

**(12) STANDARD PATENT
(19) AUSTRALIAN PATENT OFFICE**

(11) Application No. AU 2008200030 B8

(54) Title
System and method for conditionally attempting an emergency call setup

(51) International Patent Classification(s)
H04L 12/54 (2006.01) **H04W 4/22** (2009.01)
H04M 1/26 (2006.01)

(21) Application No: **2008200030** (22) Date of Filing: **2008.01.03**

(30) Priority Data

(31) Number **07100192.9** (32) Date **2007.01.05** (33) Country **EP**

(43) Publication Date: **2008.07.24**
(43) Publication Journal Date: **2008.07.24**
(44) Accepted Journal Date: **2010.12.16**
(48) Corrigenda Journal Date: **2011.01.06**

(71) Applicant(s)
Research In Motion Limited

(72) Inventor(s)
Sokondar, Eniko

(74) Agent / Attorney
Spruson & Ferguson, Level 35 St Martins Tower 31 Market Street, Sydney, NSW, 2000

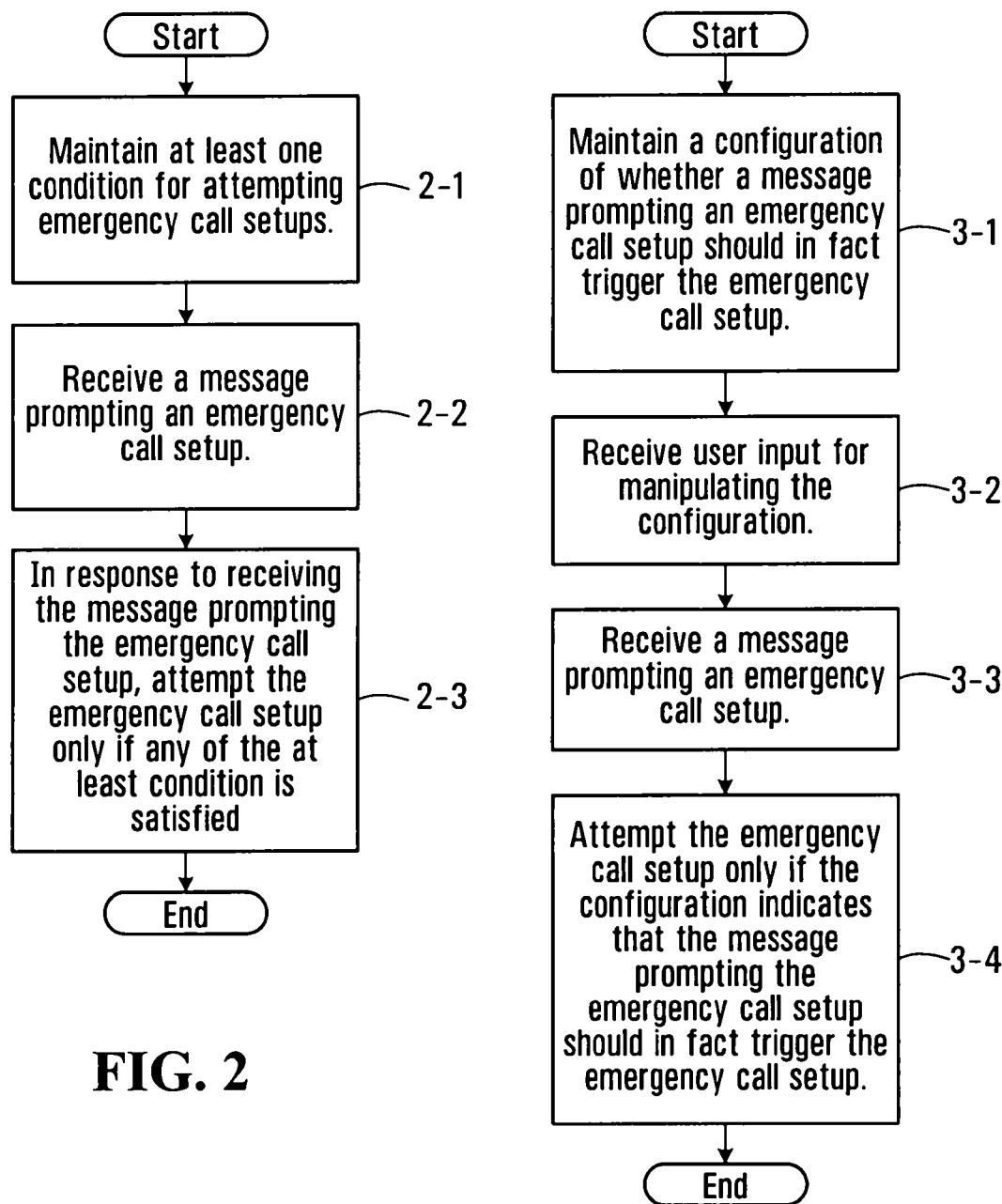
(56) Related Art
WO 2003/063536 A1 (NOKIA CORP) 31 July 2003
US 2005/0096008 A1 (SHIN) 5 May 2005
WO 2002/089515 A1 (NOKIA CORP) 7 November 2002

**System and Method for
Conditionally Attempting an Emergency Call Setup**

Abstract

A system and method is provided for a communications device (10) to conditionally attempt an emergency call setup. The communications device (10) maintains at least one condition for attempting emergency call setups. Upon receiving a message 5 prompting an emergency call setup, the communications device (10) attempts the emergency call setup only if any of the at least one condition is satisfied. The at least one least condition is defined such that the communications device (10) does not erroneously attempt to establish an emergency call 10 when there is no emergency. The at least one condition might for example include whether the message prompting the emergency call setup indicates a message source that is trusted by the user of the mobile device (10). A system and method is also provided for a communications network to block at least at 15 least some of the messages from being delivered to their target communications device.

3/9



AUSTRALIA
PATENTS ACT 1990
COMPLETE SPECIFICATION
FOR A STANDARD PATENT

Name and Address
of Applicant : Research In Motion Limited, of 295 Phillip Street,
Waterloo, Ontario, N2L 3W8, Canada

Actual Inventor(s): Eniko Sokondar

Address for Service: Spruson & Ferguson
St Martins Tower Level 35
31 Market Street
Sydney NSW 2000
(CCN 3710000177)

Invention Title: System and method for conditionally attempting an
emergency call setup

The following statement is a full description of this invention, including the best method of performing it known to me/us:

**System and Method for
Conditionally Attempting an Emergency Call Setup**

Field of the Application

The application relates to electronic communication,
5 and more particularly to emergency call setups for
communication devices.

Background

According to Section 5.1.6 of TS 24.229, version 5,
upon a mobile device receiving a 380 (Alternative Service)
10 response with a <type> child element set to "emergency", the
mobile device is to automatically attempt an emergency call
setup over the CS domain. If the emergency call setup is
successful, then an emergency call is established for the
mobile device. The mobile device normally receives the 380
15 response in response to transmitting an invite request message
to the network. Therefore, by transmitting the invite request
message, the mobile device can trigger the process of
establishing an emergency call in the event that there is an
emergency.

20 **Summary**

According to a first aspect of the present
disclosure, there is provided a method in a communications
system comprising a network and a mobile communications device,
the method performed by the mobile communications device
25 comprising:

sending a Session Initiation Protocol (SIP) INVITE
request to the network comprising a Proxy Call Session Control
Function (P-CSCF);

receiving a response message prompting an emergency
30 call setup from a message source, the response message being an

alternative service message and including identification of the message source, the message having a body in an Extensible Markup Language (XML) including an <alternative service> element with the <type> child element set to "emergency";

5 determining whether the message source is a trusted source from the identification of the message source in the response message;

attempting the emergency call setup only when the message source is a trusted source.

10 According to a second aspect of the present disclosure, there is provided a computer readable medium having computer executable instructions stored thereon for execution on a processor of a communications device so as to implement the aforementioned method.

