A Study On Signalling Protocols Of Voip Network

K.Narmatha [1], Dr V.Saravanan [2]
Department of Information Technology
[1] PG Student Hindusthan College of Arts and Science, Coimbatore, India
[2] HOD & Associate Professor, Hindusthan College of Arts and Science, Coimbatore, India

Abstract- *VoIP (Voice over Internet protocol) is becoming an attractive communications option for consumers. It is a technology that allows users to make telephone calls over an IP network. In the Secure voice call, the human voice shall be digitized by the Android APIs and the VOIP packets will travel over the SIP layer. The digitization process also includes the encryption phase wherein secure call technique is used in order to generate unique keys every time a call handshake is done. Basic VoIP access usually allows you to call others who are also receiving calls over the internet. VoIP technology reduces the operational cost with easier IT management for combined network for voice and data, which gives it an edge over PSTN (Public Switched Telephone Network). The major goal of the VoIP technology is establishing and managing communication sessions for transmitting both voice and data over a standard IP network. VOIP becomes vulnerable to different types of attacks such as Man in the middle attack, Denial of service or Eavesdropping. VoIP technology is feature rich to support next generation multimedia applications.*

Keywords- VOIP, Protocols, SIP, MGCP, MEGACO.

I. INTRODUCTION

Internet has no boundaries. Skype, Google Talk, Yahoo voice /video etc. are all applications that enable the use of the Internet for voice and video conversations. But these all are proprietary, and needs to have same software application on other end in order to established audio/video call. These propriety applications are more secure as they are passing all the information in encrypted format and optimization of protocols has been done nicely. But there is less scope for any modification in existing one. But true VoIP system does not require being dependable on single application.

Session Initiation Protocol (SIP) works on application layer and it is a text based signalling protocol. It is mostly used protocol in VoIP. It is text based protocol like HTTP. All SIP supported systems would able to established audio/video communication without having specific device or software. Just SIP supported software or hardware is needed. Many SIP User Agents (UA)/SIP clients are available in the form of soft phone, IP Audio phone, and Video IP phone. Now a day's smart phones also compatible to the SIP, so that we can even use our mobile phone in order to use VoIP services. We just need to connect them into the network/Internet. However, basic protocol for communication is Internetworking Protocol (IP). So this technology is known as VoIP (Voice/video over IP). It offers cost effective, flexible and scalable solutions, and due to these reason many new VoIP applications are coming into existence.

However, all forms of communications and original location of caller need to be monitored for security purposes to ensure their correct usage. With the development of more and more VoIP applications, monitoring and tracing of these applications is becoming a more difficult task. It is also difficult to provide emergency services (like 911 in us) using VoIP, as it is also requires identifying caller location.

Monitoring on ongoing communication can be achieved by lawful interception from server side, but most of the detection techniques are based on standard protocol and IP address identification. IP address doesn't provide actual location of caller; specifically in the form of latitude and longitude, and IP address may be spoofed, however it is not going to established the call in case of spoofed IP address. User may trick the server by using anonymous proxy servers. In that case server will have wrong IP address information. This paper presents generic techniques for detection of actual location of caller in public network. It also contains the proposed method that would be ideal for live tracking of SIP caller. Other associated terms with VoIP are IP telephony, Broadband telephony.

II. RELATED WORKS

This section describes the solutions for location identification of VoIP caller. This section also describes the issues associated with the explained solutions

GEO Track

This method uses traceroute mechanism to identify location of VoIP caller. After determining the path, the location will be inferred from the DNS names of router interfaces and the location of the last router is assumed to be estimate of the target host's location. [8, 9]

An analysis of Peer-to-Peer (P2P) VoIP calls was also presented by Xinyuan Wang et Al [6]. Most internet peer to peer VoIP calls are usually encrypted with different watermarks and anonymous identity and research has already been done to investigate the anonymity of the peer to peer data packets and how to pass them anonymously over the internet and with high level of encryption. Several other efforts on peer to peer have been carried out focusing on how peer to peer solution can impact the internet telephony system by comparing how particular P2P platforms perform call setup, call tear down, route calls and how the Network Address Translation (NAT) or firewalls are bypassed in environments with such facilities

Peer-to-Peer VoIP Solutions

Peer-to-peer (P2P) VoIP solutions provide an infrastructure where communication between parties involved does not pass through a third party after call setup as shown in Figure 3 above. Once the call is established, call traffic flows between the peers directly without going through a centralized server as in the SIP case. It's a technique designed to work in a decentralized server environment for better application sharing distribution. [14]. The P2P client software keeps a database of all the people they can talk to, select from a list, and connect directly to the other clients without going through a third party. Each peer acts as both a server and a client at the same time with full functionalities.

