

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号

特許第7014212号

(P7014212)

(45)発行日 令和4年2月1日(2022.2.1)

(24)登録日 令和4年1月24日(2022.1.24)

(51)国際特許分類

F I

H O 4 W 48/18 (2009.01)

H O 4 W 48/18

H O 4 W 12/00 (2021.01)

H O 4 W 12/00

H O 4 W 76/10 (2018.01)

H O 4 W 76/10

H O 4 W 92/24 (2009.01)

H O 4 W 92/24

請求項の数 6 (全20頁)

(21)出願番号	特願2019-195878(P2019-195878)	(73)特許権者	000004237
(22)出願日	令和1年10月29日(2019.10.29)		日本電気株式会社
(62)分割の表示	特願2018-144936(P2018-144936)の分割		東京都港区芝五丁目7番1号
原出願日	平成27年5月26日(2015.5.26)	(74)代理人	100103894
(65)公開番号	特開2020-36346(P2020-36346A)		弁理士 家入 健
(43)公開日	令和2年3月5日(2020.3.5)	(72)発明者	ジャン シャオウェイ
審査請求日	令和1年10月29日(2019.10.29)		東京都港区芝五丁目7番1号 日本電気株式会社内
(31)優先権主張番号	特願2014-112269(P2014-112269)	(72)発明者	田村 利之
(32)優先日	平成26年5月30日(2014.5.30)		東京都港区芝五丁目7番1号 日本電気株式会社内
(33)優先権主張国・地域又は機関	日本国(JP)	(72)発明者	ブラサド アナンド ラガワ
			東京都港区芝五丁目7番1号 日本電気株式会社内
		審査官	田部井 和彦

最終頁に続く

(54)【発明の名称】 U E 及び方法

(57)【特許請求の範囲】

【請求項1】

移動通信システムにおけるU E (User Equipment) であって、
 加入者情報を含むリクエストメッセージを基地局を介して第1移動管理装置に送信する送信手段と、
 前記第1移動管理装置との認証及びセキュリティ手順は実行せず、署名管理装置から署名データを受信することなく事前に構成した第2移動管理装置に関する情報に基づき、前記第1移動管理装置から前記第2移動管理装置に前記基地局を介してリダイレクトされた場合に、前記第2移動管理装置と前記認証及びセキュリティ手順を実行する制御手段と、
 前記第2移動管理装置とN A S (Non-Access Stratum) 鍵を共有することにより、前記第2移動管理装置と前記基地局を介してセキュアなコネクションを確立する通信手段と、
 を有し、

前記認証は、前記第2移動管理装置からの要求に応じて前記署名管理装置から送信された、A V (Authentication Vector) に関する情報に基づく処理である、

U E。

【請求項2】

請求項1記載のU E であって、
 前記加入者情報は、I M S I (International Mobile Subscriber Identity) である、
 U E。

【請求項3】

請求項 1 記載の U E であって、

前記第 1 移動管理装置および前記第 2 移動管理装置は、M M E (Mobility Management Entity) 又は S G S N (Serving GPRS (General Packet Radio service) Support Node) であり、前記署名管理装置は、H S S (Home Subscriber Server) 又は H L R (Home Location Register) / H S S であり、前記基地局は、e N B (evolved Node B) 又は B T S (Base Transceiver Station) / B S C (Base Station controller) である、
U E。

【請求項 4】

移動通信システムにおける U E (User Equipment) の方法であって、
加入者情報を含むリクエストメッセージを基地局を介して第 1 移動管理装置に送信し、
前記第 1 移動管理装置との認証及びセキュリティ手順を実行せず、署名管理装置から署名データを受信することなく事前に構成した第 2 移動管理装置に関する情報に基づき、前記第 1 移動管理装置から前記第 2 移動管理装置に前記基地局を介してリダイレクトされた場合に、前記第 2 移動管理装置と前記認証及びセキュリティ手順を実行し、
前記第 2 移動管理装置と N A S (Non-Access Stratum) 鍵を共有することにより、前記第 2 移動管理装置と前記基地局を介してセキュアな接続を確立し、
前記認証は、前記第 2 移動管理装置からの要求に応じて前記署名管理装置から送信された、A V (Authentication Vector) に関する情報に基づく処理である、
方法。

10

【請求項 5】

請求項 4 記載の方法であって、
前記加入者情報は、I M S I (International Mobile Subscriber Identity) である、
方法。

20

【請求項 6】

請求項 4 記載の方法であって、
前記第 1 移動管理装置および前記第 2 移動管理装置は、M M E (Mobility Management Entity) 又は S G S N (Serving GPRS (General Packet Radio service) Support Node) であり、前記署名管理装置は、H S S (Home Subscriber Server) 又は H L R (Home Location Register) / H S S であり、前記基地局は、e N B (evolved Node B) 又は B T S (Base Transceiver Station) / B S C (Base Station controller) である、
方法。

30

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、専用コアネットワーク (Dedicated Core Network) のための装置、システム、及び方法に関し、特に、ユーザ端末 (U E : User Equipment) が適切なコアネットワークによってサービスを提供されることを保証するための技術に関する。

【背景技術】

【0002】

近年、専用コアネットワークをサポートするための改善が 3 G P P (3rd Generation Partnership Project) によって研究されている。

40

【0003】

専用コアネットワークは、例えば、特定のタイプの加入者 (つまり、特定のタイプの U E) が、その U E を専用にサービスする M M E (Mobility Management Entity) / S G S N (Serving GPRS (General Packet Radio Service) Support Node) へリダイレクトされることを意味する。専用コアネットワークは、また、「特定コアネットワーク (Specific Core Network)」又は「オーバーレイコアネットワーク (Overlay Core Network)」と呼ばれることがある。

【0004】

非特許文献 1 は、専用コアネットワークを実現するために最も促進するメッセージフロー

50

を開示している。このメッセージフローでは、UEがアタッチ要求メッセージ（Attach Request message）を基地局（eNB：evolved Node B）を介して新しいMMEへ送信するとき（つまり、IMSI（International Mobile Subscriber Identity）アタッチの場合には）、その新しいMMEは、他の特定のMMEを用いるための情報をHSS（Home Subscriber Server）から取得する。そして、その新しいMMEは、基地局に対して、アタッチ要求メッセージを他の特定のMMEへリダイレクトするように指示する。そのリダイレクトの際には、基地局は、その特定のMMEに対してアタッチ手順（Attach procedure）を再び実行する。

【0005】

非特許文献2も、非特許文献1に開示されているのと同様のメッセージフローを開示している。

【先行技術文献】

【非特許文献】

【0006】

【文献】TSG SA WG2 #99 S2-133304, "Addition of Subscription Information for Selecting a Specific Network", 2013-09, pp. 4

SA WG2 #100 S2-133910, "23.401 CR2606R3: Addition of Subscription Information for Selecting a Specific Network", 2013-11, pp. 7 and 9

TSG SA WG2 #100 S2-133909, "Discussion on Core Network Type Selection based on the Subscription Information", 2013-11

【発明の概要】

【発明が解決しようとする課題】

【0007】

しかしながら、本出願の発明者等は、非特許文献1、2に開示されているメッセージフローが専用コアネットワークをサポートする際の効率を下げるという問題点があることを解明した。

【0008】

具体的には、アタッチ手順を再実行する際に、上記特定のMMEは、上記UEがアタッチを試みた異なるMMEによって既に実行された、AKA（Authentication and Key Agreement）手順及びNAS（Non-Access Stratum）SMC（Security Mode Command）手順を重複して実行する。このため、上記特定のMMEに対する過負荷だけでなく、冗長なAKA／NAS SMC手順に関係しているデバイス群／ノード群及びそれらの間のすべてのインターフェイスに対するシグナリングの過負荷が引き起こされる。

【0009】

さらに、非特許文献2、3は、それぞれ、GUTI（Globally Unique Temporary Identity）アタッチの他のメッセージフローを開示している。この他のメッセージフローでは、上記特定のMMEは、セキュリティコンテキスト（security context）を取得するために、上記GUTIによって参照される、或るMMEに連絡する。

【0010】

しかしながら、このメッセージフローにおいても、上記のシグナリングの過負荷及び上記特定のMMEに対する過負荷が引き起こされる。これは、上記GUTIがタイマの満了後に上記セキュリティコンテキストを削除した可能性のある上記旧MME（old MME）を示しているに過ぎないため、結局、上記特定のMMEは冗長な上記AKA／NAS SMC手順を実行することになるからである。

