

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6380664号
(P6380664)

(45) 発行日 平成30年8月29日 (2018. 8. 29)

(24) 登録日 平成30年8月10日 (2018. 8. 10)

(51) Int. Cl.	F I
H O 4 W 12/06 (2009. 01)	H O 4 W 12/06
H O 4 W 60/00 (2009. 01)	H O 4 W 60/00
H O 4 W 76/10 (2018. 01)	H O 4 W 76/10
H O 4 W 92/14 (2009. 01)	H O 4 W 92/14

請求項の数 18 (全 22 頁)

(21) 出願番号	特願2017-513836 (P2017-513836)	(73) 特許権者	000004237
(86) (22) 出願日	平成27年5月26日 (2015. 5. 26)		日本電気株式会社
(65) 公表番号	特表2017-520208 (P2017-520208A)		東京都港区芝五丁目7番1号
(43) 公表日	平成29年7月20日 (2017. 7. 20)	(74) 代理人	100103894
(86) 国際出願番号	PCT/JP2015/002635		弁理士 冢入 健
(87) 国際公開番号	W02015/182111	(72) 発明者	ジャン シャオウェイ
(87) 国際公開日	平成27年12月3日 (2015. 12. 3)		東京都港区芝五丁目7番1号 日本電気株
審査請求日	平成28年11月22日 (2016. 11. 22)		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
(33) 優先権主張国	日本国 (JP)		式会社内
		(72) 発明者	プラサド 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

最終頁に続く

(54) 【発明の名称】 コアネットワークノード、基地局、UE、コアネットワークノードの通信方法、基地局の通信方法、及びUEの通信方法

(57) 【特許請求の範囲】

【請求項1】

UE (User Equipment) と基地局を介して接続する第1 MME (Mobility Management Entity) 又は第1 SGSN (Serving GPRS Support Node) と、

前記UEと前記基地局を介して接続する第2 MME又は第2 SGSNと、

を具備し、

前記UEは、アタッチ要求メッセージを、前記基地局を介して前記第1 MME又は前記第1 SGSNへ送信し、

前記第1 MME又は前記第1 SGSNは、HSS (Home Subscriber Server) 又はHLR (Home Location Register) / HSSからリダイレクトに関する情報とAV群 (Authentication Vectors) とを受信し、前記UEとの認証及びセキュリティ手順をスキップし、

前記基地局は、前記第1 MME又は前記第1 SGSNから前記情報を含むリダイレクトメッセージを受信し、前記第2 MME又は前記第2 SGSNを選択し、

前記第2 MME又は前記第2 SGSNは、前記UEとの認証及びセキュリティ手順を実行する、

コアネットワークノード。

【請求項2】

前記第2 MME又は前記第2 SGSNは、専用コアネットワーク (Dedicated Core Network) に含まれる、

請求項1記載のコアネットワークノード。

【請求項 3】

前記第 1 M M E 又は前記第 1 S G S N は、前記情報を事前に設定する、
請求項 1 記載のコアネットワークノード。

【請求項 4】

U E (User Equipment) と基地局を介して接続する第 1 M M E (Mobility Management Entity) 又は第 1 S G S N (Serving GPRS Support Node) と、前記 U E と前記基地局を介して接続する第 2 M M E 又は第 2 S G S N とを含むコアネットワークノードの通信方法であって、

前記第 1 M M E 又は前記第 1 S G S N が、前記 U E から前記基地局を介して、アタッチ要求メッセージを受信し、H S S (Home Subscriber Server) 又は H L R (Home Location Register) / H S S からリダイレクトに関する情報と A V 群 (Authentication Vectors) とを受信し、前記 U E との認証及びセキュリティ手順をスキップするステップと、

前記第 2 M M E 又は前記第 2 S G S N が、前記第 1 M M E 又は前記第 1 S G S N から前記情報を含むリダイレクトメッセージを受信した前記基地局によって選択され、前記 U E との前記認証及びセキュリティ手順を実行するステップと、

を具備する、

通信方法。

【請求項 5】

前記第 2 M M E 又は前記第 2 S G S N は、専用コアネットワーク (Dedicated Core Network) に含まれる、

請求項 4 記載の通信方法。

【請求項 6】

前記第 1 M M E 又は前記第 1 S G S N は、前記情報を事前に設定する、

請求項 4 記載の通信方法。

【請求項 7】

U E (User Equipment) と、前記 U E と基地局を介して接続する第 1 M M E (Mobility Management Entity) 又は第 1 S G S N (Serving GPRS Support Node) と、前記 U E と前記基地局を介して接続する第 2 M M E 又は第 2 S G S N と、H S S (Home Subscriber Server) 又は H L R (Home Location Register) / H S S とを含む、移动通信システムのための基地局であって、

