DOI: http://dx.doi.org/10.26483/ijarcs.v8i9.5167

ISSN No. 0976-5697

Volume 8, No. 9, November-December 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

RESEARCH PAPER :VOIP PACKET ANALYZER FOR DETECTING THREATS IN SIP NETWORK

Ms. Toshima Singh Rajput
Department of Cyber law and Information Security
Barkatullah University Institute of Technology
Bhopal, India

Ms. Kamini Maheshwar
Asst.Professor,Department of Computer Science and Engineering,UIT,
Barkatullah University
Bhopal, India

Dr. Taruna Jain
HOD,Department of Cyber law and Information Security
Barkatullah University
Bhopal, India

Abstract: Video calls are increasing at a significant rate along with the voice calls, and the demand for cheaper call rates and services with low cost intensive technology is increasing. The scope of the research paper is to analyse SIP (Session Initiation Protocol) network using python sniffer program with new python library modules like pyshark and dpkt.This rich library of protocol intensive modules can help in the analysis of data packets transmitting over the network. It also helps in analysing the SIP (Session Initiation Protocol) data and extraction of RTP (Real Time Transport Protocol) data from the captured data packets and helps in the preparation of an effective software to identify Man-in the middle attacks.

Keywords: VoIP; SIP; RTP; Python library; dpkt;SIP network;pyshark

1. INTRODUCTION

Voice over Internet Protocol (VoIP) is still considered as one of the most dominant technology in the communication world. Its upgraded features has revolutionized the technology in using the Internet to make VoIP calls from desktop, laptop and smart phones at cheaper call rates. Its distinctive attributes include chats , voice, video calls using packets transmitted in a VoIP architecture platform along with the observance of some standard protocols specified by the telecommunication standards.

These services have scaled from small businesses to corporate networks with established channels of communication over private or public domains. It offers many advantages like

A person with limited technical know how can use an IP Phone to configure and install VoIP software.

Hosted Telephone systems can be used to add leased lines for every new employee added up to the business. Thus it ensures scalability of the service provided for businesses.

VoIP Services allow users to attach documents,conduct virtual meetings and share data via video conferencing .

With VoIP, call charges are nominal as the user can make unlimited free calls within a geographic area.

The hardware and standards designed to make, possible transmission of voice over IP Packets are:

ATA (Analog Telephone adapter) This adapter allows us to connect a standard IP/PBX system to the LAN using an Ethernet jack . The ATA communicates with the remote VoIP server by converting the digital signal to analog signal and vice versa. Plugging the IP Phone to this device will make it work.

IP Phones are normal phones with different connectors like instead of using RJ-11 connectors it uses RJ-45 connectors. These phones can directly connect to a router. WiFi phones can also allow their callers to make calls using WiFi hotspot.

Softphones are the easiest form of making VoIP calls. There are numerous low-cost software that we can use for using this service on our desktop or laptop.

VoIP standards was designed to transmit voices as packets over IP network. So, it can be used on data network like Intranet, Internet and Local Area Network.

The Protocols used in VoIP services are classified into

1. Signaling protocols
2. Speech Transmission Protocols
3. VoIP management Protocols

The signaling protocols are used to make phone calls over the Internet. They are used to establish sessions by setting and tearing down of calls. There are many signaling protocols like SIP, H.323, H.248, SS7(Signaling system 7), ISDN (Integrated Services Digital network).

The speech transmission protocols are classified into User Datagram Protocol(UDP), Real Time Transport Protocol (RTP) and Transmission Control Protocol(TCP)[1].

The standards and protocols for VoIP management are DHCP (Dynamic Host Configuration Protocol) , ENUM (Electronic Number Mapping system), RSVP (Resource Reservation Protocol) , BGP (Border Gateway Protocol) and COPS (Common Open Policy Service).[7]

The figure below shows a basic implementation of VoIP Protocols at different layers of TCP/IP Stack.

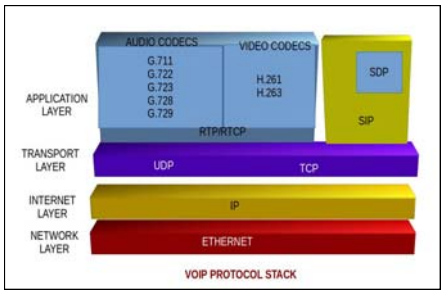

Figure 1. The protocol stack implementation of VoIP.