【0011】

ここで、これらの問題点の詳細は後述の実施形態において詳しく説明する。

【0012】

このように、本発明の典型的な目的は、専用コアネットワークをより効率的にサポートするための解決手段を提供することである。

【課題を解決するための手段】

【0013】

上記の目的を達成するために、本発明の第1の態様のネットワークシステムは、第1ノードと、第2ノードとを含んでいる。上記第1ノードは、最初にネットワークに対するアタッチを試みるUE（User Equipment）との間で無線基地局（radio base station）を介してセキュアなコネクションを確立する。上記UEは、上記無線基地局を介して上記第1ノードから上記第2ノードへリダイレクトされる。そのリダイレクトの際に、上記第1ノードは、上記第1ノード自体についての情報を、上記無線基地局を介して上記第2ノードへ送る。上記第2ノードは、上記UEとの間の上記コネクションを確立するために必要なセキュリティコンテキストを上記第1ノードから取得するために上記情報を用いる。

【0014】

さらに、本発明の第2の態様によれば、ネットワークシステムについての制御方法が提供される。該ネットワークシステムは、第1ノードと、第2ノードとを含んでいる。上記第1ノードは、最初にネットワークに対するアタッチを試みるUEとの間で無線基地局を介してセキュアなコネクションを確立する。上記UEは、上記無線基地局を介して上記第1ノードから上記第2ノードへリダイレクトされる。この方法は、そのリダイレクトの際に、上記第1ノード自体についての情報を、上記第1ノードから上記無線基地局を介して上記第2ノードへ送ること、及び、上記UEとの間の上記コネクションを確立するために必要なセキュリティコンテキストを上記第1ノードから取得するために、上記第2ノードが上記情報を用いることを含んでいる。

【0015】

さらに、本発明の第3の態様のネットワークシステムは、第1ノードと、第2ノードとを含んでいる。上記第1ノードは、最初にネットワークに対するアタッチを試みるUEからアタッチ要求（attach request）を、無線基地局を介して受け取る。上記アタッチ要求は、上記無線基地局を介して上記第1ノードから上記第2ノードへリダイレクトされる。上記アタッチ要求の受信に際して、上記第1ノードは、上記無線基地局を介した上記UEとの間のセキュアなコネクションの確立をスキップする（飛ばす）。上記リダイレクトの際に、上記第1ノードは、上記UEが上記第2ノードへリダイレクトされるべきUEであることを示す署名情報（subscription information）を、上記無線基地局を介して上記第2ノードへ送る。上記署名情報の受信に応じて、上記第2ノードは、上記UEとの間の上記セキュアなコネクションを確立する。

【0016】

さらに、本発明の第4の態様によれば、ネットワークシステムについての制御方法が提供される。該ネットワークシステムは、第1ノードと、第2ノードとを含んでいる。上記第1ノードは、最初にネットワークに対するアタッチを試みるUEとの間で無線基地局を介してセキュアなコネクションを確立する。上記UEは、上記無線基地局を介して上記第1ノードから上記第2ノードへリダイレクトされる。この方法は、上記第1ノードが上記アタッチ要求を受信したときに上記無線基地局を介した上記UEとの間のセキュアなコネクションの確立をスキップすること、上記リダイレクトに際して、上記第1ノードが、上記UEが上記第2ノードへリダイレクトされるべきUEであることを示す署名情報（subscription information）を、上記無線基地局を介して上記第2ノードへ送ること、及び、上記署名情報の受信に応じて、上記第2ノードが、上記UEとの間の上記セキュアなコネクションを確立することを含んでいる。

【0017】

さらに、本発明の第5の態様のネットワークシステムは、第1ノードと、第2ノードと、第3ノードとを含んでいる。上記第1ノードは、無線基地局を介したUEとの間のセキュアなコネクションを、上記UEがあらかじめネットワークへアタッチしたときに確立し、上記UEに対して一時的な身元証明書（temporary identity）を割り当てる。上記第2ノードは、上記無線基地局を介して上記UEから、上記一時的な身元証明書を含むアタッチ要求を受け取る。上記第3ノードは、上記無線基地局を介して上記第2ノードから上記アタッチ要求がリダイレクトされる。上記第2ノードは、上記UEとの間の上記コネクシ

10

20

30

40

50

ョンの確立に必要なセキュリティコンテキストを上記第1ノードから取得し、上記リダイレクトに際して、上記第2ノード自身についての情報を、上記無線基地局を介して上記第3ノードへ送る。上記第3ノードは、上記第2ノードから上記セキュリティコンテキストを取得するために、上記情報を用いる。

【0018】

さらに、本発明の第6の態様によれば、ネットワークシステムについての制御方法が提供される。該ネットワークシステムは、第1ノードと、第2ノードと、第3ノードとを含んでいる。上記第1ノードは、無線基地局を介したUEとの間のセキュアなコネクションを、上記UEがあらかじめネットワークへアタッチしたときに確立し、上記UEに対して一時的な身元証明書（temporary identity）を割り当てる。上記第2ノードは、上記無線基地局を介して上記UEから、上記一時的な身元証明書を含むアタッチ要求を受け取る。上記第3ノードは、上記無線基地局を介して上記第2ノードから上記アタッチ要求がリダイレクトされる。この方法は、上記第2ノードが、上記UEとの間の上記コネクションの確立に必要なセキュリティコンテキストを上記第1ノードから取得すること、上記第2ノードが、上記リダイレクトに際して、上記第2ノード自身についての情報を、上記無線基地局を介して上記第3ノードへ送ること、及び、上記第3ノードが、上記第2ノードから上記セキュリティコンテキストを取得するために、上記情報を用いることを含んでいる。

【0019】

さらに、本発明の第7の態様のネットワークシステムは、第1ノードと、第2ノードと、第3ノードとを含んでいる。上記第1ノードは、無線基地局を介したUEとの間のセキュアなコネクションを、上記UEがあらかじめネットワークへアタッチしたときに確立し、上記UEに対して一時的な身元証明書（temporary identity）を割り当てる。上記第2ノードは、上記無線基地局を介して上記UEから、上記一時的な身元証明書を含むアタッチ要求を受け取る。上記第3ノードは、上記無線基地局を介して上記第2ノードから上記アタッチ要求がリダイレクトされる。上記第2ノードは、上記UEとの間の上記コネクションの確立に必要なセキュリティコンテキストを上記第1ノードから取得し、上記リダイレクトに際して、上記セキュリティコンテキストを、上記無線基地局を介して上記第3ノードへ送信する。

【0020】

さらに、本発明の第9の態様によれば、ネットワークシステムについての制御方法が提供される。該ネットワークシステムは、第1ノードと、第2ノードと、第3ノードとを含んでいる。上記第1ノードは、無線基地局を介したUEとの間のセキュアなコネクションを、上記UEがあらかじめネットワークへアタッチしたときに確立し、上記UEに対して一時的な身元証明書（temporary identity）を割り当てる。上記第2ノードは、上記無線基地局を介して上記UEから、上記一時的な身元証明書を含むアタッチ要求を受け取る。上記第3ノードは、上記無線基地局を介して上記第2ノードから上記アタッチ要求がリダイレクトされる。この方法は、上記第2ノードが、上記UEとの間の上記コネクションの確立に必要なセキュリティコンテキストを上記第1ノードから取得すること、及び、上記第2ノードが、上記リダイレクトに際して、上記セキュリティコンテキストを、上記無線基地局を介して上記第3ノードへ送信することを含む。

【0021】

さらに、本発明の第9の態様のネットワークシステムは、第1ノードと、第2ノードと、第3ノードとを含んでいる。上記第1ノードは、無線基地局を介したUEとの間のセキュアなコネクションを、上記UEがあらかじめネットワークへアタッチしたときに確立し、上記UEに対して一時的な身元証明書（temporary identity）を割り当てる。上記第2ノードは、上記無線基地局を介して上記UEから、上記一時的な身元証明書を含むアタッチ要求を受け取る。上記第3ノードは、上記無線基地局を介して上記第2ノードから上記アタッチ要求がリダイレクトされる。上記第1ノードは、上記第3ノードからの身分証明書要求（identification request）を受け取るまでの間、上記UEとの間の上記セキュアなコネクションに必要なセキュリティコンテキストを保持し続ける。上記第3ノードは、