前記 U E から受け取ったアタッチ要求メッセージを受信し、前記 H S S 又は前記 H L R / H S S からリダイレクトに関する情報と A V 群 (Authentication Vectors) とを受信し、前記 U E との認証及びセキュリティ手順をスキップする前記第 1 M M E 又は前記第 1 S G S N から、前記情報を含むリダイレクトメッセージを受信する受信部と、

前記第 2 M M E 又は前記第 2 S G S N を選択する選択部と、

を具備し、

前記 U E と、前記第 2 M M E 又は前記第 2 S G S N との間の前記認証及びセキュリティ手順が実行される、

基地局。

【請求項 8】

前記第 2 M M E 又は前記第 2 S G S N は、専用コアネットワーク (Dedicated Core Network) に含まれる、

請求項 7 記載の基地局。

【請求項 9】

前記第 1 M M E 又は前記第 1 S G S N は、前記情報を事前に設定する、

請求項 7 記載の基地局。

【請求項 10】

U E (User Equipment) と、前記 U E と基地局を介して接続する第 1 M M E (Mobility Management Entity) 又は第 1 S G S N (Serving GPRS Support Node) と、前記 U E と前記基地局を介して接続する第 2 M M E 又は第 2 S G S N と、H S S (Home Subscriber

Server) 又は H L R (Home Location Register) / H S S とを含む、移動通信システムのための基地局の通信方法であって、

前記 U E からアタッチ要求メッセージを受信し、前記 H S S 又は前記 H L R / H S S からリダイレクトに関する情報と A V 群 (Authentication Vectors) とを受信し、前記 U E との認証及びセキュリティ手順をスキップする前記第 1 M M E 又は前記第 1 S G S N から、前記情報を含むリダイレクトメッセージを受信するステップと、

前記第 2 M M E 又は前記第 2 S G S N を選択するステップと、

を具備し、

前記 U E と、前記第 2 M M E 又は前記第 2 S G S N との間の前記認証及びセキュリティ手順が実行される、

通信方法。

【請求項 1 1】

前記第 2 M M E 又は前記第 2 S G S N は、専用コアネットワーク (Dedicated Core Network) に含まれる、

請求項 1 0 記載の通信方法。

【請求項 1 2】

前記第 1 M M E 又は前記第 1 S G S N は、前記情報を事前に設定する、

請求項 1 0 記載の通信方法。

【請求項 1 3】

U E (User Equipment) と基地局を介して接続する第 1 M M E (Mobility Management Entity) 又は第 1 S G S N (Serving GPRS Support Node) と、前記 U E と前記基地局を介して接続する第 2 M M E 又は第 2 S G S N と、H S S (Home Subscriber Server) 又は H L R (Home Location Register) / H S S とを含む、移動通信システムのための前記 U E であって、

アタッチ要求メッセージを、前記 H S S 又は前記 H L R / H S S からリダイレクトに関する情報と A V 群 (Authentication Vectors) とを受信し、前記 U E との認証及びセキュリティ手順をスキップする前記第 1 M M E 又は前記第 1 S G S N へ送信する送信部と、

前記第 1 M M E 又は前記第 1 S G S N から前記情報を含むリダイレクトメッセージを受信した前記基地局が選択した前記第 2 M M E 又は前記第 2 S G S N と、前記認証及びセキュリティ手順を実行する制御部と、

を具備する、

U E。

【請求項 1 4】

前記第 2 M M E 又は前記第 2 S G S N は、専用コアネットワーク (Dedicated Core Network) に含まれる、

請求項 1 3 記載の U E。

【請求項 1 5】

前記第 1 M M E 又は前記第 1 S G S N は、前記情報を事前に設定する、

請求項 1 3 記載の U E。

【請求項 1 6】

U E (User Equipment) と基地局を介して接続する第 1 M M E (Mobility Management Entity) 又は第 1 S G S N (Serving GPRS Support Node) と、前記 U E と前記基地局を介して接続する第 2 M M E 又は第 2 S G S N と、H S S (Home Subscriber Server) 又は H L R (Home Location Register) / H S S とを含む、移動通信システムのための前記 U E の通信方法であって、

アタッチ要求メッセージを、前記 H S S 又は前記 H L R / H S S からリダイレクトに関する情報と A V 群 (Authentication Vectors) とを受信し、前記 U E との認証及びセキュリティ手順をスキップする前記第 1 M M E 又は前記第 1 S G S N へ送信するステップと、

