

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第4268047号
(P4268047)

(45) 発行日 平成21年5月27日(2009.5.27)

(24) 登録日 平成21年2月27日(2009.2.27)

(51) Int.Cl.

F 1

H04W 24/00 (2009.01)
H04W 12/04 (2009.01)H04Q 7/00 240
H04Q 7/00 182

請求項の数 24 (全 15 頁)

(21) 出願番号 特願2003-543329 (P2003-543329)
 (86) (22) 出願日 平成14年9月30日 (2002.9.30)
 (65) 公表番号 特表2005-509380 (P2005-509380A)
 (43) 公表日 平成17年4月7日 (2005.4.7)
 (86) 國際出願番号 PCT/IB2002/004037
 (87) 國際公開番号 WO2003/041422
 (87) 國際公開日 平成15年5月15日 (2003.5.15)
 審査請求日 平成17年9月5日 (2005.9.5)
 (31) 優先権主張番号 01309352.1
 (32) 優先日 平成13年11月5日 (2001.11.5)
 (33) 優先権主張国 歐州特許庁 (EP)

(73) 特許権者 398012616
 ノキア コーポレイション
 フィンランド エフィーエン-02150
 エスプー ケイララーデンティエ 4
 (74) 代理人 100099759
 弁理士 青木 篤
 (74) 代理人 100092624
 弁理士 鶴田 準一
 (74) 代理人 100102819
 弁理士 島田 哲郎
 (74) 代理人 100108383
 弁理士 下道 晶久
 (74) 代理人 100082898
 弁理士 西山 雅也

最終頁に続く

(54) 【発明の名称】暗号化された要求メッセージに応答したネットワークへの移動局の動作およびセルフ性能テスト結果の送出

(57) 【特許請求の範囲】

【請求項 1】

方法であって、

ネットワーク内の移動局の動作中に、該移動局内において性能に関するデータの集合を決定して記憶するステップであって、前記性能に関するデータは該ネットワーク内および該移動局内での正常および異常状態の両方を示す情報を含むようにした、決定して記憶するステップと、

トリガ事象に応答して、前記性能に関するデータの集合または部分集合を、解析用にコンピュータに送信するステップと、

その解析結果をユーザに通知するためのメッセージを前記移動局にて受信するステップと、を有し、

前記トリガ事象が、前記性能に関するデータの集合または部分集合を送信するための暗号化メッセージを前記移動局が受信することからなり、さらにその受信したメッセージを該移動局内に記憶された関連する公開鍵を用いて復号化し、前記暗号化メッセージを正確に復号化することにのみ応答して、前記性能に関するデータの集合または部分集合を送信することを有し、

前記移動局内に記憶された前記公開鍵が、該移動局内に記憶された公開鍵の集合の中の1つであり、該公開鍵の集合の個々の要素が、前記ワイヤレス・ネットワークから受信した暗号化された命令および暗号化されたデータ集合の少なくとも1つとともに前記移動局によって実行可能なアプリケーションと関連し、暗号化された命令および暗号化されたデ

10

20

一タ集合は、前記公開鍵の集合の中の 1 つを用いて前記移動局が復号化する、方法。

【請求項 2】

前記性能に関するデータを、カウンタおよびレジスタに記憶する請求項 1 に記載の方法。

【請求項 3】

前記性能に関するデータが、ドロップ・コールのカウントからなる請求項 1 に記載の方法。

【請求項 4】

前記性能に関するデータが、移動局のセルフ・テスト動作モードの結果の表示からなる請求項 1 に記載の方法。 10

【請求項 5】

前記性能に関するデータの集合または部分集合を送信することが、
送信された、前記性能に関するデータの集合または部分集合を、ネットワーク・サービス・プロバイダに関するコントロール・センタにおいて受信するステップと、
前記移動局における故障、前記ネットワーク・サービス・プロバイダのシステムにおける故障、または故障がまったくない状態のうちの少なくとも 1 つが発生していることの表示を決定するために、前記のデータを解析するステップと、を有する請求項 1 に記載の方法。

【請求項 6】

前記性能に関するデータの集合または部分集合を送信することが、
送信された、前記性能に関するデータの集合または部分集合を、遠隔診断センタにおいて受信するステップと、
前記移動局における故障、前記ネットワーク・サービス・プロバイダのシステムにおける故障、または故障がまったくない状態の少なくとも 1 つが発生していることの表示を決定するために、前記のデータを解析するステップと、を有する請求項 1 に記載の方法。 20

【請求項 7】

前記の解析が、移動局の母集団に関する統計情報を決定するステップを含む請求項 1 に記載の方法。

【請求項 8】

前記解析が、動作故障が発生しているかどうかを決定すること、およびそれが発生している場合には該動作故障が発生しているのは前記移動局なのかまたは該移動局に送信する前記ワイヤレス・ネットワークなのかを決定することを含む請求項 1 に記載の方法。 30

【請求項 9】

前記性能に関するデータの集合または部分集合を送信することが、
送信された、前記性能に関するデータの集合または部分集合を、データ・インターフェースを介して、前記移動局に結合するローカル・コンピュータにおいて受信するステップと、
前記移動局における故障、前記ネットワーク・サービス・プロバイダのシステムにおける故障、または故障がまったくない状態のうちの少なくとも 1 つが発生していることの表示を決定するために、前記のデータを解析するステップと、を有する請求項 1 に記載の方法。 40

【請求項 10】

前記移動局内において性能に関するデータの集合を決定して記憶するステップが、該移動局内において該性能に関するデータの集合を連続的に決定することを含む請求項 1 に記載の方法。

【請求項 11】

ワイヤレス・ネットワークと双方向通信を行なうためのワイヤレス送受信機を備え、さらにメモリと該メモリおよび前記の送受信機に結合されたコントローラとを備える移動局であって、該コントローラは、該移動局の動作中に性能に関するデータの集合を決定する 50

ように、また決定された該性能に関するデータの集合を前記メモリ内に記憶するように動作可能であり、該性能に関するデータは前記のネットワーク内および前記移動局内での正常および異常状態の両方を示す情報を含み、前記コントローラは、トリガ事象の発生に応答して、前記性能に関するデータの前記集合または部分集合を、解析用にコンピュータへ送信することを特徴とし、

