

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4278614号

(P4278614)

(45) 発行日 平成21年6月17日(2009.6.17)

(24) 登録日 平成21年3月19日(2009.3.19)

(51) Int.Cl.

F I

H04W 12/08

(2009.01)

H04Q 7/00 184

請求項の数 24 (全 11 頁)

(21) 出願番号 特願2004-542232 (P2004-542232)
 (86) (22) 出願日 平成14年9月30日 (2002.9.30)
 (65) 公表番号 特表2006-501780 (P2006-501780A)
 (43) 公表日 平成18年1月12日 (2006.1.12)
 (86) 国際出願番号 PCT/EP2002/010962
 (87) 国際公開番号 W02004/034717
 (87) 国際公開日 平成16年4月22日 (2004.4.22)
 審査請求日 平成17年8月12日 (2005.8.12)

(73) 特許権者 507189219
 ノキア シーメンス ネットワークス ゲ
 ゼルシャフト ミット ベシュレンクテル
 ハフツング ウント コンパニー コマ
 ンディトゲゼルシャフト
 Nokia Siemens Netwo
 rks GmbH & Co. KG
 ドイツ連邦共和国 ミュンヘン ザンクト
 マルティン シュトラーセ 76
 St. Martin Str. 76,
 D-81541 Muenchen,
 Germany
 (74) 代理人 100061815
 弁理士 矢野 敏雄

最終頁に続く

(54) 【発明の名称】 アクセストークン、および最適化されたサービス品質を支援するハンドオーバープロシージャに対
 するDoS攻撃を所定の範囲のみで有効な暗号化トークンを用いて防止する方法

(57) 【特許請求の範囲】

【請求項 1】

再登録プロセスの開始前に移動無線端末機(5)が移動無線通信網のイントラドメイン
 ハンドオーバーに対して少なくとも1つのアクセス装置へ登録を問い合わせることに基づい
 て登録権限を検査する方法において、

1つのアクセス装置(4)から移動無線端末機(5)へ送信されたトークンを少なくと
 も1つのアクセス装置の少なくとも1つのトラストテーブル(7)に記憶しておく、

前記移動無線端末機(5)から登録の問い合わせがあったとき、少なくとも1つの別の
 アクセス装置では、トークンを受信し、

受信したトークンと記憶されているトークンとを登録権限の検査を開始する前に比較し
 、権限が存在する場合に登録を開始し、

前記トークンは、一度使用された後は廃止され、繰り返しては使用されないことを特徴
 とする登録権限を検査する方法。

【請求項 2】

キーで暗号化されたトークンを移動無線端末機(5)へ送信する、請求項1記載の方法
 。

【請求項 3】

登録権限の検査を再登録プロセスの開始前に行う、請求項1記載の方法。

【請求項 4】

再登録プロセスに対して接続更新プロセスを用いる、請求項1記載の方法。

10

20

【請求項 5】

再登録プロセスに対してオーセンティケーションプロセスおよびオーソリゼーションプロセスを用いる、請求項1記載の方法。

【請求項 6】

再登録プロセスに対して接続更新プロセスとオーセンティケーションプロセスおよびオーソリゼーションプロセスとを同時に用いる、請求項1記載の方法。

【請求項 7】

前記少なくとも 1 つのアクセス装置はアクセスルータである、請求項1記載の方法。

【請求項 8】

権限の検査が成功したのち前記少なくとも 1 つのアクセス装置（6）で接続プロセスの更新を開始する、請求項1記載の方法。 10

【請求項 9】

権限の検査が成功したのち前記少なくとも 1 つのアクセス装置（6）でオーセンティケーションプロセスおよびオーソリゼーションプロセスの更新を開始する、請求項1記載の方法。