15 According to a third aspect of the present disclosure, there is provided a communications device comprising:

a processor; and

20 an emergency call set-up function coupled with the processor and configured to:

send a Session Initiation Protocol (SIP) INVITE request to the network comprising a Proxy Call Session Control Function (P-CSCF);

25 receive a Session Initiation Protocol (SIP) response message from a message source prompting the device to attempt an emergency call setup, the response message being an alternative service message and including identification of the message source, the message having a body in an Extensible Markup Language (XML) including an <alternative service> element with the <type> child element set to "emergency";

determine whether the message source is a trusted source from the identification of the message source in the response message; and

attempt the emergency call setup only when the
5 message source is a trusted source.

According to a fourth aspect of the present disclosure, there is provided a method in a communications system comprising a network and a communications device, the method performed by the communications device comprising:

10 maintaining an identification of a trusted source of messages;

sending a request message to the network, the request message being a Session Initiation Protocol (SIP) INVITE request, the network comprising a Proxy Call Session Control
15 Function (P-CSCF);

receiving a response message prompting an emergency call setup from a message source, wherein the response message was sent in response to the request message, the response message being an alternative service message and including
20 identification of the message source, the message having a body in an Extensible Markup Language (XML) including an <alternative service> element with the <type> child element set to "emergency";

25 comparing the message source with the identification of a trusted source; and

attempting the emergency call setup only when the message source is equal to the identification of a trusted source.

- 3a -

According to a fifth aspect of the present disclosure, there is provided a mobile communications device comprising:

a processor; and

5 a function coupled with the processor and configured to:

maintain an identification of a trusted source of messages;

10 send a request message to the network, the request message being a Session Initiation Protocol (SIP) INVITE request, the network comprising a Proxy Call Session Control Function (P-CSCF);

15 receive a response message prompting an emergency call setup from a message source, wherein the response message is received in response to the request message, the response message being an alternative service message and including identification of the message source, the message having a body in an Extensible Markup Language (XML) including an <alternative service> element with the <type> child element set 20 to "emergency";

compare the message source with the identification of a trusted source; and

25 attempt the emergency call setup only when the message source is equal to the identification of a trusted source.

Brief Description of the Drawings

Embodiments will now be described with reference to the attached drawings in which:

Figure 1A is a block diagram of an example

5 communication system;

Figure 1B is a block diagram of a mobile device;

Figure 2 is a flowchart of an example method of conditionally attempting an emergency call setup;

Figures 3 through 6 are flowcharts of other example
10 methods of conditionally attempting an emergency call setup;

Figure 7 is a block diagram of another communications system;

Figure 8 is a flowchart of a method of blocking at least some messages from being delivered to their target mobile
15 device; and

Figures 9 and 10 are flowcharts of other example methods of blocking at least some of the messages from being delivered to their target mobile device.

Detailed Description of Embodiments

20 As noted above, a mobile device can trigger the process of establishing an emergency call when there is an emergency. However, Section 5.1.6 of TS 24.229, version 5, also allows for the possibility that the mobile device establishes an emergency call when there is not an emergency.

25 For instance, an entity can send a 380 (Alternative Service) response with the <type> child element set to "emergency" to the mobile device thereby prompting the mobile device to automatically attempt an emergency call setup. The entity

might be a rogue mobile device, a mobile device with a faulty protocol implementation, or a rogue server. In this situation, the mobile device would automatically attempt an emergency call setup even though there might be no apparent emergency. SIP 5 messages with a number 3xx - where "xx" stands for 2 digits - mean redirection and they might be sent by a rogue or faulty mobile device or server.

Conditional Emergency Call Setup: Communication System

Referring now to Figure 1A, shown is a block diagram 10 of an example communication system 40. The communication system 40 has a wireless network 20, a mobile device 10, and other mobile devices 30; the communication system 40 may have other components, but they are not shown for sake of simplicity. The mobile device 10 has a wireless access radio 16, a processor 17, and an emergency call setup function 15; the mobile device 10 may have other components, but they are not shown for sake of simplicity. The other mobile devices 30 may each have components similar to those of the mobile device 10. Alternatively, some or all of the other mobile devices 30 15 may have different components than those of the mobile device 10.

In operation, the mobile device 10 communicates with the wireless network 20 using its wireless access radio 16. The wireless communication is over a wireless connection 19 25 between the mobile device 10 and the wireless network 20. The other mobile devices 30 may similarly communicate with the wireless network 20 over respective wireless connections (not shown). The communication with the wireless network 20 might for example be telephony, or other forms of communication such 30 as email.

Some communication might include emergency calls. For instance, the mobile device 10 might attempt an emergency call upon receiving a message prompting an emergency call setup. The source of the message prompting the emergency call setup might for example be one of the other mobile devices 30, or the wireless network 20 itself. In the event that the source of the message is one of the other mobile devices 30, then the source might be a rogue mobile device attempting to trigger the mobile device 10 to attempt an emergency call setup even though there may be no apparent emergency. There may be other situations in which the mobile device 10 receives a message prompting an emergency call setup when there is no apparent emergency.

According to an embodiment of the application, the emergency call setup function 15 maintains at least one condition for attempting emergency call setups. Upon receiving a message prompting an emergency call setup, the emergency call setup is attempted only if any of the at least one condition is satisfied. This allows the mobile device 10 to disregard a message prompting an emergency call setup in the event that there is no need to setup an emergency call. Further details are provided with reference to Figures 2 through 5.

In the illustrated example, the emergency call setup function 15 is implemented as software and is executed on the processor 17. However, more generally, the emergency call setup function 15 may be implemented as software, hardware, firmware, or any appropriate combination thereof.

In the illustrated example, the communication devices 10,30 are assumed to be mobile devices. However, more generally, embodiments of the application applicable to communication devices, which may be mobile or wired. For wired devices, there is no need for a wireless access radio. Rather,

wired devices may be provided with any appropriate communications interface. For the case of wired devices, the network 20 need not be wireless.

5 The wireless network 20 is not shown with any specific components. However, it is to be understood that the wireless network 20 would have any appropriate components suitable for a wired and/or wireless network. The components are implementation specific and may depend on the type of network. The network 20 may be of any appropriate type, for 10 example GPRS, UMTS, CDMA etc. IMS services are beareragnostic. In some implementations, the wireless network 20 includes P- CSCF (Proxy Call Session Control Function) nodes for processing transmission of SIP messages. Other implementations are possible.

15 Referring now to Figure 1B, shown is a block diagram of another mobile device 80 that may implement any of the methods described herein. The mobile device 80 is shown with specific components for implementing features similar to those of the mobile device 10 of Figure 1A. It is to be understood 20 that the mobile device 80 is shown with very specific details for example purposes only.

A processing device (a microprocessor 128) is shown schematically as coupled between a keyboard 114 and a display 126. The microprocessor 128 is a type of processor with 25 features similar to those of the processor 17 of the mobile device 10 shown in Figure 1A. The microprocessor 128 controls operation of the display 126, as well as overall operation of the mobile device 80, in response to actuation of keys on the keyboard 114 by a user.

30 The mobile device 80 has a housing that may be elongated vertically, or may take on other sizes and shapes

(including clamshell housing structures). The keyboard 114 may include a mode selection key, or other hardware or software for switching between text entry and telephony entry.

In addition to the microprocessor 128, other parts of the mobile device 80 are shown schematically. These include: a communications subsystem 170; a short-range communications subsystem 102; the keyboard 114 and the display 126, along with other input/output devices including a set of LEDS 104, a set of auxiliary I/O devices 106, a serial port 108, a speaker 111 and a microphone 112; as well as memory devices including a flash memory 116 and a Random Access Memory (RAM) 118; and various other device subsystems 120. The mobile device 80 may have a battery 121 to power the active elements of the mobile device 80. The mobile device 80 is in some embodiments a two-way radio frequency (RF) communication device having voice and data communication capabilities. In addition, the mobile device 80 in some embodiments has the capability to communicate with other computer systems via the Internet.

