

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
28 December 2006 (28.12.2006)

PCT

(10) International Publication Number
WO 2006/136660 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/FI2006/050271

(22) International Filing Date: 19 June 2006 (19.06.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20055333 21 June 2005 (21.06.2005) FI
60/707,170 11 August 2005 (11.08.2005) US

(71) Applicant (for all designated States except US): SEVEN NETWORKS INTERNATIONAL OY [FI/FI]; Paciuk-senkatu 29, FI-00270 Helsinki (FI).

(72) Inventors; and

(75) Inventors/Applicants (for US only): BACKHOLM, Ari [FI/FI]; Koivistontie 14 E, FI-02140 Espoo (FI). SALORINNE, Seppo [FI/FI]; Juustilanpolku 7, FI-00950 Helsinki (FI). AHONEN, Jukka [FI/FI]; Huvilinnantie 5 C 37, FI-02600 Espoo (FI). DAAVITILA, Mikko [FI/FI]; Klaneettitie 1 A 11, FI-00420 Helsinki (FI). EVERITT, Andrew [GB/GB]; 19 Coles Road, Milton Cambridgeshire CB4 6 BL (GB). VUORNOS, Lauri [FI/FI]; Vaasankatu 23 A 28, FI-00500 Helsinki (FI).

(74) Agent: KOLSTER OY AB; Iso Roobertinkatu 23, P.O. Box 148, FI-00121 Helsinki (FI).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

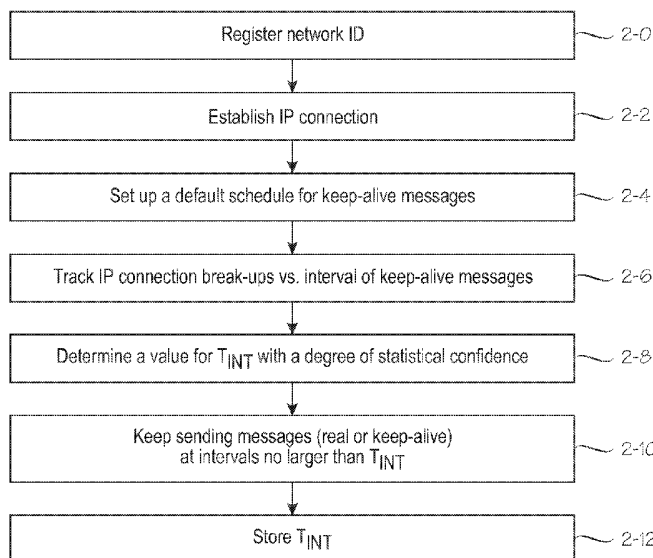
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

— as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))

[Continued on next page]

(54) Title: MAINTAINING AN IP CONNECTION IN A MOBILE NETWORK



(57) Abstract: A method for IP [=Internet Protocol] communication between a mobile terminal and its correspondent node in a mobile radio network. The method comprises establishing (2-2) an IP connection between the mobile terminal and its correspondent node. After detecting a period of inactivity in the IP connection, (2-4) keep-alive messages are sent via the IP connection at predetermined intervals, which are varied. The method comprises monitoring (2-6) the lengths of several periods of inactivity at which the mobile radio network disconnects the IP connection. Based on the monitored lengths of periods of inactivity, a maximum interval (T_{INT}) between keep-alive messages is determined (2-8) such that the maximum interval meets a predetermined criterion of statistical confidence, and the interval between keep-alive messages is set (2-10) to the maximum interval (T_{INT})-

WO 2006/136660 A1



Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Maintaining an IP connection in a mobile network

Background of the invention

[0001] The invention relates to techniques for maintaining an IP (Internet protocol) connection in a mobile network.

5 [0002] In a packet-switched mobile network, a mobile terminal is not normally assigned a dedicated circuit-switched connection. Instead, the network establishes and maintains a session for the terminal, and data packets are sent when necessary. In order to integrate mobile terminals with office applications, it is becoming increasingly popular to maintain Internet Protocol
10 (IP) connections over packet data channels in packet-switched mobile networks. Maintaining an IP connection to/from a mobile terminal is desirable in order to keep data banks synchronized between the mobile terminal and an office computer, for example.

