで、事前に設定又は動的に決定してもよい。

52. UEは、IKEv2に基づくMOBIKEを使用して、ePDGとの間で認証を行う。すなわち、UEは、MOBIKEをサポートしている旨の通知をePDGへ送信する。UEは、さらに、リモートIPアドレスがまだ割り当てられていない場合には、設定ペイロードにおいてリモートIPアドレスを要求してもよい。

30

注：ステップ51とステップ52は、実際のハンドオーバーよりも前に行ってもよい。

53. UEは、非3GPPアクセスネットワークへのハンドオーバーを行うが、その非3GPPアクセスが信頼できるものなのかあるいは信頼できないものなのかを把握していない。

54. UEは、MOBIKE INFORMATIONAL要求を送信して、ePDGとのIPsecセキュリティアソシエーションを更新する。MOBIKEを使用するので、全く新規のIKE及びIPsecのセキュリティアソシエーションを作成する必要はない。

40

55. MOBIKE更新の直後、UEは、UE-ePDG間のトンネルを介して、バインディングアップデートをPDN-GWへ送信する。UEは、BUに、複数の気付アドレス、すなわち、UEの非3GPPのローカルIPアドレスとUEのリモートIPアドレスを含める。複数のCoAを含めるために、UEは、例えば、IETF WG MONAMI6において提案されているような代替気付アドレスオプション又は拡張機能を使用してもよい。

56. ePDGは、セキュリティアソシエーションの更新が成功したことをUEに通知する。

注：ステップ56は、ステップ55よりも前に行ってもよい。

57. PDN-GWは、UEが信頼できる非3GPPアクセスにいるのかあるいは信頼で

50

きない非 3 G P P アクセスにいるのかを判定する（例えば、B U メッセージにおける U E の非 3 G P P のローカル I P アドレス、A A A サーバから得た情報、又はアクセスネットワーク識別子のような B U における追加情報に基づいて）。

5 8 .

a . U E が信頼できない非 3 G P P アクセスネットワークにいる場合には、P D N - G W は、バインディングアクノレッジ（B A C K）を U E のリモート I P アドレスへ送信する。すなわち、B A C K は、まず e P D G によって受信され、e P D G から U E へトンネリングされる。B A C K において使用されている宛先 I P アドレスに基づいて、U E は、信頼できない非 3 G P P アクセスネットワークに置かれていること、及び、P D N - G W へのトラフィックは全て e P D G を介してトンネリングしなければならないことを検出できる。

10

b . U E が信頼できる非 3 G P P アクセスネットワークにいる場合には、P D N - G W は、バインディングアクノレッジ（B A C K）を U E の非 3 G P P のローカル I P アドレスへ送信する。すなわち、B A C K は、U E - e P D G 間のトンネルを介することなく U E へ直接送信される。B A C K において使用されている宛先 I P アドレスに基づいて、U E は、信頼できる非 3 G P P アクセスネットワークに置かれていること、及び、トラフィックは全て P D N - G W へ直接送信可能であることを検出できる。

【 0 0 6 8 】

第 1 の態様の一般的な問題及び変形例

上記のシグナリングフローは例に過ぎない。他の変形例も可能である。例えば、一変形例においては、バインディングアップデートは、M O B I K E を使用せずに単純な I K E のみを使用して単独で送信してもよい。または、別の変形例においては、B U は、M O B I K E アップデートメッセージに暗黙的に含まれていてもよく、また、手順は e P D G にとってトランスペアレントでなくてもよい。

20

【 0 0 6 9 】

発明の実施の形態

「第 1 の態様」の項では、U E がクライアントモバイル I P、例えば、デュアルスタック M I P v 6（D S M I P v 6）をサポートしており、バインディングアップデートを e P D G へトンネリングすることを前提としている。しかしながら、発展型システムにおける U E 及び 3 G P P オペレータ（例えば、オペレータの P D N - G W）が全て D S M I P v 6 をサポートしているとは限らない。したがって、U E が B U を送信できない場合や、P D N - G W がユーザデータを P D N - G W へ直接トンネリングさせない場合がある。そのような場合、D S M I P - B U は受け付けられず、バインディングアクノレッジが U E に返信されることはない。

30

【 0 0 7 0 】

D S M I P v 6 がサポートされていない場合には、ネットワークベースモビリティ（N B M）、例えば、プロキシモバイル I P が、U E にモビリティを提供する。ここで、U E があるアクセスから別のアクセスへのハンドオーバーを行っているとき、モビリティ・アクセス・ゲートウェイ（M A G）は、U E に代わって、バインディングアップデートを P D N - G W（ローカル・モビリティ・アンカー、L M A）へ送信している。そして、ハンドオーバー後その新しい M A G によって U E に割り当てられた I P アドレス／プレフィックスは、前アクセスネットワークにおける前 M A G によって割り当てられた I P アドレス／プレフィックスと同じである。

40

【 0 0 7 1 】

プロキシモバイル I P が、信頼できないアクセスへの接続性のために使用されるときは、M A G の機能は、e P D G に設置される。U E は、信頼できない非 3 G P P アクセスにおけるローカル I P アドレス／プレフィックスを割り当てられ、U E がそのアクセスネットワークに接続すると同時にアクセスネットワークによって U E に割り当てられたそのローカル I P アドレスを用いて、e P D G への I K E / I P s e c トンネルを確立しなければならない。そして、e P D G は、e P D G の I P アドレスを含めて、プロキシバインデ

50

ィングアップデートをPDN-GWへ送信する。ePDGは、UEのホームIPアドレス／プレフィックスを受信し、このホームIPアドレス／プレフィックスをIKE_AUTH設定ペイロードにおいてUEに提供する。UEは、ホームIPアドレス／プレフィックスを通信セッションの確立のために使用するからである。