2. OBJECTIVE

The focus of the research was to sniff the wireless SIP network and analyse signaling protocols and media protocols used by softphone SIP Client service Providers and analyse the (Session Initiation Protocol) and Real Time Transport Protocol (RTP) protocol used for transmission of VoIP media services using a Python Packet Sniffer program.

3. SIP (SESSION INITIATION PROTOCOL)

SIP (Session Initiation Protocol) is an application layer control protocol developed by the Internet Engineering Task Force (IETF) to establish a bidirectional session for multimedia conferences, telephone calls and distribution of multimedia attachments. Its greater support for mobility, interoperability and multimedia made it scalable beyond VoIP calls.[1] It acts similar to HTTP with its request and response structure .This protocol is used to create sessions and to carry session descriptions that allow participants to agree on multimedia capability. The functions of this protocol are to :1) determine the location of an endpoint or user to be used for communication. 2) synchronize connection between the caller and the callee 3) establishing media parameters for a successful connection 4) in Progress changing the features of a session 5) adding, dropping packets, terminating sessions and invoking services[11]

SIP works in conjunction with other protocols to provide for a complete multimedia architecture like RTP (Real Time Transport protocol) or transmitting real time data along with Quality of Service (QoS) feedback, RSTP (Real Time Streaming Protocol) for delivery of streaming media. SIP works in conjuncture with SDP (Session Description Protocol) which provides a standard description of the networking environment, media details, transport addresses and other session description metadata. Thus in conjuncture with other protocols SIP provides services like conference controls, resource allocation, session description etc[[8].

A. Components of SIP

Few of the basic entities that are involved in SIP Exchange of services are:

1) User Agent Client(UAC) is an application that can initiate or terminate session through SIP request or Response structure. It can initiate up to six feasible requests to a UAS like INVITE(for call initiation), ACK (for call establishment), OPTIONS(to understand the capability of a user), BYE (to terminate the calling session), CANCEL (to cancel a request which is pending) and REGISTER(to redirect to the registered location of a user agent). When the SIP session initiates the UAC, it determines the essential information for the request including the protocol, the port and the IP address of the UAS to which the request is sent .This request URI is useful in determining the course of the SIP requests to its destination. When the UAC creates a SIP Request it must insert a via header which identifies the protocol name(SIP, protocol version, Transport protocol type(eg. UDP or TCP), IP address of the UAC and the protocol port(typically port 5060 or 5061)[7][8]

```
Via: SIP/2.0/UDP 10.0.2.20:5060;
```

2) User Agent Server(UAS) is a logical entity server that responds to the SIP requests from a UAC. It may issue multiple responses to the SIP request back to the UAC[2].

3) Proxy Server is a mediator and renders the request services to UAS or UAC. It acts as an organizational configuration through which SIP requests are routed before reaching the destination SIP client. It can also be used for name mapping for requesting a location service to map an external SIP identity to an internal SIP Client[2][][7].

4) Redirect Server allows for redirection to another geographic location but still can be contacted through the same SIP identity. The RTC (Real Time communications) server helps to implement the redirect and proxy server on one server. The SIP messages that will be processed through proxy or redirect server is determined through configuration settings on SIP Server. This technology enables rendering of services during maintenance of other servers[2][7].

5) Registrar server provides services for registration of the SIP client. SIP client sends a REGISTER request for change of an address to the registrar server which accepts the changes in the users address.

