Privacy and Packet Dispersion of Voice Applications in P2p Networks-VoIP

A.Thamizharasi
VIT university
Vellore,India

M.Vanitha
VIT university
Vellore,India

ABSTRACT

In this paper we are mainly focusing about how to improve privacy in peer to peer VOIP network without the involvement of third party. Currently we have the technologies like skype, Gtalk through which we can communicate all over the world through internet. In this technologies the voice from source to destination will be transformed through the third party server to the destination so here we cant expect privacy from that we came to the conclusion that there is a need for privacy so we are creating the personal network which connects many system through the LAN or wifi and allows users to communicate directly without any third party server in between.

Keywords

VOIP-voice over internet protocol, PSTN (Public Switched Telephone Network), p2p(peer to peer),LAN(local area network),Gtalk(Google talk),DES(data encryption standard)

1. INTRODUCTION

Voice over Internet Protocol (VoIP) is a technology that enables one to make and receive calls through the Internet instead of using the traditional analog PSTN (Public Switched Telephone Network) lines. VOIP technology converts the analog telephone communication signals into digital communication signals and transfers through the data networks it may be a wide area network ,local area network or the internet otherwise we can say that the sound is recorded and converted to computer data and transferred through internet to the destination where it again converted back to sound using speakers or headphone .In VOIP the sound is converted in to data packets and transferred to destination through the third party so privacy will not be there hence we cant able to communicate the confidential matters to overcome this disadvantage we are implementing the peer to peer VOIP personal network in this there is no third party server so privacy is achieved .this paper is implemented in eight modules by using four algorithms will see in depth about the modules in section 2 and details about the algorithms in section 3.

2. IMPLEMENTATION OF P2P VOIP PERSONAL NETWORK

VOIP environment module implementation deals with the creation of login page. First of all the new user needs to register the details in to the personal network, This details will be stored in database for future use and it needs to provide the login for already registered user by validating there username password with the help of information stored in database. Connection Module implementation need to provide the user with the details of person who are all connected to the personal network and it allows the user to select the person to whom he /she wants to communicate through p2p VOIP after selecting the user needs to enter call button. Route setup Module implementation deals with in which path the connection needs to be established between the caller and receiver .The connection between caller and receiver may be a shortest path or any other alternate path which is depends on the traffic or congestion in the network.

Proxy Node Module implementation deals with the creation of proxy node to make up a personal network through which the data will be transferred from source to destination in this module security for the data packets are provided in each and every node .Cryptography Module implementation deals with providing security for data packets which is transferred from the source to destination by using the triple DES algorithm in each and every proxy nodes. Flow analysis Module implementation is used to explain about the acknowledgement that is produced when the data is received at proxy node and the destination. Calling module explains the process of capturing the voice, converting it into packets then encrypting the voice and send to destination through proxy nodes. Dynamic Route Setup Module explains about how the path dynamically changes i.e., the route setup dynamically changes according to the congestion or network traffic with the help of naive racing algorithm. End Call Module explains about the disconnecting property that is used to end the call connection between caller and receiver after the communication gets over any one of them can disconnect the call using the end call button in the application

3. ALGORITHM AND ITS USAGE

3.1 Shortest path algorithm

In this paper we are using the shortest path algorithm in order to send the data packets from the caller to the receiver because it reduces the time and cost of making the packets to travel from source to destination. There are different types of shortest path algorithm available in that we are using the dijkstra’s algorithm mainly this algorithm was implemented to find the shortest path between the cities the same technique is used here to find the shortest distance between caller and receiver. Steps used to implement this algorithm are 1. first set the starting node tentative distance as zero and other nodes as infinity.2.mark initial node as current node and all other nodes as unvisited node .3.identity the unvisited neighbors from the initial node .4.check the distance between initial node with all other neighbor nodes and mark the distance and also the path from which the distance is calculated. 5.Find which path distance is less compared with all other and mark it as visited and start to find the neighbors from visited node and calculate the distance like for example, we are Moving from A to C so the distance of is A to B distance plus B to C distance.6.repeat step 5 until all nodes are visited. For example (see Figure 1).

3.2 Naive tracing algorithm

This algorithm is used for finding out the alternate path other than the shortest path for voice dispersion through nodes in order to send the packets without affected and to avoid collision while the packets are transferred mainly it is used to take care of traffic problems. let us consider the sample topology given in figure 2 (see Figure 2) ,the label on the edges of topology indicates the number of voice flows. A trace from caller p1 results in p1=p2=p3=p4=p5=1. Filtering out the VoIP proxy nodes (p5) and the caller (p1), the clients p2, p3 and p4 could be potential destinations for a call emerging from p1.the naive tracing algorithm doesn’t consider the shortest path route it will help to get the alternate longest route path[5].

```
TRACE(Graph G=hV , Ei, Caller src)

(1) for each vertex v 2 V
(2) f[v] = 0; label[v] = false
(3) end for
(4) f[src] = 1; label[src] = true
(5) while pick a vertex v labeled true
(6) label[v] = false
(7) for each node u such that (u, v) 2 E
(8) if (f[u] = 0)
(9) f[u] = 1; label[u] = true
(10) end if
(11) end for
(12) end while
```

3.3 Triple DES Algorithm

The DES algorithm the actual encryption and decryption is performed by taking the 64 bit block text as input and splitting it in to two half ie, left most 32 bit and right most 32 bit it can be represented as L[0]-L[15] and R[0]-R[15].