III. VOIP SIGNALLING PROTOCOLS

For IP telephony, a call can be prescribe as the multimedia session between multiple participants, while on the other hand signalling conjoined with a call is referred to as a connection.

Key roles of a signalling protocol can be divided into four functions:

- Session establishment : The callee decides, if to accept, reject or redirect the call.
- User location: The caller first has to find the location of the callee.
- Call participant management: It allows endpoints to join or leave an existing session.
- Session negotiation: The endpoints involved in the call should concur upon a set of properties for the session.

A. *H.323*

H.323 was published in 1996 and it is referred to as an umbrella standard that encompasses several other protocols which includes H.225 RAS signaling, H.225.0 call signaling (Q.931), H.245 Control signaling and others. Multipoint -multimedia or Point-to-point communication services is being provided by H.323 system when its four main elements- Multipoint control units (MCUs), gateways, Terminals, and gatekeeper, work together. It is Top-Down, very specific about protocol. The ITU-T (International Telecommunications Union) Recommendation H.323 protocol suite has evolved out of a video telephony standard. H.323 older and better deployed.

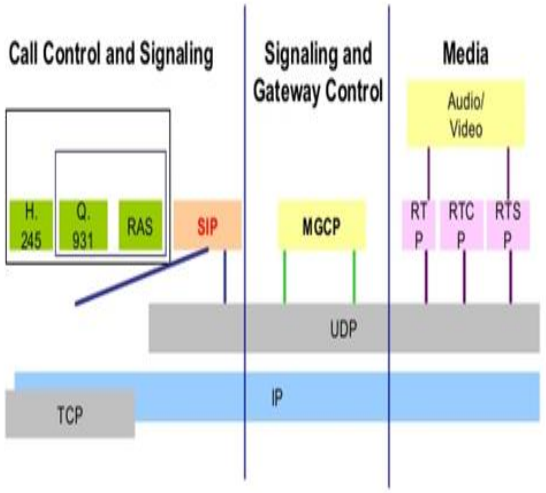

Fig 1: Pictorial Overview Of H.323

B. *SIP*

The Session Initiation Protocol (SIP)is similar to HTTP, is a communication protocol used for signaling and controlling multimedia communication and was defined by the Internet Engineering Task Force (IETF) for creating, modifying and terminating sessions such as online gaming, instant messaging and various services between two or more participants. These sessions are not limited to VoIP calls. It is a protocol that can set up and tear down any type of session. SIP generally uses port 5060 as its default protocol for either TCP or UDP. SIP growing rapidly due to ease of merging data and voice. SIP can be interpreted as the authorize protocol for voice, telephony and video over IP (VoIP) services. Server network elements are defined by SIP.

The main network elements involved in the SIP communication can be illustrated as follows:

Proxy server : It is a mediator entity which reacts as server (UAS) as well as client (UAC) for raising requests on behalf of various clients. It also performs routing to transmit the job assigned to another entity next to the targeted user.

User Agent : The User Agent (UA) is used in generating or receiving SIP messages. It can also act as User Agent Client (UAC) for transmitting SIP messages and the receiver will act as a User Agent Server (UAS).

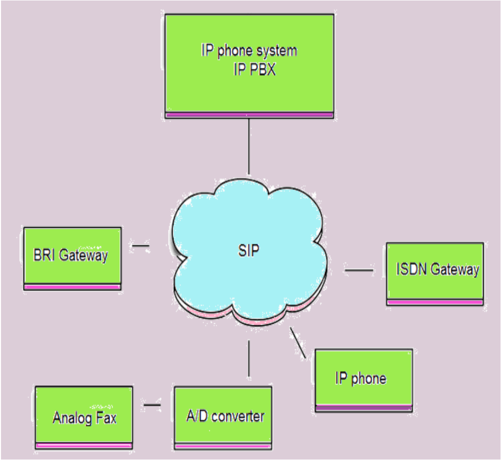

Fig 2: Session Initiation Protocol

C. *THE MEGACO/H.248*

MEGACO/H.248 is a MEdia GAteway COntrol protocol that addresses the requirements of decomposed gateways to achieve scalability and flexibility at low overall cost. The MEdia GAteway COntrol protocol uses context Id's to distinguish termination points. Megaco/H.248 provide mechanisms to interconnect with other VoIP networks, and also facilitate large-scale deployments of VoIP. It consists of the following important commands along with the flow direction:

Add: MGC ----> MG: The add command adds a termination point to a context.

Subtract: MGC ----> MG: The subtract command is used to remove a termination from a context.

Modify: MGC ----> MG: The modify command is used to change the property values, issue signals, or report specific events to termination points.

Move: MGC ----> MG: The move command is used to move a terminating from one context to another.

Audit Value: MGC ----> MG: The Audit Value command is used to obtain current values for properties, events and signals associated with terminations.