【請求項 10】

前記少なくとも 1 つのアクセス装置（6）と前記移動無線端末機（5）とのあいだの接続を更新せよとのメッセージを付してトークンを送信する、請求項1記載の方法。

【請求項 11】

前記少なくとも 1 つのアクセス装置（4）は前記移動無線端末機（5）で受信されたトークンを隣接する他のアクセス装置（1，6）へ送信する、請求項1記載の方法。 20

【請求項 12】

前記少なくとも 1 つのアクセス装置（4）は前記移動無線端末機（5）で受信されたトークンを隣接する他のアクセス装置（1，6）へ送信してトラストテーブルに記憶させる、請求項1記載の方法。

【請求項 13】

前記少なくとも 1 つのアクセス装置（4）において隣接する他のアクセス装置（1，6）から取得されたトークンを少なくとも 1 つのトラストテーブル（7）に記憶する、請求項1記載の方法。

【請求項 14】

使用済みのトークンを前記トラストテーブルに記憶する、請求項1記載の方法。 30

【請求項 15】

前記移動無線端末機（5）はイントラドメインハンドオーバの際にトークンを前記少なくとも 1 つの別のアクセス装置（6）へ送信する、請求項1記載の方法。

【請求項 16】

前記少なくとも 1 つのアクセス装置（6）はトークンの有効期間を検査する、請求項1記載の方法。

【請求項 17】

前記少なくとも 1 つのアクセス装置（6）はトークンの作成状態を検査する、請求項1記載の方法。 40

【請求項 18】

トークンのキーを表す部分と前記少なくとも 1 つのアクセス装置（6）で計算されたキーとを比較する、請求項1記載の方法。

【請求項 19】

トークンは移動無線端末機（5）の I D を含む、請求項1記載の方法。

【請求項 20】

トークンはこれを作成したアクセス装置（4）の I D を含む、請求項1記載の方法。

【請求項 21】

トークンは作成時刻を含む、請求項20記載の方法。

【請求項 22】

トークンは乱数を含む、請求項 2 0 記載の方法。

【請求項 2 3】

トークンはキーを表す付加部分を含む、請求項 2 0 記載の方法。

【請求項 2 4】

オーセンティケーションプロセスおよびオーソリゼーションプロセスの開始時に移動無線通信網のイントラドメインハンドオーバーに対して移動無線端末機（5）が少なくとも1つのアクセス装置へ登録を問い合わせることに基づいてアクセス権限を検査するアクセス権限の検査装置において、

トークンおよび移動無線端末機のアクセス権限に関する問い合わせを受信する受信ユニット（10）と、

一度使用された後は廃止され繰り返しては使用されないトークンを作成しかつ取得されたトークンを検査する処理ユニット（11）と、

作成されたトークンおよび少なくとも1つのアクセス装置から取得されたトークンを記憶する少なくとも1つのトラストテーブル（7）と、

作成したトークンを移動無線端末機（5）および少なくとも1つの別のアクセス装置へ送信しかつアクセス権限を別のネットワークユニットへ転送する送信ユニット（12）とを有する

ことを特徴とするアクセス権限の検査装置。

【発明の詳細な説明】

【技術分野】

【0001】

Subramanyam V. et al., "Security in mobile systems", Reliable Distributed Systems, 1998 Proceedings Seventeenth IEEE Symposium on West Lafayette in USA, 20-23 .Oct.1998., Los Alamitos CA USA, IEEE Comput.Soc.US., 20.Oct.1998., XP010319125, ISBN0-8186-9128-9 407頁～412頁では、ネットワークのモバイル適応能力とこれに応じて拡大しつつあるセキュリティスキーマへの要求が論じられている。ユーザにとってはネットワーク内の情報へ連続的にアクセスできることが重要であり、例えば医師が或る患者の健康状態を定常的にモバイル機器から監視しなければならないような場合が特にそうである。こうしたケースでの通信は通常ワイヤレスの接続で行われ、メッセージ交換のセキュリティが保証されることがきわめて重要である。確実なEDVコンピューティングの目標はこれまでは信用性、完全性、利用可能性、合法性および責任能力などをファイリングすることであった。

