PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
H04Q 7/38, H04L 9/32

A1

(11) International Publication Number: **WO 00/69206**

(43) International Publication Date: 16 November 2000 (16.11.00)

(21) International Application Number: PCT/FI00/00421

(22) International Filing Date: 11 May 2000 (11.05.00)

(30) Priority Data:
991088 11 May 1999 (11.05.99) FI

(71) Applicant *(for all designated States except US)*: NOKIA NETWORKS OY [FI/FI]; P.O. Box 300, FIN–00045 Nokia Group (FI).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: NIEMI, Valtteri [FI/FI]; Itämerenkatu 11–13, FIN–00180 Helsinki (FI). RAJANIEMI, Jaakko [FI/FI]; Lapinrinne 2 A 11, FIN–00180 Helsinki (FI). MUHONEN, Ahti [FI/FI]; Holperintie 39, FIN–04680 Hirvivaara (FI).

(74) Agent: BERGGREN OY AB; P.O. Box 16, FIN–00101 Helsinki (FI).

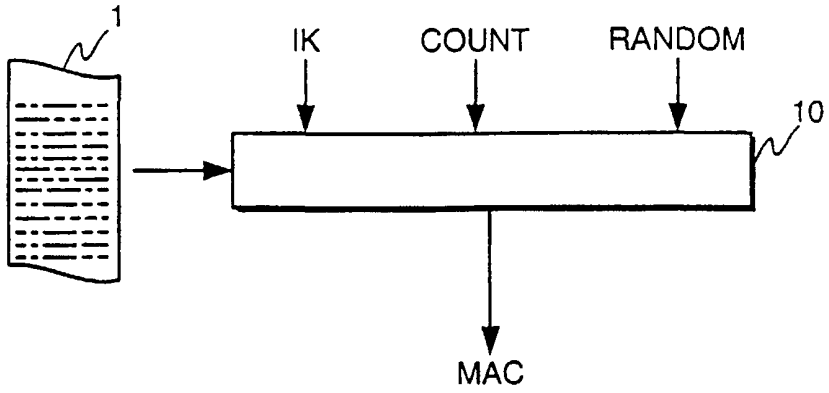
(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: INTEGRITY PROTECTION METHOD FOR RADIO NETWORK SIGNALING

(57) Abstract

The invention is directed to a method for checking the integrity of messages between a mobile station and the cellular network. Two time–varying parameters are used in MAC calculation, one of which is generated by the mobile station, and the other by the network. The parameter specified by the network is used in one session only, and is transmitted to the mobile station in the beginning of the connection. The parameter specified by the mobile station is stored in the mobile station between connections in order to allow the mobile station to use a different parameter in the next connection. The parameter specified by the mobile station is transmitted to the network in the beginning of the connection.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Integrity protection method for radio network signaling

TECHNICAL FIELD OF THE INVENTION

The invention is directed to a method for checking the integrity of messages between a mobile station and the cellular network. Particularly, the invention is directed to such a method as described in the preamble of Claim 1.

BACKGROUND OF THE INVENTION

All telecommunication is subject to the problem of how to make sure that the received information is sent by an authorized sender and not by somebody who is trying to masquerade as the sender. The problem is evident in cellular telecommunication systems, where the air interface presents an excellent platform for eavesdropping and replacing the contents of a transmission by using higher transmission levels, even from a distance. A basic solution to this problem is authentication of the communicating parties. An authentication process aims to discover and check the identity of both of the communicating parties, so that each party receives information about the identity of the other party, and can trust the identity to a sufficient degree. Authentication is typically performed in a specific procedure at the beginning of the connection. However, this leaves room for unauthorized manipulation, insertion, and deletion of subsequent messages. Thus, there is a need for separate authentication of each transmitted message. The latter task can be done by appending a message authentication code (MAC) to the message at the transmitting end, and checking the MAC value at the receiving end.

A MAC is typically a relatively short string of bits, which depends in some specified way on the message it protects and on a secret key known both by the sender and by the recipient of the message. The secret key is generated and agreed typically in connection with the authentication procedure in the beginning of the connection. In some cases the algorithm that is used to calculate the MAC based on the secret key and the message is also secret but this is not usually the case.

The process of authentication of single messages is often called integrity protection. To protect the integrity of signaling, the transmitting party computes a MAC value based on the message to be sent and the secret key using the specified algoritm, and sends the message with the MAC value. The receiving party recomputes a MAC value based on the message and the secret key according to the specified algorithm,

and compares the received MAC and the calculated MAC. If the two MAC values match, the recipient can trust that the message is intact and sent by the supposed party. One may note in passing, that integrity protection does not usually include protection of confidentiality of the transmitted messages.

