METHODS OF INTEGRATING mVoIP IN ADDITION TO A VoIP ENVIRONMENT

Paul MOZA, Marian ALEXANDRU

Transilvania University, Brașov, Romania

Abstract: *Along with the power of consumer applications and devices, expectations regarding the communication capabilities in the VoIP (Voice over Internet Protocol) environment are increasing too. The integration of the mobile VoIP (mVoIP) technology in addition to VoIP environment is illustrated in this paper and some proposed and tested by the authors integration methodologies, basic call flow and authentication method for mVoIP, common topologies and solutions to achieve mobility in VOIP networks are presented.*

Keywords: *mVoIP, mobility, SIP, VoIP, remote subscribers, SBC*

1. INTRODUCTION

The mobile VoIP technology is the new extension of a VoIP network, capable of transmitting voice packets using a software installed on the mobile phone or on other mobile communication devices. Mobile VoIP is considered extremely important in the overall scheme because VoIP will not grow if it remains wired, as the trend is connectivity within the context of mobility.

Wireless Internet is the biggest limitation for mobile VoIP. There are two choices: Wi-Fi hotspots, which are generally free, and 3G, 4G or the future 5G cellular networks, which are not. [1]

Wi-Fi hotspots are free but small, because they don't have a large coverage area. However, using the wireless network at the office alongside with the mobile VoIP applications, can offer the advantage of free VoIP calls. 3G and 4G networks calls are not free, but these networks have a large area of coverage and their users can have high mobility and speeds. Furthermore, 3G networks do not always offer a consistent connection speed. 4G networks, which are faster and becoming more prevalent on large geographical areas of the world, make connection speed more consistent for mVoIP.

Likewise, there are two methodologies of integrating a mobile device into a VoIP network. The most used one turns the mobile device into a standard SIP (Session Initiation Protocol) client and then uses a data network to send or receive SIP signaling messages and RTP (Real-time Transport Protocol) voice packets.

Another implementation of mobile deployment uses a soft-switch like a gateway to bridge SIP and RTP into the mobile network's SS7 (Signaling System no. 7) infrastructure. In this implementation, the mobile handset continues to operate as it always has (as a GSM or CDMA based device), but now it can be controlled by a SIP application server which can now provide advanced SIP-based services.[1]

There are multiple advantages of using mVoIP [8]: a mobile user can be reached via one published number regardless of his/her location or device, it reduces communication costs, it can work with the user's existing IT (Information Technology) and telephony infrastructure and it allows the user to make video calls.

Also, mVoIP offers the possibility to create or join conferences, option to easily move calls between desk phones and mobile phones, device selection, call decisions, security.

In the unified communications world, more and more voice and video communications will be launched from (and connected to) mobile wireless devices. Integrating the mobile users' voice and real-time communications services with core enterprise communications lets them do their jobs regardless of location. [9]

2. PROPOSED INTEGRATION METHODOLOGIES AND TOPOLOGIES

As we stated before there are two main methodologies of integrating a mobile device within a VoIP network, both of them being implemented and tested by the authors
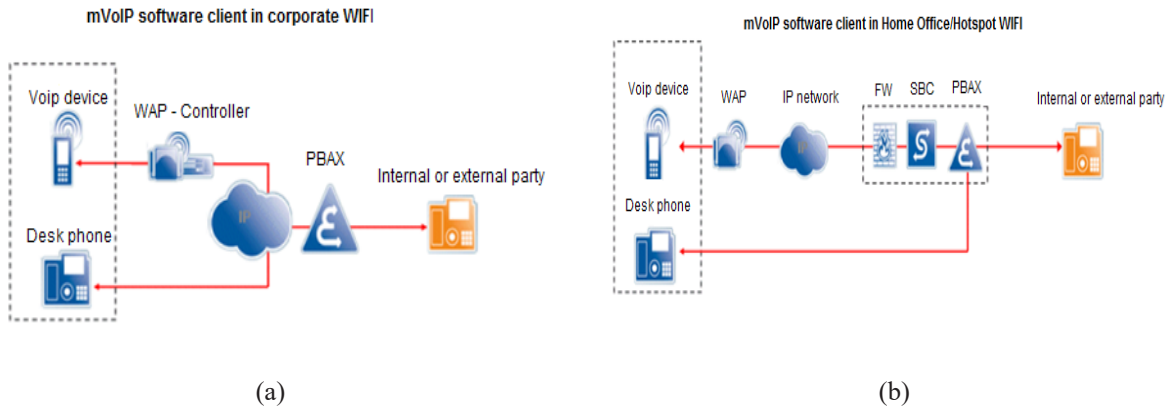
FIG. 1. mVoIP integration methodologies in VoIP networks

This figures illustrates the two typical deployment in an enterprise environment. Fig.1. (a) describes the way a mobile device is directly connected to the PBAX (Private Branch Automatic Exchange). This integration is possible only when the mobile device is connected to the corporate network, if it's in the same network as the PBAX.