【0002】

本発明はオーセンティケーションプロセスおよびオーソリゼーションプロセスの開始前に移動無線端末機が移動無線通信網のイントラドメインハンドオーバーに対して少なくとも1つのアクセス装置へ登録を問い合わせることに基づいて登録権限を検査する方法および装置に関する。

【0003】

QoS機構（サービス品質機構）はモバイルインターネット通信を支援しているネットワークのサービス特性、例えばエンドツーエンド伝搬時間などを保証するために設けられている。しかしネットワークではいわゆるサービス拒否攻撃（ディナリアルオブサービス；DoS攻撃）によりこうした機構が侵害されることがある。DoS攻撃とは、正統なユーザのサービス利用性を低下させようとする目的で、QoSシグナリング機構をネットワークへの問い合わせのためにモバイルノードの作動に利用し、リソースリザベーションを発生させることを云う。当該のネットワークは例えばモバイルノードの由来やオーソリゼーションの問い合わせによりQoS問い合わせの“信用度”を効率的に検査できないので、このときネットワークの能力は偽QoS問い合わせによって低下してしまう。移動無線端末機はホームネットワークを出てHMI Pv6およびAAAアーキテクチャのネットワークへ接続を変更する。この場合モバイルアンカーポイントMAPと各アクセスルータARとのあいだ、ローカルAAAサーバAALと各アクセスルータARとのあいだ、モバ

10

20

30

40

50

イルアンカーポイントとローカルAAAサーバとのあいだ、およびアクセスルータどうしのあいだでつねにセキュリティアソシエーションSAが生じる。移動無線端末機の登録が成功したのち、そのオーセンティケーション情報およびオーソリゼーション情報AAはローカルAAAサーバに記憶され、そのIDはモバイルアンカーポイントおよび当該の移動無線端末機が最初に登録したアクセスルータARで既知となる。また移動無線端末機はアクセスルータARの展開領域のあいだで通信の中断なしに移動することがある。イントラドメインハンドオーバを最適化するために、個々のアクセスルータでの登録の待機時間はできる限り小さくしなければならない。

【0004】

一般にDOS攻撃は通信装置の通常の利用や管理または種々のサービス提供を阻害する。サービス拒否攻撃（DOS攻撃）はたいてい特殊な目的で行われる。例えば多数の偽メッセージを送信することによってネットワーク全体の停止または遮断や過負荷による能力低下などを狙うのである。そうなるとアクセスネットワーク内の全ての移動無線端末機が通信路に沿った全てのノードヘリソースリザベーションのためにQoS問い合わせを送信してしまいかねない。攻撃者もQoS問い合わせをアクセスネットワークへ送信する。このためにアクセスルータは所定の移動無線端末機のQoS問い合わせの信用度を処理前に検査しなければならなくなる。アクセスルータがこれをローカルAAAサーバを介してリザベーションプロセスの開始前に行う場合、再登録プロセスに対して膨大な待機時間がかってしまう。

【0005】

1つのアクセスルータの展開領域内の所定の移動無線端末機が他のアクセスルータの展開領域へ移動する場合（イントラドメインハンドオーバ）、本来ならば移動無線端末機とアクセスネットワークとのあいだの通信に中断が生じてはならない。この移動無線端末機は第1のアクセスルータとの接続を保持しつつ、接続更新メッセージの送信により次のアクセスルータへの新たな登録プロセスを開始する。予め当該の移動無線端末機がアクセスネットワーク内の登録ユーザであるか否か検査されていないと、アクセスネットワークの攻撃者がオーセンティケーションおよびオーソリゼーションに関する問い合わせによって計算容量を消滅させたり、偽問い合わせによってリソースリザベーションに負荷をかけたりするおそれがある。