[0003] Maintaining an IP connection in packet-switched mobile networks
15 involves certain problems. For example, it consumes the mobile terminal's battery. Further, many networks apply operator-defined policies to break connections after a certain period of inactivity. This period can be quite short, such as five minutes. When the IP connection to/from the mobile terminal is disconnected, database synchronization is impossible before connection re-
20 establishment. Connection re-establishment must be initiated from the mobile terminal's side, the network cannot initiate connection re-establishment.

[0004] But connection re-establishment involves further expenses in tariff and/or battery consumption. Yet further, since the network cannot initiate re-establishment of the IP connection, network-initiated data synchronization
25 must be initiated by means of an out-band trigger, ie, signalling independent from the Internet Protocol. A short message service (SMS) and its derivatives are examples of theoretically suitable out-band triggering mechanisms. But a single GSM-compliant short message can only transfer approximately 160 characters, which means that it is impracticable to transfer actual data in the
30 trigger message. This has the consequence that the subscriber must bear the expenses and delays in re-establishing the IP connection.

[0005] The mobile terminal can send keep-alive messages in order to prevent the network from disconnecting a temporarily inactive IP connection. A keep-alive message is a message sent for the purpose of preventing the network
35 from disconnecting the IP connection.

[0006] The mobile terminal's operating parameters in respect of the keep-alive messages could be optimized for a single network, but connection break-up habits vary between networks and in a single network they may depend on roaming arrangements between operators.

5 **Brief description of the invention**

[0007] An object of the present invention is to provide a method, equipment and a computer program product to so as to alleviate the above disadvantages relating to connection break-up in packet-switched mobile radio networks. The object of the invention is achieved by the methods and equipment which are
10 characterized by what is stated in the independent claims. Preferred embodiments of the invention are disclosed in the dependent claims.

[0008] The invention is based on the following idea. An IP connection is established between the mobile terminal and its correspondent node. During periods of inactivity in the IP connection, keep-alive messages are sent at a
15 predetermined schedule. Keep-alive messages can be quite short, such as 10 bytes, but they prevent the network from detecting the connection as inactive, whereby it is not disconnected. The keep-alive schedule is varied. At least one of the parties monitors the lengths of several periods of inactivity at which the mobile radio network disconnects the IP connection. Based on several
20 monitored lengths of periods of inactivity, a maximum interval between keep-alive messages is determined such that the maximum interval meets some predetermined criterion of statistical confidence. In other words, spurious connection break-ups, which are not avoidable by keep-alive messages, are ignored. The interval between keep-alive messages is set to the determined
25 maximum interval.

[0009] An aspect of the invention is a method according to claim 1. Other aspects of the invention relate to computer systems or program products for implementing the above methods.

Brief description of the drawings

30 [0010] In the following the invention will be described in greater detail by means of specific embodiments with reference to the attached drawings, in which

Figure 1 shows an exemplary network arrangement in which the invention can be used;

35 Figure 2 shows a flowchart illustrating an embodiment of the invention; and

Figures 3A and 3B illustrate a technique for determining a maximum interval between keep-alive messages by means of a cumulative probability function.

Detailed description of specific embodiments

[0011] The invention is applicable to virtually any mobile network architecture.

5 The mobile network may be based on GPRS, 1xRTT or EVDO technologies, for example. The invention can also be implemented as part of a push-type mobile e-mail system, particularly in a consumer e-mail system, in which optimization of network resources is important because of the large number of users.

10 **[0012]** Figure 1 shows an exemplary system architecture which is supported by the owner of the present application. This system supports synchronization of e-mail messages and/or calendar items and/or other information between a host system and a mobile terminal.

[0013] Reference numeral 100 denotes a host system that is able to send an
15 receive e-mail messages. Reference numeral 102 denotes a mobile terminal, also able to send an receive e-mail messages. The e-mail messages may originate or terminate at external e-mail terminals, one of which is denoted by reference numeral 104. The invention aims at improving cooperation between the host system 100 and mobile terminal 102 such that they can use a single
20 e-mail account as transparently as possible. This means, for example, that the users of the external e-mail terminals 104, when sending or receiving e-mail, do not need to know if the user of the host system 100 actually uses the host system 100 or the mobile terminal 102 to communicate via e-mail. The transparency also means that e-mail manipulation at the mobile terminal 102
25 has, as far as possible, the same effect as the corresponding e-mail manipulation at the host system 100. For example, e-mail messages read at the mobile terminal 102 should preferably be marked as read at the host system.

