Method for Securing and Terminating a CS Call over a VoIP System with Multi-Device Support

David Khoury*, Elie F. Kfoury[†], Joseph Ged[‡], Jorge Crichigno[†] and Elias Bou-Harb[§]
*Department of Computer Science, American University of Science and Technology, Beirut, Lebanon
[†]Integrated Information Technology, University of South Carolina, USA
[‡]Wone Sagl, 6906 Lugano, Switzerland
[§]Cyber Threat Intelligence Lab, Florida Atlantic University, Florida, USA

***Abstract*—The deployment of Over-The-Top (OTT) Voice over IP (VoIP) applications has been accelerated after the adoption of high-speed communications technologies (e.g.: LTE) by mobile operators. Additionally, the high incurring costs imposed on subscribers who are roaming outside their Home Public Land Mobile Network (HPLMN) has also contributed to the widespread coverage of OTT VoIP. As a result, mobile operators are witnessing a dramatic drop on their Average Revenue per User (ARPU). Current OTT VoIP apps fail to interwork with circuit switched phone calls without compromising the security requirements imposed by regulators on MNOs. In this paper we propose a method that secures a competitive edge for mobile operators over current OTT VoIP apps. It bridges the CS with PS networks and provides full control by the operator while maintaining the same security requirements. Moreover, we propose an additional feature for enabling multi-device reachability through the subscriber's phone number (MSISDN) which is provided by the mobile operator. The method's implementation verifies that the system has little impact on the mobile operators infrastructure. We finally conclude by providing potential business models for MNOs to increase their ARPU and outperform OTT VoIP providers**

***Keywords*—Circuit Switch; HPLMN; High costs; OTT VoIP; Regulators; Roaming; Security**

I. Introduction

Current voice calls provided by major mobile operators are established through a Circuit Switched (CS) network. This architecture, which relies on the Mobile Switching Center (MSC) located on the operators side, was adopted since the beginning of telephony and remains in use till today. Roaming solution specified by the GSMA standardization body is complicated and costly as every single leg of the calls' journey is charged by various terminating parties [1]. Even if the mobile operators are enjoying the high costs of roaming when their subscribers are outside their HPLMN, many clients are shifting to alternative solutions for voice communications based on VoIP [2]. The deployment of LTE network has accelerated the adoption of OTT VoIP applications, which lead to a dramatic decrease of the mobile operators' ARPU in the context of CS calls [3].

On the other hand, OTT VoIP services follow a custom addressing scheme and cannot interwork with CS-based calls. As a result, GSMAs vision of having one real global phone number (subscriber's MSISDN) reachable everywhere is no longer feasible. While some existing VoIP apps use the MSISDN as the user identifier (e.g.: WhatsApp [4], Viber [5], etc.), the VoIP communication still takes part over an IP channel, which is specific to the service provider and performed in a proprietary manner completely isolated from the CS open connected networks. Therefore, a proprietary application must be installed and configured on both the caller and the callee for setting up the call.

The VoIP service in LTE, also referred to as VoLTE (Voice over LTE), is controlled by the IP Multimedia Subsystem (IMS) profile standardized in GSMA IR.92 [6]. Similar to VoIP, VoLTE is based on the Session Initiation Protocol (SIP). However, the VoLTE services has not yet reached the same level of geographic coverage as the CS-voice due to many complications, especially, the coexistence of both systems and the smooth evolution (including roaming). VoLTE could not compete with OTT VoIP applications, even though it offers several improvements in the Quality of Service (QoS) compared to OTT VoIP.

Consequently, there is a need for an *inexpensive* solution for initiating and performing mobile voice calls that does not require the caller to subscribe to a particular service or install an application. This solution should also take part of the conventional mobile network system in a *transparent* manner without compromising the security requirements enforced by the regulators.

In this paper we propose a method that secures a competitive edge for mobile operators over current OTT VoIP apps. It bridges the CS with PS networks and provides full control to the operator while maintaining the same security requirements imposed by regulators. Specifically, we frame the paper's contributions as follows:

1) Minimizing the termination call's cost by forwarding the CS calls to a VoIP system when the user is roaming outside the HPLMN.
2) Global and seamless reachability through subscriber's MSISDN.
3) Deployment of Address of Records (AOR) to allow several devices to be reached instead of only the subscriber's User Equipment (U.E.)
4) Applying security measure to the IP leg of the connection while preserving full control to the operator over the calls (signaling and media), as recommended by regulations.