【0072】

プロキシモバイルIPが、信頼できるアクセスへの接続性のために使用されるときは、MAGは、信頼できるアクセスに（例えば、アクセスポイントに）設置され、UEは、最初は、アクセス固有の手順を使用して、信頼できるアクセスネットワークへの接続を確立する。その後、3GPPベースのアクセス認証（EAP-AKAを使用）を行わなければならない。そして、認証が成功すると、MAGは、最初に割り当てられたIPアドレス／プレフィックスを含めて、プロキシバインディングアップデートメッセージをPDN-GWへ送信する。PDN-GWは、割り当てられたホームIPアドレス／プレフィックスを含めて、BACKをMAGへ送信し、MAGは、そのホームIPアドレス／プレフィックスをUEに提供する。受信したこのホームIPアドレス／プレフィックスは、その後、UEが通信セッションを確立するために使用できる。

10

【0073】

既に先に述べたように、UEは、始めは、受信したIPアドレス／プレフィックスがPDN-GWから割り当てられたものなのか、あるいは、アクセスネットワークによってローカルに割り当てられたものなのかを把握していない。しかしながら、UEは、接続手順を適切に完結するために、その情報を把握する必要がある。

20

【0074】

そうするためには、3GPP認証が使用されているか否かということに基づいてその判定を行うことはできない。より詳細には、信頼できる非3GPPアクセスにアクセスしてNBMを使用するためには、3GPPベースのアクセス認証が要求される。一方、このことは、UEが3GPPベースのアクセス認証を行わない場合には、PMIPは信頼できないアクセスネットワークにおいては使用できないので、NBMはePDGを介してのみ使用できる、ということの意味する。しかしながら、UEが信頼できない非3GPPアクセスにアクセスするときにも、3GPPベースのアクセス認証を使用してよい。したがって、3GPPベースのアクセス認証がなされることのみで、そのアクセスが信頼できるものであると結論付けることはできない、ということになる。

30

【0075】

既に述べたように、UEがNBMを使用しているときに非3GPPアクセスへのハンドオーバを行っている場合には、そのアクセスが信頼できるものであってNBMを使用できるのか否かを検出することは問題ない。UEは、ハンドオーバ以前から、既にホームIPアドレス／プレフィックスを所持している。したがって、UEは、新しいアクセスにおいて割り当てられたIPアドレス／プレフィックスから、信頼関係を検出することができる。そのIPアドレス／プレフィックスがホームIPアドレス／プレフィックスと同じ場合には、そのアクセスは信頼できるものである。IPアドレス／プレフィックスが異なる場合には、そのアクセスは信頼できないものであり、セッションの連続性を保持するためには、ePDGへのトンネルを確立しなければならない。

40

【0076】

これは、UEが、前のアクセスネットワークからのホームIPアドレス／プレフィックスをまだ所持していない、非3GPPアクセスに初期接続する場合には適用できない。UEが3GPPベースのアクセス認証を行って成功した後にIPアドレス／プレフィックスを割り当てられるときは、そのアクセスが信頼できるものであってIPアドレス／プレフィックスがホームIPアドレス／プレフィックスでありアプリケーション層のセッションに使用できるものであるのか、あるいは、そのアクセスが信頼できないものであってIPアドレス／プレフィックスがローカルIPアドレス／プレフィックスでありePDGへのトンネルを確立しなければいけないのかを、UEは把握していない。

【0077】

50

本発明は、アクセスネットワークが信頼できるものであるか否かをその場合にもUEが判定できる実施の形態を提供する。

【0078】

●プロキシMIPv6 (PMIPv6)

本発明の実施の形態をより詳細に述べる前に、PMIPv6の概要を以下に述べる。

【0079】

モバイルIPは、ホストベースの（又はクライアントベースの）モビリティ管理として分類される。モビリティ関連のシグナリングが、ホスト（又はクライアント）とHAとの間で行われるからである。したがって、場合によっては、クライアントモバイルIP（CMIP）と呼ばれる。限定された地理的領域におけるIPモビリティ管理を対象とする他のアプローチは、ネットワークによって管理されるので、MNにとってトランスペアレントである。このアプローチを、ネットワークベースのローカルIPモビリティと称する。

【0080】

ネットワークベースモビリティの主な特徴の1つは、アクセス・ネットワーク・エンティティが、MNの移動を検出してMNの現在位置についての情報を交換するように適切に構成されており、そのため、MNは、モビリティプロセスに関与する必要がないことである。したがって、ワイヤレスインタフェースを介したモビリティ関連のシグナリングが回避される。ネットワークベースモビリティ管理の他の利点は、MIPv6のカプセル化が必要ないので無線のパケットのオーバーヘッドが少ないことと、単純なIPノード（すなわち、MIP非対応ノード）に対してモビリティをサポートしていることである。インターネット・エンジニアリング・タスク・フォース（IETF）団体は、モバイルIPプロトコルベースのローカル・モビリティ管理のためのそうしたアプローチに取り組んでいる。ネットワークエンティティは、MNに代わってプロキシとして機能するので、このプロトコルは、プロキシモバイルIP（PMIP）と呼ばれる。IPv6にはPMIPv6と呼ばれる変種があり、IPv4にはPMIPv4と呼ばれる変種がある。本発明の実施の形態のほとんどは、ネットワークベースモビリティ管理用のプロトコルとしてPMIPv6を前提としているが、本発明は、PMIPv6に限定されない。PMIPv4など、他のネットワークベースモビリティ管理プロトコルに適用してもよい。実際には、本発明は、ネットワークベースモビリティに限定されず、クライアントベースモビリティ方式を使用するMNに適用してもよい。