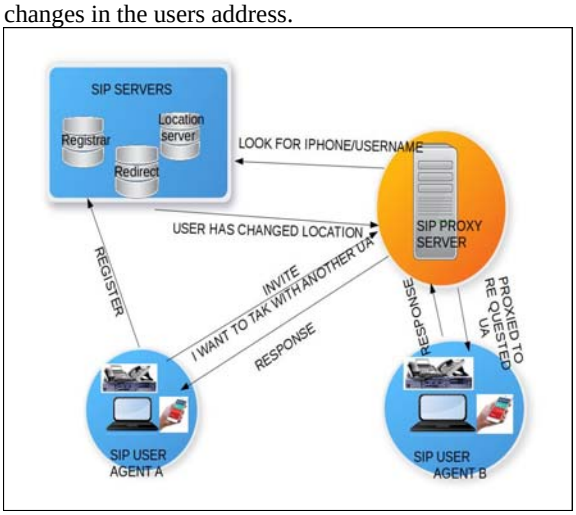

Figure 2. Flow of SIP connection between components

B. Sip Structure

SIP messages are of two types

a) Request ->sent from client to server

b) Response -> sent from server to client

SIP REQUEST MESSAGE consists of : a) Request method b) Request URI and c) Protocol version

SIP Request and Response messages utilises the basic structure specified in RFC 2822 and the character set specified in UTF-8 charset (RFC 2279).[[3]

Some of the basic signaling methods are:

Methods	Purpose
REGISTER	Binds users address to a location
INVITE	Initiate session along with session description
ACK	Confirms session establishment
BYE	Terminates sessions
CANCEL	Cancels a pending request
OPTIONS	Queries the capability of an endpoint user

SIP RESPONSE MESSAGE consists of a) Protocol version b) a 3-digit integer to indicate the output of an attempt to satisfy a request like 1xx class is for Provisional or Information Response, 2xx class for success , 3xx class for Redirection, 4xx class for Client error, 5xx class for Server error, 6xx class for Global error. These response codes show that server is performing some further action. c)Textual description that a user can read.[5]

C. Sip Header Format

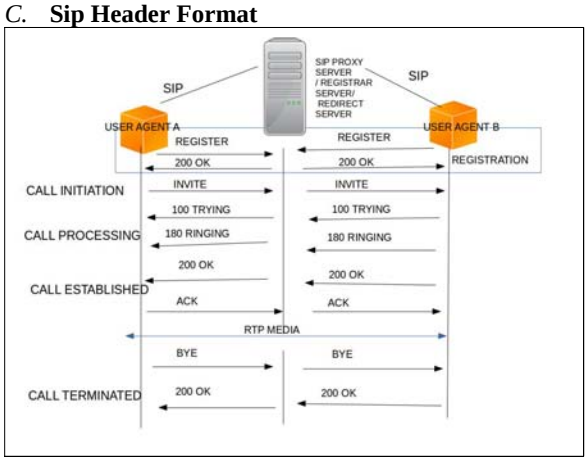

Figure 3. Illustration of an IP Phone call using SIP flow graph

SIP follows the connection flow through organized phases of transaction which starts with the registration of an user agent client with the SIP Server. The phases of each transaction passes through Call Initiation phase ,Call Processing phase , Call established state and then transmission of RTP Packet followed with the call Termination stage.[17]

D. Sip Protocol Architecture

It consists of four layers:1) In the lowest layer augmented Backus-Naur Grammar (BNF) form of encoding is used. This layer is so called as syntax and encoding layer. 2) The layer above syntax layer is Transport layer which defines how a client sends request and receive responses and works on how a server responds to the requests received. 3) The Layer above is the Transaction layer in which the Client transaction sends a request to a server transaction and gets the response back from the server transaction. Stateless proxies do not have transaction layer. 4) The layer above is the Transaction User requesting for SIP connection.

Thus SIP is structured as a layered protocol, which means its behaviour can be described in different processing stages which is loosely coupled.[6]

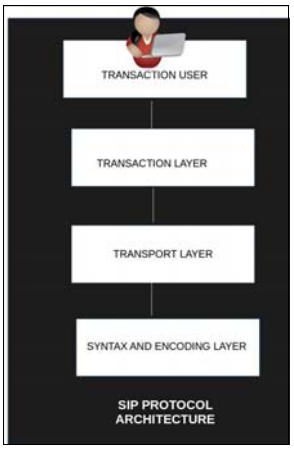

Figure 4. Illustration of an SIP Protocol architecture

4. REAL TIME PROTOCOL

This protocol is used for transmitting real time data such as audio and video or simulation data over IP network. The data is transported using Real Time Control Protocol (RTCP) which allows monitoring of data in multicast networks. This protocol supports the use of translators and mixers for audio and video simulated data transmission.

