Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.4, No.10, 2013

Voice over Internet Protocol (VoIP) Performance Analysis, QoS Measures to Minimize Packet Loss, and Identifying Link Failures during Transmission

Lalitha R.V.S, Asst.Professor
Sri Sai Aditya Institute of Science and Technology
E-mail:rvslalitha@gmail.com
Pavani N
Sri Sai Aditya Institute of Science and Technology
E-mail:pavaninarala@gmail.com

Abstract
VoIP is the recent step of telephony evolution. VoIP stands for Voice over Internet Protocol packets. Voice over the IP network is a general term that refers to any means of converting voice calls into voice data packets that are transmitted over an IP network, either public or private. PSTN is circuit switched and VoIP is packet switched. In circuit switching irrespective of amount information to be sent, full bandwidth is reserved. In VoIP, distance between sender and receiver is not based on geographical distance. The transmission time depends on bandwidth and dynamic routing algorithms adopted. VoIP facilitates voice communication over Internet.

One of the problems using VoIP is latency. When packets are sent in different routes, all the packets may not arrive at the same time. This causes latency. To retransmit/download a message all the packets are to be received. Even if one the packets are missing, complete message cannot be formed. This is not the case with PSTN. To overcome this problem, and to make transmission as efficient as PSTN, we adopt dynamic source routing algorithms.

Secondly, potentiality decreases with the degradation of QoS. Some of the packets may be lost due to timeout or lack of buffer space. This cause erroneous data received and also requires the retransmission of the same message again and again. In this paper, we present generic algorithms to reduce latency and dynamic routing algorithms to minimize packet loss.
Keywords: VoIP, Latency, QoS, Dynamic Source Routing algorithms

1.Introduction

Today voice over packet network (ATM, Frame Relay and IP) is the one most growing aspect of Multi-service access network. VOIP systems take a wide variety of forms, including traditional telephone handsets, conferencing units, and mobile units. In addition to end-user equipment, VOIP systems include a variety of other components, including call processors/call managers, gateways, routers, firewalls, and protocols. Most of these components have counterparts used in data networks, but the performance demands of VOIP mean that ordinary network software and hardware must be supplemented with special VOIP components. VOIP systems take a wide variety of forms, including traditional telephone handsets, conferencing units, and mobile units. In addition to end-user equipment, VOIP systems include a variety of other components, including call processors/call managers, gateways, routers, firewalls, and protocols. Most of these components have counterparts used in data networks, but the performance demands of VOIP mean that ordinary network software and hardware must be supplemented with special VOIP components. Network Address Translation (NAT) is a powerful tool that can be used to hide internal network addresses and enable several endpoints within a LAN to use the same (external) IP address. The benefits of NATs come at a price. For one thing, an attempt to make a call into the network becomes very complex when a NAT is introduced. The situation is somewhat similar to an office building where mail is addressed with employees' names and the building address, but internal addressing is handled by the company mailroom. There are also several issues associated with the transmission of voice data across the NAT, including an incompatibility with IPsec. Another IP network concern is network slowdowns that might increase latency, jitter or packet loss. Slowdowns can be caused for many reasons including configuration issues, denial of Service (DoS) attacks or high bandwidth utilization by other systems on the network. Configuration issues are probably best addressed with education and checking mechanisms, such as having a co-worker verify configurations. DoS attacks are difficult to defend against, but may be reduced by filtering the traffic that can communicate on the network to be only that which is allowed. This may prove difficult due to the use of random ports by VoIP. The main concern of this paper is to discuss two models of VoIP(H.323 and SIP), and application TORA algorithm to packet transmission to minimize latency. Conventional VoIP (Fig. 1) converts each sample to digital form[2], sends digitized stream across Internet in packets, and convert the stream back.

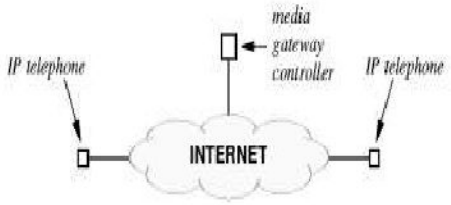

Fig. 1 Conventional VoIP

VoIP H.323 Model: H.323 is a recommendation from the ITU Telecommunication Standardization Sector (ITU-T) that defines the protocols to provide audio-visual communication sessions on any packet network. The H.323 standard addresses (Fig.2) call signaling and control, multimedia transport and control, and bandwidth control for point-to-point and multi-point conferences. It is widely implemented by voice and videoconferencing equipment.