前記トリガ事象が、前記性能に関するデータの集合または部分集合を送信するための暗号化メッセージを前記移動局が受信することからなり、前記コントローラが、前記のメッセージの受信に応答して、受信した該メッセージを移動局内に記憶された関連する公開鍵を用いて復号化し、前記暗号化メッセージを正確に復号化することにのみ応答して、前記性能に関するデータの集合または部分集合を送信し、

前記移動局内に記憶された前記公開鍵が、該移動局内に記憶された公開鍵の集合の中の1つであり、該公開鍵の集合の個々の要素が、前記ワイヤレス・ネットワークから受信した暗号化された命令および暗号化されたデータ集合のうちの少なくとも1つとともに前記移動局によって実行可能なアプリケーションに関連し、該暗号化された命令およびデータ集合は、前記公開鍵の集合の関連する1つを用いて該移動局によって復号化される、
移動局。

【請求項12】

前記性能に関するデータが、ハードウェアのカウンタ、ハードウェアのレジスタ、カウンタとして機能するメモリ場所、およびレジスタとして機能するメモリ場所の少なくとも1つに記憶される請求項11に記載の移動局。

【請求項13】

前記性能に関するデータが、ドロップ・コールのカウントと移動局のセルフ・テスト動作モードの結果の表示とのうちの少なくとも1つからなる請求項11に記載の移動局。

【請求項14】

前記トリガ事象が、前記性能に関するデータの前記集合または部分集合を送信するためのメッセージを前記コントローラが前記送受信機を介して受信することからなる請求項11に記載の移動局。

【請求項15】

前記コンピュータが、ネットワーク・サービス・プロバイダと関連するコントロール・センタの一部を構成し、該コンピュータが、前記性能に関するデータを解析して、前記移動局における故障、前記ネットワーク・サービス・プロバイダのシステムにおける故障、または故障がまったくない状態のうちの少なくとも1つが発生していることの表示を決定する請求項11に記載の移動局。

【請求項16】

前記ネットワーク・サービス・プロバイダが、前記表示を前記移動局のコントローラへ、前記移動局の送受信機を介して送信する請求項15に記載の移動局。

【請求項17】

前記コンピュータが、診断センタの一部を構成し、該コンピュータが、前記性能に関するデータを解析して、前記移動局における故障、前記ネットワーク・サービス・プロバイダのシステムにおける故障、または故障がまったくない状態のうちの少なくとも1つが発生していることの表示を決定する請求項11に記載の移動局。

【請求項18】

前記診断センタが、前記表示を前記移動局のコントローラへ、前記移動局の送受信機を介して送信する請求項17に記載の移動局。

【請求項19】

前記診断センタが、データ通信ネットワークに双方向に結合されて、送信された、前記性能に関するデータをそこから受信し、前記表示をそこへ送信する請求項17に記載の移動局。

【請求項20】

前記診断センタが、インターネットに双方向に結合されて、送信された、前記性能に関

10

20

30

40

50

するデータをそこから受信し、前記表示をそこへ送信する請求項 1 7に記載の移動局。

【請求項 2 1】

前記解析が、移動局の母集団に関する統計情報を決定することを含む請求項 1 1に記載の移動局。

【請求項 2 2】

暗号化されたメッセージは少なくとも部分的に暗号化されたSMSメッセージを有し、前記性能に関するデータの集合または部分集合を送信することは、前記暗号化されたSMSメッセージを正確に復号化することにのみ応答して応答SMSメッセージを送信することを有する、請求項 1 1に記載の移動局。

【請求項 2 3】

前記コントローラが、前記性能に関するデータの集合を連続的に決定するように動作可能である請求項 1 1に記載の移動局。

【請求項 2 4】

方法であって、

ネットワーク内での移動局の動作中に、該移動局内において性能に関するデータの集合を決定して記憶するステップであって、該性能に関するデータは該ネットワーク内および該移動局内での正常および異常状態の両方を示す情報を含むようにした、決定して記憶するステップと、

前記性能に関するデータの集合または部分集合を送信するための暗号化メッセージを、前記移動局において受信するステップと、

受信した前記暗号化メッセージを前記移動局内に記憶された関連する公開鍵を用いて正確に復号化することに応答して、前記性能に関するデータの集合または部分集合を該移動局からコンピュータへ解析用に送信するステップと、

を有し、

前記移動局内に記憶された前記関連する公開鍵が、該移動局内に記憶された公開鍵の集合の中の 1 つであり、該公開鍵の集合の個々の要素が、前記ワイヤレス・ネットワークから受信した暗号化された命令および暗号化されたデータ集合の少なくとも 1 つとともに前記移動局によって実行可能なアプリケーションと関連し、暗号化された命令および暗号化されたデータ集合は、前記公開鍵の集合の中の 1 つを用いて前記移動局が復号化する、方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は一般に、無線電話、特に無線電話または移動局であって、セルラ・ネットワークを用いた動作が可能であるもの、さらにセルフ・テストおよび他の診断手順の実行および結果の記録が可能であるものなどに関する。

【背景技術】

【0002】

移動局市場で絶えず問題となっているのは、ユーザすなわち加入者が、機能していないか機能不良であると称する移動局を販売店またはネットワーク・サービス・プロバイダに返却した後に、いわゆる故障なし (NFF) が発生することである。たとえば加入者が、移動局が特定の問題または故障モードを示していると言ってくることがある。しかし修理拠点または修理センタの専門技術者は、返却された移動局についてどのタイプの動作不良も問題も見出すことができず、NFF の報告書を発行しなければならないことになる。典型的なケースでは、加入者が遭遇している問題が実際には、ワイヤレス・ネットワーク自体が遭遇している何らかの一時的な問題の結果であって、移動局によるものではないことがある。たとえば何らかのネットワーク問題が原因で、移動局が繰り返してコール (call) をドロップ (drop) することや、またはサービスを受けられなくなることが起こり得る。

【発明の開示】

10

20

30

40

50

【発明が解決しようとする課題】**【0003】**

この種の問題は、販売店および／またはサービス・プロバイダだけでなく、製造業者にとってもコスト増となり得ることが理解される。加えて、ユーザが遭遇する問題が製造業者には全く手の打ちようがないものであるにも拘らず、ユーザが移動局の製造業者に対してあまり良くない印象を抱くことも考えられる。

