(51) International Patent Classification:
H04W 4/10 (2009.01)  H04W 92/02 (2009.01)

(21) International Application Number:
PCT/US2016/016371

(22) International Filing Date:
3 February 2016 (03.02.2016)

(25) Filing Language:
English

(26) Publication Language:
English

(30) Priority Data:
62/1 11,561 3 February 2015 (03.02.2015) US
15/013,718 2 February 2016 (02.02.2016) US

(71) Applicant: KODIAK NETWORKS, INC. [US/US];
1501 10th Street, Suite 130, Piano, Texas 75074 (US).

(72) Inventors: PATEL, Krishnakan M.;

(74) Agent: VICE, Lizabeth; Slater & Matsil, LLP, 17950 Preston Rd., Suite 1000, Dallas, Texas 75252 (US).

(54) Title: SESSION MANAGEMENT AND NOTIFICATION MECHANISMS FOR PUSH-TO-TALK (PTT)

(57) Abstract: An embodiment method includes receiving, by a notification service running on a processor, a notification from a first component of a push-to-talk (PTT) platform. The notification is for transmission to a PTT client. The method further includes determining, by the notification service, an access transport type used by the PTT client to communicate with the PTT platform, and selecting, by the notification service, a second component to transmit the notification to the PTT client. Selecting the second component is in accordance with the access transport type used by the PTT client. The method further includes transmitting, by the notification service, the notification to the second component.
SESSION MANAGEMENT AND NOTIFICATION MECHANISMS FOR PUSH-TO-TALK (PTT)


This application also claims priority to U.S. Provisional Application No. 62/111,561 filed on February 3, 2015, entitled "Session Management and Notification Mechanisms for Next Generation Push-To-Talk-Over-Cellular (PoC) Service," which application is hereby incorporated herein by reference.

TECHNICAL FIELD

The present invention relates generally to communications over a telecommunications network, and in particular embodiments, to techniques and mechanisms for a system and method for elastic scaling in push-to-talk (PTT).

BACKGROUND

Push-to-talk (PTT) platforms involve providing PTT functionality (e.g., call group management, call origination, call transmittal, talk-back call termination, floor management, filtering, etc.) through clients on client devices. The PTT functions may be performed by one or more servers, and communications between the client devices and the servers may be performed over a telecommunications network (e.g., a carrier network in the case of PTT-Over-Cellular (PoC) or other types of networks). An aspect of PTT solutions is to provide robust client connectivity and notification mechanism(s).

SUMMARY OF THE INVENTION

Technical advantages are generally achieved, by embodiments of this disclosure which describe systems and methods for providing session management and notifications in a PTT environment.

In accordance with an embodiment, a method includes receiving, by a notification service running on a processor, a notification from a first component of a push-to-talk (PTT) platform. The notification is for transmission to a PTT client. The method further includes determining, by the notification service, an access transport type used by the PTT client to communicate with the PTT platform, and selecting, by the notification service, a second component to transmit the notification to the PTT client. Selecting the second component is in accordance with the access
transport type used by the PTT client. The method further includes transmitting, by the
notification service, the notification to the second component.

In accordance with an embodiment, a notification service includes one or more processors
and a computer readable storage medium storing programming for execution by the one or more
processors. The programming includes instructions to receive a notification from a first
component of a push-to-talk (PTT) platform. The notification is for transmission to a PTT client
on a client device. The programming includes further instructions to determine an access transport
type used by the PTT client to communicate with the PTT platform, select a second component to
transmit the notification to the PTT client, and transmit the notification to the second component.
The access transport type used by the PTT client is stored in a database, and selecting the second
component is in accordance with the access transport type used by the PTT client.

In accordance with an embodiment, a push-to-talk (PTT) platform includes a database,
one or more processors, and a computer readable storage medium storing programming for
execution by the one or more processors. The programming includes instructions to provide a
session initial proxy (SIP) registrar. The SIP registrar is configured to store an access transport
type of a PTT client in the database. The programming includes instructions to provide a PTT
application service to a PTT client on a client device and provide a notification service. The
notification service is configured to receive a notification from the PTT application service. The
notification is addressed to the PTT client. The notification service is further configured to
determine the access transport type of the PTT client, select a component to transmit the
notification to the PTT client, and transmit the notification to the component. Selecting the
component is in accordance with the access transport type of the PTT client.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention, and the advantages thereof,
reference is now made to the following descriptions taken in conjunction with the accompanying
drawings, in which:

FIG. 1 illustrates a diagram of an embodiment communications network according to
some embodiments;

FIGS. 2 through 6 illustrate block diagrams of various network interfaces between a PTT
platform and a PTT clients according to some embodiments;

FIG. 7 illustrates a block diagram of server components for session management and
notification in a PTT platform according to some embodiments;

FIGS. 8 through 11 illustrate block diagrams of notification mechanisms between a PTT
platform and PTT clients according to some embodiments;
FIGS. 12 through 16 illustrate block diagrams of session recovery and redundant notification mechanisms between a PTT platform and PTT clients according to some embodiments;

FIG. 17 illustrates a diagram of an embodiment processing system; and
FIG. 18 illustrates a diagram of an embodiment transceiver.

Corresponding numerals and symbols in the different figures generally refer to corresponding parts unless otherwise indicated. The figures are drawn to clearly illustrate the relevant aspects of the embodiments and are not necessarily drawn to scale.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

The making and using of embodiments of this disclosure are discussed in detail below. It should be appreciated, however, that the concepts disclosed herein can be embodied in a wide variety of specific contexts, and that the specific embodiments discussed herein are merely illustrative and do not serve to limit the scope of the claims. Further, it should be understood that various changes, substitutions and alterations can be made herein without departing from the spirit and scope of this disclosure as defined by the appended claims.

Various embodiments are described within a specific context, namely, session management and notification in a push-to-talk (PTT) system. Various embodiments may, however, be applied to other systems and networks, such as other telecommunications services platforms, where session management and notification services are desired.

Various embodiments as described below provide connectivity (e.g., session management) and notification mechanisms with reduced latency. Various embodiments may further provide carrier-grade reliability features, such as geographical level fault-tolerance for session management and/or notification.

Figure 1 illustrates a communications system 100, which provides an architecture for supporting a PTT communications solution in accordance with some embodiments.

Communications system 100 includes client devices 102, a communications network 104, and a PTT platform 106. As used herein, the term "client device" refers to any component (or collection of components) capable of establishing a connection with a communications network, such as a user equipment (UE), a mobile station (STA), a cellular phone, a tablet, a laptop, and other wired/wirelessly enabled devices. Applications (referred to hereinafter as "PTT clients") reside on client devices 102 for accessing various PTT functions.

Client devices 102 may communicate with PTT platform 106 over network 104, which may be accessed by client devices 102 through a cellular network deployed by a carrier, a WiFi network, a radio access network (RAN), other wireless networks, a wired internet protocol (IP) network, combinations thereof, or the like. Network 104 may include one or more components configured to provide wireless or wired network access, such as an enhanced base station (eNB),
a macro-cell, a femtocell, a Wi-Fi access point (AP), combinations thereof, or the like. Furthermore, network 104 may operate in accordance with one or more wireless communication protocols, e.g., open mobile alliance (OMA), long term evolution (LTE), LTE advanced (LTE-A), High Speed Packet Access (HSPA), Wi-Fi 802.11a/b/g/n/ac, etc. In some embodiments, network 104 may comprise various other devices, such as relays, low power nodes, etc. Network 104 may further include backhaul network components, such as various gateways, routers, controllers, schedulers, and the like.

In an embodiment where PTT platform 106 is a PTT-over-Cellular (PoC) platform, subscribers to a PTT solution (e.g., users operating client devices 102) may be provisioned onto system 100 via interfaces to carriers (e.g., cellular carriers). PTT customers (e.g., enterprises) can administer these subscribers to form closed groups for PTT communications. The PTT solution may interface with the carrier, for example, by including connectivity to the carrier’s core network, billing interfaces, provisioning interfaces, lawful intercept interfaces, customer care interfaces, and the like. PTT platform 106 may provide a plurality of PTT functions to client devices 102 through the PTT clients on client devices 102 as described in greater detail below.

In some embodiments, PTT platform 106 uses container technology for virtualization of a PTT system architecture, such as, the virtualization of provided PTT services. Example container technologies may include Docker, Rocket, LXD, and the like although the architecture is not limited to a specific container technology. Virtualization using container technology may allow PTT platform 106 to adopt a micro-services model in which service clusters are considered the building blocks of the system architecture. For example, each function provided by PTT platform 106 may be virtualized in a unique service cluster, and each service cluster may perform a different function in PTT platform 106. Service clusters are hosted on virtual machines of an embodiment cloud network. An embodiment cloud network may include a plurality of geographically diverse deployment sites (e.g., data centers) where various virtual machines are physically deployed. Decomposition of the system into a set of services allows each service (e.g., each function provided by the PTT platform) to be independently deployed and managed. Thus, system resilience may be improved as failures are localized to individual services. Furthermore, rapid and agile deployment of services may also be achieved.

In some embodiments, PTT platform 106 incorporates distributed databases, clustering technologies, data analytics tools, and messaging middleware to provide a robust, scalable platform. PTT platform 106 may use fully virtualized components with a layered approach to service orchestration, which allows PTT platform 106 to be integrated into various cloud environments, such as a carrier’s private cloud infrastructure, a dedicated PTT cloud infrastructure, combinations thereof, and the like. A more detailed description of an embodiment telecommunications platform may be found in commonly-assigned U.S. Patent Application No. 14/994,757 filed on January 13, 2016, entitled "System and Method for Elastic Scaling using a
Container-Based Platform,” which is hereby incorporated by reference. Other telecommunication services platforms, including other PTT platforms, may be used in other embodiments.

Various PTT clients on client devices 102 may use different access transport types to communicate with PTT platform 106. In an embodiment, PTT clients on client devices 102 connect to PTT platform 106 through an IP multimedia subsystem (IMS) core network, and various servers of PTT platform 106 are connected to the IMS core network.