Operating system software executed by the microprocessor 128 is in some embodiments stored in a persistent store, such as the flash memory 116, but may be stored in other types of memory devices, such as a read only memory (ROM) or similar storage element. In addition, system software, specific device applications, or parts thereof, may be temporarily loaded into a volatile store, such as the RAM 118. Communication signals received by the mobile device 80 may also be stored to the RAM 118.

The microprocessor 128, in addition to its operating system functions, enables execution of software applications on the mobile device 80. A predetermined set of software applications that control basic device operations, such as a voice communications module 130A and a data communications

2008200030 03 Jan 2008

- 9 -

module 130B, may be installed on the mobile device 80 during manufacture. In addition, a personal information manager (PIM) application module 130C may also be installed on the mobile device 80 during manufacture. The PIM application is in some 5 embodiments capable of organizing and managing data items, such as e-mail, calendar events, voice mails, appointments, and task items. The PIM application is also in some embodiments capable of sending and receiving data items via a wireless network 110. In some embodiments, the data items managed by the PIM 10 application are seamlessly integrated, synchronized and updated via the wireless network 110 with the device user's corresponding data items stored or associated with a host computer system. As well, additional software modules, illustrated as another software module 130N, may be installed 15 during manufacture. One or more of the modules 130A, 130B, 130C, 130N of the flash memory 116 can be configured for implementing features similar to those of the emergency call setup function 15 of the mobile device 10 shown in Figure 1A. For example, one of the other modules 130N can be 20 configured so that when it is executed on the microprocessor 128, the mobile device 80 maintains at least one condition for attempting emergency call setups. In response to receiving a message prompting an emergency call setup, the mobile device 80 attempts the emergency call setup only if any of the at least 25 one condition is satisfied. There may be provided video calling capability in addition to voice calling capability.

Communication functions, including data and voice communications, are performed through the communication subsystem 170, and possibly through the short-range 30 communications subsystem 170. The communication subsystem 170 includes a receiver 150, a transmitter 152 and one or more antennas, illustrated as a receive antenna 154 and a transmit antenna 156. In addition, the communication subsystem 170 also

2008200030 03 Jan 2008

- 10 -

includes a processing module, such as a digital signal processor (DSP) 158, and local oscillators (LOs) 160. The communication subsystem 170 having the transmitter 152 and the receiver 150 is an implementation of a wireless access radio 5 with features similar to those of the wireless access radio 16 of the mobile device 10 shown in Figure 1A. The specific design and implementation of the communication subsystem 170 is dependent upon the communication network in which the mobile device 80 is intended to operate. For example, the 10 communication subsystem 170 of the mobile device 80 may be designed to operate with the Mobitex™, DataTAC™ or General Packet Radio Service (GPRS) mobile data communication networks and also designed to operate with any of a variety of voice communication networks, such as Advanced Mobile Phone Service 15 (AMPS), Time Division Multiple Access (TDMA), Code Division Multiple Access CDMA, Personal Communications Service (PCS), Global System for Mobile Communications (GSM), etc. Other types of data and voice networks, both separate and integrated, may also be utilized with the mobile device 80.

20 Network access may vary depending upon the type of communication system. For example, in the Mobitex™ and DataTAC™ networks, mobile devices are registered on the network using a unique Personal Identification Number (PIN) associated with each device. In GPRS networks, however, network access is 25 typically associated with a subscriber or user of a device. A GPRS device therefore typically has a subscriber identity module, commonly referred to as a Subscriber Identity Module (SIM) card, in order to operate on a GPRS network.

When network registration or activation procedures 30 have been completed, the mobile device 80 may send and receive communication signals over the communication network 110. Signals received from the communication network 110 by the

receive antenna 154 are routed to the receiver 150, which provides for signal amplification, frequency down conversion, filtering, channel selection, etc., and may also provide analog to digital conversion. Analog-to-digital conversion of the received signal allows the DSP 158 to perform more complex communication functions, such as demodulation and decoding. In a similar manner, signals to be transmitted to the network 110 are processed (e.g., modulated and encoded) by the DSP 158 and are then provided to the transmitter 152 for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the communication network 110 (or networks) via the transmit antenna 156.

In addition to processing communication signals, the DSP 158 provides for control of the receiver 150 and the transmitter 152. For example, gains applied to communication signals in the receiver 150 and the transmitter 152 may be adaptively controlled through automatic gain control algorithms implemented in the DSP 158.

In a data communication mode, a received signal, such as a text message or web page download, is processed by the communication subsystem 170 and is input to the microprocessor 128. The received signal is then further processed by the microprocessor 128 for an output to the display 126, or alternatively to some other auxiliary I/O devices 106. A device user may also compose data items, such as e-mail messages, using the keyboard 114 and/or some other auxiliary I/O device 106, such as a touchpad, a rocker switch, a thumb-wheel, or some other type of input device. The composed data items may then be transmitted over the communication network 110 via the communication subsystem 170.

In a voice communication mode, overall operation of the device is substantially similar to the data communication

mode, except that received signals are output to a speaker 111, and signals for transmission are generated by a microphone 112. Alternative voice or audio I/O subsystems, such as a voice message recording subsystem, may also be implemented on the 5 mobile device 80. In addition, the display 126 may also be utilized in voice communication mode, for example, to display the identity of a calling party, the duration of a voice call, or other voice call related information.

The short-range communications subsystem 102 enables 10 communication between the mobile device 80 and other proximate systems or devices, which need not necessarily be similar devices. For example, the short-range communications subsystem may include an infrared device and associated circuits and components, or a Bluetooth™ communication module to provide for 15 communication with similarly-enabled systems and devices.

Conditional Emergency Call Setup: Device Methods

Referring now to Figure 2, shown is a flowchart of an example method of conditionally attempting an emergency call setup. This method may be implemented in a communications 20 device, for example by the emergency call setup function 15 of the mobile device 10 shown in Figure 1A. Alternatively, the method may be implemented in the mobile device 80 shown in Figure 1B. More generally, the method may be implemented in any appropriate communications device.

25 At step 2-1, the communications device maintains at least one condition for attempting emergency call setups. At step 2-2, the communications device receives a message prompting an emergency call setup. At step 2-3, in response to receiving the message prompting the emergency call setup, the 30 communications device attempts the emergency call setup only if any of the at least one condition is satisfied. Otherwise, the

communications device does not attempt the emergency call setup.

There are many possibilities for the message prompting the emergency call setup. In some implementations, 5 the message is a 380 alternative service message that prompts the emergency call setup. The 380 alternative service message might prompt the emergency call setup for example by having an XML (Extensible Markup Language) body that includes an <alternative service> element with the <type> child element set 10 to "emergency". Alternatively, the 380 alternative service message might prompt the emergency call setup using any other type of encoding. More generally, the message may be any message that prompts an emergency call setup.

There are many possibilities for the at least one 15 condition. The at least one condition includes one or more conditions, at least one of which is to be satisfied for attempting an emergency call setup. Since there are many possibilities for the at least one condition, it follows that there are many possibilities for attempting the emergency call 20 setup only if any of the at least one condition is satisfied. There may be many configurations for the at least one condition. Satisfying a given condition can be any Boolean function of these configurations. To illustrate this point, further examples are provided below with reference to Figures 3 25 through 6. It is to be understood that these further examples are a mere sample of the possibilities.

Referring now to Figures 3 through 6, shown are flowcharts of other example methods of conditionally attempting an emergency call setup. These methods may be implemented in a 30 communications device, for example by the emergency call setup function 15 of the mobile device 10 shown in Figure 1A. Alternatively, these methods may be implemented in the mobile

device 80 shown in Figure 1B. More generally, these methods may be implemented in any appropriate communications device. These methods may be implemented separately, or in any appropriate combination.

