# Proposing a New Solution to Reduce the International Roaming Call Cost

D.R. Ranasinghearachchi(✉), A.K.S.T. Chaminda,
W.M.D.H. Wanasinghe, and T.L. Weerawardane

Department of Electrical, Electrical and Telecommunication,
Faculty of Engineering, General Sir John Kotelawala Defence University,
Ratmalana, Sri Lanka
dumindurr@gmail.com, thilina.chaminda@gmail.com,
tlwkdu@gmail.com, wdilantha@ymail.com

**Abstract.** The cost of an international roaming call is high for majority of the countries. As a remedy for this, free VoIP services can be utilized, but both originating and terminating parties need to have suitable internet connectivity. Though, this issue is already addressed by certain VoIP services, by terminating the calls via lines owned by them, the call charges are still relatively high. This research paper is directed towards implementation of a cost effective solution for international roaming, where only the international roaming party requires internet connectivity and the local terminating party does not need internet connectivity. This roaming solution is assisted by the Public Switched Telephone Network (PSTN) line of a local fixed operator. The service architecture includes two components. The Customer Network (CN), which consists of a Customer Premises Equipment (CPE), VoIP Gateway (GW), Internet connectivity (preferably ADSL line) and PSTN phone line. The Provider Network (PN) which consists mainly of a Roaming Connectivity Server (RCS) and Call Accounting Server (CAS). Through this proposed system, the cost of originating a call when roaming can be reduced nearly to a local call charge. This solution will have marginal initial cost but still economical from customer point of view.

**Keywords:** Roaming · CN · PN · CPE · RCS

## 1 Introduction

International roaming is the primary option which is used by the roaming users while travelling to other regions. But in this method the calling cost is very high. So the subscribers are searching for a low cost voice call connection when roaming abroad, especially for official work, to talk to relatives, friends and other persons in the home country.

The roaming charges vary from operator to operator and country to country. Generally, these costs are predefined by the relevant operators (home network and visited network) according to business agreements between the two operator. These agreements depend on many aspects such as profit, taxes, cost of setting up connectivity between the two networks etc. If a roaming party latches on to a visited network whom with which the home network does not have an agreement with, the charges will be even higher.


R. Agüero et al. (Eds.): MONAMI 2016, LNICST 191, pp. 119–130, 2017.
DOI: 10.1007/978-3-319-52712-3_9

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. If the customer does not make the deposit, the charges are added until the customer's credit limit is reached, thereafter he/she will be barred from service.

The charges for originating and terminating calls when roaming, generally range from 5–20 times that of normal local call charges. But is some extreme cases these charges are 30–400 times higher than the local call charges.

As a solution for this issue, VoIP Services such as Skype and Viber can be utilized. But in this case, to generate a free call using these services both parties have to be connected to a stable internet connection to complete the call successfully. However, with the increase of data traffic and online applications, mobile network coverage might not be eligible to provide customers sufficiently. The above mentioned services also have the option to terminate calls using lines (PSTN/PLMN) owned by them for a certain charge. Yet these charges are relatively high compared to the proposed system in this paper.

Recently, the roaming costs between the European countries have been reduced drastically due to the EU roaming rules. But in the rest of the world, the costs are still too much high. A majority of these effected countries are developing countries. The proposed system is a solution mainly targeted towards the roaming subscribers of these countries.

Therefore, in this paper, we address the main problems which are high cost of roaming and the need of an internet connectivity for both parties. Through this concept, this solution will terminate the roaming call for any subscriber connected to the system at nearly the same cost of local outgoing call charges. This is beneficial for both single users as well as large scale organizations.

This system is an Over-The-Top (OTT) solution to reduce charges for internationally roaming users. It was developed solely with the roaming user's best interests in mind. Even though, it is targeted towards internationally roaming PLMN subscribers, this system negates the need of a PLMN home operator when roaming and relies on stable internet connectivity only on the roaming party's end.

In this paper, we'll be discussing how the node of this system are deployed. Section 2 will focus on the Conceptual Architecture. Section 3 will concentrate on the Customer Network (CN) portion of the system. Section 4 will discuss about the Provider Network (PN) portion of the system. Section 5 will elaborate on connectivity between the major nodes of the system. Section 6 discusses about the codecs used in the system. Section 7 talks about the deployment and testing to the system. Section 8 discusses result of the analysis. And finally Sect. 9 talks about the future work regarding this solution.

