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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 October 2017 (05.10.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/167701 A1

(51) International Patent Classification:
H04W 36/00 (2009.01) *H04W 84/12* (2009.01)
H04W 36/30 (2009.01) *H04W 76/04* (2009.01)
H04W 36/36 (2009.01)

(21) International Application Number:
PCT/EP2017/057225

(22) International Filing Date:
27 March 2017 (27.03.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16163457.1 31 March 2016 (31.03.2016) EP

(71) Applicant: **BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY** [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB).

(72) Inventor: **FAUS GREGORI, Francisco Jose**; Ground Floor, Faraday Building, 1 Knightrider Street, London EC4V 5BT (GB).

(74) Agent: **CHAN, Robin**; BT Intellectual Property Department, Ground Floor, Faraday Building, 1 Knightrider Street, London EC4V 5BT (GB).

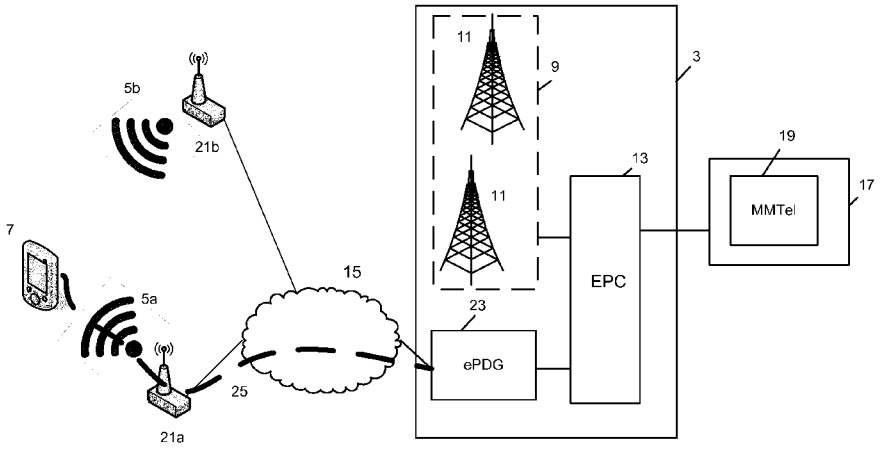
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS,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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report (Art. 21(3))*

(54) Title: HANDOVER METHOD

Fig. 1



1

(57) Abstract: A method of performing network handover between wireless local area network devices for a mobile device connected to a voice service via a secure data tunnel to a packet data gateway of a cellular network, comprising: determining that a quality of a connection to a current wireless local area network is below a threshold value; determining that a handover target network is available; establishing connectivity with the target handover network; suppressing a connection to a base station of the cellular network; sending a new network address of the mobile device to the packet gateway using a set of credentials relating to the secure data tunnel so as to change an endpoint of the secure data tunnel to the new network address.

WO 2017/167701 A1

Handover method

The present invention relates to wireless networks and in particular to a method for performing handover between Wireless local area networks supporting a VoWiFi voice service.

Background

Wireless Local Area networks

Wireless local area networks (WLAN) provide wireless data connectivity to wireless client devices over a limited coverage range. Commonly known as WiFi™, the wireless networking protocol is defined by the IEEE 802.11 family of standards. The standards specify how frequencies, data rates, authentication, etc. to allow internetworking between devices from different manufacturers.

VoWiFi

A recent development is the ability for client devices to offer voice calling through the standard dialler application on mobile device. In contrast to Voice over IP (VoIP) services, the mobile device is contactable via the cellular number associated with the device via a cellular, and in particular Long Term Evolution (LTE) data network.

The VoWiFi application resides within the IMS platform and therefore can allow handover between the cellular network and VoWiFi supporting WiFi network estate. A typical handover scenario is when a user returns home and the mobile device which is connected to a macrocell of the LTE network hands over to the user's home network wireless network to maintain the same service. When the user leaves the range of their home network, then their mobile device will be configured to handover from the home WLAN to the macrocell eNodeB.

In the current implementations, only handovers from VoLTE to VoWiFi and VoWiFi to VoLTE are considered.

Although a WiFi network generated by a single Wireless Access Point may only extend for tens of metres due to transmission power constraints, it is known to configure several WAPs to have the same SSID and authentication settings to allow client devices to change physical location while still being connected to WiFi. A corporate network in a large office building is an example. Furthermore, public hotspot networks are also known whereby the access points are placed over a geographic area such as a city and configured to have the same SSID but no WLAN authentication. A centralised server carries out authentication at a higher network layer and client WiFi devices with a valid login are able

to access the hotspot network wherever there is a hotspot device. An example of a hotspot network is the BT WiFi™ network.

Especially in densely populated areas, the range of these hotspot WAPs may result in there being a contiguous range of WiFi connectivity such that the user can travel for a range beyond their home WiFi network and still be connected to the same WiFi hotspot network. However, for VoWiFi, the standard handover mechanisms require the VoWiFi service to handover to the VoLTE service before then handing over back to the newly connected WiFi network and VoWiFi service. This processing to switch between three different physical networks is costly in terms of time and processing power.

Similarly, if the user does not wish to use VoLTE or their device is not capable of supporting the LTE network, it is not possible to seamlessly switch between WAPs so that VoWiFi connectivity is maintained without a temporary break in service where calls and messages may be missed.

Aspects of the present invention address the above problem of handover between non-3GPP access networks.

Statements of invention

In one aspect, the present invention provides a method of performing network handover between wireless local area network devices for a mobile device connected to a voice service via a secure data tunnel to a packet data gateway of a cellular network, comprising: determining that a quality of a connection to a current wireless local area network is below a threshold value; determining that a handover target network is available; establishing connectivity with the target handover network; suppressing a connection to a base station of the cellular network; sending a new network address of the mobile device to the packet gateway using a set of credentials relating to the secure data tunnel so as to change an endpoint of the secure data tunnel to the new network address.

In a second aspect, an embodiment of the invention provides an apparatus for connecting to a voice service via a secure data tunnel to a packet data gateway of a cellular network and operable to perform network handover between wireless local area network devices via a secure data tunnel to a packet data gateway of a cellular network, comprising: a cellular network interface; a wireless local area network interface; means for determining that a quality of a connection to a current wireless local area network is below a threshold value; means for determining that a handover target network is available; means for establishing connectivity with the target handover network; means for suppressing a connection to a base station of the cellular network; means for sending a new network address of the mobile device to the packet gateway using a set of credentials relating to the secure data tunnel so as to change an endpoint of the secure data tunnel to the new network address.

Figures

A first embodiment of the present invention will now be described with reference to the following figures in which:

Figure 1 is an overview of a voice service network formed of both a cellular network and a number of wireless access points;

Figure 2 shows the voice service network where a mobile device has connected to the cellular network;

Figure 3 shows the voice service network where the mobile device has connected to a second wireless access point and established a new data tunnel to the cellular network;

Figure 4 shows the functional components of a mobile device;

Figure 5 shows the functional components of a packet data gateway;

Figure 6 is a flowchart of the processing of the handover manager shown in Figure 4;

Figure 7 is a flowchart of the processing of the IPSec manager shown in Figure 4; and

Figure 8 is a flowchart showing the processing of an IPSec manager shown in Figure 5.

Description

Figure 1 shows an overview of voice system 1 including a cellular network system 3 and a number of wireless local area networks (WLAN) 5. The system also includes mobile devices 7 having cellular network interfaces to enable connection to the cellular network 3 and wireless local area network (WLAN) interfaces to enable connection to the WLANs 5 so that a voice service can be provided via both interfaces. For ease of explanation, only a single mobile device 7 is shown and described.