【0006】

したがって本発明の課題は、通信網の能力を最適に保証しながら偽問い合わせを効果的に防止することである。

【0007】

この課題は、1つのアクセス装置から移動無線端末機へ送信されたトークンを少なくとも1つのアクセス装置の少なくとも1つのトラストテーブルに記憶しておき、前記移動無線端末機から登録の問い合わせがあったとき、少なくとも1つの別のアクセス装置では、トークンを受信し、受信したトークンと記憶されているトークンとを登録権限の検査を開始する前に比較し、権限が存在する場合に登録を開始し、前記トークンは、一度使用された後は廃止され、繰り返しては使用されないことにより解決される。さらに本発明の課題は、トークンおよび移動無線端末機のアクセス権限に関する問い合わせを受信する受信ユニットと、一度使用された後は廃止され繰り返しては使用されないトークンを作成しかつ取得されたトークンを検査する処理ユニットと、作成されたトークンおよび少なくとも1つのアクセス装置から取得されたトークンを記憶する少なくとも1つのトラストテーブルと、作成したトークンを移動無線端末機および少なくとも1つの別のアクセス装置へ送信しかつアクセス権限を別のネットワークユニットへ転送する送信ユニットとを有する装置を構成することにより解決される。

【0008】

本発明のコンセプトは、イントラドメインハンドオーバに際して接続更新プロセスやオーセンティケーションプロセスおよびオーソリゼーションプロセス（AAAプロセス）を開始する前にトークン（権限票）を用いた登録権限の検査を行い、DOS攻撃を防止する

10

20

30

40

50

ということである。この手法の利点は再登録プロセスにおける僅かな待機時間のみで効果的にD o S攻撃を防止できることにある。この手法を用いれば、D o S攻撃（D o S攻撃とはシステムのメモリを満杯にしてシステムが正統な問い合わせに対処できなくなるようにさせるものである）によるアクセスルータのメモリフルロード、偽問い合わせによるアクセスネットワークにおけるシグナリングキャパシティの能力低下およびローカルA A Aサーバの不当なリソース占有などを回避することができる。

【0009】

有利な実施形態は従属請求項に記載されている。トークンが繰り返し送信されてしまうC o o k i eのような危険は、トークンの受容される有効範囲を狭く制限することにより低減される。

10

【0010】

本発明を図示の実施例に則して詳細に説明する。図1には最初のトークン（トークン）を移動無線端末機へ送信する様子が示されている。図2には有効範囲の制限なしに、また他のアクセス装置での使用可能性の表示なしに予め作成されていたトークンを送信する様子が示されている。図3には制限された有効範囲内での使用を示すインジケータなしで予め作成されていたトークンを送信する様子が示されている。図4には予め作成されていたトークンに制限された有効範囲内での使用を示すインジケータを付して送信する様子が示されている。図5にはイントラドメインハンドオーバ後にトークンを移動無線端末機へ送信する様子が示されている。図6にはトークンを送信および検査する装置のブロック図が示されている。

20

【0011】

図1には移動無線端末機5がスイッチオンに際してまたはアクセスネットワークでの最初の報知に際して最初の登録問い合わせを第1のアクセスルータ4へ送信したあとの様子が示されている。ローカルA A AサーバがホームA A Aサーバからオーセンティケーション情報およびオーセンティケーション情報の肯定を受け取ったのち、ローカルA A AサーバはモバイルアンカーポイントM A Pへオーセンティケーションおよびオーソリゼーションの検査を通ったことを知らせる。そののちモバイルアンカーポイント2はセッションキーを第1のアクセスルータ4へ送信する。セッションキーはホームA A Aサーバで作成され、オーセンティケーション情報およびオーセンティケーション情報とともに転送されたものである。これにより第1のアクセスルータ4は当該の移動無線端末機5とのセキュリティアソシエーションを築くことができる。第1のアクセスルータ4はトークンを作成し、これをセッションキーで暗号化して移動無線端末機5へ送信する。移動無線端末機5は長期のセキュリティアソシエーションによりこのセッションキーを確実にホームA A Aサーバから受け取る。

