Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2467905 A1 2003/06/05

(21) 2 467 905

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2002/11/20
(87) Date publication PCT/PCT Publication Date: 2003/06/05
(85) Entrée phase nationale/National Entry: 2004/05/19
(86) N° demande PCT/PCT Application No.: US 2002/037331
(87) N° publication PCT/PCT Publication No.: 2003/047301
(30) Priorités/Priorities: 2001/11/21 (60/332,117) US;
2002/11/05 (10/289,507) US

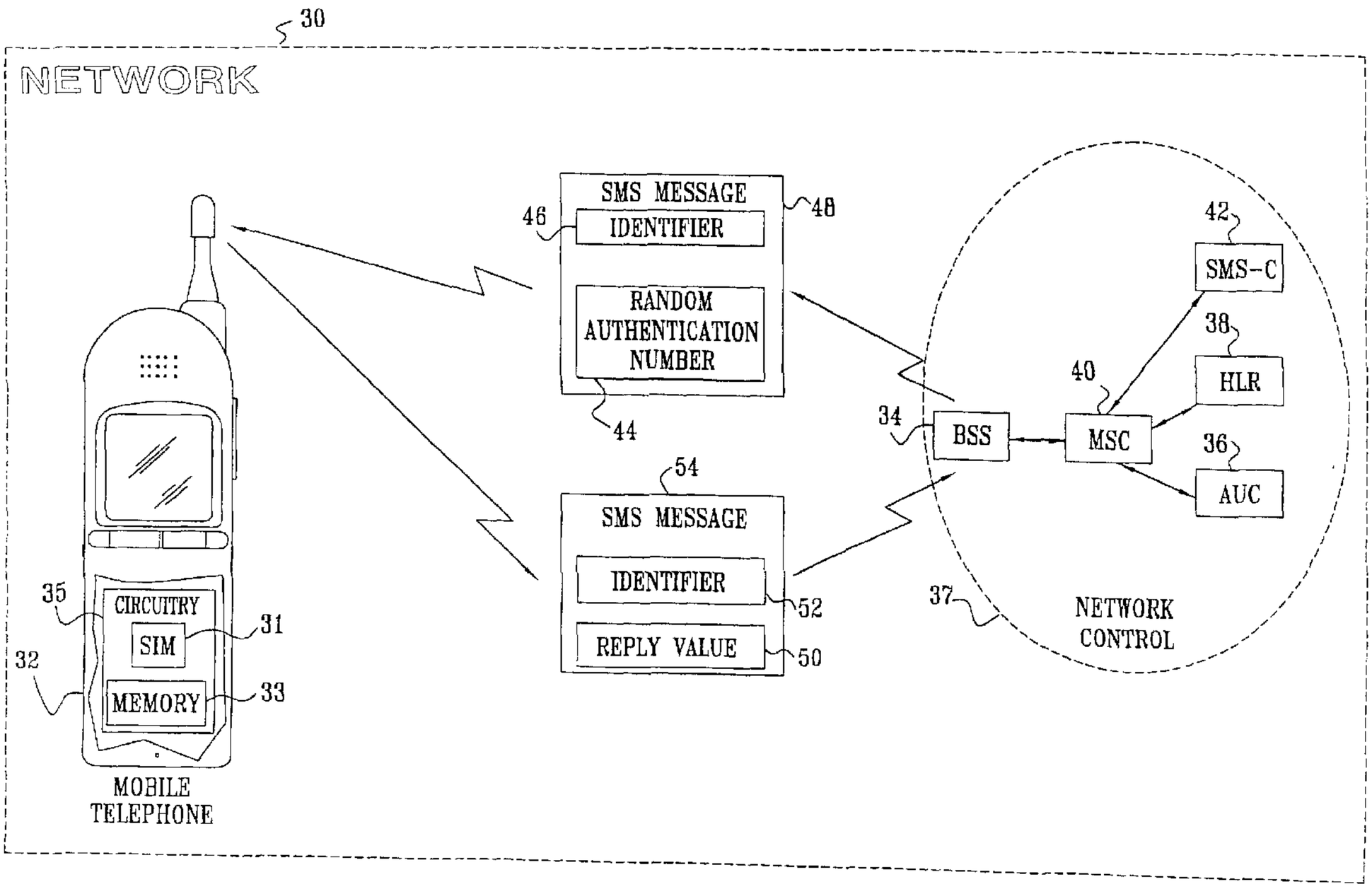
(51) Cl.Int.^{7}/Int.Cl.^{7} H04Q 7/38

(71) Demandeur/Applicant:
QUALCOMM INCORPORATED, US

(72) Inventeurs/Inventors:
GREEN, MICHAEL, IL;
RIMONI, YORAM, IL

(74) Agent: SMART & BIGGAR

(54) Titre : AUTHENTIFICATION D'UN TELEPHONE MOBILE
(54) Title: AUTHENTICATION OF A MOBILE TELEPHONE



(57) Abrégé/Abstract:
A method for enabling a mobile telephone to operate in a communications network, including: generating a random authentication number and an expected response to the random authentication number, and transmitting a forward short message service (SMS) message incorporating the random authentication number to the mobile telephone. The method further includes generating at the mobile telephone, responsive to the random authentication number, an authentication response, and receiving from the mobile telephone a return SMS message incorporating the authentication response. The method also includes performing a comparison between the authentication response in the return SMS message and the expected response, and authenticating the mobile telephone to operate in the communications network responsive to the comparison.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 June 2003 (05.06.2003)

PCT

(10) International Publication Number
WO 03/047301 A1

(51) International Patent Classification[7]: H04Q 7/38

(21) International Application Number: PCT/US02/37331

(22) International Filing Date:
20 November 2002 (20.11.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/332,117 21 November 2001 (21.11.2001) US
10/289,507 5 November 2002 (05.11.2002) US

(71) Applicant: **QUALCOMM INCORPORATED** [US/US]; 5775 Morehouse Drive, San Diego, CA 92121 (US).