The cellular network 3 provides wide area cellular connectivity to the mobile device 7 which is a mobile phone. In this embodiment the cellular network is a Long Term Evolution (LTE) network. The cellular network 3 includes a radio access network 9 of macrocells 11, implemented as eNodeBs in LTE, and the mobile device 7 accesses the cellular network via one of the macrocells 11. The radio access network is connected within the cellular network to a mobile network core 13, implemented as an Evolved Packet Core (EPC) in LTE, which contains functionality for managing the non-Access aspects of the cellular network such as performing control functions including allocating network addresses, cell tracking area updates, mobile device authentication and billing, etc. In addition to the control

plane functions, the network core also contains Serving Gateways and Packet Gateways for routing mobile device packets between the devices and network resource which may be located on external wide area networks such as the Internet 15.

To allow mobile devices to access a voice service in the LTE network, and in particular a Voice over LTE (VoLTE) service, the network core 3 is connected to an IP Multimedia Subsystem (IMS) 17 which includes a Multimedia Telephony (MMTel) service 19 which manages voice services for mobile devices 7 in accordance with VoLTE. MMTel is defined in the 3rd Generation Partnership Project (3GPP) specification TS 22.173.

The mobile devices 7 have a cellular interface to allow them to connect to one of the macrocells 11 forming the radio access network 9 of the cellular network 3. Once connected to the radio access network 9 and authenticated with the network core 13, the client device 7 can access voice and data services such as VoLTE.

The mobile device 7 also contains a wireless local network interface to access wireless local area networks (WLAN) 5 which are generated by a respective wireless access point 21. In Figure 1, two wireless access points are shown. The mobile device 7 is connected to a first wireless access point 21a which generates a WLAN 5a in accordance with the IEEE 802.11 family of protocols commonly known as Wi-Fi. A second wireless access point 21b is also shown which generates a second WLAN 5b. The second wireless access point 21b is located such that the extent of the second WLAN 5b overlaps with the extent of the first WLAN 5a such that the mobile device could connect to either WLAN 5 but has connected to WLAN 5a due to a stronger signal strength to WLAN 5a from the mobile device's 7 current location.

The wireless access point 21 associated with each WLAN 5 is connected to a wide area network such as the Internet 15 so that the mobile device can access remote data services and resources. Furthermore the mobile device 5 is allocated an Internet Protocol (IP) address so that data sessions can be correctly routed to and from the remote resources. In this example, the wireless access point 21 is allocated a global IP address which can be addressed by any remote resource and then uses Network Address Translation (NAT) to allocate a local IP address from a private range of addresses. However due to the NAT feature, the mobile device is deemed by external devices to also have the same address as the wireless access point 21. For example the wireless access point 21a has a global IP address of 89.1.5.53 and allocates the client device has a local address of 192.168.1.45 which is only valid within the WLAN. To external devices, the mobile device has an IP address of 89.1.5.53.

In this embodiment, the client also supports Voice over WiFi (VoWiFi) whereby the mobile device 7 can access the MMTel voice service 19 when connected to a WLAN instead of VoLTE via the cellular network 3. To enable VoWiFi, the cellular network 3 includes an Evolved Packet Data Gateway (ePDG) 23 in the network core 13 for communication with the WLANs 5 which are deemed in 3GPP to be untrusted non-3GPP access networks into the cellular network.

Since the WLANs 5 are untrusted access networks, any data session between a VoWiFi client (not shown) in the mobile device 7 and the ePDG 23 for VoWiFi must be secured using an encrypted data tunnel 25. In this embodiment the Internet Protocol Security (IPSec) framework relating to data confidentiality, data integrity and data authentication is used to secure the tunnel. IPSec is described in RFC 2401. Any other data sessions which do not involve access to the cellular network 3 would not travel via the data tunnel 25.

To enable the establishment of an IPSec tunnel, the ePDG 23 has a global IP address which in this example is 204.83.73.84.

In accordance with IPSec routines, the VoWiFi client in the mobile device 7 and the ePDG 23 establish a secure data tunnel through a series of authentication, verification steps including Internet Security Association and Key Management Protocol (ISAKMP).

The IPSec tunnel is actually formed of a pair of Security Associations (SA). In IPSec, SAs are a bundle of algorithms and parameter data sets which are used to encrypt and authenticate a particular flow in one direction. Therefore a pair of SAs are used to secure the bi-directional session. Each SA data set contains a Security Parameter Index (SPI), destination address, security keys, transforms, lifetime, etc. The SPI is an identification tag which is added to a packet header when tunnelling the IP traffic. The tag is added by a sender and used by the receiver to uniquely associate a received tunnelled packet with an IP flow where different encryption protocols and algorithms may be in use.

As shown in Figure 1, the VoWiFi client of the mobile device 7 has at least the following IPSec SA data:

UE IP address: 89.1.5.53

SA1: SPI 1be0ac4585574a8f, Dest IP 204.83.73.84,

SA2: SPI: 84167b6600000000, Dest IP: 89.1.5.53,

In the context of VoWiFi, the mobile device 7 will only be connected to a single ePDG and therefore only stores details of a single IPSec tunnel.

The ePDG 23 can potentially be the end point for several IPSec tunnels and therefore it can store state data for a number of IPSec tunnels including the mobile device 7 address, an IPSec identifier and SA configuration data.

An example of the data stored at the ePDG 23 relating to the IPSec tunnel to the mobile device 7:

Device 1	Device 2	Device 3
UE IP address 89.1.5.53	empty	empty
IP Sec tunnel identifier A		
Device 1 IPSec SA config data.		

Once the IPSec tunnel 25 has been established, the mobile device 7 is authenticated by the network core 13 functions in a conventional manner using for example, EAP-SIM. To enable VoWiFi for the mobile device 7, the network core 13 establishes a link from the mobile device data packets flowing via the IPSec tunnel 25 with the MMTel service 13 within the IMS 11.

While the mobile device 7 is connected to the WLAN 5a generated by the first wireless access point, the mobile device 7 will remain connected to VoWiFi in preference to VoLTE and data will continue to flow via the IPSec tunnel 25.

However, when the mobile device 7 changes location such that it cannot stay connected to the WLAN 5a generated by the first wireless access point 21a, it will connect to another WLAN in range. As shown in Figure 2 the mobile device has connected to WLAN 5b generated by wireless access point 21b.

As currently defined in the VoWiFi standards, the loss of the WLAN connection triggers the mobile device 7 to attempt to register with VoLTE.

Figure 2 shows the voice system 1 when the client device 7 has changed location so that it is not within the connectivity range of the first wireless access point 15. The client device 5 is now physically located nearer to the WLAN 5b of the second wireless access point 21b.

In this embodiment, the general behaviour of the mobile device 7 is to try to connect to a WLAN connection in preference to an LTE connection. Therefore when the mobile device 7 loses its link to the WLAN 5a of the first wireless access point 21, if it detects the WLAN 5b of the second wireless access point 21b it will connect to the WLAN 5b without checking the status of the cellular network connection and any non-real time data sessions will not be disrupted.

However, in the processing for VoWiFi and VoLTE, the default action defined in the standards in response to a loss of VoWiFi is to try to connect to VoLTE. As a result, mobile device 7 will perform a cleanup process to remove its end of the tunnel and the eDPG 23 will remove its settings for the IPSec tunnel to the mobile device 7 since the tunnel is deemed to be no longer required.

However, since the client device has connected to WLAN 5b of the second access point 21b, the mobile device 7 will try to re-establish the VoWiFi service via the ePDG 23.

Figure 3 shows the voice system 1 where the mobile device 7 has connected to the second wireless access point 21b, and a new IPSec data tunnel 31 is formed between the VoWiFi manager of the mobile device 5 and ePDG 23.