【0004】

したがって本発明の第1の目的および利点は、前述の問題および他の問題を開ける改善された無線電話およびサービス・プロバイダの相互関係を提供することである。

【0005】

本発明の別の目的および利点は、移動局の電気的状態および動作状態を示す複数の製品性能カウンタ（PPC）を記憶して保持する移動局を提供することである。

10

【0006】

本発明のさらなる目的および利点は、PPCの集合を記憶して保持するとともに、さらにPPCの完全な集合または部分集合を、解析用に外部の場所へ送信することができる移動局を提供することである。

【0007】

本発明のさらなる目的および利点の1つは、移動局の外部の場所でのコンピュータであって、PPCだけでなく他のデータ入力も解析して、移動局および／またはワイヤレス・ネットワークの故障状態を決定することができるコンピュータを、提供することである。

20

【0008】

本発明の他の目的および利点は、PPCの集合を記憶して保持するとともに、暗号化されたPPC要求メッセージの受信に応答してPPCの完全な集合または部分集合を外部場所へ送信するように動作する移動局を提供することである。

【課題を解決するための手段】**【0009】**

本発明の実施例による方法および装置によって、前述した問題および他の問題が開かれ、目的および利点が実現される。

【0010】

本明細書で開示されるのは、移動局の動作方法とともに、この方法に従って動作する移動局およびワイヤレス・システムである。本方法は、（A）移動局の動作中に、性能に関するデータ（PPC）の集合を決定して移動局内に記憶するステップと、（B）トリガ事象の発生に応答して、性能に関するデータの集合または部分集合を、解析用にコンピュータに送信するステップと、を有する。性能に関するデータは、カウンタおよびレジスタ内に、またはカウンタおよびレジスタとして機能するように扱われるメモリ場所内に記憶することができる。例として、性能に関するデータは、ドロップ・コール（dropped call）のカウント、および／または移動局のセルフ・テスト動作モード結果の表示を含むことができる。トリガ事象は、性能に関するデータの集合または部分集合を送信するためのメッセージを移動局が受信すること、または移動局のユーザからの入力を移動局が受信すること、またはタイマの時間切れ、または性能に関するデータの少なくとも1つが閾値に等しい（たとえば、ドロップ・コールの数がある閾値に到達する）ことと、することができる。

30

【0011】

本発明の現時点での好ましい実施例においては、移動局が受信するトリガ事象メッセージは、移動局に、暗号化形式で、たとえばRSAフォーマットで送信される。この実施例においては、移動局は、受信したメッセージを復号化するための公開鍵を記憶しており、メッセージへの応答を、PPCデータの集合または部分集合を暗号化または非暗号化のフォーマットでネットワークへ送信することによって行なう。

40

【0012】

性能に関するデータの集合または部分集合を送信するステップは、送信された性能に関

50

するデータを、ネットワーク・サービス・プロバイダに付隨するコントロール・センタまたは（遠隔）診断センタ、またはローカル・コンピュータにおいて受信するステップと、コンピュータを用いてデータを解析して、移動局における故障、ネットワーク・サービス・プロバイダのシステムにおける故障、または故障がまったくない状態の少なくとも1つが発生していることの表示を決定するステップと、を含むことができる。任意選択のステップにおいて、決定された表示を移動局へ送信する。解析はさらに、移動局の母集団に関する統計情報を決定することを含んでいても良い。

【0013】

性能に関するデータを解析するステップは、ワイヤレス・ネットワーク性能データまたは移動局のユーザから得た情報の少なくとも1つと組み合わせて実行しても良い。

10

【0014】

移動局内に記憶された公開鍵は、移動局内に記憶された公開鍵の集合の中の1つであっても良く、公開鍵の集合の個々の要素が、ワイヤレス・ネットワークから受信した暗号化された命令および暗号化されたデータ集合の少なくとも1つとともに移動局によって実行可能なアプリケーションと、関連している。暗号化された命令および/またはデータ集合は、公開鍵の集合の中の1つを用いて移動局が復号化する。

【0015】

本発明の前述した特徴および他の特徴は、以下の本発明の詳細な説明を添付の図面とともに読むことで、より明瞭になる。

【発明を実施するための最良の形態】

20

【0016】

最初に、本発明の実施に適した無線電話、本明細書ではワイヤレス移動局10とも言うが、示されている図1および2を参照する。移動局10は、これに限定されないが、携帯電話またはパーソナル・コミュニケータであっても良い。移動局10は、基地サイトまたは基地局30との間で信号を送受信するためのアンテナ12を備える。基地局30は、セルラ・ネットワークの一部とすることができます、そのセルラ・ネットワークは、ワイヤレス・ネットワーク・プロバイダ・システム32、本明細書では簡単にワイヤレス・ネットワーク32とも言うが、を含み、ワイヤレス・ネットワーク・プロバイダ・システム32はさらに移動交換局(MSC)34を含む。移動局10が呼び出されるときに、MSC34によって、陸上通信中継線に対する接続が行なわれる。またネットワーク・コントロール・センタ33を設けても良い。ネットワーク・コントロール・センタ33は、MSC34に結合されて、ネットワーク・プロバイダ・システム32の動作を制御するとともに、移動局10から基地局30を介して情報を受信する。ネットワーク・コントロール・センタ33は、ネットワーク・プロバイダ・システム32内の1つまたは複数の他の点において接続することができる。

30

【0017】

移動局は、変調器(MOD)14A、送信機14、受信機16、復調器(DEMOD)16Aとともに、送信機14および受信機16からそれぞれ信号の供給および受け取りを行なうコントローラ18を備える。これらの信号には、適用可能なセルラ・システムのエア・インターフェース標準に基づくシグナリング情報、ならびにユーザ通話および/またはユーザ生成データが含まれる。本発明の動作に対しては、特定のタイプのエア・インターフェース標準が重要というわけではない。と言うのは、本発明の教示は、アナログ・ワイヤレス・システム(たとえばAMPSシステム)だけでなく、デジタル・システム、たとえば時分割/多元アクセス(TDMA)および符号分割/多元アクセス(CDMA)システム、にも適用されるからである。たとえば従来型および最新式のGSM型システムの両方とも、本発明の教示から利益を得ることができる。