In another embodiment, PTT clients on client devices 102 connect to PTT platform 106 through non-IMS IP networks, which may include trusted and/or un-trusted networks. In an embodiment, connection through a trusted network may include an operator providing a direct interface to the operator’s wireless data network (e.g., a LTE packet data network gateway (PGW)). In such embodiments, specific firewall rules may be provided to mark PTT server traffic of PTT platform 106 as trusted, which may relax one or more operator firewall rules and allow for simplified connectivity/notification mechanisms. In an embodiment, connection through an untrusted IP network (e.g., the internet) includes addressing additional security and firewall issues as explained in greater detail below. For both trusted and untrusted network connectivity, transport protocols (e.g., user datagram protocol (UDP), transmission control protocol (TCP), a combination thereof, or the like) are utilized to provide various notification channels for connection recovery methods as described in subsequent paragraphs.

In some embodiments, notification mechanisms (e.g., push notification mechanisms) are based on the access transport type, such as of transport protocol and/or the type of network connection (e.g., trusted or untrusted), used for connectivity between PTT clients on client devices 102 and PTT platform 106. Various notification mechanisms may include using a generic push notification service utilizing IMS registration, allowing in-network application servers and external application servers to push notifications to PTT clients, using operating system (OS) push notification services (e.g., Andriod or iOS push services), using WebSocket or other UDP-based session initiation protocol (SIP) registration with keep-alive functionality, combinations thereof, and the like.

In an embodiment, a generic push notification uses IMS registration procedures (e.g., SIP registration), which may not require maintaining redundant paths with application server(s) pushing the notification(s). In an embodiment, allowing in-network app servers and external app servers to push notifications to PTT clients may include a token based authentication scheme where a user (e.g., client device 102) provides an authentication token allowing application servers to push notifications to the user. In an embodiment, using OS push notification services may risk notifications being delivered to a specific device instead of a specific user. To address this risk, an IMS-based method can provide mechanism(s) to bind user identification (ID) with UE registration, which allows applications to deliver notifications to specific users instead of a device. For example when a user switches to a second device from a first device, the application
may deliver the notification to the second device based on the user ID (as identified by the service from device registration), rather than the first device. The user-based notification delivery mechanism may further be extended to non-IMS notification schemes as well in some embodiments. In an embodiment, non-IMS notification schemes (e.g., using WebSocket or UDP based SIP registration with keep-alive) may use redundant paths to maintain a constant connection between the PTT servers and a PTT client.

Embodiments may provide robust session management for PTT platform 106. An embodiment session management and notification mechanism may provide redundancies so that failure of one or more service components (e.g., failed container instances, failed service clusters, failed data centers, etc.) does not cause a service outage for PoC users. For example, various failover and reconnection mechanisms are may be handled seamlessly by PTT platform 106 for a user. Mechanisms for handling seamless failover/reconnection may include one or more of: a geographically redundant notification channel to recover from stale sessions, event driven recovery logic, session management and registrar load balancing, and redundancy logic as explained in greater detail below.

Furthermore, embodiments may use “home” sites for load balancing and reducing latency during a session. An embodiment session registration protocol includes PTT platform 106 receiving a session registration request (e.g., a SIP REGISTER request) from a PTT client. PTT platform 106 then selects a deployment site to serve the SIP REGISTER request. For example, PTT platform 106 may include a plurality of geographically diverse deployment sites for hosting various application servers (e.g., virtual servers encapsulated in containers and hosted on virtual machines at the deployment site). A SIP proxy server at one of the deployment sites may be selected to serve the SIP REGISTER request based on the PTT client’s geographic location (e.g., as determined by an IP address of the PTT client), a weighted round robin scheme, or the like.

Once a deployment site is selected for serving the SIP REGISTER request from the PTT client, the deployment site is considered the home site for the duration of the PTT client’s connection session. Various services used by the client are provided from the same home site. For example, the home site information may be returned as SIP path information in the REGISTER response to the PTT client, and the PTT client uses this SIP path information to direct all subsequent SIP service requests to the home site. Similarly, the PTT client is provided home site specific route information as part of a login session establishment procedure for other services.

Figure 2 illustrates a block diagram of an embodiment PTT platform 106 according to some embodiments. Specifically, Figure 2 illustrates interfaces between PTT platform 106 and various external networks. An IMS network 204 provides connectivity between PTT platform 106 and IMS-based PTT clients 202 in an operator’s network 206 (e.g., a carrier’s cellular network). As illustrated by Figure 2, PTT platform 106 may also maintain non-IMS interfaces for carrying out additional functions to complement IMS network 204 and provide a more comprehensive PTT
solutions. For example, PTT platform 106 may maintain internetworking with non-IMS LTE networks 208 to support non-IMS-based clients 216 (e.g., web browser based applications, third party client applications, non-IMS PTT clients, and the like), provide PTT service administration for corporations (e.g., corporate administrators 210) over the Internet, provide subscription life cycle management and monitoring over the Internet and/or a managed network to an operator’s information technology (IT) network 212, provide internetworking connections with land mobile radio (LMR) systems or other PTT systems through one or more gateways 214, and the like.

Table 1 below illustrates details regarding PTT client connectivity options in a first embodiment communications platform.

<table>
<thead>
<tr>
<th>PTT Client Type</th>
<th>Interface</th>
<th>Access Network</th>
<th>Transport Protocol</th>
<th>Network Address Translation (NAT) Timer Dependent?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Client</td>
<td>SIP –Primary Channel</td>
<td>LTE/4G, WiFi</td>
<td>TLS/TCP/IPV4</td>
<td>Auto-detected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LTE/4G</td>
<td>UDP/IPV6</td>
<td>No NAT</td>
</tr>
<tr>
<td>Media –Primary Channel</td>
<td>LTE/4G</td>
<td>RTP/RTCP over DTLS/UDP/IPV4</td>
<td>At least 30 minutes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WiFi</td>
<td>RTP/RTCP over UDP/IPV6</td>
<td>No NAT</td>
<td></td>
</tr>
<tr>
<td>Browser Client</td>
<td>SIP</td>
<td>WiFi/Internet</td>
<td>TLS/TCP</td>
<td>Auto-detected</td>
</tr>
<tr>
<td></td>
<td>RTP, RTCP</td>
<td>WiFi/Internet</td>
<td>WebRTC</td>
<td>Auto-detected</td>
</tr>
<tr>
<td></td>
<td>MBCP</td>
<td>WiFi/Internet</td>
<td>MBCP over SIP</td>
<td>Auto-detected</td>
</tr>
</tbody>
</table>

As another example, Table 2 below illustrates details regarding PTT client connectivity options in a second embodiment communications platform. In some embodiments, the second embodiment communications platform provides unification of transport protocols in a next generation architecture.

Table 2: PTT Client Connectivity Options in a Second Embodiment Communications Platform

<table>
<thead>
<tr>
<th>Client Type</th>
<th>Interface</th>
<th>Access Network</th>
<th>Transport Protocol</th>
<th>NAT Timer Dependent?</th>
</tr>
</thead>
</table>

-7-
Mobile SIP - Primary LTE/4G, TLS/TCP/IPV4 Taken care by Client/Channel over WiFi or IPV6 IMS

<table>
<thead>
<tr>
<th>Mobile Client/ Browser Client</th>
<th>SIP - Primary Channel over IMS(ISC)</th>
<th>LTE/4G, WiFi</th>
<th>TLS/TCP/IPV4 Or IPV6</th>
<th>Taken care by IMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary Notification Channel - WebSocket</td>
<td>LTE/4G, WiFi</td>
<td>WebSocket/TLS/TCP/IPV4 or IPV6</td>
<td>Yes, Auto-detected</td>
<td></td>
</tr>
<tr>
<td>Media - Primary Channel</td>
<td>LTE/4G</td>
<td>SRTP/SRTCP over UDP/IPV4 or IPV6</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>WiFi</td>
<td>RTP/RTCP over WebRTC (UDP or TLS)</td>
<td>Auto-detected</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A more detailed description of the types of connectivity interfaces listed in Tables 1 and 2 is provided with respect to Figures 3 through 6 below.

Figure 3 illustrates a more detailed diagram of network connections between PTT platform 106 and IMS network 204 to support IMS-based PTT clients 202. Throughout the description an IMS-based PTT client may be used to reference a PTT client communication with a PTT platform over an IMS network. In some embodiments, PTT platform 106 supports IMS-based PTT clients 202 by acting as an application server to IMS network 204 and using an IMS service control (ISC) interface 304 for connectivity. Various IMS-based clients (e.g., PTT clients 202) may interact with IMS core 204/operator network 206 for activation and provisioning of the IMS-based client.

In an embodiment, ISC interface 304 includes a subscriber content charging function (SCCF), and PTT platform 106 uses ISC interface 304 to connect with IMS-based PTT clients 202. ISC interface 304 may be a SIP interface in an embodiment. For example, PTT platform 106 may use ISC/SIP interface 304 over IMS network 204 for PTT signaling between PTT servers and PTT clients 202 to provide PTT call sessions (e.g., PoC call sessions as described Open Mobile Alliance Ltd., "OMA PoC Control Plane," OMA-TS-PoC_ControlPlane-V2_0-201 10802-A, 02 Aug 2011; Open Mobile Alliance Ltd., "OMA PoC Document Management," OMA-TS-PoC_Document_Management-V2_0-20110802-A, 02 Aug 2011; and Open Mobile Alliance Ltd., "PoC User Plane," OMA-TS-PoC_UserPlane-V2_0-20110802-A, 02 Aug 2011 (collectively hereinafter "OMA PoC 2.0")). PTT clients 202 may utilize pre-established PTT sessions or on-demand PTT sessions as appropriate for PTT call setup. PTT platform 106 may further use SIP/IP signaling for message exchange with presence servers and/or resource list servers (RLS) for presence information. Throughout the description the format protocol1/protocol2 may be used to designate protocol 1 over protocol2 signaling. For example, "SIP/IP" designates SIP over IP signaling. In an embodiment, PTT platform 106 supports TCP transport protocols, UDP transport protocols, or a combination thereof as an ISC interface between PTT client 202 and IMS core network 204.
As further illustrated by Figure 3, secure real-time transport protocol (SRTP)/IP, secure real-time control protocol (SRTCP)/IP, media burst control protocol (MBCP) over STCP/IP, or a combination thereof (illustrated in Figure 3 as interface 306) may be used for packets exchange between PTT platform 106 and session border controller (SBC) 302 of IMS network 204. In an embodiment, SBC 302 may be co-located with proxy-call session control function (P-CSCF) in operator network 206. SBC 302 may forward packets between media servers and PTT clients 202 for bearer traffic exchange of PTT call sessions. In an embodiment, the SRTP/SRTCP interface may utilize UDP as a transport protocol between PTT platform 106 and IMS network 204 although other transport protocols may be used as well.