The rest of the paper is divided as follows. Section II provides some background on different technologies used in the method, while Section III discusses the related work. Section IV introduces the proposed system, its architecture and its components. Section V demonstrates the implementation and the results. Finally, Section VI concludes with the intended future work.

II. Motivation

According to Huawei Leading Edge issue 38 Feb 2008 Voice over HSPA [7], for the wireless and fixed networks offering VoIP services, the biggest difference lies in air interface resources. The development of wireless networks is mostly driven by the fact that wireless networks can provide greater service bandwidth with less spectrum bandwidth. The VoIP can be smoothly carried by a variety of technologies such as WCDMA, HSPA, HSPA+, LTE, or even the forthcoming 5G technology. Moreover, Klink et. al conducted a simulation to compare the bandwidth consumption for voice transmission in CS and PS networks [8].

Figure 1 shows a simulation results of bandwidth consumption for voice transmission in CS and PS networks.

The results show that VoIP consumes at least 20 percent bandwidth less than the CS. With the deployment of LTE network and all IP network, there are abundant capacity in the air interface and the bandwidth consumption of voice over IP calls represents a very small portion of the total bandwidth available in one cell (LTE a bandwidth of 100 Mbits compared to 1 Mbits per second for 100 users). The VoIP calls are charged per bytes which makes the VoIP calls very cheap compared to the CS.

III. Background

This section provides a background on several technologies and concepts used in the proposed system.

A. Session Initiation Protocol (SIP)

SIP is a signaling protocol used in VoIP systems to setup, maintain, and terminate voice calls between terminals [9]. It is based on the IP protocol, and can be ported on top of both transport layer protocols UDP and TCP.

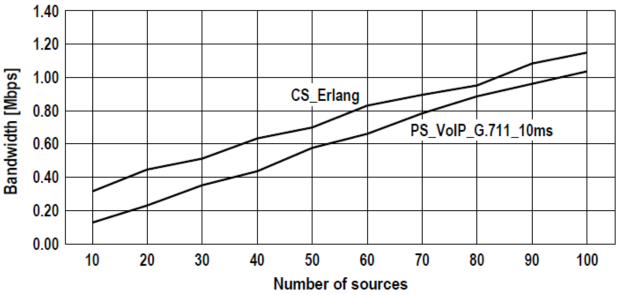


Fig. 1. Bandwidth Consumption for Voice Transmission in CS and PS Networks

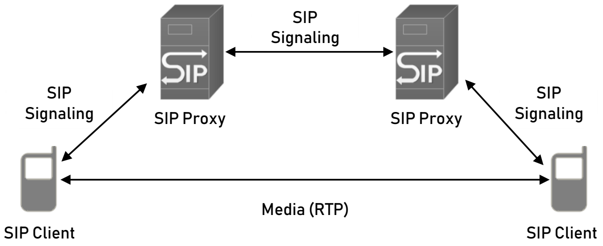


Fig. 2. SIP Trapezoid Architecture

Figure 2 depicts a typical SIP architecture, where SIP clients (U.E.) establish a call by allowing SIP proxies (servers) to handle the signaling. The media payload (voice) is then exchanged between the two clients directly, without going to the SIP server. Instead, the media typically goes to a media proxy which forwards the payload to the other end.

B. Mobile Switching Center (MSC) /GMSC

Figure 3 illustrates the operator's network architecture (3G UMTS R99). It is divided into two parts: Radio Access Network (RAN) and Core Network (CN). RAN provides UEs with radio access while CN connects access networks. The MSC is a switching node that routes voice calls and SMS messages. Its primary purpose is to set and release the connection between UEs in an end-to-end approach. Moreover, it handles mobility and hand-over requirements during the call.

The Gateway MSC (GMSC) is a node responsible for interfacing the PSTN. Therefore, all calls between mobiles and PSTN are routed through this node.

C. Direct Inward Dial (DID)

Direct Inward Dialing is a feature that allows subscribers to connect to their own private branch exchange (PBX) using trunk lines [10]. In a VoIP environment, DID numbers are usually assigned to a gateway, providing users of the public switched telephone network (PSTN) the ability to directly reach users with VoIP phones.