40

【0018】

コントローラ18には、移動局の音声機能(通話パス)および論理機能を実行するためには必要な回路も含まれることが理解される。例として、コントローラ18は、デジタル信号プロセッサ・デバイス、マイクロプロセッサ・デバイス、種々のアナログ・デジタル変

50

換器、デジタル・アナログ変換器、および他のサポート回路で構成しても良い。移動局の制御機能および信号処理機能は、これらのデバイス間に、それらの個々の能力に応じて割り当てられる。

【0019】

ユーザ・インターフェースには、従来のイヤホーンまたはスピーカ17、従来のマイクロフォン19、ディスプレイ20、およびユーザ入力デバイス、典型的にはキーパッド22が含まれる。これらはすべて、コントローラ18に結合されている。キーパッド22には、移動局10の操作に用いられる従来の数字(0~9)および関連キー(#+*)22a、ならびに他のキー22bが含まれる。これら他のキー22bには、たとえば、SENDキー、種々のメニュー・スクロール・キーおよびソフト・キー、ならびにPWRキーが含まれていても良い。10

【0020】

移動局10は、移動局の動作に必要な種々の回路に電力を与えるための取り外し可能な電池26も備えている。

【0021】

また移動局10は、一括してメモリ24として示す種々のメモリも備える。メモリには、移動局の動作中にコントローラ18によって使用される複数の定数および変数が記憶される。たとえばメモリ24には、ワイヤレス・システム・パラメータの値および番号割り当てモジュール(NAM)が記憶される。コントローラ18の動作を制御するための動作プログラムも、メモリ24に、典型的にROMデバイス内に記憶される。メモリ24内の動作プログラムとしては、メッセージおよびメッセージ関連機能をユーザに対してディスプレイ20上で、典型的には種々のメニュー項目として示すルーチンが挙げられる。メモリ24には、後述する移動局によって実施される方法を実行するためのルーチンも含まれる。20

【0022】

本発明の一態様によれば、メモリ24には、製品性能力ウンタ(PPC)24Aの集合が記憶されている。個々のカウンタは、移動局10の動作の何らかの様相を示す。一般に、PPC24Aの個々のカウンタを本当のカウンタとすることができる、たとえばあるものをドロップ・コール数の記録用にすることができる一方で、他のものは、それよりも、例として特定のコールがドロップした時点での受信信号強度(RSS)の大きさなどのいくつかの値を記憶するためのレジスタと考えても良い。メモリ24のメモリ場所に記憶されたときに、ソフトウェアが、メモリ場所を用いてカウンタおよびレジスタの機能をエミュレートすること(たとえばドロップ・コールが起きるたびに特定のメモリ場所をインクリメントすることによって)が、理解できる。30

【0023】

一般に、PPC24Aは、ワイヤレス・ネットワークの品質に関する情報とともに、移動局10の動作に関する情報を与える。本発明のさらなる態様によれば、PPC24Aの集合、またはその部分集合は、移動局からネットワーク・プロバイダ・システム32へ、基地局30を介して伝送される。PPC24Aの伝送は、ネットワーク・プロバイダ・システム32もしくは何らかの他の要求者から受ける要求に応じて、または移動局10のユーザからの命令と同時に、または周期的にある所定の時間間隔で、または何らかの他のトリガ事象(たとえばある所定の動作時間内にドロップ・コールの所定の閾値数に達する)と同時に、行なうことができる。40

【0024】

PPC24Aを用いることは、新しいワイヤレス仕様特性および新しいネットワーク・アプリケーション・サービスを特徴づけるときに、たとえば移動局のテスト・グループまたは母集団をネットワーク・プロバイダ・システム32のサービスエリア内に配置するときに、特に有益である。移動局のテスト・グループを用いることで、サービス・プロバイダは、PPC24Aを電波によって収集することができ、その結果、重要なサービスエリアおよび他の特性が特徴づけられる。移動局10のユーザにフィードバックを与えること50

もでき、これはネットワーク・プロバイダから送信してディスプレイ20上に表示することによって、および／または従来のPCによってアクセスできるかまたは移動局10からワイヤレスでアクセスできるウェブ・ページ上に、結果を掲示することなどの他の手段によって、行なわれる。

【0025】

呼の期間中に、PPC24Aの集合または選択された部分集合をコントローラ18によって送信機14を介して転送することができ、これはたとえばショート・メッセージ・サービス(SMS)機能を用いて、またはGSMの非構造付加データ・サービス機能などの何らかの他のメッセージ関連機能によって、またはインターネット37によって送られるTCP/IPフォーマットに準拠するパケット・データなどのパケット・データとして、転送される。また送信すべきPPC24Aをディスプレイ20上に表示して、ユーザに、ネットワーク・コントロール・センタ33の人間または機械(音声認識)オペレータに結果を口頭で話してもらうことも、本発明の範囲内である。PPC24Aの解析を、ネットワーク・コントロール・センタ33において、および／またはネットワーク・プロバイダ・システム32に従来の電話線(たとえば公衆交換電話網(PSTN)36)を通してまたは別個の通信ネットワークを通して結合された遠隔診断センタ38において、行なうことができる。こうするために、インターネット37への接続を用いることもできる。遠隔診断センタ38は、移動局10の製造業者に、販売もしくはサービス・センタに、研究開発センタに、または便利もしくは好適であればどんな場所に配置しても良い。