前記第 1 M M E 又は前記第 1 S G S N から前記情報を含むリダイレクトメッセージを受信した前記基地局が選択した前記第 2 M M E 又は前記第 2 S G S N と、前記認証及びセキ

10

20

30

40

50

セキュリティ手順を実行するステップと、
を具備する、
通信方法。

【請求項 17】

前記第 2 MME 又は前記第 2 S G S N は、専用コアネットワーク (Dedicated Core Network) に含まれる、

請求項 16 記載の通信方法。

【請求項 18】

前記第 1 MME 又は前記第 1 S G S N は、前記情報を事前に設定する、

請求項 16 記載の通信方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、コアネットワークノード、無線基地局、移動端末、コアネットワークノードの通信方法、無線基地局のための通信方法、及び移動端末のための通信方法に関し、特に、ユーザ端末 (UE: User Equipment) が適切なコアネットワークによって仕えら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。

【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 UE) が、その UE を専用サービスする MME (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、I M S I (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 H S S (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】

【非特許文献 1】TSG SA WG2 #99 S2-133304, "Addition of Subscription Information for Selecting a Specific Network", 2013-09, pp. 4

【非特許文献 2】SA WG2 #100 S2-133910, "23.401 CR2606R3: Addition of Subscription Information for Selecting a Specific Network", 2013-11, pp. 7 and 9

【非特許文献 3】TSG SA WG2 #100 S2-133909, "Discussion on Core Network Type Sele

10

20

30

40

50

ction 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) を単に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ノードヘ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ノードヘ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ノードヘ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ノードヘ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。

10

【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ノードヘ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ノードヘ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。

20

【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ヘ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。

30

【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ヘ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。

40

【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

50

、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。

【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。

【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。

10

【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。

20

【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コアネットワークノードへ送る。

30

【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。

40

【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。

50

【図 7】典型的な I M S 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 G U T 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。

【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、M M E 3 0 と、
M M E 4 0 とを含んでいる。M M E 3 0 は、U E 1 0 が無線基地局としての e N B 2 0 を
介して最初にアタッチする M M E であり、このため、以下では、「新 M M E (New M M E)
」と呼ばれることがある。一方、M M E 4 0 は、署名 (subscription) に応じて U E 1 0
を専用にサービスする M M E であり、且つ、U E 1 0 が M M E 3 0 からリダイレクトされ
る M M E であり、このため、以下では、「専用 M M E (Dedicated M M E)」又は「D M M
E」と呼ばれる。ここで、M M E 4 0 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 M M E (Spe
cific M M E)」と呼ぶこともできる。必要ならば、M M E 3 0 及び M M E 4 0 は、それぞ
れ、H S S 5 0 から、U E 1 0 についての署名情報 (subscription information)、及び
、U E 1 0 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 M M E 3 0 は、ま
た、S - G W (Serving Gateway) 及び／又は P - G W (PDN (Public Data Network) Gat
eway) に接続される。同様に、専用 M M E 4 0 も、専用 S - G W 及び／又は専用 P - G W
に接続される。

【0031】

概して、第 1 実施形態は、E - U T R A N (Evolved Universal Terrestrial Radio Ac
cess Network) における I M S I アタッチを扱い、特に、新 M M E 3 0 が、e N B 2 0 か
ら受け取ったアタッチ要求メッセージ (Attach Request message) を、H S S 5 0 から取
得した U E 1 0 についての署名情報に基づいて、D M M E 4 0 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 I M S 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 I M S I アタッチ手順において、U E 1 1 0 は、その I
M S I を含むアタッチ要求メッセージを、e N B 1 2 0 へ送り (ステップ S 1 0 1)、e
N B 1 2 0 は、上記アタッチ要求メッセージを新 M M E 1 3 0 へ転送する (ステップ S 1
0 2)。

【0034】

上記アタッチ要求メッセージを受け取ると、新 M M E 1 3 0 は、認証データ要求メッ
セージ (Authentication data request message) を H S S 1 5 0 へ送り、それに対する応
答として、A V 群 (Authentication Vectors) を含む認証データ応答メッセージ (Authen
tication data response message) を受け取る (ステップ S 1 0 3)。それから、新 M M
E 1 3 0 は、U E 1 1 0 と協働して、A K A 手順及び N A S S M C 手順を実行する (ス
テップ S 1 0 4)。結果として、U E 1 0 及び新 M M E 1 3 0 は、それぞれ、K a s m e
(Key for access security management entity) 及び N A S 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 U E 1 0 と新 M M E 1 3 0 の間に

確立される（ステップS105）。

【0035】

その後、新MME130は、更新位置要求メッセージ（Update Location Request message）をHSS150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IMS I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MME140についての情報（以下では、「DMM E情報」と呼ばれることがある）を含んでいる。