## 2 Conceptual Architecture

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 Inter-Asterisk eXchange (IAX) Trunks.

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 to maintain security and privacy between the separate CNs.

# 3 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. This PSTN connection will be used to terminate the user's roaming call to the destination number. 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. The two main components are the Voice over IP (VoIP) Gateway and the Customer Premises Equipment (CPE) (Fig. 1).

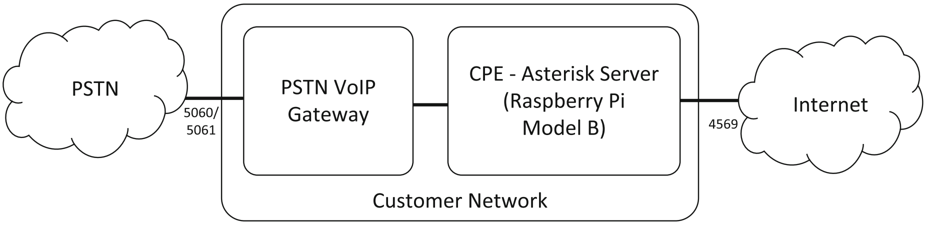


**Fig. 1.** Customer network components

## 3.1 Customer Premises Equipment (CPE)

The CPE is a low powered, low cost server running FreePBX. FreePBX is a Graphical User Interface (GUI) with Asterisk PBX server. This serves as a VoIP server within the CN which provide VoIP serves. And this also the main entity that provides IAX connectivity to the RCS for the CN. Additionally, this serves as a routing point which is used to connect to the VoIP Gateway of the CN.

## 3.2 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.

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.

# 4 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 entities to its relevant Customer Network via an IAX trunk which is established between the two networks. The Provider Network consists of several main components. This includes the Remote Connectivity Server (RCS), the Call Accounting Server (CAS) and a Mail Server. Of which the CAS and the Mail Server performing value added supporting roles such as generating Call Detail Records (CDR) and sending the said CDR to the relevant user (Fig. 2).

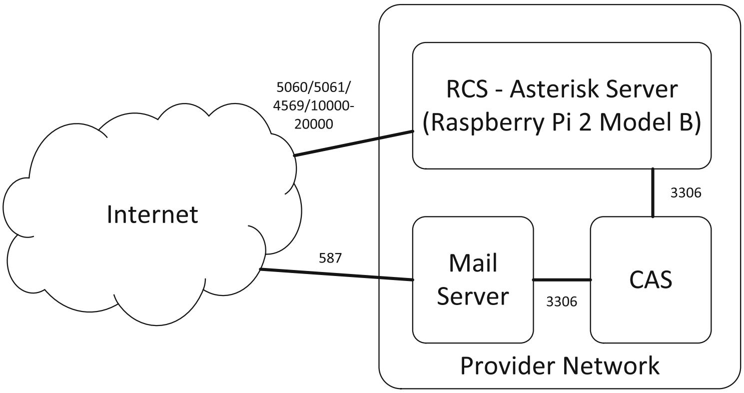


**Fig. 2.** Provider network components

## 4.1 Roaming 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.

The RCS runs 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].

# 5 Connectivity

## 5.1 Connectivity Between the CN and PN

In order to fulfill the primary function of this solution, 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 trunks has some advantages over SIP Trunks. (i) IAX uses less bandwidth than SIP. This is because the header size of the IAX packets are comparatively smaller than the SIP packet headers. (ii) In SIP the RTP packets are sometimes dropped during call sessions due to NAT issues. IAX was specifically designed to overcome issues caused by NAT by sending the RTP packets and the signaling together on the same channel. (iii) 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. Due to these reasons the IAX trunk is used connect the CPE and the RCS.

Taemoor Abbasi et al. [7], compared SIP and IAX signalling, structure, media transfer, signalling efficiency, and NAT issue. In this study, it was observed that, performance with packet loss of IAX is 24.70% higher than that of SIP. Also, performance with packet delay was 7.16% higher in IAX than that of SIP performance with packet reordering was 7.27% higher in IAX than that of SIP. Therefore, in general, IAX is better compared to SIP.