As shown in Figure 4, a mobile phone calling a DID number will be redirected to the VoIP gateway through the PSTN network. Afterwards, the VoIP gateway typically routes the call to an IP/PBX (SBC). SBC is a device deployed on the border of a VoIP network, to have access on the signalling and media between communicating units and interfacing the CS network. It is generally composed of a SIP proxy and a media proxy. An SBC is responsible for maintaining the full session state and offers additional features, namely, security, Quality

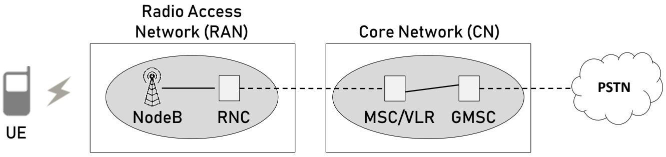


Fig. 3. Operators Network Architecture (3G UMTS R99)

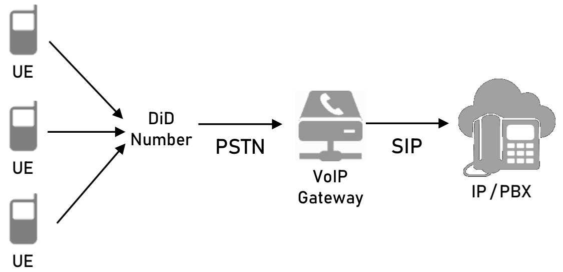


Fig. 4. VoIP DiD Scenario Architecture

of Service (QoS), regulatory, and media services (transcoding, DTMF relay, etc.).

D. CS and PS Interworking

The interworking between the CS network and the VoIP system are based on the protocol SIP-I/T according to the RFC 3398 [11] as shown in Figure 5. This RFC describes a method that is applicable in scenarios where a SIP call involves interworking with the PSTN. It maps the SIP signaling and the Integrated Services Digital Network (ISDN) User Part (ISUP) of the Signaling System No. 7 (SS7). In addition to the protocol mapping also the complete ISUP message is transferred (encapsulated). It is assumed that the receiving SIP User Agent can process ISUP. On the other hand, SIP Trunking enables the connection of SIP-based private branch exchange (IP-PBX) and the Internet telephony service providers (ITSPs).

IV. Proposed System

In this section, we describe an overview of the system architecture. Figure 6 illustrates the high level architecture of the system. The callee's device includes a SW-module which consists of a soft-phone (SIP client) connected to the Internet through any means of connectivity (WiFi, LTE, etc.). The SW module could be installed in any type of devices not necessarily a 3GPP UE. The subscriber's MSISDN (E.164) which is provided by the MNO is assigned to the SW module and mapped to an Address of Records (AoR). In SIP, AoR allows multiple devices to share one SIP address after being authenticated.

A. Configuration

The configuration steps of the SW-module are depicted in Figure 7. Initially, the SW-module on the callee's U.E. is installed (can be downloaded or integrated in the OS). Afterwards, the configuration proceeds as follows:

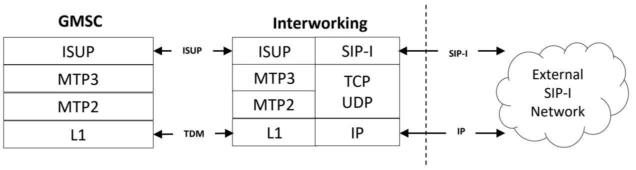


Fig. 5. CS/PS Interworking

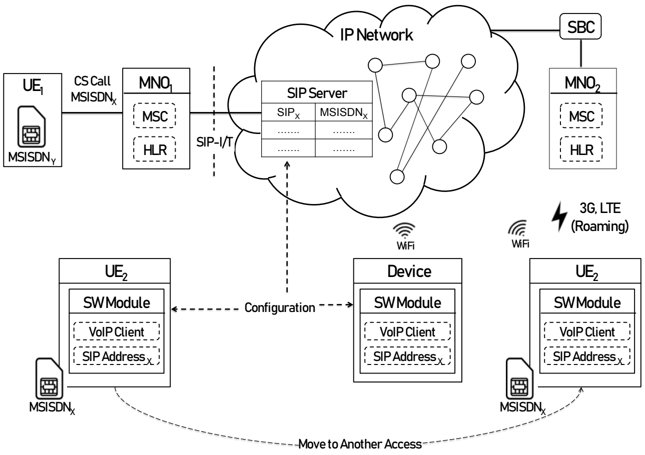


Fig. 6. System Architecture Overview

1) Upon starting the app for the first time, the SW-module prompts the device to specify the MSISDN. A request is then sent to the Configuration Server.
2) Optionally, the Configuration Server contacts the Home Location Register (HLR) to verify that the user has registered to the service.
3) The Configuration Server then generates a random PIN code, and sends it through SMS to the received MSISDN. It then waits for verification from the SW-module.
4) The SW-module prompts the user to input the PIN code, and sends a verification request to the server.
5) The server verifies the validity of the received PIN code. Then, it checks whether this is the first device trying to register to the service. If so, the SW-module is requested to create a new password for the SIP address. Else, the registration ends, and the SW-module redirects the user to the login screen.
6) The server then stores the SIP address which contains the MSISDN and the password.
7) When the registration is successful on the server side, the SW-module stores the credentials in the client device.

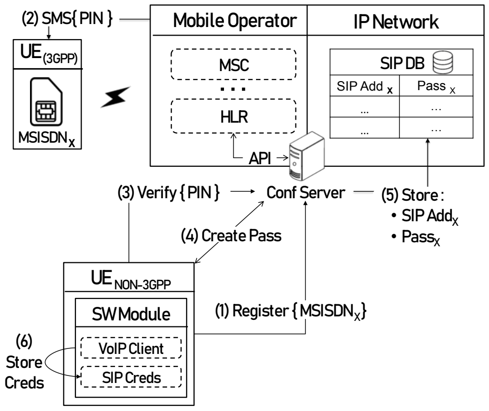


Fig. 7. SW Module Configuration

It is worth noting that the SIP address is not modified, and follows the standard specification of the SIP protocol.

Incoming CS calls are forwarded by the MSC to the SBC using Call Forwarding. To improve the user experience, the call forwarding function is automatically activated or deactivated by the Configuration Server whenever the user is roaming outside or inside the HPLMN. Moreover, the caller should not worry which number to call in order to reach the callee as the forwarding is done in a transparent manner.

B. CS to PS Call Setup

Outgoing calls from a UE (CS) are controlled by the MSC. In case the callee is roaming outside the HPLMN, the subscriber's profile is updated in the HLR/HSS. The configuration server then automatically activates call forwarding to the VoIP server. The role of the MSC became a forwarding node and a gateway to the SIP server. The caller initiates the call through the CS dial up user interface without the need for a dedicated application. Then, the call is routed from the MSC to the SIP server using SIP-I [12]. The SIP server finally forwards the call to the SIP client (Software module in the callee UE).

C. Authentication and Security

The proposed solution is designed to allow lawful interception, by keeping the same security requirements imposed by regulators on mobile operators. In other words, the call's journey should be secure and protected from interception in an end-to-access (e2a) method. The CS leg of the call is by default secured using the Authentication and Key Agreement (AKA) architecture [13]. However, the IP leg is vulnerable by default, and needs to be e2a secured.

To establish trust with the SIP proxy and to encrypt the channel between the SIP client and the SIP server, the Transport Layer Security (TLS) [14] is used as shown in Figure 9. For each established call, the MSC generates a random session key K_S (AES-256) and inserts it into the Session Description Protocol (SDP) part of the SIP INVITE. Specifically, it uses the `k=` field to insert the master key, which then is used as input to the Secure Real Time Protocol (SRTP) by the SIP client to encrypt the media streams [15]. Other more complicated methods for securing the media stream are discussed in [16] and [17].