As with the first data tunnel 25, the configuration of the second data tunnel 31 is stored at both the mobile device 7 and the ePDG 23. The mobile device 7 now stores a new set of IPSec SA config data:

UE IP address 10.210.207.41

SA1: SPI 1be0ac4585574a8f, Dest IP 204.83.73.84, etc

SA2: SPI: 84167b6600000000, Dest IP: 10.210.207.41, etc

The ePDG 23 stores new IPSec tunnel data for the mobile device 7.

Device 1	Device 2	Device 3
Empty	UE IP address 10.210.207.41	empty
	IPSec tunnel identifier B	
	2 IPSec SA config data	

The ePDG 23 regards the mobile device 7 as a new device with a new IPSec tunnel identifier and SA config data because the state data for the mobile device 7 had already been deleted when the connection to VoWiFi via the WLAN 5a of the first wireless access point 21a was broken.

The processing required to tear down and re-establish a data tunnel for the same device within a short period of time is wasteful of resources.

To improve the utilisation of network resources, in the first embodiment, the processing of the mobile device 7 and the ePDG 23 is altered to allow the mobile device 7 to move from one WLAN to another WLAN while maintaining an existing IPSec tunnel. In particular, the new network location of the mobile device end of the IPSec tunnel is securely updated at the ePDG.

For example, using the processing of the first embodiment, a transition from the voice network shown in Figure 1 to the voice network 1 shown in Figure 3 is possible while omitting the intermediary state shown in Figure 2.

After the update, the IPSec tunnel state data for the mobile device is:

UE IP address **10.210.207.41**

SA1: SPI 1be0ac4585574a8f, Dest IP 204.83.73.84, etc

SA2: SPI: 84167b6600000000, Dest IP: **10.210.207.41**, etc

The entry for the mobile device 7 in the ePDG (device 1) is updated as shown below:

UE IP address 89.1.5.53	→	UE IP address **10.210.207.41**
IP Sec tunnel identifier A		IPSec tunnel identifier A
Device 1 IPSec SA config data.		Device 1 IPSec SA config data

The components of the voice system which implement the first embodiment will now be described.

Figure 4 shows the functional components of the mobile device 7. The mobile device includes a cellular network interface 41 and a WLAN network interface 43 for connection and communication with cellular networks 3 and WLANs 5 respectively. A data link interface 45 manages which interface 41, 43 is in use for communication sessions with external devices since in general only one interface is active at a time to prevent excessive batter consumption.

An operating system layer 47 is an interface between the data link interface 45 and higher network level layers such as applications and services layer 49. A telephony application 51 resides in the application layer 49 and is the operable to use the MMTel voice service via VoLTE or VoWiFi.

In accordance with the first embodiment, the client device also includes a modified Handover manager 53 and IPSec manager 55.

The handover manager 53 is responsible for managing the data connection to a radio access network which will be either a Wireless access point using WLAN or a macrocell/small cell using LTE. Functions

of the handover manager 53 include monitoring the quality of the current physical layer connection; determining when connectivity is about to be lost with currently connected wireless access point 21, storing handover and user preferences, WLAN or VoLTE preferences, options for Voice over BB if VoLTE is not available, time threshold for waiting for a handover before dropping the SA configuration, SSID blacklists, WLAN quality threshold to initiate handover.

The handover manager is also arranged to use a combination of the network policies or user preference to consider a VoWiFi switch to another wireless access point instead of registering to a macrocell and VoLTE as soon as a break in VoWiFi service is detected.

The IPSec manager 55 in the first embodiment manages the IPSec tunnels and connections to the ePDG 23 and in particular when instructed by the handover manager to make internal changes to the IPSEC SA and send an updated source address and the new IP address of the client device on the new wireless access point to the ePDG in a ISAKMP informational message.

In this embodiment, the IPSec manager 55 uses the IKEv2 Mobility and Multihoming Protocol (MOBIKE) defined in Request for Comments (RFC) 4555 for the signalling exchange which is an extension of the regular IKEv2 protocol as specified in the usual VoWiFi standards.

Figure 5 shows the functional components of an ePDG 23 in the first embodiment. The ePDG includes a tunnel interface 61 for communication with devices located on the untrusted non-3GPP network and a core network interface 63 for communication with components of the network core 13 of the cellular network 3. For the processing of the first embodiment, the ePDG also includes a modified ePDG IPSec manager for processing update messages from the mobile devices when they have changed to a WLAN and to update IPSec tunnel entries stored in an IPSec configuration store 67.

The operation of the handover manager 53, IPSec manager 55 of the mobile device 7 and the IPSec manager 65 of the ePDG 23 will now be described with the aid of the Figures 6 to 8.

Figure 6 is a flowchart of the processing of the Handover manager. When the mobile device 7 has established a VoWiFi data session via the ePDG 23, in step s1, the handover manager accesses the handover and user preferences database to set various control thresholds and preferences governing handover behaviour. Such preferences include:

WLAN or VoLTE HO preferred,

Voice over mobile BB if no VoLTE available,

new connection HO max wait time before SA drop,

SSID blacklist,

WLAN quality thresholds to initiate HO.

Once loaded, in step s3, the handover manager monitors the quality of the wireless connection to the connected wireless access point 21 which is used as an indication of the relative proximity of the mobile device 7 and wireless access point 21. In this embodiment, quality is the SNR signal strength but the signal strength can also be calculated in combination with other variables such as throughput, error rate, dropped packet rate, etc.

In step s5, the handover manager compares the signal strength against a threshold handover value loaded from the handover and user preferences database. If the quality is above the threshold, then no handover action is required and so the processing returns to step s3.

If the processing of step s5 determines that the quality of the connection has dropped below the threshold, this is an indication that the mobile device is moving outside of the range of the wireless access point, or that there is interference in the vicinity which is affecting the connection quality. In either case, since the quality to that wireless access point 21 is deteriorating, the handover manager must try to handover the mobile device 7 to a different connection to maintain the voice data link to the MMTel service.

In step s7, the handover manager first checks whether a set of conditions have been satisfied, namely:

if WiFi handover is preferred for the client device;

are alternative WLANs available; and

are any of the identified neighbouring wireless access points in the blacklist.

If it is determined that there is at least one non-blacklisted access point, then in step s9 the handover manager hands over the mobile device 7 to a new candidate WLAN, in the example above the WLAN 5b of the wireless access point 21b.

In step s11, the handover manager instructs the IPSec manager to update the tunnel. The processing for the IPSec manager will be explained later.

After step s11 the processing of the handover manager in respect to the first wireless access point 15 ends. However, now that the mobile device 7 is connected to WLAN 5b of the second wireless access point 21b, the processing of the handover manager will repeat on the WLAN 5b from step s1.

Returning to step s7, if the conditions are not met, then there are no non-blacklisted WLAN handover options currently available. Therefore in step s13 the handover manager checks to see whether the mobile device 7 is configured so that VoLTE is preferred and available. If the LTE connection is preferred and available, then in step s15 a handover is initiated to VoLTE via the cellular network and processing ends until the mobile device 7 reconnects to a wireless access point 21.

If VoLTE is not available, the in step s17 a check is performed to see whether the settings will allow a handover to a mobile non-LTE cellular connection. If available, then in step s19 there is a handover to a mobile broadband connection and in step s11 the IPSec manager is instructed to update the tunnel to the ePDG and processing ends.

Finally, if the VoBB is not available, then processing ends such that the user will temporally lose connectivity until a suitable VoWiFi or VoLTE connection can be re-established.

Figure 7 is a flowchart showing the processing of the IPSec tunnel manager.

