(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4637185号
(P4637185)

(45)発行日　平成23年2月23日(2011.2.23)　(24)登録日　平成22年12月3日(2010.12.3)

(51)Int.Cl.　　F I
G06F 13/00 (2006.01)　　G06F 13/00 500A
H04W 12/06 (2009.01)　　H04Q 7/00 183

請求項の数 36　(全 16 頁)

(21)出願番号　特願2007-554663 (P2007-554663)
(86)(22)出願日　平成18年1月11日 (2006.1.11)
(65)公表番号　特表2008-532114 (P2008-532114A)
(43)公表日　平成20年8月14日 (2008.8.14)
(86)国際出願番号　PCT/IB2006/000041
(87)国際公開番号　WO2006/085170
(87)国際公開日　平成18年8月17日 (2006.8.17)
審査請求日　平成19年10月15日 (2007.10.15)
(31)優先権主張番号　60/652,633
(32)優先日　平成17年2月14日 (2005.2.14)
(33)優先権主張国　米国(US)

(73)特許権者　398012616
ノキア　コーポレイション
フィンランド　エフイーエンー０２１５０
エスプー　ケイララーデンティエ　４
(74)代理人　100127188
弁理士　川守田　光紀
(72)発明者　ペッカ　ラッチネン
フィンランド　ヘルシンキ　ＦＩＮ－００８００　ヒートマエンティエ　４４　Ａ　２
(72)発明者　フィリップ　ギンズボルグ
フィンランド　エスプー　ＦＩＮ－０２３６０　ヤカウピンクヤ　１　Ｂ　１０

審査官　北岡　浩

最終頁に続く

(54)【発明の名称】無線通信システム内の最適なデータ転送のための方法及び装置

(57)【特許請求の範囲】
【請求項１】
ＢＳＦ（ブートストラッピング・サーバ機能）を備える装置であって、
前記ＢＳＦは、第１のメッセージをＨＳＳ（ホーム加入者サーバ）に送信するように構成され、ここで前記第１のメッセージは、前記ＨＳＳに記憶されているＧＵＳＳ（汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定）に対応するタイムスタンプ・パラメータと比較されるべく、前記ＢＳＦに記憶されているＧＵＳＳに対応するタイムスタンプ・パラメータを含み、
前記ＢＳＦは、さらに、
前記ＢＳＦに記憶されているＧＵＳＳに対応する前記タイムスタンプ・パラメータと、前記ＨＳＳに記憶されているＧＵＳＳに対応する前記タイムスタンプ・パラメータとが等しい場合は、ＧＵＳＳを含まない第２のメッセージを前記ＨＳＳから受信し、
前記ＢＳＦに記憶されているＧＵＳＳに対応する前記タイムスタンプ・パラメータと、前記ＨＳＳに記憶されているＧＵＳＳに対応する前記タイムスタンプ・パラメータとが等しくない場合は、ＧＵＳＳおよび該ＧＵＳＳに対応するタイムスタンプ・パラメータを含む第２のメッセージを前記ＨＳＳから受信すると共に、前記受信したＧＵＳＳおよびタイムスタンプ・パラメータを用いて前記ＢＳＦを更新する、
ように構成され、前記ＢＳＦは、前記ＨＳＳと共に無線通信システムにおける認証機能を提供する、装置。
【請求項２】

特定のＧＵＳＳに対応する前記タイムスタンプ・パラメータは、同一のＧＵＳＳの一部となる、請求項１に記載の装置。

【請求項３】

前記第１のメッセージは、認証ベクトル（ＡＶ）要求を含む、請求項１に記載の装置。

【請求項４】

前記ＨＳＳは、前記タイムスタンプ・パラメータを前記ＧＵＳＳに割り当てるように構成されている、請求項１に記載の装置。

【請求項５】

前記ＨＳＳは、前記ＧＵＳＳのデータが修正された場合は、当該ＧＵＳＳの前記タイムスタンプ・パラメータを変更するように構成されている、請求項１に記載の装置。

【請求項６】

前記ＨＳＳは、前記ＧＵＳＳに関する前記タイムスタンプ・パラメータを単調増加順又は単調減少順で割り当てるように構成されている、請求項４に記載の装置。

【請求項７】

前記ＨＳＳは、前記ＧＵＳＳに関する前記タイムスタンプ・パラメータを、前記ＢＳＦ及び前記ＨＳＳの前記ＧＵＳＳの特定のインスタンスに関するハッシュとして又は前記ハッシュの一部として割り当てるように構成されている、請求項４に記載の装置。

【請求項８】

前記ＢＳＦは、前記タイムスタンプ・パラメータを、前記ＨＳＳに記憶されている前記タイムスタンプ・パラメータに由来する異なる数字又は英数字の形式で記憶するように構成されている、請求項１に記載の装置。

【請求項９】

前記ＢＳＦは、前記タイムスタンプ・パラメータを、前記ＨＳＳの前記タイムスタンプ・パラメータに由来する異なる数字又は英数字の形式で送信するように構成されている、請求項１に記載の装置。

【請求項１０】

前記タイムスタンプは、前記ＧＵＳＳが最初に作成されるときに、ある数値に初期化され、又は前記ＨＳＳ内のクロックによって指示される時間及び／又は日付を示す値に初期化される、請求項４に記載の装置。

【請求項１１】

前記ＧＵＳＳが修正されるたびに、前記ＧＵＳＳは新しいバージョンになり、前記タイムスタンプは１ずつ増分又は減分され、あるいは前記ＨＳＳ内のクロックによって指示される現在の時間及び／又は日付に変更される、請求項４に記載の装置。

【請求項１２】

前記ＧＵＳＳには、前記ＧＵＳＳの特定のインスタンスに関するハッシュに相当する又は当該ハッシュの一部に相当するタイムスタンプ値が割り当てられる、請求項４に記載の装置。

【請求項１３】

ＢＳＦ（ブートストラッピング・サーバ機能）からＨＳＳ（ホーム加入者サーバ）に第１のメッセージを送信すること、ここで前記第１のメッセージは、前記ＨＳＳに記憶されているＧＵＳＳ（汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定）に対応するタイムスタンプ・パラメータと比較されるべく、前記ＢＳＦに記憶されているＧＵＳＳに対応するタイムスタンプ・パラメータを含む、前記送信することと、

前記ＢＳＦに記憶されているＧＵＳＳに対応する前記タイムスタンプ・パラメータと、前記ＨＳＳに記憶されているＧＵＳＳに対応する前記タイムスタンプ・パラメータとが等しい場合は、ＧＵＳＳを含まない第２のメッセージを前記ＨＳＳから受信することと、

前記ＢＳＦに記憶されているＧＵＳＳに対応する前記タイムスタンプ・パラメータと、前記ＨＳＳに記憶されているＧＵＳＳに対応する前記タイムスタンプ・パラメータとが等しくない場合は、ＧＵＳＳおよび該ＧＵＳＳに対応するタイムスタンプ・パラメータを含む第２のメッセージを前記ＨＳＳから受信すると共に、前記受信したＧＵＳＳおよびタイ