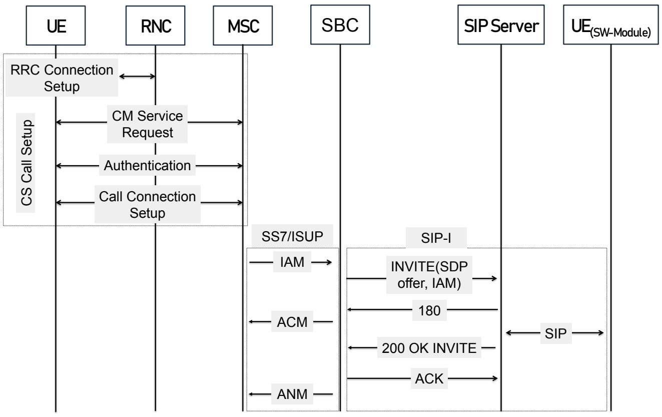


Fig. 8. Call Setup

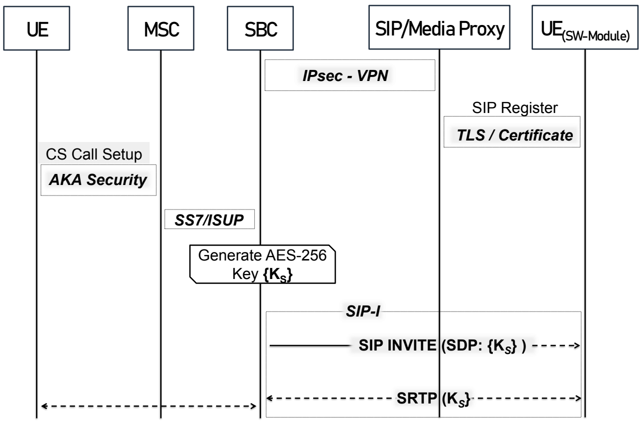
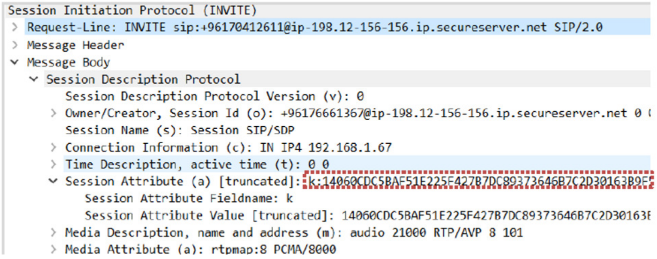


Fig. 9. Secure Call Setup

V. Implementation and Results

To validate the solution, we have built a standalone system without integration with a mobile operator. The system consists mainly of a SIP server, SBC node interfacing the PLMN/PSTN network and a VoIP application. The SIP server based on OpenSIPS [18]: Open source software which has the function of SIP proxy and RTP proxy: a media proxy used with OpenSIPS for relaying media streams, a Dispatching SBC also known as a front-end node and Registrar. The Registrar processes registration requests from customers IP phones and stores their location information. NodeJS: the Server side scripting for the Configuration Server [19]. The SBC is a device deployed on the border of a VoIP network, to have access on the signalling and media between communicating units. DID numbers are assigned by these SBCs to specific countries and provided to subscribers. The SBC is connected to the Application's SBC (SIP server) using SIP trunks.

We have used Voxbone's SBC interface for connection to the MNO through DID numbers and Twilio for SMS. The interconnection process with other carriers and customers becomes simple. The GMSC is used to route calls outside the mobile network. When a subscriber originates/receives a call to/from outside the home land mobile network, the call is



```
Session Initiation Protocol (INVITE)
 > Request-Line: INVITE sip:+96170412611@ip-198.12-156-156.ip.secureserver.net SIP/2.0
 > Message Header
 v Message Body
   v Session Description Protocol
       Session Description Protocol Version (v): 0
     > Owner/Creator, Session Id (o): +96176661367@ip-198.12-156-156.ip.secureserver.net 0 (
       Session Name (s): Session SIP/SDP
     > Connection Information (c): IN IP4 192.168.1.67
     > Time Description, active time (t): 0 0
     v Session Attribute (a) [truncated]: k:14060CDC5BAF51E225F427B7DC89373646B7C2D30163B9F
         Session Attribute Fieldname: k
         Session Attribute Value [truncated]: 14060CDC5BAF51E225F427B7DC89373646B7C2D30163E
     > Media Description, name and address (m): audio 21000 RTP/AVP 8 101
     > Media Attribute (a): rtpmap:8 PCMA/8000
```

Fig. 10. SIP invite with K_S in SDP

routed through the GMSC. The GMSC can connected to the IP network, specifically to the SBC, through SS7 or SIP with encapsulated ISUP (SIP-I).

The mobile application is built on SIPDroid client [20] which supports voice and video calls, and instant messaging. The subscribers register the application with their own mobile phone number MSISDN provided by the HPLMN. Once registered fetches a DID number from the SIP server and activates unconditional call forwarding to the DID number. For a single call the server needs to transfer 10-20 Kbytes of SIP signaling data, which is about 50 bps of the channel. If one call takes up 50 bps of the channel, 1000 calls can take up 50,000 bps which equals 0.05 Mbps. The bandwidth used by the RTP stream: 1000 calls using the G.711 codec [21] consume up to 163 Mbps of bandwidth. The 1,000 concurrent proxied calls must allocate a sufficient amount of bandwidth for signaling and for RTP proxying approximately 165 Mbps in total. Figure 10 demonstrates the packet capture of the SIP INVITE message on the SIP proxy using Wireshark network protocol analyzer.

