International Journal of Research
ISSN: 2348-6848 Vol-3, Special Issue-3
International Conference on Research and Recent Trends in Engineering and Technology. (ICRRTET)
Held on 27th January 2016 organized by **Sai Polytechnic College,** Kinhi Jawade, Yavatmal, Maharastra, India.

A Comparative Analysis and Design of TCP\SCTP for Secure Voice Communication Protocol

AUTHOR NAME

Prof K.V. Warker
Pallavi Mude
Surabhi Rathi
Radhika Bajaj
Pallavi Mude
Rashi vidhwani
Shubhangi Satdeve

ABSTRACT

Voice over Internet Protocol (VoIP) is a growing Communication and Information technology that assists voice communication through the Internet. VoIP is becoming popular due to their cost effective service and convenience. A VoIP technique has two significant features i.e. Privacy and QoS of the network. Unfortunately, most VoIP network doesn't provide Privacy as well as QoS to the end user. A work has done previously on Security and Quality of Services for VoIP applications, yet these issues has not been completely solved. To overcome these issues in VoIP proposed a novel phenomenon i.e. permutation of Stream Control Transmission Protocol (SCTP), Advanced Encryption Standard (AES) and Secure Hash Algorithm -1 (SHA-1) for Client-Server model. Here, AES and SHA-1 are used to afford secrecy. As well as SCTP transmission algorithm would be intended to raise the QoS for VoIP.

INTRODUCTION

1.1 Background:

1.1.1 IP Telephony:

Internet Protocol Telephony (IP telephony) is a technology which provides voice communication over the network. It conduct telephone call using packet switch base network. It is also known as "Voice over Internet Protocol (VoIP)". It is design to swap traditional circuit switched based network. It is fully depend on Internet Protocol instead of telephone line like circuit switch based network [1].

In VoIP travels call as a packet of data. The task in VoIP is to transport speech packet in a reliable stream. The chief benefit of IP telephony is that long distance call is also on

regular cost. VoIP is a significant quantity of the union of telephones and computers into a solitary united information atmosphere.

Two protocols are employed in IP telephony, one for signaling and second for transport purpose. Basically transport of packet is offered by TCP or UDP and signaling in which call is establish, terminate, forwarding etc. done using signaling protocol which are similar to SIP or H.323 [2].

1.2 Overview:

1.2.1 VoIP:

Now a day, Information and Communication technology plays momentous role to communicate over the Internet. VoIP is also a technology which attained award of proficient communication technology in the communication world. In additional it is also having an exponential innovation in Internet world. VoIP endows speech conversation through Internet. It is also called as IP Telephony which lets calls correspondent to large distance, International and local at small charges [4]. VoIP sends packet via Packet Switch Base Network. This speech packet data is entirely reliant on Internet and doesn't require traditional telephone line. Besides, PSTN is immovable on circuit switch base network and it imposes devoted link for communication [3].

Table 1.2.1 Comparison between VoIP and PSTN

Feature	VoIP	PSTN
Switching	Packet switching	Circuit switching
Cost	Cheap	Expensive
Connectivity	Internet Connectivity	Dedicated telephone line
Reliability	Less Reliable	More Reliable
Path	No dedicated path	Dedicated Path
Scalability	Update require more bandwidth and simple software update	Update require more hardware which can be more costly and complex

Analog data is rehabilitated into digital data format. By using Internet this data is consignment from one terminal to another. Finally, this digital format data is turned into analog data at receiver [5]. IP Telephony network is dissimilar from traditionalist telephone network in which voice data superiority is extravagant via variety network inadequacies such as packet loss, delay, end to end discussion, jitter, network secrecy and throughput. Therefore, communication quality is not commendable as acquaintance to probable telephone route in VoIP. Hence, to confiscate quality of service (QoS) and Privacy associated hitches are crucial work in IP telephony.