ムスタンプ・パラメータを用いて前記ＢＳＦを更新することと、
を含み、ここで前記ＢＳＦは前記ＨＳＳと共に無線通信システムにおける認証機能を提供するものである、方法。
【請求項１４】
前記第１のメッセージを送信する前記ステップは、認証ベクトル（ＡＶ）要求を送信するステップを含む、請求項１３に記載の方法。
【請求項１５】
前記ＧＵＳＳに関する前記タイムスタンプ・パラメータを割り当てる前記ステップは、単調増加順又は単調減少順で実行される、請求項１３に記載の方法。
【請求項１６】
前記ＧＵＳＳに関する前記タイムスタンプ・パラメータを割り当てる前記ステップは、前記ＢＳＦ及び前記ＨＳＳの前記ＧＵＳＳの特定のインスタンスに関するハッシュとして又は前記ハッシュの一部として実行される、請求項１３に記載の方法。
【請求項１７】
前記ＢＳＦの前記タイムスタンプ・パラメータを、前記ＨＳＳに記憶されている前記タイムスタンプ・パラメータに由来する異なる数字又は英数字の形式で記憶するステップを更に含む、請求項１３に記載の方法。
【請求項１８】
前記ＢＳＦの前記タイムスタンプ・パラメータと、前記ＨＳＳのタイムスタンプ・パラメータとを異なる数字又は英数字の形式で送信するステップを更に含む、請求項１３に記載の方法。
【請求項１９】
異なる数字又は英数字の形式で送信された前記タイムスタンプ・パラメータをそれ自体の元の形式に変更するステップを更に含む、請求項１３に記載の方法。
【請求項２０】
前記タイムスタンプに単調増加順又は単調減少順で値を割り当てるステップを更に含む、請求項１３に記載の方法。
【請求項２１】
前記ＧＵＳＳが最初に作成されるときに、前記タイムスタンプをある数値に初期化し、又は前記ＨＳＳ内のクロックによって指示される時間及び／又は日付に初期化するステップを更に含む、請求項１３に記載の方法。
【請求項２２】
前記タイムスタンプを、前記ＧＵＳＳが修正されるたびに前記タイムスタンプの現在の時間及び／又は日付に変更するステップを更に含む、請求項１３に記載の方法。
【請求項２３】
前記ＧＵＳＳの特定のインスタンスに関するハッシュに相当する又は当該ハッシュの一部に相当するタイムスタンプ値を前記ＧＵＳＳに割り当てるステップを更に含む、請求項１３に記載の方法。
【請求項２４】
ＢＳＦ（ブートストラッピング・サーバ機能）を備える装置のプロセッサで実行されると、該装置に、
ＢＳＦ（ブートストラッピング・サーバ機能）からＨＳＳ（ホーム加入者サーバ）に第１のメッセージを送信すること、ここで前記第１のメッセージは、前記ＨＳＳに記憶されているＧＵＳＳ（汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定）に対応するタイムスタンプ・パラメータと比較されるべく、前記ＢＳＦに記憶されているＧＵＳＳに対応するタイムスタンプ・パラメータを含む、前記送信することと、
前記ＢＳＦに記憶されているＧＵＳＳに対応する前記タイムスタンプ・パラメータと、前記ＨＳＳに記憶されているＧＵＳＳに対応する前記タイムスタンプ・パラメータとが等しい場合は、ＧＵＳＳを含まない第２のメッセージを前記ＨＳＳから受信することと、
前記ＢＳＦに記憶されているＧＵＳＳに対応する前記タイムスタンプ・パラメータと、

前記ＨＳＳに記憶されているＧＵＳＳに対応する前記タイムスタンプ・パラメータとが等しくない場合は、ＧＵＳＳおよび該ＧＵＳＳに対応するタイムスタンプ・パラメータを含む第２のメッセージを前記ＨＳＳから受信すると共に、前記受信したＧＵＳＳおよびタイムスタンプ・パラメータを用いて前記ＢＳＦを更新することと、
を実行させるように構成され、ここで前記ＢＳＦは前記ＨＳＳと共に無線通信システムにおける認証機能を提供するものである、コンピュータ・プログラム。

【請求項２５】

前記第１のメッセージを送信する前記ステップは、認証ベクトル（ＡＶ）要求を送信するステップを含む、請求項２４に記載のコンピュータ・プログラム。

【請求項２６】

前記ＧＵＳＳに関する前記タイムスタンプ・パラメータを割り当てる前記ステップは、単調増加順又は単調減少順で実行される、請求項２４に記載のコンピュータ・プログラム。

【請求項２７】

前記ＧＵＳＳに関する前記タイムスタンプ・パラメータを割り当てる前記ステップは、前記ＢＳＦ及び前記ＨＳＳの前記ＧＵＳＳの特定のインスタンスに関するハッシュとして又は前記ハッシュの一部として実行される、請求項２４に記載のコンピュータ・プログラム。

【請求項２８】

前記ＢＳＦの前記タイムスタンプ・パラメータを、前記ＨＳＳに記憶されている前記タイムスタンプ・パラメータに由来する異なる数字又は英数字の形式で記憶するステップを更に含む、請求項２４に記載のコンピュータ・プログラム。

【請求項２９】

前記ＢＳＦの前記タイムスタンプ・パラメータと、前記ＨＳＳのタイムスタンプ・パラメータとを異なる数字又は英数字の形式で送信するステップを更に含む、請求項２４に記載のコンピュータ・プログラム。

【請求項３０】

前記タイムスタンプに単調増加順又は単調減少順で値を割り当てるステップを更に含む、請求項２４に記載のコンピュータ・プログラム。

【請求項３１】

前記ＧＵＳＳが最初に作成されるときに、前記タイムスタンプをある数値に初期化し、又は前記ＨＳＳ内のクロックによって指示される時間及び／又は日付に初期化するステップを更に含む、請求項２４に記載のコンピュータ・プログラム。

【請求項３２】

前記タイムスタンプを、前記ＧＵＳＳが修正されるたびに現在の時間及び／又は日付に変更するステップを更に含む、請求項２４に記載のコンピュータ・プログラム。

【請求項３３】

前記ＧＵＳＳの特定のインスタンスに関するハッシュに相当する又は当該ハッシュの一部に相当するタイムスタンプ値を前記ＧＵＳＳに割り当てるステップを更に含む、請求項２４に記載のコンピュータ・プログラム。

【請求項３４】

通信システムであって、

ネットワーク・アプリケーション機能（ＮＡＦ）と、

前記ネットワーク・アプリケーション機能と通信し、認証情報要求を送信するように構成されたユーザ機器と、

前記要求を受信することに応じて第１のメッセージを送信するように構成されるＢＳＦ（ブートストラッピング・サーバ機能）、ただし前記第１のメッセージは、前記ＢＳＦに記憶されているＧＵＳＳ（汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定）に対応するタイムスタンプ・パラメータを含むメッセージである、前記ＢＳＦと、

前記第１のメッセージを受信するように構成されるＨＳＳ（ホーム加入者サーバ）であって、前記第１のメッセージに含まれる、前記ＢＳＦに対応する前記タイムスタンプ・パラメータと、前記ＨＳＳに記憶されているＧＵＳＳに対応するタイムスタンプ・パラメータとを比較し、前記ＢＳＦに記憶されているＧＵＳＳに対応する前記タイムスタンプ・パラメータと、前記ＨＳＳに記憶されているＧＵＳＳに対応する前記タイムスタンプ・パラメータとが等しい場合は、ＧＵＳＳを含まない第２のメッセージを前記ＢＳＦに送り返すように構成される、前記ＨＳＳと、
を備え、ここで前記ＢＳＦは前記ＨＳＳと共に無線通信システムにおける認証機能を提供する通信システム。
【請求項３５】
ＢＳＦ（ブートストラッピング・サーバ機能）からＨＳＳ（ホーム加入者サーバ）に第１のメッセージを送信する手段、ここで前記第１のメッセージは、前記ＨＳＳに記憶されているＧＵＳＳ（汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定）に対応するタイムスタンプ・パラメータと比較されるべく、前記ＢＳＦに記憶されているＧＵＳＳに対応するタイムスタンプ・パラメータを含む、前記送信する手段と、
前記ＢＳＦに記憶されているＧＵＳＳに対応する前記タイムスタンプ・パラメータと、前記ＨＳＳに記憶されているＧＵＳＳに対応する前記タイムスタンプ・パラメータとが等しい場合は、ＧＵＳＳを含まない第２のメッセージを前記ＨＳＳから受信する手段と、
前記ＢＳＦに記憶されているＧＵＳＳに対応する前記タイムスタンプ・パラメータと、前記ＨＳＳに記憶されているＧＵＳＳに対応する前記タイムスタンプ・パラメータとが等しくない場合は、ＧＵＳＳおよび該ＧＵＳＳに対応するタイムスタンプ・パラメータを含む第２のメッセージを前記ＨＳＳから受信すると共に、前記受信したＧＵＳＳおよびタイムスタンプ・パラメータを用いて前記ＢＳＦを更新する手段と、
を備え、ここで前記ＢＳＦは前記ＨＳＳと共に無線通信システムにおける認証機能を提供するものである、装置。
【請求項３６】
ＨＳＳ（ホーム加入者サーバ）を備える装置であって、前記ＨＳＳが、
ＢＳＦ（ブートストラッピング・サーバ機能）に記憶されているＧＵＳＳ（汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定）に対応するタイムスタンプ・パラメータを含む第１のメッセージを受信すると共に、
第１のメッセージに含まれる前記タイムスタンプ・パラメータと、前記ＨＳＳに記憶されているＧＵＳＳに対応するタイムスタンプ・パラメータとを比較し、
前記ＢＳＦのＧＵＳＳに対応する前記タイムスタンプ・パラメータと、前記ＨＳＳのＧＵＳＳに対応する前記タイムスタンプ・パラメータとが等しい場合は、ＧＵＳＳを含まない第２のメッセージを前記ＢＳＦへ送信し、
前記ＢＳＦのＧＵＳＳに対応する前記タイムスタンプ・パラメータと、前記ＨＳＳのＧＵＳＳに対応する前記タイムスタンプ・パラメータとが等しくない場合は、ＧＵＳＳおよび該ＧＵＳＳに対応するタイムスタンプ・パラメータを含む第２のメッセージを前記ＢＳＦへ送信する、
ように構成され、前記ＨＳＳは、前記ＢＳＦと共に無線通信システムにおける認証機能を提供する、装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、保護されたデータを通信システム内の各機能及び要素間で共有する装置及び方法に関するものであり、特に、安全なデータの有効性を判定した後に、当該判定結果に基づいて当該データを共有する装置及び方法に関するものである。
【背景技術】
【０００２】
近年、通信システム、より具体的には無線通信システムは、世界中の大部分の人々に利