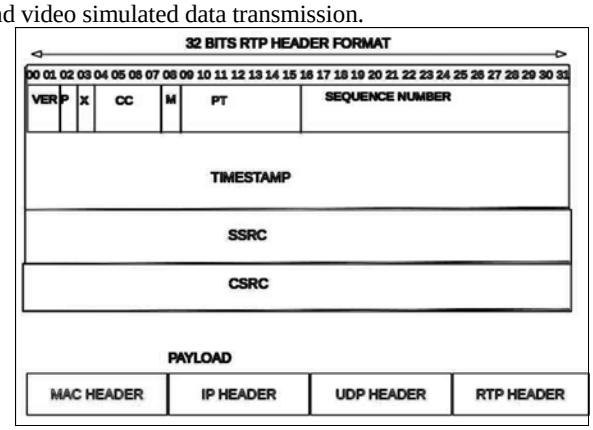

Figure 5. The protocol stack implementation of VoIP

The elements of the header are explained as below:

a) Ver is a 2 bit display of the Version number of the RTP which is always set to 2.

b) P-Padding, if the padding is set then it is of 2 bits and contains one or more additional padding bytes at the end. It contains padding bytes that is needed by some encryption algorithm with fixed block sizes for carrying several RTP packets in a lower layer protocol data unit.

c) X-Extension is of 1 bit which shows header extension.

d) Marker is of 1 bit which allows important events to be marked with frame boundaries in the packet stream.

e) Payload Type is a 7 bit field which identifies the format of the payload .A set of default payload types are defined by non RTP means.

f) Sequence number is a 16 bit field which identifies the RTP packet data sent and may be used by receiver to detect and packet losses during transmission.

g) Timestamp is a 32 bit sampling instant of the first octet in the RTP data packet. This instant is derived from the

clock that increments monotonically and linearly in time to allow synchronization. If an audio application reads 160 sampling periods from the input device the time-stamp would be increased by 160 for each block regardless of whether the data packet is transmitted or lost.

h) SSRC is a 32 bit which identifies the synchronization source .The value of SSRC is chosen as random so that no two synchronization sources within the same RTP session has the same SSRC.

i) CSRC Contributing source is of 32 bits which identifies the contributing source for the payload .Only 15 contributing sources are identified. They are inserted by mixers using the SSRC identifiers of contributing sources.[4]

Audio codecs are G.711, G.722, G.723, G.728, G.729 while video codecs are H.261 and H.263 used in a VoIP service platform.[2]

5. EXPERIMENTAL STUDY

The packet sniffer program uses the python library modules to analyse protocols to assess the security of a network. The following modules has been used in the program for sniffing VoIP packets from the Ethernet interface and analysis of SIP and RTP payload. The following describes the modules of the python sniffer program.

Pyshark is considered as a python wrapper for tshark a command line version of Wireshark which allows python packet parsing using Wireshark dissectors.

This uses the tshark's ability to export XML's to use its parsing. The module of a pyshark capture features Live Capture and File Capture to capture packets. Each of those captured objects has filters which can filter some of the incoming packets.

From a live interface data packets can be captured using sniff() method to capture a given amount of packets or sniff_continuously() method as a generator and work on each packet as it arrives.[12]

dpkt is a python module which allows simple creation of a packet or parsing of a packet with simple methods and has access to all the basic TCP/IP protocols. A study of the module helps in extraction of the protocols from a raw PCAP file.[13]

Netifaces module works on Windows as well as many UNIX like platforms. It helps the programmers to access all the network interfaces on the system to use their network addresses.[14]

Pygeoip is a python GeoIP API based on MaxMind's C based API which is used for finding the geographic location of an IP address. It provides the MaxMind's database of geographic location country wise and city wise.[15]

Socket is a python module which provides an access to BSD(Berkeley sockets division) socket interface. It is available on all platforms like Windows, Linux and other platforms. It is rich in system calls and library interface methods for socket programming. Various socket families are supported in this module.[16]

A. Observation:

The pcap files from G.711, G.722, G.726, H.264 audio and video codecs from Wireshark wiki has been used for the analysis of the packet sniffer program.