Integrity protection schemes are not completely perfect. A third party can try to manipulate and succeed in manipulating a message transmitted between a first and a second party. There are two main alternative methods for forging a MAC value for a modified or a new messages, namely by obtaining the secret key first, and by trying directly without the secret key.

The secret key can be obtained by a third party basically in two ways:
- by computing all possible keys until a key is found, which matches with data of observed message-MAC pairs, or by otherwise breaking the algorithm for producing MAC values; or
- by directly capturing a stored or transmitted secret key.

The original communicating parties can prevent a third party from obtaining the secret key by using an algorithm that is cryptographically strong and which uses a long enough secret key to prevent exhaustive search of all keys, and using other security means for transmission and storage of secret keys.

A third party can try to disrupt messaging between the two parties without a secret key basically by guessing the correct MAC value, or by replaying of some earlier message transmitted between the two parties, for which message the correct MAC is known from the original transmission.

Correct guessing of the MAC value can be prevented by using long MAC values. The MAC value should be long enough to reduce the probability of guessing right to a sufficiently low level compared to the benefit gained by one successful forgery. For example, using a 32 bit MAC value reduces the probability of a correct guess to 1 / 4 294 967 296, which is small enough for most applications.

Obtaining a correct MAC value using the replay attack i.e. by replaying an earlier message can be prevented by introducing a varying parameter to the calculation of the MAC values. For example, a time stamp value, a sequence number, or a random number can be used as a further input to the MAC algorithm in addition to the secret integrity key and the message. The present invention is associated with this basic method. In the following, the prior art methods are described in more detail.

When using a time stamp value, each communicating party needs to have an access to a reliable clock in order to be able to calculate the MAC in the same way. The problem with this approach is the need of the reliable clock. The clocks of both parties must be very accurate and be very accurately in time. However, this condition is unacceptable in cellular telecommunication systems: both parties, i.e. the mobile station (MS) and the network do not have access to a clock, that is reliable enough.

When using sequence numbers, each party has to keep track of those sequence numbers that have already been used and are not acceptable any more. The easiest way to implement this is to store the highest sequence number used in MAC calculations so far. This approach has the drawback, that between connections each party must maintain state information which is at least to some level synchronized. That is, they need to store the highest sequence number used so far. This requires the use of a large database at the network side.

A further approach is to include a random number in each message, which the other side must use in MAC calculation when for the next time sending a message, for which MAC authentication is required. This approach has the same drawback as the previous one, i.e. between connections each party must maintain state information, which requires the use of a large database at the network side.

SUMMARY OF THE INVENTION

An object of the invention is to realize a method for integrity checking, which avoids the problems associated with prior art. A further object of the invention is to provide a method for integrity checking, which does not require storage of state information on the network side.

The objects are reached by using two time-varying parameters in MAC calculation, one of which is generated by the mobile station, and the other by the network. The parameter specified by the network is used in one session only, and is transmitted to the mobile station in the beginning of the connection. The parameter specified by the mobile station is stored in the mobile station between connections in order to allow the mobile station to use a different parameter in the next connection. The parameter specified by the mobile station is transmitted to the network in the beginning of the connection.

The method according to the invention is characterized by that, which is specified in the characterizing part of the independent method claim. The dependent claims describe further advantageous embodiments of the invention.

According to the invention, both parties specify a varying parameter to be used in the generation of MAC values. On the network side in a mobile network, all state information about the particular user can be discarded after the connection is released. According to the invention, both a sequence number and a network specified value such as a pseudorandom number is used in calculation of the MAC value. In the beginning of the connection, the mobile station determines the initial value used for the sequence counting, and transmits the value to the network. In addition to the initial value, a counter value is used. The initial value and the counter value are concatenated, added or combined in some other way to produce the parameter to be used in the calculation of the MAC value of a message. One way of combining the two values is using the initial value as the starting value of the counter, which corresponds to the addition of the counter value and the initial value. The invention does not limit which counter values are used in the inventive method. A suitable value is for example the protocol data unit (PDU) number of the radio link control (RLC) protocol, i.e. the RLC PDU number. Another suitable value is the use of a counter, which is incremented at fixed intervals, for example every 10 milliseconds. Preferably, a counter such as the RLC PDU counter which is already present in mobile stations and in the network is used in a method according to the invention. Further, also counters associated with ciphering of data over the radio interface can be used in a method according to the invention. Further, the invention does not limit which initial value is used in the inventive method. For example, the current hyperframe number at the time of initiating of the connection can be used as the initial value. Further, the counter values do not need to be transmitted after the transmission of the initial value, since both sides of the connection can update the counters in the same way during the connection, preserving synchronization. Preferably, when a connection is released, the mobile station stores into its memory the initial value used in the connection or at least the most significant bits of the initial value, which allows the mobile station to use a different initial value next time. The mobile station can save the information for example in the SIM (Subscriber Identity Module) card or another memory device, for allowing the mobile station to use a value previously stored in the SIM card of the mobile station in specifying the initial value.