VI. Conclusion

In this paper we have proposed a method that terminates a CS call over a VoIP system with multi-device support while providing the operator with full control over the security requirements. Implementation shows that the system has minimal impact over the operator's infrastructure as only a configuration server should be added. What we have developed is a method in Telecom that bridges the CS and PS network by using VoIP as the core communication engine for terminating circuit switched voice telephony securely under the MNO/MVNO control. The method offers global reachability through one global real phone number based on the E.164 standard, aiming at replacing the existing 3GPP roaming function of CS voice. As future work, the solution could be further developed to replace the roaming architecture standardized by 3GPP.

References

[1] J. S. Marcus, "Call termination fees: The us in global perspective," in *4th ZEW Conference on the Economics of Information and Communication Technologies, Mannheim, Germany*, 2004.

[2] GSMA, "The future of mobile communications." A GSMA Insight Report.

[3] "Mobile arpu hits seven-year low - the hindu businessline." https://www.thehindubusinessline.com/info-tech/mobile-arpu-hits-seven-year-low/article24373836.ece.

[4] K. P. O'Hara, M. Massimi, R. Harper, S. Rubens, and J. Morris, "Everyday dwelling with whatsapp," in *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*, pp. 1131–1143, ACM, 2014.

[5] T. Sutikno, L. Handayani, D. Stiawan, M. A. Riyadi, and I. M. I. Subroto, "Whatsapp, viber and telegram which is best for instant messaging?," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 6, no. 3, pp. 909–914, 2016.

[6] G. Association *et al.*, "Official document ir. 92ims profile for voice and sms," *Version*, vol. 7, p. 32, 2013.

[7] Huwaei, "Huawei leading edge issue 38 feb 2008 voice over hspa," tech. rep., Huwaei, 2008.

[8] J. H. Klink and T. Uhl, "Quality-aware network dimensioning for the voip service," in *2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pp. 1–6, IEEE, 2017.

[9] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "Sip: session initiation protocol," tech. rep., 2002.

[10] D. E. Woo and P. M. Barnett, "Direct inward dial integration apparatus," Mar. 7 1989. US Patent 4,811,381.

[11] I. R. 3398, "Integrated services digital network (isdn) user part (isup) to session initiation protocol (sip) mapping," 2002.

[12] G. Camarillo, A. Roach, J. Peterson, and L. Ong, "Integrated services digital network (isdn) user part (isup) to session initiation protocol (sip) mapping," tech. rep., 2002.

[13] M. Zhang and Y. Fang, "Security analysis and enhancements of 3gpp authentication and key agreement protocol," *IEEE Transactions on wireless communications*, vol. 4, no. 2, pp. 734–742, 2005.

[14] T. Dierks and E. Rescorla, "The transport layer security (tls) protocol version 1.2," tech. rep., 2008.

[15] M. Baugher, D. McGrew, M. Naslund, E. Carrara, and K. Norrman, "The secure real-time transport protocol (srtp)," tech. rep., 2004.

[16] E. F. Kfoury and D. J. Khoury, "Secure end-to-end volte based on ethereum blockchain," in *2018 41st International Conference on Telecommunications and Signal Processing (TSP)*, pp. 1–5, IEEE, 2018.

[17] E. F. Kfoury and D. J. Khoury, "Secure end-to-end voip system based on ethereum blockchain," *Journal of Communications*, vol. 13, no. 8, pp. 450–455, 2018.

[18] F. E. Goncalves and B.-A. Iancu, *Building Telephony Systems with OpenSIPS*. Packt Publishing Ltd, 2016.

[19] M. Satheesh, B. J. D'mello, and J. Krol, *Web Development with MongoDB and NodeJS*. Packt Publishing Ltd, 2015.

[20] N. S. SIPdroid, "Voip client for android."

[21] T. Daengsi, C. Wutiwiwatchai, A. Preechayasomboon, and S. Sukparungsee, "A study of voip quality evaluation: User perception of voice quality from g. 729, g. 711 and g. 722," in *2012 IEEE Consumer Communications and Networking Conference (CCNC)*, pp. 342–345, IEEE, 2012.