用され、益々身近なものになっている。そのような無線通信システムの成功によって、一方では加入者数の急激な増加に対処することが必要とされている。加入者数の急激な増加に対処する必要を満たす１つの方法は、拡張可能な無線通信システムを実現するものである。別の方法は、無線通信システムを構成する各要素及び機能を最適化するものである。その結果、通信システム・アーキテクチャの枠組みは拡大の一途を辿っている。

【０００３】

拡大の一途を辿る領域の１つは、無線通信システムにおける認証アーキテクチャである。無線通信システムにおいて、いくつかのアプリケーションは共通して、更なる通信を行う上でクライアント／ユーザ機器（ＵＥ）とアプリケーション／アプリケーション・サーバとの間の相互認証を必要とする。その例としては、必ずしもそれだけに限定されるわけではないが、クライアントとプレゼンス・サーバとの間の通信又はコンテンツ・サーバとの間の通信が挙げられる。多くのアプリケーションは共通してこのようなピア認証の仕組みを必要とすることから、一般認証アーキテクチャ（Ｇｅｎｅｒｉｃ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ａｒｃｈｉｔｅｃｔｕｒｅ：ＧＡＡ）が開発された。

【０００４】

第３世代パートナーシップ・プロジェクト（３ＧＰＰ）の一般認証アーキテクチャ（ＧＡＡ）の初期認証（即ち、ブートストラッピング）は、ＡＫＡ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｋｅｙ Ａｇｒｅｅｍｅｎｔ Ｐｒｏｔｏｃｏｌ：認証付き鍵交換プロトコル）に基づいている。ＧＡＡアーキテクチャは、第３世代パートナーシップ・プロジェクト（３ＧＰＰ）作成の文書に記載されている。当該文書は、付属書類Ａとして本明細書に添付した３ＧＰＰ ＴＳ ３３．９１９：「３ｒｄ Ｇｅｎｅｒａｔｉｏｎ Ｐａｒｔｎｅｒｓｈｉｐ Ｐｒｏｊｅｃｔ；Ｔｅｃｈｎｉｃａｌ Ｓｐｅｃｉｆｉｃａｔｉｏｎ Ｇｒｏｕｐ Ｓｅｒｖｉｃｅｓ ａｎｄ Ｓｙｓｔｅｍ Ａｓｐｅｃｔｓ；３Ｇ ｓｅｃｕｒｉｔｙ；Ｇｅｎｅｒｉｃ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ａｒｃｈｉｔｅｃｔｕｒｅ（ＧＡＡ）；Ｓｙｓｔｅｍ ｄｅｓｃｒｉｐｔｉｏｎ」であり、その内容を参考として本明細書に援用する。

【０００５】

ＧＡＡの特筆すべき側面の１つは、クライアント／ＵＥ及びアプリケーション／アプリケーション・サーバに共通の共有シークレットが提供される、アプリケーションに依存しない仕組みが含まれている点である。当該共有シークレットを使用すると、クライアント／ユーザ機器とアプリケーション／アプリケーション・サーバとの間の無線通信の認証を行うことができる。この側面については第３世代パートナーシップ・プロジェクト（３ＧＰＰ）作成の次の文書、即ち、付属書類Ｂとして本明細書に添付した３ＧＰＰ ＴＳ ３３．２２０：「３ｒｄ Ｇｅｎｅｒａｔｉｏｎ Ｐａｒｔｎｅｒｓｈｉｐ Ｐｒｏｊｅｃｔ；Ｔｅｃｈｎｉｃａｌ Ｓｐｅｃｉｆｉｃａｔｉｏｎ Ｇｒｏｕｐ Ｓｅｒｖｉｃｅｓ ａｎｄ Ｓｙｓｔｅｍ Ａｓｐｅｃｔｓ；３Ｇ ｓｅｃｕｒｉｔｙ；Ｇｅｎｅｒｉｃ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ａｒｃｈｉｔｅｃｔｕｒｅ（ＧＡＡ）；Ｇｅｎｅｒｉｃ ｂｏｏｔｓｔｒａｐｐｉｎｇ ａｒｃｈｉｔｅｃｔｕｒｅ（Ｒｅｌｅａｓｅ ７）」、及び付属書類Ｃとして本明細書に添付した３ＧＰＰ ＴＳ ２９．１０９：「３ｒｄ Ｇｅｎｅｒａｔｉｏｎ Ｐａｒｔｎｅｒｓｈｉｐ Ｐｒｏｊｅｃｔ；Ｔｅｃｈｎｉｃａｌ Ｓｐｅｃｉｆｉｃａｔｉｏｎ Ｇｒｏｕｐ Ｃｏｒｅ Ｎｅｔｗｏｒｋｓ ａｎｄ Ｔｅｒｍｉｎａｌｓ；Ｇｅｎｅｒｉｃ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ａｒｃｈｉｔｅｃｔｕｒｅ （ＧＡＡ）；Ｚｈ ａｎｄ Ｚｎ Ｉｎｔｅｒｆａｃｅｓ ｂａｓｅｄ ｏｎ ｔｈｅ Ｄｉａｍｅｔｅｒ ｐｒｏｔｏｃｏｌ；Ｓｔａｇｅ ３（Ｒｅｌｅａｓｅ ７）」にそれぞれ記載されており、これらの内容も参考として本明細書に援用する。

【発明の開示】

【０００６】

本発明の一実施形態によれば、通信システム内のデータを共有する装置であって、それ自体に記憶されている汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定（ｇｅｎｅｒｉｃ ｂｏｏｔｓｔｒａｐｐｉｎｇ ａｒｃｈｉｔｅｃｔｕｒｅ ｕ

ｓｅｒ ｓｅｃｕｒｉｔｙ ｓｅｔｔｉｎｇｓ：ＧＵＳＳ）に対応するタイムスタンプ・パラメータを含む第１のメッセージを送信するように構成されたサーバ・ブートストラッピング機能（ＢＳＦ）を含む装置が提供される。ホーム加入者サーバ（ＨＳＳ）は、前記第１のメッセージを受信し、前記ＢＳＦに記憶されている前記ＧＵＳＳに対応する前記タイムスタンプ・パラメータと、それ自体に記憶されているＧＵＳＳに対応するタイムスタンプ・パラメータとを比較し、前記ＢＳＦの前記ＧＵＳＳに関する前記タイムスタンプ・パラメータと、それ自体の前記ＧＵＳＳに関する前記タイムスタンプ・パラメータとが等しい場合は、前記ＧＵＳＳを含まない第２のメッセージを前記ＢＳＦに送り返すように構成されている。