In step s21, the IPSec manager receives instructions to handover from the handover manager. In this case the client device has already been re-connected to a new wireless access point and now the IPSec tunnel needs to be updated so that the ePDG 23 is aware of the new location for the mobile device 7.

In step s23, a new connection is established to the WLAN 5b of the second wireless access point 21b. In step s25, the SA is updated with new local address information, in particular the new IP address of the mobile device connected to the wireless access point 21 (or mobile broadband in accordance with the functioning of the handover manager).

Once the mobile device's 7 IPSec tunnel information has been updated, in step s27 the IPSec manager sends an informational message to the ePDG's 23 IPSec manager using the existing Internet Security Association and Key Management Protocol (ISAKMP) session to notify the updated local IP address and handover manager decision. In this embodiment, this step is carried out using the MOBIKE protocol defined in RFC 4555 herein incorporated by reference.

Next in step s29 the Encapsulation Security Payload (ESP) packets are routed using the new interface and local source IP address. These packets are carried via the unmodified outbound SA. The ESP is one

of the protocols forming part of the IPSec and relates to origin authenticity, integrity and confidentiality protection of packets.

In step s31 a check is performed to determine whether the tunnel update has been successful based on the reception of a response message from the ePDG IPSec manager. If a response is received, then processing ends because the update has been successful. VoWiFi data packets are routed via the tunnel until the handover manager determines otherwise.

If a response is not received, then in accordance with user preference information, the IPSec manager waits for a period of time before re-transmitting in step s33. At step s35, while a timeout period has not expired, then processing returns to step s31 to test for a response. However, if the timeout period expires and there is no response, then in step s37 a clean up operation is carried out to delete the SA and end the call.

Figure 8 is a flowchart showing the processing of the ePDG IPsec manager.

Processing begins in step s41, when the ePDG IPSec manager receives a message from a client device IPSec manager including a notification that there has been a change to the local IP interface. The message includes identifier information such as the SA SPI and destination IP address.

In step s43, the ePDG IPSec manager determines which of the IPSec SAs is associated with the message.

In step s45, if the received SA information cannot be used to identify an existing stored SA, then there is no IPSec information to update and so processing ends.

However if an SA can be identified, then in step s47, that SA is updated with a new destination address for the outbound SA.

Next, in step s49, the ePDG IPSec manager's ESP packets are sent with downstream RTP traffic through the updated SA. And in step s51 the ePDG IPSec manager confirms the SA update using the new destination IP address provided.

In step s53 the ePDG IPSec manager verifies the updated IP address as a true client device end point of the IPSec SA, in this embodiment this is carried out using a Return Routability Check procedure.

In step s55 a check is carried out to test whether a response has been received from the client device which requested the update. If a response has been received then processing ends. If a response has not yet been received, then in step s57 a timer is started so that the ePDG IPSec manager waits a

predetermined period of time before trying to re-transmit the client device response initially delivered in step s51. At step s59 the timeout period is evaluated and if the timeout has not been reached the ePDG IPSec manager waits again to retransmit the response message.

If however, the timeout period has elapsed, in step s61, the SA is deleted and processing ends.

In the first embodiment, the handover behaviour of the client device is modified to enable VoWiFi to VoWiFi handovers where possible. This processing reduces the overhead on the ePDG and client device for the maintenance of data tunnels because there is need to tear down and re-establish a sets of data tunnels following the migration from a first wireless access point to a second wireless access point.

Insofar as embodiments of the invention described are implementable, at least in part, using a software-controlled programmable processing device, such as a microprocessor, digital signal processor or other processing device, data processing apparatus or system, it will be appreciated that a computer program for configuring a programmable device, apparatus or system to implement the foregoing described methods is envisaged as an aspect of the present invention. The computer program may be embodied as source code or undergo compilation for implementation on a processing device, apparatus or system or may be embodied as object code, for example.

Suitably, the computer program is stored on a carrier medium in machine or device readable form, for example in solid-state memory, magnetic memory such as disk or tape, optically or magneto-optically readable memory such as compact disk or digital versatile disk etc., and the processing device utilises the program or a part thereof to configure it for operation. The computer program may be supplied from a remote source embodied in a communications medium such as an electronic signal, radio frequency carrier wave or optical carrier wave. Such carrier media are also envisaged as aspects of the present invention.

It will be understood by those skilled in the art that, although the present invention has been described in relation to the above described example embodiments, the invention is not limited thereto and that there are many possible variations and modifications which fall within the scope of the invention.

The scope of the present invention includes any novel features or combination of features disclosed herein. The applicant hereby gives notice that new claims may be formulated to such features or combination of features during prosecution of this application or of any such further applications derived therefrom. In particular, with reference to the appended claims, features from dependent claims may be combined with those of the independent claims and features from respective independent claims may be combined in any appropriate manner and not merely in the specific combinations enumerated in the claims.

Claims

1. A method of performing network handover between wireless local area network devices for a mobile device connected to a voice service via a secure data tunnel to a packet data gateway of a cellular network, comprising:

determining that a quality of a connection to a current wireless local area network is below a threshold value;

determining that a handover target network is available;

establishing connectivity with the target handover network;

suppressing a connection to a base station of the cellular network;

sending a new network address of the mobile device to the packet gateway using a set of credentials relating to the secure data tunnel so as to change an endpoint of the secure data tunnel to the new network address.

2. A method according to claim 1, wherein the secure data tunnel is an IPSec tunnel and an IP address is updated as the endpoint of the tunnel.

3. A method according to claim 1or 2, further comprising receiving confirmation from the packet gateway that the tunnel endpoint has been updated.

4. Apparatus for connecting to a voice service via a secure data tunnel to a packet data gateway of a cellular network and operable to perform network handover between wireless local area network devices via a secure data tunnel to a packet data gateway of a cellular network, comprising:

a cellular network interface;

a wireless local area network interface;

means for determining that a quality of a connection to a current wireless local area network is below a threshold value;

means for determining that a handover target network is available;

means for establishing connectivity with the target handover network;

means for suppressing a connection to a base station of the cellular network;