30

【0012】

トークンはこの場合つねにアクセスルータによって作成される。移動無線端末機5はその報知を受け取るべきアクセスルータまたはイントラドメインハンドオーバを行うアクセスルータから第1のトークンを受け取る。すなわち登録が有効となった後、セッションキーで暗号化されたトークンが移動無線端末機5とアクセスネットワークの全てのアクセスルータとのあいだに設定され、第1のアクセスルータ4から当該の移動無線端末機5へ接続更新メッセージとともに送信される。各アクセスルータは少なくとも1つのトラストテーブル7を有している。第1のタイプのトラストテーブルすなわちトラステッドリストにはトークンを受け取るべきアクセスルータに関する情報が記憶され、第2のタイプのトラストテーブルすなわちトラスティングリストには自身の作成したトークンを送るべきアクセスルータに関する情報が記憶される。第3のタイプのトラストテーブルには既に使用されたトークンが記憶される。ここには所定の移動無線端末機によって既に一度有効に使用された全てのトークンが記憶される。このようにトークンは一度使用された後は“廃止”され、繰り返しては使用されない。他の2つのトラストテーブルは使用された各トークンを全アクセスネットワークの各アクセスルータにいちいち記憶せず、2つのタイプのトラストテーブル（トラステッドリストおよびトラスティングリスト）によって実現された有効

40

50

範囲内にあるアクセスルータのみに記憶すればよいように設けられている。

【0013】

このように有効範囲を制限しないと、本発明の方法は大規模なアクセスネットワークに対してスケーリングされない。本発明の方法によれば、第1のアクセスルータ4によって作成され、トラストテーブル内に存在するトークンのみが受容される。別のトラストテーブルには第1のアクセスルータ4の作成したトークンを受容すべきアクセスルータのリストが含まれている。セキュリティ性を高めるために第1のアクセスルータ4によって隣接するアクセスルータのトークンがトラストテーブルに記憶される。これによりトークンの受容に対して制限された有効範囲が形成される。これは第1のアクセスルータ4が自身の作成したトークンおよび隣接するアクセスルータ6の作成したトークンのみを受容するからである。移動無線端末機5がイントラドメインハンドオーバを行おうとする場合、当該の移動無線端末機5は再登録問い合わせにトークンを付加し、これをテキストとして新たなアクセスルータ6へ送信する。

10

【0014】

新たなアクセスルータ6は当該のトークンを検査するために3つのアクションを行う。
すなわち

- 1) トークンの伝搬時刻から有効期間を検査し、
- 2) トークンを作成したアクセスルータのIDがトラストテーブル内にあるか否かを検査し、
- 3) 上述のポイントの検査が終了したのち、乱数付加部分(キーハッシュダイジェスト)をトークンのキーを用いて計算し、さらにこれとトークン内に既に存在している乱数付加部分とを比較する。

20

【0015】

トークンの検査が成功すると、接続更新プロセスおよび再登録プロセスが開始される。新たなアクセスルータ6は再登録問い合わせ(BUACKメッセージ)に含まれているセッションキーがモバイルアンカーポイントMAPから受け取られると再登録問い合わせの認証を行う。認証が認められない場合には新たなアクセスルータ6は再登録問い合わせをそれ以上は処理しない。所定の時間が経過しても再登録についての回答を新たなアクセスルータから得られない場合には、移動無線端末機5はローカルAAAサーバ3およびホームAAAサーバに関するオーソリゼーションプロセスおよびオーセンティケーションプロセスをイントラドメインハンドオーバまたはスイッチオンの際と同様に開始しなければならない。このときには当該の移動無線端末機5は最適なハンドオーバプロセスを利用できない。