【0081】

ネットワークの制限されたトポロジ的局所に存在するあらゆるIPv6ホストに、ホストの関与を必要とせずにモビリティサポートを提供するために、プロキシモバイルIP（PMIP）は、アクセスリンクに接続されているモバイルノードに対するモビリティ関連のシグナリングを管理する、アクセスネットワークにおけるプロキシ・モビリティ・エージェントであるモバイル・アクセス・ゲートウェイ（MAG）と呼ばれる新しい論理エンティティを導入している。MAGは、モバイルノードのリンクへの接続のトラッキングとモバイルノードのローカル・モビリティ・アンカーへのシグナリングとに関与するエンティティである。MAGは、通常、アクセスルータ（AR）と同じ場所に設置され、モバイルノードに代わってモバイルIPv6シグナリングメッセージを行い、例えば、MNに代わってBUメッセージを送信できる。それらのBUメッセージにはフラグが付けられるので、プロキシBU（PBU）メッセージとして識別できる。また、PBUメッセージは、ネットワークアクセス識別子（NAI）オプション、ホーム・プレフィックス・オプション、及び、タイムスタンプオプションを含んでもよい。NAIオプションは、「username@realm」という形式の、MNの識別に使用されるNAIを含む。ホーム・プレフィックス・オプションは、使用時、MNのHoA又はホームプレフィックスを含む。いわゆるper-MN-prefixアドレッシングモデルにおいては、各MNは、固有のホームプレフィックスを持ち、MNの1つ又は複数のグローバルIPアドレスは、このプレフィックスに基づいて設定される。固有のホームプレフィックスは、PBUメッセージにおいて、HoAの代わりに使用できる。タイムスタンプオプションは、PBUがMAGによって

送信された時刻を含み、ローカル・モビリティ・アンカー（LMA）によって、PBUメッセージの新しさを識別するために使用される。PBUメッセージのシーケンス番号の値は、LMAには無視される。

【0082】

ローカル・モビリティ・アンカー（LMA）は、プロキシモバイルIPv6ドメインにおけるモバイルノードのホームエージェントである。LMAは、モバイルノードのホームプレフィックスのトポロジー上のアンカーポイントであり、モバイルノードの到達可能性状態を管理するエンティティである。LMAが、モバイルIPv6の基礎仕様において定義されているように、ホームエージェントの機能と、プロキシモバイルIPv6をサポートするために必要なその他の機能とを持っているということを理解することが重要である。

10

【0083】

MNは、信頼できるアクセスネットワークにおいて新しいMAGに接続すると、EAPフレームワークとEAP-AKAなどのEAPメソッドとを使用して、そのネットワークとの間で認証を行う。MAGは、典型的には、パススルー認証を行うオーセンティケータとして機能し、MNに関連付けられたAAAサーバ/インフラストラクチャへEAPパケットを転送する。MNは、NAIを識別子として使用する。ネットワーク認証が成功した場合には、MAGは、LMAにおいて割り当てられたMNのホームプレフィックスを含めて、MNのプロファイルをAAAサーバから取得する。その後、MAGは、PBUをLMAへ送信し、ホームプレフィックスをMNに告知する。MNは、ARとの間で認証を行った後、IP設定を開始する。すなわち、MNは、リンクローカル（LL）IPアドレスを設定し、チェックすべきLLアドレスの要請ノードマルチキャストアドレスへ近隣要請（NS）メッセージを送信することによって、LLアドレスに対して重複アドレス検出（DAD）を行う。この手順が成功した場合には、MNは、対応するマルチキャストアドレスを介して、ルータ要請（RS）メッセージを全てのルータへ送信し、ルータ広告（RA）を受信するまで待機する。AR/MAGは、MNのホームプレフィックスを含むユニキャストRAで応答する。

20

【0084】

グローバルIPアドレスを設定した後、MNはIPリーチャブルになり、そのPMIPドメイン内を移動している限りはそのIPアドレスを使用することができる。初期接続手順におけるPMIPv6用の上記した例としてのシグナリングフローを図6に示す。

30

【0085】

上記においては、ネットワークベースモビリティ方式を詳細に説明した。本発明の以下の実施の形態については、PMIPが、UEに対して使用され通信セッション時のモビリティを可能にするものと想定しているからである。ただし、本発明はそれに限定されず、本発明の種々の実施の形態の思想と原理とは、MIPなどのクライアントベースモビリティ方式をUEが使用する場合にも同様に適用できる。実際、PMIPは、部分的にMIPをベースにしている。

【0086】

「発明の概要」の項で概説したように、本発明の主な思想の1つは、セキュリティトンネル確立手順を使用して非3GPPアクセスの信頼関係を検出することである。より詳細には、UEは、セキュリティトンネルの確立を開始し、トンネルを確立する際又はその後に、非3GPPアクセスの信頼関係を把握する。本発明の一実施の形態においては、セキュリティトンネル確立手順は、IPsecトンネルがIKEv2を使用して、そのIPsecトンネルに使用されるセキュリティアソシエーションを取り決めることによって行うことができる。

40

【0087】

IPsec（IKEv2）

本発明の種々の実施の形態をより詳細に説明する前に、IPsec（IKEv2）の手順について簡単に説明する。

50

【0088】

インターネット鍵交換（IKE）プロトコルは、IPsec用の自動鍵管理を運用するのに役立つ。IKEは、安全でないコンピュータネットワークを介しての安全な鍵交換を行うために、Diffie-Hellman鍵交換を使用する。IKEは、セキュリティパラメータの取り決め方と共有鍵の交換の仕方とを規定している。IPsecによる暗号化接続を実際に開始する前に、両サイドは、お互いの認証を行い、使用する鍵アルゴリズムを取り決める必要がある。