The output generated from the program helped the analysis of G.711 audio codec PCAP file for SIP data analysis.

```
INVITE sip:test@10.0.2.15:5060 SIP/2.0
Via: SIP/2.0/UDP 10.0.2.20:5060;branch=z9hG4bK-1966-1-0
From: "PCMU/8000" <sip:sipp@10.0.2.20:5060>;tag=1
To: test <sip:test@10.0.2.15:5060>
Call-ID: 1-1966@10.0.2.20
CSeq: 1 INVITE
Contact: sip:sipp@10.0.2.20:5060
Max-Forwards: 70
Content-Type: application/sdp
Content-Length:   123
```

Figure 6. The SIP data audio codec of G.711 PCAP file

The output from the program displays the data header of the SIP packet request and response message between UAC and UAS.[9]

```
From: "PCMU/8000" <sip:sipp@10.0.2.20:5060>;tag=1
To: test <sip:test@10.0.2.15:5060>
```

Figure 7. This figure shows the From: and the To: header of the SIP data

The From packet displays the IP source address from which the call request was sent i.e. from 10.0.2.20 to the IP Destination address 10.0.2.15 along with the display of the destination port 5060.The SIP call request and response port is normally 5060 or 5061 but varies depending on the kind of platform support.

The different SIP data displayed from the python sniffer program in different PCAP files of Audio codecs like G.722,G.726 are as follows:

```
********VOIP CALL ANALYSIS***************

 Source Port---->Destination Port

 5060----->5060
 ***Session Initiation Protocol data analysis**
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 10.0.2.20:5060;branch=z9hG4bK-2161-1-0
From: "G722/8000" <sip:sipp@10.0.2.20:5060>;tag=1
To: test <sip:test@10.0.2.15:5060>
Call-ID: 1-2161@10.0.2.20
CSeq: 1 INVITE
User-Agent: FreeSWITCH-mod_sofia/1.6.12-20-b91a0a6~64bit
Content-Length: 0
```

Figure 8. This figure shows the SIP data of G.722 data audioc codec PCAP file

```
 5060----->5060
 ***Session Initiation Protocol data analysis**
INVITE sip:test@10.0.2.15:5060 SIP/2.0
Via: SIP/2.0/UDP 10.0.2.20:5060;branch=z9hG4bK-2134-1-0
From: "G726-16/8000" <sip:sipp@10.0.2.20:5060>;tag=1
To: test <sip:test@10.0.2.15:5060>
Call-ID: 1-2134@10.0.2.20
CSeq: 1 INVITE
Contact: sip:sipp@10.0.2.20:5060
Max-Forwards: 70
Content-Type: application/sdp
Content-Length:   128
```

Figure 9. This figure shows the SIP data of G.726 data audioc codec PCAP file

The output of the program also displayed the sniffed RTP Packets. The Packet header format can be observed as follows.

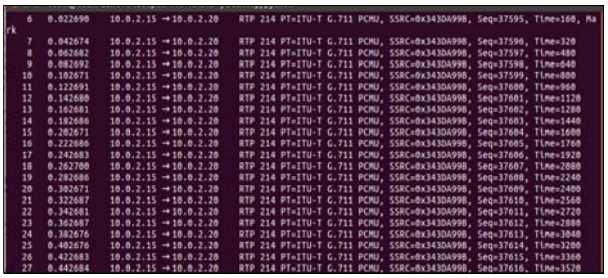

Figure 10. This figure shows the RTP packets of G.711 audio PCAP file

The RTP packet capture displays the time instance of the data packet captured ,IP Source to destination address , the Payload type, the audio codec , SSRC sequence no and the time taken to capture the data packet.

The VoIP SIP softphone service has been installed to capture live packets from the interface to analyse data. Communication between the mobile VoIP softphone and the desktop system VoIP SIP softphone services has been established for sending and receiving VoIP calls. The data packet that has been captured from the live interface after establishing communication between these two endpoint has been saved in SIP.pcap file. Wireshark is an open source software which has many filtering options and its command line version tshark is used for analysis of RTP packet[10].The flow graph observed in Wireshark software displays the following:

Figure 11. This figure shows the flowgraph of RTP packets of SIP.pcap file

The above flowgraph shows the RTP data packet details captured from the Live Ethernet interface of an SIP phone service through the sniffer program. The flow graph displays the connection flow between the source port to destination port along with different protocol packets including TCP, STUN ,SIP, and RTP.