(72) Inventors: **GREEN, Michael**; 9 Yafe Nof Street, 30900 Zichron Yaakov (IL). **RIMONI, Yoram**; 10 Keren Hayesod Street, 31999 Haifa (IL).

(74) Agents: **WADSWORTH, Philip, R.** et al.; QUALCOMM Incorporated, 5775 Morehouse Drive, San Diego, CA 92121 (US).

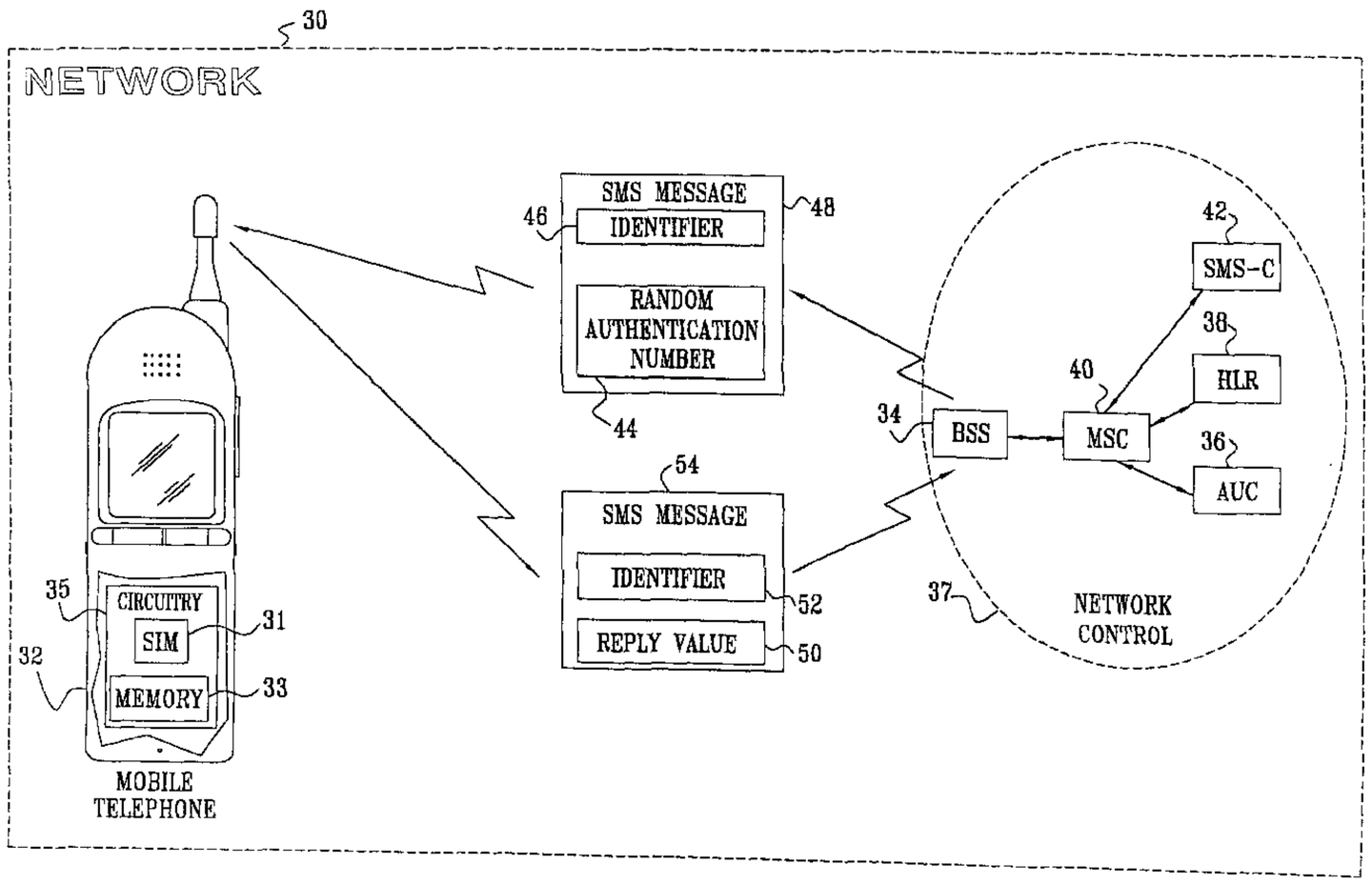
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, 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 receipt of amendments*

[Continued on next page]

(54) Title: AUTHENTICATION OF A MOBILE TELEPHONE



(57) Abstract: A method for enabling a mobile telephone to operate in a communications network, including: generating a random authentication number and an expected response to the random authentication number, and transmitting a forward short message service (SMS) message incorporating the random authentication number to the mobile telephone. The method further includes generating at the mobile telephone, responsive to the random authentication number, an authentication response, and receiving from the mobile telephone a return SMS message incorporating the authentication response. The method also includes performing a comparison between the authentication response in the return SMS message and the expected response, and authenticating the mobile telephone to operate in the communications network responsive to the comparison.

WO 03/047301 A1

WO 03/047301 A1

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.

AUTHENTICATION OF A MOBILE TELEPHONE

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Patent Application No. 60/332,117, filed November 21, 2001, which is incorporated herein by reference.

I. Field Of The Invention

[0002] The present invention relates generally to methods of verification, and specifically to a method for authenticating a mobile telephone operating in a cellular communication network.

II. Background Of The Invention

[0003] Mobile telephones operating within a cellular communication network undergo a process of authentication before being able to place or receive calls. The authentication, *inter alia*, prevents fraudulent use of the mobile. Two types of networks wherein authentication is performed are a Code Division Multiple Access (CDMA) network, and a Global System for Mobile Communications (GSM) network, which operates in a Time Division Multiple Access (TDMA) format.