【0089】

このように、IKEは、一对の通信ピア間でセキュリティアソシエーションを取り決めるのに使用される。IKEは、インターネット・プロトコル・セキュリティ（IPsec）の一部として定義されている。セキュリティアソシエーション（SA）は、両ピア間の取り決めであり、例えば、ID、IPsec接続用の鍵アルゴリズム、及び／又は、IPsec接続の確立元及び確立先ネットワークを含んでもよい。

10

【0090】

IKEv2は、セキュリティアソシエーションの取り決めに、IKE_SA_INIT及びIKE_AUTHという、2つのフェーズを使用する。各フェーズは、要求と応答で構成される。従って、IKE_SAを確立するには、少なくとも4つのメッセージが必要になる。IKE_SA_INIT交換においては、両ピアは、暗号アルゴリズムの使用を取り決め、鍵の取り決めに使用する情報を交換する。この交換の後、各ピアは、認証及び暗号化用の共有対称鍵を導出するために使用する鍵素材を生成する。これらの鍵は、IKE_SAと関連付けられている。IKE_SAは双方向性である。この時点では、両ピアは、暗号鍵を取り決めてはいるが、お互いの認証は行っていない。これらの鍵は、IKE_AUTH交換を保護するために使用される。

20

【0091】

IKE_AUTH交換は、ピアの相互認証を提供するために、及び、両IKEv2ピア間でIPsecを使用するためのセキュリティアソシエーションを確立するために使用される。各ピアは、自身のID（例えば、IPアドレス、フルドメイン名）をアサートし、認証機構を使用してそのアサーションを証明する。この認証機構としては、電子署名、拡張認証プロトコル（EAP）、又は事前共有鍵を使用してもよい。各ピアは、相手のピアのアサーションの確認を行う。確認されると、相互エンティティ認証が与えられる。確認が失敗した場合には、セキュリティアソシエーションの取り決めは失敗し、IKE_SA_INIT交換において取り決められたIKE_SAは解除される。

30

【0092】

両ピアは、使用する暗号アルゴリズムと、両ピア間の保護対象となるトラフィックとを取り決める。また両ピアは、任意で、鍵の取り決めのための追加の素材をIKE_AUTH交換において交換するようにしてもよい。証明書の交換も行ってもよい。この交換において、2つの単方向セキュリティアソシエーションが作成される。

【0093】

図7は、本発明の実施の形態に係る信頼検出手順を示すシグナリングフローである。本実施の形態においては、UEは、アクセスネットワークが信頼できるものなのかあるいは信頼できないものなのかを判定するのに必要な情報を入手するために、ePDGとの間でIKEv2の手順を開始する。ここで、その判定は、UE自身が行う。

40

【0094】

既に何度も述べたように、UEは、非3GPPアクセスに接続するときは、まず3GPPベースのアクセス認証を行う。認証が成功すると、IPアドレス／プレフィックスがUEに割り当てられるが、UEは、そのIPアドレス／プレフィックスが通信セッションに使用できるものであるか否か、すなわち、そのアクセスが信頼できるものであるかを把握していない。

【0095】

本発明のこの実施の形態では、まず、このIPアドレス／プレフィックスを使用して、

50

例えばDNSを介して（ドメイン名解決）ePDGを発見することを提案する。IPプレフィックスを受信する場合には、まず、UEがIPプレフィックスからIPアドレスを生成することが必要である。これにより、UEは、DNSサーバと通信できるようになる。

【0096】

そうして、ePDGが発見され、UEは、以下より明らかになるように、このePDGとの間でIKEv2 SAのセットアップを開始する。以下のシグナリングフローは、図7に図示されている。PDN-GWは、UEのLMAであることを前提とし、ePDGは、アクセスネットワークが信頼できないものである場合のUEのMAGであることを前提とする。

71. まず、ePDGとの間でIKE__SA__INITを行ってePDGへの安全な接続を確立することにより、IKEの手順がUEによって開始される。

10

72. 開始が成功すると、IKE__AUTHのシグナリングにおいて、UEは、自身のID(NAI)をIDiペイロードに、APN情報をIDrペイロードに含める。さらに、UEは、ホームIPアドレス／プレフィックスを取得したい旨を設定ペイロードにおいて示す。

73. ePDGは、AAAサーバでUEの認証を開始する。ここでは、EAP-AKAが使用される。

74. 認証後、ePDGは、プロキシバインディングアップデートメッセージをPDN-GWへ送信する。PBUメッセージは、UEのIDと要求されたAPNとを含む。本発明の有利な一実施の形態によれば、このPBUは、例えばフラグによって、仮のものであると示さなければならない。そして、PDN-GW内にバインディングキャッシュエントリ(Binding Cache Entry)が既に存在する場合には、PDN-GW(LMA)は、パスをePDGに切り替えない。このようにするのは、このIKEの手順は、アクセスネットワークの信頼関係を判定するために使用されるだけであり、UEに到達するためのIPsecトンネルを実際に確立するために使用されるわけではないからである。もしPBUが仮のもの等でなければ、PDN-GWは、ePDGを介したUEへのデータパスを確立してしまう。そうすると、UEが信頼できるアクセスネットワークにいる場合には、ePDG経由の迂回路なしでUEと直接通信することが可能になり、IPsecトンネルをまた解除しなくななくなる。

20

75. PDN-GWは、プロキシバインディングアクノレッジにおいて、UEの割り当てられたホームIPアドレス／プレフィックスで応答する。

30

76. ePDGは、ステップ73の認証が成功したことをUEに通知する。

77. IKE__AUTH ResponseにおいてEAP successを受信すると、UEは、最初のIKE__SA__INITメッセージの認証を行うための生成されたAUTHパラメータと共にIKE__AUTH RequestをePDGへ送信する。