上記リダイレクトに際して、上記第1ノードから上記セキュリティコンテキストを取得するために、上記身分証明書要求を上記第1ノードへ送る。

【0022】

さらに、本発明の第10の態様によれば、ネットワークシステムについての制御方法が提供される。該ネットワークシステムは、第1ノードと、第2ノードと、第3ノードとを含んでいる。上記第1ノードは、無線基地局を介したUEとの間のセキュアな接続を、上記UEがあらかじめネットワークへアタッチしたときに確立し、上記UEに対して一時的な身元証明書(temporary identity)を割り当てる。上記第2ノードは、上記無線基地局を介して上記UEから、上記一時的な身元証明書を含むアタッチ要求を受け取る。上記第3ノードは、上記無線基地局を介して上記第2ノードから上記アタッチ要求がリダイレクトされる。この方法は、上記第1ノードが、上記第3ノードからの身分証明書要求(identification request)を受け取るまでの間、上記UEとの間の上記セキュアな接続に必要なセキュリティコンテキストを保持し続けること、及び、上記第3ノードが、上記リダイレクトに際して、上記第1ノードから上記セキュリティコンテキストを取得するために、上記身分証明書要求を上記第1ノードへ送ることを含んでいる。

10

【0023】

さらに、本発明の第11の態様のコアネットワークシステムは、複数のコアネットワークノードと、サーバとを含んでいる。このシステムにおいて、UEは、メッセージを、無線基地局を介して第1コアネットワークノードへ送る。上記UEは、上記サーバによって与えられた署名情報(subscription information)に基づいて、上記第1コアネットワークノードから第2コアネットワークノードへリダイレクトされる。上記第1コアネットワークノードは、上記リダイレクトについての情報を含む第1メッセージを、上記無線基地局へ送る。上記無線基地局は、上記情報を含む第2メッセージを、上記第2コアネットワークノードへ送る。

20

【0024】

さらに、本発明の第12の態様によれば、複数のコアネットワークノードとサーバとを含むコアネットワークシステムのための方法が提供される。この方法は、UE(User Equipment)がメッセージを無線基地局を介して第1コアネットワークノードへ送るステップと、上記UEが、上記サーバによって与えられた署名情報(subscription information)に基づいて、上記第1コアネットワークノードから第2コアネットワークノードへリダイレクトされるステップと、上記第1コアネットワークノードが、上記リダイレクトについての情報を含む第1メッセージを、上記無線基地局へ送るステップと、上記無線基地局が、上記情報を含む第2メッセージを、上記第2コアネットワークノードへ送るステップと、を含んでいる。

30

【0025】

さらに、本発明の第13の態様のUEは、メッセージを無線基地局を介して第1コアネットワークノードへ送る手段を含んでいる。上記UEは、上記サーバによって与えられた署名情報(subscription information)に基づいて、上記第1コアネットワークノードから第2コアネットワークノードへリダイレクトされる。上記リダイレクトにおいて、上記第1コアネットワークノードが、上記リダイレクトについての情報を含む第1メッセージを、上記無線基地局へ送り、上記無線基地局が、上記情報を含む第2メッセージを、上記第2コアネットワークノードへ送る。

40

【0026】

さらに、本発明の第14の態様によれば、UEについての方法が提供される。この方法は、上記UEが、メッセージを無線基地局を介して第1コアネットワークノードへ送るステップと、上記UEが、上記サーバによって与えられた署名情報(subscription information)に基づいて、上記第1コアネットワークノードから第2コアネットワークノードへリダイレクトされるステップと、を含んでいる。上記リダイレクトにおいて、上記第1コアネットワークノードが、上記リダイレクトについての情報を含む第1メッセージを、上記無線基地局へ送り、上記無線基地局が、上記情報を含む第2メッセージを、上記第2コ

50

アネットワークノードへ送る。

【発明の効果】

【0027】

本発明によれば、上記の複数の問題のうちの少なくとも1つを解決すること、例えば、専用コアネットワークをより効率的にサポートするための解決手段を提供することが可能となる。

【図面の簡単な説明】

【0028】

【図1】本発明の第1実施形態のネットワークシステムの構成例を示すブロック図である。

【図2】第1実施形態のネットワークシステムの動作の第1例を示すシーケンス図である。

【図3】第1実施形態のネットワークシステム動作の第2例を示すシーケンス図である。

【図4】本発明の第2実施形態のネットワークシステムの動作の第1例を示すシーケンス図である。

【図5】第2実施形態のネットワークシステムの動作の第2例を示すシーケンス図である。

【図6】第2実施形態のネットワークシステムの動作の第3例を示すシーケンス図である。

【図7】典型的なIMS Iアタッチ手順における複数の問題点の説明に供するシーケンス図である。

【図8】典型的なGUTIアタッチ手順における複数の問題点の説明に供するシーケンス図である。

【発明を実施するための形態】

【0029】

以下では、本発明の複数の実施形態を、添付の複数の図面を参照して、説明する。

【0030】

<第1実施形態>

図1に示すように、第1実施形態のネットワークシステムは、例えば、MME30と、MME40とを含んでいる。MME30は、UE10が無線基地局としてのeNB20を介して最初にアタッチするMMEであり、このため、以下では、「新MME (New MME)」と呼ばれることがある。一方、MME40は、署名 (subscription) に応じてUE10を専用にサービスするMMEであり、且つ、UE10がMME30からリダイレクトされるMMEであり、このため、以下では、「専用MME (Dedicated MME)」又は「DMME」と呼ばれる。ここで、MME40は、上記専用コアネットワークが「特定のコアネットワーク (Specific Core Network)」と呼ばれることに合わせて、「特定のMME (Specific MME)」と呼ぶこともできる。必要ならば、MME30及びMME40は、それぞれ、HSS50から、UE10についての署名情報 (subscription information)、及び、UE10を認証するために必要な情報等を取得することができる。新MME30は、また、S-GW (Serving Gateway) 及び／又はP-GW (PDN (Public Data Network) Gateway) に接続される。同様に、専用MME40も、専用S-GW及び／又は専用P-GWに接続される。

【0031】

概して、第1実施形態は、E-UTRAN (Evolved Universal Terrestrial Radio Access Network) におけるIMS Iアタッチを扱い、特に、新MME30が、eNB20から受け取ったアタッチ要求メッセージ (Attach Request message) を、HSS50から取得したUE10についての署名情報に基づいて、DMME40へリダイレクトするケースを扱う。

【0032】

次に、第1実施形態の動作例を記述する前に、図7を参照して、非特許文献1, 2に開示されている典型的なIMS Iアタッチ手順における問題点を、最初に明らかにする。それから、複数の動作例として、これらの問題点を解決するための複数の解決策を説明する。該複数の解決策は、図2に示されたオプション1及び図3に示されたオプション2を含む。

【0033】

明らかにされた問題点：

図 7 に示すように、典型的な IMSI アタッチ手順において、UE 110 は、その IMSI を含むアタッチ要求メッセージを、eNB 120 へ送り（ステップ S101）、eNB 120 は、上記アタッチ要求メッセージを新 MME 130 へ転送する（ステップ S102）。

【0034】

上記アタッチ要求メッセージを受け取ると、新 MME 130 は、認証データ要求メッセージ（Authentication data request message）を HSS 150 へ送り、それに対する応答として、AV 群（Authentication Vectors）を含む認証データ応答メッセージ（Authentication data response message）を受け取る（ステップ S103）。それから、新 MME 130 は、UE 110 と協働して、AKA 手順及び NAS SMC 手順を実行する（ステップ S104）。結果として、UE 110 及び新 MME 130 は、それぞれ、Kasme（Key for access security management entity）及び NAS キー群（NAS keys）を共有することができ、この結果、セキュアなコネクションが UE 110 と新 MME 130 の間に確立される（ステップ S105）。

【0035】

その後に、新 MME 130 は、更新位置要求メッセージ（Update Location Request message）を HSS 150 へ送り、これに対する応答として、更新位置応答メッセージ（Update Location Response message）を受け取る（ステップ S106）。更新位置応答メッセージは、上記 IMSI 及び上記署名情報／データを含んでいる。さらに、上記署名情報は、専用 MME 140 についての情報（以下では、「DMME 情報」と呼ばれることがある）を含んでいる。

【0036】

それから、新 MME 130 は、上記 UE 110 がリダイレクトされるべき専用 MME 140 を、上記 DMME 情報に基づいて選択し（ステップ S107）、リダイレクトメッセージ（Redirect message）を eNB 120 へ送る（ステップ S108）。該リダイレクトメッセージを受け取ると、eNB 120 は、上記アタッチ要求メッセージを専用 MME 140 へ転送する（ステップ S109）。

【0037】

しかしながら、このとき、以下の複数の問題点が生じる。

（a）上記アタッチ要求メッセージは保護されていないので、専用 MME 140 は、UE 110 に対する AKA 手順を開始する。

（b）上記（a）に起因して、専用 MME 140 は、認証データ要求メッセージを HSS 150 へ送ると共に認証データ応答メッセージを HSS 150 から受信し、更新位置要求メッセージを HSS 150 へ送ると共に更新位置応答メッセージを HSS 150 から受信し、UE 110 と協力して AKA 手順及び NAS SMC 手順を実行する。