PTT platform 106 may further include client data management interfaces 308. Client data management interfaces 308 may traverse over the Internet using extensible markup language (XML) configuration access protocol (XCAP)/hypertext transfer protocol (HTTP)/IP or representational state transfer (REST)/HTTP/IP interfaces between PTT platform 106 and PTT clients 202. These client data management interfaces 308 may allow for XCAP document management, affiliated groups information management, and the like. In some embodiments, client data management interfaces 308 are IMS independent interfaces, which may utilize HTTPS over TCP (TCP) transport protocols. Other transport protocols may be used as well in other embodiments.

As further illustrated by Figure 3, PTT platform 106 includes a receive (Rx) interface 310 with policy and changing rules function (PCRF) 302. Rx interface 310 may be used to support one or more of the following features: network based quality of service (QoS) support, dynamically assigning priority for users or groups of users, and the like. Rx interface 310 may use Diameter as a base protocol, which may be implemented over TCP transport protocols. Other transport protocols may be used as well.

Figure 4 illustrates a more detailed block diagram of IMS-based LTE interfaces and protocols between PTT platform 106 and an IMS-based PTT client 202. PTT platform 106 may include a plurality of servers, which may provide services to PTT client 202. In some embodiments, the servers are virtual service clusters encapsulated in containers and hosted on virtual machines of a cloud platform. PTT platform 106 may include a presence server 402, PTT call servers 404, media servers 406, extended markup language (XML) document manager (XDM) server 408, and SIP proxy/registrar servers 410. PTT platform 106 further includes border components, such as a SIP application level gateway (ALG) 412 and a media ALG 414. SIP ALG 412 may communicate with IMS network 204 over an ISC/SIP as described above, and media ALG 414 may communicate with IMS network 204 over SRTP/SRTCP interfaces as described above. SIP ALG 412 and media ALG 414 may be components of a SBC of PTT platform 106. Although Figure 4 illustrates a particular combination of servers and gateways, and embodiment
PTT platform may include any combination of the illustrated servers and/or gateways as well as other servers and/or gateways.

Figure 4 further illustrates various interfaces between IMS-based PTT client 202 and IMS network 204. These interfaces may include SIP interface 416, SRTP/SRTCP interface 418, XCAP interface 420, and IMS provisioning interface 422, and these interfaces may be connected to IMS network 204 over the Internet and a wireless network 424. In some embodiments, wireless network 424 may include a cellular network (e.g., LTE/4G), a WiFi network, or the like. PTT client 202 may utilize SIP interface 416 to communicate with PTT platform 106 through IMS network 204 for PTT, presence, and other SIP signaling. In an embodiment, SIP interface 416 uses a TLS (e.g., TCP) transport protocol. However, an operator’s actual transport interface (e.g., UDP or TCP) is selected based on a configuration (e.g., a supported transport interface) of IMS network 204, and SIP interface 416 may be adapted according to the configuration of IMS network 204. Application signaling (e.g., by servers in PTT platform 106) may be in accordance with one or more standards, such as, OMA PoC (e.g., OMA PoC 2.0), presence (e.g., as described in Open Mobile Alliance Ltd., "Presence SIMPLE Specification,” OMA-TS-Presence_SIMPLE-V2_0-20120710-A, 10 Jul 2012; Open Mobile Alliance Ltd., "Resource List Server (RLS) Specification,” OMA-TS-Presence_SIMPLE_RLS-V1_0-20120710-A, 10 Jul 2012; Open Mobile Alliance Ltd., "Presence XDM Specification,” OMA-TS-Presence_SIMPLE_XDM-V2_0-20120710-A, 10 Jul 2012; Open Mobile Alliance Ltd., "Resource List Server (RLS) XDM Specification,” OMA-TS-Presence_SIMPLE_RLS_XDM-V2_0-201207 10-A, 10 Jul 2012 (collectively hereinafter "OMA Presence 2.0")), and XDM standards (e.g., as described in Open Mobile Alliance Ltd., "XML Document Management (XDM) Specification," OMA-TS-XDM_Core-V2_0-20120403-A, 03 Apr 2012; Open Mobile Alliance Ltd., "Shared List XDM Specification,” OMA-TS-XDM_Shared_List-V2_0-20120403-A, 03 Apr 2012; Open Mobile Alliance Ltd., "Shared Group XDM Specification,” OMA-TS-XDM_Shared_Group-V1_0-20120403-A, 03 Apr 2012 (collectively hereinafter "OMA XDM 2.0").

PTT client 202 may further use SRTP/SRTCP interface 418, as provided by PTT server 404 (e.g., a media server 406 of PTT call server 404) for carrying voice data. SRTP/SRTCP interface 418 may use UDP as a transport protocol, and may be forwarded without modification, by SBC 302, between PTT client 202 and PTT call server 404. In an embodiment, IMS network 204 may support web real-time communications (WebRTC) to transport SRTP/SRTCP packets over non-LTE networks (e.g., WiFi networks). In an embodiment based on the OMA PoC 2.0 standard, the floor control messages are carried over floor control-specific RTCP App messages, referred to as a media burst control protocol (MBCP). RTCP App messages may also be used for implementing predictive wakeup functions in PTT platform 106 (e.g., as described in U.S. Patent No. 8,478,261, entitled "Predictive Wakeup for Push-To-Talk-Over-Cellular (PoC) Call Setup Optimizations,” patented July 2, 2013, which application is hereby incorporated by reference).
PTT client 202 may use XCAP interface 420 for XDM operations including document retrieval, contact management, group management, and the like. XCAP interface 420 may be provided by XDM Server 408. In an embodiment, XCAP interface 420 supports OMA XDM XCAP standards based requests and responses as defined in OMA XDM 2.0. Legacy PTT clients may use HTTP transport protocol for XCAP operations, and newer PTT clients may use HTTP or HTTPS transport protocols as desired based on a desired security.

PTT client 202 may further use an IMS provisioning interface 422 for provisioning messages with IMS network 204. IMS provisioning interface may be a custom, operator specific interface. For example, HTTPS transport protocol may be used by some operators. IMS provision interface 422 may be used to activate and provision PTT client 202.

Figure 5 illustrates various interfaces between PTT platform 106 and network components to support non-IMS clients 216. Such interfaces may include a SGi interface 502, an Rx interface 504, a short message peer-to-peer (SMPP) interface 506, and an IP interface 508. For example, SGi is a reference point between a packet data network (PDN) gateway and the PDN itself. The PDN may be an operator external public/private PDN, an intra-operator PDN (e.g., for provision of IMS services), or a combination thereof. Furthermore, SGi may correspond to Gi for 3GPP accesses. In an embodiment, PTT platform 106 may support TLS (TCP) transport protocols for communication between PTT clients 216 and PTT servers of PTT platform 106.

In some embodiments, SGi interface 502 includes a packet data network gateway (PGW)/gateway general packet radio service (GPRS) support node (GGSN) to transfer IP packets between non-IMS PTT clients 216 and servers of PTT platform 106. The types of traffic carried over SGi interface 502 may include PTT signaling between a PTT call server of PTT platform 106 and PTT clients 216 for PTT call sessions as described in the OMA PoC 2.0 standards. PTT clients 216 may utilize pre-established PTT sessions or on-demand PTT session as desired for PTT call set up. The types of traffic carried over SGi interface 502 may further include SIP/IP signaling messages between presence/RLS servers of PTT platform 106 and PTT client 216 for presence information. The types of traffic carried over SGi interface 502 may further include SRTP/IP, SRTCP/IP and MBCP over STCP/IP packets exchange with a SBC of PTT platform 106. The SBC of PTT platform 106 may forward the packets between media servers of PTT platform 106 and PTT client 216 for bearer traffic exchange for PTT call sessions. Furthermore, SGi interface 502 may utilize WebRTC as a transport protocol between PTT platform 106 and PTT client 216 over a wireless network (e.g., an LTE network). WebRTC standards allow utilization of various types of transport protocols to traverse through client side access network and firewall/NATs. Special or improved QoS can be applied to the traffic flowing through SGi interface 502 for PTT clients 216 over a LTE network. Other transport protocols may be used in other embodiments.
In some embodiments Rx interface 504 includes PCRF to support one or more of the following features: network based QoS support, dynamically assignment of priority for a set of users, dynamically assignment of priority for a user group. Rx interface 504 may use Diameter as a base protocol, which implemented over TCP transport protocol. Other transport protocols may be used in other embodiments.

In some embodiments, IP interface 506 may handle miscellaneous traffic between PTT client 216 and PTT platform 106 that does not traverse over SGi interface 502. For example, some traffic may not require LTE QoS, and such traffic may be handled over IP interface 506. Both IPV4 and IPV6 transport protocols may be supported by IP interface 506. Other transport protocols may be used in other embodiments.

PTT platform 106 may further maintain an SMPP interface 508 with an operator's short message server center (SMSC)/SMPP gateway. SMPP interface 508 may be provided by an XDM server of PTT platform 106 to receive activation command SMS's sent by the PTT clients 216 through a SMSC/SMPP gateway of an operator or a third Party SMPP provider who interworks with the operator. SMPP interface 508 may use SMPP v3.4. Other transport protocols may be used in other embodiments. Activation commands received over SMPP interface 508 may include a unique user ID generated by each PTT client 216, which is used for verifying the identity of a subscriber whose account is being activated.

Figure 6 illustrates a more detailed block diagram of non-IMS-based LTE interfaces and protocols between PTT platform 106 and non-IMS-based PTT clients 216. PTT platform 106 may include a plurality of servers, such as those described above with respect to Figure 4. As further illustrated by Figure 6, PTT platform 106 may include a WebSocket gateway 602 and an HTTP load balancer (LB) 604 for interfacing with non-IMS-based clients 216 (e.g., mobile clients 216a and browser/third party clients 216b). WebSocket gateway 602 provides transport level functionality to receive WebSocket connections from PTT clients using WebSocket as transport for SIP signaling or notification services. WebSocket gateway 602 forwards SIP packets to SIP Proxy.