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 ports 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, When the PN is exposed to the internet rather than the CN, the PN serves as a first line of defense for the network and protects the CN.

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].

Another reason for connecting to the VoIP gateway via the CPE rather than connecting directly, is due to the fact that VoIP gateways that support IAX connectivity are rather expensive. Due to this, a low cost SIP VoIP Gateway is used.

## 5.2 Connectivity Between the RCS and the User

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 mobile device (with SIP compatibility). Once the user is connected to the system, calls can be originated to the home country via the system as long at the CPE is in operational state. The user simply needs to initiate the call to the desired terminating number and the call session will begin. The call will be terminated via the PSTN line at the customer premises, that is owned by the user.

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 3 illustrates the signaling flow between each node during a call.

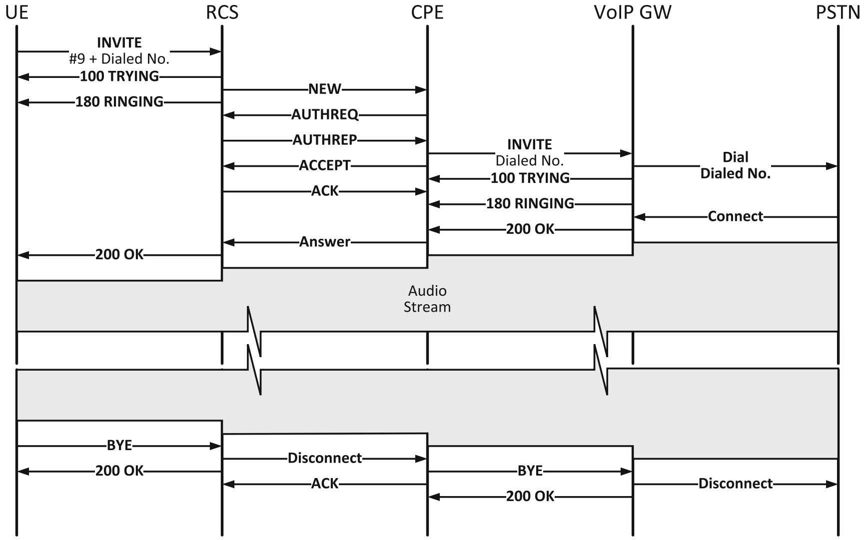


**Fig. 3.** Roaming user call initiation call flow

## 6 Codecs

During deployment, the default audio codec used was G.722 wideband codec. This codec has a bit rate of 64kbps. Due to its wideband property, this codec is used for high definition audio streaming between the nodes. The IAX Trunk between the RCS and the CPE, and the SIP connectivity between the RCS and the UE are configured to utilize the G.722 codec by default. The UE can use this codec only if it supports it. If the UE does not support G.722, the next alternative, G.711 will be used.

The VoIP Gateway used during testing (Cisco SPA3102) only supported G.711 narrowband audio codec. Therefore, all calls that were terminated within the CN and PN network had high definition audio support. Whereas all calls terminated to PSTN/PLMN subscribers were all subjected to the G.711 narrow band audio codec. Due to this the audio experienced when termination out via the VoIP Gateway was of narrow band audio quality.

## 7 Deploying the System and Testing

This system was deployed and tested in relatively controlled environment. The CN and PN were deployed in two geographically separate locations within Sri Lanka. Both of which had stable internet connectivity.

The primary goal was to reduce the roaming cost. Therefore, we wanted to keep the cost of the CN to a minimum. Due to this, the CPE was 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].

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.

For testing purposes, the RCS was deployed on a “Raspberry Pi 2 Model B”. 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.

When setting up the CN (CPE and VoIP Gateway), the user merely needs to connect it to the home network. Further configuration can be done via the CPE and VoIP Gateway web interface or by the PN via the internet.

For Android devices the native 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.

Finally, when the system was setup the operational architecture illustrated by Fig. 4.