【0036】

それから、新MME130は、上記UE110がリダイレクトされるべき専用MME140を、上記DMM E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eNB120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、eNB120は、上記アタッチ要求メッセージを専用MME140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MME140は、UE110に対するAKA手順を開始する。

（b）上記（a）に起因して、専用MME140は、認証データ要求メッセージをHSS150へ送ると共に認証データ応答メッセージをHSS150から受信し、更新位置要求メッセージをHSS150へ送ると共に更新位置応答メッセージをHSS150から受信し、UE110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MME140に対する過負荷だけではなく、HSS150、専用MME140、eNB120、UE110、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MME30は、新MME30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eNB20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）、又は、新MME30に割り当てられたIP（Internet Protocol）アドレスを含んでいる。そして、eNB20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MME40へ転送する（ステップS9）。

【0040】

専用MME40は、既にUE110と新MME30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MME30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MME40は、身分証明書要求（identification request）メッセージを新MME30へ送信し（ステップS10）、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S11）。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MME40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S12）。

【0041】

その後、3GPP TS23.401のセクション5.3.2.1に記載されている

10

20

30

40

50

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MME40は、専用MME40が新MME30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MME40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(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。

10

【0043】

さらに、上記ステップS11で、新MME30は、身分証明書応答メッセージの中に、UE10が専用MME40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)を含めてもよい。この場合、専用MME40は、UE10を認証する目的でHSS50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。

【0044】

(オプション2)

20

図3は、オプション2のシーケンス図を示す。ステップS21及びステップS22は、図2のステップS1及びステップS2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MME30は、最初に、上記DMME情報を含む上記署名情報(subscription information)をHSS50から取得する(ステップS23a)。

【0046】

上記の通り、上記DMME情報は、UE10が専用MME40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MME30は、UE10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MME30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。

30

【0047】

それから、新MME30は、上記DMME情報に基づいて、専用MME40を選択し(ステップS24)、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eNB20へ送信する(ステップS25)。それから、eNB20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MME40へ転送する(ステップS26)。

【0048】

上記署名情報(すなわち、DMME情報)の受信に応答して、専用MME40は、新MME30の代わりとして、eNB20を介してUE10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MME40は、認証データ要求メッセージをHSS50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S27)。そして、専用MME40は、UE10と効力してAKA手順及びNAS SMC手順を実行する(ステップS28)。結果として、UE10及び専用MME40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、UE10と専用MME40との間でeNB20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S29)。

40

【0049】

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。

50

【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MME30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MME30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S23aの代わりとして、新MME30において、DMME情報が事前に構成されてもよい(ステップS23b)。この場合、新MME30は、UE10から最初のアタッチ要求を受信したときに、HSS50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。

10

【0052】

さらに、上記ステップS23aで、新MME30は、さらに、HSS50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S25で示されたリダイレクトメッセージ及びステップS26で示されたアタッチ要求メッセージと一緒に、eNB20を介して専用MME40へ転送されることができる。この場合、専用MME40は、上記ステップS27に示された、HSS50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。

【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MME30及びMME40に加えて、MME60をさらに含んでいる。MME60は、UE10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MME60は、上記署名情報、DMME情報、上記AV群等を、HSS50から取得することもできる。ここで、UE10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。

20

【0054】

概して、第2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、旧MME60から取得した上記DMME情報に基づいて、DMME40へリダイレクトするケースを扱う。

30

【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。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、UE110は前に旧MME160へアタッチしており、旧MME160がUE110へGUTIを割り当てており、この結果、UE110がGUTIを取得しているものとする。

40

【0057】

典型的なGUTI アタッチ手順において、UE110は、GUTIを含むアタッチ要求メッセージをeNB120へ送信し(ステップS201)、eNB120は新MME130へアタッチ要求メッセージを転送する(ステップS202)。

【0058】

アタッチ要求メッセージを受信すると、新MME130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MME160へ送信し(ステップS203)、これに対する応答として、UE110のIM

50

S I 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 S 2 0 4)。

【0059】

それから、新 MME 1 3 0 は、専用 MME 1 4 0 を選択し (ステップ S 2 0 5)、eNB 1 2 0 へリダイレクトメッセージを送信する (ステップ S 2 0 6)。リダイレクトメッセージを受信すると、eNB 1 2 0 は、専用 MME 1 4 0 へ上記アタッチ要求メッセージを転送する (ステップ S 2 0 7)。