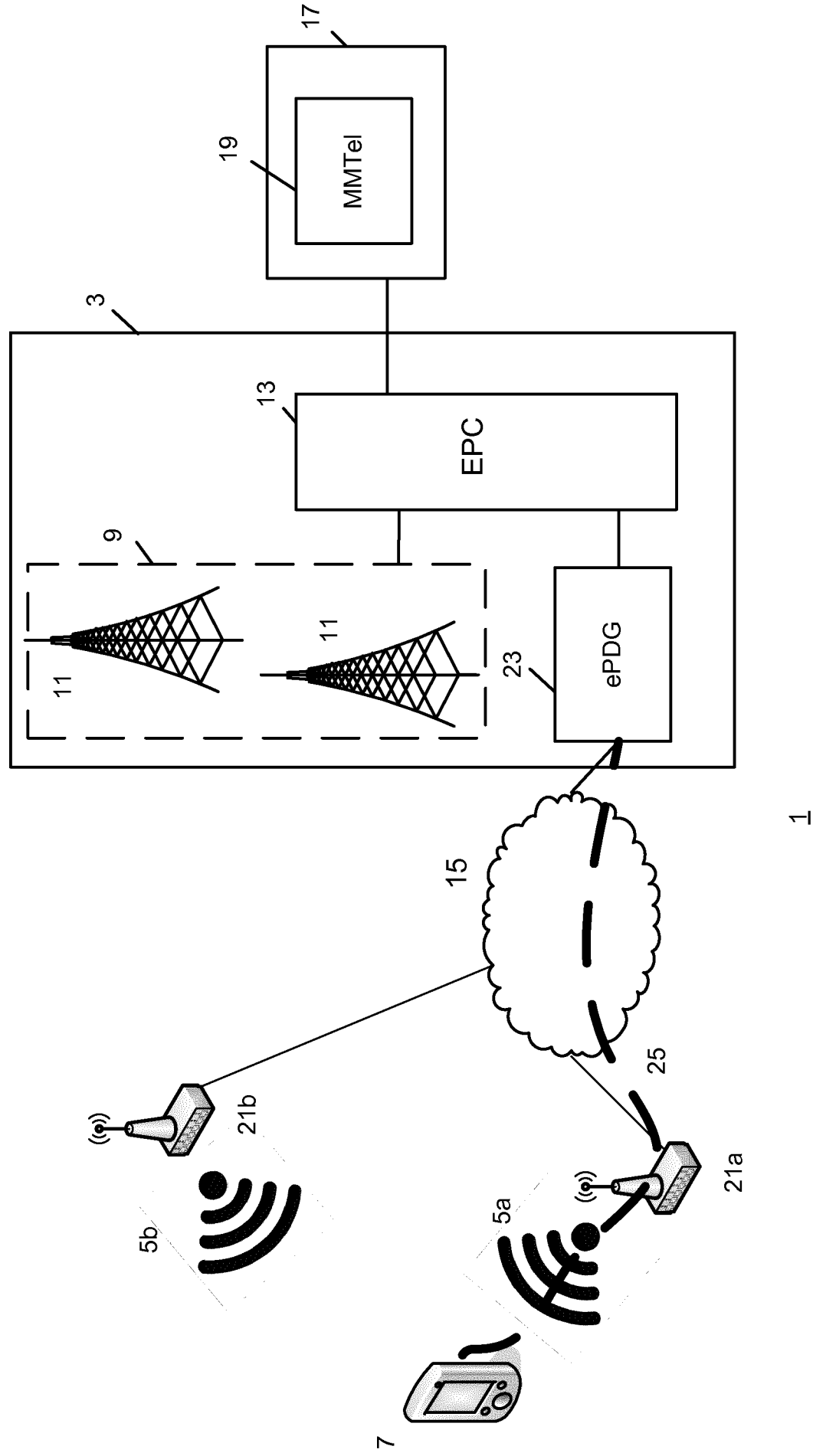
means for sending a new network address of the mobile device to the packet gateway using a set of credentials relating to the secure data tunnel so as to change an endpoint of the secure data tunnel to the new network address.

5. Apparatus according to claim 4, wherein the secure data tunnel is an IPSec tunnel and an IP address is updated as the endpoint of the tunnel.

6. Apparatus according to claim 4 or 5, further comprising receiving confirmation from the packet gateway that the tunnel endpoint has been updated.

7. A computer program product storing processor executable instructions for causing a programmable processor to carry out the method of claims 1 to 3.