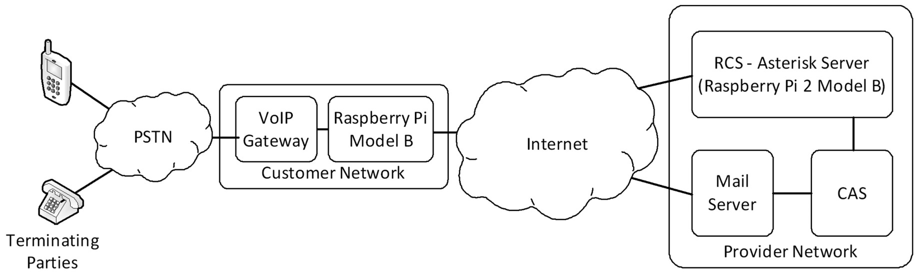


**Fig. 4.** Operational architecture

During the testing phase, the system was tested thoroughly. Data for call setup delays, bandwidth usage etc. where gathered. Moreover, the system was tested for relatively high loads. The RCS, with it Raspberry Pi 2 Model B was easily able to support 5–6 call simultaneously within its network without any sign of delay or packet loss.

Furthermore, the exposure of the ports of the PN to the internet caused many security issues. On three separate occasions, the system was encroached by hackers 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.

# 8 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. Additionally, we compared the call setup time and the average call costs on the proposed system and existing solutions such as Viber and Skype.

## 8.1 Data Usage of Roaming User

The data flow between the RCS and the CRE flows entirely in SIP and RTP. From the trace obtained from the RCS, we were able to analyse the data flow between the two nodes. The graphical interpretation on the data flow of a call of 2 min duration can be seen in Fig. 5.

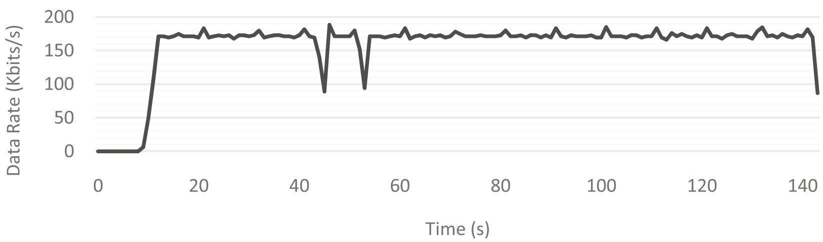


**Fig. 5.** Data usage of roaming user

From this analysis, we were able to calculate that, on average a 2-min call will have a usage of 2.7 MB of data. That is, if the roaming user takes a 10-min call, the data usage on average is 13.5 MB. This results in an average data rate of 23.04 kbps.

## 8.2 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. The graphical interpretation of the data flow of a call of 2 min duration can be seen in Fig. 6.

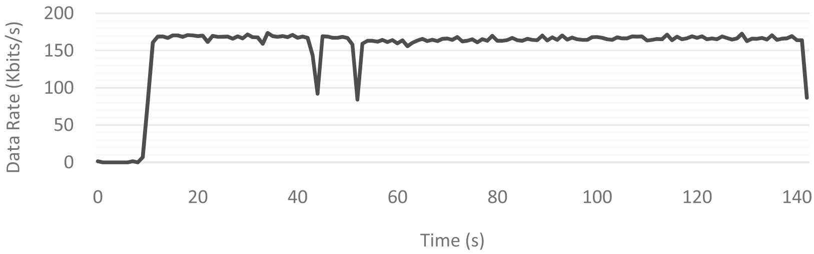


**Fig. 6.** Data usage of CPE

From this analysis we were able to calculate that on average a 2-min call will have a usage of 2.6 MB of data. That is, if the call session is 10 min long, the data usage at the CN is 13 MB. This results in an average data rate of 28.19 kbps.

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-min long calls can be seen in Table 1.

**Table 1.** Data rates and usages of 2-min 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 h 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.

The difference in the data rates is mostly due to the fact that the RTP and IAX media have different header sizes. i.e., RTP media has a header size of 12 bytes and IAX media has a header size of 4 bytes. This can be clearly be observed in Figs. 5 and 6.

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 s when initiating the call from WLAN or 4G connection. Generally, the time taken by the signalling within the CN and PN to setup the call is around 1–2 s. It is usually due to the signalling and setting up of security parameters between the nodes of the system [3, 4]. The addition delay is due to the in-band DTMF dialling of the VoIP Gateway and call setup time at the PSTN end.

### 8.3 Call Setup Time and Costs

The call setup times were analyzed during testing by initiating calls in the proposed system and existing VoIP services such as Viber and Skype. The out dialing functions were also tested. The results of these test are shown in the Table 2.