Clients 216 may use SIP interface 606 to communicate with PTT platform 106 for PTT call, presence, and other SIP signaling. SIP interface 606 may use TLS (e.g., TCP) transport protocols for mobile clients 216a, and SIP interface 606 may use WebSocket over TLS transport protocols for browser/third party clients 216b. Application signaling for PTT platform 106 may be in accordance with OMA PoC, Presence, and XDM standards as defined in OMA PoC 2.0, OMA Presence 2.0 and OMA XDM 2.0.

PTT clients 216 may further use SRTP/SRTCP interface 608, as provided by PTT call server 404 (e.g., a media server 406 of PTT call server 404) for carrying voice data. SRTP/SRTCP interface 418 may use UDP as a transport protocol for voice data, and data may be forwarded without modification, by a SBC (e.g., SBC 620), between PTT clients 216 and PTT

-12-
call server 404. In an embodiment, WebRTC may be used to transport SRTP/SRTCP packets over different types of networks (including non-LTE networks, such as, WiFi networks). By using WebRTC, SRTP/SRTCP packets may be transmitted regardless of the access transport type used by PTT clients 216 to access PTT platform 106. In an embodiment based on the OMA PoC 2.0 standard, the floor control messages are carried over special RTCP App messages, referred to as MBCP. RTCP App messages may also be used for implementing predictive wakeup functions in PTT platform 106 (e.g., as described in U.S. Patent No. 8,478,261). Other transport protocols may be used in other embodiments.

PTT clients 216 may use XCAP interface 610 for XDM operations including document retrieval, contact management, group management, and the like. XCAP interface 610 may be provided by XDM Server 408. In an embodiment, XCAP interface 610 supports OMA XDM XCAP standards based requests and responses as defined in OMA XDM 2.0. Legacy PTT clients may use HTTP transport protocol for XCAP operations, and newer PTT clients may use HTTP or HTTPS transport protocols depending on a desired security level. Other transport protocols may be used in other embodiments.

Furthermore, third party APIs may be used to provide interfaces to allow control room/third party applications to easily access PTT platform 106. Benefits of using third party APIs may include client data management interfaces for XCAP/HTTP/IP or REST/HTTP/IP interfaces between PTT platform 106 and PTT clients 216. These client data management interfaces may allow for XCAP document management, affiliated groups information management, and the like. In some embodiments, client data management interfaces are IMS independent interfaces, which may utilize HTTPS over TLS (TCP) transport protocols. Other transport protocols may be used in other embodiments.

As further illustrated by Figure 6, a secondary notification interface 612 may be used to provide alternate means of reaching PTT clients 216 under error or server fault conditions. This interface enables full geographical redundancy with carrier grade service availability to users of PTT platform 106. Secondary notification interface 612 may utilize WebSocket over TLS (TCP) as a transport protocol. Other transport protocols may be used in other embodiments for secondary notification interface 612.

In various embodiments, session information is provided to service clusters of PTT platform 106 in order to support sessions in a load balanced architecture model (e.g., a container-based platform described above). Various sessions may be transparent within a local region (e.g., contained to a single deployment site) and/or span across multiple geographically, device deployment sites. Deployment site may refer to data centers having host processors for hosting a virtual machines on which PTT platform 106 is deployed.

Some embodiment sessions are transparent only within a local region, such as within a datacenter, (referred to as sessions with intra-site scope). Sessions with intra-site scope may
include transport level sessions, which cannot be easily ported across different sites. Interruptions to sessions with intra-site scope may require re-establishment of such sessions. Examples of sessions with intra-site scope include UDP sessions (e.g., used for media or SIP sessions), TCP sessions (e.g., used for SIP or WebSocket sessions), and the like. In some circumstances, sessions with intra-site scope cannot be ported from a physical server node on which the session has been established to a different server node within the same deployment site. For example, when a transport session utilizes a federal information processing standards (FIPS) mode of encryption, stringent key generation and management functions under FIPS encryption may not allow porting of sessions across different physical nodes.

A complete deployment site failure (e.g., datacenter failure) may result in the loss of transport level sessions, so an alternate mechanism to reach and notify PTT clients when such errors occur is desired for sessions with intra-site scope. When transport level session continuity is handled by intermediate network infrastructure, additional alternate notification mechanisms are not necessary. For example, in IMS-based architectures, transport level session management for SIP related sessions are handled by the IMS network by itself, and no additional notification mechanisms are required.

Regarding sessions that are transparent across different deployment sites (referred to as sessions with inter-site scope), various application layer sessions can be made available across geographical boundaries of different deployment sites using databases (e.g., distributed databases), for example. Thus, a geographical diverse, highly available PTT platform may be provided with increased redundancy and reduced service interruption to PTT users. Examples of sessions with inter-site scope include: client initiated presence SUBSCRIBE sessions, client initiated XDM SUBSCRIBE sessions, and the like.

Table 3 below provides example session recovery methods for different types of sessions established with different types of PTT clients according to some embodiments. Session recovery may include recovering a primary connection using a notification sent over a secondary connection as described below.

**Table 3: Session Recovery Methods for Different Types of PTT Sessions**

<table>
<thead>
<tr>
<th>Client Type</th>
<th>Access Network</th>
<th>Session Purpose</th>
<th>Scope</th>
<th>Session Loss Impact(s)</th>
<th>Session Recovery Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile IMS Clients</td>
<td>All types of Access Networks</td>
<td>SIP INVITE Pre-arranged PoC Session</td>
<td>In-site Service Cluster</td>
<td>In-time Pre-arranged PTT session over IMS or on-demand PTT session over IMS</td>
<td>Handled by IMS, no additional methods necessary</td>
</tr>
<tr>
<td>Mobile Non-IMS Clients</td>
<td>IPV6 LTE Networks</td>
<td>SIP REGISTER over UDP</td>
<td>Client is Online and reachable</td>
<td>Multisite Service Cluster (Assuming UDP is unsolicited)</td>
<td>In-time Pre-arranged PTT session over IMS or on-demand PTT session over unsolicited UDP</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------</td>
<td>-----------------------</td>
<td>--------------------------------</td>
<td>---------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>WiFi or non-IPV6 LTE Networks</td>
<td>SIP REGISTER over WebSocket/TLS</td>
<td>Client is online and reachable</td>
<td>In-site Service Cluster (Assuming TLS connections can be mirrored within site)</td>
<td>Notification or PoC Call cannot be reached.</td>
<td>Use of secondary notification method. For example, use a lightweight notification mechanism (e.g., messaging queue (MQ), telemetry transport (MQTT), or SIP). As another example, use Open OS notification mechanisms (e.g., Android, iOS).</td>
</tr>
<tr>
<td>Third Party Clients or Web-Browser based Clients</td>
<td>Any type of access Network</td>
<td>SIP REGISTER over WebSocket/TLS</td>
<td>Client is online and reachable</td>
<td>In-site Service Cluster (Assuming TLS connections can be mirrored within site)</td>
<td>Notification or PoC Call can’t be reached.</td>
</tr>
</tbody>
</table>

As indicated by Table 3 above, IMS networks may handle session recovery notification for mobile IMS-based clients without an additional secondary notification mechanism. However, additional secondary notification mechanisms may still be included in some embodiments if desired. As further indicated by Table 3 above, UDP handles session recovery for mobile non-IMS clients using an unsolicited UDP transport protocol and no additional secondary notification mechanisms are necessary. For example, a notification path can be recovered using IPv6 unsolicited path.

However, as further indicated above, PTT clients (e.g., non-IMS-based clients or third party clients) connecting using SIP REGISTER sessions over WebSocket/TLS use one or more
secondary notification methods to help recover a primary connection. For example, a lightweight notification mechanism (e.g., MQTT) or SIP may be used. As another example, Open OS notification mechanisms (e.g., Android, iOS) may be used as a secondary notification mechanism for such clients.

Figure 7 illustrates various components in PTT platform 106 for providing a session management and notification service. As illustrated by Figure 7, PTT platform 106 includes SIP ALGs 412, WebSocket gateways 602, SIP proxies/SIP registrars 410, notification services 702, third party notification service(s) 708, and databases 706. In an embodiment, databases 706 may be one or more distributed databases although other types of storage mechanisms may be used as well in other embodiments. Components of the session management and notification service (e.g., SIP proxy/SIP registrar 410, notification service 702, and database 706) may be deployed at a first deployment site 710 and at a second geographically different deployment site 710. Deployment sites 710 and 712 may further include various applications 704 to provide services for users of PTT platform 106. A PTT client 714 (e.g., an IMS-based client or a non-IMS-based client) may maintain a primary notification channel connection with deployment site 710. PTT client 714 may optionally maintain a secondary notification channel with secondary deployment site 704, for example, in accordance with a connection type between PTT client 714 and PTT platform 106 as described in Table 3 above.

SIP ALG 412 provides SIP aware transport level functionality, which accepts UDP or TCP sessions from PTT client 714 directly or IMS core networks. SIP ALG may then forward the UDP/TCP sessions to SIP proxy 410 at a respective deployment site 710/712.

WebSocket gateway 602 provides transport level functionality to receive WebSocket connections when PTT client 714 uses WebSocket as a transport protocol for SIP signaling or notification service. WebSocket gateway 602 may forward SIP packets to SIP proxy 410 at a respective deployment site 710/712.

SIP proxy 410 provides a single point of contact at a deployment site 710/712 for SIP signaling from PTT client 714. SIP proxy 410 aggregates PTT client 714 destined SIP traffic from various SIP servers (e.g., a PTT call server, presence servers, and the like) over a TCP/UDP session. SIP proxy 410 may further distribute PTT client 714 originated SIP traffic to appropriate SIP servers (e.g., a PTT call server, presence servers, and the like). In some embodiments SIP proxy 410 may provide load balancing functionality by load balancing SIP traffic to different SIP server instances.

SIP registrar 410 authenticates PTT subscribers over an SIP interface. SIP registrar 410 authenticates PTT client 714 prior to accepting a registration request. After PTT client 714 is successfully registered, SIP registrar 410 stores the SIP registration information along with access transport type used for the SIP Session in a database 706 of a respective deployment site 710/712.
SIP registrar 410 may also send third party SIP registration requests to other services that depend on registration (e.g., presence/RLS services).