（c）上記（a）及び（b）に起因して、鍵の計算（key computation）に関する専用 MME 140 に対する過負荷だけではなく、HSS 150、専用 MME 140、eNB 120、UE 110、及びそれらのすべてのインターフェイスに対するシグナリングの過負荷が引き起こされる。

【0038】

解決策：

（オプション 1）

図 2 は、オプション 1 についてのシーケンス図である。ステップ S1 からステップ S7 は、上記の図 7 のステップ S101 からステップ S107 と同じように実行される。

【0039】

一方で、上記リダイレクトの際に、新 MME 30 は、新 MME 30 自体の情報（以下では、そのような情報を「MME 情報」と呼ぶことがある）を含むリダイレクトメッセージを eNB 20 へ送信する（ステップ S8）。例えば、上記 MME 情報は、ID（identification, identity）、FQDN（完全修飾ドメイン名：Fully Qualified Domain Name）、

10

20

30

40

50

又は、新MME 30に割り当てられたIP (Internet Protocol) アドレスを含んでいる。そして、eNB 20は、アタッチ要求メッセージに含まれた状態で、上記MME 情報を専用MME 40へ転送する(ステップS 9)。

【0040】

専用MME 40は、既にUE 10と新MME 30との間で確立されているセキュアなコネクションについてのセキュリティコンテキストを新MME 30から取得するために、受信したMME 情報を用いる。具体的には、専用MME 40は、身分証明書要求 (identification request) メッセージを新MME 30へ送信し(ステップS 10)、これに対する応答として、UE コンテキストを含む身分証明書応答 (Identification Response) メッセージを受信する(ステップS 11)。UE コンテキストは、上記AV 群及びすべてのセキュリティコンテキストを含んでいる。そして、専用MME 40は、受信したUE コンテキストから、上記Kasme 及び上記NAS キー群を抽出する(ステップS 12)。

10

【0041】

その後、3GPP TS 23.401のセクション5.3.2.1に記載されているメッセージ5b 及びそれに続く複数のメッセージシーケンスが続く。

【0042】

このオプション1によれば、専用MME 40は、専用MME 40が新MME 30から必要なセキュリティコンテキストを取得できるように、上記MME 情報について示される。それゆえ、上記の典型的なIMS I アタッチ手順と異なり、専用MME 40は、AKA 手順及びNAS SMC 手順を実行する必要がない。このため、上記の典型的なIMS I アタッチ手順と比較して、鍵の計算 (key computation) に関する専用MME に対する過負荷だけでなく、シグナリングの過負荷を劇的に減らすことができる。さらに、現存の複数のメッセージシーケンスを再利用することができる(後述するように、身分証明書要求 (identification request) メッセージ及び身分証明書応答 (Identification Response) メッセージも現存するメッセージである) ので、上記移動通信システムに対するインパクトを最小化することができる。

20

【0043】

さらに、上記ステップS 11で、新MME 30は、身分証明書応答メッセージの中に、UE 10が専用MME 40へリダイレクトされるべきものとして既に認証されていることを示す、認証表示 (Authentication Indication) を含めてよい。この場合、専用MME 40は、UE 10を認証する目的でHSS 50と接触する必要はなく、この結果として、シグナリングの過負荷をさらに減らすことができる。

30

【0044】

(オプション2)

図3は、オプション2のシーケンス図を示す。ステップS 21 及びステップS 22 は、図2のステップS 1 及びステップS 2 と同様に実行される。

【0045】

一方で、上記アタッチ要求メッセージを受信する際に、新MME 30は、最初に、上記DMME 情報を含む上記署名情報 (subscription information) をHSS 50から取得する(ステップS 23a)。

40

【0046】

上記の通り、上記DMME 情報は、UE 10が専用MME 40へリダイレクトされるべきであることを示している。それゆえ、新MME 30は、UE 10との間でセキュアコネクションを確立することをスキップすることができる。具体的には、新MME 30は、上記AKA 手順、上記NAS SMC 手順、及びNAS 鍵の計算等を実行しない。

【0047】

それから、新MME 30は、上記DMME 情報に基づいて、専用MME 40を選択し(ステップS 24)、署名情報を含んでいるリダイレクトメッセージ(これはDMME 情報も含んでいる)をeNB 20へ送信する(ステップS 25)。それから、eNB 20は、アタッチ要求メッセージに含まれた状態で上記署名情報を専用MME 40へ転送する(ステ

50

ップ S 2 6)。

【0048】

上記署名情報（すなわち、DMME 情報）の受信に応答して、専用 MME 40 は、新 MME 30 の代わりとして、eNB 20 を介して UE 10 との間でセキュアコネクションを確立する。具体的には、専用 MME 40 は、認証データ要求メッセージを HSS 50 へ送り、それに対する応答として、上記 AV 群を含む認証データ応答メッセージを受信する（ステップ S 2 7）。そして、専用 MME 40 は、UE 10 と効力して AKA 手順及び NAS SMC 手順を実行する（ステップ S 2 8）。結果として、UE 10 及び専用 MME 40 は、それぞれ、Kasme 及び NAS 鍵群を共有することができ、この結果、UE 10 と専用 MME 40 との間で eNB 20 を介してセキュアなコネクションが確立される（ステップ S 2 9）。

10

【0049】

その後、3GPP TS 23.401 のセクション 5.3.2.1 に記載されているメッセージ 5b 及びそれに続く複数のメッセージシーケンスが続く。

【0050】

オプション 2 によれば、図 2 及び図 3 に示されているシーケンスを比較することで理解されるように、上記オプション 1 と比べて、シグナリング量を減らすことができる。さらに、新 MME 30 はセキュアなコネクションを確立することをスキップするので、新 MME 30 に対する過負荷を減らすこともできる。

【0051】

さらに、上記ステップ S 23a の代わりとして、新 MME 30 において、DMME 情報が事前に構成されてもよい（ステップ S 23b）。この場合、新 MME 30 は、UE 10 から最初のアタッチ要求を受信したときに、HSS 50 から署名情報を取得することもスキップすることができ、結果として、シグナリング量をさらに減らすことができる。

20

【0052】

さらに、上記ステップ S 23a で、新 MME 30 は、さらに、HSS 50 から上記 AV 群を取得してもよい。上記 AV 群は、上記ステップ S 25 で示されたリダイレクトメッセージ及びステップ S 26 で示されたアタッチ要求メッセージと一緒に、eNB 20 を介して専用 MME 40 へ転送されることができる。この場合、専用 MME 40 は、上記ステップ S 27 に示された、HSS 50 から AV 群を取得することをスキップすることができ、この結果、シグナリング量をさらに減らすことができる。

30

【0053】

<第 2 実施形態>

図 4 に示すように、第 2 実施形態のネットワークシステムは、上記の MME 30 及び MME 40 に加えて、MME 60 をさらに含んでいる。MME 60 は、UE 10 が前にアタッチした MME であり、このため、以下では、「旧 MME (Old MME)」と呼ばれることがある。必要であれば、旧 MME 60 は、上記署名情報、DMME 情報、上記 AV 群等を、HSS 50 から取得することもできる。ここで、UE 10 は前に SGSN（つまり、「旧 SGSN」）へアタッチするケースもある。このケースであっても、旧 MME についての以下の記述は、旧 SGSN についての記述へ同様に適用することができる。

40

【0054】

概して、第 2 実施形態は、E-UTRAN (Evolved Universal Terrestrial Radio Access Network) における IMSI アタッチを扱い、特に、新 MME 30 が、eNB 20 から受け取ったアタッチ要求メッセージ (Attach Request message) を、旧 MME 60 から取得した上記 DMME 情報に基づいて、DMME 40 へリダイレクトするケースを扱う。

【0055】

次に、第 2 実施形態の動作例を記述する前に、図 8 を参照して、非特許文献 2, 3 に開示されている典型的な GUTI アタッチ手順における問題点を、最初に明らかにする。それから、複数の動作例として、これらの問題点を解決するための複数の解決策を説明する。

50

該複数の解決策は、図 4 に示されたオプション 1、図 5 に示されたオプション 2、及び、図 6 に示されたオプション 3 を含む。

【0056】

明らかにされた問題点：

図 8 において点線で示されるように、UE 110 は前に旧 MME 160 へアタッチしており、旧 MME 160 が UE 110 へ GUTI を割り当てており、この結果、UE 110 が GUTI を取得しているものとする。

【0057】

典型的な GUTI アタッチ手順において、UE 110 は、GUTI を含むアタッチ要求メッセージを eNB 120 へ送信し（ステップ S201）、eNB 120 は新 MME 130 へアタッチ要求メッセージを転送する（ステップ S202）。