Additionally Fig.1. (b), remote users can connect to PBAX via Wi-Fi/3G/4G through a Session Border Controller (SBC). The SBC is mandatory when users are connected to a different network than PBAX. SBC is used for initiating, maintaining and closing the SIP sessions, and also for security and media anchoring.

The user can use two devices, a desk phone and a mobile device with an VoIP application loaded on it. He can be reached via one number, for example 40268334711 which is a number assigned to the desk phone. For the mVoIP application a new subscriber is needed to be assigned, for example 40268334711 (we will assign on this subscriber the 40268334711 One Number Service) which connects or registers to the PBAX via Wi-Fi.

In case of an incoming or outgoing call, PBAX knows which one of this two devices is the preferred one. One Number Service lets calls follow the user to whatever device he selects – whether office, home, mobile or desk phone – completely transparent to the caller.

Fig. 2. (a) below describes an example of a network architecture proposed by the authors to be used in a company. The communication platform (PBAX) is connected to the UC (Unified Communications) server and communicates with it via CSTA (Computer-supported Telecommunication Applications) messages.
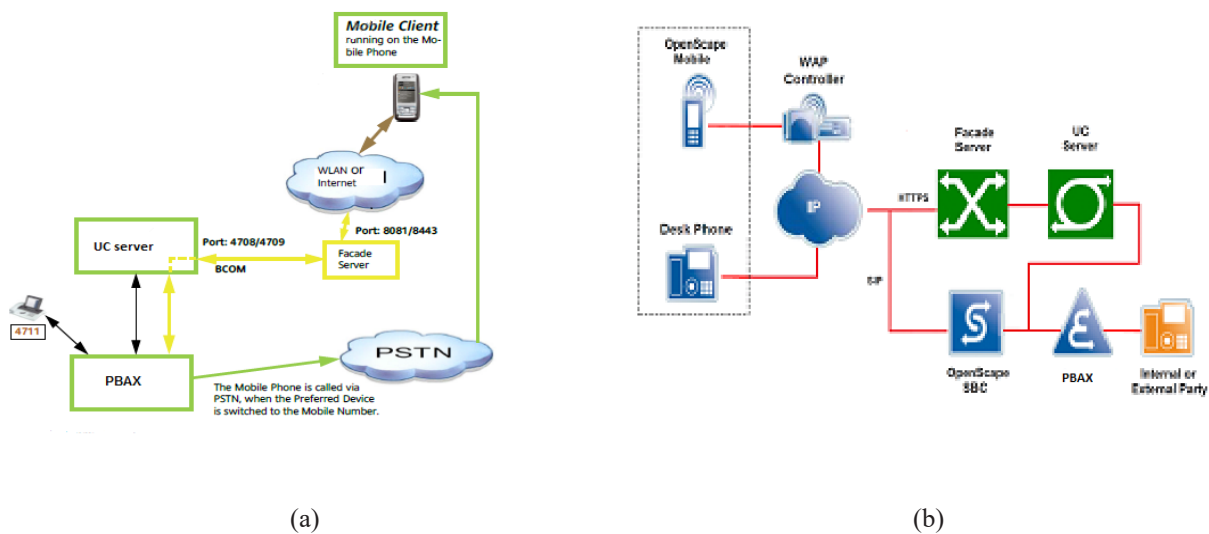
(a)   (b)

FIG. 2. The proposed mVoIP topology

Unified communications server (UC Server) [9] is a comprehensive solution that ties different services, applications in a single component. UC is not a single product but rather a solution made up of a variety of communication tools and components. UC components include all control and multimodal communications, presence, instant messaging, unified messaging, speech access and personal assistant, conferencing - audio, Web and video, collaboration tools, mobility, Business Process Integration (BPI), software to enable business process integration, One Number Service and the management of the PBAX.

On the UC Server side a DMZ (demilitarized zone)[11] with internet connectivity is required. In computer security, a DMZ is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. Within the DMZ, a so-called Façade Server is installed which is the endpoint of the incoming internet connection from the client. This connection required only one port to be open in the outer firewall (in Fig.2. (a) the opened port is 8081). The Façade server communicates with UC server via the https protocol. Any request coming from Façade server to UC will be processed by UC and if needed the PBAX will be contacted via CSTA messages [4].