5 Referring first to Figure 3, at step 3-1, the communications device maintains a configuration of whether a message prompting an emergency call setup should in fact trigger the emergency call setup. In some implementations, as shown in step 3-2, the communications device receives user 10 input for manipulating the configuration. This may for example be accomplished through a user interface of the communications device. At step 3-3, the communications device receives a message prompting an emergency call setup. At step 3-4, the communications device attempts the emergency call setup only if 15 the configuration indicates that the message prompting the emergency call setup should in fact trigger the emergency call setup. Otherwise, the communications device does not attempt the emergency call setup. Therefore, the condition is that the configuration indicates that the message prompting the 20 emergency call setup should in fact trigger the emergency call setup.

In the illustrated example, the communications device receives user input for manipulating the configuration. This provides the user with the ability to specify whether messages 25 prompting an emergency call setup should in fact trigger the emergency call setup. In some implementations, the user can manipulate the configuration at any appropriate time. Note that there does not need to be any user input even though the user may be provided with the opportunity to provide user 30 input. In other implementations, the configuration is non- configurable by the user. The configuration may be non-

configurable for example by being hard-coded. Other implementations are possible.

In another implementation, the communications device receives network input for manipulating the configuration.

5 This allows the configuration to be manipulated by the communications network. In another implementation, the communications device receives both user input and network input for manipulating the configuration. Other implementations are possible.

10 Referring now to Figure 4, at step 4-1 the communications device receives a message prompting an emergency call setup. At step 4-2, the communications device determines whether the message prompting the emergency call setup is in response to a request transmitted by the communications device 15 for establishing a voice call session. At step 4-3, the communications device attempts the emergency call setup only if the message prompting the emergency call setup is in response to a request transmitted by the communications device for establishing a voice call session. Otherwise, the 20 communications device does not attempt the emergency call setup. Therefore, the condition is that the message prompting the emergency call setup is in response to a request transmitted by the communications device for establishing a voice call session. For instance, if the message prompting the 25 emergency call setup is in response to a request transmitted by the communications device for establishing an IM (Instant Messaging) session, then the communications device does not attempt the emergency call setup.

In the illustrated example, behaviour is defined for 30 a specific type of session, namely a voice call session. However, it is to be understood that behaviour may be defined for other types of communication sessions, for example a video

call session. In another implementation, the communications device determines whether the message prompting the emergency call setup is in response to a request transmitted by the communications device for establishing a video call session.

5 According to this implementation, the communications device attempts the emergency call setup only if the message prompting the emergency call setup is in response to a request transmitted by the communications device for establishing a video call session.

10 In the example presented above with reference to Figure 4, the communications device might assume that IM session services should not be redirected to an emergency number. In some implementations, the communications device maintains an identification of services that can be redirected 15 to an emergency number. An example of this is provided below with reference to Figure 5.

Referring now to Figure 5, at step 5-1, the communications device maintains an identification of services that can be redirected to an emergency number. At step 5-2, 20 the communications device receives a message prompting an emergency call setup. At step 5-3, the communications device attempts the emergency call setup only if the message prompting the emergency call setup is in respect of a service that according to the identification can be redirected to an 25 emergency number. Otherwise, the communications device does not attempt the emergency call setup. Therefore, the condition is that the message prompting the emergency call setup is in respect of a service that according to the identification can be redirected to an emergency number.

30 In some implementations, the identification of services that can be redirected to an emergency number may be configurable by the user. In other implementations, the

identification of services that can be redirected to an emergency number is non-configurable. The configuration may be non-configurable for example by being hard-coded. Other implementations are possible.

5 Referring now to Figure 6, at step 6-1, the communications device maintains an identification of trusted sources. At step 6-2, the communications device receives a message prompting an emergency call setup. At step 6-3, the communications device attempts the emergency call setup only if
10 there is indication that the message prompting the emergency call setup was sent from a message source that according to the identification is a trusted source. In some implementations, the message prompting the emergency call setup indicates a message source. In other implementations, the communications
15 device is aware of the message source by other means.

Otherwise, the communications device does not attempt the emergency call setup, as the message prompting the emergency call setup may have originated from a rogue communications device or some other rogue entity. Therefore, the condition is
20 that the message prompting the emergency call setup indicates a message source that according to the identification is a trusted source.

According to the example present above with reference to Figure 6, the message prompting the emergency call setup may
25 be provided with an identification of the message source, which allows a determination of whether to trust the message source. More generally, embodiments of the application are applicable to any SIP message, as there may be other SIP messages received from unknown sources. Such SIP messages might cause other
30 undesirable situations aside from prompting an emergency call setup. Appropriate authentication can be performed to verify

the message source. Further examples are provided in the additional sections below.

In the examples presented herein, there are situations in which receiving a message prompting an emergency call setup does not trigger the communications device to attempt an emergency call setup. In some implementations, the communications device warns a user of the communications device if the emergency call setup is not attempted in response to the message prompting the emergency call setup. The warning may be issued by the communications device, for example via a user interface of the communications device.

Conditional Emergency Call Setup: Another Communication System

In the examples presented above, the communications device conditionally attempts an emergency call setup in response to receiving a message prompting the communications device to attempt an emergency call setup. In another embodiment, the communications network blocks at least some of the messages. In another embodiment, the communications network blocks at least some messages while communications devices conditionally attempt emergency call setups in response to receiving messages prompting emergency call setups.

Referring now to Figure 7, shown is a block diagram of another communications system 70. The communications system 70 has a communications network 72, which has a message blocking function 73 coupled to a processor 76. The communications network 72 may have other components, but they are not shown for sake of simplicity. The communications system 70 has a communications device 74, and may have other communication devices 71. The communication devices 71,74 may each be mobile devices or wired devices. Details of the communication devices 71,74 are omitted for sake of simplicity.

The communication system 70 may have other components, but they are not shown for sake of simplicity.

In operation, the communication devices 71, 74 communicate over the communication network 72. The 5 communication might for example include messages of a defined type that prompt a target communications device to attempt an emergency call setup. For example, one of the other communication devices 71 might send a message of the defined type to the communications device 74. For each messages of the 10 predefined type that is sent, the communications network 72 receives the message. According to an embodiment of the application, the message blocking function 73 blocks at least some of the messages of the predefined type from being forwarded along a signaling data path. Further details are 15 provided below with reference to Figure 8 through 10.

In the illustrated example, the message blocking function 73 is implemented as software and is executed on the processor 76. However, more generally, the message blocking function 73 may be implemented as software, hardware, firmware, 20 or any appropriate combination thereof. Although shown as a single component, more generally, the message blocking function 73 may have one or more components. The one or more components may be distributed throughout the communications network 72 or located on a single network element. The one or more 25 components may be integrated with other components of the communications network 72. In some implementations, the message blocking function 73 includes both a message blocking function for delivering messages to target devices, and a message blocking function for forwarding messages to another 30 component of the communications network 72. Other implementations are possible.

In some implementations, the communications network 72 is a wireless network. However, for the case of wired devices, the communications network 72 need not be wireless. Therefore, in other implementations, the communications network 5 72 is a wired network. In other implementations, the communications network 72 includes a wired network and a wireless network. Other implementations are possible.

The communications network 72 is shown without specific components. However, it is to be understood that the 10 communications network 72 would have any appropriate components suitable for a wired and/or wireless network. The components are implementation specific and may depend on the type of network. The communications network 72 may be of any appropriate type, for example GPRS, UMTS, CDMA etc. IMS 15 services are beareragnostic. In some implementations, the communications network 72 includes P-CSCF (Proxy Call Session Control Function) nodes for processing transmission of SIP messages. Other implementations are possible.

Conditional Emergency Call Setup: Network Methods

20 Referring now to Figure 8, shown is a flowchart of a method of blocking at least some messages from being delivered to their target communications device. This method may be implemented in a communication network, for example by the message blocking function 73 of the communications network 72 25 shown in Figure 7.