【0060】

しかしながら、旧 MME 1 6 0 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 1 6 0 を単に示しているだけである。それゆえ、専用 MME 1 4 0 は、旧 MME 1 6 0 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 1 5 0、専用 MME 1 4 0、eNB 1 2 0、UE 1 1 0、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 1 4 0 に対する過負荷である。

【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 S 3 1 からステップ S 3 5 のプロセスは、上記の図 8 のステップ S 2 0 1 からステップ S 1 0 5 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 3 0 は、新 MME 3 0 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 2 0 へ送信する (ステップ S 3 6)。それから、eNB 2 0 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 4 0 へ転送する (ステップ S 3 7)。

【0064】

専用 MME 4 0 は、上記ステップ S 3 4 で旧 MME 6 0 から新 MME 3 0 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 3 0 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 4 0 は、身分証明書要求メッセージを新 MME 3 0 へ送信し (ステップ S 3 8)、そ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 S 3 9)。上記の通り、上記 UE コンテキストは、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。それから、専用 MME 4 0 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 4 0)。

【0065】

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 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 4 0 は、MME 情報について示されることで、専用 MME 4 0 は、新 MME 4 0 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 GUTI と異なり、専用 MME 4 0 は、旧 MME 6 0 から上記 AV 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 6 0 へ接触する必要がなく、これにより、旧 MME 6 0 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、AKA 手順を開始する必要がない。このため、典型的な GUTI 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

10

20

30

40

50

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S39において、新MME30は、UE10が専用MME40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も含めてもよい。この場合、専用MME40は、UE10を認証する目的でHSS50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S41からステップS45は、図4のステップS31からステップS35と同様に実行される。

【0069】

一方で、リダイレクトの際に、新MME30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eNB20へ送信する(ステップS46)。それから、eNB20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MME40へ転送する(ステップS47)。上記の通り、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。

【0070】

それから、専用MME40は、受信したUE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S48)。

【0071】

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。

【0072】

このオプション2によれば、専用MME40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MME40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S43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S47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

10

20

30

40

50

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MME 60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MME 60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MME 40へ送り返す（ステップS59）。

【0079】

それから、専用MME 40は、受信したMM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S60）。

【0080】

その後、3 G P P T S 2 3 . 4 0 1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G U T Iと同様に、専用MME 40は、G U T I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MME 60から取得することができ、これにより、A K A手順を開始する必要がある。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、G U T I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MME 30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MME 40に対して、A Vが取得されていないことを知らせ、旧MME 60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A V群だけを専用MME 40に対して知らせる。これにより、専用MME 40は、U E 1 0との間の通信を行うために、上記有効なA V群を用いることができる。ここで、上記有効なA V群の代わりとして又はこれに追加して、旧MME 60は、他の追加的な情報を専用MME 40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MME 60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MME 40及び旧MME 60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-U T R A Nを例にとることにより説明を行ったが、本発明は、U T R A Nにおける、I M S I アタッチ及びP-T M S I（パケット-T 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。

- ・MMEをS G S Nで置き換えること。
- ・DMME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 M M E 3 0、専用 M M E 4 0、及び旧 M M E 6 0 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 2 0 を介して U E 1 0 と通信を行い、e N B 2 0 を介して又は介さずに M M E 3 0、4 0、6 0 との間の通信を行い、且つ、H S S 5 0 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に、これらの通信機を制御する。

10

【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、

20

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)

30

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】

40

(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、U E 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U E 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U E 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

50

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、

10

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)