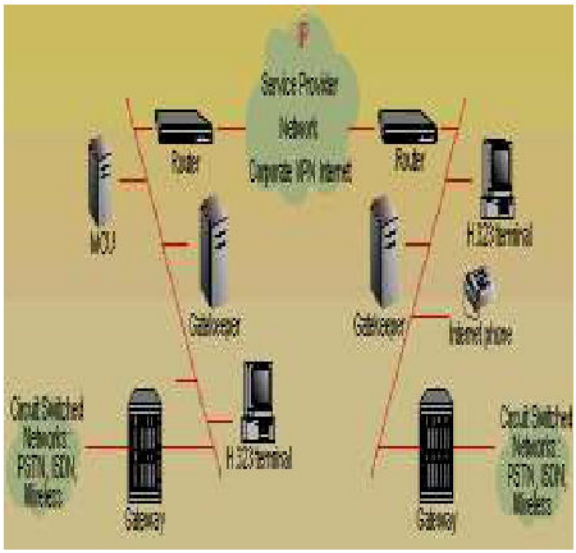

Fig. 2 H3.23 Network Model

SIP Model:
SIP defines three main elements that comprise a signaling system(Fig. 3):
User Agent: IP phone or applications
Location servers: stores information about user's location or IP address
Support servers: SIP uses three types of servers. They are
Proxy Server: forwards requests from user agents to another location.
Redirect Server: provides an alternate called party's location for the user agent[10] to contact.
Registrar Server: receives user's registration requests and updates the database that location server consults.
SIP encompasses all aspects of signaling, e.g. location of called party, ringing a phone, accepting a call, and terminating a call

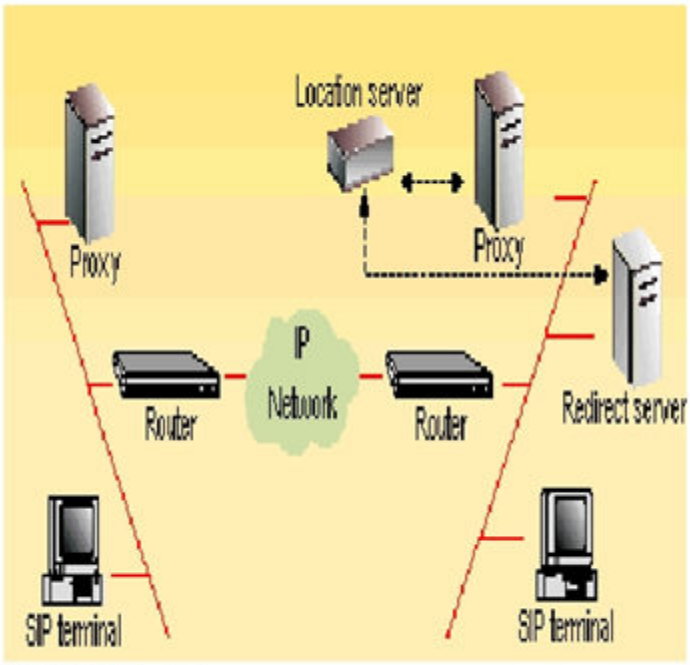

Fig.3 SIP Model

2. Related Work and Problem Statement: Of course, while changing platform to a data-based one, VoIP encounters many problems. First and the biggest one is the ***latency***. The acceptable delay in telephony is maximally 200 milliseconds[1]. By higher values, it might be difficult to carry out a conversation. Unfortunately, the available bandwidth in VoIP is not reserved, so there is no guaranteed Quality of Service (QoS), as in the PSTN. Because of too low bandwidth available, voice packets may be forced to wait, what will create a delay.

Another problem occurs, if subsequent packets experience delays of different lengths. The receiver needs to collect all the packets in order to reconstruct the full traffic stream and play it to the user. That is why the difference of delays between packets forces the receiver to buffer the traffic and wait for the delayed packets, even if most of the packets is already available. This way even though the mean packet delay over the network may be relatively small,

the total delay will be much bigger. It will be considerably increased by single delayed packets. Such a variation of latencies over the network is called ***jitter***. As said jitter may increase the total delay, but also cause break and silence periods. It will happen if if some of packets arrive later than the mentioned 200 milliseconds, they will be simply considered lost. TORA algorithm implementation also convenient for route discovery and root maintenance. The key feature of TORA is its reaction to link failures. It erases invalid routes, searches for new routes and builds new routes in a single-pass of the distributed algorithm.

3. Solution analysis to avoid delay in transmission:

During transmission of IP packets over Internet, heavy traffic and weak connection cause packet failures at destination end. To minimize this problem, this paper presents a better proposal to find link failure and also to trace the data from other nodes to recover.

In this paper, we discuss two scenarios for route trace and root maintenance.This can be illustrated using the following network.

Procedure to transmit a packet:

Each packet is associated with a header containing four information regarding id, data, size, time, and destination.

Size-The size field decides whether the packets are to be fragmented or not.

Time-Time field denotes time sent based on that after a particular time interval, if the data is not received, path is traced.