Audit Capabilities: MGC ----> MG: The Audit Capabilities command is used to obtain all possible values for properties, events and signals associated with terminations.

Notify: MGC <---- MG: The Notify command is used to inform the MGC about events that occurred within the MG.

Service Change: MGC <---- MG: The Service Change command is used to inform the MGC that a group of terminations are taken out of service.

Service Change: MGC ----> MG: When the group of terminations previously taken out of service, return back into service, the MGC sends this command to inform the MG to resume services.

D. *MGCP*

Media Control Protocols are responsible for the creation and tearing down of media connections. They are used to open and close media pin-holes on VoIP gateways and to process notifications coming from those gateways. The Media Gateways are the VoIP components that transport media between the IP and PSTN networks. They are controlled by an entity that is called Media Gateway Controller.

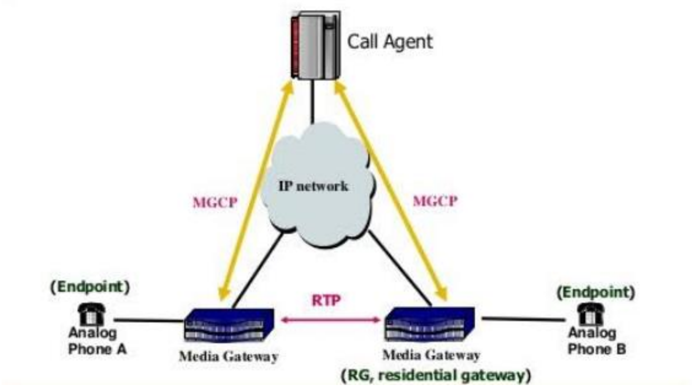

FIG 3: MGCP

IV. CONCLUSION

This paper has demonstrated the signaling protocols of VOIP.VOIP will replace standard telephony. The growth of VOIP going to continue more than this. VoIP nowadays enjoys the fruits of labours during the past few years and it can be considered a mature technology. Factors involved in designing a high-quality VoIP system include the choice of codec and call signaling protocol. None of the solution is passing location information in terms of latitude longitude except one solution, which was only useful for emergency call services which are integrated with PSTN. So for enhancing the security in terms of location identification, it is not that useful

In internet scenario, server needs to fetch exact location information in order to enhance security, and to provide live tracking functionality. Some Ideal Solution should be provided to provide location information in the context of security. It should provide accurate location information on the fly (live tracking should be possible) .It should provide location information even in the case if someone is using the anonymous proxy server to established the call.

REFERENCES

[1] Lu Tian, Nicolas Dailly, Qiao Qiao, Jihua Lu1, Jiannan Zhang, Jing Guo and Ji'ao Zhang (2010), "Study of SIP Protocol Through VOIP Solution of Asterisk", IEEE.

[2] Onofrei, A., Rebahi, Y. & Magedanz,T. (2010) „Preventing Distributed Denial-of-Service Attacks on the IMS Emergency Service Support through Adaptive Firewall Pinholing‟ International Journal of Next Generation Network.

[3] M. Desantis (2008), 'Understanding Voice over Internet Protocol (VoIP),' US-CER.

[4] E.Bernex,A.Gatineau,"Quality of service in VoIP environments", White Paper, www.neotip.com

[5] Geneiatakis, D., Lambrinoudakis, C. & Kambourakis, G. (2007) „An ontology-based policy for deploying secure SIP-based VoIP services‟, Computer & Security, 2006.

[6] Bhan, S., Clark, J., Cuneo, J., & Mejia-Ramirez, J. (2006) Information Security Issues in Voice over Internet Protocol. Available at http://users.ecegatech.edu

[7] Ghafarian, A., Draughorne,R., Hargraves, S., Grainger, S., High, S., & Jackson. (2007) Securing Voice over Internet Protocol‟ journal of information Assurance and Security, 2(2007).

[8] Chung-Hsin Liu and Chun-Lin Lo (2009), "The study of the SIP for the VOIP", Fifth International Joint Conference on INC, IMS and IDC.

[9] "Media Gateway Control Protocol (MGCP) Technology", Ixia, White Paper, 2004.

[10] A. Benyassine, E. Schlomot, H. Y. Su, D. Massaloux, C. Lamblin, and J. P. Petit, "ITU-T G.729 annex B: A silence compression scheme for use with G.729 optimized for V.70 digital simultaneous voice and data applications," IEEE Commun. Mag., vol. 35, pp. 64–73, Sept. 1997.

[11] B. Goode, "Voice Over Internet Protocol (VoIP)", IEEE Communication Magazine Sept. 2002.

[12] Zourzouvillys, T. Rescorla, (2009) "An Introduction to Standards-Based VOIP: SIP, RTP, and Friends", Internet Computing, IEEE.