[0004] Fig. 1 is a schematic diagram illustrating a process of authentication in a cellular network 10, as is known in the art. A mobile telephone 12 in network 10 transmits an initial signal to a mobile switching center (MSC) 16 communicating with a base-station system (BSS) 14. In order to be authenticated for operation in the network, MSC 16 instructs an authentication center (AUC) 18 to generate a random authentication number 20, typically as a triplet. Authentication number 20 is transmitted to mobile telephone 12 within an authentication packet 22. The generation is performed using data derived from a home location register (HLR) 29. MSC 16, AUC 18, and HLR 29 are comprised in a backbone of network 10, to which BSS 14 is coupled. The mobile telephone processes the number through an authentication algorithm comprised in the mobile in order to generate a reply value 24. The reply value is transmitted in an authentication response packet 26 to the MSC. The MSC checks, with AUC 18 and HLR 29, if random number 20 and reply 24 satisfy authentication criteria of the network. If the criteria are

satisfied, the mobile telephone is allowed to continue operating within the network.

[0005] Network 10 also comprises a short message service center (SMS-C) 28 in the backbone of the network, which is able to transmit and receive short alphanumeric messages. Mobile telephone 12 may be implemented to receive and transmit such SMS messages. Typically, alphanumeric messages transmitted and received by an SMS-C consist of approximately 128 characters, although higher numbers of characters may be transferred.

[0006] If network 10 comprises a CDMA network operating according to an industry-standard protocol, such as a TIA/EIA/IS-2000-A-1 standard published by the Telecommunications Industry Association, Arlington, VA, mobile 12 comprises a CDMA mobile. AUC 18 implements an ANSI-41 protocol, published by the 3rd Generation Partnership Project 2, which may be found at http://www.3gpp2.org, and which is incorporated herein by reference. In this case, random authentication number 20 sent from the authorization center is a 32-bit number, and reply value 24 generated by the CDMA mobile is an 18-bit number. In order to perform the authentication, the CDMA mobile thus needs to be able to transmit its authentication reply as an 18-bit number.

[0007] If network 10 comprises a GSM network operating according to an industry-standard protocol, such as an ETSI TS 100 940 V7.8.0 technical specification, published by the European Telecommunications Standards Institute, Sophia Antipolis Cedex, France, mobile 12 comprises a GSM mobile. Section 4.3 of the specification, incorporated herein by reference, describes the authentication procedure followed in a GSM network. In this case, the random authentication number sent from the authorization center is a 128-bit number, and the reply value generated by the GSM mobile is a 32-bit number. In order to perform the authentication in the GSM network, the GSM mobile needs to be able to transmit its authentication reply as a 32-bit number.

[0008] If a CDMA mobile is to operate in a GSM network, however, the authentication reply which the mobile needs to generate, a 32-bit number, is larger than the 18-bit capability of the CDMA mobile. Methods known in the art for overcoming the limited capability of the CDMA mobile include changing software in both the GSM authentication center and the CDMA mobile. When the CDMA mobile is to operate in its native CDMA environment, the software is replaced by the original software. An

alternative procedure which is known in the art is to change software in the GSM center so that only "CDMA-type" authentication is performed on CDMA mobiles operative in the GSM network. It will be appreciated that both methods are problematic.

SUMMARY OF THE INVENTION

[0009] It is an object of some aspects of the present invention to provide a method and apparatus for authenticating a mobile telephone to operate in a communications network.

[0010] In a preferred embodiment of the present invention, a mobile telephone is to be operated within a cellular communications network. A base station or a switching center in the network authenticates the mobile telephone by transmitting an authentication request in the form of a message, most preferably a short messaging system (SMS) message, to the mobile. The SMS message comprises a first identifier defining the SMS message as the authentication request, together with a random number which is used as part of an authentication procedure. By analyzing the first identifier, the mobile telephone recognizes the SMS message as the authentication request and processes the accompanying random number through an authentication algorithm comprised in the mobile telephone, so as to generate an authentication response. The response is sent in a return SMS message transmitted from the mobile to the network. The return SMS message comprises a second identifier defining the return message as including the authentication response. The network recovers the response from the return message, and compares the recovered response with an expected response, in order to authenticate the mobile telephone. Using SMS messages as delivery systems for authentication requests and responses avoids limitations on sizes of the random number and of responses in systems known in the art.

[0011] In some preferred embodiments of the present invention, the mobile telephone is able to operate in more than one communications network. Each network comprises a different authentication protocol, each protocol defining a different size for the random number and response. The mobile can be authenticated in its "native" network, or in a network operating under a different protocol, without software or hardware changes in the mobile as it moves from network to network.

[0012] In an alternative preferred embodiment of the present invention, where the

network within which the mobile operates supports data burst messages (DBMs), the authentication request message to the mobile, and the authentication response message from the mobile, are sent as DBMs. Most preferably, the DBMs are of a type already supported by a communications protocol under which the network is operating.

[0013] The present invention will be more fully understood from the following detailed description of the preferred embodiments thereof, taken together with the drawings, in which:

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] Fig. 1 is a schematic diagram illustrating a process of authentication in a cellular communications network, as is known in the art;

[0015] Fig. 2 is a schematic diagram illustrating a process of authentication of a mobile telephone, according to a preferred embodiment of the present invention; and

[0016] Fig. 3 is a sequence diagram showing steps involved in authentication of the mobile telephone of Fig. 2 operating in a communications network, according to a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0017] Reference is now made to Fig. 2, which is a schematic diagram illustrating a process of authentication of a mobile telephone 32, according to a preferred embodiment of the present invention. Mobile telephone 32 is adapted to operate in a cellular communications network 30, which functions according to a first industry-standard cellular communications protocol. The mobile comprises circuitry 35 enabling the mobile to operate. Most preferably, mobile 32 is adapted to operate according to the first protocol, as well as being operative according to a second industry-standard cellular communications protocol. For example, the first protocol comprises a Global System for Mobile Communications (GSM) protocol, such as an ETSI TS 100 940 V7.8.0 technical specification referred to in the Background of the Invention, and the second protocol comprises a Code Division Multiple Access (CDMA) protocol, such as a TIA/EIA/IS-2000-A-1 standard also referred to in the Background of the Invention. Alternatively, mobile 32 is operative according to either a GSM or a CDMA industry-standard protocol, or according to another protocol known in the art.