At step 8-1, the communication network receives messages, each message being directed at a target communications device for prompting the target communications device to attempt an emergency call setup. At step 8-2, the 30 communication network blocks at least some of the messages from being delivered to their target communications device.

There are many possibilities for each message that is directed at a target communications device for prompting the target communications device to attempt an emergency call setup. Each message may be any appropriate message that 5 prompts an emergency call setup, examples of which have been provided above.

There are many ways for the communication network to block at least some of the messages from being delivered to their target communications device. To illustrate this point, 10 other example methods of blocking at least some of the messages from being delivered to their target communications device are provided below.

Referring now to Figures 9 and 10, shown are flowcharts of other example methods of blocking at least some 15 of the messages from being delivered to their target communications device. These methods may be implemented in a communications network, for example by the message blocking function 73 of the communications network 72 shown in Figure 7.

Referring first to Figure 9, at step 9-1 the 20 communications network maintains at least one condition for forwarding messages that prompt a target communications device to attempt an emergency call setup. At step 9-2, the communications network receives messages, each message being directed at a target communications device for prompting the 25 target communications device to attempt an emergency call setup. At step 9-3, for each message received, the communications network forwards the message to its target communications device only if any of the at least one condition is satisfied.

30 There are many possibilities for maintaining at least one condition for forwarding the messages. In some

implementations, the communications network maintains an identification of trusted sources. Accordingly, in some implementations, for each message received, the communications network forwards the message only if there is indication that
5 the message was sent from a message source that according to the identification is a trusted source. In some implementations, the message prompting the emergency call setup indicates a message source. In other implementations, the communications network is aware of the message source by other
10 means. Other implementations are possible.

In the illustrated example, the communications network forwards the message to its target communications device. In another implementation, the communications network forwards the message to a network component within the
15 communications network. More generally, the communications network forwards the message along a signaling data path, which might involve forwarding the message to its target communications device or forwarding the message to a network component within the communications network. If forwarded to a
20 network component, the message might be forwarded to its target communications device or forwarded to yet another network component within the communications network.

Referring now to Figure 10, at step 10-1 the communications network receives messages, each message being
25 directed at a target communications device for prompting the target communications device to attempt an emergency call setup. At step 10-2, for each message received, the communications network blocks all of the messages from being delivered to their target communications device.

30 In the illustrated example, the communications network blocks all of the messages from being delivered to their target communications device. This might be executed by
1075085_1.DOC

a network component that is in a position to deliver messages to the target communications device, or by a network component that forwards messages to another network component in order for the communications device to receive the messages.

5 Numerous modifications and variations of the present application are possible in light of the above teachings. It is therefore to be understood that within the scope of the appended claims, the application may be practised otherwise than as specifically described herein.

The claims defining the invention are as follows:

1. A method in a communications system comprising a network and a mobile communications device, the method performed by the mobile communications device comprising:

5 sending a Session Initiation Protocol (SIP) INVITE request to the network comprising a Proxy Call Session Control Function (P-CSCF);

receiving a response message prompting an emergency call setup from a message source, the response message being an alternative service message and including identification of the message source, the message having a body in an Extensible Markup Language (XML) including an <alternative service> element with the <type> child element set to "emergency";

determining whether the message source is a trusted source from the identification of the message source in the response message;

attempting the emergency call setup only when the message source 15 is a trusted source.

2. The method of claim 1, wherein the determining whether the message source is a trusted source comprises:

maintaining an identification of a trusted source; and

comparing the identification of the message source with the

20 identification of the trusted source.

3. The method of claim 1 or claim 2, wherein the alternative service message is a redirection message sent in response to the SIP INVITE request message from the communications device.

4. The method of any one of claims 1 to 3, wherein the message 25 source is the network.

5. The method of any one of claims 1 to 4, wherein the attempting the emergency call setup occurs over the circuit-switched (CS) domain.

6. A computer readable medium having computer executable instructions stored thereon for execution on a processor of a communications device so as to implement the method of any one of claims 1 to 5.

7. A communications device comprising:
5 a processor; and
an emergency call set-up function coupled with the processor and configured to:
10 send a Session Initiation Protocol (SIP) INVITE request to the network comprising a Proxy Call Session Control Function (P-CSCF);
receive a Session Initiation Protocol (SIP) response message from a message source prompting the device to attempt an emergency call setup, the response message being an alternative service message and including identification of the message source, the message having a body in an Extensible Markup Language (XML) including an <alternative service> element with the <type> child element set to "emergency";
15 determine whether the message source is a trusted source from the identification of the message source in the response message; and
20 attempt the emergency call setup only when the message source is a trusted source.

8. The communications device of claim 7, wherein to determine whether the message source is a trusted source, the emergency call function is configured to:
25 maintain an identification of a trusted source; and
compare the identification of the message source with the identification of the trusted source.

9. The communications device of claim 7 or claim 8, wherein the alternative service message is a redirection message sent in response to the SIP INVITE request message from the communications device.
30

10. The communications device of any one of claims 7 to 9, wherein the communications device is a mobile device comprising a wireless access radio.

11. A method in a communications system comprising a network and a communications device, the method performed by the communications device comprising:

5 maintaining an identification of a trusted source of messages;

sending a request message to the network, the request message being a Session Initiation Protocol (SIP) INVITE request, the network comprising a Proxy Call Session Control Function (P-CSCF);

10 receiving a response message prompting an emergency call setup from a message source, wherein the response message was sent in response to the request message, the response message being an alternative service message and including identification of the message source, the message having a body in an Extensible Markup Language (XML) including an <alternative service> element with the <type> child element set to "emergency";

15 comparing the message source with the identification of a trusted source; and

attempting the emergency call setup only when the message source is equal to the identification of a trusted source.

20 12. A mobile communications device comprising:

a processor; and

a function coupled with the processor and configured to:

25 maintain an identification of a trusted source of messages;

send a request message to the network, the request message being a Session Initiation Protocol (SIP) INVITE request, the network comprising a Proxy Call Session Control Function (P-CSCF);

30 receive a response message prompting an emergency call setup from a message source, wherein the response message is received in response to the request message, the response message being an alternative service message and including identification of the message source, the message having a body in

an Extensible Markup Language (XML) including an <alternative service> element with the <type> child element set to "emergency";

5 compare the message source with the identification of a trusted source; and

attempt the emergency call setup only when the message source is equal to the identification of a trusted source.

13. A method in a communications device, said method being substantially as described herein with reference to the accompanying drawings.

14. A computer readable medium having computer executable 10 instructions stored thereon for execution on a processor of a communications device so as to implement a method in a communications device, said method being substantially as described herein with reference to the accompanying drawings.

15. A communications device configured to implement a method in a 15 communications device, said method being substantially as described herein with reference to the accompanying drawings.

16. A network method for emergency call setup, said network method being substantially as described herein with reference to the accompanying drawings.

20 17. A computer readable medium having computer executable instructions stored thereon for execution on a processor of a communications network so as to implement a network method for emergency call setup, said network method being substantially as described herein with reference to the accompanying drawings.

- 28 -

18. A communications network configured to implement a network method for emergency call setup, said network method being substantially as described herein with reference to the accompanying drawings.