[0014] Reference numeral 106 denotes a data network, such as an IP (Internet
30 Protocol) network, which may be the common Internet or its closed subnetworks, commonly called intranets or extranets. Reference numeral 108 denotes an e-mail server and its associated database. There may be separate e-mail servers and/or server addresses for incoming and outgoing e-mail. The database stores an e-mail account, addressable by means of an e-mail
35 address, that appears as a mailbox to the owner of the e-mail account. In order to communicate with mobile terminals 102, the data network 106 is connected,

via a gateway 112 to an access network 114. The access network comprises a set of base stations 116 to provide wireless coverage over a wireless interface 118 to the mobile terminals 102.

[0015] Reference numeral 110 denotes a messaging centre that is largely responsible for providing the above-mentioned transparency between the host system 100 and the mobile terminal 102. The system architecture also comprises a connectivity function 120, whose task is to push e-mail messages to the mobile terminal. In the embodiment shown in Figure 1, the connectivity function 120 is considered a physically integral but logically distinct element of the messaging centre 110.

[0016] The mobile terminal 102 may be a pocket or laptop computer with a radio interface, a smart cellular telephone, or the like. Depending on implementation, the host system 100, if present, may have different roles. In some implementations the host system 100 is optional and may be a conventional office computer that merely acts as the mobile terminal user's principal computer and e-mail terminal. In other implementations the host system may act as a platform for a single user's connectivity function, in addition to being an office computer. In yet other implementations the host system 100 may comprise the connectivity function for several users. Thus it is a server instead of a normal office computer.

[0017] We assume here that the access network 114 is able to establish and maintain a IP connection 122 between the messaging centre 110 and the mobile terminal 102.

[0018] Figure 1 shows an embodiment in which the messaging centre 110 is largely responsible for e-mail transport to/from the mobile terminal 102 via the access network 114, while a separate connectivity function 120 is responsible for data security issues. The connectivity function 120 may be physically attached to or co-located with the messaging centre 110, but they are logically separate elements. Indeed, a definite advantage of the separate connectivity function 120 is that it can be detached from the messaging centre, for instance, within the company that owns the host system 100 or the e-mail server 108. For a small number of users, the connectivity function 120 can be installed in each host system 100, or the host system 100 can be interpreted as a separate server configured to support multiple users. It is even possible to implement some or all the above-mentioned options. This means, for example, that there is one or more messaging centres 110 that offer services to several

network operators, or they may be a dedicated messaging centre for each network operator (somewhat analogous to short messaging centres). Each messaging centre 110 may have an integral connectivity function 120 to support users who don't wish to install a separate connectivity function in a host system 100. For users who do install a separate connectivity function 120 in their host systems 100, such connectivity functions bypass the connectivity function in the messaging centre 110 and address the messaging centre 110 directly.

[0019] A real e-mail system supports a large number of mobile terminals 102 and IP connections 122. In order to keep track of which e-mail account and which IP connection belongs to which mobile terminal, the messaging centre 110 and the connectivity function collectively maintain an association 124, 124' for each supported mobile terminal. Basically, each association 124, 124' joins three fields, namely an e-mail address 124A assigned to the mobile terminal or its user, encryption information 124C and a temporary wireless identity 124D of the mobile terminal in the access network. The embodiment shown in Figure 1 also employs a terminal identifier 124B which may be the same as the e-mail address 124A of the mobile terminal 102, in which case the association 124 actually associates three information items. Alternatively, the terminal identifier 124B may be an identifier arbitrarily assigned to the mobile terminal. In a preferred implementation the terminal identifier 124B is the mobile terminal's equipment identifier or its derivative. The encryption information 124C is preferably related to the mobile terminal's equipment identity and is preferably generated by the mobile terminal itself, so as to ensure that no other terminal besides the one used for creating the encryption information 124C will be able to decrypt incoming encrypted e-mail messages. The temporary wireless identity 124D may be the identifier of the IP connection 122 to the mobile station.

[0020] In the above-described system, the messaging centre 110 and connectivity function 120 were arranged to support a fairly large number of users of e-mail and/or calendar data. In order to satisfy the needs of the present invention, virtually any communication server able to maintain an IP connection to the mobile terminal can be used.

