Cost Effective Calling Mechanism for Roaming Users

WMDH Wanasinghe, AKST Chaminda, DR Ranasinghearachchi#, TL Weerawardane
Department of Electrical, Electrical and Telecommunication, Faculty of Engineering,
General Sir John Kotelawala Defence University,
Ratmalana, Sri Lanka.
#dumindurr@gmail.com

Abstract—The cost of initiating a call when roaming in a foreign PLMN network is considerably high. As a remedy for this, VoIP services can be used, but both calling and called parties have to have internet connectivity with suitable QoS at both ends. This research paper is directed towards implementation of a cost effective solution for international roaming, where only the calling party (roaming in foreign country) requires internet connectivity and the called party (in home country) does not need internet connectivity. This roaming architecture is assisted by the Public Switched Telephone Network (PSTN) of a local fixed operator. The service network consists of Customer Network (CN) and Provider Network (PN). CN consists of a Customer Premises Equipment (CPE), VoIP Gateway (GW), Internet connectivity (preferably ADSL line) and PSTN line. The PN consists mainly of a Roaming Connectivity Server (RCS) and Call Accounting Server (CAS). These specifications are only used in-order to simulate the conceptual network which is further described. Network infrastructure described in this paper can be subjected to change, according to the customer base, network security, and other parameters. In the customer end, accessibility is increased by using several applications and configurations. This network service can be deployed without interfering the other operator revenue generation and still be cost effective from customer point of view.

Keywords— Roaming, CPE, RCS

I. Introduction

Presently we have plenty of options to connect with the users who are roaming in different countries using options such as International Roaming, Skype, Viber, etc. The cost we are proposing is somewhat high. So the subscribers are searching for a low cost voice call connection when roaming abroad, especially to talk to the relatives, friends and other persons in the home country.

Initiating and terminating a call when roaming is very expensive for the roaming user. The charges range from operator to operator and country to country. These costs are predefined by the relevant operators (home operator and roaming operator) according to legal agreements between the two operator.

In international roaming, the customer has the option to make a considerable high deposit to the operator before roaming. The charges are deducted from this deposit until it is depleted.

As a solution for this issue, internet voice calling software such as Skype and Viber were introduced. But in this, case to generate a free call the parties of the both end have to be connected to the internet and also a stable internet connection is essential to complete the call successfully. However, with the increase of data traffic and online applications, mobile network coverage might not eligible to provide customers sufficiently.

Also, for corporate roaming users, the annual cost of roaming calls is very high as sometimes, their employees spend a lot of time abroad for formal work.

So in this paper, we address the main problems which are high cost of roaming and need of an internet connection in both sides. From this concept we terminate the roaming call for any subscriber at the cost of local outgoing call. This is beneficial to both single users as well as large scale organizations.

II. Conceptual Design

In this design, the system can be divided into two main networks. The Customer Network (CN) and the Provider Network (PN). Both of these networks are connected to one another other internet via IAX Trunks. A graphical illustration of the basic system can be seen in Figure 1.

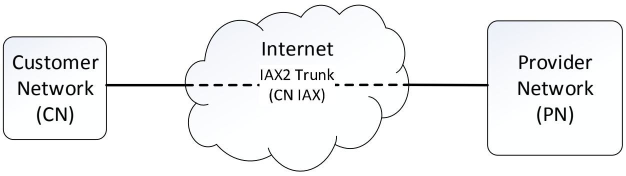

Figure 1: Basic system concept

Each consists of components crucial for the deployment of the service. There can be more than one Customer Network, but only one Provider Network. This setup is used to provide seamless connectivity for the Customer Roaming Entity (CRE), device/softphone used to connect to the PN, to the relevant CN. Each CRE can only connect to the CN that it is registered to CREs cannot connect to other CNs. This is done maintain security and privacy between the separate CNs. (Figure 2).

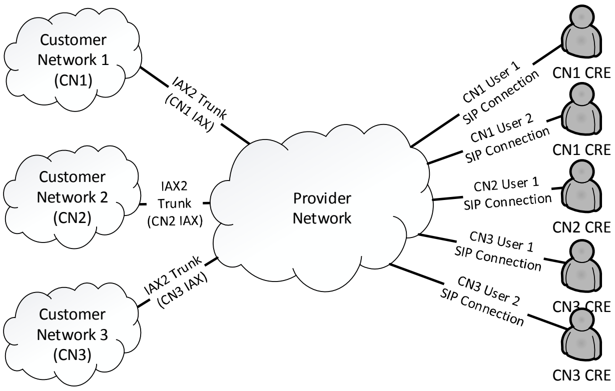

Figure 2: Multiple CRE connected to relevant CNs via one PN

III. Customer Network (CN)

The Customer Network is the network on the customer's side of the system. In order for this part of the network to function the customer must have existing internet connection, preferably ADSL internet connection, and a PSTN telephone line connection. In the CN there are two main components that need to be introduced to the network to provide the connectivity between the Provider Network and the PSTN connection of the customer. This PSTN connection will be used to terminate the user's roaming call to the destination number. The two main components are the Voice over IP (VoIP) Gateway and the Customer Premises Equipment (CPE). (Figure 3).