Destination-A check is to be done till the destination node is at one hop distance.

The sample network is:

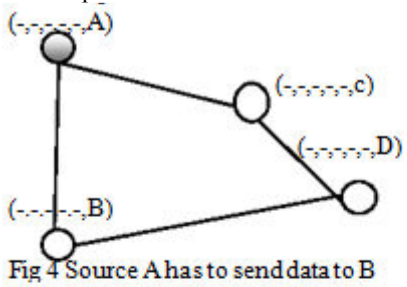

Fig 4 Source A has to send data to B

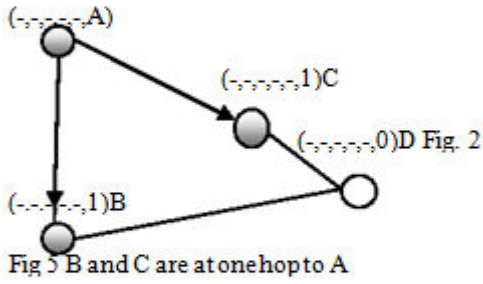

Fig 5 B and C are at one hop to A

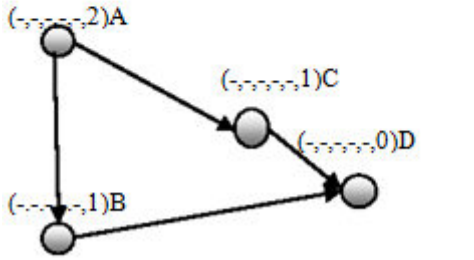

Fig.6 B and C finds D that they are at one hop

Tracing the Route:

1. A has to send a packet to D (Fig 4)
2. A broadcasts to B,C (Fig 5)
3. B knows that D is at single hop and it updates its information bit to 1 Fig 6)
4. C also knows that D is at single hop and it updates its information bit to 1
5. Evidently, A also updates its information bit to 2.
6. Now , there are two paths[9]from A-D, one is A-C-D and other is A-B-D
7. The packet can choose the path either using A-C-D or A-B-D.

Route Maintenance:

1. Suppose, the link between B-D is delinked.
2. Then, i) if the node is already updated and and delinked: Then, failure at node to transmit acknowledgement.
3. ii) If node is not updated and delinked. Then, A information bit can be not be updated. Thereby A does not know the D's existence.
4. But, Because of the another route A-C-D A's information bit is updated. 5.

We set flag bit for updating the information bit.

4. Comparative Analysis using Multinomial Distribution*:* A **multinomial distribution** is the probability distribution of the outcomes from a multinomial experiment. The multinomial formula defines the probability of any outcome from a multinomial experiment. A message cannot be transmitted by single attempt, so we send the same message so that all the nodes will receive the message, so, n, no. of trials=5.

5 trials produce N1, 2N2, N3, N4.

On any particular trial, the probability of receiving a message by N1 is 0 or 1, N2 is 0.5, N3 is 0 or 1 and N4 is again 0 or 1.

Considering p1=0.25, p2=0.25,p3=0.25 and p4=0.25

$P= [n! / (n_1! * n_2! * ... n_k!)] * (p_{1n1} * p_{2n2} * . . . * p_{knk})$

$P=[5! / (1! * 2! * 1!*1!] * (0.25^1 * 0.25^2 * 0.25^1 * 0.25^1)$

$P=0.05859375$

Table 1 shows comparative analysis between the current scenario and the proposed system.

Factor	Proposed Analysis	Normal Broadcasting
Guarantee that data is received	100%	All the nodes may not receive information,(Information is partly broadcasted)
Link failure known	Yes	No
Network Failure	Known	Can be known only by introducing acknowledgement
Hopping Distance	Known after finding destination	Not Known
Loss of Packets	Minimized	Depends on the strength of the signal

6.Implementation*:* This can be implemented using Bluetooth programming, J2ME, and Java.

7.Performance Analysis*:* The uncertainty in transmission of packets can be minimized. The performance can be improved by introducing FPgrowth tree algorithm and Hierarchical Clustering down to its transmission.

References

1. Pawel Lawecki," Master Thesis VoIP Security in Public Networks", February 2007Alcate
2. D. Richard Kuhn "Security considerations for Voice over IP Systems",National Institute of Standards and Technology
3. "Voice over InternetProtocol and Secruity(VoIP)",SANS Institute
4. A.Rehman,"Voice Over IP(VoIP)"
5. "Optimizing Performance for Voice over IP and UDP Traffic",A Riverbed Technology White paper
6. D.Wang,"Voice over IP"
7. NACT VoIP Industry Tutorial
8. D.B.Johnson "Dynamic Source Routing in Ad Hoc Wireless Networks"
9. Park and Corson, "TORA algorithm" Park 1997
10. Daniel-Constantin Mierla "SIP Tutorial"