10

【0058】

アタッチ要求メッセージを受信すると、新 MME 130 は、GUTI を含む身分証明書要求メッセージ及び完了アタッチ要求（complete Attach Request）メッセージを、旧 MME 160 へ送信し（ステップ S203）、これに対する応答として、UE 110 の IMSI と MM（移動性管理：Mobility Management）コンテキストとを含む身分証明書応答メッセージを受信する（ステップ S204）。

【0059】

それから、新 MME 130 は、専用 MME 140 を選択し（ステップ S205）、eNB 120 へリダイレクトメッセージを送信する（ステップ S206）。リダイレクトメッセージを受信すると、eNB 120 は、専用 MME 140 へ上記アタッチ要求メッセージを転送する（ステップ S207）。

20

【0060】

しかしながら、旧 MME 160 は、予め決められたタイマが満了した後に、UE コンテキスト（つまり、セキュリティコンテキスト）を削除するかもしれない。さらに、GUTI は、旧 MME 160 を単に示しているだけである。それゆえ、専用 MME 140 は、旧 MME 160 から上記 AV 群及びセキュリティコンテキストを受信することに失敗し、このため、AKA 手順を開始する。

【0061】

これにより、典型的な IMSI アタッチ手順と同様に、以下の複数の問題点が生じる。すなわち、HSS 150、専用 MME 140、eNB 120、UE 110、及びそれらのインターフェイスに対する、シグナリングの過負荷、及び、鍵の計算に関する専用 MME 140 に対する過負荷である。

30

【0062】

解決策：

（オプション 1）

図 4 は、オプション 1 についてのシーケンス図である。ステップ S31 からステップ S35 のプロセスは、上記の図 8 のステップ S201 からステップ S105 と同じように実行される。

【0063】

一方で、リダイレクトの際に、新 MME 30 は、新 MME 30 自身についての情報（つまり、MME 情報）を含むリダイレクトメッセージを eNB 20 へ送信する（ステップ S36）。それから、eNB 20 は、上記 MME 情報をアタッチ要求メッセージに含められた状態で専用 MME 40 へ転送する（ステップ S37）。

40

【0064】

専用 MME 40 は、上記ステップ S34 で旧 MME 60 から新 MME 30 によって既に取得されている上記セキュリティコンテキストを新 MME 30 から取得するために、受信した MME 情報を用いる。具体的には、専用 MME 40 は、身分証明書要求メッセージを新 MME 30 へ送信し（ステップ S38）、これに対する応答として、UE コンテキストを含む身分証明書応答メッセージを受信する（ステップ S39）。上記の通り、上記 UE コ

50

ンテキストは、A V 群及びすべてのセキュリティコンテキストを含んでいる。それから、専用MME 40は、受信したUE コンテキストから、上記K a s m e 及びN A S 鍵群を抽出する（ステップS 40）。

【0065】

その後、3 G P P T S 23.401のセクション5.3.2.1に記載されているメッセージ5 b 及びそれに続く複数のメッセージシーケンスが続く。

【0066】

このオプション1により、専用MME 40は、MME 情報について示されることで、専用MME 40は、新MME 40から必要なセキュリティコンテキストを取得することができる。それゆえ、典型的なG U T I と異なり、専用MME 40は、旧MME 60から上記A V 群及びセキュリティコンテキストを取得する目的で、旧MME 60へ接触する必要がなく、これにより、旧MME 60から上記セキュリティコンテキストを取得することに失敗した場合でも、A K A 手順を開始する必要がない。このため、典型的なG U T I と比較して、鍵の計算に関する専用MME に対する過負荷だけではなく、シグナリングの過負荷を劇的に減らすことができる。さらに、現存の複数のメッセージシーケンスを再利用することができるので、上記移動通信システムに対するインパクトを最小化することができる。

【0067】

さらに、上記ステップS 39において、新MME 30は、UE 10が専用MME 40へリダイレクトされるべきものとして既に認証されていることを示す、認証表示（Authentication Indication）を、上記身分証明書要求メッセージの中に含めてもよい。この場合、専用MME 40は、UE 10を認証する目的でH S S 50と接触する必要はなく、この結果として、シグナリングの過負荷をさらに減らすことができる。

【0068】

（オプション2）

図5は、オプション2のシーケンス図を示す。ステップS 41からステップS 45は、図4のステップS 31からステップS 35と同様に実行される。

【0069】

一方で、リダイレクトの際に、新MME 30は、上記UE コンテキストを含むリダイレクトメッセージをe N B 20へ送信する（ステップS 46）。それから、e N B 20は、上記UE コンテキストをアタッチ要求メッセージに含められた状態で、専用MME 40へ転送する（ステップS 47）。上記の通り、UE コンテキストは、上記A V 群及びすべてのセキュリティコンテキストを含んでいる。

【0070】

それから、専用MME 40は、受信したUE コンテキストから、上記K a s m e 及びN A S 鍵群を抽出する（ステップS 48）。

【0071】

その後、3 G P P T S 23.401のセクション5.3.2.1に記載されているメッセージ5 b 及びそれに続く複数のメッセージシーケンスが続く。

【0072】

このオプション2によれば、専用MME 40は、UE コンテキストを取得するために、いかなるMME とも接触する必要がない。それゆえ、上記オプション1に比べて、シグナリング量を減らすことができ、また、専用MME 40に対する過負荷も減らすことができる。

【0073】

さらに、このオプション2は、上記ステップS 43で上記アタッチ要求メッセージについてのインテグリティチェック（integrity check）が為されたことを旧MME 60が記憶しているように、最適化されてもよい。この場合、専用MME 40は、上記ステップS 47で再度インテグリティチェックを行う必要がなく、この結果として、専用MME 40に対する過負荷をさらに減らすことができる。

【0074】

（オプション3）

図6は、オプション3についてのシーケンス図である。ステップS51からステップS55は、上記の図4のステップS31からステップS35と同じように実行される。

【0075】

一方で、このオプション3において、旧MME60は、加入者のための上記DMMEとして仕えるので、旧MME60は、専用MMEから第2の身分証明書要求メッセージを受信するまでのしばらくの間、上記セキュリティコンテキストを除去することなく保持する。

【0076】

リダイレクトの際に、新MME30は、リダイレクトメッセージをeNB20へ送信する(ステップS56)。それから、eNB20は、上記アタッチ要求メッセージを専用MME40へ転送する(ステップS57)。

【0077】

上記アタッチ要求メッセージを受信すると、専用MME40は、GUTIを含む身分証明書要求メッセージ及び完了アタッチ要求メッセージを、旧MME160へ送信する(ステップS58)。

【0078】

ここで、上記第2の身分証明書要求メッセージが受信されるので、旧MME60は、上記保持していたMMコンテキスト(セキュリティコンテキスト)を含む身分証明書応答メッセージを専用MME40へ送り返す(ステップS59)。

【0079】

それから、専用MME40は、受信したMMコンテキストから、上記Kasme及びNAS鍵群を抽出する(ステップS60)。

【0080】

その後、3GPP TS23.401のセクション5.3.2.1に記載されているメッセージ5b及びそれに続く複数のメッセージシーケンスが続く。

【0081】

このオプション3によれば、典型的なGUTIと同様に、専用MME40は、GUTIを使うことだけによって、必要なセキュリティコンテキストを旧MME60から取得することができ、これにより、AKA手順を開始する必要がない。それゆえ、鍵の計算に関する専用MMEに対する過負荷だけではなく、シグナリングの過負荷を劇的に減らすことができる。さらに、専用MMEは、GUTIによって示されたMMEにだけ接触すればよいので、言い換えれば、専用MMEだけが上記現存の複数のメッセージシーケンスを実行するので、専用MMEに対するインパクトを最小化することができる。

【0082】

さらに、好ましくは、新MME30は、上記ステップS56及びステップS57で示したリダイレクトメッセージ及びアタッチ要求メッセージによって、専用MME40に対して、AVが取得されていないことを知らせ、旧MME60は、上記ステップS59で示した第2の身分証明書要求メッセージにおいて、有効なAV群だけを専用MME40に対して知らせる。これにより、専用MME40は、UE10との間の通信を行うために、上記有効なAV群を用いることができる。ここで、上記有効なAV群の代わりとして又はこれに追加して、旧MME60は、他の追加的な情報を専用MME40に対して知らせてもよい。

【0083】

さらに、このオプション3は、上記ステップS53で上記アタッチ要求メッセージについてのインテグリティチェックが為されたことを旧MME60が記憶しているように、最適化されてもよい。この場合、専用MME40は、上記ステップS57で再度インテグリティチェックを行う必要がなく、また、旧MME60も上記ステップS58で再度インテグリティチェックを行う必要がなく、この結果として、専用MME40及び旧MME60に対する過負荷をさらに減らすことができる。