In some situations (e.g., for non-IMS-based clients), SIP registrar 410 may also authenticate PTT client. For example, PTT client 714 may create and transmit a SIP REGISTER request to SIP proxy/SIP registrar 410 for SIP and PTT registration. SIP registrar 410 may respond with a SIP digest challenge to PTT client 714 in a SIP “401 Unauthorized” response. PTT client 714 may then create an appropriate SIP challenge response, which may be included in a SIP REGISTER request sent to SIP registrar 410 by PTT client 714. SIP registrar 410 verifies the response. If the response is valid, SIP registrar 410 accepts the registration. If the response is not valid (e.g., authentication failure), SIP registrar 410 rejects the registration and sends a SIP "403 Forbidden" response to PTT client 714. PTT client 714 and SIP registrar 410 may use a username and password exchanged at the time of client activation for SIP digest authentication.

In another embodiment (e.g., for IMS-based clients), SIP authentication is handled by an IMS core network (e.g., IMS core 204, see Figure 3). In such embodiments, SIP registrar 410 functions as a registration information repository. For example, SIP registrar may receive third Party REGISTRATION transmissions from the IMS network and track registration status of various users (e.g., the online status of different users). SIP registrar 410 may store registration information (e.g., client type/access transport type/user IDs) of various PTT clients in database 706.

Notification service 702 may be available for various application services 704 such as presence, messaging, PTT calling services, and the like. Notification service 702 may be implemented in a dedicated server, such as a virtual server (e.g., encapsulated in a container and hosted on virtual machine running on a physical processor of a cloud platform), or the like. Notification service 702 may be used to decouple notification delivery as an independent service, which is deployed independently of various other services in PTT platform 106 (e.g., application servers, SIP proxy, SIP registrar, and the like). Thus, mechanisms to choose a correct transport type for notifications and fallback mechanisms can be implemented.

Notification service may use session information stored in databases 706 to select an appropriate transport protocol for delivering notifications to PTT client 714. In some embodiments databases may be synchronized across different deployment sites so notification services at each deployment site may have access to PTT client information of inter-site sessions. In some embodiments, notification service may select a transport type for delivering notifications in accordance with a client type/ access transport type of PTT client 714. For example, IMS-based PTT clients may have a primary notification mechanism of SIP over IMS with no separate secondary notification mechanism; LTE based clients that utilize IP firewalls allowing unsolicited traffic may have a primary notification mechanism of SIP over a UDP session with not separate secondary notification mechanism; and all other types of clients may have SIP over a primary
WebSocket session as a primary notification mechanism and a secondary SIP over a secondary WebSocket session as a secondary notification mechanism. Other secondary notification mechanisms may include a redundant SIP session established over WebSocket, TLS, TCP, UDP, or the like, a third party notification mechanism (e.g., Mobile OS notification mechanisms), a MQTT session, or a combination thereof as described in greater detail below. In such embodiments, the secondary notification session (e.g., secondary SIP over secondary WebSocket) may be used to notify PTT client 714 when the primary transport level session is not reachable (e.g., as a result of network, infrastructure, and/or server cluster failure(s)). Notification service 702 may optionally utilize third party notification services (e.g., notification services unrelated to the PTT platform) such as native notification mechanisms provided by Android or iOS; native SMS as a notification mechanism; or the like as a secondary or tertiary notification service. In other embodiments, notifications service 702 may select other notification mechanisms for the listed client types/ access transport types and/or other client types/ access transport types.

Table 4 below provides a description of some internal and external interfaces of a PTT call service according to an embodiment as illustrated by Figure 7. An embodiment PTT call service may include any combination of the described interfaces as well as other interfaces.

<table>
<thead>
<tr>
<th><strong>Table 4: Interfaces of a PTT Call Service</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface</strong></td>
</tr>
<tr>
<td>E1. Primary Notification Channel</td>
</tr>
<tr>
<td>E2. Secondary Notification Channel</td>
</tr>
<tr>
<td>E3. SIP Interface</td>
</tr>
<tr>
<td>I1. SIP REGISTER Interface</td>
</tr>
<tr>
<td>I2. SIP Notifications</td>
</tr>
<tr>
<td>I3. Third Party Notifications</td>
</tr>
<tr>
<td>I4. Notifications</td>
</tr>
</tbody>
</table>
Figure 8 illustrates a service flow of session management in an embodiment PTT platform 106 for an IMS-based PTT client 202. In step 804, the IMS-based client 202 registers with IMS network 204 (e.g., by transmitting a SIP registration). Because IMS network 204 is separate from PTT platform 106, the SIP registration may be referred to as a third party SIP registration.

In step 806, IMS core network 204 forwards the third party SIP registration to PTT platform 106. For example, the third party SIP registration may be sent to PTT platform 106 over a standard IP multimedia service control (ISC) interface. When PTT platform 106 is deployed in a multi-site configuration (e.g., having multiple deployment sites), IMS core network 204 may use a load balancing policy, such as a geo-proximity policy to select an appropriate deployment site 710/712 to send the third party SIP registration. An embodiment geo-proximity policy selects a deployment site closest to PTT client (e.g., as determined by an IP address of the PTT client and as determined by a domain name search (DNS) on services of PTT platform 106). In such embodiments, a geo-proximity policy benefits PTT platform 106 as subscribers from a particular location will be load balanced to a same deployment site 702/704, which may allow re-use of cache data stored in nodes of PTT platform 106. In an embodiment, PTT platform 106 load balances the SIP registration to an available SIP registrar within a deployment site 710/712.

In step 808, the SIP registrar stores the third party SIP registration information in database 706, which registers PTT client 202. For example, the SIP register may store an access transport type of PTT client 202 in database 706. Registering PTT client 202 may result in indicating the subscriber is ONLINE and available to receive PoC application services.

When an application service needs to deliver a message, such as a text or presence update, to a registered IMS-based PTT client 202 the following process may be employed. In step 810, an application service initiates a message delivery request to a notification service. In step 812, the notification service looks up PTT client 202 in database 706 and determines the type of notification mechanism to be used, for example, based on a client type/access transport type of the PTT client 202. For example, Figure 8 describes a notification process for IMS-based PTT client 202. Because PTT client 202 is IMS-based, the notification service may select any SIP proxy to send the notification. In such embodiments, notification service may transmit the notification to a local SIP proxy cluster to be transmitted to the PTT client in step 814. In step 816, the SIP proxy delivers the notification over IMS network 204 to PTT client 202. In step 818, IMS network 204 delivers the SIP message/notification to PTT Client 202. Although Figure 8 illustrates two application services simultaneously sending notifications to PTT client 202, notifications may or may not be transmitted by application services at different deployment sites at any given time.

Figure 9 illustrates a service flow of session management in an embodiment PTT platform 106 for a PTT client 216 that utilizes an unsolicited IP network connection to connect with PTT platform 106. In some embodiments, PTT client 216 may be LTE based and/or use an
IPV6 unsolicited UDP transport protocol. An unsolicited UDP transport protocol may be used to refer to an embodiment transport protocol where an operator network’s firewall 920 is configured to allow unsolicited traffic. For example, firewall 920 may allow traffic from a server to a mobile device (e.g., a mobile device running PTT client 216) without requiring the mobile device to initiate an IP connection with the server. In some embodiments, an unsolicited IP network typically uses a network configuration (e.g., as provided by a network operator) that is specific to IP address ranges of PTT servers to access PTT platform 106. This network configuration allows application services from any data center (e.g., deployments sites 710/712) to transmit IP/UDP packets to PTT client 216.

Session management for PTT client 216 may be provided as follows. In step 902, PTT client 216 registers with PTT platform 106, for example, by transmitting an SIP registration request. In an embodiment, PTT platform 106 load balances the SIP registration to an available SIP registrar at a deployment site 710/712. In step 904, the SIP registrar authenticates PTT client 216. Once authenticated, the SIP registrar stores the SIP registration information of PTT client 216 in database 706, which registers PTT client 216. Registering PTT client 216 may result in indicating the subscriber is ONLINE and available to receive PoC application services.

When an application service needs to deliver a message, such as a text or presence update, to a registered PTT client 216 the following process may be employed. In step 910, an application service initiates a message delivery request to a notification service. In step 912, the notification service looks up PTT client 216 in database and determines the type of notification mechanism to be used, for example, based on a client type/access transport type of PTT client 216. For example, Figure 9 describes a notification process for PTT client 216, which uses an unsolicited IP network to access PTT platform 106. Because PTT client 216 is using an unsolicited IP network, the notification service may select any SIP proxy to send the notification.

In such embodiments, notification service may transmit the notification to a local SIP proxy cluster for transmission to the PTT client in step 914. In step 916, the SIP proxy delivers the notification over the unsolicited IP network using an IPV6 UDP transport protocol.

Figure 10 illustrates a service flow of session management in an embodiment PTT platform 106 for a PTT client 1000 that utilizes any other type of network connection (e.g., other than an IMS-based or unsolicited IP network connection) to connect with PTT platform 106. For example, the operator’s network firewall 1002 may allow a server to transmit messages to PTT client 1000 only if PTT client 1000 has initiated and kept an active transport session (e.g., UDP or TCP) with the specific server. Furthermore, PTT client 1000 may be a web browser based PTT client, a third party PTT client (e.g., a client provided by third party independent from a provider of PTT platform 106), a non-IMS client or the like. Because of the configuration of firewall 1002 (e.g., unsolicited traffic is not allowed), only the border nodes that received the client transport
sessions can only terminate IP packets to PTT client 1000, and not all servers (e.g., not all SIP proxies) in PTT platform 106 can directly transmit IP packets to PTT client 1000.

Session management for PTT client 1000 may be provided as follows. In step 1004, PTT client 216 registers with PTT platform 106, for example, by establishing a WebSocket connection with a WebSocket gateway. In an embodiment, PTT platform 106 transmits a WebSocket request, and PTT platform 106 load balances the WebSocket request to an available WebSocket gateway at a first deployment site 710. PTT client 1000 initiates an SIP REGISTER session over WebSocket. In step 1006, WebSocket gateway forwards the SIP REGISTER request to a local SIP at the first deployment site 710. In step 1008, SIP registrar authenticates PTT client 216.

Once authenticated, the SIP registrar store the SIP registration information of PTT client 216 in database 706, and SIP registrar may further store information identifying the particular WebSocket gateway cluster that received the client connection in database 706.