30

【0016】

新たなアクセスルータ6で再登録プロセスの認証が認められた場合、セッションキーを付して新たなトークンを作成し、次のイントラドメインハンドオーバのために移動無線端末機5へ送信する。ここで古い第1のトークンはもはや使用できなくなる。第1のトークンの失効は第2のアクセスルータ6からトークンを作成した第1のアクセスルータ4へ伝えられる。当該のトークンを作成したアクセスルータ4はこれを使用している第2のアクセスルータ6を除くトラストテーブル内の全てのアクセスルータにこれを知らせ、第1のトークンが重用されないよう阻止する。トークンの有効期間が終了時点に達すると、当該のトークンは各アクセスルータのトラストテーブルから消去される。

40

【0017】

トークンはトークン情報および乱数付加部分(ハッシュコード)を含む。トークン情報は

- 1) 移動無線端末機5のID: アクセスネットワーク内での移動無線端末機5の1回限りのID(最初の登録後に取得したものであってよい)
- 2) 当該のトークンを作成したアクセスルータのID: アクセスネットワーク内で1回限り使用される一義的なアクセスルータのID(IPアドレスまたは他の一義的な識別子)
- 3) トークンの有効期間を制限するために用いられる作成時刻

50

4) 同時刻に作成された2つのトークンを区別するために用いられる乱数を含む。

【0018】

乱数付加メッセージはトークン情報およびトークンキーから成る。乱数付加部分の計算はHMAC-MD5またはHMAC-SHA1の機能部によって行われる。トークンキーはモバイルアンカーポイントMAPから各アクセスルータへ分配され、周期的に更新される。

【0019】

トークンは次のように構成されている。

トークン：トークン情報，トークン乱数付加部分

トークン情報：移動無線端末機のID，アクセスルータのID，作成時点，乱数

トークン乱数付加部分：HMAC（トークンキー，トークン情報）

図2には作成されたトークンに対する有効範囲がアクセスネットワーク全体となっているケースが示されている。或るトークンが最初の使用のためにアクセスルータ6へ送信される場合、当該のアクセスルータ6のみ確実にDOS攻撃から保護される。なぜなら当該のアクセスルータ6はトークンが使用されていることを知っている唯一のルータであり、2回目のトークンの使用を阻止できるからである。このトークンの使用に関する情報を有していない他のアクセスルータはDOS攻撃に気づかないおそれがある。これはアクセスルータ6がアクセスネットワーク内でのトークンの使用に関する情報を提供しなかったためである。ただしこの情報がアクセスネットワーク全体へ送信されるとアクセスネットワーク内のシグナリングトラフィックスがきわめて大きくなってしまう。

【0020】

図3、図4には、各アクセスルータが自身および2つの隣接するアクセスルータを少なくとも1つのトラストテーブルにエントリしてトークンの有効範囲を低減する様子が示されている。例えばアクセスルータ4は自身およびアクセスルータ1，6を少なくとも1つのトラストテーブルへ入力する。これにより当該のアクセスルータで作成されたトークンはこれらのアクセスルータ1，4，6のみによって受容される。アクセスルータ4はアクセスルータ1，6とのセキュリティアソシエーションを形成しており、各アクセスルータ1，4，6は自身らがどのトークンを受容するかを表す情報を有する少なくとも1つのトラストテーブル7を有している。

【0021】

移動無線端末機5は第1のアクセスルータ4で作成されたトークンを受け取り、これをイントラドメインハンドオーバーのために第2のアクセスルータ6へ送信する。トークンの検査の成功が識別されると、接続更新プロセスおよびAAAプロセスが開始される。第1のアクセスルータ4のトラストテーブル7に含まれていないアクセスルータ（例えばアクセスルータ1，4，6以外の全てのアクセスルータ）は既に使用されたトークンが反復して受け取られる危険を被らない。トークンを使用している第2のアクセスルータ6ももちろんこの使用について情報を有しているので、DOS攻撃があるとすればこのトークンを受容しうるアクセスルータ1，4のみがその危険を有することになる。