**Table 2.** Call setup time compared with existing services

| | | Call Setup Time (Seconds) | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Sample 1 | Sample 2 | Sample 3 | Sample 4 | Sample 5 | Sample 6 | Sample 7 | Average |
| Proposed System | VoIP | 2.64 | 2.10 | 1.74 | 5.12 | 7.12 | 1.83 | 3.40 | **3.42** |
| | Out | 9.16 | 8.84 | 8.26 | 9.00 | 11.75 | 9.62 | 6.96 | **9.08** |
| Viber | Normal | 4.17 | 3.74 | 4.58 | 4.05 | 4.13 | 10.19 | 9.94 | **5.83** |
| | Out | 8.39 | 17.90 | 9.10 | 7.80 | 7.34 | 13.30 | 12.43 | **10.89** |
| Skype | Normal | 3.34 | 4.21 | 3.67 | 3.98 | 4.23 | 4.42 | 4.32 | **4.02** |
| | Out | 9.82 | 8.76 | 9.24 | 9.54 | 8.43 | 9.23 | 9.14 | **9.17** |

The call cost during the test were recorded for comparison purposes. The following table illustrates the calling charge induced by the proposed system and by existing VoIP services such as Viber Out and Skype Out.[1] (Table 3)

**Table 3.** The call charges of proposed system compared with existing systems

| | | Call Charges (Per Minute) | |
|---|---|---|---|
| | | USD | LKR |
| Proposed System | Out | $0.03 | LKR 3.64 |
| Viber | Out | $0.23 | LKR 33.50 |
| Skype | Out | $0.41 | LKR 59.71 |

## 9 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.

To avoid security threats similar to that which was experienced during testing, VPN (Virtual Private Network) can be implemented between the RCS and the CPE, and an

[1] These result were obtained by tests done in Sri Lanka. These values were obtained during the month on September, 2016, and may be subject to change.

advanced firewall can be implemented to protect the RCS from threats from the internet. This will reduce the risk of the RCS being vulnerable to hacks and threats.

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 and VoIP Gateway efficiency.

As an additional functionality, the ability to show the roaming user's Caller Line Identification to the terminating party needs to be integrated to the system.

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.

## 10 Conclusion

This paper proposes a solution to reduce the roaming charges solely with the roaming user's best interests in mind. This concept reduces the call costs of the user when roaming nearly to the cost of local call charges. This is achieved through the support of the PSTN line owned by the user in the home country.

The roaming user merely need to use a SIP compatible device/softphone to connect to the RCS server via SIP protocol. After connection is established, the user can initiate call where they will be terminated out through the user's PSTN line in the home country.

Furthermore, the results show that this system is relatively cost effective compared to the existing systems.

## References


1. Zhuang, W., Tang, Y., Hu, Y.: Design and implementation of SIP B2BUA server. In: International Conference on Anti-Counterfeiting, Security and Identification (ASID), pp. 1–5 (2013)
2. Gallo, P., Levický, D., Bugár, G.: Authentication threats in PSTN-VoIP architecture using multi-service gateways, ELMAR, pp. 153–156 (2012)
3. Subramanian, S.V., Dutta, R.: Measurements and analysis of M/M/1 and M/M/c queuing models of the SIP proxy server. In: International Conference on Computer Communication and Networks (ICCCN), pp. 1–7 (2009)
4. Subramanian, S.V., Dutta, R.: Comparative study of secure vs non-secure transport protocols on the SIP proxy server performance, an experimental approach. In: Conference on Advances in Recent Technologies in Communication and Computing (ARTCom), pp. 301–305 (2010)
5. Alexander, A., Wijesinha, A.L., Karne, R.: A study of bare PC SIP server performance. In: Fifth International Conference on System and Networks Communication, An Experimental Approach, Conference on Advances in Recent Technologies in Communication and Computing, pp. 392–397 (2010)

6. Dakur, A., Dakar, S.: Eavesdropping and interception security hole and its solution over VoIP Service. In: An Experimental Approach, IEEE Global Conference on Wireless Computing and Networking (GCWCN), pp. 6–10 (2014)
7. Abbasi, T., Prasad, S., Seddigh, N., Lambadaris, I.: A comparative study of the sip and iax voip protocols. In: Canadian Conference on Electrical and Computer Engineering (2014)