【０００７】

本発明の一実施形態によれば、通信システム内のデータを共有する方法であって、サーバ・ブートストラッピング機能（ＢＳＦ）に記憶されている汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定（ＧＵＳＳ）に対応するタイムスタンプ・パラメータを含む第１のメッセージを、前記ＢＳＦからホーム加入者サーバ（ＨＳＳ）に送信するステップと、前記ＢＳＦに記憶されている前記ＧＵＳＳに対応する前記タイムスタンプ・パラメータと、前記ＨＳＳに記憶されているＧＵＳＳに対応するタイムスタンプ・パラメータとを比較するステップと、前記ＢＳＦの前記ＧＵＳＳに関する前記タイムスタンプ・パラメータと、前記ＨＳＳの前記ＧＵＳＳに関する前記タイムスタンプ・パラメータとが等しい場合は、前記ＧＵＳＳを含まない第２のメッセージを前記ＢＳＦに送り返すステップと、を含む方法が提供される。

【０００８】

本発明の一実施形態によれば、コンピュータ可読媒体内に実装され、通信システム内のデータ共有を実現するコンピュータ・プログラムであって、サーバ・ブートストラッピング機能（ＢＳＦ）に記憶されている汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定（ＧＵＳＳ）に対応するタイムスタンプ・パラメータを含む第１のメッセージを、前記ＢＳＦからホーム加入者サーバ（ＨＳＳ）に送信するステップと、前記ＢＳＦに記憶されている前記ＧＵＳＳに対応する前記タイムスタンプ・パラメータと、前記ＨＳＳに記憶されているＧＵＳＳに対応するタイムスタンプ・パラメータとを比較するステップと、前記ＢＳＦの前記ＧＵＳＳに関する前記タイムスタンプ・パラメータと、前記ＨＳＳの前記ＧＵＳＳに関する前記タイムスタンプ・パラメータとが等しい場合は、前記ＧＵＳＳを含まない前記第２のメッセージを前記ＢＳＦに送り返すステップと、を含むコンピュータ・プログラムが提供される。

【０００９】

本発明の一実施形態によれば、装置、通信システムであって、ネットワーク・アプリケーション機能（ＮＡＦ）と、前記ＮＡＦと通信し、認証情報要求を送信するように構成されたユーザ機器と、前記要求を受信し、第１のメッセージを送信するように構成されたサーバ・ブートストラッピング機能（ＢＳＦ）と、を備える装置、通信システムが提供される。前記第１のメッセージは、前記ＢＳＦに記憶されている汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定（ＧＵＳＳ）に対応するタイムスタンプ・パラメータを含む。ホーム加入者サーバ（ＨＳＳ）は、前記第１のメッセージを受信し、前記ＢＳＦに記憶されている前記ＧＵＳＳに対応する前記タイムスタンプ・パラメータと、それ自体に記憶されているＧＵＳＳに対応するタイムスタンプ・パラメータとを比較し、前記ＢＳＦの前記ＧＵＳＳに関する前記タイムスタンプ・パラメータと、それ自体の前記ＧＵＳＳに関する前記タイムスタンプ・パラメータとが等しい場合は、前記ＧＵＳＳを含まない第２のメッセージを前記ＢＳＦに送り返すように構成されている。

本発明の更なる理解を与えるために添付される添付図面は、本明細書に組み込まれその一部を形成し、本発明の諸実施形態を図示するものであり、本明細書と併せてこれらの諸実施形態を利用することにより、本発明の諸原理を説明する。

【発明を実施するための最良の形態】

【００１０】

次に、本発明について、本発明のすべてではなく一部の諸実施形態が示される添付図面を参照しながらより詳細に説明する。本発明は実際には様々な形で実施することができ、本明細書に記載の諸実施形態に限定されるものと解釈されるべきではない。これらの実施形態はむしろ、適用され得る法上の要件を本開示によって満足させるために与えるものである。図面全体を通じて同様の参照番号は同様の要素を指す。

【００１１】

３ＧＰＰ　ＧＢＡは、（各内容を参考として本明細書に援用する、付属書類Ｂとして本明細書に添付した３ＧＰＰ　ＴＳ　３３．２２０、及び付属小類Ｃとして本明細書に添付した３ＧＰＰ　ＴＳ　２９．２０９で）提案される認証インフラストラクチャである。このインフラストラクチャは、ネットワーク・サイド及びユーザ・サイドが通信を行うことができない状況でも、このインフラストラクチャを利用することにより、ネットワーク・サイド及びユーザ・サイドのアプリケーション機能の通信を可能にすることができる。このような機能は「アプリケーション・セキュリティのブートストラッピング」と呼ばれ、より一般的には単に「ブートストラッピング」と呼ばれる。

【００１２】

ブートストラッピングの一般原理は、一般的なサーバ・ブートストラッピング機能（ｂｏｏｔｓｔｒａｐｐｉｎｇ　ｓｅｒｖｅｒ　ｆｕｎｃｔｉｏｎ：ＢＳＦ）によって当該機能とユーザ機器（ＵＥ）との間の認証及びセッション鍵の交換を実現することである。そのような認証は、認証付き鍵交換プロトコル（ＡＫＡ）に基づいて行われることもある。ＡＫＡを実行することによってモバイル端末とネットワークとが相互に認証を行い、各鍵の交換、特に機密鍵（ｃｏｎｆｉｄｅｎｔｉａｌｉｔｙ　ｋｅｙ：ＣＫ）及びインテグリティ鍵（ｉｎｔｅｇｒｉｔｙ　ｋｅｙ：ＩＫ）の交換を行う。この認証が行われた後に、ＵＥ及びサービス・プロバイダと呼ばれることもあるネットワーク・アプリケーション機能（ＮＡＦ）は、メッセージ認証がＵＥとＢＳＦとの間で交換されるセッション鍵に基づいて行われる、アプリケーション特有の何らかのプロトコルを実行することができる。

【００１３】

上記のブートストラッピング機能は、何らかの特定のネットワーク・アプリケーション機能に依存するものではない。ブートストラッピング機能が実装されたサーバは、認証ベクトルを取り扱うホーム・オペレータから信頼されるものでなければならない。ネットワーク・アプリケーション機能は、オペレータのホーム・ネットワーク、訪問ネットワーク、あるいは第３のネットワークでサポートすることができる。

【００１４】

図１は、本発明の一実施形態に係る例示的なネットワーク・アーキテクチャを示している。このネットワーク・アーキテクチャは、ユーザ機器（ＵＥ）１００と、少なくとも１つのネットワーク・アプリケーション機能（ＮＡＦ）１０２と、サーバ・ブートストラッピング機能（ＢＳＦ）１０４と、ホーム加入者システム（ＨＳＳ）１０６とを含む。ＢＳＦ　１０４及びＨＳＳ　１０６は、ホーム・モバイル・ネットワーク・オペレータ（ＭＮＯ）１０８の一部を形成している。ＵＥ　１００は、周知のモバイル通信技法に従ってＭＮＯ　１０８に接続される。

【００１５】

例えば、ＮＡＦ　１０２はＭＮＯ　１０８の制御下で、あるネットワーク要素内でホストされ、ＢＳＦ　１０４もまたＭＮＯ　１０８の制御下で、あるネットワーク要素内でホストされ得る。したがって、事実上、ＮＡＦ　１０２とＢＳＦ　１０４はそれぞれネットワーク要素と見なすことができる。更に、ＭＮＯ　１０８は、図３Ａ及び図３Ｂに記載される処理を実行するコントローラ（図示せず）を含むこともできる。当該コントローラは、本発明のプロセス及びデータ構造を記憶し分散させることが可能な磁気ディスク、光ディスク、ＲＡＭ、ＲＯＭ等の永久記憶装置又は取外し可能な記憶装置を含むことができる。

【００１６】

図１に示されるように、ＵＥ　１００は、Ｕａインターフェイス１１０を介してＮＡＦ

１０２と通信する。ＵＥ　１００は、Ｕｂインターフェイス１１２を介してＢＳＦ　１０４と通信する。ＮＡＦ　１０２は、Ｚｎインターフェイス１１４を介してＢＳＦ　１０４と通信する。ＢＳＦ　１０４は、Ｚｈインターフェイス１１６を介してＨＳＳ　１０６と通信する。