The usage of an SBC (Session Border Controller) [7] enables enterprises to extend SIP-based applications beyond the Enterprise network boundaries, when users are not all within the same IP network.

SBC provides secure remote user access to the IP telephony infrastructure of an PBX system for SIP phones regardless of location. It supports the necessary near-end and far-end Network Address Translation (NAT) traversal functions for connection using a public IP addresses through the Internet. SBC can also support remote users that are installed behind a far-end NAT/firewall as shown in Fig.2 (b). It is mandatory to have such equipment in the context of mobile VoIP.

When the remote user is a hard phone there is generally no support for a VPN (Virtual Private Network) connection at the phone and use of an SBC, to allow connection to the communication platform, is necessary.

3. THE DIAGRAM FOR A POSSIBLE CALL FLOW AND SCENARIO

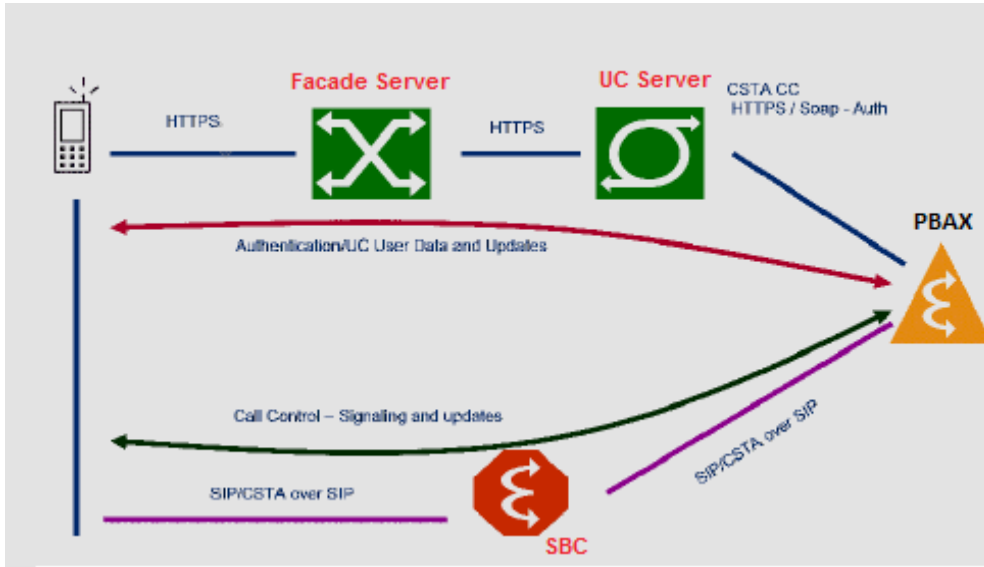The diagram for a possible call flow, in case a mobile SIP client is used, is described in the Fig. 3. below:

FIG. 3. mVoIP call flow

The mobile SIP software contacts the Façade Server via https protocol and sends a request for authentication. The Façade Server forwards this request to UC server, which checks the UC user id and asks the PBAX (via CSTA protocol) if this user has a mobile subscriber configured.

If PBAX has assigned a specific subscriber for mobility usage then the authentication will be successful and UC Server will answer to the initial request with SIP Login Info. This SIP Info needs to contain the SIP IP public address of the centralized SBC. When this SIP Login info is received the mobile phone knows where to send the SIP signaling messages.

For example the INVITE message will be sent from mobile phone to the public SBC address through the Internet, the SBC will forward the message from its access side to the core side (private IP address) and the core side will continue to forward the message to PBAX. When the connection with the called party is made (from the signaling point of view) the RTP messages will be sent to SBC, which behaves as an anchor for them and forwards the packets to a SIP trunk, gateway or another subscriber if the called party is a SIP subscriber located in the same network. [2]

A real call flow example with two participants is represented below. The first participant is 74995799173 which uses an application called OSMO installed on a Sony SGP771 28.0.A.8.251 Android 5.0.2. The second participant is 749957991721 with ONS 74995799172 which uses an application installed on a computer. Both participants are connected to a Wi-Fi 802.11n network with 300 MB speed. In our test the participant one calls the second participant. The IP addresses of all involved equipments are as follows: SBC WAN IP address 95.163.87.42, PBAX 10.10.222.12 in trace, UC server - 10.10.222.22, Facade - 95.163.87.43/10.10.222.56, SBC LAN - 95.163.87.44.