78. ePDGは、2番目のIKE__SA__INITメッセージの認証を行うための生成されたAUTHパラメータを含み、かつ割り当てられたホームIPアドレス／プレフィックスを設定ペイロードに含むIKE__AUTH Responseで応答する。

79. UEは、ePDGからのIKE__AUTH ResponseにおけるIPアドレス／プレフィックスを、ローカルに割り当てられたIPアドレス／プレフィックスと比較する。両IPアドレス／プレフィックスが一致する場合には、信頼できるアクセスであり、UEはePDGへのトンネルを使用する必要がない。両IPアドレス／プレフィックスが一致しない場合には、信頼できないアクセスであり、UEは、PDNにアクセスするためには、ePDGへのトンネルを使用しなければならない。

40

【0097】

例としての上記シグナリングフローは、しかしながら、本発明の思想と原理とをどのように適用できるかということに関する、単なる一つの可能性を表わしているにすぎない。当然、いくつかの変形例があり、そのうちのいくつかを以下に述べる。

【0098】

例えば、受信したホームIPアドレス／プレフィックスをIKE__AUTH Resp

50

onseメッセージにてステップ78において送信する代わりに、ePDGは、このホームIPアドレス／プレフィックスをステップ76のIKE_AUTH Responseメッセージ内で既にUEに受け渡しておいてもよい。ホームIPアドレス／プレフィックスは、その時点で既にePDG内に存在するからである。

【0099】

上記手順に代わる更に別の方法の1つは、PDN-GWによってUEに割り当てられたホームIPアドレス／プレフィックスをAAA (Authentication (認証)、Authorization (認可)、Accounting (アカウントिंग)) /HSS (Home Subscriber Service (ホーム加入者サービス)) サーバに記憶することである。そのとき、ePDGがステップ73の認証の際にUEのホームIPアドレス／プレフィックスを入手できるようにしてもよい。この場合、ePDGによるPDN-GWへのPBUの送信(ステップ74参照)をIKEの手順によってトリガする必要はない。従って、ステップ75も必要なくなる。認証手順の際にUEのホームIPアドレス／プレフィックスを入手したePDGは、その後、図7のステップ76～78で既に示したように、UEへのIKE_AUTH Responseメッセージの送信を進めることができる。

【0100】

次に、図7のステップ74における仮のPDUの使用に関し、さらに別の選択肢について述べる。仮のPDUの代わりに、ePDG(MAG)は、最初に受信したUEのIPアドレス／プレフィックスをPBUに含め、さらに、Handover Indicatorを「attachment」又は「unknown」に設定してもよい。その結果、PBUは、PDN-GW(LMA)へ送信され、次に、PDN-GW(LMA)は、上記IPアドレス／プレフィックスが既にUEに割り当てられているか否かを単独で判定する。より詳細には、アクセスネットワークが信頼できるものである場合には、アクセスネットワークのアクセスポイントは、UEのホームIPアドレス／プレフィックスを入手するため、UEの接続と同時にPDN-GWとコンタクトを取る。これにより、PDN-GWは、ホームIPアドレス／プレフィックスをUEに対して生成して、対応するテーブルに格納する。

【0101】

最初に割り当てられたIPアドレス／プレフィックスを含むPBUを受信したときは、PDN-GWは、受信したIPアドレス／プレフィックスが既にUEに割り当てられていると判定することができる。PDN-GWは、その判定、すなわち、アクセスネットワークは信頼できるものである旨をePDGへのProxy-BACK応答において示してもよい。逆に、アクセスネットワークが信頼できないものであるときは、PDN-GWは、最初はアクセスネットワークにおけるアクセスポイントによってコンタクトが取られていなかったもので、PBUメッセージ内で受信したIPアドレス／プレフィックスは、PDN-GWにとって未知である。したがって、PDN-GWは、UEが信頼できないネットワークにいと推測する。さらに、PDN-GWは、新しいホームIPアドレス／プレフィックスをUEに割り当てて、そのホームIPアドレス／プレフィックスをProxy-BACK応答においてePDGへ送信してもよい。

【0102】

上記の結果、PDN-GWは、トンネルをePDGに切り替えるべきときと、切り替えるべきでないときを知る。詳細には、PDN-GWがアクセスネットワークは信頼できるものであると判定した場合(受信したPBUにおけるIPアドレス／プレフィックスが前に割り当てられたUEのIPアドレス／プレフィックスに一致する場合)には、トンネルのePDGへの切り替えは行われない。しかしながら、PDN-GWがアクセスネットワークは信頼できないものであると判定した場合(受信したIPアドレス／プレフィックスがPDN-GWにとって未知の場合)には、トンネルは、既にePDGに切り替えられているであろう。UEがコアネットワーク(PDN-GW)と通信するために、ePDGを使用するはずだからである。

【0103】

既に先に述べたように、UE以外のエンティティがアクセスネットワークの信頼関係を判定してもよい。ePDGは、ステップ73又はステップ75の後、最初に割り当てられたIPアドレス／プレフィックスと、UEのホームIPアドレス／プレフィックスとを把握してもよい。さらに詳細には、ePDGは、最初に割り当てられたホームIPアドレス／プレフィックスをIKE__SA__INITメッセージ交換により把握する。UEは、この最初に割り当てられたホームIPアドレス／プレフィックス（例えば、UEからePDGへ送信される最初のIKE__SA__INITメッセージの送信元アドレスとして）に基づいて、ePDGと通信するからである。または、そのIPアドレス／プレフィックスは、UEからePDGへ送信されるIKE__SA__INITメッセージのペイロードフィールドに挿入することができる。さらに、ePDGは、ステップ73の認証手順の際（上記の選択可能な方法参照）、又は、図7のステップ75で、UEのホームIPアドレス／プレフィックスを知る。