【0084】

ここで、本実施形態の以上の説明ではE-UTRANを例にとることにより説明を行ったが、本発明は、UTRANにおける、IMS Iアタッチ及びP-TMSI (パケット-T

10

20

30

40

50

M S I (Temporary Mobile Subscriber Identity)) アタッチに対して適用することもできる。そのメカニズムは、例えば専用MME / S G S N情報を伝えるためにメッセージが交換されることを除いて、基本的にはE - U T R A Nにおけるアタッチと同じである。

【0085】

上記実施形態がU T R A N及びG E R A N (G S M (登録商標) (Global System for Mobile communications) E D G E (Enhanced Data GSM (登録商標) Environment) R A N) を参照する場合には、以下の置き換えを行う必要がある。

- ・ M M E を S G S N で置き換えること。
- ・ D M M E を D S G S N で置き換えること。
- ・ e N B を B T S (Base Transceiver Station) / B S C (Base Station Controller) で置き換えること。
- ・ H S S を H L R (Home Location Register) / H S S で置き換えること。
- ・ G U T I を P - T M S I で置き換えること。

【0086】

さらに、図示は省略されているが、新MME 30、専用MME 40、及び旧MME 60は、それぞれ、1つ又は複数の通信機、及び、C P U (Central Processing Unit) のようなコントローラによって、構成されてもよい。その1つ又は複数の通信機は、例えば、e N B 20を介してU E 10と通信を行い、e N B 20を介して又は介さずにMME 30、40、60との間の通信を行い、且つ、H S S 50との間の通信を行う。そのコントローラは、図示したシーケンス図に示したプロセス又はそれと同等のプロセスを実行するため

【0087】

ここで、本発明は、上記実施形態に限定されるものではなく、クレームの記述に基づいて当業者によって種々の変更が為され得ることは明らかである。

【0088】

上記の複数の実施形態の全部又は一部は、これに限定されるものではないが、以下の付記として記載されてもよい。

【0089】

(付記1)

無線基地局を介して最初にネットワークへアタッチすることを試みて、U E (User Equipment) との間でセキュアなコネクションを確立する第1ノードと、前記U E が前記無線基地局を介して前記第1ノードからリダイレクトされる第2ノードと、を具備し、前記リダイレクトの際に、前記第1ノードは、前記第1ノード自身についての情報を、前記無線基地局を介して前記第2ノードへ送信し、前記第2ノードは、前記情報を用いて、前記第1ノードから前記U E との間の前記コネクションを確立するために必要なセキュリティコンテキストを取得する、ネットワークシステム。

【0090】

(付記2)

無線基地局を介して最初にネットワークへアタッチすることを試みて、U E との間でセキュアなコネクションを確立する第1ノードと、前記U E が前記無線基地局を介して前記第1ノードからリダイレクトされる第2ノードと、を具備するネットワークシステムのための制御方法であって、上記リダイレクトの際に、前記第1ノードから前記第2ノードへ前記無線基地局を介して前記第1ノードについての情報を送信し、前記第2ノードが前記情報を用いて、前記第1ノードから前記U E との間の前記コネクションを確立するために必要なセキュリティコンテキストを取得する、制御方法。

【0091】

(付記3)

無線基地局を介して最初にネットワークへアタッチすることを試みて、UEからアタッチ要求を受信する第1ノードと、
前記アタッチ要求が前記無線基地局を介して前記第1ノードからリダイレクトされる第2ノードと、
を具備し、
前記アタッチ要求のリダイレクトの際に、前記第1ノードは、前記無線基地局を介した前記UEとの間のセキュアなコネクションの確立をスキップし、
前記リダイレクトの際に、前記第1ノードは、前記無線基地局を介して前記第2ノードへ、前記UEが前記第2ノードへリダイレクトされるものであることを示す加入者情報を送信し、
前記加入者情報の受信に応じて、前記第2ノードは、前記UEとの間で前記セキュアなコネクションを確立する、
ネットワークシステム。

【0092】

(付記4)

無線基地局を介して最初にネットワークへアタッチすることを試みて、UEからアタッチ要求を受信する第1ノードと、前記アタッチ要求が前記無線基地局を介して前記第1ノードからリダイレクトされる第2ノードと、を具備するネットワークシステムのための制御方法であって、
前記アタッチ要求のリダイレクトの際に、前記第1ノードが、前記無線基地局を介した前記UEとの間のセキュアなコネクションの確立をスキップし、
前記リダイレクトの際に、前記第1ノードが、前記無線基地局を介して前記第2ノードへ、前記UEが前記第2ノードへリダイレクトされるものであることを示す加入者情報を送信し、
前記加入者情報の受信に応じて、前記第2ノードが、前記UEとの間で前記セキュアなコネクションを確立する、
制御方法。

【0093】

(付記5)

UEが以前にネットワークへアタッチしたときに、無線基地局を介して前記UEとの間でセキュアなコネクションを確立し、前記UEに対して一時的な身元証明書(temporary identity)を割り当てる第1ノードと、
前記無線基地局を介して前記UEから前記一時的な身元証明書を含むアタッチ要求を受信する第2ノードと、
前記アタッチ要求が前記無線基地局を介して前記第2ノードからリダイレクトされる第3ノードと、
を具備し、
前記第2ノードは、前記UEとの間で前記コネクションを確立するために必要なセキュリティコンテキストを前記第1ノードから取得し、前記リダイレクトの際に、前記第2ノード自身についての情報を、前記無線基地局を介して前記第3ノードへ送信し、
前記第3ノードは、前記情報を用いて、前記第2ノードから前記セキュリティコンテキストを取得する、
ネットワークシステム。

【0094】

(付記6)

UEが以前にネットワークへアタッチしたときに、無線基地局を介して前記UEとの間でセキュアなコネクションを確立し、前記UEに対して一時的な身元証明書を割り当てる第1ノードと、前記無線基地局を介して前記UEから前記一時的な身元証明書を含むアタッチ要求を受信する第2ノードと、前記アタッチ要求が前記無線基地局を介して前記第2ノ

ードからリダイレクトされる第3ノードと、を具備するネットワークシステムのための制御方法であって、

前記第2ノードが、前記UEとの間で前記コネクションを確立するために必要なセキュリティコンテキストを前記第1ノードから取得し、

前記リダイレクトの際に、前記第2ノード自身についての情報を、前記無線基地局を介して前記第2ノードから前記第3ノードへ送信し、

前記第3ノードが、前記情報を用いて、前記第2ノードから前記セキュリティコンテキストを取得する、

制御方法。

【0095】

(付記7)

UEが以前にネットワークへアタッチしたときに、無線基地局を介して前記UEとの間でセキュアなコネクションを確立し、前記UEに対して一時的な身元証明書を割り当てる第1ノードと、

前記無線基地局を介して前記UEから前記一時的な身元証明書を含むアタッチ要求を受信する第2ノードと、

前記アタッチ要求が前記無線基地局を介して前記第2ノードからリダイレクトされる第3ノードと、

を具備し、

前記第2ノードは、前記UEとの間で前記コネクションを確立するために必要なセキュリティコンテキストを前記第1ノードから取得し、前記リダイレクトの際に、前記セキュリティコンテキストを、前記無線基地局を介して前記第3ノードへ送信する、ネットワークシステム。

【0096】

(付記8)

UEが以前にネットワークへアタッチしたときに、無線基地局を介して前記UEとの間でセキュアなコネクションを確立し、前記UEに対して一時的な身元証明書を割り当てる第1ノードと、前記無線基地局を介して前記UEから前記一時的な身元証明書を含むアタッチ要求を受信する第2ノードと、前記アタッチ要求が前記無線基地局を介して前記第2ノードからリダイレクトされる第3ノードと、を具備するネットワークシステムのための制御方法であって、

前記第2ノードが、前記UEとの間で前記コネクションを確立するために必要なセキュリティコンテキストを前記第1ノードから取得し、

前記リダイレクトの際に、前記セキュリティコンテキストを、前記無線基地局を介して前記第2ノードから前記第3ノードへ送信する、

制御装置。

【0097】

(付記9)

UEが以前にネットワークへアタッチしたときに、無線基地局を介して前記UEとの間でセキュアなコネクションを確立し、前記UEに対して一時的な身元証明書を割り当てる第1ノードと、

前記無線基地局を介して前記UEから前記一時的な身元証明書を含むアタッチ要求を受信する第2ノードと、

前記アタッチ要求が前記無線基地局を介して前記第2ノードからリダイレクトされる第3ノードと、

を具備し、

前記第1ノードは、前記第3ノードからの身分証明書要求 (identification request) を受け取るまでの間、前記UEとの間の前記セキュアなコネクションに必要なセキュリティコンテキストを保持し、