【００１７】

ＮＡＦ　１０２は、別個のネットワーク内に設けられてもよい。例えば、図１に示されるように、ＮＡＦ　１０２が訪問ネットワーク内に所在する例示的なネットワーク・アーキテクチャが提供される。ＵＥ　１００がホーム・ネットワークとは別のネットワークで処理されるＮＡＦ　１０２とやり取りしている場合は、当該訪問される側のＮＡＦ　１０２は、ＮＡＦネットワークのダイアメータ・プロキシ（Ｄ‐プロキシ）を使用して加入者のＢＳＦ（即ち、ホームＢＳＦ）１０４と通信することができる。次に、ＮＡＦ　１０２は、Ｄ‐プロキシへと通じるＺｎインターフェイス１１４と、ＢＳＦ　１０４へと通じるＺｎインターフェイス１２０とを介してＢＳＦ　１０４と通信する。

【００１８】

図１では、ブートストラッピングの原理は、ＵＥ　１００とサーバ・ブートストラッピング機能とが例えばＡＫＡプロトコルを使用して相互に認証を行い、マスタ共有シークレット（ｍａｓｔｅｒ　ｓｈａｒｅｄ　ｓｅｃｒｅｔ）を交換することである。その後、マスタ共有シークレットを使用して１つ又は複数のネットワーク・アプリケーション機能に特有の共有シークレットが導出され、それらのシークレットは、ＵＥ　１００と該当する特定のＮＡＦとの間で適用される。具体的には、ＮＡＦ特有の共有秘密鍵素材が各ネットワーク・アプリケーション機能毎に個別に生成される。ブートストラッピング処理が完了した後、ＵＥ　１００及びネットワーク・アプリケーション機能は、メッセージの安全化がＵＥ　１００とサーバ・ブートストラッピング機能との間の相互認証中に生成される鍵に基づいて行われる、いくつかの特有のプロトコルを実行することができる。かくして、各鍵を使用して認証及びインテグリティ保護ならびに機密性を実現することができる。次に、ネットワーク・アプリケーション機能は、ユーザ機器とサーバ・ブートストラッピング機能との間で確立されたマスタ共有シークレットから導出されるＮＡＦ特有の共有シークレットを取得することができる。

【００１９】

更に、通信Ｕｂインターフェイス１１２は、ＵＥ　１００とＢＳＦ　１０４との間の相互認証及び鍵交換を実現する、ブートストラッピング認証及び鍵交換プロトコルをサポートする。Ｚｈインターフェイス１１６を用いると、ＢＳＦ　１０４が必要な認証情報及び加入者プロファイル情報（例えば認証ベクトル（ＡＶ））をＨＳＳ　１０６から取り出すことが可能となる。加入者のユーザ・セキュリティ設定（ＵＳＳ）セットは、ＨＳＳに記憶可能な加入者のＧＵＳＳの一部となる。１人の人物が複数の加入物を有する場合、即ち、複数のＩＰマルチメディア・サブシステム加入者識別モジュール・カード（ＩＳＩＭ）を有する場合、又はユニバーサル移動電話システム集積回路カード（ＵＩＣＣ）上の複数の汎用加入者識別モジュール・アプリケーションを有する場合には、１つ又は複数の任意の識別子、例えばＩＰマルチメディア・プライベート識別子（ＩＭＰＩ）や国際移動体加入者識別子（ＩＭＳＩ）等とマッピング可能な１つ又は複数のＧＵＳＳが、ＨＳＳ　１０６に収容されることになる。Ｕａインターフェイス１１０は、Ｕｂインターフェイス１１２によってサポートされるプロトコルに基づいて、ＵＥ　１００とＢＳＦ　１０４との間で交換されるマスタ共有シークレットから導出されたＮＡＦ特有の共有シークレットを使用して安全化される、アプリケーション特有の任意のプロトコルをサポートする。Ｚｎインターフェイス１１４は、Ｕｂインターフェイス１１２上でサポートされるプロトコルで交換されるマスタ共有シークレットから導出されたＮＡＦ特有の共有シークレットをＢＳＦ　１０４から取り出すためにＮＡＦ　１０２によって使用されるものである。Ｚｎインターフェイス１１４は、加入者プロファイル情報をＢＳＦ　１０４から取り出すのに使用することもできる。

【００２０】

ＢＳＦ　１０４からＮＡＦ　１０２に送信されるメッセージとしては、ブートストラッピング情報が挙げられる。ブートストラッピング情報は、トランザクション識別子、ＮＡＦ特有の共有シークレット、及び加入者プロファイル情報（「ｐｒｏｆ＿ｎａｆ」又は「ａｎｙ　ＮＡＦ　ｓｐｅｃｉｆｉｃ　ＵＳＳｓ」）を含むことができる。

【００２１】

更に、１組の汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定（ＧＵＳＳ）は、ブートストラッピング情報に含めることも、すべてのアプリケーションに特有の１組のＵＳＳに含めることもできる。典型的には、ＢＳＦは特定の加入者に関するＡＶを要求した後は、要求したＡＶと共に加入者のＧＵＳＳも受信する。動作中のある時点で、ＢＳＦ　１０４は、ＢＳＦ　１０４からのＨＳＳインターフェイスの１つであるＺｈを介して単一の認証ベクトル（ＡＶ）をＨＳＳ　１０６から検索することができ、それによって、ＢＳＦ　１０４は、ＵＥ　１００によってブートストラッピングされたときに、それ自体に記憶されているＧＵＳＳをＨＳＳ　１０６からのＧＵＳＳの新しいコピーで更新できるようになる。したがって、ＮＡＦ　１０２は、更新済みのＵＳＳ又は複数のＵＳＳをＢＳＦ　１０４から取得する必要がある場合は、ＵＥ　１００に対してＢＳＦ　１０４をブートストラッピングする、即ちＢＳＦ　１０４とネゴシエートするよう要求する必要があり、次回ＢＳＦ　１０４に特定のＵＳＳを要求したときは、ＧＵＳＳが最新のものであることを認識することになる。

【００２２】

しかしながら、この更新手続きによって、ＨＳＳ　１０６は、ＢＳＦ　１０４がＧＵＳＳを最後に受信した時点から当該ＧＵＳＳの更新状態が維持されているかどうかに関わらず、新しいＡＶが要求されるたびにＧＵＳＳを送信することを強いられる。更新手続き中はＡＶがＧＵＳＳと共に送信されるが、ＧＵＳＳのサイズは非常に大きくなる可能性がある故に、ＢＳＦ　１０４とＨＳＳ　１０６との間のトラフィック負荷は大きくなる。ＢＳＦ　１０４が既に同一のＧＵＳＳのコピーを有する場合にまでＧＵＳＳをＢＳＦ　１０４に送信する必要はなく、これによって帯域幅及びコンピュータ資源が浪費されることになる。したがって、ＨＳＳ　１０６からＢＳＦ　１０４にＧＵＳＳを転送する回数を最小限に抑える必要がある。

【００２３】

このため、本発明の装置及び方法は、ＧＵＳＳがタイムスタンプを含むように構成し、当該ＧＵＳＳをＨＳＳ　１０６からＢＳＦ　１０４に送信して、ＢＳＦ　１０４とＨＳＳ　１０６との間のＧＵＳＳの転送手続きに関するトラフィック負荷を最小限に抑えるようにしている。したがって、本発明の装置及び方法を用いると、安全なデータの有効性を判定した後に、当該判定結果に基づいて当該データを共有することにより、通信システム内の各機能及び要素間での安全なデータ共有が可能となる。

【００２４】

本発明の諸実施形態によれば、送信側即ち発信側ネットワーク要素内のデータ、例えばＧＢＡにおけるＨＳＳ　１０６内のデータは、要求側即ち受信側ネットワーク要素、例えばＧＢＡにおけるＢＳＦ　１０４が、送信側即ち発信側ネットワーク要素上に存在するデータと全く同じデータのコピーを有さない場合、又は当該データへのアクセス権を有さない場合にのみ、要求側即ち発信側ネットワーク要素に転送され、又は当該要素と共有される。