【0026】

次に図3も参照して、ネットワーク・コントロール・センタ33は、PCまたはメインフレーム・コンピュータで動作するソフトウェアなどの故障解析モジュール(FAM)33Aを備えていても良い。FAM33が入力として受け取るのは、送信されたPPC24Aの集合または部分集合とともに、PPC24Aの一部でない場合、移動局セルフ・テスト結果、ネットワーク・オペレータからの入力、たとえば移動局10のユーザから得た情報とともにある種のネットワーク・パラメータ、たとえば基地局電力である。他の入力を供給することもできる。たとえばネットワーク・プロバイダ・システム32のサービスエリアにおけるRF伝搬状態である。FAM33Aはこれらの入力を、たとえばエキスパート・システムまたはニューラル・ネットワークを用いて処理して、移動局/ネットワーク機能の適切な表示を出力する。これらの表示には、移動局10の故障の表示、ネットワーク・プロバイダ・システム32の故障の表示、または故障なし(NFF)の表示を含めることができる。FAM33Aの出力表示を中継して移動局10へ戻すことによって、ユーザにリアル・タイムのまたはほぼリアル・タイムの故障解析および障害検出を提供することも、本発明の教示の範囲内である。例として、ユーザに、すでに送信されたPPC24Aだけでなくネットワーク・オペレータから得た情報にも基づく閉ループのやり方で、移動局10は十分に機能している可能性が高いこと(障害はまったく存在しないかネットワーク・プロバイダ・システム32内などの他の場所に存在することを意味する)、または移動局10は何らかの動作不良を起こしている可能性が高いことを知らせても良い。この後者の場合、ユーザは、移動局10を現地のサービス・センタまたは販売店へ持つて行き、交換または修理を行なっても良い。しかしこの後者の場合には、移動局10が動作不良を起こしている可能性が高いことがすぐにはっきりしているので、前述した故障なし(NFF)の状況が生じることは無いか著しく少ないことが理解できる。

【0027】

PPC24Aの集合には、移動局の機能についての様々な多くの表示を含むことができる。たとえば、ドロップ・コールの数および／または不成功だった起呼の試み(とともに信号強度表示)に加えて、他の表示として、内部セルフ・テスト・プログラムの結果(たとえばメモリ・エラー、異常プログラム状態および終了など)ならびに明らかに正常な動作期間中に周期的に収集されたデータなどである。この後者の表示は、他の表示との比較ができるベースラインを設けるのに有益である。またPPC24Aには、フレーム誤り率、シンボル誤り率、ある時間の間に発生する再送信リクエストの数などの表示を含めるこ

10

20

30

40

50

とができる。

【0028】

図4に示す方法を参照して、ステップAでは、移動局10がPPC24Aの集合を記憶する。このステップは、移動局10の動作中にかなりの期間を通して行なっても良い。ステップBでは、何らかのトリガ事象が発生したかどうかを判定する。トリガ事象は、たとえばPPC24Aの集合もしくは部分集合の送信をリクエストするメッセージの移動局10による受信、または移動局10のユーザからの入力、またはタイマの時間切れとすることができる。トリガ事象が発生していない場合には、制御はステップAに戻って、PPC24Aの集合の記憶および/または更新を続ける。トリガ事象が発生している場合には、PPC24Aの集合または部分集合が、移動局10からネットワーク・プロバイダ・システム32へ、基地局30を介して伝送される。PPC24Aの選択的な送信を、たとえば要求されたPPC24A(たとえば移動局10へ送信されるメッセージで要求される)のみを送信することで、またはPPC24Aの部分集合のみをネットワーク・コントロール・センタ33へ送信する一方でPPC24Aの完全な集合を遠隔診断センタ38へ送信することで行なうことも、本発明の範囲内である。送信されるPPC24Aを、伝送前に暗号化して、後で受信場所で復号化しても良い。こうすることで、送信されるPPC情報のプライバシが保証される。

【0029】

本発明の現時点で好ましい実施例においては、後で詳述するように、ワイヤレス・ネットワーク32から受信したトリガ事象メッセージを暗号化して、移動局10によって受信後に復号化される。PPC応答データをワイヤレス・ネットワーク32に向けて送り返す前に、このデータを移動局10が暗号化しても良いし、しなくても良い。

【0030】

いずれにしてもステップCにおいて、FAM33A、または遠隔診断センタ38での等価なシステムによるPPC24Aの解析を、好ましくは、前述した他の情報、たとえばネットワーク関連情報および/またはオペレータが移動局10のユーザから得た情報とともに行なう。ステップDにおいて、PPC24A(および任意選択の他の情報)が移動局の故障を示すかどうかを判定する。もしそうならば制御はステップGに移るが、移動局の故障が示されない場合には、ステップEにおいて、ネットワーク故障が示されるかどうかが判定される。もしそうならば制御はステップGに移るが、ネットワーク動作不良が示されない場合には、ステップFにおいて、故障または障害なし(NFF)が決定される。次に制御がステップGに移って、そこでメッセージを形成して移動局10へ送り、ユーザにPPC解析の結果を示しても良い。

【0031】

好ましい実施例との関連で説明しているが、当業者であれば、当然のことながらこれらの教示に対する多くの変更に気付くであろう。例として、種々のタイプの移動局10が種々のタイプのPPC24Aを記憶しても良いことが理解できる。たとえばTDMA移動局10が、フレームおよび時間スロット同期機能に関する1つまたは複数のPPCを記憶しても良いし、一方でCDMA移動局が、擬似ノイズ(PN)拡散符号相関関数に関する1つまたは複数のPPCを記憶しても良い。

【0032】

さらに、当然のことながら、PPC24Aをネットワーク・オペレータおよび/または移動局の製造業者が使用することで、移動局10の母集団の動作に関する統計データを取得できる。たとえば、ある地理的領域内での(たとえば所定の隣接セル集合内の)ドロップ・コールの数に関する統計情報を、コールがドロップした時点で受信する信号強度の関数として、さらに発生しているフレーム誤り率も(任意選択で)、携帯電話形式によって集めて解析することができる(たとえば新モデルの移動局の動作を旧モデルの移動局の動作と対照させることができる)。

【0033】

さらに、この例を拡張して、故障場所の決定を対象とするようにすることもできる。例

として、PPCデータ24Aが、移動局10がこの10分間にコールを3回ドロップしたことを示し、かつ関連する信号強度表示が適切な量の信号強度を示す場合には、FAM33Aは、故障は移動局10内に存在し得ると決定することができる。しかし複数の移動局がコールをドロップしていることが見出され、かつこれらのほとんどが同じセル内に位置していることがPPCデータ24Aからまたはネットワーク関連パラメータ・データから判定される場合には、故障は、移動局10内ではなく、むしろ基地局30内に存在し得る。これは、移動局セルフ・テストの結果が移動局の動作不良を示さない場合に、特に正しい。

【0034】

他の例としては、PPCデータ24Aが、移動局10がコールをドロップしていることを示し、かつ関連する信号強度表示が適切な量の信号強度を示さない（受信信号が弱い）場合には、移動局のセルフ・テストの結果がある移動局の動作不良を示す限り、FAM33Aはやはり、故障は移動局内10にある可能性が高いことを示すことができる。