DATED this Twenty-Fifth Day of October, 2010

Research In Motion Limited

Patent Attorneys for the Applicant

SPRUSON & FERGUSON

5

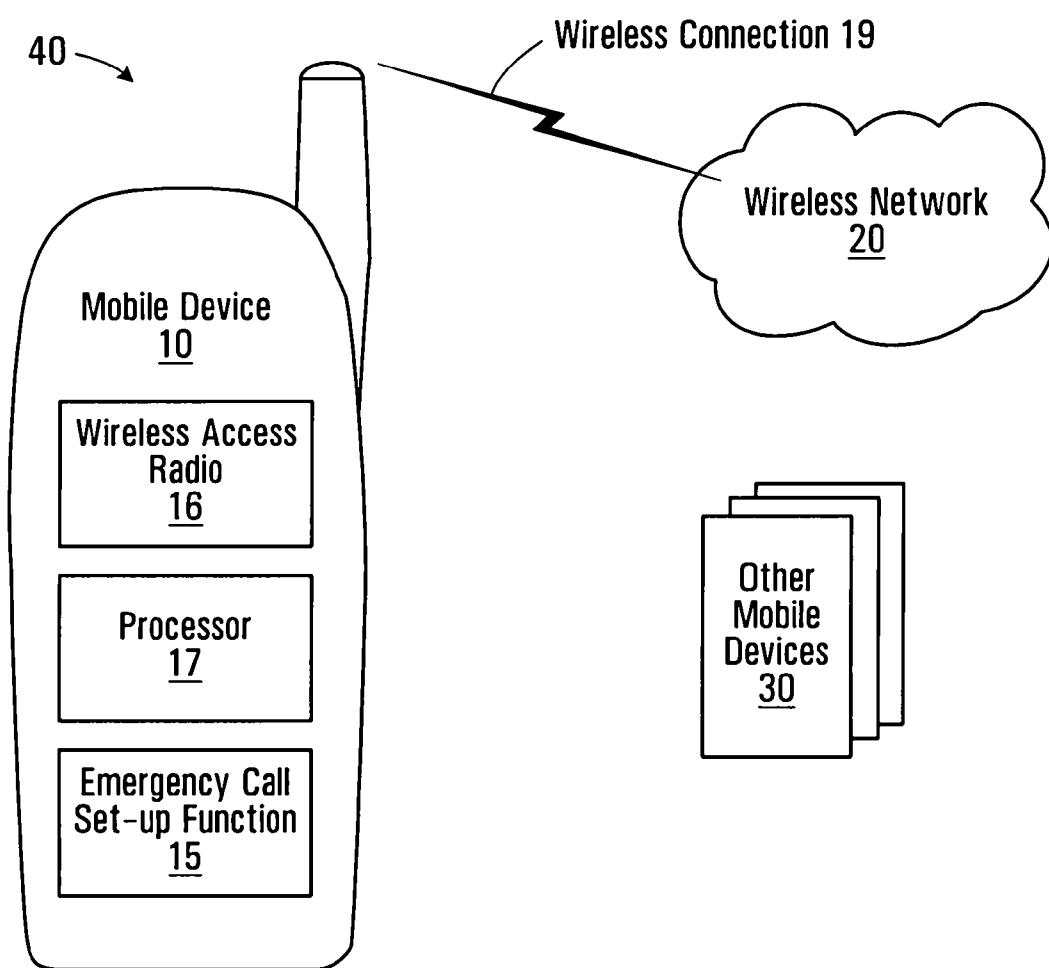


FIG. 1A