The network specifies the random number, or in practice a pseudorandom number in the beginning of the connection. The random number is session specific, i.e. it does not need to be changed within a connection or transmitted to the mobile station more than once in the beginning of the connection, and neither does it need to be stored in the network between connections. Advantageously, the network element generating the random number and taking care of MAC value generation and checking of received messages and MAC values is the radio network controller (RNC). However, the invention is not limited to that, since these functions can be realized in many other network elements as well. The use of RNC is advantageous, since in that case the core network of the cellular telecommunication system does not need to participate in integrity checking of single messages, and since radio access network messaging may also need to be protected by integrity checking.

The invention allows both sides of the connection to perform integrity checking. Since the network specifies a random value in the beginning of the connection, a mobile station of a hostile party cannot succesfully perform a replay attack by replaying a message recorded from a previous connection. Since the mobile station specifies the initial value for the connection, replay attacks from a bogus network element operated by a hostile party will not succeed.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is described in more detail in the following with reference to the accompanying drawings, of which

Figure 1 illustrates an advantageous embodiment of the invention,

Figure 2 illustrates a method according to an advantageous embodiment of the invention, and

Figure 3 illustrates signalling according to an advantageous embodiment of the invention.

Same reference numerals are used for similar entities in the figures.

DETAILED DESCRIPTION

Figure 1 illustrates a way of calculating the MAC value according to the invention. The IK is the secret integrity key, which is generated during a mobile station authentication procedure in the beginning of a connection. Because the same IK key is used to authenticate many messages possibly even during many consecutive

connections, time-varying parameters are needed to avoid hostile attacks during the connection. For that purpose, a counter value COUNT and a random value RANDOM are used in the MAC calculation as well. According to the invention, a message 1 and the IK, COUNT, and RANDOM values are input into a calculation means 10, which calculates a MAC value according to the inputs and the particular authentication algorithm. We note here, that the invention is not limited to any specific way of calculating the MAC value from the inputs illustrated in figure 1. The invention is not limited to any specific lengths of the input values. For example, for the UMTS (Universal Mobile Telecommunication System) cellular system suitable lengths are 128 bits for the IK value, 32 bits for the COUNT value, 32 bits for the RANDOM value, and 16 bits for the MAC value. However, other lengths could be used even for the UMTS system, and other inputs can be used in addition to these values.

If a new IK value is generated in an authentication process in the beginning of the current connection, the mobile station can reset the initial value of COUNT, since new IK value provides security against replay attacks. The storing of the initial value or a part of it for use with the next connection is necessary, since the IK value might not change, when the next connection is established. This is very probable for example when using a multifunction mobile station in the UMTS system, since the mobile station can have multiple simultaneous connections of various types, and establish and release new connections during a single communication session. The network does not necessarily perform full authentication for each new connection, whereby the mobile station will not always receive a new IK value for each new connection. However, when the IK is changed, the mobile station can reset the initial COUNT values without danger of compromising security.

Figure 2 illustrates a method according to an advantageous embodiment of the invention. Figure 2 illustrates a method for integrity checking of a message transmitted during a connection between a cellular telecommunication network and a mobile station.

In the first step 50, the transmitting party calculates the authentication value (MAC) of the message on the basis of the message, a first value specified by the network, said first value being valid for one connection only, a second value specified at least in part by the network, and a third value at least partly specified by the mobile station. Preferably, said first value is a pseudorandom value such as the RANDOM value described previously. Further, said third value is preferably a counter value such as the COUNT value described previously, which value is incremented during

the connection. For example, the RLC PDU value can be used for generation of the COUNT value. As described previously, the mobile station specifies an initial value for the counter value in the beginning of the connection. The initial value can be used as a starting value for a counter producing the COUNT values, or the initial value can be combined with some other counter value such as the RLC PDU value for producing said third value.