First the authentication [6] for 74995799173 takes place and the Façade server check with the UC server the account for this specific subscriber:

[OSMCService] Login for 74995799173@system using OpenScape Mobile 72550 on Sony SGP771 28.0.A.8.251 Android 5.0.2 with mobile
[74995799173@system/3] Calling user: 74995799173@system [74995799173@system/3] Transport protocol (http): org.apache.axis.transport.http.HTTPTransport@8c74fa01
INFO   [OSMCService] User is OSMO capable, get OSV/PBAX Data

After the authentication the device of the first participant send a SIP invite message to the SBC WAN IP address 95.163.87.42 which will be next forwarded to SBC LAN - 95.163.87.44 and then to PBAX 10.10.222.12.

Based on this INVITE message PBAX communicates with the UC server and checks the options for 74995799172 where 749957991721 is set as the preferred number. As stated above, each application used has a different subscriber number configured behind the 74995799172 ONS number.

LogId Event="update" User="74995799172@system" /> Registered Device: +749957991721 set for user: 74995799172@system

FINE   [com.siemens.symphonia.bcom.addressmanager.impl.SystemDataImpl]   <LogId Event="update" User="74995799172@system" /> Preferred Number: +749957991721 set for user: 74995799172@system

When UC server finds out that the preferred device for this 74995799172 participant is 749957991721 configured on a computer, it forwards the SIP invite to this device. From this point all the signaling messages follow this path: participant 1 device ⟷SBC ⟷PBAX⟷SBC⟷ participant 2 device.

CONCLUSIONS

The paper shows how can be added the mobility feature in addition to VoIP environment by using different topologies and methodologies. Basically the implementation of this service requires the development of a SIP application which will act as a standard SIP client by using a data network to send or receive SIP signaling messages and RTP voice packets.

In addition to the SIP application a Session Border Controller is needed to manage the remote sessions and a Façade server to verify the user data and authentication data. The usage of mobile VoIP technology offers a complex set of new and interesting features, independent of the operating system, such as the possibility to be reached on one number regardless of you location or device, possibility to create or join conferences, video calls, option to easily move calls between desk phones and mobile phones, etc.

From the infrastructure cost point of view this solution seems to be a good choice since the purpose of the mVoIP is to reduce costs and achieve flexibility.

The mVoIP technology is a pretty stable one and offers a lot of features and capabilities but it can be improved in many ways: the security can be enhanced, the voice quality can be increased, the achievement of new features such as voicemail to email transcription, music on hold, find me/ follow me call routing, call detail reports, call screening, single sign on, etc.

This paper is a small guide for anyone looking towards voice mobility as a solution to real-world business problems: IT engineers looking to understand the potential for converting offices to all-wireless; network designers and architects planning on rolling out a fully-mobile voice network; and administrators operating or troubleshooting voice mobility networks.

REFERENCES

[1] Eliot van Buskirk, Five Reasons Cellphones and Mobile VoIP Are Forging an Unlikely Truce, http://www.wired.com/2010/04/mobile-voip-truce/, accessed on 10 Jan. 2016;

[2] R.R. Roy, H.323 Mobility Architecture and Protocol for Terminal, User and Service Mobility, AT&T, Document APC-1652, Oct. 1999;

[3] A. Fladenmuller, R. De Silva, The effect of Mobile IP handoffs on the performance of TCP, Mobile Networks and Applications, Vol. 4, 1999, pp. 131-135;

[4] S. Niccolini, VoIP Security Threats, Internet-Draft, NEC SPEERMINT Working Group, 2007;

[5] S.W. Cho, et. al., mVoIP Service attack and authentication mechanism on s Smart work device, In Proc. of International Conference on Computer Science and Network Technology (ICCSNT2011), Vol.1, pp.482-486, 2011;

[6] S. Salsano, et. al., SIP Security Issues: The SIP authentication procedure and its processing load, IEEE Network, November/December, 2002.

[7]http://www.ibm.com/support/knowledgecenter/SSKTXQ_8.5.1/com.ibm.help.sametime. v8512.sut.doc/osv_sbc/osv_sbc_config_remote_users.html, accessed on 05 Feb. 2016;

[8] https://www.mobilevoip.com/call_types, accessed on 17 Jan. 2016;

[9] B. Klepec, S. Tomazic, Techniques for performance improvement of VoIP applications, Electrotechnical Conference, MELECON 2002, 11th Mediterranean, IEEE, pp.250 – 254;

[10] J. Epstein, Scalable VoIP Mobility, ISBN: 978-1-85617-508-1, Elsevier Inc., 2009.

[11] ***DMZ Server, http://searchsecurity.techtarget.com/definition/DMZ, accessed on 10 Feb. 2016.

.