[0018] A base-station system (BSS) 34 is coupled to a mobile switching center (MSC) 40, which is in turn coupled to an authentication center (AUC) 36, and a home location register (HLR) 38. Optionally, a short message service center (SMS-C) 42 may also be coupled to MSC 40. One or more of BSS 34, AUC 36, HLR 38, and MSC 40 act as a network control center 37, controlling transmissions within network 30. Except for the differences described below, AUC 36, HLR 38, MSC 40, and SMS-C 42 respectively operate generally as AUC 18, HLR 29, MSC 16, and SMS-C 28, described with reference to Fig. 1 in the Background of the Invention.

[0019] Mobile 32 wishes to operate in network 30, and transmits an initial signal to BSS 34. In order to authenticate the mobile, BSS 34 transmits a random authentication number 44, encapsulated in a first, forward, message 48, to mobile 32. Except where otherwise stated hereinbelow, message 48 is assumed to comprise an SMS message. Message 48 incorporates an identifier 46 within the message, so that mobile 48 is able to recognize SMS message 48 as a special message conveying the random authentication number. On receipt of SMS message 48, mobile 32 decodes the message, recovers the value of random authentication number 44, and applies the recovered value to an authentication algorithm comprised in the mobile, to generate an authentication response. Preferably, software for decoding message 48, recovering number 44, and the authentication algorithm is incorporated as a separate replaceable element 31, most preferably as a subscriber identity module (SIM) within mobile 32. Alternatively, the software is incorporated integrally within a memory 33 of the mobile.

[0020] Mobile 32 incorporates the authentication response in a second, return, message 54, as a reply value 50, and transmits the message to BSS 34. Except where otherwise stated hereinbelow, message 54 is assumed to comprise an SMS message. Mobile 32 incorporates an identifier 52 in message 54, so that the message may be recognized as a special message conveying the authentication reply. SMS message 54 is routed by BSS 34 to MSC 40, which, from identifier 52, recognizes the message as comprising the authentication reply, and extracts reply value 50 from the message. MSC 40 checks that value 50 corresponds with an expected response to random number authentication 44, and if there is a correspondence, authenticates mobile 32. By incorporating random number authentication 44 and reply value 50 in SMS messages, limitations on sizes of the random number authentication and the reply value, as defined by the different

protocols under which mobile 32 operates, are overcome. The limitations are overcome since SMS messages are able to transmit 128 or more 8-bit characters.

[0021] Fig. 3 is a sequence diagram 60 showing steps involved in authentication of mobile telephone 32 operating in network 30, according to a preferred embodiment of the present invention. By way of example, network 30 is assumed to operate according to a GSM protocol. Sequence diagram 60 illustrates steps performed before and after mobile 32 has made an initial transmission, received by BSS 34, and is awaiting authentication. The initial transmission incorporates an international mobile subscriber identity (IMSI), typically the telephone number of mobile 32, which has been allocated to the mobile when it is initially registered in the network, and which is also stored in AUC 36. Also at registration, mobile 32 is allocated a subscriber authentication key (Ki), which is stored both in the mobile and in AUC 36.

[0022] In a first step 62, AUC 36 generates a random number (RAND), and uses RAND to calculate an identification parameter, termed signal response (SRES), which is a function of RAND and Ki. AUC 36 also calculates an encryption key (Kc) which is a function of Ki and RAND. IMSI, Kc, RAND, and SRES are transferred and stored in HLR 38.

[0023] In a second step 64, HLR 38 transfers the values of IMSI, Kc, RAND, and SRES to MSC 40, after the MSC has received the initial transmission via BSS 34. MSC 40 stores IMSI, Kc, RAND, and SRES for later comparison purposes.

[0024] In a third step 66, MSC 40 incorporates the RAND value, corresponding to random authentication number 44 (Fig. 2) into SMS message 48. The SMS message is transferred to BSS 34 via either a traffic or a control channel. Alternatively, if network 30 comprises a CDMA 2000 network, the transfer may be made using an Application Data Delivery Service (ADDS).

[0025] In a fourth step 68, BSS 34 adds identifier 46 to the message and transmits the message to mobile 32.

[0026] In a fifth step 70, mobile 32 identifies SMS message 48, by identifier 46, as a message comprising number 44, using software comprised in SIM 31 or memory 33 of the mobile. The mobile uses number 44, and the mobile's stored values of IMSI and Ki, to generate reply value 50 as a signal response to number 44. The mobile then constructs SMS message 54, incorporating reply value 50 and identifier 52.

[0027] In a sixth step 74 the mobile transmits SMS message 54 to BSS 34.

[0028] In a final step 76, BSS 34 transfers SMS message 54 to MSC 40, which identifies the SMS message, from identifier 52, as a response to the authentication SMS message 48. MSC 40 then recovers the value of reply value 50, as a signal response, from message 54, and compares the recovered value with an expected value of SRES received from HLR 38 in second step 64. If the two signal responses tally, MSC 40 authenticates the mobile; if the responses do not tally, the mobile is not authenticated.

[0029] It will be appreciated that the descriptions above with respect to Figs. 2 and 3 apply to substantially any mobile transceiver operating in a cellular communication network, wherein the transceiver is capable of transmitting and receiving SMS messages. Thus, the scope of the present invention is not limited to any specific protocol or method of transmission utilized by the transceiver and/or the network.