Fig. 1



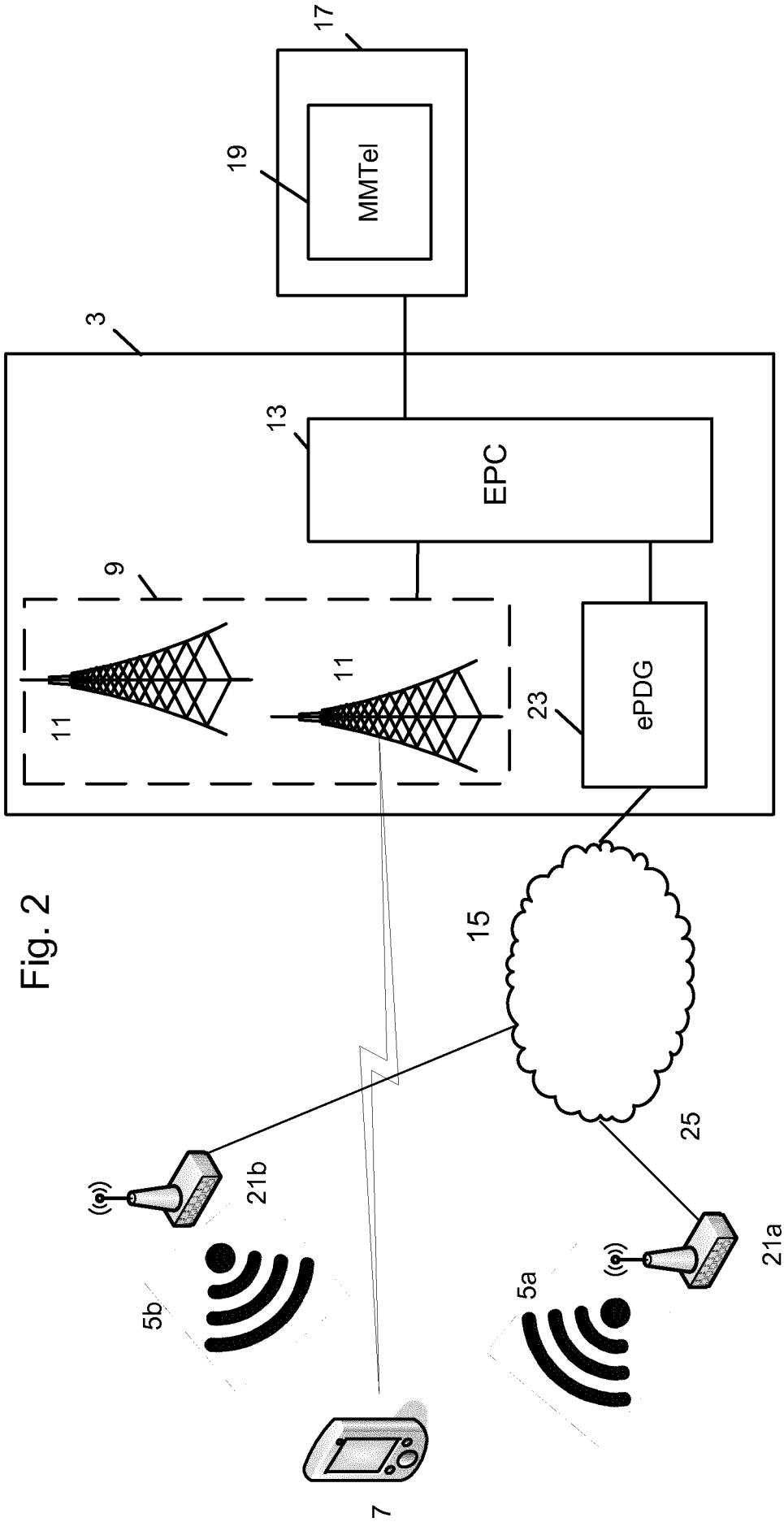


Fig. 2

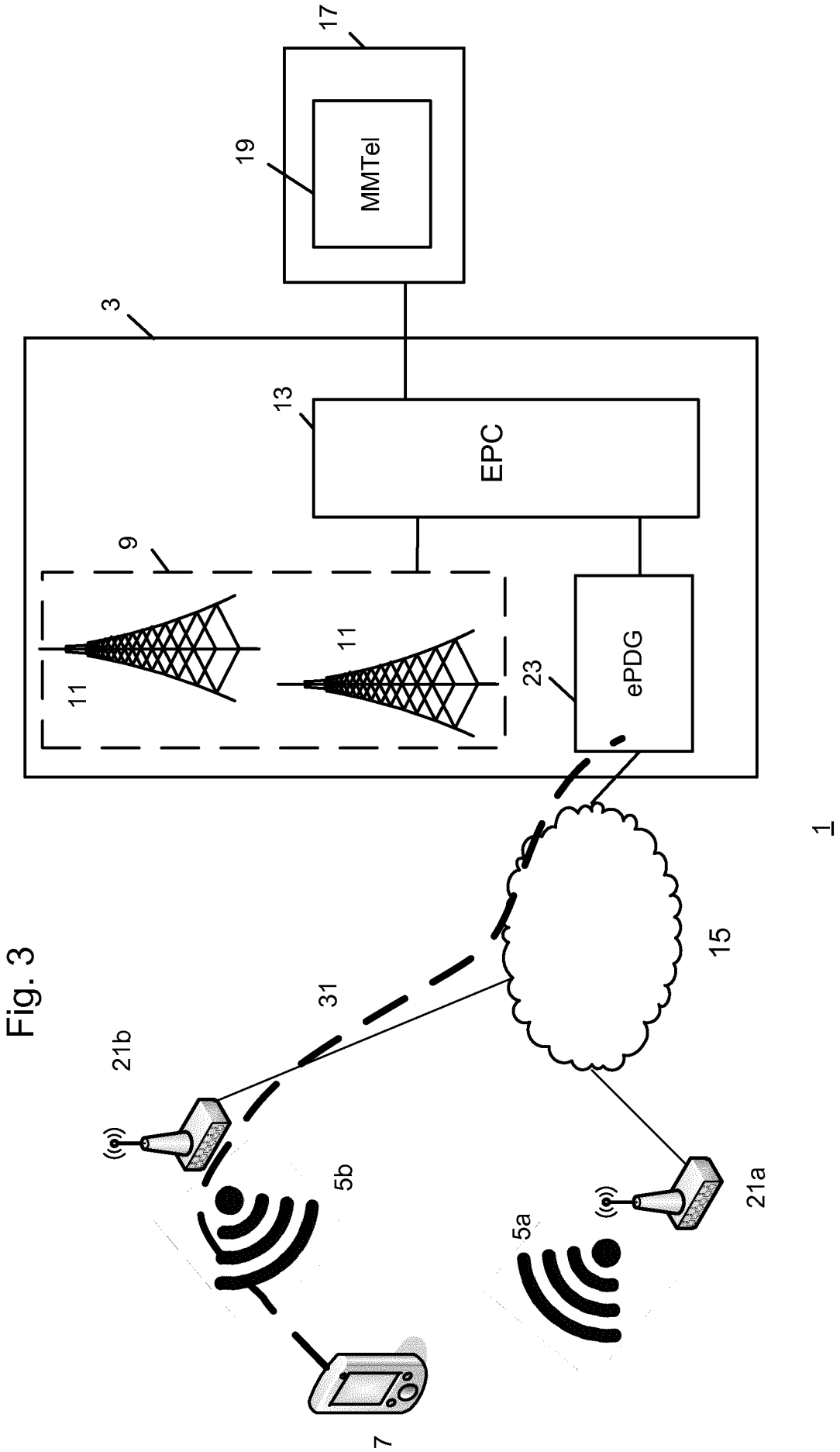


Fig. 3

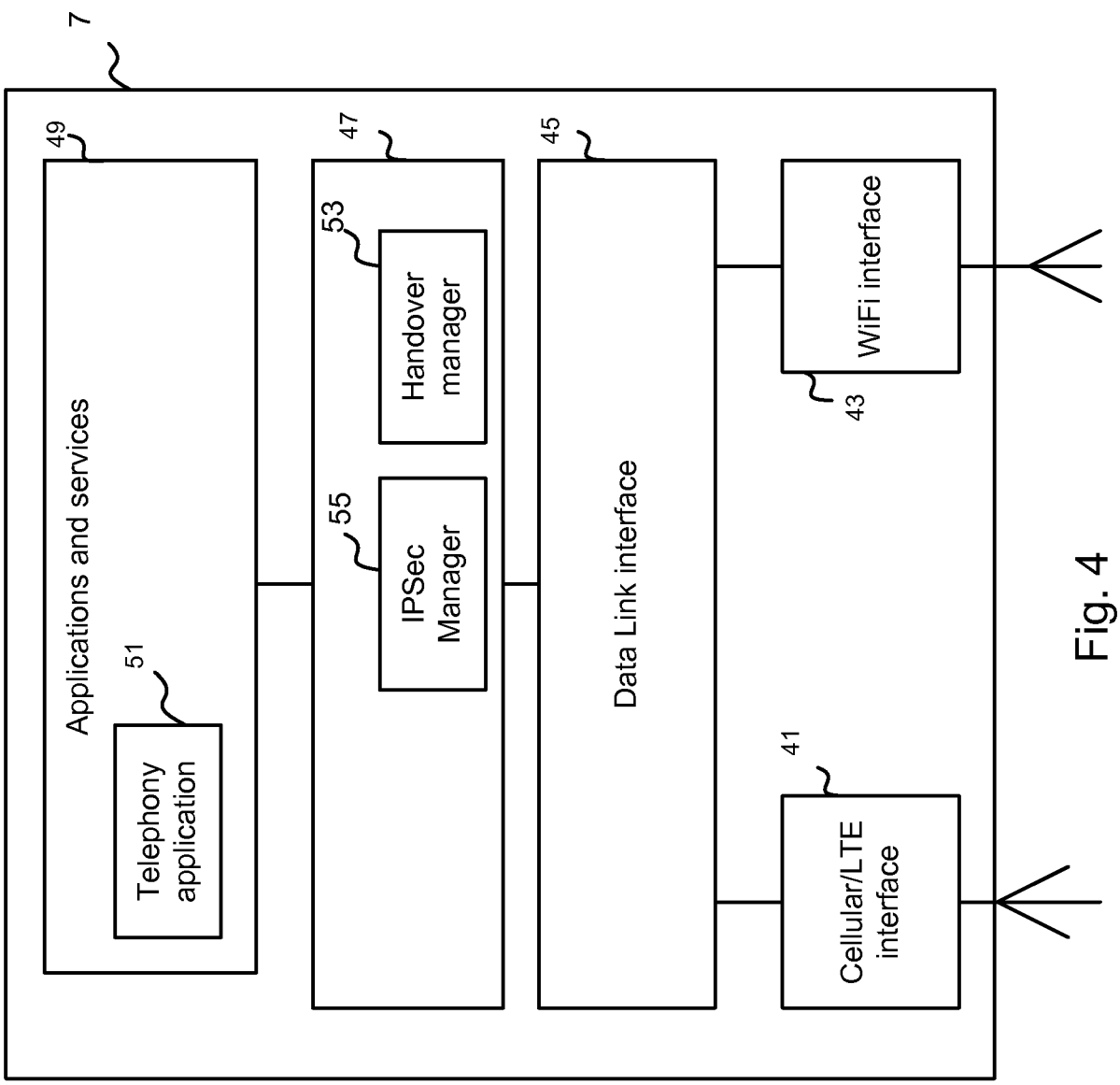

7
49
Applications and services
51
Telephony application
47
53
Handover manager
55
IPSec Manager
45
Data Link interface
43
WiFi interface
41
Cellular/LTE interface

Fig. 4

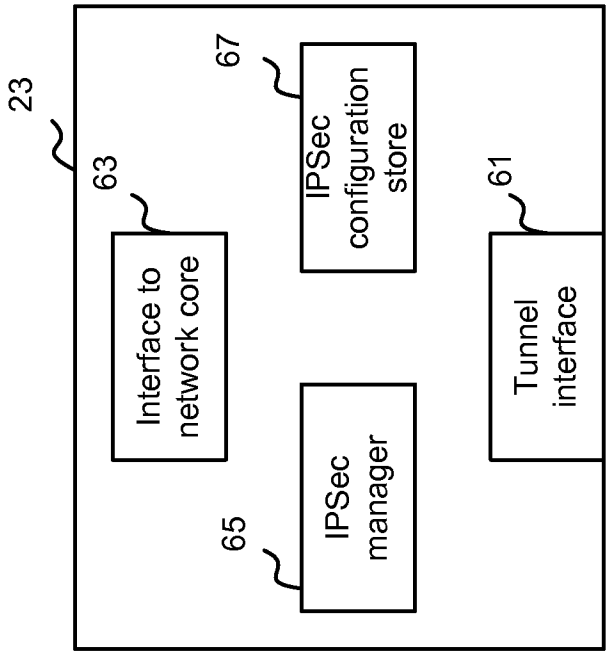

23
63
Interface to network core
67
IPSec configuration store
61
Tunnel interface
65
IPSec manager