6. ALGORITHM

Step 1 import dpkt, pcapy, pyshark, netifaces, socket, pygeoip modules
Step 2 Detect the interface used for sniffing packets
Step 3 Use pyshark module to capture live traffic from the interface for 50 seconds in an output file
Step 5 Editcap the captured file to proper PCAP files to remove the anomalies.
Step 6 Display the menu for choice
Step 6.1 if the choice is 1 then
  Step 6.1.1 Use the dpkt module to Capture the ethernet data
  Step 6.1.2 Use the dpkt module to Extract the ip data from the Ethernet data
  Step 6.1.3 Use the pygeoip module to display the geographic location of the data
Step 6.2 else if the choice is 2 then
  Step 6.2.1 Use the dpkt module to Capture the Ethernet data
  Step 6.2.2 Use the dpkt module to Extract the ip data from the Ethernet data
  Step 6.2.3 check if the destination port is 5060
  Step 6.2.4 print source port to destination port
Step 6.3. else if the choice is 3 then
  6.3.1Extract the RTP packets from the capture data using tshark with filter **-Y rtp** and output it to the screen or redirect to the file for analysis.
Step 6.4 Otherwise
  Step 6.4.1 print "Invalid choice"

The figure below shows SIP and RTP data analysis.

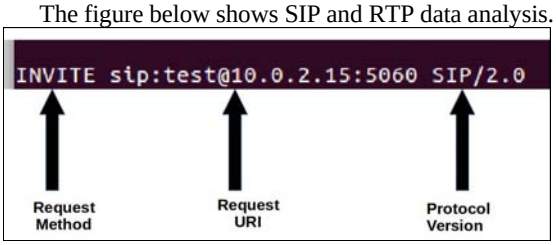

Figure 12. This figure illustrates the SIP data request header format

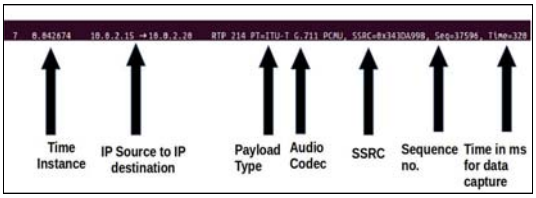

Figure 13. This figure illustrates the RTP data packet analysis

7. CONCLUSION

Thus Session Initiation Protocol (SIP) is a protocol that is a 3GPP (Third Generation Partnership Project) signaling protocol. The scalability ranging from IP phones to conventional telephone lines have rendered Communication services to rely on this protocol. It requires less set up time than its predecessor protocols. It helps to establish real time sessions. It's text based services allows ease of programming. The base of the protocol has been its implementation in the network level which makes it a peer-to-peer protocol. SIP will be a lot of promise for today and tomorrow in the communication world. SIP trunks can provide many advantages when business has multiple locations of establishments. It reduces the call rates whether you call locally or use company's SIP trunking system. The VoIP services like Skype, Linphone, Viber offers cheaper rates to make international calls. These services can easily adapt or upgrade their services to provide customer satisfaction. But with single trunk systems for multiple connections can often lead to loss of communication for the entire line at a single point of failure.[18]

Security has been one of the biggest issues in packet communication today. A hacker can hack into thousands of

computers, if the company does not practise proper security measures. Security in a SIP network should use the following parameters like Authentication, Authorization, Confidentiality, Integrity, Privacy and Non-repudiation which forms the basis of security essentials of any Network security algorithms. The SIP network can practise some security measures like Password and Access control mechanisms during proper call establishment, Encryption of the headers instead of carrying plain text headers which can be captured easily, use of strict record route during REGISTER and proper record routing implemented through the use of proxy servers address generated from the redirect server.

The sniffer program provides for data breach through man in the middle attacks as it helps to sniff IP Source and Destination address and helps in identifying the geographic locations of endpoints of connections.