【００２５】

したがって、各ＧＵＳＳには、ＨＳＳ　１０６によって当該ＧＵＳＳが最後に変更された時点を示すＧＵＳＳタイムスタンプが追加される。当該タイムスタンプを使用してＨＳＳ　１０６とＢＳＦ　１０４との間のＧＵＳＳ転送ポリシーが最適化される。ＢＳＦ　１０４は、加入者に関する新しい認証ベクトル（ＡＶ）を検索する必要が生じた場合に、当該加入者のＧＵＳＳがメモリ内に存在するならば、ＡＶ要求にもＧＵＳＳタイムスタンプを含めることになる。ＨＳＳ　１０６は、当該ＧＵＳＳタイムスタンプを受信すると、当該ＧＵＳＳタイムスタンプと、それ自体のデータベースに記憶されているＧＵＳＳのタイ

ムスタンプとを比較する。２つのタイムスタンプ同士が等しい場合には、ＢＳＦ　１０４が既に当該ＧＵＳＳのコピーを有することになるので、当該ＧＵＳＳがＨＳＳ　１０６からＢＳＦ　１０４に送信されることはない。２つのタイムスタンプ同士が等しくない場合には、ＢＳＦ　１０４が更新する必要がある無効なＧＵＳＳを有することになるので、ＨＳＳ　１０６からＧＵＳＳが送信される。例えば、ＨＳＳ　１０６の管理インターフェイスを使用してＧＵＳＳが削除されたことでＨＳＳ　１０６内にＧＵＳＳが存在しない場合には、ＨＳＳ　１０６は「ｎｏ　ＧＵＳＳ」メッセージをＢＳＦ　１０４に送信し、ＢＳＦ　１０４によって古いＧＵＳＳが削除される。

【００２６】

図２は、本発明の一実施形態に係るＧＵＳＳタイムスタンプを含めたＢＳＦ　１０４とＨＳＳ　１０６との間の通信の様子を示している。処理１５０で、ＵＥ　１００は、ＵＥ　１００に関するユーザ識別子情報を含む新しいブートストラッピング要求を発行する。処理１５２で、ＢＳＦ　１０４がＨＳＳ　１０６から新しいＡＶを検索し、又はＨＳＳ　１０６に新しいＡＶを要求するときに、ＧＵＳＳが既にＢＳＦ　１０４のメモリ（即ち、ＢＳＦメモリ）内に存在し、又は当該メモリに記憶されているならば、新しいＡＶ要求にもＧＵＳＳタイムスタンプが含められることになる。ＨＳＳ　１０６はＧＵＳＳタイムスタンプを受信すると、当該ＧＵＳＳタイムスタンプをチェックし、当該ＧＵＳＳタイムスタンプと、ＨＳＳ　１０６自体に設けられたメモリ（即ち、ＨＳＳメモリ）に記憶されているＧＵＳＳタイムスタンプとを比較する。処理１５４で、ＢＳＦ　１０４から受信されたＧＵＳＳタイムスタンプと、ＨＳＳ　１０６に記憶されているＧＵＳＳタイムスタンプとが異なる場合には、ＨＳＳ　１０６は、更新済みのＧＵＳＳと、当該更新済みのＧＵＳＳに関するＧＵＳＳタイムスタンプと、要求された新しいＡＶとを含んでいることになる。２つのＧＵＳＳタイムスタンプ同士が同一である場合、即ち、ＢＳＦ　１０４のメモリ内のＧＵＳＳと、ＨＳＳ　１０６のメモリ内のＧＵＳＳとが同一である場合には、ＧＵＳＳが要求された新しいＡＶと共にＢＳＦ　１０４に送信されることはない。

【００２７】

無論、ＧＵＳＳタイムスタンプは、ＢＳＦ　１０４がそれ自体のメモリ内に特定の加入者に関するＧＵＳＳを有する場合にのみ、ＢＳＦ　１０４からＨＳＳ　１０６に送信することができる。この場合、ＧＵＳＳタイムスタンプがＨＳＳ　１０６に送信されることはなく、ＨＳＳ　１０６は、それ自体のデータベースから加入者特有のＧＵＳＳを取り出してＢＳＦ　１０４に送り返す。

【００２８】

処理１５６で、ＢＳＦ　１０４は、ＵＥ　１００にＢＳＦ　１０４自体の認証を求めるメッセージの形でランダム・チャレンジ・データ（ＲＡＮＤ）と認証トークン（ＡＵＴＮ）とをＵＥ　１００に転送する。処理１５８で、ＵＥ　１００に関連するクライアントは、認証付き鍵交換プロトコル（ＡＫＡ）アルゴリズムを実行し、ＡＵＴＮを検証し、認証結果（ＲＥＳ）を導出する。ＵＥ　１００は、機密鍵（ＣＫ）、インテグリティ鍵（ＩＫ）、及びＲＥＳの計算も行い、その結果、ＢＳＦ　１０４とＵＥ　１００の両方に所在するセッション鍵ＩＫ及びＣＫが同一のものとされる。処理１６０で、ＵＥ　１００は、ＲＥＳを使用して計算されたＡＫＡ応答を含むハイパーテキスト転送プロトコル（ＨＴＴＰ）要求をＢＳＦ　１０４に送信する。処理１６２で、ＢＳＦ　１０４は、ＡＫＡ応答を検証することによってＵＥ　１００を認証する。処理１６４で、ＢＳＦ　１０４は、ＣＫとＩＫを連結することによって鍵素材（Ｋｓ）を生成する。処理１６６で、ＢＳＦ　１０４は、ＯＫメッセージ、ブートストラッピング・トランザクション識別子（Ｂ‐ＴＩＤ）、及び鍵Ｋｓの寿命をＵＥ　１００に送信して、認証が成功したことを指示する。更に、処理１６８で、ＵＥ　１００は、ＢＳＦ　１０４が処理１６４で鍵素材を生成したのと同様の手法で鍵素材（Ｋｓ）を生成し、Ｋｓ、Ｂ‐ＴＩＤ、及びＫｓの寿命を記憶する。

【００２９】

したがって、ＨＳＳ　１０６内の各ＧＵＳＳは、例えばＧＵＳＳＴＩＭＥＳＴＡＭＰと標示される新しいタイムスタンプ・パラメータを含む。ＧＵＳＳのＧＵＳＳＴＩＭＥＳＴ

ＡＭＰは、ＨＳＳ　１０６によって設定され、ＨＳＳ　１０６によって当該ＧＵＳＳが最後に修正された時間を示す数字又は英数字で表されるパラメータである。パラメータであるＧＵＳＳＴＩＭＥＳＴＡＭＰは、ＧＵＳＳデータのバージョンを示すこともできる。ＧＵＳＳＴＩＭＥＳＴＡＭＰは、ＧＵＳＳの内容が変更されたときに変更される。即ち、ＨＳＳ　１０６内のＧＵＳＳが修正され又は更新された場合、ＨＳＳ　１０６は、新しいＧＵＳＳＴＩＭＥＳＴＡＭＰを更新済みのＧＵＳＳに割り当てる。

【００３０】

また、ＧＵＳＳＴＩＭＥＳＴＡＭＰは、それ自体がＧＵＳＳと共にＨＳＳ　１０６に記憶又は保存されるのと同一の形式で、あるいは異なる形式（即ち、数字又は英数字）で記憶又は通信することができる。しかしながら、異なる形式で記憶又は通信される場合には、そのような別の形式のＧＵＳＳＴＩＭＥＳＴＡＭＰは、ＨＳＳ　１０６において当該ＧＵＳＳＴＩＭＥＳＴＡＭＰの元の表現に戻るように変換することができる。この変換は、例えば複数のＧＵＳＳＴＩＭＥＳＴＡＭＰ同士を比較する必要が生じたときに行われる。

【００３１】

本発明の一態様によれば、ＢＳＦ　１０４は、ＨＳＳ　１０６からＧＵＳＳ又はその均等物を受信し、当該ＧＵＳＳをＢＳＦメモリに記憶する。ＢＳＦ　１０４がＨＳＳ　１０６にＡＶを要求し、且つそれに対応するＧＵＳＳをそれ以前に受信している場合には、当該要求はＧＵＳＳＴＩＭＥＳＴＡＭＰを含んでいる可能性がある。ＨＳＳ　１０６は、受信されたＧＵＳＳＴＩＭＥＳＴＡＭＰと、ＨＳＳ　１０６に既に記憶されているＧＵＳＳＴＩＭＥＳＴＡＭＰとを比較し、２つのＧＵＳＳＴＩＭＥＳＴＡＭＰ同士が異なる場合にのみ当該ＧＵＳＳを応答に含める。２つのＧＵＳＳＴＩＭＥＳＴＡＭＰは、例えばＢＳＦ　１０４が無効なＧＵＳＳ又は古いＧＵＳＳを有する場合に異なる可能性がある。２つのＧＵＳＳＴＩＭＥＳＴＡＭＰ同士が等しい場合には、当該ＧＵＳＳがＡＶと共にＨＳＳ　１０６からＢＳＦ　１０４に送信されることはない。