[0021] Figure 2 shows a flowchart illustrating an embodiment of the invention. In an optional step 2-0 the network identifier is registered, which means that the method steps should be performed and the resulting parameters

maintained separately for each network. In step 2-2 an IP connection is established between the mobile terminal and its correspondent node. The connection establishment can be entirely conventional. Initially, in step 2-4, the mobile terminal and/or its correspondent node sends keep-alive messages when the IP connection is otherwise idle, ie, when there is no net user data to send. The keep-alive messages are sent according to a predetermined schedule. The schedule may be empty, which means that the mobile terminal may initially send no keep-alive messages at all. In step 2-6 the mobile terminal and/or its correspondent node keeps track of the periods of time after which the network disconnects the IP connection. The period of inactivity after which the network disconnects the IP connection will be called maximum inactivity period. A problem is that the mobile terminal does not know the true value of the maximum inactivity period; the network operator does not publish it. In an embodiment of the invention, the true value of the maximum inactivity period is approached from either direction (upwards and downwards) by altering the schedule for transmitting the keep-alive messages. On the other hand, it is not economically feasible to simply accept the shorted inactivity period before connection break-up as the value of the maximum inactivity period, because connection break-ups may occur for reasons which are not repeatable. In other words, many of the early connection break-ups occur regardless of the keep-alive messages, and attempting to eliminate such spurious break-ups by more frequent keep-alive messages will only result in increased battery drain and/or telecommunication tariffs.

[0022] Accordingly, step 2-8 comprises achieving a desired degree of statistical confidence in respect of the detected maximum inactivity period. In order to achieve statistical significance, the mobile terminal applies a confidence measure, such as variance. In a typical but non-restricting implementation, the mobile terminal may regard the connection break-up as regular if it happens after a certain inactivity period with a variance lower than some predetermined value. For example, the connection break-up may be considered regular if the network has discontinued the IP connection a predetermined minimum number x of times after an inactivity period of t , wherein the distribution of t has a variance $\text{var}(t)$ which is smaller than some predetermined value y .

[0023] The act of achieving a desired degree of statistical confidence preferably comprises subtracting a safety margin Δt from the detected

maximum inactivity period. For example, the safety margin may be expressed in minutes, such as 1 - 2 minutes, or as a percentage, such as 10 - 20%. If the detected maximum inactivity period is, say, 15 minutes, the mobile terminal may store a value of 13 - 14 minutes as a maximum safe interval between
5 keep-alive messages. Let us denote this interval value by T_{INT} .

[0024] In step 2-10 the mobile terminal and/or its correspondent node set up a schedule for sending keep-alive messages at intervals no higher than T_{INT} in absence of net user traffic. By sending keep-alive messages via an otherwise
10 idle IP connection at intervals no higher than T_{INT} , the network regards the IP connection as active and, under normal operating conditions, does not disconnect it.

[0025] The keep-alive messages can be sent by either end of the connection, ie, by the mobile terminal and/or its correspondent node, such as a server, in the fixed part of the mobile radio network.

[0026] Sending the keep-alive messages at intervals no higher than T_{INT} can
15 be accomplished by means of a timer, which may be a physical timer or a logical one, such as a program thread or process. Each time any message is sent (either a real message or a keep-alive message), a timer with a value T_{INT} is triggered. When the timer expires, a keep-alive message is sent and the
20 timer is re-triggered.

[0027] The optimum value for the safety margin safety margin Δt depends on the costs (battery-wise and tariff-wise) of sending keep-alive messages and re-
25 establishing disconnected IP connections. It may also depend on the behaviour of the network, ie, the regularity by which it breaks up temporarily inactive connections. If the network's behaviour is poorly predictable, and break-ups occurs with a certain safety margin, the safety margin should be increased.

[0028] In a further optional step 2-12, the maximum safe interval between
30 keep-alive messages, T_{INT} , is stored together with an identifier of the network in which the T_{INT} was determined, whereby it can be quickly taken into use on re-entry to the same network. This value can be stored in the mobile terminal. Instead of storing the value in the mobile terminal, or in addition to it, the mobile terminal may send the value to its home network to be stored in a data
35 base which can be inquired by mobile terminals which are about to begin roaming in a foreign network. The value stored by other mobile terminals in the

data base in the home network may override any default value otherwise used by the roaming mobile terminal.

[0029] Instead of sending the keep-alive messages from the mobile terminal, or in addition to it, the keep-alive messages may be sent from a stationary server connected to the mobile radio network.