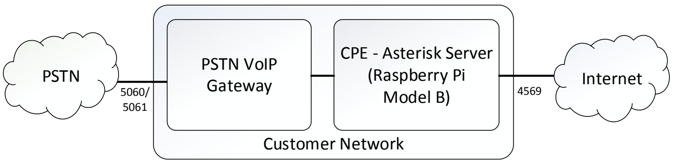

Figure 3: Customer Network Components

A. Customer Premises Equipment (CPE)

The CPE is a low powered, low cost server running FreePBX. FreePBX is a Graphical User Interface (GUI) for Asterisk. In our system, the CPE is deployed on a "Raspberry Pi Model B". The single core CPU of the Raspberry Pi Model B is generally clocked to 700 MHz. This was overclocked to 800 MHz to provide better performs without effecting the Raspberry Pi. This version of Raspberry Pi can run Linux in a stable manner. The Raspbian is the most stable and function of all the Operating Systems supported by Raspberry Pi. It is a version of Debian Linux modified to run on the Raspberry Pi platform. [5].

B. VoIP Gateway

The VoIP Gateway is used to provide an interface between the internal VoIP network and the external PSTN network. It basically converts the VoIP Real-Time Protocol (RTP) packet data to analog signals and sends them through the PSTN interface and vice versa. This also performs the function of dialing the number in Dual Tone – Multi Frequency (DTMF) tone when taking a call to the PSTN network and signaling the VoIP server for an incoming call.

The VoIP Gateway that was used in this system was the Cisco SPA3102 VoIP Gateway. This VoIP gateway has the option to connect to the PSTN line at the user's home. This device can also be connected to the home telephone network as well, therefore the user can terminate calls directly to existing telephones at home when roaming without dialing out.

A SIP Trunk is setup between the CPE and the VoIP Gateway. All the calls that are terminated to the PSTN line from the CPE are sent on this trunk.

C. Network Configuration

In order for the system to work properly, certain configurations need to be made in order for the CPE to connect to the RCS. The user's router must port forward the port 4569 to the IP address of the RCS. This port forward function is done to route all packets that the router receives on the 4569 port to the RCS.

IV. Provider Network (PN)

The Provider Network is the network of nodes in the provider's side of the system. This is used to provide connectivity between the Customer Network and the Customer Roaming Entity (CRE), customer device/equipment used to connect to the system. This connects the relevant customer entity to its relevant Customer Network via an IAX trunk which is established between the two networks over the internet. The Provider Network consists of several main components. This includes the Remote Connectivity Server

(RCS), the Call Accounting Server (CAS), a Mail Server, and a Web Server. Each of these provides a crucial role in the system (Figure 4).

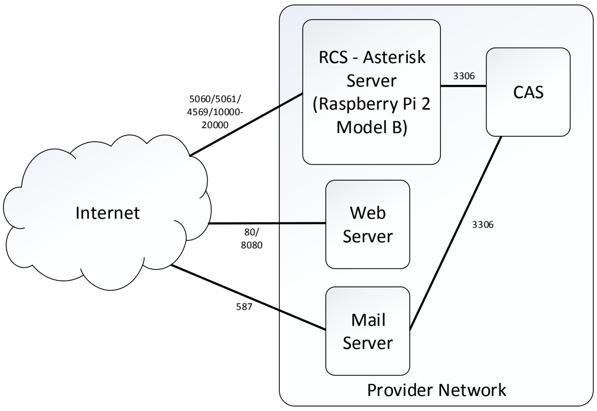

Figure 4: Provider Network Components

A. Remote Connectivity Server (RCS)

The RCS is the main entity that provides the connectivity between the Customer Network and the Customer Roaming Entity (CRE). It does this by establishing an IAX trunk between the CPE of the Customer Network and the RCS. This trunk will use only the 4569 port on both the CPE and the RCS. This is better compared to a SIP trunk as both the signaling and the VoIP RTP data is sent through the 4569 port, where as in SIP it utilizes port 5060 for signaling and any two random ports between the port numbers 10,000 and 20,000 to send the RTP data. And this consumes less bandwidth compared to SIP trunks as the header sizes are comparatively lower.