【0035】

あるいは、PPCデータ24Aが、移動局10がコールをドロップしていることを示し、かつ関連する信号強度表示が示すフィールド強度が弱く（受信信号が弱い）、しかし移動局セルフ・テストの結果が移動局の動作不良を示さない場合には、故障は多分ネットワーク・プロバイダ・システム32内にあると示すことができる。

【0036】

あるいは、PPCデータ24Aが、移動局10がコールをドロップしていることを示し、かつ関連する信号強度表示が示すフィールド強度の読みが適切または良好であり、かつ移動局セルフ・テストの結果が移動局の不良動作を示さない場合には、この場合もやはり、故障は多分ネットワーク・プロバイダ・システム32内にあると示すことができる（たとえばネットワークの負荷が重過ぎるか、またはあるネットワーク電子ユニットが限界に近いかもしくは良かつたり悪かつたりする）。

【0037】

また当然のことながら、図4に示した方法のうちのあるステップを図示した順番以外で実行でき、追加のステップを加えることができ、それでも好ましい結果がやはり得られる。たとえばステップDおよびEの実行の順番を逆にすることができる、ステップGを完全にまたは選択的に迂回することができる（たとえばユーザが通知されるのは、故障が移動局10内にあると決定されたときのみ）。

【0038】

さらにPPC24Aを移動局10から出力することが、ワイヤレス送信機14を通した送信のみによって行われることは、必須ではないことに注意されたい。たとえば、図1を再び参照して、移動局データ・インターフェース28を用いてPPC24Aを、ケーブルまたはIRリンクを通して、ネットワーク・コントロール・センタ33または遠隔診断センタ38内で動作するプログラムと類似または同一の適切な診断プログラムを有するローカル・コンピュータ29（図2に示す）に、送信または出力することができる。この場合、ローカル・コンピュータ29を、販売時点場所もしくはサービス・センタまたは便利であれば他のどんな場所に設置することもでき、ユーザが遭遇している問題に関する考えられる原因について迅速なフィードバックをユーザに与えることができる。またこの場合、コントローラ18にPPC24Aを送信させるトリガ事象は、ローカル・コンピュータ29から送信された問い合わせ信号を、データ・インターフェース28を通してコントローラ18が受信したものとすることができる。

【0039】

すでに簡単に述べたように、ワイヤレス・ネットワーク32がPPC要求メッセージを暗号化またはこれに「署名」することを、移動局10にメッセージを送信する前に行なうことを要求することは、本教示の範囲内である。こうして、PPC要求メッセージの構造が、第三者が容易に判定できるものではなくなり、その結果、移動局10が、PPC要求メッセージの許可された発信源以外から送られたPPC要求メッセージに応答する可能性

10

20

30

40

50

が減る。このことは、移動局 10 が要求者に応答することが、たとえばSMSメッセージを用いて行なわれる、移動局のユーザがSMSメッセージの送信費用を請求される場合には、重要であり得る。現時点では嬉しいがもちろん限定的でない暗号化アルゴリズムは、RSAに基づくものである。

【0040】

簡単に言えば、RSAは、インターネットのセキュリティ確保を支援しようとする試みの中で1977年にMITで開発された公開鍵暗号システムである。暗号システムは、入力データを認識不能な何かに変換し（暗号化）、その認識不能なデータを変換してその元の形へ戻す（復号化）アルゴリズムとを考えることができる。データを暗号化するためには、データ（「平文」）と暗号化鍵とを、アルゴリズムの暗号化部分に入力する。「暗号文」を復号化するためには、適切な復号化鍵をアルゴリズムの復号化部分において用いる。これらの鍵は、それぞれ公開鍵および秘密鍵と言われる。たとえばデータをAからBに送るためには、AはBの公開鍵を調べるかそうでなければその鍵のことを知っており、そしてBの公開鍵を用いてデータを暗号化する。しかし公開鍵では、暗号文は復号化されない。Bが、受信した暗号文を復号化するためには、BはBの秘密鍵を用いなければならない。Bが、暗号化した応答を用いてAに応答したい場合には、Bはその応答をAの公開鍵を用いて暗号化しなければならない。

【0041】

RSAなどの公開鍵暗号システムにおいて重要なのは、ユーザの秘密鍵を判定できることである。これは、一方向関数を用いることで実現される。一方向関数を用いれば、ある入力値が与えられたときに結果を計算することは簡単である。しかし結果から始めた場合に、元の値を決定することは極めて難しく、ほとんど不可能である。RSAで使用される一方向関数は、素数の掛け算である。一般に、2つの大きな素数を掛け合わせることは比較的簡単であるが、素数が非常に大きくなるとほとんどの場合に、それらの因数分解には極めて時間がかかる。こうして公開鍵暗号化では、2つの大きな素数を用いて秘密鍵を形成し、素数の積を用いて公開鍵を形成する暗号システムが構築される。

【0042】

本発明の一態様によれば、非公開の秘密鍵（Private Key）35Aが、ネットワーク32内に、たとえばネットワーク・コントロール・センタ33または遠隔診断センタ38において、特定のサービス、この場合はPPCサービスに関連する移動局の一般的な公開鍵（GPK）35Bとともに、記憶されている。移動局10には、一般的な公開鍵PubKeyが記憶されており、このPubKeyは移動局10内に、たとえばメモリ24の場所24Bに記憶されている。暗号化メッセージがワイヤレス・ネットワーク32から届くと、そのメッセージは、移動局10のデータ・プロセッサ18によって、場所24Bに記憶された関連する公開鍵を用いて復号化される。PPCデータに対する正当な要求を復号化することにのみ応答して、移動局10はPPCデータの集合または部分集合を、ワイヤレス・ネットワーク32へ送信する（図4のステップB）。移動局10は応答を暗号化することができるが、これは、PPCデータ応答などのほとんどの応答形式においては要求されない。と言うのは、典型的には、応答データには秘密または機密なことは何もないからであり、そうでなくとも第三者には認識できないからである。