Fig. 5

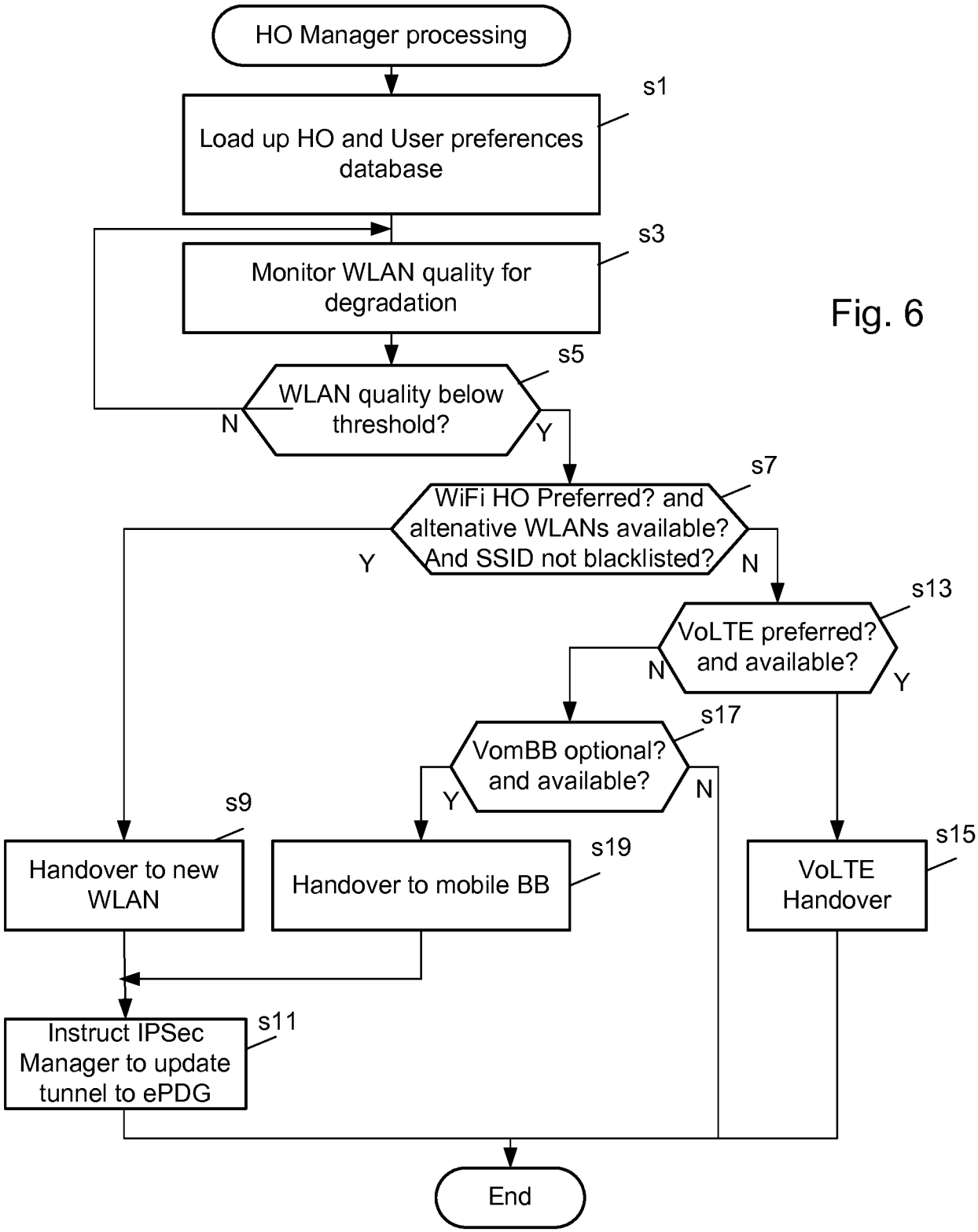

HO Manager processing
s1
Load up HO and User preferences database
s3
Monitor WLAN quality for degradation
s5
WLAN quality below threshold?
N
Y
s7
WiFi HO Preferred? and altenative WLANs available? And SSID not blacklisted?
Y
N
s13
VoLTE preferred? and available?
N
Y
s17
VomBB optional? and available?
Y
N
s9
Handover to new WLAN
s19
Handover to mobile BB
s15
VoLTE Handover
s11
Instruct IPSec Manager to update tunnel to ePDG
End