[0030] In an alternative preferred embodiment of the present invention, wherein BSS 34 and mobile 32 are able to communicate via a spread spectrum system such as a code division multiple access (CDMA) system, messages 48 and 54 (Fig. 2) comprise short data burst messages. Data burst messages are described and characterized in TIA/EIA/IS-2000-A-1 standard, referred to in the Background of the Invention. The data burst messages are preferably implemented according to one of the predefined types incorporated in the standard, or alternatively via a custom-defined type. If messages 48 and 54 are in the form of data burst messages, then in sixth step 74 and final step 76 BSS 34 identifies the data burst message as an authentication response, recovers reply value 50, and provides the value to MSC 40. The MSC then performs the comparison between the recovered value and the expected value of SRES.

[0031] By incorporating random authentication numbers and responses to these numbers in SMS or data burst messages, limitations on sizes of the numbers and of the responses are avoided. Such size limitations, i.e., respective numbers of bits for the random authentication number and its response, are typically defined by a specific protocol. Using SMS or data burst messages as delivery systems thus enables a mobile telephone to be authenticated in a variety of protocols, without changing software or hardware in the mobile telephone.

[0032] It will be appreciated that the preferred embodiments described above are cited by way of example, and that the present invention is not limited to what has been

particularly shown and described hereinabove. Rather, the scope of the present invention includes both combinations and subcombinations of the various features described hereinabove, as well as variations and modifications thereof which would occur to persons skilled in the art upon reading the foregoing description and which are not disclosed in the prior art.

CLAIMS

1. A method for enabling a mobile telephone to operate in a communications network, comprising:

generating a random authentication number and an expected response to the random authentication number;

transmitting a forward short message service (SMS) message incorporating the random authentication number to the mobile telephone;

generating at the mobile telephone, responsive to the random authentication number, an authentication response;

receiving from the mobile telephone a return SMS message incorporating the authentication response;

performing a comparison between the authentication response in the return SMS message and the expected response; and

authenticating the mobile telephone to operate in the communications network responsive to the comparison.

2. A method according to claim 1, wherein the mobile telephone is adapted to be operative in a plurality of different communication protocols.

3. A method according to claim 2, wherein the random authentication number comprises a random-authentication-number-size, and the expected response and the authentication response each comprise an expected-response-size, and wherein the random-authentication-number-size and the expected-response-size have values responsive to respective protocols comprised in the plurality of protocols.

4. A method according to claim 1, and comprising:

incorporating into the forward SMS message a forward identifier adapted to enable the mobile telephone to recognize the forward SMS message as an authentication request; and

the mobile telephone incorporating into the return SMS message a reverse identifier, so that the return SMS message is recognized as an authentication answer.

5. Apparatus for enabling a mobile telephone to operate in a communications network, comprising:

a network control center which is adapted to:

generate a random authentication number and an expected response to the random authentication number,

incorporate the random authentication number in a forward short message service (SMS) message, and

transmit the forward SMS message to the mobile telephone; and

circuitry, comprised in the mobile telephone, which is adapted to:

generate, responsive to the random authentication number, an authentication response,

incorporate the authentication response in a return SMS message, and

transmit the return SMS message to the network control center,

the network control center being further adapted to make a comparison between the authentication response and the expected response, and to authenticate the mobile telephone for operation in the communications network responsive to the comparison.

6. Apparatus according to claim 5, wherein the network control center comprises at least one of a base-station system (BSS), a mobile switching center (MSC), and an authentication center (AUC).

7. Apparatus according to claim 5, wherein the circuitry is adapted to operate the mobile telephone in a plurality of different communication protocols.

8. Apparatus according to claim 7, wherein the random authentication number comprises a random-authentication-number-size, and the expected response and the authentication response each comprise an expected-response-size, and wherein the random-authentication-number-size and the expected-response-size have values

responsive to respective protocols comprised in the plurality of protocols.

9. Apparatus according to claim 5, wherein the network control center is adapted to incorporate into the forward SMS message a forward identifier that enables the circuitry to recognize the forward SMS message as an authentication request, and wherein the circuitry is adapted to incorporate into the return SMS message a reverse identifier that enables the network control center to recognize the return SMS message as an authentication answer.

10. A method for enabling a mobile telephone to operate in a communications network adapted to transmit and receive data burst messages, comprising:

generating a random authentication number and an expected response to the random authentication number;

transmitting a forward data burst message incorporating the random authentication number to the mobile telephone;

generating at the mobile telephone, responsive to the random authentication number, an authentication response;

receiving from the mobile telephone a return data burst message incorporating the authentication response;

performing a comparison between the authentication response in the return data burst message and the expected response; and

authenticating the mobile telephone to operate in the communications network responsive to the comparison.

11. Apparatus for enabling a mobile telephone to operate in a communications network adapted to transmit and receive data burst messages, comprising:

a network control center which is adapted to:

generate a random authentication number and an expected response to the random authentication number,

incorporate the random authentication number in a forward data burst message, and

transmit the forward data burst message to the mobile telephone; and

circuitry, comprised in the mobile telephone, which is adapted to:

generate, responsive to the random authentication number, an authentication response,

incorporate the authentication response in a return data burst message, and

transmit the return data burst message to the network control center,

the network control center being further adapted to make a comparison between the authentication response and the expected response, and to authenticate the mobile telephone for operation in the communications network responsive to the comparison.

12. Apparatus for enabling a mobile telephone to operate in a communications network, comprising:

network controlling means which are adapted to:

generate a random authentication number and an expected response to the random authentication number,

incorporate the random authentication number in a forward short message service (SMS) message, and

transmit the forward SMS message to the mobile telephone; and

circuitry means, comprised in the mobile telephone, which are adapted to:

generate, responsive to the random authentication number, an authentication response,

incorporate the authentication response in a return SMS message, and

transmit the return SMS message to the network controlling means,

the network controlling means being further adapted to make a comparison between the authentication response and the expected response, and to authenticate the mobile telephone for operation in the communications network responsive to the comparison.

13. Apparatus according to claim 12, wherein the circuitry means are

adapted to operate the mobile telephone in a plurality of different communication protocols.