In steps 1010-1014, PTT client 1000 may further establish a secondary notification channel (sometimes referred to as a redundant notification channel) by establishing another WebSocket connection and a secondary SIP registration session at a second deployment site 712. Establishing the secondary notification channel may be done using a similar procedure as the primary notification channel described in steps 1004 to 1008 above. PTT client 1000 may implement logic to ensure primary and secondary WebSocket connections are not established at the same data centers. For example, PTT client 1000 may transmit a location of the primary WebSocket connection with the second WebSocket registration request to PTT platform 106. PTT client 1000 may further transmit an indication the registration request is a secondary WebSocket registration request to PTT platform 106. In another embodiment, the location of the primary WebSocket connection may be stored in database 706. When PTT platform 106 receives the second WebSocket registration request with the location of the primary connection, PTT platform 106 load balances the second WebSocket connection to a WebSocket gateway at a different deployment site than the primary WebSocket connection. The secondary notification channel may be used to recover a session when a connection with the primary notification channel fails. The SIP registrar may further store information identifying the WebSocket gateway maintaining the secondary notification channel in database 706.

When an application service needs to deliver a message, such as a text or presence update, to a registered PTT client 1000 the following process may be employed. In step 1020, an application service initiates a message delivery request to a notification service. In step 1022, the notification service looks up PTT client 216 in database and determines the type of notification mechanism to be used, for example, based on a client type/access transport type of PTT client 1000. For example, Figure 10 describes a notification process for PTT client 1000 using a network connection that is not IMS-based and does not allow unsolicited traffic. Because PTT client 1000 is using this type of connection, the notification service instructs the SIP proxy to
utilize a specific WebSocket gateway maintaining a primary connection with PTT client 1000 to send the notification. For example, in Figure 10, the application service originating the notification is located in a same deployment site 710 as the WebSocket gateway with which PTT client 1000 maintains a primary connection. Thus, in step 1024, the notification service instructs the SIP proxy to forward the notification to the WebSocket gateway in deployment site 710. In step 1026, the WebSocket gateway then forwards the notification over the established WebSocket transport session with PTT client 1000.

Figure 11 illustrates another example where the application service originating the notification is a different deployment site 712 as deployment site 710 where the WebSocket gateway maintaining a connection with PTT client 1000 is located. In step 1102, the notification service instructs the SIP proxy in deployment site 712 to forward the notification to the WebSocket gateway in deployment site 710. In step 1104, the WebSocket gateway in deployment site 710 then forwards the notification over the established WebSocket session with PTT client 1000.

In various embodiments, most in-site node failure (e.g., failure of a container in a service cluster) does not impact the application server (e.g., the virtual application server encapsulated in containers of a service cluster). An embodiment PTT platform may include built-in fault recovery mechanisms. For example, transport level sessions may be made highly available within deployment site using real-time session replication for each service cluster in PTT platform 106 for failed containers. Thus, the loss of a container may not impact PTT clients connected to the PTT platform. However, security protocols may provide exceptions where real-time replication is disallowed. For example, FIPS transport sessions may provide such an exception. In these situations, it may be desirable to deliberately re-establish sessions even when a specific transport session node fails.

Figure 12 illustrates recovery mechanisms for IMS-based clients 202 and/or PTT clients 216 connecting to the PTT platform using an unsolicited IP network connection. Recovery mechanisms may be initiated when a deployment site (e.g., deployment site 710) maintaining a primary connection with the PTT client 202/216 fails. When PTT clients 202/216 are utilizing an IMS access network or an unsolicited IP network, failure of a deployment site may not impact session mobility as any deployment site can communicate with the PTT client 202/216.

Session recovery may begin in step 1202 when an application service at an online site (e.g., deployment site 712) initiates a message delivery request to a notification service. In step 1204, the notification service looks up PTT client 202/216 in database 706 to determine the type of notification mechanism to be used, for example, based on a client type/access transport type of PTT client 202/216. Because PTT client 202/216 is using an IMS network or an unsolicited IP network, the notification service may select any SIP proxy to send the notification to PTT client 202/216. In such embodiments, notification service may transmit the notification to a local SIP
proxy cluster for transmission to PTT client 202/216 in step 1206. In step 1208, the SIP proxy delivers the notification over the IMS network or the unsolicited IP network using an IPv6 UDP transport protocol as described above, and the IMS network/unsolicited IP network delivers the notification to PTT client 202/206 in step 1210.

Figure 13 illustrates recovery mechanisms for PTT clients 1000, which do not use an IMS-based or unsolicited IP network connection to communicate with PTT platform 106. Recovery mechanisms may be initiated when a deployment site (e.g., deployment site 710) maintaining a primary connection with the PTT client 1000 fails. For example, PTT client 1000 may be using a network connection where unsolicited traffic is not allowed, and PTT client 1000 may use WebSocket to communicate with the PTT platform as described above. Because the network connection does not allow unsolicited traffic, any notification to PTT client 1000 needs to follow an established transport session path. Thus, transport level sessions (e.g., TCP, TLS, or WebSocket sessions) cannot be recovered by another deployment site (e.g., deployment site 712) seamlessly. In such embodiments, the notification service uses the secondary notification channel to reach PTT client 1000 and delivery notifications when deployment site 710 fails. The notification service may inform PTT client 1000 its primary notification channel has been disrupted and request PTT client 1000 to re-establish a primary notification channel with PTT platform 106.

Figure 13 illustrates a flow for delivering a message to PTT client 1000, which maintains a primary notification channel with a WebSocket gateway of a failed deployment site 710. In step 1302, an application service at an active deployment site 712 initiates a message delivery request to a notification service. In step 1304, the notification service looks up PTT client 1000 in database 706 to determine the type of notification mechanism to be used, for example, based on a client type/access transport type of PTT client 1000 and where the primary notification channel with PTT client 1000 is located. In Figure 13, the notification service determines the WebSocket gateway maintaining a primary notification channel with PTT client 1000 is not reachable because deployment site 710 has failed. Thus, the notification service instructs the SIP proxy to utilize a secondary notification service to deliver the notification, and the SIP proxy transmits the notification using the secondary notification channel’s WebSocket gateway in step 1308. In step 1310, the SIP proxy transmits the notification over the secondary notification channel to PTT client 1000.

An indication of primary channel unavailability may also be provided in the notification to trigger PTT client 1000 to re-establish its primary session. As further illustrated by Figure 13, PTT client 1000 may re-establish its primary WebSocket session based on the indication of primary channel unavailability in steps 1312, 1314, and 1316. Re-establishing the primary notification channel may follow a similar procedure as described above with respect to steps 1004, 1006, and 1008 in Figure 10. The primary notification channel re-establishment request
may be load balanced by PTT platform 106 to an available data center (e.g., deployment site 1320) and registration may be processed as described above.

Figure 13 illustrates a target application server (e.g., server attempting to communicate with PTT client 1000) and the WebSocket gateway having a secondary notification channel as being co-located in a same deployment site 712. In another embodiment, session recovery may be performed using a redundant notification service at a third party deployment site as illustrated by Figures 14 and 15. In Figures 14 and 15, PTT client 1000 may not use an IMS-based connection or a connection that allows unsolicited IP traffic to communicate with PTT platform 106. In other embodiments, an IMS-based PTT client or a client communicating with PTT platform 106 with an unsolicited IP connection may maintain a secondary notification channel in an independent data center for improved resiliency. The redundant notification channel provided by the independent data center may be in lieu of or in addition to a secondary notification channel using a WebSocket gateway as described above. In such embodiments, a redundant notification mechanism is provided by a server that is deployed in separate data center than where a target application service is deployed. For example, in Figure 14, a redundant notification mechanism is provided by a MQTT broker cluster deployed at a third party data center 1402 deployed by a different service provider (e.g., Amazon Web ServicesTM (AWS), and the like) than a provider of PTT platform 106. Thus, failure of any data center in PTT platform 106 does not affect the redundant notification path through the third party deployment site, and system resiliency may be increased to handle any number of simultaneous data center failures in which target applications are deployed.

As illustrated by Figure 14, PTT client 1000 may register and maintain a primary notification channel with a deployment site 710 of PTT platform 106 (e.g., as described above with respect to Figure 10). PTT client 1000 may also maintain a secondary notification channel with a server 1404 (e.g., a MQTT broker cluster) at third party data center 1402. Server 1404 may have no relationship with services provided by PTT platform 106. In some embodiments, the secondary notification channel may use MQTT as a transport protocol for the redundant notification. Other types of session protocols (e.g., protocols using SIP) may be used in other embodiments, for example, based on the configuration of the third party deployment site.

Figure 15 illustrates a flow diagram for delivering a message to PTT client 1000, which maintains a primary notification channel with a WebSocket gateway of a failed deployment site 710. In step 1502, an application service at an active deployment site 712 initiates a message delivery request to a notification service. In step 1504, the notification service looks up PTT client 1000 in database 706 to determine the type of notification mechanism to be used, for example, based on a client type/access transport type of PTT client 1000. The notification service may further use database 706 to determine locations (e.g., WebSocket gateway instances) of a primary secondary notification channel between PTT client 1000 and PTT platform 106. In Figure 15, the
notification service determines the WebSocket gateway maintaining a primary notification channel with PTT client 1000 is not reachable. Thus, the notification service uses a secondary notification service to deliver the notification. The notification service may determine the location/type of secondary notification service from database 706. In step 1506, the notification service forwards the notification to the third party server 1404, which maintains a secondary notification channel with PTT client 1000. In step 1508, third party server 1404 sends the notification to PTT client 1000. An indication of primary channel unavailability may also be provided in the notification to trigger PTT client 1000 to re-establish its primary session.

Figures 14 and 15 illustrate redundant notification channel provided a third party notification mechanism provided by a server at a third party deployment site. In another embodiment, the redundant notification may be provided by a third party notification mechanism provided by a generic, mobile open operating system (OS) platform-specific notification service 1602, such as Apple Notification Service, Google Notification Service, or the like as illustrated by Figure 16. In Figure 16, PTT client 1000 does not use an IMS-based connection or a connection that allows unsolicited IP traffic to communicate with PTT platform 106. In other embodiments, an IMS-based PTT client or a client communicating with PTT platform 106 with an unsolicited IP connection may maintain a secondary notification channel using a third party notification mechanism for improved resiliency. The third party notification mechanism may be in lieu of or in addition to a secondary notification channel using a redundant notification mechanism as described above. Because the notification service is provided by a third party (e.g., independent from PTT platform 106), the third party notification service may be running in a separate data center than deployment sites running various services provided by PTT platform 106. The redundant notification path may be used when a primary notification path with PTT client 1000 is not available or failed. Transmitting a notification to PTT client 1000 when a primary notification channel fails may be similar to that described above with respect to Figures 13 and 15 using a third party notification mechanism, such as, a mobile OS platform-specific notification service 1602. An indication of primary channel unavailability may also be provided in the notification to trigger PTT client 1000 to re-establish its primary session.