20

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、

30

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、

40

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】

50

(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

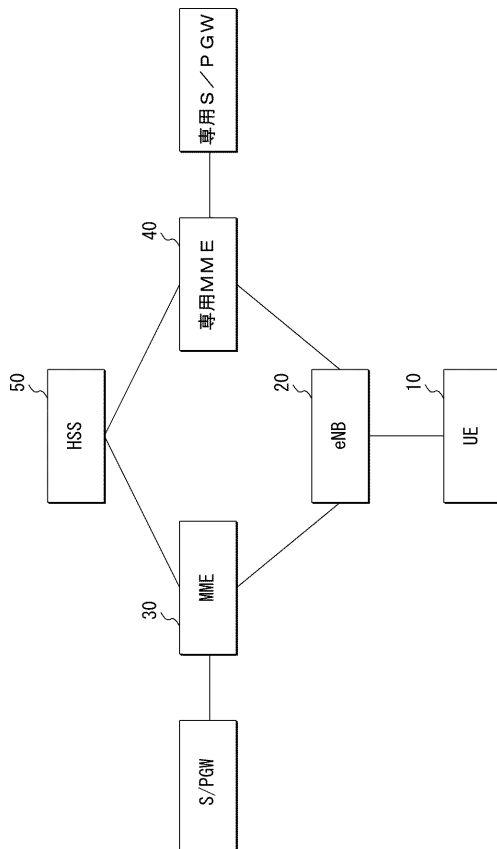
20, 120 eNB

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

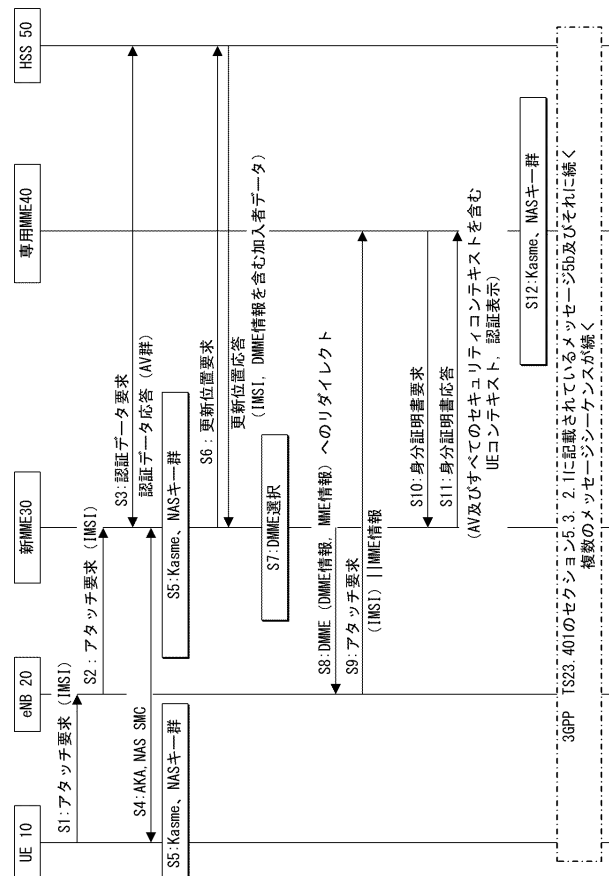
50, 150 HSS

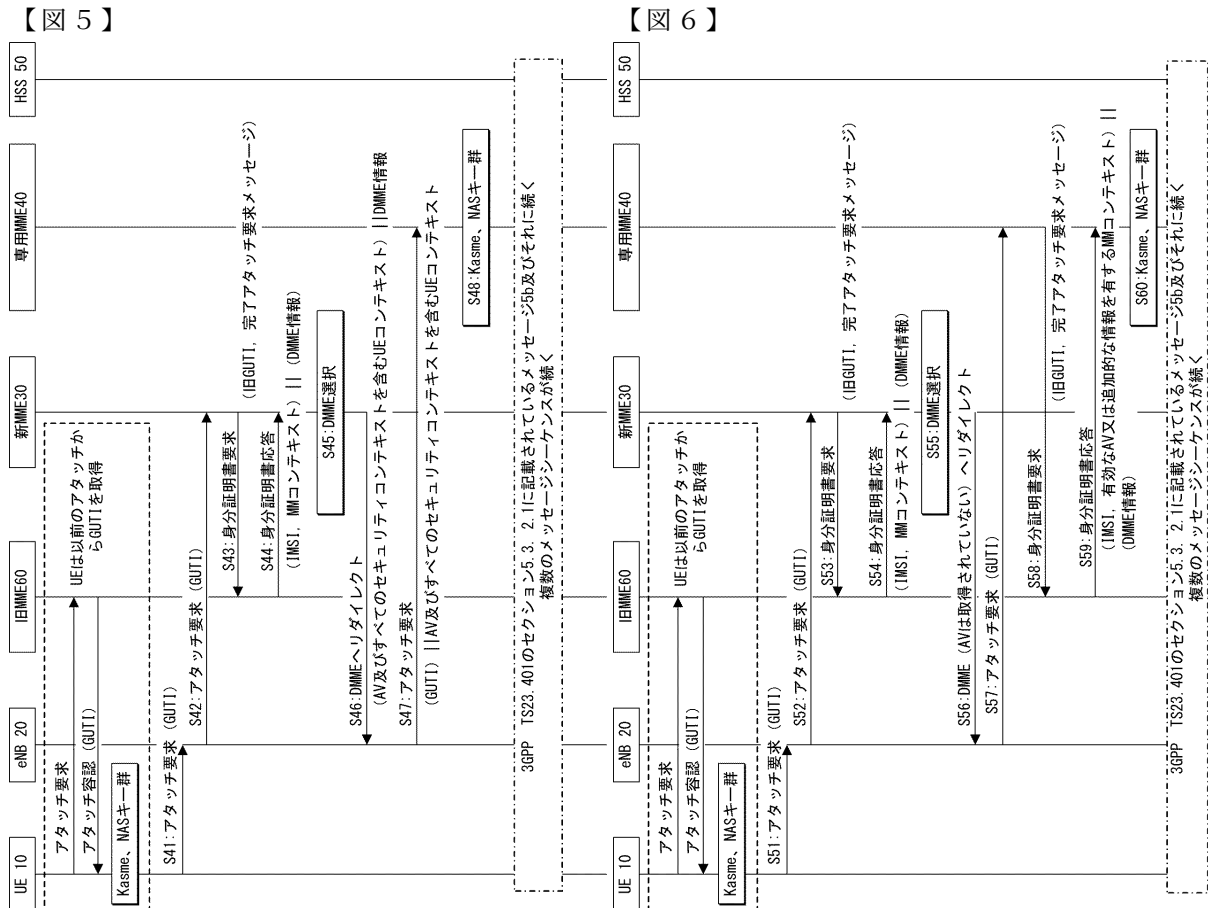
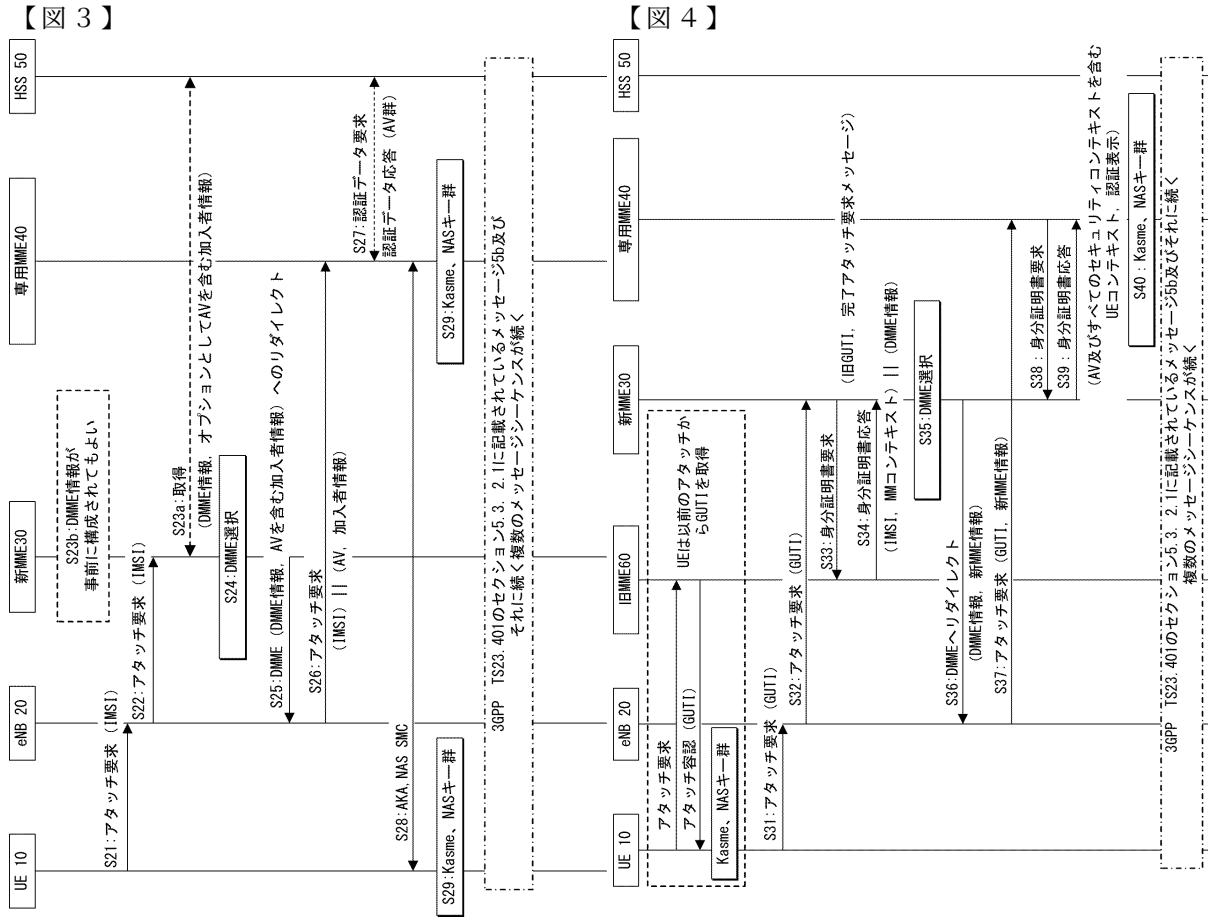
10