10

【0104】

そのとき、ePDGは、両IPアドレス／プレフィックス、すなわち、最初に割り当てられたものとホームIPアドレス／プレフィックスとを比較することによって、アクセスネットワークが信頼できるものなのかあるいは信頼できないものなのかを推測することができる。そして、両IPアドレス／プレフィックスが一致する場合には、ePDGは、UEにその判定結果を通知するため、またそれによってアクセスネットワークの信頼特性を通知するために、ステップ76又はステップ78のIKE__AUTH Response

20

【0105】

にNotify-Payloadを含めてもよい。また、前記選択可能な方法において、アクセスネットワークが信頼できるものであるということをePDGが判定すると想定すると、そのことをePDGはUEに通知してもよく、さらに、残りの手順は、中断することができる。例えば、ステップ76においてUEがその判定をIKE__AUTH__RESPONSEメッセージで通知される場合には、ステップ77とステップ78は行われない。同様に、ホームIPアドレス／プレフィックスをAAAサーバから受信して、ePDGが、好ましくは認証手順のメッセージにおいて、MNに通知する場合には、ステップ74～ステップ78は行われない。

【0106】

30

しかしながら、両IPアドレス／プレフィックスが一致しない場合には、ePDGは、手順を継続し、PDN-GWによって割り当てられた新しいホームIPアドレス／プレフィックスを、最初（ステップ76）又は最後（ステップ78）のIKE__AUTH__RESPONSEメッセージを介してUEに通知する。また、この場合、PDN-GWに対して仮のPBUを使用する必要はない。アクセスネットワークは信頼できないものであり、PDN-GWはいずれにしてもePDGを介してUEと通信しなければならないからである。

【0107】

ePDGへのIKEv2シグナリングの際にUEに通知する代わりに、UEは、ePDGへのトンネルのセットアップが成功した後のある時点で、例えば、PDN-GWとのシグナリング交換、又は、ePDGによりトリガされるIKE__INFORMATIONAL交換によって、信頼関係を検出してもよい。この場合、UEは、上記の手順と同様に、ePDGへのIKEv2トンネルを確立し、最初は、セッション開始の際の遅延を減少させるために、非3GPPアクセスの信頼関係とは無関係に、そのトンネルを使用する（非信頼モード）。そして、UEがある時点で非3GPPアクセスが信頼できるものであるということを検出した場合には、UEは、ネットワークを（例えば、IKE__INFORMATIONAL交換において）トリガしてパスを切り替え、ePDGトンネルを以後使用しないようにさせもよい（信頼モード）。

40

【0108】

この最適化の問題の1つは、UEが、同じプレフィックスを、一方では、非3GPPア

50

クセスにおいてローカルIPプレフィックスとして使用し、他方で、ePDGによって割り当てられた（ホーム）IPプレフィックスとしても使用する、ということができないことである。このことは、PDN-GWにおいて矛盾を引き起こす。PDN-GWは、このプレフィックスに対するパケットを、ePDG及び非3GPPアクセスにおけるMAGのどちらか一方にしかトンネリングさせることができないからである。

【0109】

したがって、（ホーム）IPプレフィックスとしてePDGを介してPDN-GWによって割り当てられたIPプレフィックスは、非3GPPアクセスにおいて割り当てられたIPプレフィックスとは異なるものでなければならない。そうすると、UEは、両IPアドレス／プレフィックスを比較することによっては非3GPPアクセスの信頼関係を検出せず、前に述べた他の方法、例えば、PDN-GWとの間の直接のシグナリング又はIKE INFORMATIONAL交換によって検出することになる。

10

【0110】

本発明の別の実施の形態によれば、IKEv2の手順は、ePDGの代わりにPDN-GWとの間で行うことができる。この実施の形態においては、PDN-GWは、IKE_SA_INITメッセージを受け付けるように構成されていることを想定する。ただし、多くの場合はこの想定と違っている。これは、図8に示されている。図8は、シグナリングフローを表わしており、そのシグナリングフローにおいて、UEは、アクセスネットワークが信頼できるものなのかあるいは信頼できないものなのかを判定する。本発明のこの実施の形態においては、必要な情報は、以下に詳細に述べるように、PDN-GWから直接UEへ提供される。図8においてePDGは省略されているが、ePDGはこれまで通り存在している。しかしながら、メッセージはUEとPDN-GWとの間で直接交換されるので、ePDGは、図8の例としてのシグナリング手順には関与しない。

20

【0111】

前記と同様に、UEは、非3GPPアクセスに接続するときは、まず3GPPベースのアクセス認証を行う。認証が成功すると、IPアドレス／プレフィックスがUEに割り当てられる。そのIPアドレス／プレフィックスは、ローカルに割り当てられたもの（アクセスネットワークが信頼できないものであるとき）でもよく、あるいは、PDN-GWにおいて割り当てられたもの（アクセスネットワークが信頼できるものであり、アクセスポイントがPDN-GWとコンタクトを取ることができるとき）でもよい。UEは、このIPアドレス／プレフィックスを使用して、例えば、DNSを利用し、PDN-GWのIPアドレスを発見する（例えば、このPDNのアクセスポイント名を使用してFQDNを構成することによって）。そして、UEは、以下の記載からより明らかになるように、PDN-GWとの間でIKEv2 SAの確立を開始する。