In this system, the RCS was deployed on a “Raspberry Pi 2 Model B”. This is similar to the Raspberry Pi Model B, but it is almost six time more powerful in comparison. The CPU of the Raspberry 2 is a Quad-Core ARM Cortex-A7 CPU clocked are 900 MHz We did not over clock this as we felt that this clock rate on a quad core CPU was sufficient enough to sever the function of the RCS. The RCS runs version 11 of Asterisk IP PBX server.

Asterisk is a back-to-back user agent (B2BUA). It can function as a server on one end and a client on the other to control all aspects of a VoIP call [1].

B. Call Accounting Server (CAS)

The CAS is the entity that gets call details from the RCS and calculates the call cost which were originated when roaming, and generate a simple and easy to understand Call Detail Record (CDR) to be sent to the Email server to be sent to the customer’s email address at the end of each day.

This is done through a program written in PHP programming language. The RCS records the CDR of every call that originates and terminates to its users in a MySQL database. The PHP program retrieves the CDR of each customer during that day (24 hours from previous 00:00 GMT) from the RCS server. Finally, after the calculations are done and the results are obtained. This process is repeated according to each CPE.

C. Mail Server

The mail server is a server used to send emails to the users and the system administrators. It sends CDR information email to the users, and send system notifications and other administrative related information to the administrators of the system.

D. Web Server

The Web Server is an Apache server which hosts the CDR information webpage. Users can login to this webpage and view their CDR information real-time.

E. Network Configuration

Certain network configurations were needed to be made at the PN. Just like in the CN, port 4569 is port forwarded to the RCS. In addition to the SIP ports 5060,5061 and ports 10,000 to 20,000 are port forwarded to the RCS. This exposes more than 10,000 port to the internet.

V. Connectivity Between CN And PN

In order to fulfill the primary function of this project, both the Customer Network and the Provider Network must be connected together through internet. This connection is established between the CPE and the RCS of the respective networks. The connection is established to route VoIP data from one network to the other and vice versa. This is done through the use of an IAX trunk.

IAX trunk has some advantages over SIP Trunk. One being that IAX uses less bandwidth than SIP. This is because the header size of the IAX packets are comparatively smaller than the SIP packet headers.

In SIP the RTP packets are dropped during call sessions due to NAT issues. This is reduced in IAX by sending the RTP packets and the signaling together on the same channel.

In SIP, the signaling is done on port 5060/5061 and the RTP packets are sent through any two random port numbers between 10,000 and 20,000. Whereas in IAX, the signaling and RTP packets are sent through the same port, port 4569.

And IAX was specifically design to overcome issues caused by NAT. This was made by Asterisk and is specific to asterisk systems. Due to these reasons the IAX trunk is used connect the CPE and the RCS.

Just like the SIP Trunk configured in Customer Network the IAX Trunk must be setup between the CPE and the RCE. This IAX trunk is encrypted, therefore the security is considerably higher compared to SIP Trunk.

Another reason for use IAX trunk over SIP trunk was that, SIP exposes 10,000 port to the internet. That is, these ports would be port forwarded from the user's home router to CPE server. This exposes the CPE to the internet and open for hackers to encroach the system. Therefore, when only one port is exposed to the internet, the number of paths a hacker can use to enter the system are significantly less.

Additionally, the trunk is encrypted using AES-128 encryption standard. This helps to protect the trunks even from eavesdropping attacks by hackers. Also, MD5 algorithm is used to check the authentication details at the initiation of each call session. [2][6].

VI. Connectivity Between The RCS And The User

In order for the user to connect to the PN, the user must use a device or softphone to connect to the RCS. Most of these devices/software do not support IAX protocol for communication. Therefore, we have to use SIP protocol to communicate with the RCS.

For Android devices the in-built internet calling settings can be configured. Further for IOS and Windows phones, a softphone application can be used to setup the user account in the mobile device. For desktop/laptops, running Windows/Mac OS/Linux, softphone applications can be used to connect to the RCS.

VII. Operation Of The System

In this system, when a user is roaming in a foreign country, the user simply needs to use a connection with suitable QoS and connect to the RCS server via softphone or other compatible device. Once the user is connected to the system, the user can take calls to the home country via the system as long at the CPE that is owned by the used is in operational state. The user simply needs to initiate the call to the desired terminating number and the call session will begin.