Table 1.2.2 Advantages and Disadvantages of VoIP

Advantages	Disadvantages
Low cost.	Users cannot make calls during power outages.
Free VoIP calls from anywhere for long distances or international calls.	Emergency calling is not provided by VoIP. IP network does not provide guarantee quality of service.
More scalable.	Depends on Internet connection condition.
Easy to implement and install.	IP network that does not guarantee Quality of Service for voice communication.
Integration with other available services over the Internet.	
Flexibility	

1.2.2 Issues of VoIP:

- Delay occurs during packet transmission process from source to destination.
- More variation in the delay among successive packet i.e. Jitter.
- Throughput is less.
- Rate of packet loss is high.
- Packet incoming excessively late at the destination side [6].
- Echo sound is also generated during conversation.
- Frequent discontinuation among sender and receiver.

1.2.3 VoIP Component:

VoIP consists of three essential components.

- Codec (Coder/Decoder)
- Packetizer
- Playout Buffer

- **Codec:**
  The utility of codec is to wrapping and encodes the analog speech into digital speech. Codec bid good worth of speech even after compression with tiniest delay [6] [7] [8].

- **Packtetizer:**
  Fragments of encoded speech are crammed into persistent bit rate speech packets via packetization progression [6] [7] [8].

- **Playout Buffer:**
  It is place at receiver end. It imposes speech frames to be decrypted at the same intermission at which they were produced by the encoder. There are two types of playout

buffer i.e. Adaptive and Fixed. Adaptive playout buffer delay based on the networking circumstances and network delay is perpetual in fixed playout buffer [6] [7] [8].

Problem Definition:

VoIP over wireless LAN (WLAN) network appearances huge challenges like confidentiality and quality of services (QoS) disputes due to the loose environment of WLAN. Moreover, real time applications necessitate moral speech superiority. To provide appropriate balance between QoS and Confidentiality for the speech data is the decisive to the achievement of any VoIP deployment. Here, VoIP network needs quality of service in terms low delay, low jitter and high throughput.

Objective:

- Our objective is to study numerous qualities of services and secrecy concerns in VoIP and their effect on the communication data.
- Study several technologies to overcome VoIP glitches and implement more effectively in our VoIP network.
- To develop durable connection between source and destination for reliable data transmission.

LITERATURE SURVEY & REVIEW

Many researchers have worked on Secrecy and Quality of Services (QoS) disputes in VoIP network to address numerous restrictions. In this sections several techniques have been studied which is used in VoIP. Security as well as Preserving QoS of the network is major challenging task in VoIP system.

Wireless LAN (WLAN) is the fundamentally structured wireless technologies all over the world. WLAN architecture is equivalent to Local Area Network (LAN) but communication ensues in WLAN by Radio frequency (RF) or Infrared (IR) and by physical lines in LAN. Cost effectiveness, Simplicity, Scalability and Mobility are the main characteristics in WLAN. WLAN carries association using IP and VoIP applications are also successively running through Internet Protocol.

2.1 Hybrid Network:

The determination of hybrid network in VoIP is to offer security for VoIP system. This network is able to afford safety for high latency conversation via routing network traffic. But, it doesn't offer quality of services desires. It is unable to offer both secrecy as well as quality of services at a time. Here, user plays a router roll which obscures the scheme. Also, it is accountable to disruptions the perception of sharing work on the unalike element of the network. Moreover low latency applications on unify network may be susceptible to Timing Analysis Attack [1].

2.2 P2P Network:

Peer to peer (P2P) network offers neither personalization nor assurances a measurable safety level. This P2P frequently involves of a core proxy and a fixed of patrons that are attaching to the brink of this core proxy. In P2P, each user acts as a client and server. Therefore any one of these two exposes its identity then entire network will be insecure [2].

2.3 Random Walk Search Algorithm:

This algorithm is corresponding to route setup protocol. Four typical stages are executed under random walk protocols which are initSearch, processSearch, processResult and finSearch. Shortest outlet is not screening by this algorithm. Habitually, this algorithm doesn't indeed opportunity shortest street intimate any two nodes [3] [2].