[0030] Figures 3A and 3B illustrate a technique for determining a maximum interval between keep-alive messages by means of a cumulative probability function. The vertical bars in Figure 3A, collectively denoted by reference numeral 32, show counts of connection break-up versus interval between keep-alive messages. In this example, one break-up was detected at intervals of 5, 7, 8 and 9 minutes. Two break-ups were detected at an interval of 10 minutes, five at 11 minutes, seven at 12 minutes and, finally, three break-ups at an interval of 13 minutes. No idle connection survived for longer than 13 minutes.

[0031] Reference numeral 34 in Figure 3B shows a cumulative probability function which illustrates a cumulative probability for the network breaking up an idle connection versus interval between keep-alive messages, given the monitoring data shown in Figure 3A. As shown by function 34, all idle connection survived for 4 minutes and none survived for longer than 13 minutes. Reference numeral 35 denotes a line of maximum derivative in the cumulative probability function 34. It is reasonable to assume that the line of maximum derivative coincides with the maximum period of inactivity tolerated by the network. Or, if the cumulative probability function 34 is drawn as discrete steps (jumps), the position of line 35 can be determined by the highest jump in line 34.

[0032] This maximum period is denoted by reference numeral 36, and its value is approximately 11.5 minutes in this example. A value of 10 minutes for T_{INT} is appropriate, as indicated by dashed line 37. Reference numeral 38 denotes a safety margin between the lines 36 and 37.

[0033] Although this example shows that as much as 30% of connections were disconnected after 10 minutes of inactivity, it is reasonable to assume that these disconnections were caused by spurious effects rather than the network's policy to break up idle connections.

[0034] It is readily apparent to a person skilled in the art that, as the technology advances, the inventive concept can be implemented in various

ways. The invention and its embodiments are not limited to the examples described above but may vary within the scope of the claims.

Claims

1. A method for IP [=Internet Protocol] communication between a mobile terminal and its correspondent node in a mobile radio network, the method comprising:
- 5 - establishing (2-2) an IP connection between the mobile terminal and its correspondent node;
- in response to detecting a period of inactivity in the IP connection, sending (2-4) keep-alive messages via the IP connection at predetermined intervals;
- 10 - varying the predetermined intervals and monitoring (2-6) the lengths of several periods of inactivity at which the mobile radio network disconnects the IP connection;
- based on the several monitored lengths of periods of inactivity, determining (2-8) a maximum interval (T_{INT}) between keep-alive
- 15 messages such that the maximum interval meets a predetermined criterion of statistical confidence; and
- setting (2-10) the interval between keep-alive messages to the maximum interval (T_{INT}).
2. A method according to claim 1, further comprising sending the
- 20 keep-alive messages from the mobile terminal.
3. A method according to claim 1 or 2, further comprising sending the keep-alive messages from the correspondent node.
4. A method according to any one of the preceding claims, further comprising determining the maximum interval (T_{INT}) in the mobile terminal.
- 25 5. A method according to any one of the preceding claims, further comprising determining the maximum interval (T_{INT}) in the correspondent node.
6. A method according to any one of the preceding claims, further comprising storing (2-12) the maximum interval (T_{INT}) in the mobile terminal, in association with an identifier of the mobile radio network.
- 30 7. A method according to any one of claims 1 - 5, further comprising sending the maximum interval (T_{INT}) in association with the identifier of the