【図1】

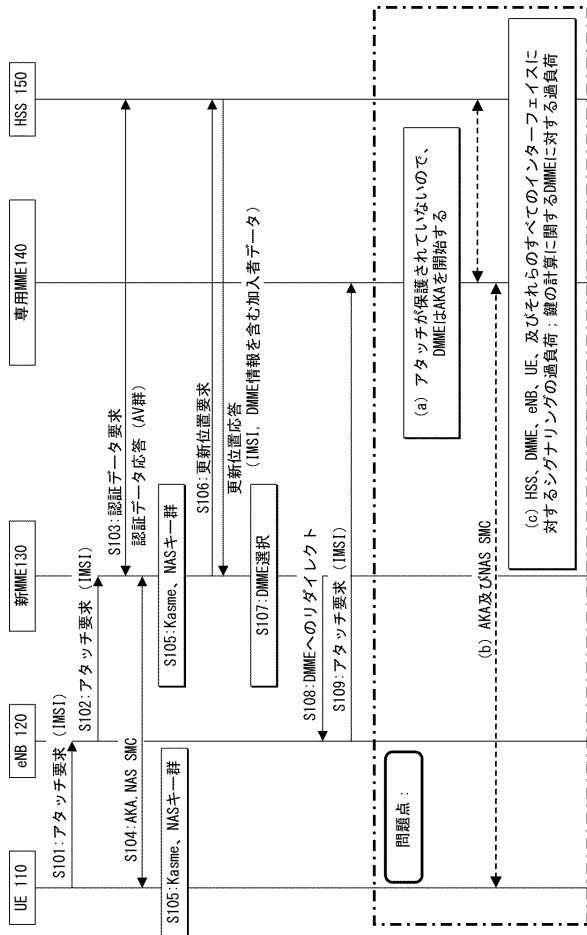


【図2】

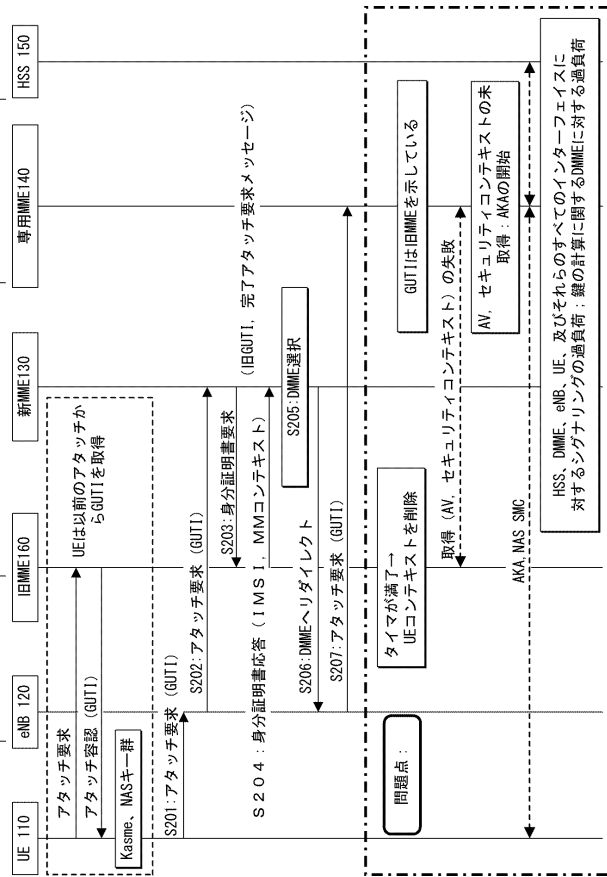




【図 7】



【図 8】



フロントページの続き

審査官 田部井 和彦

- (56)参考文献 米国特許出願公開第2010/0080186 (US, A1)
国際公開第2015/172088 (WO, A1)
特表2017-518006 (JP, A)
国際公開第2013/047822 (WO, A1)
米国特許出願公開第2011/0230188 (US, A1)
NTT DOCOMO, Discussion on Core Network Type Selection based on the Subscription Information [online], TSG SA WG2 #100 S2-133909, [retrieved on 2018.01.26], Retrieved from the Internet: <URL: http://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_100_San_Francisco/Docs/S2-133909.zip>, 2013年11月 5日, 第1-21頁

- (58)調査した分野(Int.Cl., DB名)

H04W	4/00-99/00
H04B	7/24- 7/26
3GPP TSG RAN	WG1-4
	SA WG1-4
	CT WG1、4