14. Apparatus according to claim 13, wherein the random authentication number comprises a random-authentication-number-size, and the expected response and the authentication response each comprise an expected-response-size, and wherein the random-authentication-number-size and the expected-response-size have values responsive to respective protocols comprised in the plurality of protocols.

15. Apparatus according to claim 12, wherein the network controlling means are adapted to incorporate into the forward SMS message a forward identifier that enables the circuitry means to recognize the forward SMS message as an authentication request, and wherein the circuitry means are adapted to incorporate into the return SMS message a reverse identifier that enables the network controlling means to recognize the return SMS message as an authentication answer.

FIG. 1 (PRIOR ART)

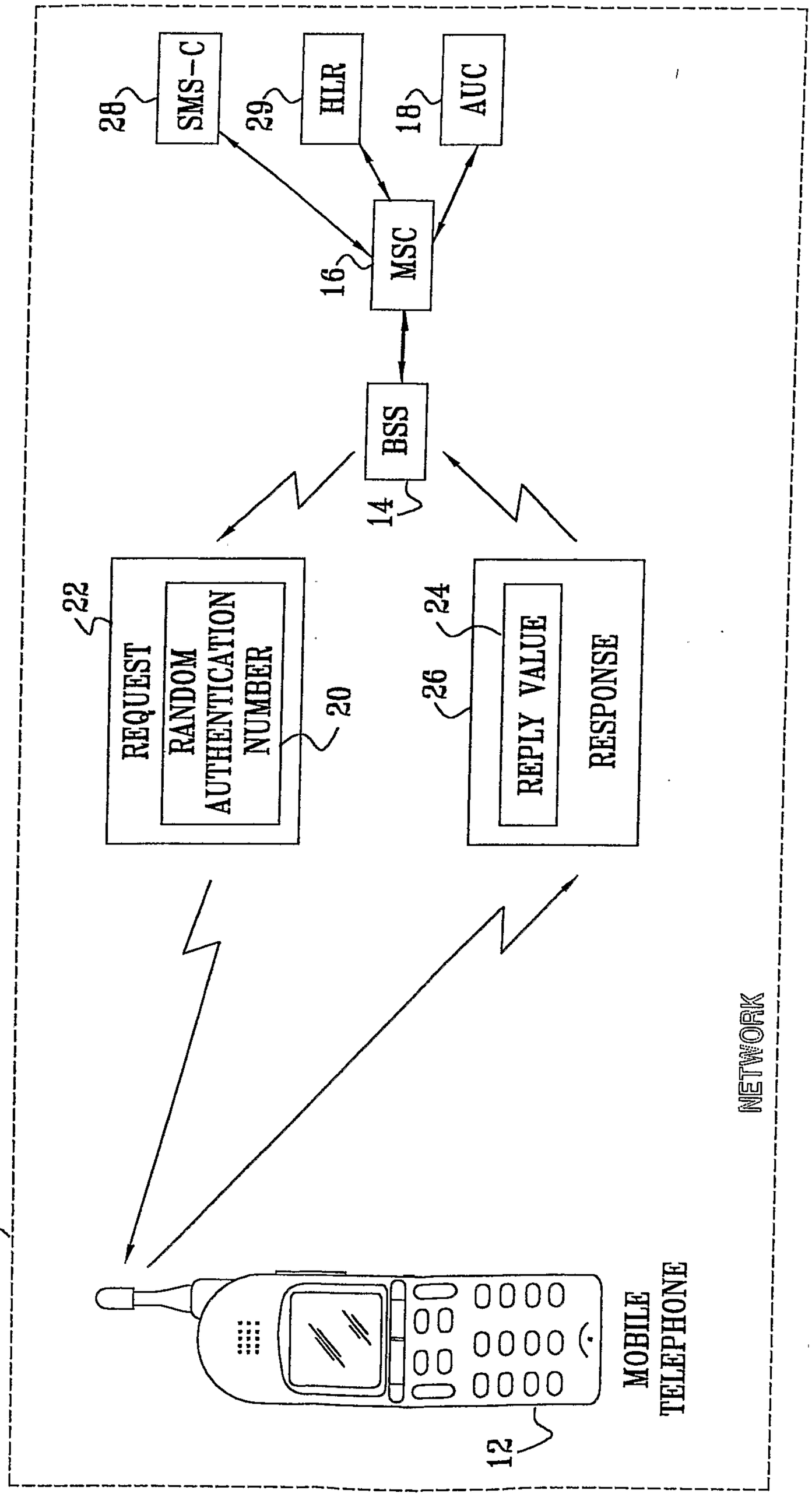


FIG. 2

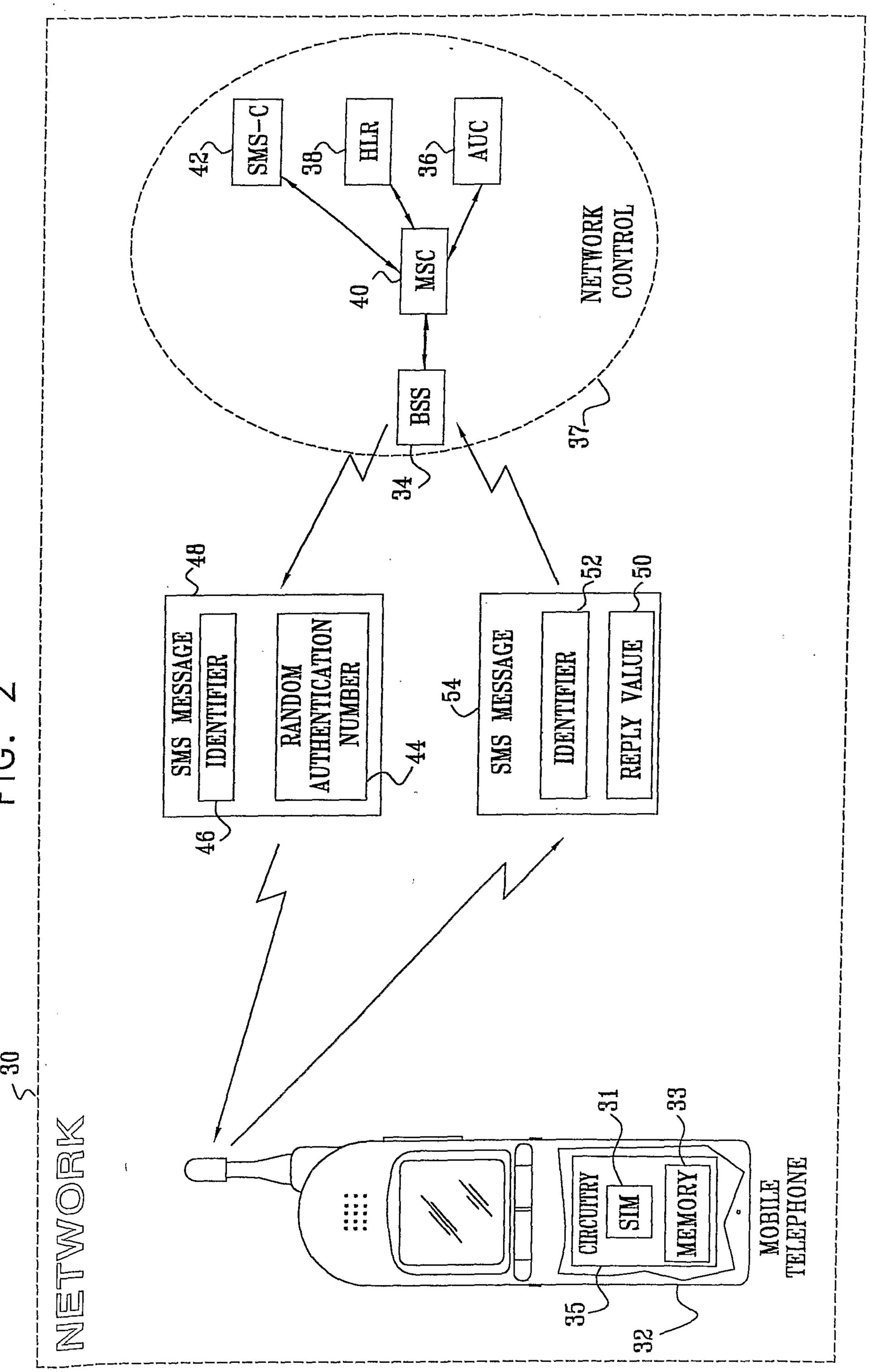
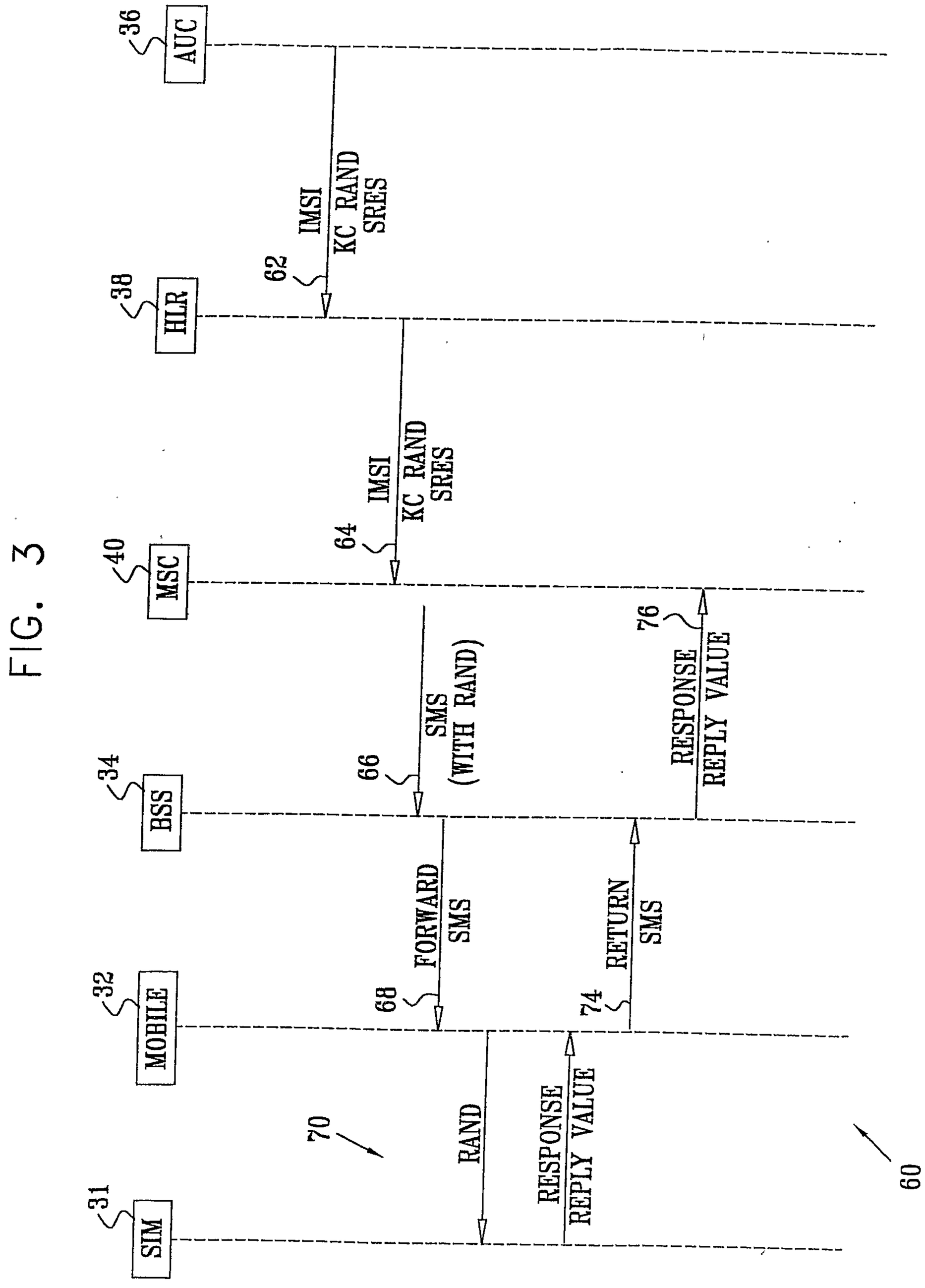
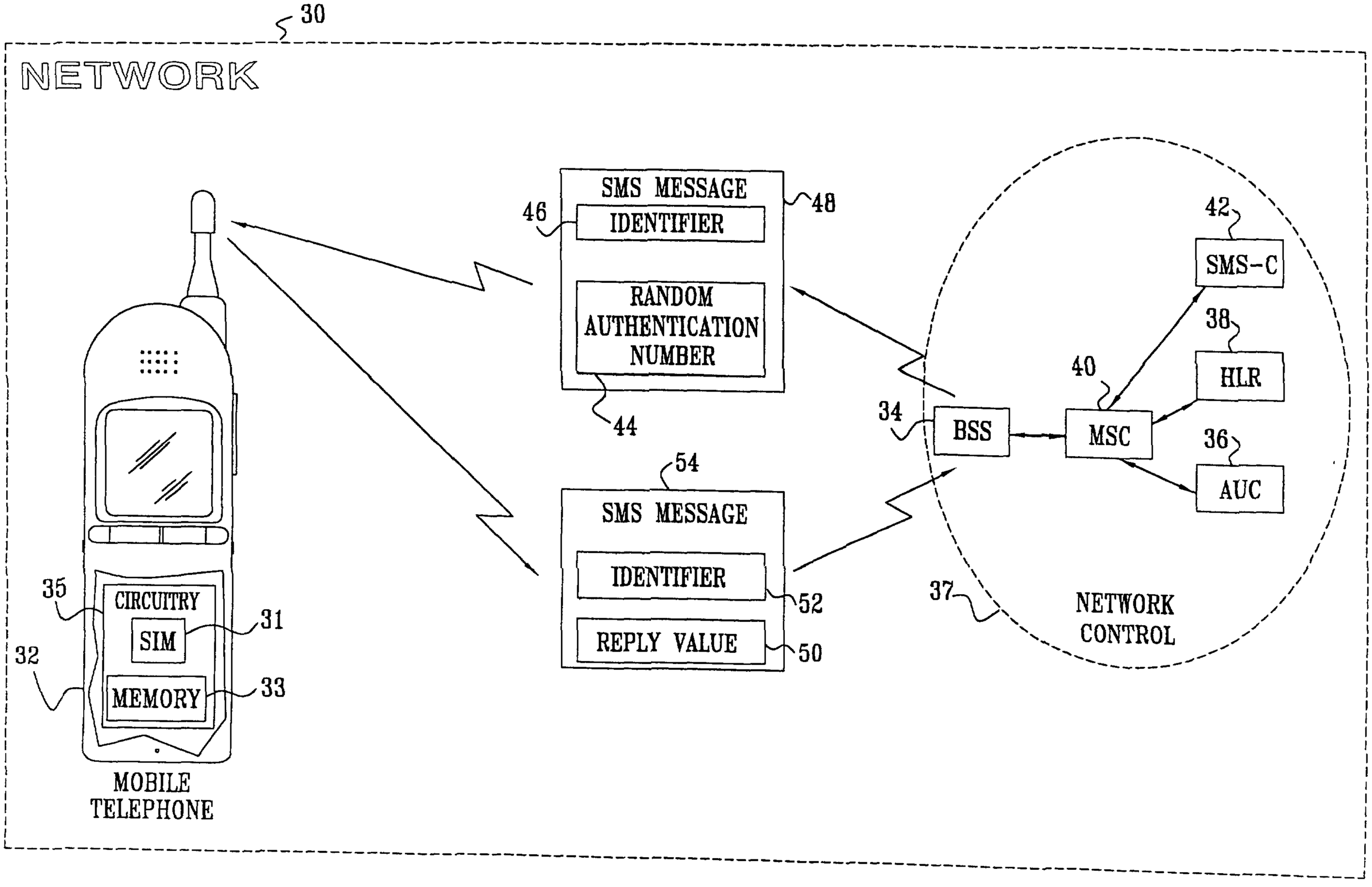

NETWORK
30
NETWORK CONTROL
37
SMS-C
42
HLR
38
AUC
36
MSC
40
BSS
34
SMS MESSAGE
IDENTIFIER
RANDOM AUTHENTICATION NUMBER
44
46
48
SMS MESSAGE
IDENTIFIER
REPLY VALUE
52
50
54
MOBILE TELEPHONE
CIRCUITRY
SIM
MEMORY
31
33
35
32

FIG. 3


36
AUC
IMSI
KC RAND
SRES
62
38
HLR
IMSI
KC RAND
SRES
64
40
MSC
SMS
(WITH RAND)
66
76
RESPONSE
REPLY VALUE
34
BSS
FORWARD
SMS
RETURN
SMS
68
74
32
MOBILE
RAND
RESPONSE
REPLY VALUE
70
31
SIM
60


30
NETWORK
SMS MESSAGE
46
IDENTIFIER
48
RANDOM AUTHENTICATION NUMBER
44
54
SMS MESSAGE
IDENTIFIER
52
REPLY VALUE
50
42
SMS-C
38
HLR
40
34
BSS
MSC
36
AUC
37
NETWORK CONTROL
35
CIRCUITRY
SIM
31
32
MEMORY
33
MOBILE TELEPHONE