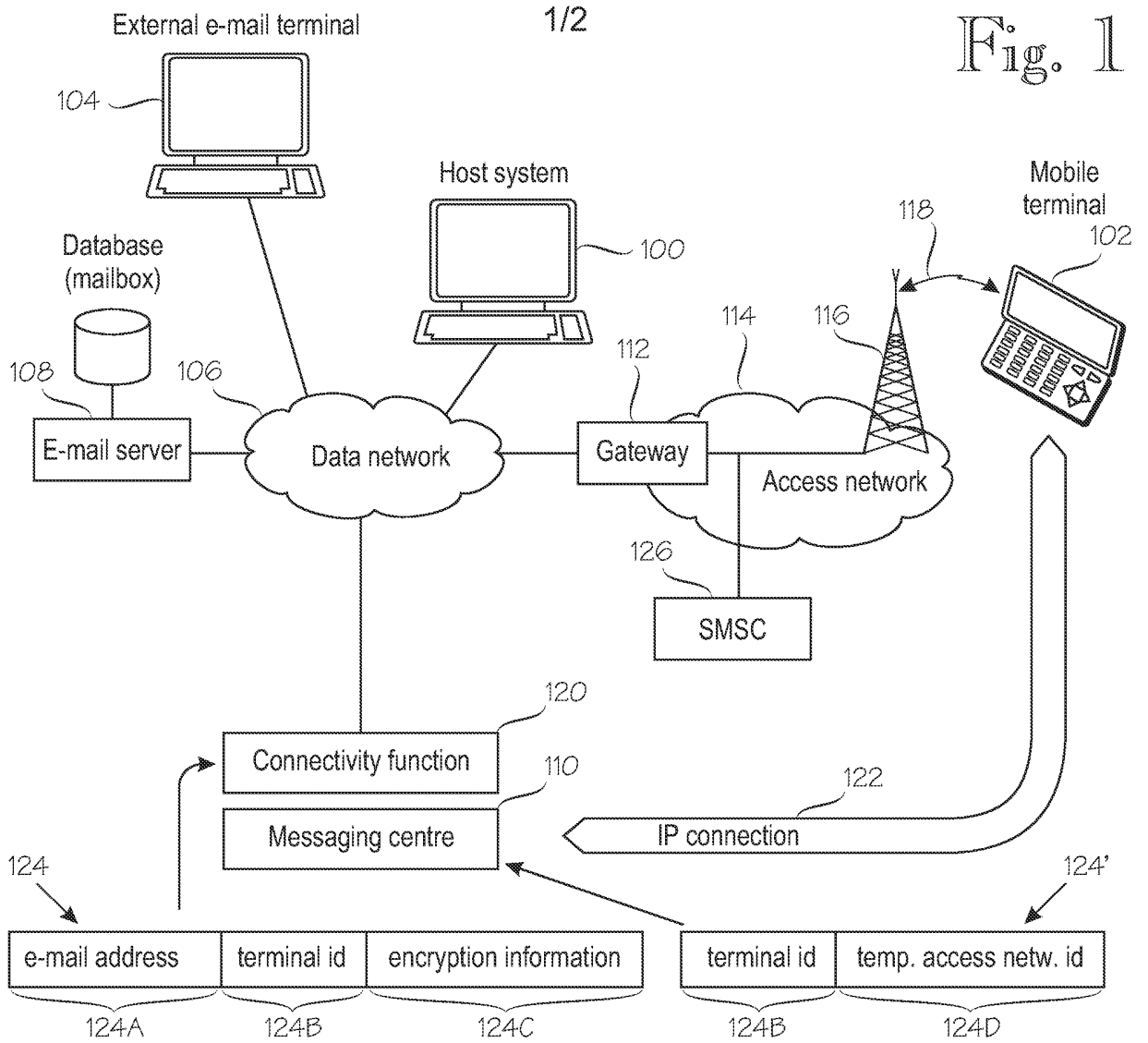
mobile radio network to the mobile terminal's home network for storage and future inquiry.

8. A mobile terminal for a mobile network, the mobile terminal comprising:

- 5 - means for establishing (2-2) an IP connection between the mobile terminal and its correspondent node;
- means, responsive to detecting a period of inactivity in the IP connection, for sending (2-4) keep-alive messages via the IP connection at predetermined intervals;
- 10 - means for varying the predetermined intervals and monitoring (2-6) the lengths of several periods of inactivity at which the mobile radio network disconnects the IP connection;
- means for determining (2-8) a maximum interval (T_{INT}) between keep-alive messages such that the maximum interval meets a predetermined criterion of statistical confidence, based on the
15 several monitored lengths of periods of inactivity; and
- means for setting (2-10) the interval between keep-alive messages to the maximum interval (T_{INT}).

9. A computer program product for a mobile terminal, the computer
20 program product causing the mobile terminal to carry out the steps of claim 1 when the computer program product is executed in the mobile terminal.