【0043】

この技術では、移動局10内に記憶する必要があるのは一般的な公開鍵のみであり、これに対して非公開すなわち秘密鍵35Aは、ワイヤレス・サービス・プロバイダ32が保持するメイン・サーバ内に安全に記憶されることが理解できる。こうすることで、移動局10へ送られる命令の集合および/またはデータも安全が確保される。その結果、アプリケーション構造が秘密に保たれ、未許可の第三者がアプリケーションおよびシステムの関連部分の使用を試みることが防止される。

【0044】

この技術を用いる際、移動局10は、n個の異なるアプリケーションの集合に対応してn個の別個の公開鍵を記憶できることに注意されたい。こうすることによって、移動局1

10

20

30

40

50

0が、ワイヤレス・ネットワーク32によって開始される所定のアプリケーションに応答するのは、トリガ事象、たとえば正当なメッセージおよび任意選択のデータ集合の受信を、記憶されたn個の公開鍵の1つを用いて正確に復号化できる場合のみとなる。

【0045】

本発明の他の実施例においては、RSA暗号システム以外のものを用いることもできる。

【0046】

図5に、本教示の一態様による無線起動(OTA)システムを含むシステム・レベルの図を示す。このシステムには、サービス層60、ウェブ・サーバ層62、およびクライアント層64が存在する。サービス層60には、グローバル・システム・サービス・データ・ベース68と通信するOTAソフトウェア(SW)実行用OTAサーバ66が含まれる。ウェブ・サーバ層62には、ウェブ・サーバ70が配置され、クライアント層64には、一般に端末72と言われるPCおよび/またはワークステーションが配置される。これらはたとえば、研究開発(R&D)施設、顧客サポート場所、および販売時点(POS)場所に位置する。端末72はOTAサーバ66と、インターネットまたは他の何らかのネットワークを介して、ウェブ・サーバ層62を通して通信する。本教示によれば、PPCデータ集合は移動局10から、OTAサーバ66から送られる暗号化されたPPC要求メッセージを用いて、取得される。次に、取り出した情報をグローバル・データ・ベース68内に記憶することができ、および/またはその情報を、クライアント層64における端末72の1つまたは複数に送って検討および解析することができる。

【0047】

図6に、本教示による典型的なPPC取り出し方法の論理フローチャートを示す。ステップAにおいて、顧客はヘルプ・ラインを呼び出して、顧客の移動局10について分かっている問題を報告する。顧客によるこの呼び出しは、インターネット37を通して行なうこともでき、音声による呼び出しである必要はない。ステップBおよびCにおいて、顧客の移動局10内で想定される故障に関して顧客との会話がなされる。ステップDにおいて、PPCデータを送信させるために、トリガSMSメッセージを顧客の移動局10に送る。トリガSMSメッセージの一部または全部の暗号化を、たとえば前述したRSA暗号化技術を用いて行なうことができる。ステップEにおいて、PPCデータを送信すべきかどうかについて顧客を促すことによって、PPCデータを送信するかどうかが判定される。PPCデータの送信は、顧客には無料とすることもできるし、費用は含まれても良い。顧客がPPCデータを送信しないと決めた場合には、制御はステップBに戻り、顧客との会話が続けられる。PPCデータを送信すべきであると顧客が指示した場合には、制御はステップFに移って、PPCデータの全部または部分集合が移動局10からOTA-SW66を介して送信され、データは、ワイヤレス・ネットワーク32におけるPPCデータ・ベースに記憶される。PPCデータ・ベースは、図5に示すグローバル・データ・ベース68であっても良い。ステップGおよびHにおいて、移動局10からのPPCデータについてPPCデータ・ベースに照会し、データが解析される。ステップIでのウェブ・ツールを用いて解析結果をヘルプ・ラインに戻して、顧客に口頭で結果を通知することができるし、または結果を顧客に、インターネット37を通して図5のウェブ・サーバ層62を介して、送ることができる。必要に応じて、ステップIでのウェブ・ツールが直接、PPCデータ・ベースにステップJで照会しても良い。

【0048】

最終的な結果は、顧客が認識する移動局故障の診断を改善すること、ネットワーク・オペレータ32およびおそらく移動局10の製造業者に対するコストを下げること、そして顧客満足度を向上させることである。

【0049】

本発明を、好ましい実施例に関して特に図示し説明してきたが、当業者であれば、当然のことながら本発明の範囲および趣旨から逸脱することなく形態および詳細の変更を行なうことができる。