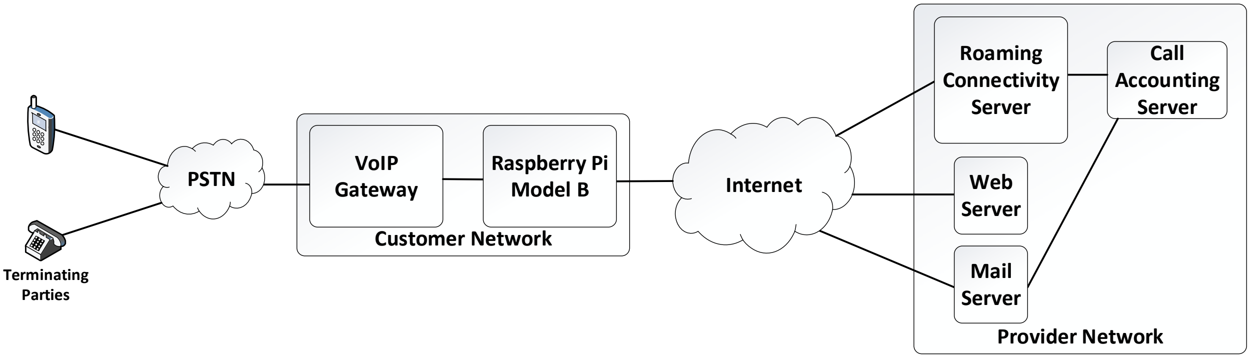

Figure 5: Operational Architecture of CN and PN Connectivity

VIII. Control Plane Information Flow

In this system, the call is routed through multiple nodes before it is terminated to the intended terminating parting. Signals are exchanged through both SIP and IAX protocols between the relevant nodes. (Figure 5).

When the call is initiated by the roaming party, the user's device/soft phone connects to the RCS via the SIP protocol and initiates the call session through the "INVITE" message. In this message, the dialed number is sent with the prefix "#9". The RCS uses this prefix to recognize that this is a call that needs to be terminated through the PSTN at the relevant customer's home. Then the RCS initiates a call session through the IAX trunk between the RCS and the relevant customer's CPE through the "NEW". After some additional messages such as, "AUTHREQ" and "AUTHREP" are exchanged between the RCS and the CPE, the CPE initiates a call session to the VoIP Gateway connected to its network. This is achieved through the SIP Trunk between the VoIP Gateway and the CPE. Like the initial call initiation at the user end, a "INVITE", containing, the dialed number is sent to the VoIP gateway. At the VoIP gateway, once the "INVITE" message is received, the VoIP gateway starts initiating (dialing) the call through the PSTN line connected to it.

Once the call is initiated (i.e. once dialing is finished, but the call is not connected to the terminating party), the VoIP Gateway sends a "200 OK" message back to the CPE. During this time an audio session is already established between the PSTN line and the VoIP Gateway. After this, an "ANSWER" message is sent on the IAX trunk stablished between the CPE and the RCS. Once the RCS receives the message, it sends a "200 OK" message to the User Device.

After all this signaling is done, an audio session is established between the PSTN line and the User Device. This is done even before the terminating party answers the call.

After the call has ended, the user hangs up from the User Device. This initiates the disconnection process of the call. It is initiated by the "BYE" message sent to the RCS from the User Device. Once the RCS receives the message, it sends a "DISCONNECT" message to the CPE and return the "200 OK" message to the User Device. Subsequently, the sends a "BYE" message to the VoIP Gateway and returns an "ACK" message back to the RCS. After this, the VoIP Gateway disconnects the session to the PSTN line and returns a "200 OK" message to the CPE. (Figure 6).

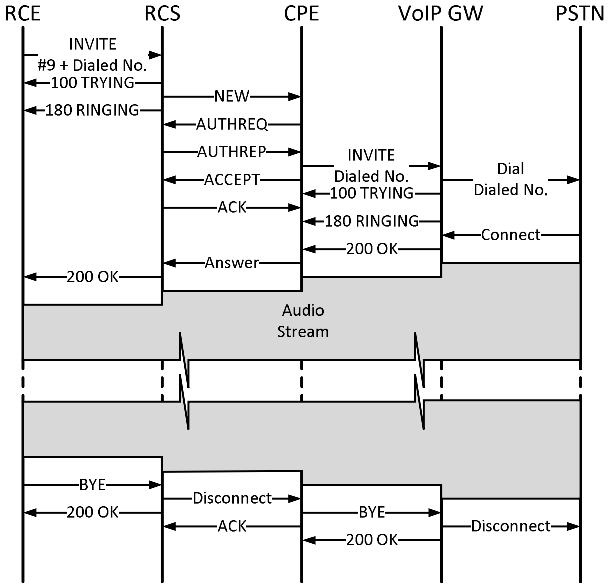

Figure 6: Roaming user call initiation call flow

IX. Data Usage Analysis

The data flow in system was analysed by obtaining traces from RCS and CPE. From these traces we were able obtain the average data usage between the respective nodes.