Fig. 1



2/2

Fig. 2

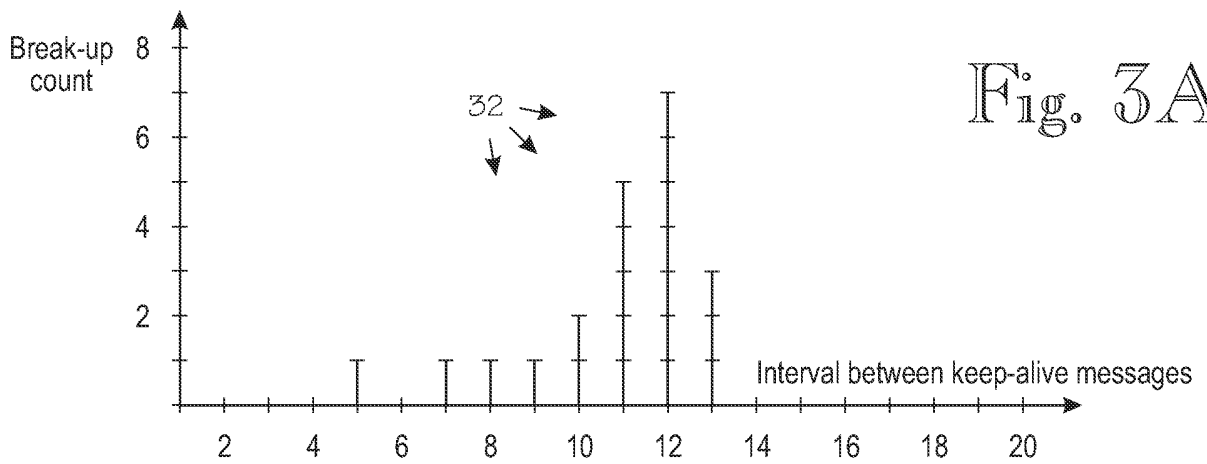
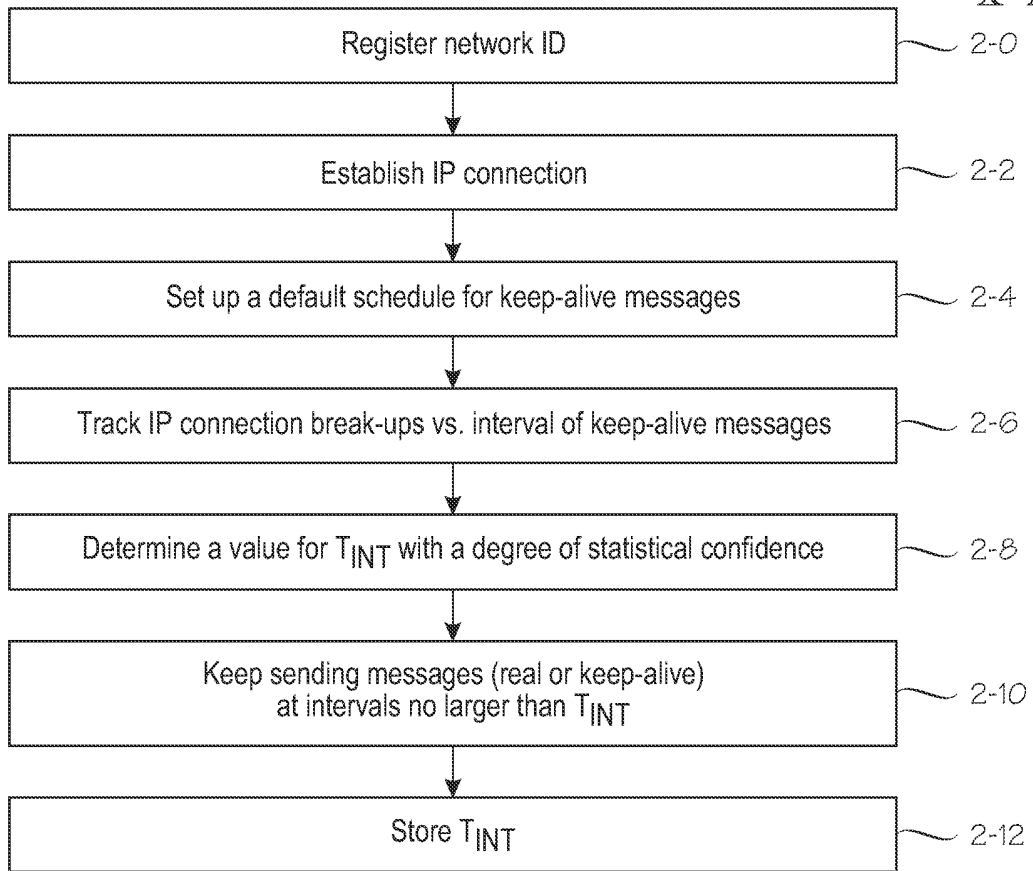