30

81. まず、IKE_SA_INITを行って、PDN-GWへの安全な接続を確立する。

82. その後、IKE_AUTHのシグナリングにおいて、UEは、自身のID（NAI）をID_iペイロードに、APN情報をID_rペイロードに含める。さらに、UEは、非3GPPアクセスにおいてローカルに割り当てられたIPアドレスを設定ペイロードにおいて示すことができる。

40

83. PDN-GWは、AAAサーバでUEの認証を開始する。EAP-AKAが使用される。

84. PDN-GWは、認証が成功したことをUEに通知する。

85. IKE_AUTH ResponseにおいてEAP successを受信すると、UEは、最初のIKE_SA_INITメッセージの認証を行うための生成されたAUTHパラメータと共にIKE_AUTH RequestをPDN-GWへ送信する。

86. PDN-GWは、2番目のIKE_SA_INITメッセージの認証を行うための生成されたAUTHパラメータを含み、かつ割り当てられたホームIPアドレス／プレフィックスを設定ペイロードに含むIKE_AUTH Responseで応答する。

87. UEは、PDN-GWからのIKE_AUTH ResponseにおけるIPア

50

ドレス／プレフィックスを、非 3 G P P アクセスにおいて割り当てられた I P アドレス／プレフィックスと比較する。両 I P アドレス／プレフィックスが一致する場合には、信頼できるアクセスである。両 I P アドレス／プレフィックスが一致しない場合には、信頼できないアクセスであり、U E は、P D N への接続性を得るために e P D G へのトンネルを確立しなければならない。

【0112】

上記のシグナリングフローが図 7 のシグナリングと異なる点は、主に、I P s e c トンネル確立の手順が、e P D G ではなく P D N - G W との間で行われることである。P D N - G W は U E の L M A なので、P B U メッセージ及び P - B A C K メッセージは不要になる。また、P D N - G W が U E のホーム I P アドレス／プレフィックスを保持しているので、U E のホーム I P アドレス／プレフィックスを入手するために追加のシグナリング (P B U 及び P - B A C K) は必要ない。

10

【0113】

図 7 の実施の形態に関連して述べた多数の変形例及び選択可能な方法は、図 8 の実施の形態にも適用可能である。例えば、ステップ 8 6 の代わりにステップ 8 4 の I K E _ A U T H _ R E S P O N S E メッセージにおいて U E のホーム I P アドレス／プレフィックスを U E に通知してもよい。

【0114】

実際は、図 9 から明らかになるように、U E はアクセスネットワークの信頼特性をより早い時点で知るようにしてもよい。図 9 におけるシグナリングフローも、U E によって信頼関係が判定された後に行われるステップを、信頼できる場合と信頼できない場合の両方について図示する。

20

9 1. U E は、最初に割り当てられた I P アドレス／プレフィックスを (送信元アドレスに、あるいは、メッセージのペイロードに付加的に) 含めて、I K E _ S A _ I N I T を P D N - G W へ送信する。

9 2. P D N - G W は、受信した、U E により使用された I P アドレス／プレフィックスに基づいて、U E が信頼できる非 3 G P P アクセスにいることあるいは信頼できない非 3 G P P アクセスにいることを検出してもよい。例えば、使用された I P アドレス／プレフィックスがその P D N - G W によって割り当てられたものである場合には、信頼できるアクセスのはずである。逆に、I P アドレス／プレフィックスが P D N - G W によって割り

30

9 3. P D N - G W は、N o t i f y ペイロードを I K E _ S A _ I N I T (又は I K E _ A U T H) R e s p o n s e メッセージに含め、アクセスが信頼できるもの (又は信頼できないもの) であるということを U E に通知してもよい。

9 4 a. U E は、非 3 G P P アクセスが信頼できないものであることを示す I K E _ S A _ I N I T (又は I K E _ A U T H) R e s p o n s e メッセージの N o t i f y ペイロードを受信すると、e P D G への I K E v 2 トンネル確立の手順を開始する。

9 5 a. U E の認証が成功すると、e P D G は、P B U を P D N - G W へ送信し、割り当てられた I P アドレス／プレフィックスと共に P B A を受信する。

9 6 a. I K E v 2 / I P s e c トンネルのセットアップを完了する。

40

9 7 a. e P D G は、設定ペイロードにおいて、割り当てられた I P アドレス／プレフィックスを U E に通知する。

9 8 a. U E は、P D N - G W によって割り当てられたホーム I P アドレス／プレフィックスを使用して、アプリケーション層のセッションを開始できる。

9 4 b. U E は、非 3 G P P アクセスが信頼できるものであることを示す I K E _ S A _ I N I T (又は I K E _ A U T H) R e s p o n s e メッセージの N o t i f y ペイロードを受信すると、I K E v 2 の手順を中止する。そして、U E は、割り当てられた I P アドレス／プレフィックスで、アプリケーション層のセッションをすぐに開始することができる。