In the next step 52, the message is transmitted from the transmitting party to the receiving party, which calculates a second MAC value as described previously, and compares the received MAC value and the calculated MAC value in step 56. If they are found to be equal, the message is accepted in step 58, and if they are found to be unequal, the message is rejected in step 60. In the case of uplink messaging, the steps of calculation 54 and comparison 56 can advantageously be performed by a radio network controller in the cellular telecommunication network. The method of figure 2 is used for checking the integrity of at least some of uplink and downlink messages.

Figure 3 illustrates one example of how to initiate a connection according to an advantageous embodiment of the invention. Figure 3 shows an advantageous solution to the problem of how to exchange two initial values for the purposes of integrity checking. We note here that the signalling sequence shown in figure 3 is in no way limited to passing only the COUNT and RANDOM values described previously. Signalling according to figure 3 can be used for exchange of any two keys in the beginning of a connection. Figure 3 shows as an example signalling associated with a mobile originated call, but corresponding signalling sequences can be used also in other situations, such as in establishing a mobile terminating call, or in a paging response procedure.

Figure 3 shows a particular example of a method according to the invention. The central idea in figure 3 is, that the RNC stores the message or messages received from the mobile station and authenticated with a MAC value until the time, when it is able to check the MAC value of the message(s). If one or all of the MAC values are later found to be false, the network can then decide, if it should discard the initiated connection.

Figure 3 illustrates signalling between a mobile station MS 20, a radio network controller RNC 30, and core network CN 40 in a situation, in which the mobile station initiates a connection. Figure 3 illustrates the signalling using terminology of the UMTS system. In the first step 100, the mobile station sends the initial

connection request message RRC SETUP REQ to the network. After receiving the connection request message, the RNC generates the RANDOM value, after which the RNC replies by sending 105 an acknowledgment message ACK to the mobile station. The RNC specifies the RANDOM value to the mobile station by attaching the value as a parameter to the ACK message, which is shown in figure 3 by the label RANDOM appearing under the arrow 105. After receiving the acknowledgment and the RANDOM value, the mobile station needs to send the initial COUNT value to the network. This can be realized basically in two ways: by defining a new message for that purpose, for example in the RRC level, or by attaching the COUNT value as a parameter to an existing message. Arrow 110 denotes the former approach, i.e. denotes a message specifically defined for transmitting the COUNT value. Arrow 115 denotes the latter approach, i.e. attaching the COUNT value as a parameter to an existing message. In the example of figure 3, the existing message is a CM SERV REQ message. Further, also an IK key identification number may be transmitted as a parameter to the message. During an authentication process in which an IK is generated, each IK is assigned an identification number, whereafter the MS and the network may refer to the IK simply by using the identification number.

In the example of figure 3, the mobile station sends a classmark service request message CM SERV REQ to the network, specifying a temporary identifier TMSI and a capability class identifier CM2 to the network. If a specific message was not used to transport the initial COUNT value to the network, the initial COUNT value is passed to the network as a further parameter to the CM SERV REQ message. Further, the mobile station transmits a MAC value calculated on the basis of the COUNT and RANDOM values, and an IK value received and stored during a previous connection. Upon receiving the message, the RNC removes and stores the MAC value from the message as well as the possibly existing COUNT value, and forwards 120 the rest of the message to the core network. The RNC stores the whole message as well for later use, which will be described later. According to UMTS specifications, the core network may perform an authentication procedure at this stage, which is represented by arrows 125 and 130 in figure 3, corresponding to authentication request AUTH REQ and authentication response AUTH RSP messages.

The next step depends on whether the network has an IK value for the mobile station or not. If the network performed the authentication in steps 125 and 130, the network has the IK value determined in the authentication. Alternatively, the

network may have an old IK value stored in relation to a previous connection. The IK value is stored in the core network registers. If the network has an IK value, the method continues at step 135; if not, at step 150. This is represented by step 132 and the associated dashed arrow in figure 3.

In step 135, the core network sends a ciphering mode CIPH MODE message to the RNC, attaching the ciphering key CK and the IK value as parameters to the message. With this message, the CN supplies the IK value to the RNC, which was previously unaware of the IK value, if the authentication procedure was not performed at steps 125 and 130. At this stage, the RNC is able to check the CM SERV REQ message stored at step 115, since it now has the COUNT, the RANDOM, and the IK values necessary for calculating the MAC value of the message. The RNC calculates a MAC value and compares 137 it to the MAC value stored previously at step 115. If the match, the method continues at step 140. If they do not match, the method continues at step 160.