2008200030 03 Jan 2008

2/9

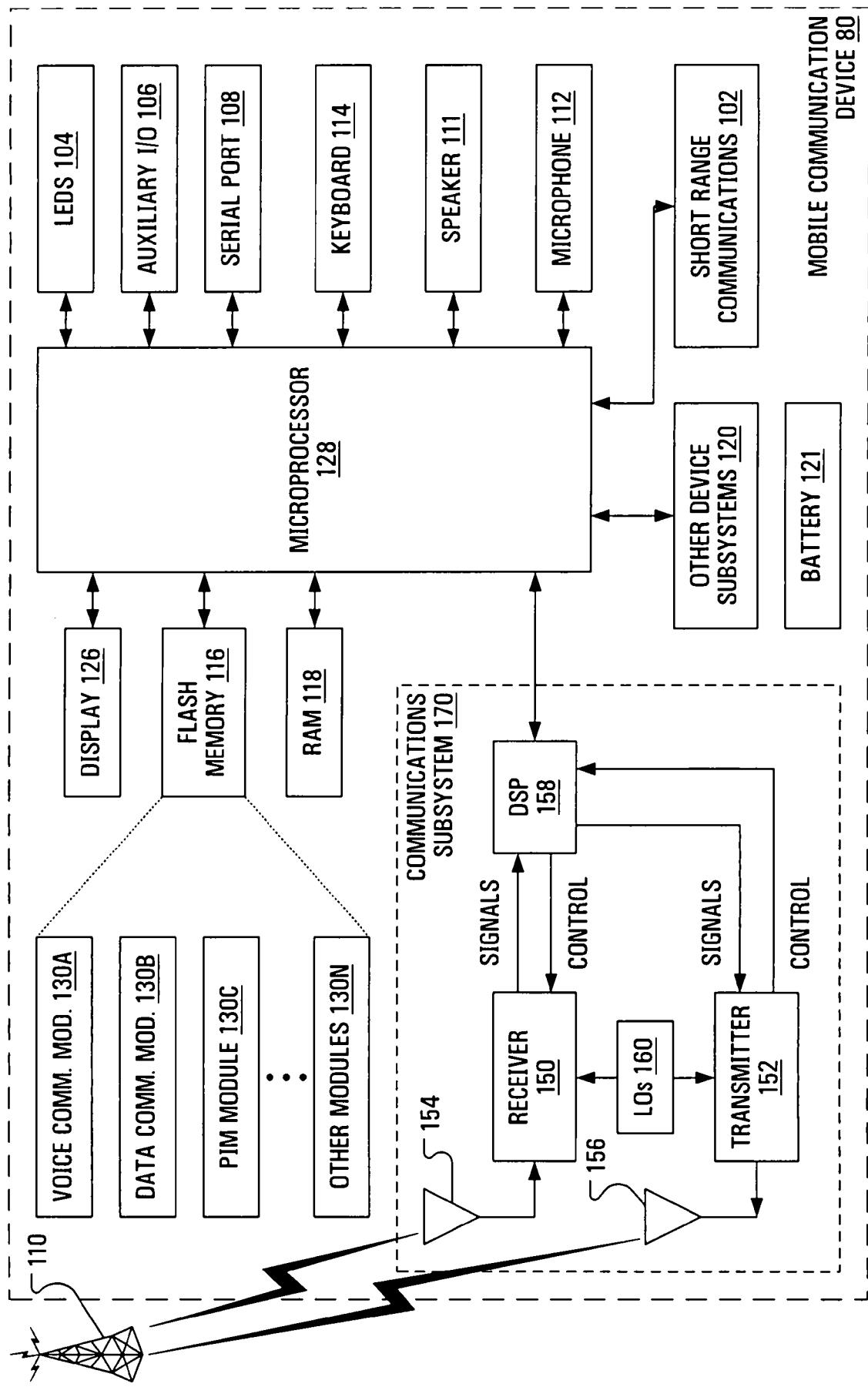
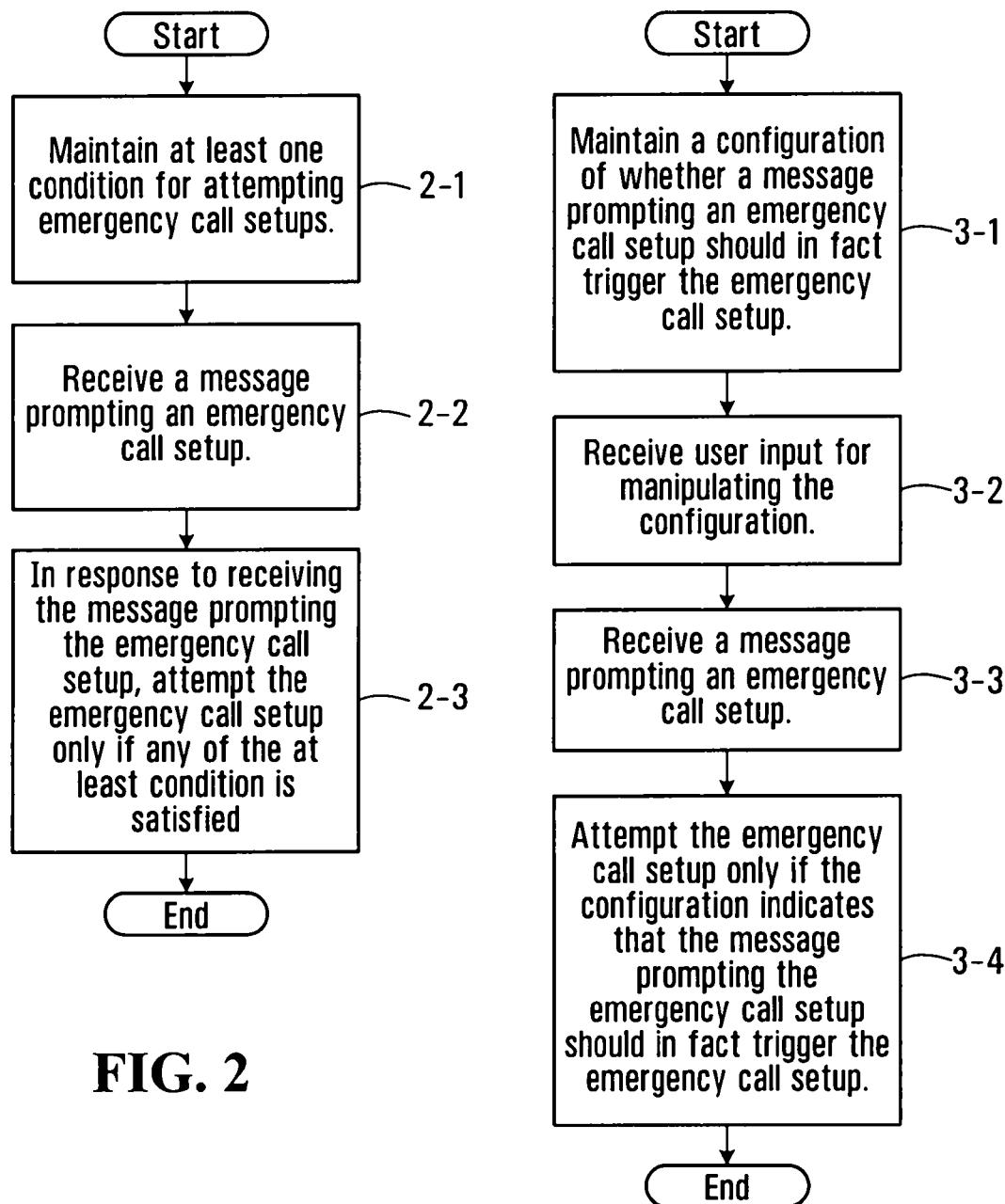
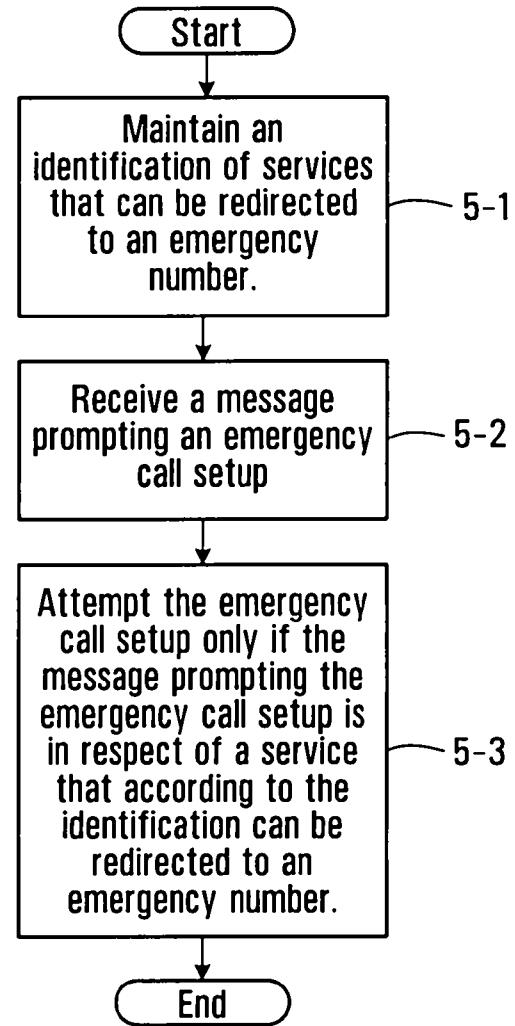
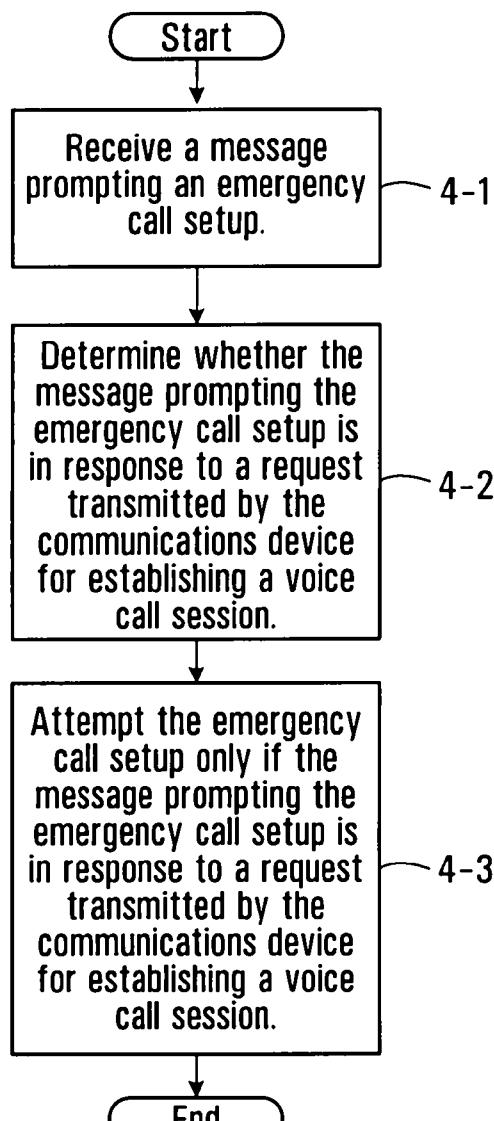