【００３２】

図３Ａは、本発明の一実施形態に係るＧＵＳＳＴＩＭＥＳＴＡＭＰを作成し修正する方法を示している。ＧＵＳＳＴＩＭＥＳＴＡＭＰの初期化は、特定のＧＵＳＳが作成されたときに行われる。処理２００で、ＨＳＳ　１０６はＧＵＳＳを作成する。処理２１０で、ＨＳＳ　１０６はＧＵＳＳＴＩＭＥＳＴＡＭＰを初期化する。ＧＵＳＳＴＩＭＥＳＴＡＭＰの更新処理は、特定のＧＵＳＳが修正されるたびに行われる。処理２２０で、ＨＳＳ　１０６はＧＵＳＳを修正する。処理２３０で、ＨＳＳ　１０６はＧＵＳＳＴＩＭＥＳＴＡＭＰを更新する。

【００３３】

ＨＳＳ内の特定のＧＵＳＳに関するＧＵＳＳＴＩＭＥＳＴＡＭＰパラメータの値を割り当てる複数の方法が存在する可能性がある。本発明の一実施形態によれば、ＧＵＳＳＴＩＭＥＳＴＡＭＰは、単調増加順（ｍｏｎｏｔｏｎｉｃａｌｌｙ　ｉｎｃｒｅａｓｉｎｇ　ｓｅｑｕｅｎｃｅ）あるいは単調減少順（ｍｏｎｏｔｏｎｉｃａｌｌｙ　ｄｅｃｒｅａｓｉｎｇ　ｓｅｑｕｅｎｃｅ）で割り当てることができる。例えば、ＧＵＳＳが最初に作成されるときに、ＧＵＳＳＴＩＭＥＳＴＡＭＰを割り当て、あるいは何らかの数値に初期化し、あるいはＨＳＳ　１０６内のクロックによって指示される時間及び／又は日付に初期化することができる。ＧＵＳＳが修正されることによって新しいバージョンになるたびに、例えばＧＵＳＳＴＩＭＥＳＴＡＭＰを１ずつ増分又は減分させ、あるいはＨＳＳ　１０６内のクロックによって指示される現在の時間及び／又は日付に変更することができる。別の実施形態では、ＧＵＳＳの特定のインスタンスに関するＳＨＡ‐１やＭＤ５のようなハッシュに相当する又は当該ハッシュの一部に相当するＧＵＳＳＴＩＭＥＳＴＡＭＰ値をＧＵＳＳに割り当てることができる。

【００３４】

図３Ｂは、本発明の一実施形態に従ってトラフィック負荷を最小限に抑える汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に関するタイムスタンプを提供する方法を示している。処理３００で、ＢＳＦ　１０４は、認証ベクトル要求、即ち

ＡＶ要求の準備を行う。処理３１０で、ＢＳＦ　１０４は、当該ＧＵＳＳが既にＢＳＦメモリに記憶されているものかどうかを判定する。ＧＵＳＳが既に記憶されていることが判定された場合には、処理３２０で、ＢＳＦ　１０４は、ＢＳＦ　１０４に記憶されているＧＵＳＳに関連するＧＵＳＳＴＩＭＥＳＴＡＭＰを読み出し、当該ＧＵＳＳＴＩＭＥＳＴＡＭＰをＡＶ要求に含める。一方、ＧＵＳＳがＢＳＦ　１０４に記憶されていないことが判定された場合には、処理３３０で、ＢＳＦ　１０４は、ＡＶ要求をＨＳＳ　１０６に送信する。

【００３５】

処理３４０で、ＨＳＳ　１０６は、ＢＳＦ　１０４からのＡＶ要求を受信する。処理３５０で、ＨＳＳ　１０６は、ＡＶ要求内にＧＵＳＳＴＩＭＥＳＴＡＭＰが存在するかどうかを判定する。ＡＶ要求内にＧＵＳＳＴＩＭＥＳＴＡＭＰが存在することが判定された場合には、処理３６０で、ＨＳＳ　１０６は、ＢＳＦ　１０４から受信されたＧＵＳＳＴＩＭＥＳＴＡＭＰと、ＨＳＳ　１０６に記憶されているＧＵＳＳＴＩＭＥＳＴＡＭＰとが等しいかどうかに関する別の判定を実行する。一方、処理３５０の後に、ＡＶ要求内にＧＵＳＳＴＩＭＥＳＴＡＭＰが存在することが判定された場合には、後述の処理３８０に進む。

【００３６】

処理３６０で、ＢＳＦ　１０４から受信されたＧＵＳＳＴＩＭＥＳＴＡＭＰと、ＨＳＳ　１０６に記憶されているＧＵＳＳＴＩＭＥＳＴＡＭＰとが等しいことが判定された場合には処理３８０に進み、そうでない場合には処理３７０に進む。処理３７０で、ＨＳＳ　１０６に記憶されているＧＵＳＳが応答に含められ、処理３８０に進む。

【００３７】

処理３８０で、ＨＳＳ　１０６は、応答をＢＳＦ　１０４に送信するように構成される。処理３９０で、ＢＳＦ　１０４は、ＨＳＳ　１０６からの応答を受信する。処理４００で、ＢＳＦ　１０４は、応答内にＧＵＳＳが存在するかどうかを判定する。応答内にＧＵＳＳが存在する場合には、処理４１０で、ＢＳＦ　１０４は、ＧＵＳＳが既にＢＳＦ　１０４内に存在するものかどうかを判定する。そうでない場合には、後述の処理４４０に進む。ＧＵＳＳがＢＳＦ　１０４内に存在することが判定された場合には、処理４２０に進む。そうでない場合には、後述の処理４３０に進む。

【００３８】

処理４２０で、ＢＳＦ　１０４は、それ自体に記憶されているＧＵＳＳを削除し、処理４３０に進む。ＢＳＦ　１０４は、処理４３０では受信されたＧＵＳＳの記憶を行い、処理４４０では受信されたＡＶの記憶を行う。

【００３９】

本発明の上記の実施形態では、各処理が図示の順序及び様式で実行されているが、本発明の趣旨及び範囲から逸脱することなく、いくつかの処理の順序等を変更できることが理解されるだろう。

【００４０】

したがって、本発明は、ＧＵＳＳがＨＳＳによって最後に変更された時点を示す、ＢＳＦとＨＳＳとの間で交換される各ＧＵＳＳにＧＵＳＳタイムスタンプを追加することができる。ＧＵＳＳタイムスタンプは、ＢＳＦとＨＳＳとの間のデータ転送ポリシーを最適化するものである。具体的には、加入者からユーザ機器を介して新しい認証ベクトルの検索要求が受け取られたときに、ＢＳＦが当該加入者に関連するデータをメモリ内に有するならば、新しいＡＶ要求には、ＢＳＦのメモリに記憶されているＧＵＳＳに関連するＧＵＳＳタイムスタンプも含められることになる。ＧＵＳＳタイムスタンプが受信されると、ＨＳＳは、受信されたＧＵＳＳタイムスタンプと、ＨＳＳのメモリに記憶されているＧＵＳＳタイムスタンプとを比較する。２つのＧＵＳＳタイムスタンプ同士が同一である場合、即ちそれらが等しい場合には、ＢＳＦが既に当該ＧＵＳＳのコピーを有することになるので、当該ＧＵＳＳがＨＳＳからＢＳＦに送信されることはない。２つのＧＵＳＳタイムスタンプ同士が等しくない場合には、ＢＳＦ　１０４が更新する必要がある無効なＧＵＳＳ