In step 140, the RNC sends to the MS a CIPHERING COMMAND message to start ciphering, to which the MS replies 145 by sending a ciphering response message CIPHERING RSP back to RNC. After that, the communication continues normally, and the continuation is not depicted in figure 3.

In step 150, the network performs an authentication process, which is represented by arrows 150 and 155 in figure 3, corresponding to authentication request AUTH REQ and authentication response AUTH RSP messages. After that, the core network informs the RNC about the new IK (not shown).

At this stage the RNC needs to make sure, that the MS is the correct one and can calculate the MAC values accordingly. The RNC can perform for example a classmark request procedure or some other suitable procedure to that effect. That is, the RNC sends 160 a classmark request CLASSMARK REQ message to the MS, which replies by sending 165 a response message RSP back to the RNC, attaching the classmark information CM2 as a parameter to the message, and the calculated MAC value at the end of the message. Now the RNC can again check the MAC, and if no hostile party has replayed any of the previous messages, the MAC values calculated by the RNC and the MS will match, since the three key values IK, RANDOM, and COUNT are now known both to the MS and the RNC. After receiving the classmark response message RSP, the RNC sends 170 the classmark information in a CLASSMARK message to the core network, as required by the UMTS specifications.

Although in the previous description, the network is described to specify a random number to be used as the network-specified varying parameter, also other than random values can be used. For example, although being a less advantageous example of an embodiment of the invention, the network may use a counter value, and store the counter value in a central register in order to be able to use a different value during the next connection. Naturally, this embodiment has the disadvantage of the burden of storage of the values of the users to be used in the following connections.

In the previous examples, the invention has been described in relation to a cellular telecommunication system. The invention can be very advantageously used in such a system, since it requires very little messaging, and thus uses only a diminutive amount of valuable air interface resources. However, the invention can be applied also in other communication systems.

The invention has several advantages. For example, according to most advantageous embodiments there is no need for maintaining synchronized state information between different connections. That is, these embodiments do not require the network to store any counter information for effecting the integrity checking which is a considerable advantage, since such storage would have to be effected in a central register such as the VLR (Visitor Location Register) or the HLR (Home Location Register). According to these most advantageous embodimetnts, all state information about the connection can be discarded on the network side in a mobile network after the connection is released. The invention allows the integrity checking to be performed by a network element outside the core network, such as the RNC in the case the UMTS cellular system.

The invention does not specify any upper limit for the number of values used in calculation of MAC values. Any other values in addition to those described for example in relation to figure 1 may be used as well. Further, the invention does not limit, which messages are subjected to integrity checking: all messages, a certain group of messages, or messages selected in some other way.

The name of a given functional entity, such as the radio network controller, is often different in the context of different cellular telecommunication systems. For example, in the GSM system the functional entity corresponding to a radio network controller (RNC) is the base station controller (BSC). Therefore, the term radio network controller is intended to cover all corresponding functional entities regardless of the term used for the entity in the particular cellular tele-

communication system. Further, the various message names such as the RRC SETUP REQ message name are intended to be examples only, and the invention is not limited to using the message names recited in this specification.

In view of the foregoing description it will be evident to a person skilled in the art that various modifications may be made within the scope of the invention. While a preferred embodiment of the invention has been described in detail, it should be apparent that many modifications and variations thereto are possible, all of which fall within the true spirit and scope of the invention.

Claims

1. Method for integrity checking of messages transmitted during a connection between a first party and a second party, in which method an authentication value is calculated for a message,
characterized in that the method comprises steps, in which
the authentication value of a message is calculated on the basis of
- the message,
- a first value specified by the first party, said first value being valid for one connection only,
- a counter value at least partly specified by the second party.

2. A method according to claim 1, **characterized** in that said first party is a cellular telecommunication network and said second party is a mobile station.

3. A method according to claim 1, **characterized** in that the authentication value of a message is calculated also on the basis of a second value specified at least in part by the first party.

4. A method according to claim 1, **characterized** in that said first value is a pseudorandom value.

5. A method according to claim 2, **characterized** in that the mobile station specifies an initial value for the counter value.

6. A method according to claim 2, **characterized** in that the mobile station specifies an initial value which is combined with a counter value for producing said third value.

7. A method according to claim 5, **characterized** in that the mobile station uses a value previously stored in the SIM card of the mobile station in specifying said initial value.

8. A method according to claim 1, **characterized** in that said cellular telecommunication network is an UMTS network, and said first value is specified by a radio network controller.