前記リダイレクトの際に、前記第3ノードは、前記身分証明書要求を前記第1ノードへ送

10

20

30

40

50

信して、前記第1ノードから前記セキュリティコンテキストを取得する、ネットワークシステム。

【0098】

(付記10)

UEが以前にネットワークへアタッチしたときに、無線基地局を介して前記UEとの間でセキュアなコネクションを確立し、前記UEに対して一時的な身元証明書を割り当てる第1ノードと、前記無線基地局を介して前記UEから前記一時的な身元証明書を含むアタッチ要求を受信する第2ノードと、前記アタッチ要求が前記無線基地局を介して前記第2ノードからリダイレクトされる第3ノードと、を具備するネットワークシステムのための制御方法であって、

前記第1ノードが、前記第3ノードからの身分証明書要求を受け取るまでの間、前記UEとの間の前記セキュアなコネクションに必要なセキュリティコンテキストを保持し、前記リダイレクトの際に、前記第3ノードが、前記身分証明書要求を前記第1ノードへ送信して、前記第1ノードから前記セキュリティコンテキストを取得する、制御方法。

【0099】

本願は、2014年5月30日に出願された日本特許出願2014-112269に基づくと共にその優先権の利益を主張し、その開示は全体として参照することによって本願に組み込まれる。