を有することになるので、ＨＳＳからＧＵＳＳが送信される。

【００４１】

更に、本発明の説明ではパケット及びデータグラムという用語が使用されているが、本発明には多くのタイプのネットワーク・データが含まれる。本発明では、パケットという用語は、パケット、セル、フレーム、データグラム、ブリッジ・プロトコル・データ・ユニット・パケット、パケット・データ、及びそれらの均等物を含む。

【００４２】

上記の詳細な説明を読めば本発明の多くの特徴及び利点が明らかとなる。それ故、添付の特許請求の範囲には、本発明の真の趣旨及び範囲に含まれる本発明の特徴及び利点がすべて含まれることが本出願人の意図するところである。更に、様々な修正形態及び変更形態が当業者に容易に想到されるはずであることから、本発明を本明細書に記載され図示されるとおりの構成及び処理に限定することは本出願人の意図するところではなく、したがって、本発明の範囲に含まれる適切なすべての修正形態及び均等物を同様に利用することができる。

【図面の簡単な説明】

【００４３】

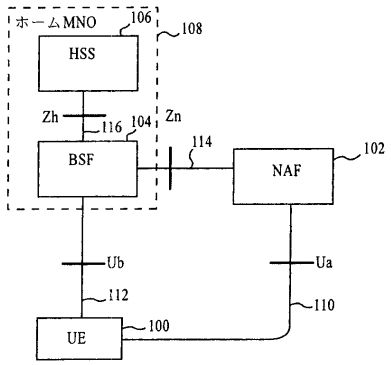
【図１】本発明の一実施形態に係るネットワーク・アプリケーション・サーバ用の一般的な仕組みを提供する装置を示す図である。

【図２】サーバ・ブートストラッピング機能とホーム加入者サーバとの間で転送される情報の一例に関する一実施形態を示す図である。

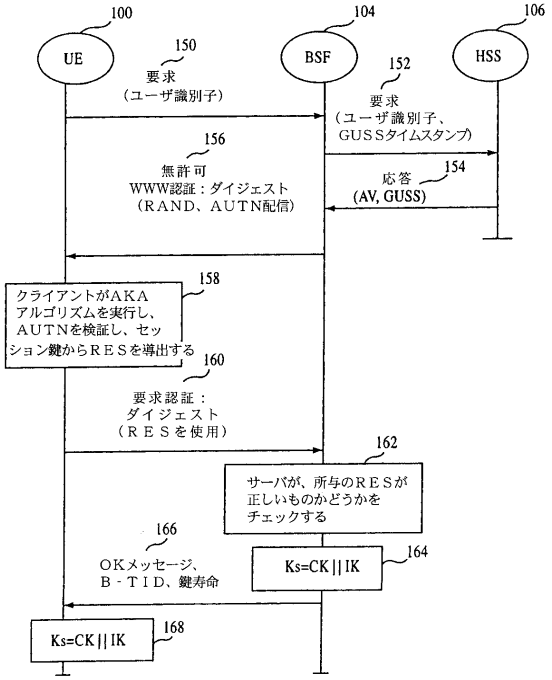
【図３Ａ】本発明の一実施形態に従ってトラフィック負荷を最小限に抑える汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に関するタイムスタンプを提供する方法を示す図である。

【図３Ｂ】本発明の一実施形態に従ってトラフィック負荷を最小限に抑える汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に関するタイムスタンプを提供する方法を示す図である。

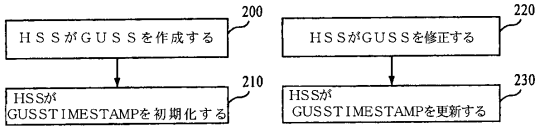
【図１】


ホームMNO
106
108
HSS
Zh
116
104
Zn
BSF
114
NAF
102
Ub
Ua
112
110
UE
100

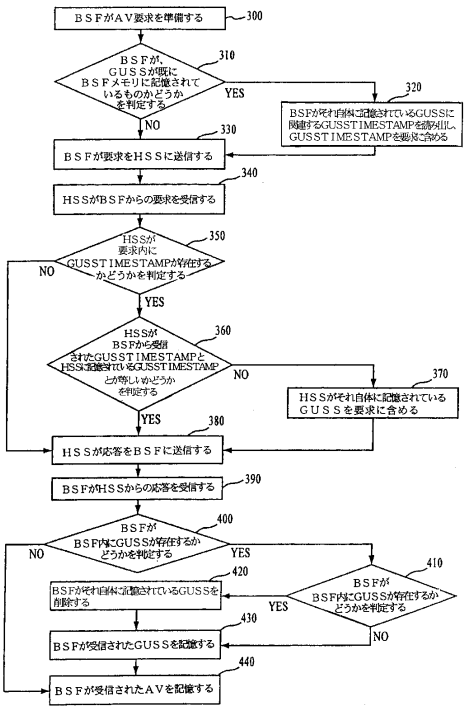
【図２】


100
UE
104
BSF
106
HSS
150
要求
（ユーザ識別子）
152
要求
（ユーザ識別子、
GUSSタイムスタンプ）
156
無許可
WWW認証：ダイジェスト
（RAND、AUTN配信）
154
応答
(AV, GUSS)
158
クライアントがAKA
アルゴリズムを実行し、
AUTNを検証し、セッ
ション鍵からRESを導出する
160
要求認証：
ダイジェスト
（RESを使用）
162
サーバが、所与のRESが
正しいものかどうかを
チェックする
166
OKメッセージ、
B-TID、鍵寿命
164
Ks=CK||IK
Ks=CK||IK
168

【図３Ａ】


200
ＨＳＳがＧＵＳＳを作成する
210
HSSが
GUSSTIMESTAMPを初期化する
220
ＨＳＳがＧＵＳＳを修正する
230
HSSが
GUSSTIMESTAMPを更新する

【図３Ｂ】


ＢＳＦがＡＶ要求を準備する
300
ＢＳＦが、
ＧＵＳＳが既に
ＢＳＦメモリに記憶されて
いるものかどうか
を判定する
310
YES
320
BSFが元々自身に記憶されているGUSSに
関連するGUSSTIMESTAMPを識別し、
GUSSTIMESTAMPを要求に含める
NO
330
ＢＳＦが要求をＨＳＳに送信する
340
HSSがBSFからの要求を受信する
HSSが
要求内に
GUSSTIMESTAMPが存在する
かどうかを判定する
350
NO
YES
HSSが
BSFから受信
されたGUSSTIMESTAMPと
HSSに記憶されているGUSSTIMESTAMP
とが等しいかどうか
を判定する
360
NO
370
HSSがそれ自体に記憶されている
ＧＵＳＳを要求に含める
YES
380
ＨＳＳが応答をＢＳＦに送信する
390
BSFがHSSからの応答を受信する
BSFが
BSF内にGUSSが存在するか
どうかを判定する
400
NO
YES
410
BSFが
BSF内にGUSSが存在するか
どうかを判定する
420
BSFが元々自身に記憶されているGUSSを
削除する
YES
NO
430
BSFが受信されたGUSSを記憶する
440
ＢＳＦが受信されたＡＶを記憶する

フロントページの続き

(56)参考文献 特開２００２－２９７９３２（ＪＰ，Ａ）
米国特許出願公開第２００４／０２３０８６２（ＵＳ，Ａ１）
国際公開第２００３／１０７５８４（WO，Ａ１）
国際公開第２００３／０４１４４２（WO，Ａ１）
特開２００２－０８４２７６（ＪＰ，Ａ）
カナダ国特許出願公開第０２４９５３４３（ＣＡ，Ａ１）
再公表特許第２００５／０１１１９２（ＪＰ，Ａ１）
特開２００１－１０１３２１（ＪＰ，Ａ）
特開２００４－１８１１４０（ＪＰ，Ａ）
国際公開第２００６／０８４１８３（WO，Ａ１）
特表２００８－５３０８６１（ＪＰ，Ａ）
北口善明、他６名，時刻情報を用いたアプリケーションのための高精度ＮＴＰサーバの設計，情報処理学会研究報告，日本，社団法人情報処理学会，２００１年 7月１７日，Ｖｏｌ．２００１、Ｎｏ．７０ ，ｐ４７－ｐ５３

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 13/00
H04W 12/06
H04Q 7/00