10

20

30

40

50

【図面の簡単な説明】

【0050】

【図1】本発明の実施に適した移動局を示すブロック図である。

【図2】図1に示した移動局を示す正面図であり、さらに、移動局がワイヤレスRFリンクを介して双方向に結合するワイヤレス通信システムとサービス・プロバイダとを示す。

【図3】PPCおよび他の情報を解析して移動局の動作状態を示す出力を提供するソフトウェア・モジュールの入力および出力を示す図である。

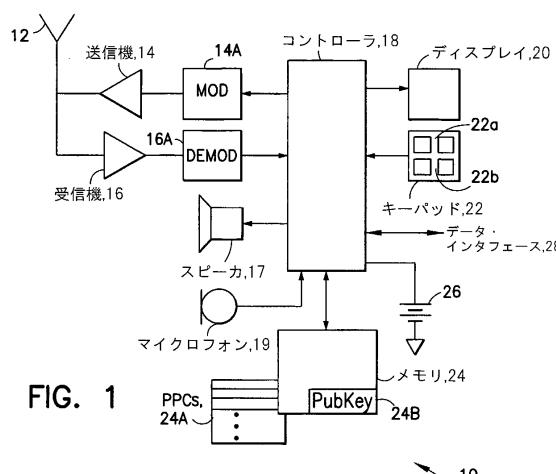
【図4】本発明の方法による論理フローチャートである。

【図5】本教示の態様による無線起動(OTA)システムを示すシステム・レベルの図である。

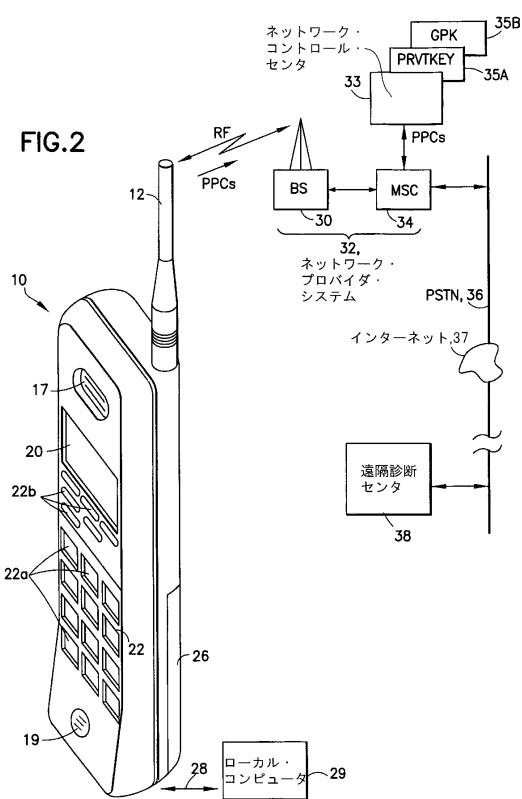
10

【図6】本教示によるPPC取り出し方法を示す論理フローチャートである。

【図1】



【図2】



【図3】

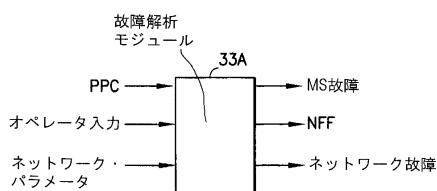


FIG.3

【図4】

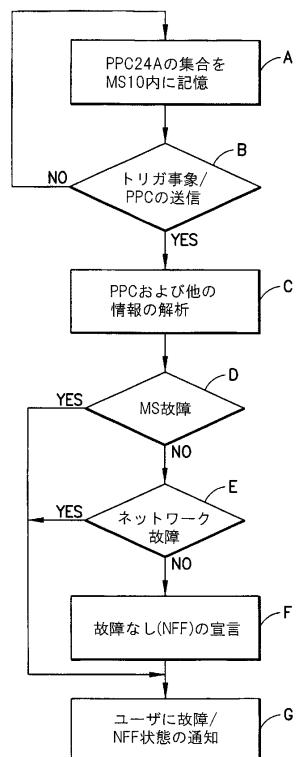


FIG.4

【図5】

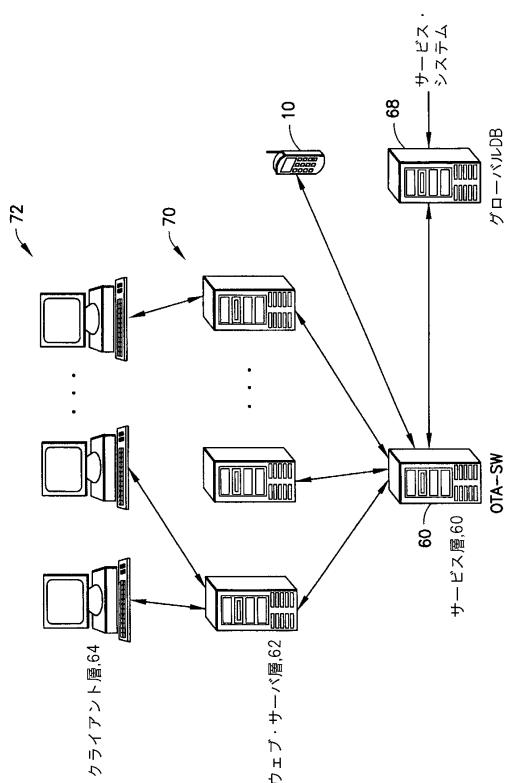


FIG.5

【図6】

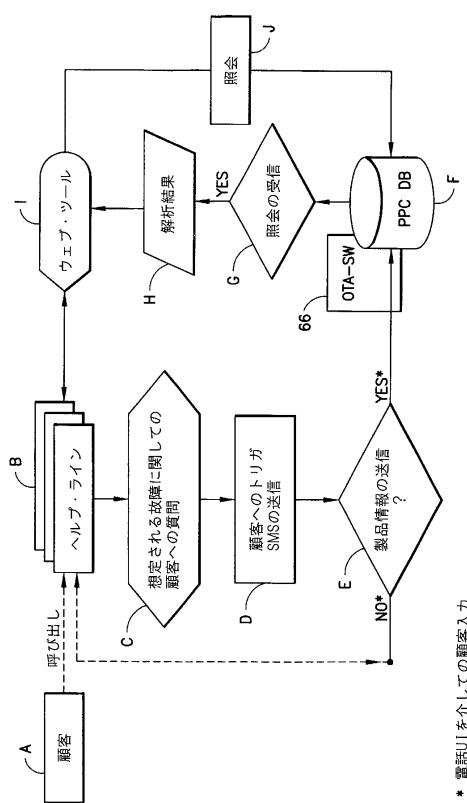


FIG.6

フロントページの続き

(72)発明者 コイブカンガス , タピオ
　　フィンランド国 , エフィーエン - 9 0 8 5 0 マルティンニエミ , クーシコンムトカ 9
(72)発明者 サロウ , セッポ
　　フィンランド国 , エフィーエン - 9 0 8 0 0 オウル , ポンッティイティエ 5
(72)発明者 テルボ , ティモ ペー .
　　フィンランド国 , エフィーエン - 9 0 5 2 0 オウル , キラモカトウ 4 セー 5
(72)発明者 ハイリュネン , アンッティ
　　フィンランド国 , エフィーエン - 9 0 1 0 0 オウル , アルバーティンカトウ 1 1 アー 1 0
(72)発明者 ルイロ , ベサ
　　フィンランド国 , エフィーエン - 9 0 3 1 0 オウル , アイサケッロンティエ 3 アー 6

審査官 望月 章俊

(56)参考文献 米国特許第 0 6 0 8 8 5 8 8 (U S , A)
　　国際公開第 9 9 / 0 2 3 8 4 9 (WO , A 1)
　　国際公開第 9 8 / 0 3 8 8 2 3 (WO , A 1)
　　国際公開第 0 1 / 0 7 6 1 3 6 (WO , A 1)
　　国際公開第 0 0 / 0 0 2 3 5 8 (WO , A 1)
　　欧州特許出願公開第 0 1 0 6 3 8 6 1 (E P , A 1)

(58)調査した分野(Int.CI. , D B 名)

H04B7/24-H04B7/26
H04W4/00-H04W99/00