【符号の説明】

【0100】

10, 110 UE

20, 120 eNB

30, 40, 60, 130, 140, 160 MME

50, 150 HSS

10

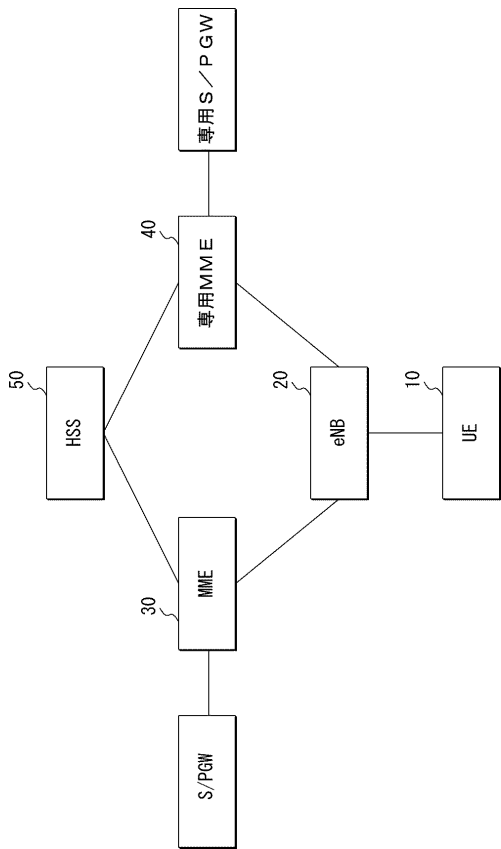
20

30

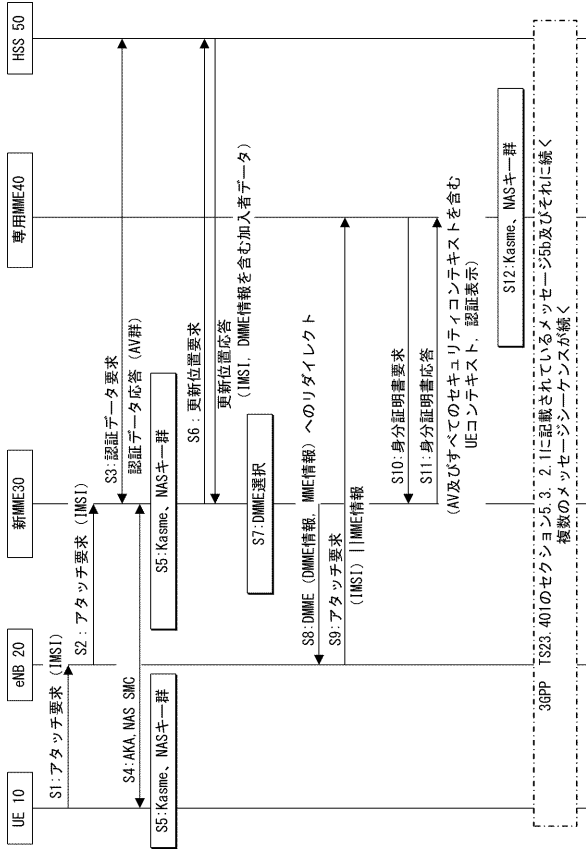
40

50

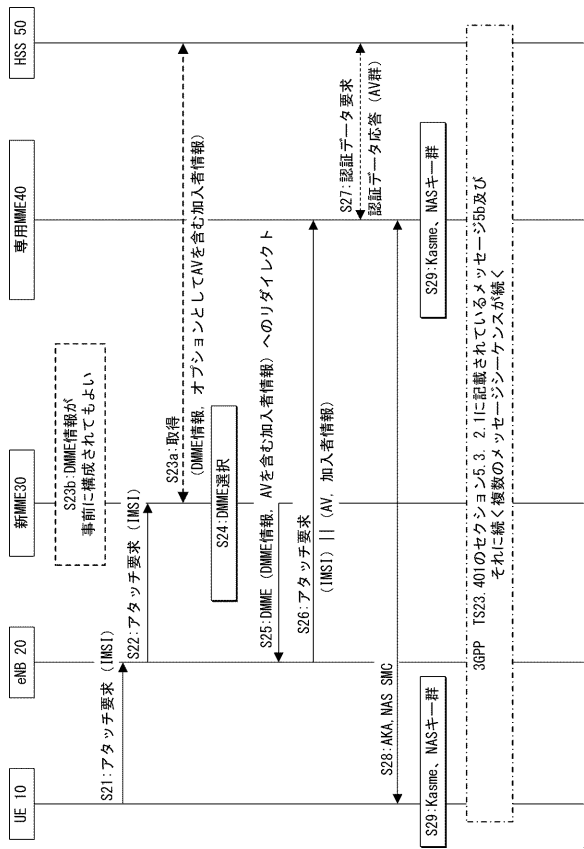
【図面】
【図 1】



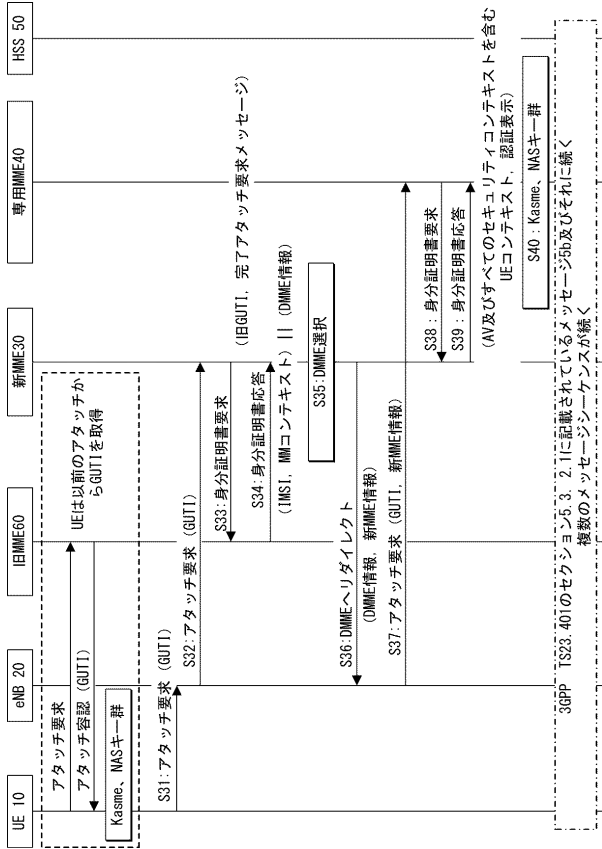
【図 2】



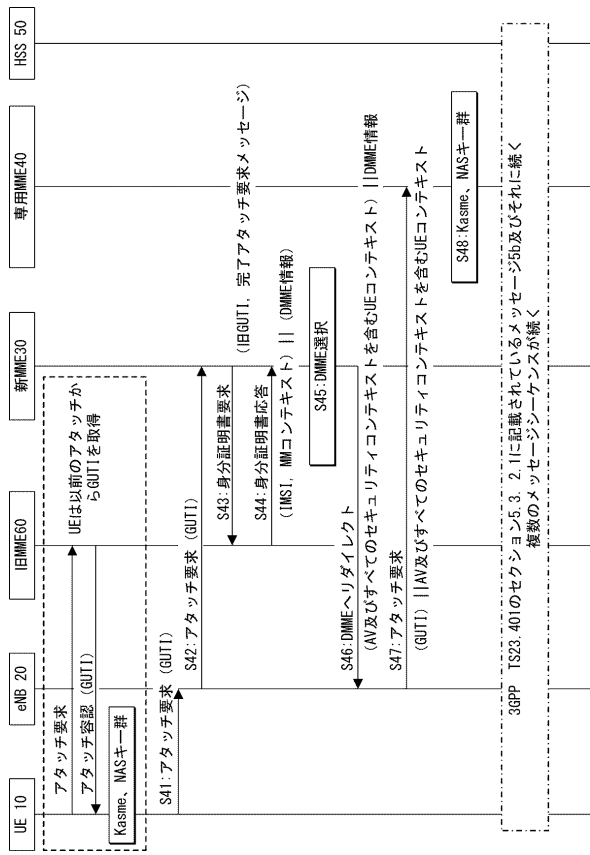
【図 3】



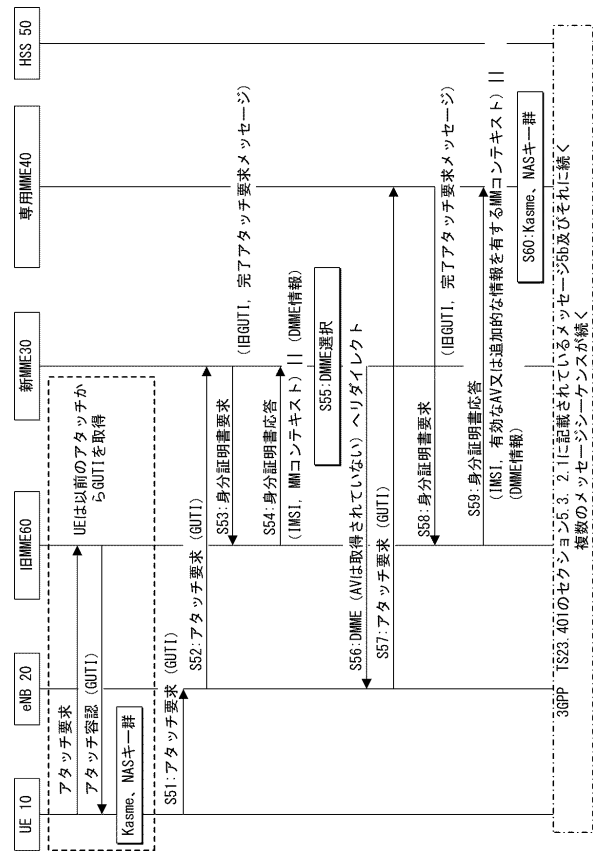
【図 4】



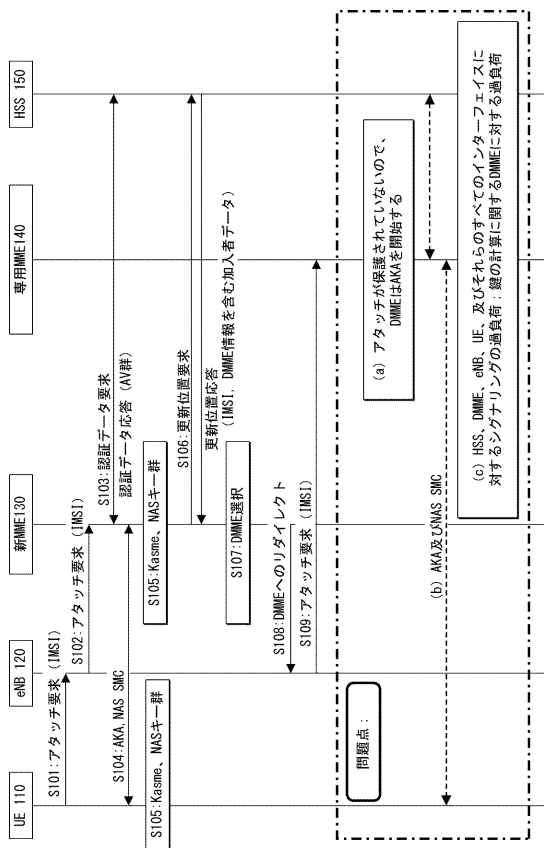
【図 5】



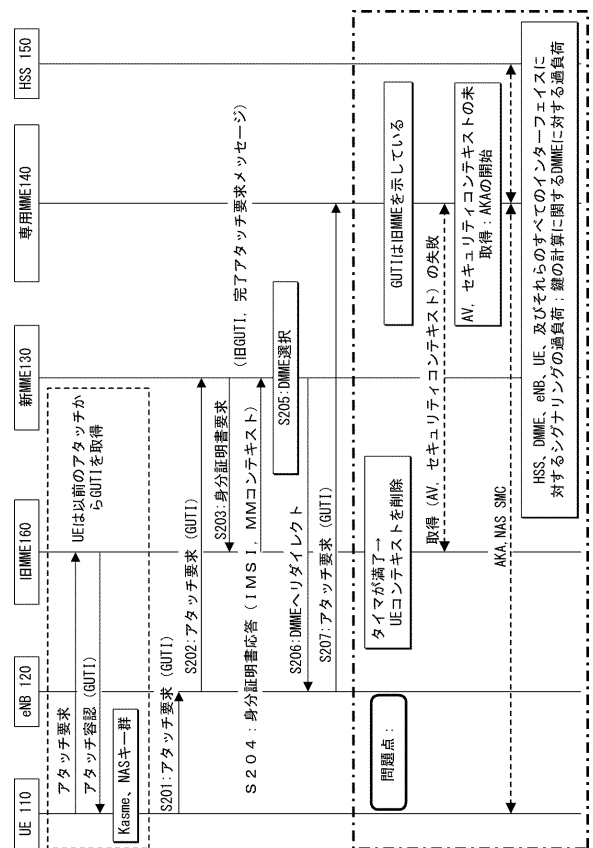
【図 6】



【図 7】



【図 8】



フロントページの続き

- (56)参考文献 米国特許出願公開第2010/0080186 (US, A1)
 特表2012-500511 (JP, A)
 特表2010-536283 (JP, A)
 国際公開第2013/047822 (WO, A1)
 国際公開第2015/172088 (WO, A1)
 特表2017-518006 (JP, A)
 NTT DOCOMO, Discussion on Core Network Type Selection based on the Subscription Information [online], TSG SA WG2 #100 S2-133909, [検索日 2020.12.07], インターネット<URL: http://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_100_San_Francisco/Docs/S2-133909.zip>, 2013年11月05日, p.1-21
 NTT DOCOMO, Addition of Subscription Information for Selecting a Specific Network [online], TSG SA WG2 #99 S2-133304, [検索日 2020.12.07], インターネット <URL: https://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_99_Xiamen/docs/S2-133304.zip>, 2013年09月18日, p.1-6
 NTT DOCOMO, Addition of Subscription Information for Selecting a Specific Network [online], SA WG2 Meeting #100 S2-133910, [検索日 2020.12.07], インターネット <URL: https://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_100_San_Francisco/Docs/S2-133910.zip>, 2013年11月05日, p.1-47
 NTT DOCOMO, Discussion on Core Network Type Selection based on the Subscription Information - REPORT OF OFFLINE DISCUSSION - [online], TSG SA WG2 #100 S2-134328, [検索日 2020.12.07], インターネット <URL: https://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_100_San_Francisco/Docs/S2-134328.zip>, 2013年11月13日, p.1-26
 NTT DOCOMO et al., Addition of Subscription Information for Selecting a Specific Network [online], SA WG2 Meeting #100 S2-133910, [検索日 2020.12.07], インターネット <URL: https://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_100_San_Francisco/Docs/S2-133910.zip>, 2013年11月05日, p.1-47
 NTT DOCOMO et al., Discussion on Core Network Type Selection based on the Subscription Information [online], TSG SA WG2 #100 S2-133909, [検索日 2020.12.07], インターネット<URL: http://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_100_San_Francisco/Docs/S2-133909.zip>, 2013年11月05日, p.1-21
 NTT DOCOMO et al., Discussion on Core Network Type Selection based on the Subscription Information - REPORT OF OFFLINE DISCUSSION - [online], TSG SA WG2 #100 S2-134328, [検索日 2020.12.07], インターネット <URL: https://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_100_San_Francisco/Docs/S2-134328.zip>, 2013年11月13日, p.1-26
- (58)調査した分野 (Int.Cl., DB名)
 H04W 4/00-99/00
 DB名 3GPP TSG RAN WG1-4
 SA WG1-4
 CT WG1、4