Fig. 6

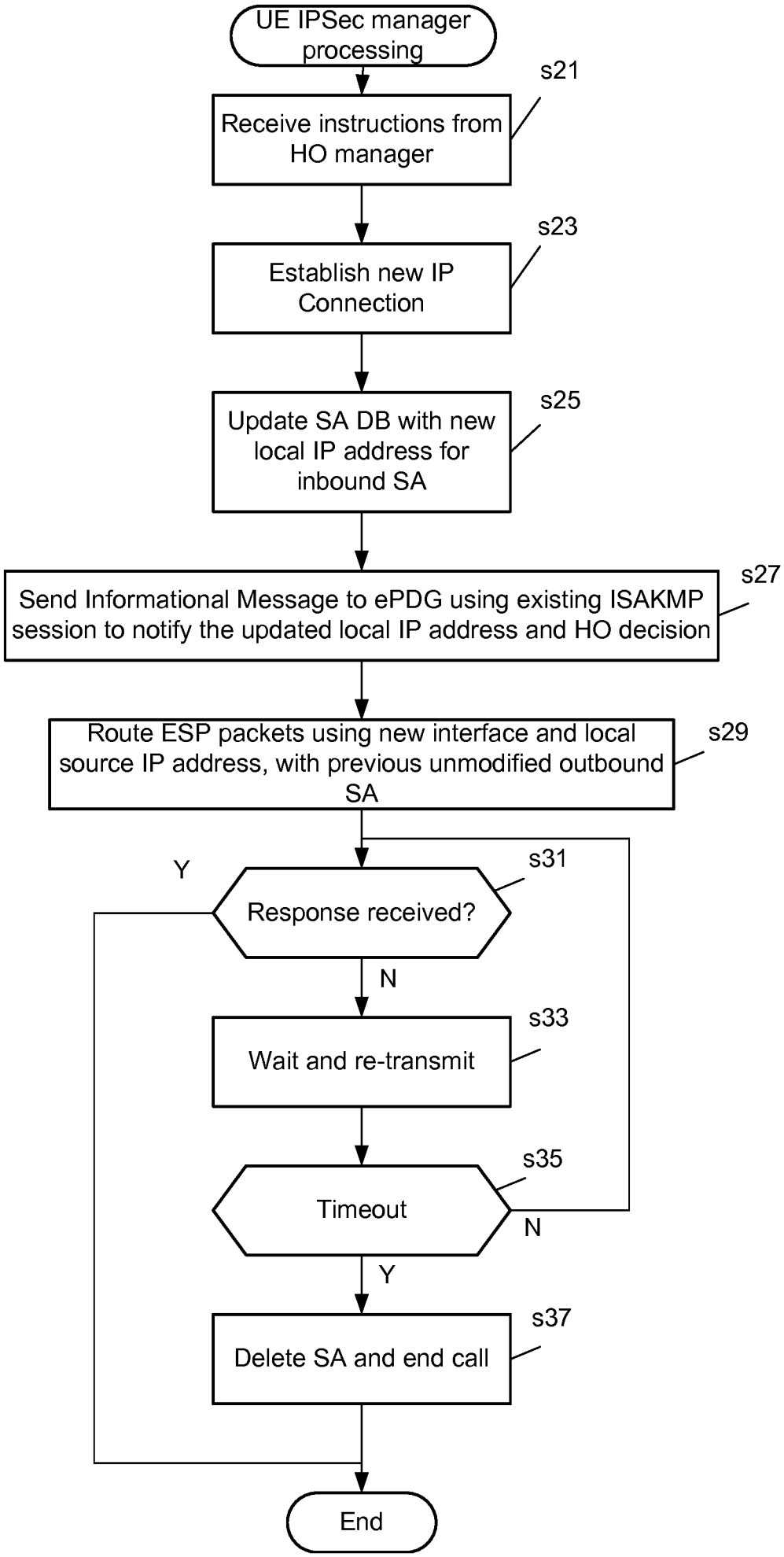

UE IPSec manager processing
s21
Receive instructions from HO manager
s23
Establish new IP Connection
s25
Update SA DB with new local IP address for inbound SA
s27
Send Informational Message to ePDG using existing ISAKMP session to notify the updated local IP address and HO decision
s29
Route ESP packets using new interface and local source IP address, with previous unmodified outbound SA
s31
Y
Response received?
N
s33
Wait and re-transmit
s35
Timeout
N
Y
s37
Delete SA and end call
End

Fig. 7

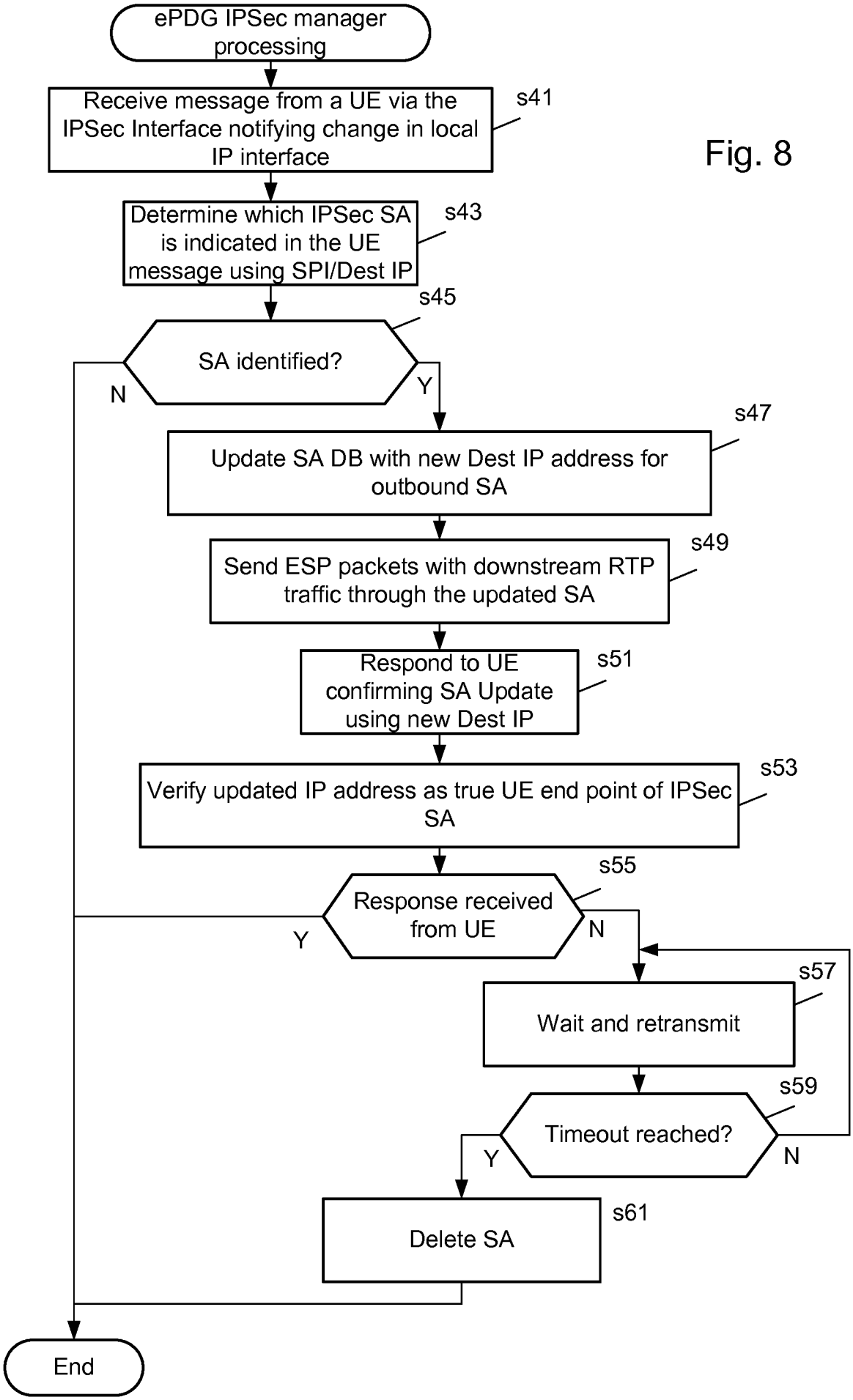

ePDG IPSec manager processing
Receive message from a UE via the IPSec Interface notifying change in local IP interface
s41
Determine which IPSec SA is indicated in the UE message using SPI/Dest IP
s43
s45
SA identified?
N
Y
s47
Update SA DB with new Dest IP address for outbound SA
s49
Send ESP packets with downstream RTP traffic through the updated SA
s51
Respond to UE confirming SA Update using new Dest IP
s53
Verify updated IP address as true UE end point of IPSec SA
s55
Response received from UE
Y
N
s57
Wait and retransmit
s59
Timeout reached?
Y
N
s61
Delete SA
End

Fig. 8

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/057225

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W36/00
ADD. H04W36/30 H04W36/36 H04W84/12 H04W76/04

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)
H04W

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)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 2011/002466 A1 (KWAK DONG-JIN [KR] ET AL) 6 January 2011 (2011-01-06) abstract paragraphs [0003], [0004], [0013] - [0020], [0038], [0040], [0060], [0064], [0068], [0094], [0128], [0129], [0142], [0143], [0166] figures 9,10 ----- -/--	1,2,4,5, 7 3,6

[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" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 May 2017	18/05/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Valpondi Hereza, F

1

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	C.Kaufman, P.Hoffman, Y.Nir, P.Eronen, T.Kivinen: "RFC 7296 - Internet Key Exchange Protocol Version 2 (IKEv2)", , 1 October 2014 (2014-10-01), XP055243756, Retrieved from the Internet: URL:http://tools.ietf.org/html/rfc7296#page-58 [retrieved on 2016-01-21]	3,6
A	section 1.4; page 17 - page 18	1,2,4,5, 7

A	P. Eronen: "RFC 4555 - IKEv2 Mobility and Multihoming Protocol (MOBIKE)", , 1 June 2006 (2006-06-01), XP055299729, Retrieved from the Internet: URL:https://tools.ietf.org/html/rfc4555 [retrieved on 2016-09-05] sections 1, 2, 3; page 3 - page 20	1-7

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2017/057225

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011002466 A1	06-01-2011	KR 20110003796 A	13-01-2011
		US 2011002466 A1	06-01-2011