Risk analysis and Quality of service using VoIP management protocols and its study will be the scope of further research in the SIP network.

8. ACKNOWLEDGMENT

I would like to express my sincere gratitude to my guides Prof. Ms. Kamini Maheshwar (Barkatullah University Institute of Technology) for providing proper support material to me in the preparation of the software and to my Head of Department in Cyber Law and Information Security Prof. Dr. Taruna Jain (Barkatullah University Institute of Technology) for the moral support and being a guidance counsellor.

9. REFERENCES

[1] Basma Basem, Atef Z. Ghalwash, and Rowayda A. Sadek, "Multilayer Secured SIP Based VoIP Architecture", International Journal of Computer Theory and Engineering , IJCTE 2015 ,ISSN: 1793-8201 ,Vol.7(6), pp.453-462, doi: 10.7763/ IJCTE.2015.V7.1002 .

[2] Sheetal Jalendry, Shradha Verma"A Detail Review on Voice over Internet Protocol (VoIP)", International Journal of Engineering Trends and Technology (IJETT), ISSN:2231-5381, V23(4), ,May 2015, pp. 161-166, published by seventh sense research group.

[3] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002, doi.10.17487/RFC3261, https://www.rfc-editor.org/info/rfc3261.

[4] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, July 2003, doi:10.17487/RFC3550, http://www.rfc-editor.org/info/rfc3550.

[5] Sheeba P, "Adapting SIP for Enabling Voice Calls in MANET", International Journal of Computer Science and Mobile Computing , IJCSMC, ISSN 2320–088X, Vol. 6, Issue. 3, March 2017, pp.191 – 195.

[6] Benju Xie, "Verification of Session Initiation Protocol Using Petri Nets, " International Journal of Engineering and Technology, vol. 4, 2012, pp. 416-417, doi: 10.7763/IJET.2012.V4.398

[7] Luan Dang, Cullen Jennings, and David Kelly, " Practical VoIP: using vocal" , O'Reilly, 2002, 2nd ed., ISBN 0-596-00078-2, pp.17-27.

[8] A. D. Keromytis, "A comprehensive survey of voice over IP security research," in IEEE communications surveys & tutorials, vol. 14, no. 2, Second Quarter 2012, pp. 514-537, doi: 10.1109/SURV.2011.031611.00112.

[9] Dimitris Geneiatakis, Georgios Kambourakis, Costas Lambrinoudakis, Tasos Dagiuklas, Stefanos Gritzalis, "A framework for protecting a SIP-based infrastructure against malformed message attacks", In Computer Networks, , ISSN 1389-1286, Volume 51, Issue 10, 2007, pp. 2580-2593, https://doi.org/10.1016/j.comnet.2006.11.014.

[10] Dr. Charu Gandhi ,Gaurav Suri , Rishi P. Golyan , Pupul Saxena , Bhavya K. Saxena "Packet sniffer – a comparative study" in International Journal of computer networks and communications security, IJCNCS, ISSN 2308-9830, vol. 2, No. 5, May 2014 ,pp. 179-187.

[11] Rahul Singh and Ritu Chauhan, "A Review Paper: Voice over Internet Protocol" International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471, Vol. 3, Issue 1, January-2014, pp.15-23.

[12] Kiminewt, "Pyshark", https://kiminewt.github.io

[13] Dug Song , "dpkt" , https://github.com/kbandla/dpkt

[14] Alastair Houghton, "netifaces" , https://pypi.python.org/pypi/netifaces/0.8

[15] Jennifer Ennis, "pygeoip" , https://pypi.python.org/pypi/pygeoip/0.3.2

[16] Gordon McMillan, "Socket Programming HOWTO" , https://docs.python.org/2/howto/sockets.html

[17] Urjashee Shaw and Bobby Sharma. Article: A Survey Paper on Voice over Internet Protocol (VOIP). International Journal of Computer Applications April 2016. Published by Foundation of Computer Science (FCS), NY, USA,139(2) , pp.16-22, doi: 10.5120/ijca2016909112.

[18] Janne Magnusson, "SIP Trunking Benefits and Best Practices" White Paper, https://www.ingate.com/files/white_paper_What_is_SIP_Trunking_A.pdf