Fig. 3A

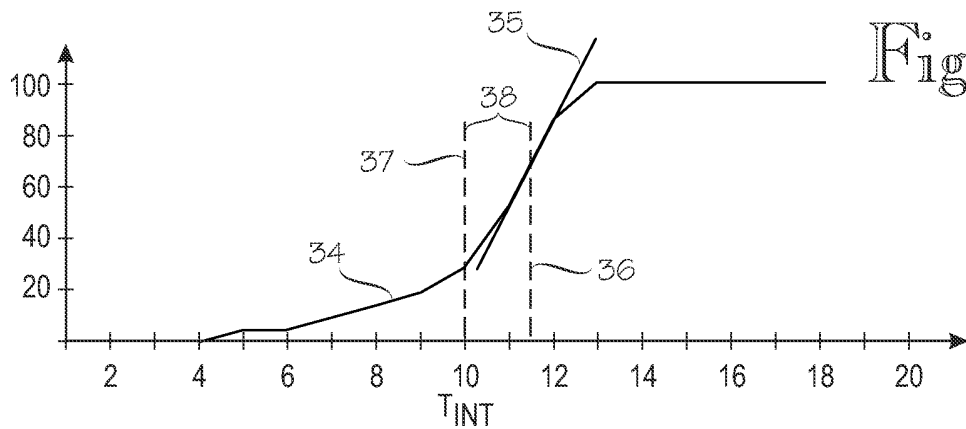


Fig. 3B

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2006/050271

A. CLASSIFICATION OF SUBJECT MATTER		
See extra sheet		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols)		
IPC 8: H04L, H04Q		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
DK, FI, NO, SE		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
EPO-Internal, WPI, PAJ		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6212175 B1 (HARSCH) 03 April 2001 (03.04.2001)	
A	EP 1107519 B1 (NORTEL NETWORKS CORPORATION) 13 June 2001 (13.06.2001)	
A	US 2003128676 A1 (LEE) 10 July 2003 (10.07.2003)	
A	WO 03067447 A1 (KT FREETEL CO LTD) 14 August 2003 (14.08.2003)	
A	WO 2005024569 A2 (MAIN, JAMES) 17 March 2005 (17.03.2005)	
A	US 6006259 A (ADELMAN ET AL.) 21 December 1999 (21.12.1999)	
A	Internet Engineering Task Force. Network Working Group RFC 1122. October 1989. 4.2.3.6 TCP Keep-Alives pages 101-102. Retrieved from Internet address <URL:http://www.ietf.org/rfc/rfc1122.txt?number=1122> [Retrieved on 28.08.2006]	
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed		"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family
Date of the actual completion of the international search		Date of mailing of the international search report
30 August 2006 (30.08.2006)		25 September 2006 (25.09.2006)
Name and mailing address of the ISA/FI National Board of Patents and Registration of Finland P.O. Box 1160, FI-00101 HELSINKI, Finland Facsimile No. +358 9 6939 5328		Authorized officer Tapio Ikäheimo Telephone No. +358 9 6939 500

CLASSIFICATION OF SUBJECT MATTER

Int.Cl.
H04L 29/06 (2006.01)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2006/050271

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P, X	EP 1569404 A1 (RESEARCH IN MOTION LIMITED) 31 August 2005 (31.08.2005), paragraphs [0015]-[0018], [0023], [0033]-[0034]	1-5, 8-9

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/FI2006/050271

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
US 6212175 B1	03/04/2001	None	
EP 1107519 B1	13/06/2001	DE 60018023D D1 DE 60018023T T2 CA 2311108 A1	17/03/2005 14/07/2005 08/06/2001
US 2003128676 A1	10/07/2003	KR 2003060491 A	16/07/2003
WO 03067447 A1	14/08/2003	AU 2002232275 A1	02/09/2003
WO 2005024569 A2	17/03/2005	US 2005050209 A1	03/03/2005
US 6006259 A	21/12/1999	EP 1131931 A1 WO 0031945 A1 JP 2003517221T T AU 6518899 A CA 2351414 A1	12/09/2001 02/06/2000 20/05/2003 13/06/2000 02/06/2000
EP 1569404 A1	31/08/2005	CA 2498311 A1 CN 1658558 A	25/08/2005 24/08/2005