【0022】

図4には第2のアクセスルータ6がトークンを受容した後、情報をただちに当該のトークンを作成した第1のアクセスルータ4へ送信する様子が示されている。その後第1のアクセスルータ4はトラストテーブル内の第3のアクセスルータ1にこれを通知し、トークンのコピーが受容されないようにする。

【0023】

トークンの検査で偽と識別された場合には再登録プロセスは開始されないが、そうでない場合には接続更新プロセスおよび再登録プロセスが同時に開始される。再登録プロセスの問い合わせ（BUACKメッセージ）がセッションキー付きで第2のアクセスルータ6に到来すると、当該のアクセスルータ6はデジタル署名を検査する。このデジタル署名はモバイルノードによって作成されたものであり、QoS問い合わせの全伝搬時間にわ

10

20

30

40

50

たって再オーセンティケーションに関連するセッションキーを含む。トークンの検査で真と識別された場合には、図5に示されているように、第2のアクセスルータ6はセッションキーによって暗号化された新たなトークンを再登録プロセスの問い合わせ（BUACKメッセージ）に付加し、これを移動無線端末機5へ送信する。

【0024】

図6には第1のアクセスルータ4が処理ユニット11によりトークンを作成し、これを送信ユニット12を介して移動無線端末機5へ送信する様子が示されている。第2のアクセスルータ6で作成されたトークンは受信ユニット10を介して処理ユニット11へ供給され、さらに別のトラストテーブルへ送信される。各アクセスルータは少なくとも1つのトラストテーブル7を有している。第1のタイプのトラストテーブルすなわちトラステッドリストにはそのトークンを受け取るべきアクセスルータに関する情報が記憶され、第2のタイプのトラストテーブルすなわちトラスティングリストには作成したトークンを送るべきアクセスルータに関する情報が記憶される。第3のタイプのトラストテーブルには既に使用されたトークンが記憶される。ここには既に一度移動無線端末機で有効に使用された全てのトークンが記憶される。

10

【0025】

イントラドメインハンドオーバーが行われる際には、移動無線端末機5は再登録問い合わせにトークンを付加し、これをテキストとして新たなアクセスルータ6へ送信する。新たなアクセスルータ6は当該のトークンを受信ユニット10を介して受け取り、検査のために処理ユニット11へ供給する。処理ユニット11はトークンの検査のために次の3つの機能を実行する。すなわち

20

- 1) 当該のトークンの伝搬時点から有効期間を検査し、
- 2) 当該のトークンを作成したアクセスルータのIDをトラストテーブル7に照らして検査し、
- 3) 上述の検査が終了したのち当該のトークンのキーを用いてトークン情報を備えた乱数付加部分（キーハッシュドダイジェスト）を計算し、これと既存の乱数付加部分とを比較する。

【0026】

トークンの検査で真と識別された場合には、接続更新プロセスおよび再オーソリゼーションプロセスが開始される。新たなアクセスルータ6は再登録問い合わせ（BUACKメッセージ）に含まれているセッションキーをモバイルアンカーポイントMAPから受信ユニット10を介して受け取ったのち再登録問い合わせをオーセンティケーションする。認証が偽と識別された場合には、第2のアクセスルータ6は再登録問い合わせをもはや処理できない。所定の時間を過ぎても再登録についての応答をアクセスルータ6から得られない場合、移動無線端末機5はオーソリゼーションプロセスおよびオーセンティケーションプロセスをローカルAAAサーバおよびホームAAAサーバを介してイントラドメインハンドオーバーまたはスイッチオンの際と同様に開始しなければならない。