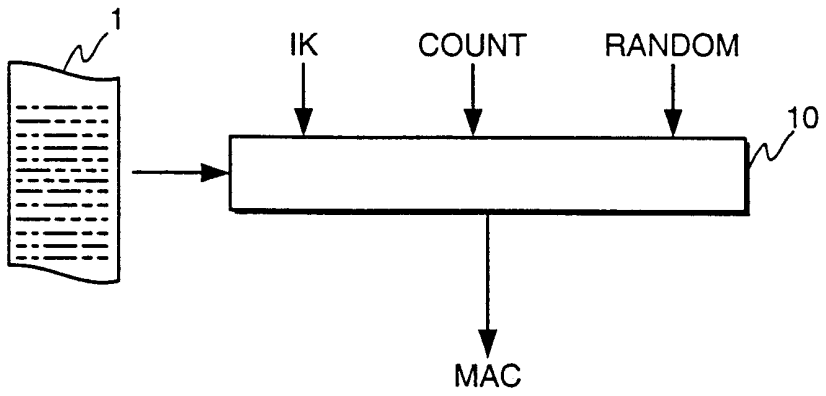

1
IK
COUNT
RANDOM
10
MAC

Fig. 1

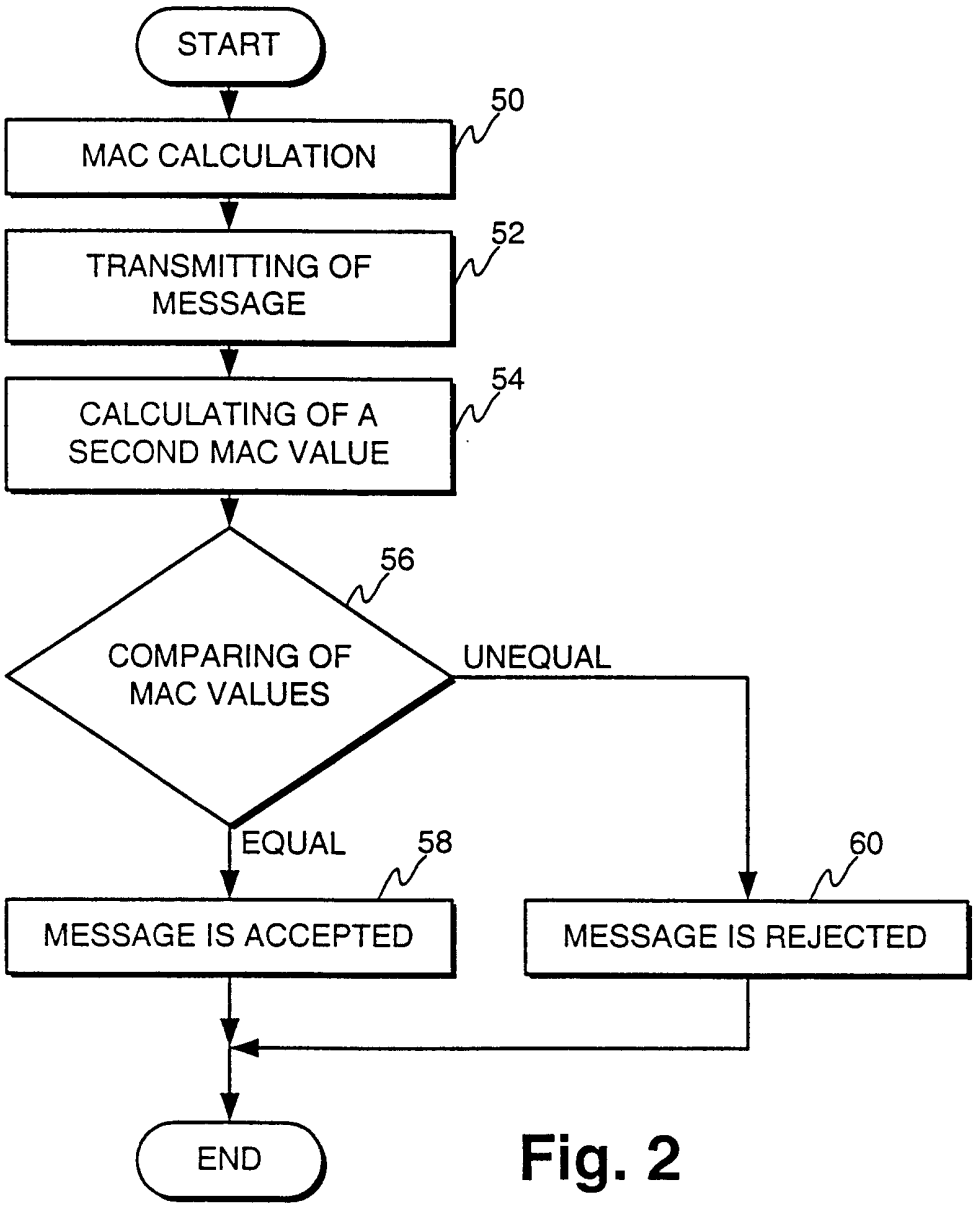

START
MAC CALCULATION
50
TRANSMITTING OF MESSAGE
52
CALCULATING OF A SECOND MAC VALUE
54
COMPARING OF MAC VALUES
56
UNEQUAL
EQUAL
58
60
MESSAGE IS ACCEPTED
MESSAGE IS REJECTED
END