FIG. 1B

3/9



4/9



5/9

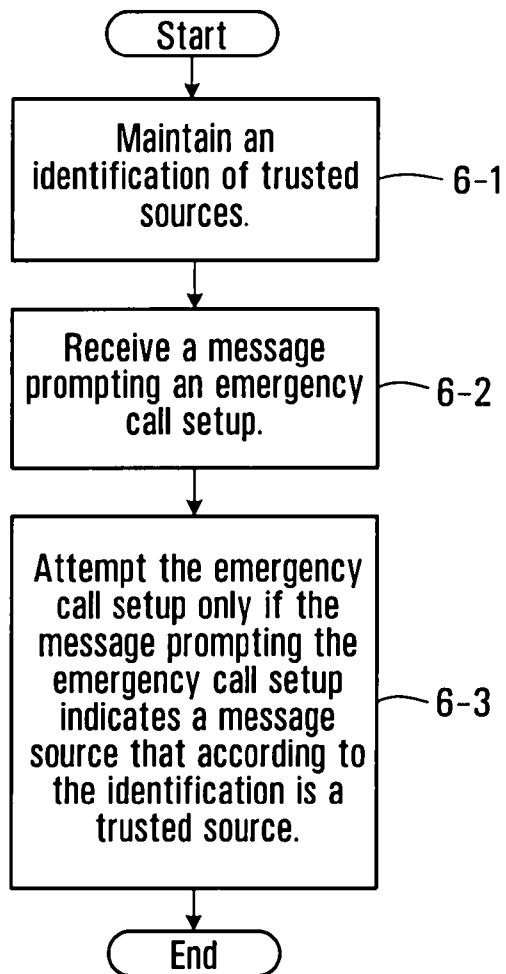


FIG. 6

6/9

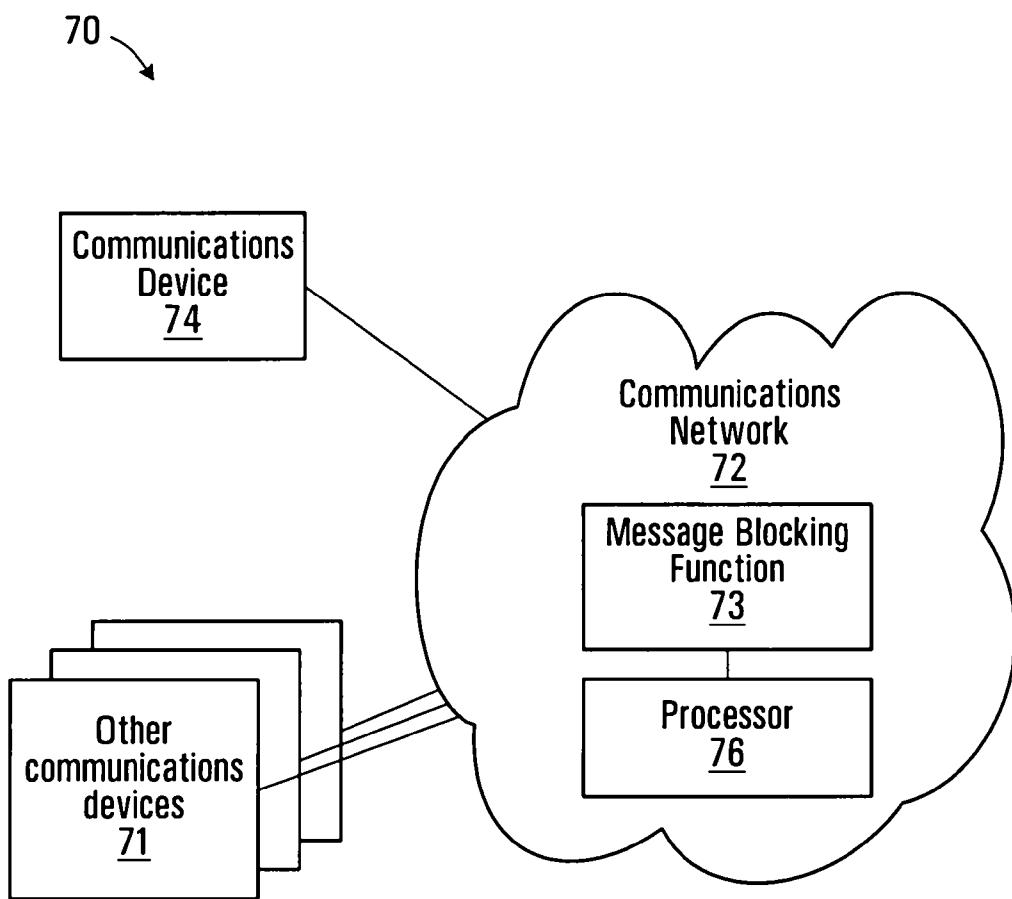


FIG. 7

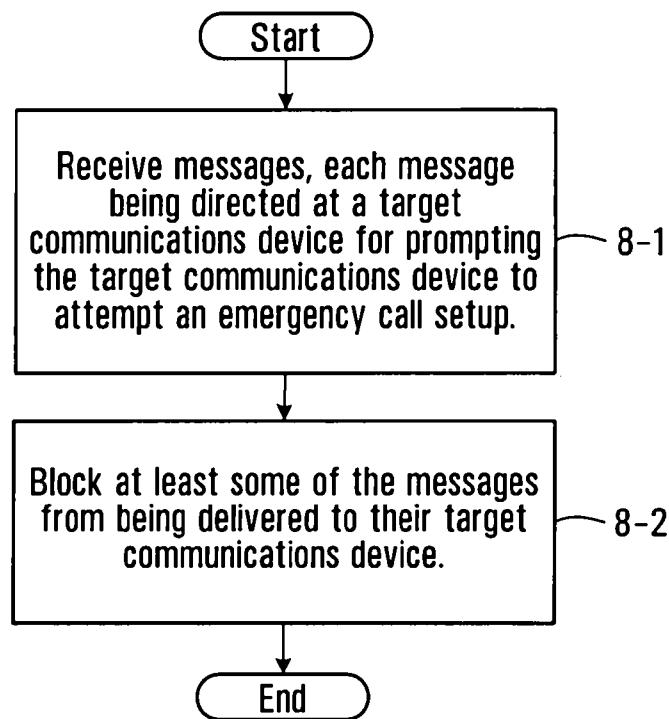


FIG. 8

8/9

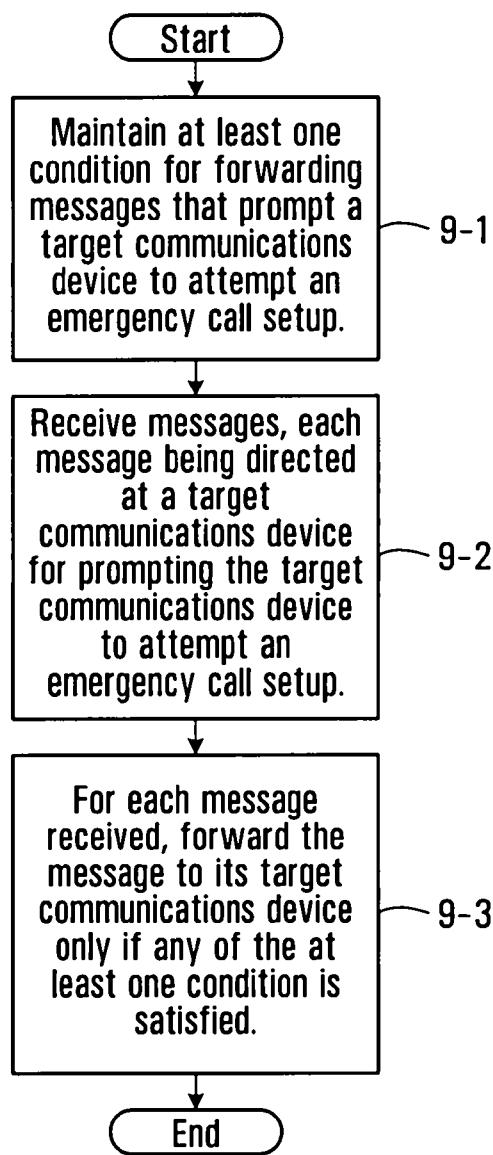


FIG. 9

9/9

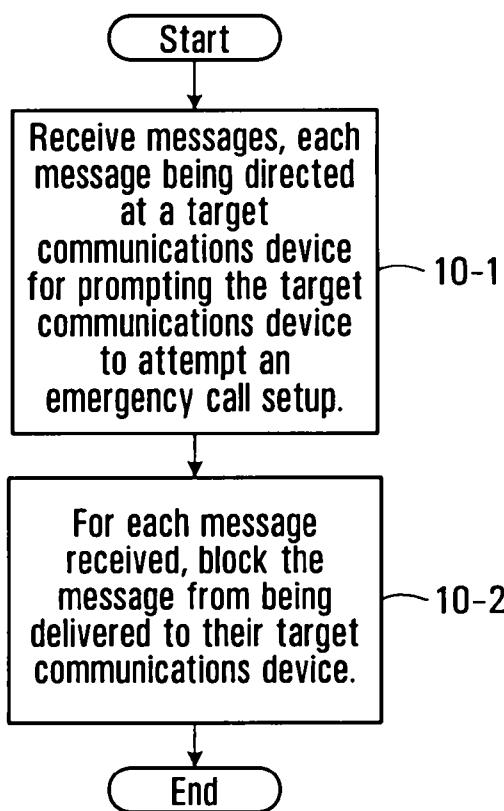


FIG. 10