30

【図面の簡単な説明】

【0027】

【図1】最初のトークンを移動無線端末機へ送信する様子を示す図である。

40

【0028】

【図2】有効範囲の制限なしに、また他のアクセス装置での使用可能性の表示なしにトークンを送信する様子を示す図である。

【0029】

【図3】制限された有効範囲内での使用を示すインジケータなしでトークンを送信する様子を示す図である。

【0030】

【図4】トークンに制限された有効範囲内での使用を示すインジケータを付して送信する様子を示す図である。

【0031】

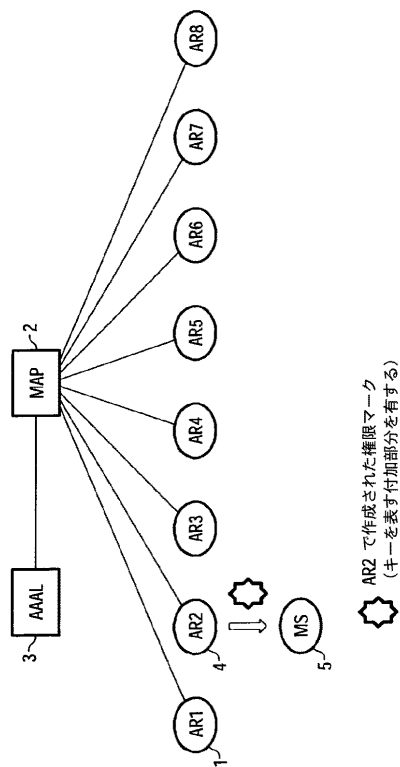
50

【図 5】イントラドメインハンドオーバ後にトークンを移動無線端末機へ送信する様子を示す図である。

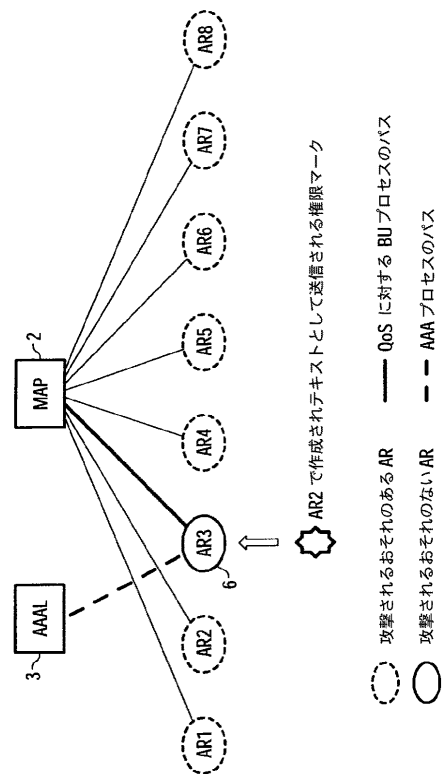
【0032】

【図 6】トークンを送信および検査する装置のブロック図である。

【図 1】



【図 2】



フロントページの続き

- (74)代理人 100094798
弁理士 山崎 利臣
- (74)代理人 100099483
弁理士 久野 琢也
- (74)代理人 100110593
弁理士 杉本 博司
- (74)代理人 100128679
弁理士 星 公弘
- (74)代理人 100135633
弁理士 二宮 浩康
- (74)代理人 100114890
弁理士 アインゼル・フェリックス＝ラインハルト
- (72)発明者 ティアンウェイ チェン
ドイツ連邦共和国 ベルリン トルフシュトラッセ 19
- (72)発明者 チャンペン ファン
ドイツ連邦共和国 ベルリン オットー＝ディクス＝シュトラッセ 7
- (72)発明者 ギュンター シェーファー
ドイツ連邦共和国 ベルリン トゥルムシュトラッセ 47

審査官 小河 誠巳

- (56)参考文献 国際公開第00/049827 (WO, A1)
特表2002-537739 (JP, A)
国際公開第01/022685 (WO, A1)
国際公開第01/037586 (WO, A1)
国際公開第01/078306 (WO, A1)
国際公開第02/041661 (WO, A1)
特開2001-203703 (JP, A)
特開2002-247652 (JP, A)
国際公開第00/079827 (WO, A1)

(58)調査した分野(Int.Cl., DB名)

H04W 4/00-99/00

H04B 7/24-7/26