【0115】

50

【 0 1 1 6 】

10

20

30

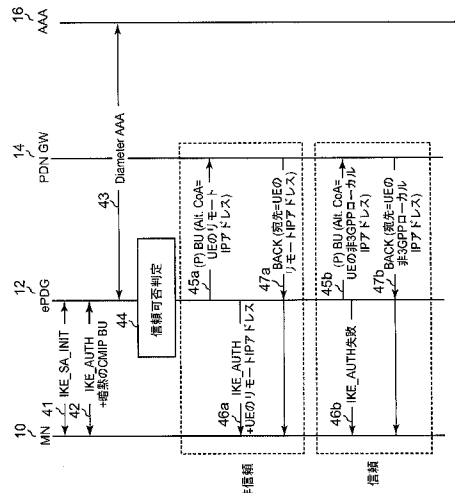
【 0 1 2 0 】

40

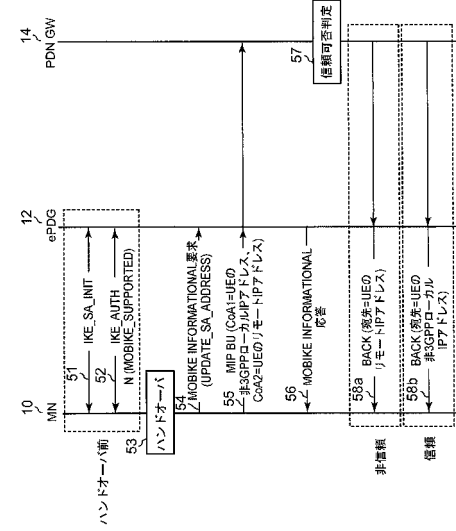
【 0 1 2 2 】

50

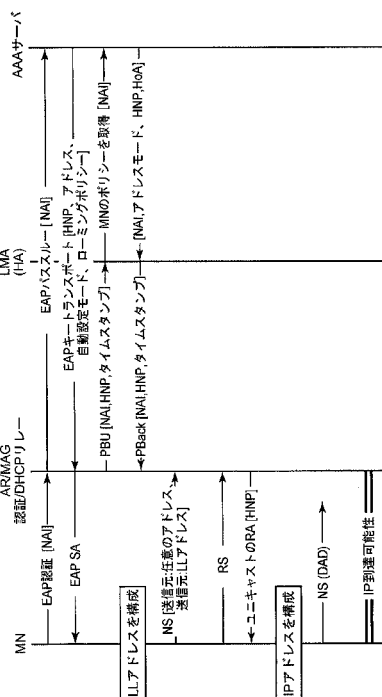
【図 4】



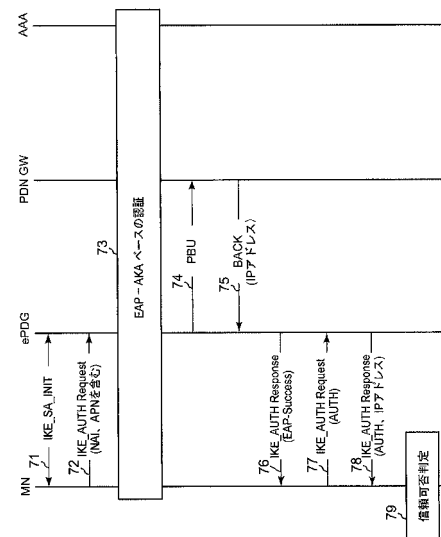
【図 5】



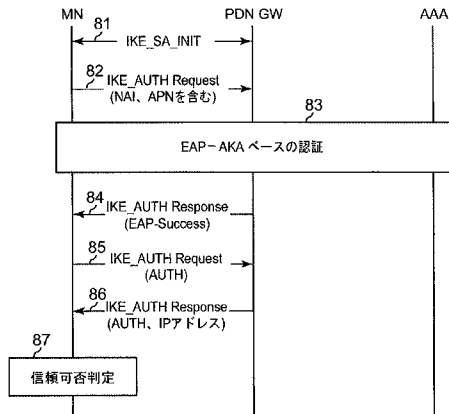
【図 6】



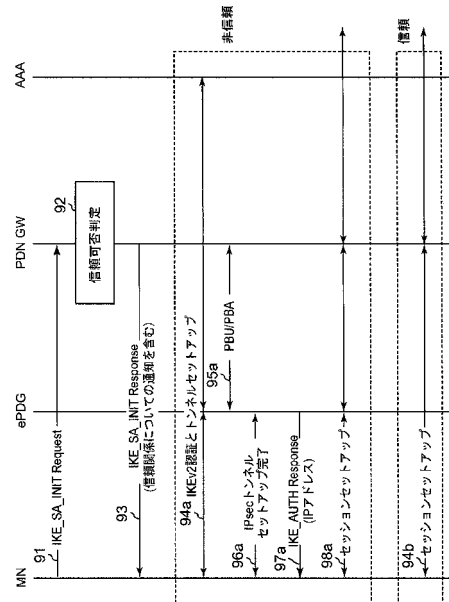
【图 7】



【図 8】



【図 9】



フロントページの続き

- (72)発明者 ヴェニゲル キリアン
ドイツ連邦共和国 63225 ランゲン モンツァシュトラッセ 4c パナソニック アール
アンドディー センター ジャーマニー ゲゼルシャフトミットベシュレンクテルハフツング内
- (72)発明者 荒牧 隆
大阪府門真市大字門真1006番地 パナソニック株式会社内
- (72)発明者 シュリンガー ヨン
ドイツ連邦共和国 63225 ランゲン モンツァシュトラッセ 4c パナソニック アール
アンドディー センター ジャーマニー ゲゼルシャフトミットベシュレンクテルハフツング内
- (72)発明者 平野 純
大阪府門真市大字門真1006番地 パナソニック株式会社内
- (72)発明者 池田 新吉
大阪府門真市大字門真1006番地 パナソニック株式会社内

審査官 北元 健太

- (56)参考文献 米国特許出願公開第2007/0006295 (US, A1)
Architecture Enhancements for non-3GPP accesses (Release 8), 3GPP TS 23.402, 2007
年 5月, V1.0.0
S. Vaarala, Mobile IPv4 Traversal Across IPsec-based VPN Gateways, [online], draft-ietf-mobileip-vpn-problem-solution-03, 2003年 9月29日, URL, <http://tools.ietf.org/pdf/draft-ietf-mobileip-vpn-problem-solution-03.txt>

- (58)調査した分野(Int.Cl., DB名)
H04W 4/00 - 99/00
H04B 7/24 - 7/26