Fig. 2

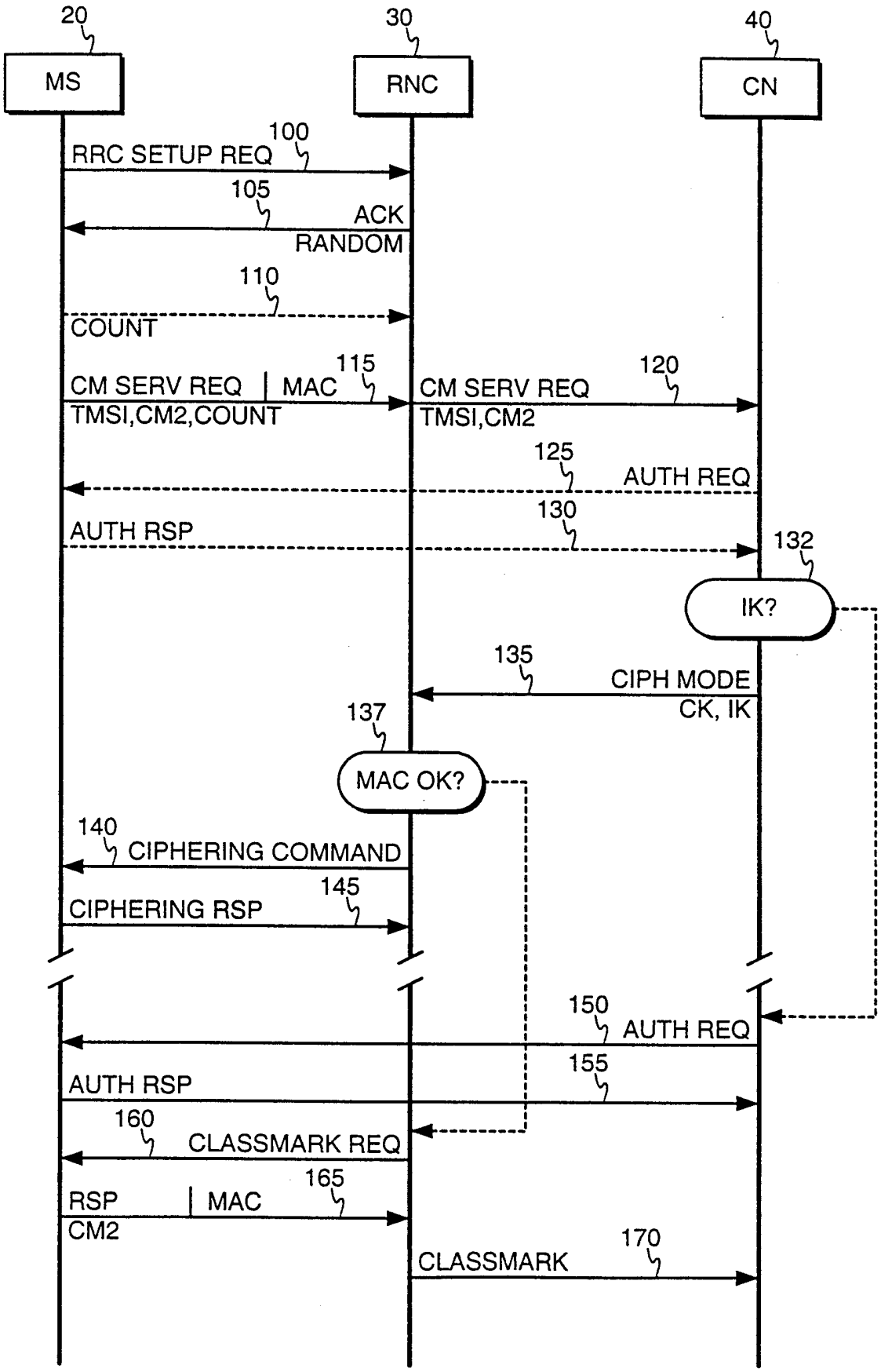

20
30
40
MS
RNC
CN
100
RRC SETUP REQ
105
ACK
RANDOM
110
COUNT
115
CM SERV REQ | MAC
TMSI,CM2,COUNT
120
CM SERV REQ
TMSI,CM2
125
AUTH REQ
130
AUTH RSP
132
IK?
135
CIPH MODE
CK, IK
137
MAC OK?
140
CIPHERING COMMAND
145
CIPHERING RSP
150
AUTH REQ
155
AUTH RSP
160
CLASSMARK REQ
165
RSP | MAC
CM2
170
CLASSMARK

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 00/00421

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/38, H04L 9/32
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)

IPC7: H04Q, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0798673 A1 (KONINKLIJKE PTT NEDERLAND N.V.), 1 October 1997 (01.10.97), column 1, line 46 - column 2, line 49; column 4, line 1 - column 7, line 29, figure 6, claims 1,2,8, abstract	1,3
A	--	2,4-8
Y	US 5475763 A (CHARLES W. KAUFMAN ET AL), 12 December 1995 (12.12.95), column 2, line 35 - column 3, line 4, figure 1, claims 1-12, abstract	1,3
A	--	2,4-8

[X] Further documents are listed in the continuation of Box C. [X] 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" erlier document 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
25 August 2000	29. 09. 2000
Name and mailing address of the International Searching Authority European Patent Office P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel(+31-70)340-2040. Tx 31 651 epo nl. Fax(+31-70)340-3016	Authorized officer Klas Arvidsson/mj Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 00/00421

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 9421066 A1 (TELSTRA CORPORATION LIMITED), 15 Sept 1994 (15.09.94), page 3, line 22 - page 4, line 15, figure 1, claim 1, abstract	1,3
A	--	2,4-8