FIG. 17 illustrates a block diagram of an embodiment processing system 1700 for performing methods described herein, which may be installed in a host device. As shown, the processing system 1700 includes a processor 1704, a memory 1706, and interfaces 1710-1714, which may (or may not) be arranged as shown in FIG. 17. The processor 1704 may be any component or collection of components adapted to perform computations and/or other processing related tasks, and the memory 1706 may be any component or collection of components adapted to store programming and/or instructions for execution by the processor 1704. In an embodiment, the memory 1706 includes a non-transitory computer-readable medium. The interfaces 1710, 1712, 1714 may be any component or collection of components that allow the processing system
1700 to communicate with other devices/components and/or a user. For example, one or more of
the interfaces 1710, 1712, 1714 may be adapted to communicate data, control, or management
messages from the processor 1704 to applications installed on the host device and/or a remote
device. As another example, one or more of the interfaces 1710, 1712, 1714 may be adapted to
allow a user or user device (e.g., personal computer (PC), etc.) to interact/communicate with the
processing system 1700. The processing system 1700 may include additional components not
depicted in FIG. 17, such as long term storage (e.g., non-volatile memory, etc.).

In some embodiments, the processing system 1700 is included in a network device that is
accessing, or part otherwise of, a telecommunications network. In one example, the processing
system 1700 is in a network-side device in a wireless or wireline telecommunications network,
such as a base station, a relay station, a scheduler, a controller, a gateway, a router, an
applications server, or any other device in the telecommunications network. In other
embodiments, the processing system 1700 is in a user-side device accessing a wireless or wireline
telecommunications network, such as a mobile station, a user equipment (UE), a personal
computer (PC), a tablet, a wearable communications device (e.g., a smartwatch, etc.), or any other
device adapted to access a telecommunications network.

In some embodiments, one or more of the interfaces 1710, 1712, 1714 connects the
processing system 1700 to a transceiver adapted to transmit and receive signaling over the
telecommunications network. FIG. 18 illustrates a block diagram of a transceiver 1800 adapted to
transmit and receive signaling over a telecommunications network. The transceiver 1800 may be
installed in a host device. As shown, the transceiver 1800 comprises a network-side interface
1802, a coupler 1804, a transmitter 1806, a receiver 1808, a signal processor 1810, and a device-
side interface 1812. The network-side interface 1802 may include any component or collection of
components adapted to transmit or receive signaling over a wireless or wireline
telecommunications network. The coupler 1804 may include any component or collection of
components adapted to facilitate bi-directional communication over the network-side interface
1802. The transmitter 1806 may include any component or collection of components (e.g., up-
converter, power amplifier, etc.) adapted to convert a baseband signal into a modulated carrier
signal suitable for transmission over the network-side interface 1802. The receiver 1808 may
include any component or collection of components (e.g., down-converter, low noise amplifier,
etc.) adapted to convert a carrier signal received over the network-side interface 1802 into a
baseband signal. The signal processor 1810 may include any component or collection of
components adapted to convert a baseband signal into a data signal suitable for communication
over the device-side interface(s) 1812, or vice-versa. The device-side interface(s) 1812 may
include any component or collection of components adapted to communicate data-signals
between the signal processor 1810 and components within the host device (e.g., the processing
system 1700, local area network (LAN) ports, etc.).
The transceiver 1800 may transmit and receive signaling over any type of communications medium. In some embodiments, the transceiver 1800 transmits and receives signaling over a wireless medium. For example, the transceiver 1800 may be a wireless transceiver adapted to communicate in accordance with a wireless telecommunications protocol, such as a cellular protocol (e.g., long-term evolution (LTE), etc.), a wireless local area network (WLAN) protocol (e.g., Wi-Fi, etc.), or any other type of wireless protocol (e.g., Bluetooth, near field communication (NFC), etc.). In such embodiments, the network-side interface 1802 comprises one or more antenna/radiating elements. For example, the network-side interface 1802 may include a single antenna, multiple separate antennas, or a multi-antenna array configured for multi-layer communication, e.g., single input multiple output (SIMO), multiple input single output (MISO), multiple input multiple output (MIMO), etc. In other embodiments, the transceiver 1200 transmits and receives signaling over a wireline medium, e.g., twisted-pair cable, coaxial cable, optical fiber, etc. Specific processing systems and/or transceivers may utilize all of the components shown, or only a subset of the components, and levels of integration may vary from device to device.

In accordance with an embodiment, a method includes receiving, by a notification service running on a processor, a notification from a first component of a push-to-talk (PTT) platform. The notification is for transmission to a PTT client. The method further includes determining, by the notification service, an access transport type used by the PTT client to communicate with the PTT platform, and selecting, by the notification service, a second component to transmit the notification to the PTT client. Selecting the second component is in accordance with the access transport type used by the PTT client. The method further includes transmitting, by the notification service, the notification to the second component. Determining the access transport type of the PTT client includes looking up the PTT client in a database.

The embodiment method further includes storing, by a session initiation protocol (SIP) registrar running on a processor, the access transport type of the PTT client in the database when the PTT client registers with the PTT platform.

In an embodiment method, the access transport type used by the PTT client is an internet protocol (IP) multimedia subsystem (IMS) network, and selecting the second component includes selecting a session initiation protocol (SIP) proxy at a same deployment site as the first component to transmit the notification to the PTT client over the IMS network.

In an embodiment method, the access transport type used by the PTT client is an unsolicited internet protocol (IP) network connection, and wherein selecting the second component includes selecting a session initiation protocol (SIP) proxy at a same deployment site as the first component to transmit the notification to the PTT client using a user datagram (UDP) transport protocol.
In an embodiment method, the access transport type used by the PTT client is not over an IMS network, and the access transport type used by the PTT client does not allow unsolicited internet protocol (IP) traffic. In this embodiment, selecting the second component includes selecting a first gateway maintaining a first notification channel with the PTT client to transmit the notification to the PTT client. In an embodiment method, the first gateway is located at a same deployment site of the PTT platform or a different deployment site of the PTT platform as the first component. In an embodiment method, a primary notification channel between the PTT client and a second gateway of the PTT platform is unreachable, and the first notification channel is a redundant notification channel between the PTT client and the first gateway. The embodiment method further includes including an indication the primary notification channel is unreachable in the notification. In an embodiment method, the first gateway is deployed as part of the PTT platform, and the first gateway is located at a different deployment site of the PTT platform than the second gateway. In an embodiment method, the first gateway is deployed at a third party deployment site independent from the PTT platform. An embodiment method further includes transmitting the notification to the PTT client using a mobile operating system (OS) platform-specific notification service. An embodiment method further includes transmitting the notification to the PTT client using messaging queue telemetry transport (MQTT) as a transport protocol.

In an embodiment method, the access transport type used by the PTT client is an internet protocol (IP) multimedia subsystem (IMS) network or an unsolicited internet protocol (IP) network connection. In the embodiment method, failure of a deployment site of the PTT platform does not change a notification method for transmitting notifications to the PTT client.

In accordance with an embodiment, a notification service includes one or more processors and a computer readable storage medium storing programming for execution by the one or more processors. The programming includes instructions to receive a notification from a first component of a push-to-talk (PTT) platform. The notification is for transmission to a PTT client on a client device. The programming includes further instructions to determine an access transport type used by the PTT client to communicate with the PTT platform, select a second component to transmit the notification to the PTT client, and transmit the notification to the second component. The access transport type used by the PTT client is stored in a database, and selecting the second component is in accordance with the access transport type used by the PTT client.

In an embodiment notification service, the database provides information on the access transport type of the PTT client to a plurality of notification services in the PTT platform. Each of the plurality of notification services is deployed at a geographically different deployment site of the PTT platform.

In an embodiment notification service, the instructions to select the second component comprise further instructions to: select a session initiation protocol (SIP) proxy at a same deployment site as the first component to transmit the notification to the PTT client over an
internet protocol (IP) multimedia subsystem (IMS) network when the access transport type is the
IMS network; and select the SIP proxy at the same deployment site as the first component to
transmit the notification to the PTT client using a user datagram (UDP) transport protocol when
the access transport type is an unsolicited IP network. In an embodiment notification service, the
PTT client does not maintain a redundant notification path with the PTT platform when the access
transport type is the IMS network or the unsolicited IP network.

In an embodiment notification service, the instructions to select the second component
comprise further instructions to select first gateway maintaining a first notification channel with
the PTT client to transmit the notification to the PTT client when the access transport type is not
over an IMS network or when the access transport type used by the PTT client does not allow
unsolicited internet protocol (IP) traffic.

In an embodiment notification service, the access transport type is not over an IMS
network, and the access transport type used by the PTT client does not allow unsolicited internet
protocol (IP) traffic. In an embodiment notification service, a primary notification channel
between the PTT client and the PTT platform is unreachable, and the instructions to select the
second component to transmit the notification comprises further instructions to select a first
gateway maintaining a redundant notification channel with the PTT client. In an embodiment
notification service, the PTT client established the primary notification channel with a second
gateway of the PTT platform. The first gateway maintaining the redundant notification channel
with the PTT client is: deployed as part of the PTT platform at a different deployment site of the
PTT platform than the second gateway, deployed at a third party deployment site independent
from the PTT platform, or deployed as part of a mobile operating system (OS) platform-specific
notification service. In an embodiment notification service, the PTT client is a web browser based
PTT client, a PTT client provided by a third party independent from a provider of the PTT
platform, or a combination thereof.

In accordance with an embodiment, a push-to-talk (PTT) platform includes a database,
one or more processors, and a computer readable storage medium storing programming for
execution by the one or more processors. The programming includes instructions to provide a
session initial proxy (SIP) registrar. The SIP registrar is configured to store an access transport
type of a PTT client in the database. The programming includes instructions to provide a PTT
application service to a PTT client on a client device and provide a notification service. The
notification service is configured to receive a notification from the PTT application service. The
notification is addressed to the PTT client. The notification service is further configured to
determine the access transport type of the PTT client, select a component to transmit the
notification to the PTT client, and transmit the notification to the component. Selecting the
component is in accordance with the access transport type of the PTT client. In an embodiment
PTT platform, the component is a SIP proxy of the PTT platform located in a same deployment
site as the PTT application service. In an embodiment PTT platform, the component is a WebSocket gateway of the PTT platform. In an embodiment PTT platform, the component is deployed at a third party deployment site independent from the PTT platform or deployed as part of a mobile operating system (OS) platform-specific notification service.

