【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成19年4月19日(2007.4.19)

【公開番号】特開2004-222313(P2004-222313A)
【公開日】平成16年8月5日(2004.8.5)
【年通号数】公開・登録公報2004-030
【出願番号】特願2004-58623(P2004-58623)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０９Ｃ　1/00　(2006.01)
Ｈ０４Ｑ　7/38　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ａ
Ｇ０９Ｃ　1/00　６４０Ｄ
Ｈ０４Ｂ　7/26　１０９Ｒ

【手続補正書】
【提出日】平成19年3月6日(2007.3.6)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
通信ネットワークと移動局との間の接続の間において伝送されるメッセージの完全性をチェックし、メッセージについて認証値が計算される方法において、
認証が必要とされる全てのメッセージについて、前記通信ネットワークと前記移動局との間の両方向の伝送に関し、該メッセージの認証値が、
前記メッセージと、
前記通信ネットワークにより指定され、かつ、１つの接続のみに対して有効である擬似乱数値と、
前記移動局により少なくとも部分的に指定されるカウント値と、
を基礎にして計算される工程（５０）を具備することを特徴とする方法。
【請求項２】
メッセージの前記認証値は、前記通信ネットワークにより少なくとも一部が指定される第２値をも基礎にして計算される（５４）請求項１に記載の方法。
【請求項３】
前記移動局（２０）は、前記カウンタ値について初期値を指定する請求項２に記載の方法。
【請求項４】
前記移動局（２０）は、第３値を生成するためのカウンタ値と結合される初期値を指定する請求項２に記載の方法。
【請求項５】
前記移動局（２０）は、前記初期値を指定する際に、前記移動局のＳＩＭカードに以前記憶した値を用いる請求項３に記載の方法。
【請求項６】
前記通信ネットワークはＵＭＴＳネットワークであり、前記擬似乱数値は無線ネットワーク制御装置（３０）により指定される請求項１に記載の方法。

【請求項７】
通信ネットワークと移動局との間でメッセージを送受信するネットワーク構成要素であって、該ネットワーク構成要素は、前記通信ネットワークと前記移動局との間の接続の間において伝送されるメッセージの完全性をチェックするものであり、認証が必要とされる全てのメッセージの認証値が前記通信ネットワークと前記移動局との間の両方向の伝送に関して計算されるようにメッセージの認証値を計算する手段を備えており、前記メッセージの認証値が、
前記メッセージと、
前記通信ネットワークにより指定され、かつ、１つの接続のみに対して有効である擬似乱数値と、
前記移動局により少なくとも部分的に指定されるカウント値と、
を基礎にして計算されることを特徴とするネットワーク構成要素。
【請求項８】
メッセージの前記認証値は、前記通信ネットワークにより少なくとも一部が指定される第２値をも基礎にして計算される（５４）請求項７に記載のネットワーク構成要素。
【請求項９】
前記移動局（２０）は、前記カウンタ値について初期値を指定する請求項８に記載のネットワーク構成要素。
【請求項１０】
前記移動局（２０）は、第３値を生成するためのカウンタ値と結合される初期値を指定する請求項８に記載のネットワーク構成要素。
【請求項１１】
前記移動局（２０）は、前記初期値を指定する際に、前記移動局のＳＩＭカードに以前記憶した値を用いる請求項９に記載のネットワーク構成要素。
【請求項１２】
前記通信ネットワークはＵＭＴＳネットワークであり、前記擬似乱数値は無線ネットワーク制御装置（３０）により指定される請求項７に記載のネットワーク構成要素。
【請求項１３】
請求項７乃至１２のいずれかのネットワーク構成要素を備えた電気通信システム。