2.4 K-anonymity algorithm:

This algorithm is sustenance to build surreptitious network. Stream of packet is not analyzed by third party in it. Consider S as a sender (source) and R as a receiver (destination). Voice packet data are prerequisite to exchange over superior network. This superior network grasps proxy nodes. Thus, third party can acquire voice conversation merely from proxy node [4].

2.5 Authentication Techniques:

Authentication is the important phenomenon in any service associated network which respites to distinguish and remove any dishonest network accessory. For IEEE 802.11s and 802.11i centralized server is obligatory for authentication phase. But, centralized server endeavors as a third party. It also inhibits discrete activities and thus suffering scalability concerns [5].

2.6 Encryption Technique:

In comparative study associated with AES, RC4 and DES. AES is additional active than RC4 and DES in families of packet loss, delay and throughput. Using codec in VoIP analog speech packet data is rehabilitated into digital speech packet data. Then these packet data undoubtedly encrypt and decrypt using Advanced Encryption Standard (AES) algorithm [6].

2.7 Transmission Technique:

Characteristically User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) is used for assigning data from one terminal to another terminal [2].

UDP is a connectionless protocol. It is not launch any association among interactive end users. Also, there is no any privacy mechanism in UDP. In UDP Packets may be delivered or not.

TCP is a connection oriented protocol. It launches association among end to end user using 3-way handshake technique. 3-way handshake technique also helps to secure transmission of data [2] [6]. However, TCP never assurances that a packet reaches in require time. It happens due to segmentation. TCP need segmentation when frames are longer than MTU [1] [7].

2.8 H.323:

H.323 is a protocol standard, which is offer real time audio as well as video multimedia conversation over packet network. It is provision to session establishment and transforming mechanism. To maintain quality of services (QoS) is the significant feature of H.323.

2.8.1 H.323 involves four types of constituent:

- **Terminal:**
  Terminal is usually a software or hardware in VoIP. It is useful for real time bidirectional conversation.

- **Gateways:**
  It sanctions bidirectional conversation within disparate devices network.

- **Gatekeepers:**
  In H.323 network, gatekeeper is considered as a central controller. Registration of end points and session admittance are the imperative assignment of gatekeeper. It also manages set endpoint which is called as zone.

- **Multipoint conference unit (MCU):**
  It provides multiparty conferencing within H.323 terminal. In MCU involves two functions i.e. Multipoint Controller (MC) and Multipoint Processor (MP). This function is liable for fraternization the audio as well as video channels during conferencing [8] [9].

2.9 Session Initiation Protocol (SIP):

It is an application layer end to end signaling protocol for Internet telephony. It provides instigating, transforming and ending real time user's session. SIP protocol empowers one user to place a call to another user.

SIP implemented on IPv4 as well as IPv6 which helpful to reduces overhead, thus speeding performance. SIP uses proxy in their communication message. Proxy deeds as an intermediately system, once the call is create between both participants the communication perform without including proxy [10] [11] [12].

2.9.1 Essential SIP functions for VoIP system:

Table 2.9.1 Function in SIP

Function	Description
User location with registration	SIP accomplishes which end-point will join in a call and end-point warns SIP proxies to their locality.
User availability	End-point uses SIP to elect whether they will "answer" a call or not.
User capability	End-point uses SIP to convey media competencies.
Session setup	Point to point call is established by approve session constraint.
Session management	In this step call is transfer and terminate, amending call constraint using SIP.