While this invention has been described with reference to illustrative embodiments, this description is not intended to be construed in a limiting sense. Various modifications and combinations of the illustrative embodiments, as well as other embodiments of the invention, will be apparent to persons skilled in the art upon reference to the description. It is therefore intended that the appended claims encompass any such modifications or embodiments.
WHAT IS CLAIMED IS:

1. A method comprising:
   receiving, by a notification service running on a processor, a notification from a first
   component of a push-to-talk (PTT) platform, wherein the notification is for transmission to a PTT
   client;
   determining, by the notification service, an access transport type used by the PTT client to
   communicate with the PTT platform;
   selecting, by the notification service, a second component to transmit the notification to the
   PTT client, wherein selecting the second component is in accordance with the access transport type
   used by the PTT client; and
   transmitting, by the notification service, the notification to the second component.

2. The method of claim 1, wherein determining the access transport type of the PTT client
   comprises looking up the PTT client in a database.

3. The method of claim 2 further comprises storing, by a session initiation protocol (SIP)
   registrar running on a processor, the access transport type of the PTT client in the database when the
   PTT client registers with the PTT platform.

4. The method of claim 1, wherein the access transport type used by the PTT client is an internet
   protocol (IP) multimedia subsystem (IMS) network, and wherein selecting the second component
   comprises selecting a session initiation protocol (SIP) proxy at a same deployment site as the first
   component to transmit the notification to the PTT client over the IMS network.

5. The method of claim 1, wherein the access transport type used by the PTT client is an
   unsolicited internet protocol (IP) network connection, and wherein selecting the second component
   comprises selecting a session initiation protocol (SIP) proxy at a same deployment site as the first
   component to transmit the notification to the PTT client using a user datagram (UDP) transport
   protocol.

6. The method of claim 1, wherein the access transport type used by the PTT client is not over
   an IMS network, wherein the access transport type used by the PTT client does not allow unsolicited
   internet protocol (IP) traffic, and wherein selecting the second component comprises selecting a first
   gateway maintaining a first notification channel with the PTT client to transmit the notification to the
   PTT client.

7. The method of claim 6, wherein the first gateway is located at a same deployment site of the
   PTT platform or a different deployment site of the PTT platform as the first component.

8. The method of claim 6, wherein a primary notification channel between the PTT client and a
   second gateway of the PTT platform is unreachable, wherein the first notification channel is a
   redundant notification channel between the PTT client and the first gateway, and wherein the method
further comprises including an indication the primary notification channel is unreachable in the notification.

9. The method of claim 8, wherein first gateway is deployed as part of the PTT platform, and wherein the first gateway is located at a different deployment site of the PTT platform than the second gateway.

10. The method of claim 8, wherein the first gateway is deployed at a third party deployment site independent from the PTT platform.

11. The method of claim 8 further comprising transmitting the notification to the PTT client using a mobile operating system (OS) platform-specific notification service.

12. The method of claim 8 further comprising transmitting the notification to the PTT client using messaging queue telemetry transport (MQTT) as a transport protocol.

13. The method of claim 1, wherein the access transport type used by the PTT client is an internet protocol (IP) multimedia subsystem (IMS) network or an unsolicited internet protocol (IP) network connection, and wherein failure of a deployment site of the PTT platform does not change a notification method for transmitting notifications to the PTT client.

14. A notification service comprising:
   one or more processors; and
   a computer readable storage medium storing programming for execution by the one or more processors, the programming including instructions to:
   receive a notification from a first component of a push-to-talk (PTT) platform,
   wherein the notification is for transmission to a PTT client on a client device;
   determine an access transport type used by the PTT client to communicate with the PTT platform, wherein the access transport type used by the PTT client is stored in a database;
   select a second component to transmit the notification to the PTT client, wherein selecting the second component is in accordance with the access transport type used by the PTT client; and
   transmit the notification to the second component.

15. The notification service of claim 14, wherein the database provides information on the access transport type of the PTT client to a plurality of notification services in the PTT platform, wherein each of the plurality of notification services is deployed at a geographically different deployment site of the PTT platform.

16. The notification service of claim 14, wherein the instructions to select the second component comprise further instructions to:
   select a session initiation protocol (SIP) proxy at a same deployment site as the first component to transmit the notification to the PTT client over an internet protocol (IP) multimedia subsystem (IMS) network when the access transport type is the IMS network; and
select the SIP proxy at the same deployment site as the first component to transmit the notification to the PTT client using a user datagram (UDP) transport protocol when the access transport type is an unsolicited IP network.

17. The notification service of claim 16, wherein the PTT client does not maintain a redundant notification path with the PTT platform when the access transport type is the IMS network or the unsolicited IP network.

18. The notification service of claim 14, wherein the instructions to select the second component comprise further instructions to select first gateway maintaining a first notification channel with the PTT client to transmit the notification to the PTT client when the access transport type is not over an IMS network or when the access transport type used by the PTT client does not allow unsolicited internet protocol (IP) traffic.

19. The notification service of claim 14, wherein the access transport type is not over an IMS network, and wherein the access transport type used by the PTT client does not allow unsolicited internet protocol (IP) traffic, wherein a primary notification channel between the PTT client and the PTT platform is unreachable, and wherein the instructions to select the second component to transmit the notification comprises further instructions to select a first gateway maintaining a redundant notification channel with the PTT client.

20. The notification service of claim 19, wherein the PTT client established the primary notification channel with a second gateway of the PTT platform, wherein the first gateway maintaining the redundant notification channel with the PTT client is:

   deployed as part of the PTT platform at a different deployment site of the PTT platform than the second gateway;

   deployed at a third party deployment site independent from the PTT platform; or

   deployed as part of a mobile operating system (OS) platform-specific notification service.

21. The notification service of claim 19, wherein the PTT client is a web browser based PTT client, a PTT client provided by a third party independent from a provider of the PTT platform, or a combination thereof.

22. A push-to-talk (PTT) platform comprising:

   a database;

   one or more processors; and

   a computer readable storage medium storing programming for execution by the one or more processors, the programming including instructions to:

   provide a session initial proxy (SIP) registrar, wherein the SIP registrar is configured to store an access transport type of a PTT client in the database;

   provide a PTT application service to a PTT client on a client device; and

   provide a notification service, wherein the notification service is configured to:

   receive a notification from the PTT application service, wherein the notification is
addressed to the PTT client;

determine the access transport type of the PTT client;

select a component to transmit the notification to the PTT client, wherein selecting
the component is in accordance with the access transport type of the PTT client; and

transmit the notification to the component.

23. The PTT platform of claim 22, wherein the component is a SIP proxy of the PTT platform located in a same deployment site as the PTT application service.

24. The PTT platform of claim 22, wherein the component is a WebSocket gateway of the PTT platform.

25. The PTT platform of claim 22, wherein the component is deployed at a third party deployment site independent from the PTT platform or deployed as part of a mobile operating system (OS) platform-specific notification service.
FIG. 2
Fig. 3
Fig. 4
Fig. 5
Fig. 6
FIG. 7
FIG. 8
FIG. 12
FIG. 13
FIG. 16
FIG. 17

FIG. 18
INTERNATIONAL SEARCH REPORT

International application No.
PCT/US16/16371

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - H04W4/10; H04W6/005; H04W9/02 (2016.01)
CPC - H04W4/10; H04W9/02; H04W6/005

According to International Patent Classification (IPC) or to both national classification and IPC

R FIFI 11 SFARCHHD

Minimum documentation searched (classification system followed by classification symbols)

IPC(8) Classifications: H04W4/10; H04W9/02; H04L29/06; H04W6/005 (2016.01)
CPC Classifications: H04W4/10; H04W9/02; H04L6/00; H04W6/005

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)
Keywords: PTT, push-to-talk, POC, notification, notification service, secure, gateway, SIP, session initiation protocol, WebSocket

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 2008/0316610 A1 (BHASKARAN, H et al.) 25 December 2008, figure 8, paragraphs [0041], [0044]-[0046] [0055]-[0056], [0071]-[0072].</td>
<td>1, 2, 14</td>
</tr>
<tr>
<td>Y</td>
<td>A1 (MOTOROLA MOBILITY LLC) 7 August 2014, paragraph [0049], [0052]</td>
<td>3, 15, 18, 22-25</td>
</tr>
<tr>
<td>A</td>
<td>Y1 US 2010/0208648 A1 (NARKAR, V et al.) 19 August 2010, paragraphs [0004]-[0009], [0022], claim 5</td>
<td>4, 16-17</td>
</tr>
<tr>
<td>Y</td>
<td>A1 (STRATMEYER, C et al.) 11 September 2003, paragraphs [0028], [0040], [0049]</td>
<td>5</td>
</tr>
<tr>
<td>Y</td>
<td>A1 (KODIAK NETWORKS, INC.) 01 August 2013, paragraph [0034], [0049]</td>
<td>6, 7, 13, 18</td>
</tr>
<tr>
<td>Y</td>
<td>A1 (KOMPPELLA, V ET AL) 20 September 2012, paragraphs [0009], [0041], [0065]-[0066]</td>
<td>13</td>
</tr>
<tr>
<td>Y</td>
<td>A1 (BROWN, K et al.) 12 March 2009, figure 1, paragraphs [0020], [0024], [0056]</td>
<td>8</td>
</tr>
<tr>
<td>Y</td>
<td>A1 (CASSIDIAN FINLAND OY) 31 December 2014, paragraph 3, lines 4-12, page 4, lines 25-37, page 5, lines 15-29</td>
<td>24, 25</td>
</tr>
<tr>
<td>A</td>
<td>A1 (XI, M) 19 May 2005, paragraphs figure 7, [0006], [0008], [00017]</td>
<td>8-12, 19-21</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C. 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 prior in time to the international filing date but later than the priority date claimed

Date of the actual completion of the international search
27 April 2016 (27.04.2016)

Date of mailing of the international search report
1 MAY 2016

Name and mailing address of the ISA:
Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No. 571-273-8300

Authorized officer
Shane Thomas
PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)