A	US 5369707 A (ROY D. FOLLENDORE, III), 29 November 1994 (29.11.94), column 2, line 60 - column 4, line 8, figure 4, claims 1-28, abstract	1,3,4
	--	
A	US 5239294 A (MARY B. FLANDERS ET AL), 24 August 1993 (24.08.93), column 4, line 29 - column 5, line 68, figures 2,3, claims 1-32, abstract	1,3,4
	--	
A	US 5592553 A (RICHARD H. GUSKI ET AL), 7 January 1997 (07.01.97), column 2, line 63 - column 4, line 9, figure 3, claims 1-31, abstract	1,3,4
	--	
A	US 5757919 A (HOWARD C. HERBERT ET AL), 26 May 1998 (26.05.98), column 1, line 58 - column 2, line 5; column 6, line 31 - column 7, line 22, figures 5a,b, claims 1-24, abstract	1,3,4
	--	

INTERNATIONAL SEARCH REPORT

Information on patent family members

08/05/00

International application No.
PCT/FI 00/00421

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0798673 A1	01/10/97	AU 712353 B	04/11/99
		AU 2506297 A	22/10/97
		CA 2245921 A	09/10/97
		CN 1215489 A	28/04/99
		CZ 9802956 A	17/02/99
		EP 0960404 A	01/12/99
		JP 11506560 T	08/06/99
		NO 984535 A	28/09/98
		NZ 331258 A	28/10/99
		WO 9737331 A	09/10/97
US 5475763 A	12/12/95	NONE	
WO 9421066 A1	15/09/94	AU 683646 B	20/11/97
		AU 6255694 A	26/09/94
US 5369707 A	29/11/94	CA 2101198 A	28/07/94
US 5239294 A	24/08/93	AU 6034790 A	06/02/91
		CA 2063447 A,C	13/01/91
		IL 94467 A	31/12/95
		JP 2684118 B	03/12/97
		JP 5503816 T	17/06/93
		MX 166091 B	17/12/92
		WO 9101067 A	24/01/91
		CA 2087433 A,C	17/01/92
		JP 2750638 B	13/05/98
		MX 9100231 A	28/02/92
		WO 9202103 A	06/02/92
		US 5572193 A	05/11/96
US 5592553 A	07/01/97	EP 0636963 A	01/02/95
		JP 7107086 A	21/04/95
		US 5661807 A	26/08/97
US 5757919 A	26/05/98	AU 5688998 A	03/07/98
		DE 19782169 T	28/10/99
		GB 2334866 A	01/09/99
		GB 9912947 D	00/00/00
		WO 9826535 A	18/06/98