A. Data Usage of The Roaming User

The data flow between the RCS and the CRE flows entire in SIP and RTP. From the trace obtained from the RCS, we were able to analyse the data flow between the two nodes.

From this analysis, we were able to calculate that, on average a 2-minute call will have a usage of 2.7 MB of data. That is, if the roaming user takes a 10-minute call, the data usage on average is 13.5 MB.

B. Data Flow Between RCS and CPE

The data flow between the RCS and CPE flows entirely on the IAX trunk. From the trace obtained from the CPE, we were able to analyse the data flow between the two nodes.

From this analysis we were able to calculate that on average a 2-minute call will have a usage of 2.6 MB of data. That is, if the call session is 10 minutes long, the data usage at the CN is 13 MB.

C. Analysis

From the analysis of the traces we were able to calculate that, the data usage of the IAX trunk is 4% less than that of the SIP data flow. This is due to the smaller header size of the IAX packets compared to the SIP packets. Additional statistical data obtained from three different 2-miunte long calls can be seen in Table 1.

Table 1: Data Rates and Usages of 2-minute long calls

Call #	Node	Usage (MB)	Average (Kbits/s)	% Diff
1	CPE	2.59	149.68	3.28%
	User	2.70	154.66	
2	CPE	2.65	150.74	4.32%
	User	2.73	157.40	
3	CPE	2.55	150.42	4.60%
	User	2.69	157.50	

If a user made calls with the total duration of 1 hour per day, the average total amount of data usage at the CN end is 78 MB and the usage for the roaming user is 81 MB.

In the initial stages of the call session, we observed that the delay is due to signalling between nodes. This delay ranges from 3-8 seconds when initiating the call from WLAN or 4G connection. It is generally due to the signalling and setting up of security parameters between the nodes of the system. [3][4].

X. Future Work

There are several areas in which the system can be improved. Some are in areas of security of the system and others in the efficiency of the system.

When referring to the security aspects of the system, solutions need to be found for external threats such as brute force attacks and SIP vicious attacks. These attacks render the SIP servers unusable.

During the testing phase of the system, the exposure of the ports of the PN to the internet caused many security issues. On three separate occasions, the system was encroached by hacker from outside the network. This was a serious issue as in all these occasions, the RCS became inoperable. The RCS was manually rebooted in order to get it back to a useable state.

To avoid these kind of security threats VPN (Virtual Private Network) can be implemented between the RCS and the CPE, and an advanced firewall can be implemented to protect the RCS from threats from the internet. This will ensure to reduce the risk of the RCS being vulnerable to hacks and threats when port forwarding a large number of ports.

Further, The RCS can be deployed in cloud environment to coup with expanding customer base. The cloud environment will let the RCS virtual machine expand with load. This will also enable higher efficiency, availability and resource sharing.

Additionally, the delay experienced at the beginning of the call needs to be reduced. This need to be reduced to improve the system efficiency.

In commercial deployment of this service we can preferably come to an agreement with a fixed operator such that the generated revenue will be profitable to the utilized network operator. This will help to deny any unauthorized access to the system via the fixed operator.

REFERENCES

[1] Weiyin Zhuang, Yuliang Tang and Yibo Hu, "Design and Implementation of SIP B2BUA Server", International Conference on Anti-Counterfeiting, Security and Identification (ASID), 2013, pp. 1-5.

[2] Patrik Gallo, Dušan Levický and Gabriel Bugár, "Authentication Threats in PSTN-VoIP Architecture Using Multi-Service Gateways", ELMAR, 2012, pp. 153-156.

[3] Sureshkumar V. Subramanian andRudra Dutta, "Measurements and Analysis of M/M/1 and M/M/c Queuing Models of the SIP Proxy Server", International Conference on Computer Communication and Networks (ICCCN), 2009, pp. 1-7.

[4] Sureshkumar V. Subramanian and Rudra Dutta, "Comparative Study of Secure Vs Non-Secure Transport Protocols on the SIP Proxy Server Performance: An Experimental Approach", Conference on Advances in Recent Technologies in Communication and Computing (ARTCom), 2010, pp. 301-305.

[5] A. Alexander, A. L. Wijesinha and R. Karne, "A study of bare PC SIP Server Performance", Fifth International Conference on System and Networks Communication", 2010, pp. 392-397.

[6] Aditya Dakur and Shruthi Dakar, "Eavesdropping and Interception Security Hole and Its solution over VoIP Service", IEEE Global Conference on Wireless Computing and Networking (GCWCN), 2014, pp. 6-10.