System Flowchart:

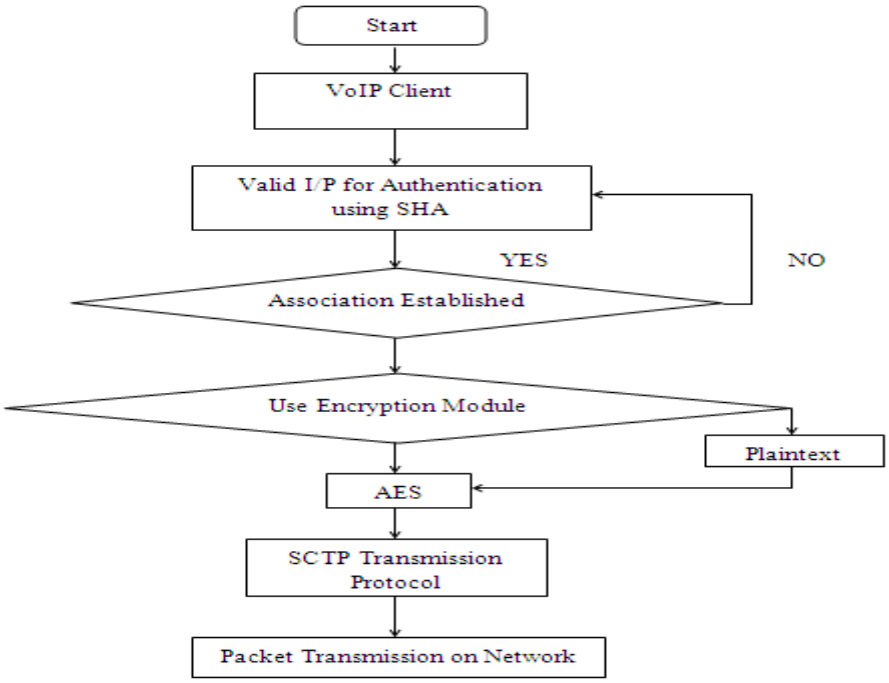

Fig. 3.1 Flow of propose system

References

[1] Prashant N. Kubde and N. A.Chavhan, "Improve Privacy and Performance of QoS Parameter for VoIP Applications over Client-Server Networks," IEEE International Conference on Engineering an Technology (ICETECH'15), pp.388-391, Mar.2015.

[2] M.V.Sreeraj, T. Satya Savitri, "SCTP and FEC based Loss Recovery Technique for VoIP," International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering Vol. 2, Issue1, January 2014.

[3] http://www.webopedia.com/TERM/I/ip_telephone_system.html.

[4] http://www.pcmag.com/encyclopedia/term/45379/ip-telephony

[5] Haniyeh Kazemitabar, Sameha Ahmed, Kashif Nisar, Abas B Said and Halabi B Hasbullah, "A comprehensive review on VoIP over Wireless LAN networks," 2009-2012 All rights reserved. ISSR Journal 2010.

[6] Mrs. K. Maheswari, Dr. M. Punithavalli, "Receiver Based Packet Loss Replacement Technique for High Quality VoIP Streams," 978-1-4244-5612-3/09/$26.00, 2009 IEEE.

[7] Preetinder Singh and Ravneet Kaur, "VOIP Over Wimax: A Comprehensive Review," International Journal of Computer Science and Information Technologies, Vol. 5 (4), 2014, 5533-5535.

[8] Haniyeh Kazemitabar, Sameha Ahmed, Kashif Nisar, Abas B Said and Halabi B Hasbullah, "A comprehensive review on VoIP over Wireless LAN networks," 2009-2012 All rights reserved. ISSR Journal 2010.

[9] http://en.wikipedia.org/wiki/Infinite_impulse_response.

[10] http://www.dspguru.com/dsp/faqs/iir/basics.

[11] http://music.tutsplus.com/tutorials/filters-and-you-iir-filters--audio-23061.

[12] http://en.wikipedia.org/wiki/Real-time_Transport_Protocol.

[13] http://searchnetworking.techtarget.com/definition/Real-Time-Transport-Pr.

[14] http://www.techopedia.com/definition/4755/real-time-transport-protocol-rtp.

[15] http://en.wikipedia.org/wiki/Client–server_model.

[16] http://www.webopedia.com/TERM/C/client_server_architecture.html.

[17] http://www.techopedia.com/definition/438/clientserver-architecture.