1. R[I-1] – in which I represents the round number which starts from 1 and fed in to E-bit selection table ,which is like a permutation , except that some of the bits are used more than once this will expand the number R[I-1] from 32 to 48 bits to prepare for the next step.

2. The 48-bit R[I-1] is XORed with K[I] and stored in a temporary buffer so that R[I-1] is not modified.

3. The second step result is now split into 8 segments of 6 bits each. The left-most 6 bits named as B[1], and the right-most 6 bits are named as B[8]. The Substitution boxes, known as S-boxes are a set of 8 two-dimensional arrays, each with 4 rows and 16 columns. The numbers in the boxes are always 4 bits in length, so their values range from 0-15. The S-boxes are numbered S[1]-S[8] which is used in step 4.

4. Starting with B[1], the first and last bits of the 6-bit block are taken and used as an index into the row number of S[1], which can range from 0 to 3, and the middle four bits are used as an index into the column number, which can range from 0 to 15. The number from this position in the S-box is retrieved and stored away. This is repeated with B[2] and S[2], B[3] and S[3], and the others up to B[8] and S[8]. At this point, you now have 8 4-bit numbers, which when strung together one after the other in the order of retrieval, give a 32-bit result.

5. The result from the 5th step is now passed into the P Permutation.

6. This number is now XORed with L[I-1], and moved into R[I]. R[I-1] is moved into L[I].

7. At this point we have a new L[I] and R[I]. Here, we increment I and repeat the core function until I = 17, which means that 16 rounds have been executed and keys K[1]-K[16] have all been used.

When we get the values L[16] and R[16] it will be combined together in a same fashion in which it is splinted. when this two halves are swapped R[16] will be the left most 16 bit and L[16] will be the right most 16 bit . this algorithm we are going to use three 56 bit keys. It uses the following steps, 1.Encryption using the first 56 bit key.2.Decryption using the second 56 bit key.3.Again Encryption using the third 56 bit key. The encryption method of DES and triple DES is similar even the decryption is the reverse operation of encryption .triple DES is secured because here DES is used three times that’s why it is called as triple DES.

```
static TripleDES CreateDES(int key)
 {
 MD5 md5 = new MD5CryptoServiceProvider();
 TripleDES des = new TripleDESCryptoServiceProvider();
des.Key=md5.ComputeHash(Encoding.Unicode.GetBytes(
 key.ToString()));
 des.IV = new byte[des.BlockSize / 8];
  return des;
  }
 public static byte[] Encryp(string PlainText, int key)
  {
 TripleDES des = CreateDES(key);
  ICryptoTransform ct = des.CreateEncryptor();
  byte[] input = Encoding.Unicode.GetBytes(PlainText);
  return ct.TransformFinalBlock(input, 0, input.Length);
   }
```

3.4 Flow analysis algorithm

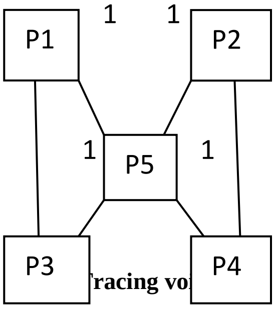
Flow analysis algorithm is used to identity the flow of information in the VOIP network here we assume that the physical infrastructure is owned by the un trusted third party network so the VOIP service must route the voice through the third party so the third party service provider will know all the details about VOIP network topology[1][2] and the flow rates[3][4]. The network service provider can obtain flow information using traffic analysis in the VOIP topology(see Figure 3) or using ring search on the network topology[6]. We represent the VoIP network topology as a weighted graph G = hV , Ei, where V is the set of nodes and E _V ×V is the set of undirected edges. The weight of an edge e = (p, q) (denoted by w(p, q)) is the latency between the nodes p and q. We assume that the adversary can observe the network and thus knows nf(p ! q) the number of voice flows between two nodes p and q on the VoIP network such that (p, q) 2 E. To illustrate the effectiveness of our flow analysis attacks, we use a synthetic network topology with 1024 nodes. The topology is constructed using the GT-ITM topology generator [7][8] and our experiments were performed on c# [9][10]. GT-ITM models network geography and the small world phenomenon [11][12].

3. 5 .K- Anonymity algorithm

K-anonymity algorithm is used for providing the anonymous network so that hackers could not identify the flow of packets over the network. let us consider the caller as S and the receiver as R the voice packets need to move through the personal network which consists of proxy nodes p1,p2,p3,p4.the hacker can hack the voice easily from the proxy node which is present next to the caller or at the proxy node which is present before the destination R so we are using the k-anonymity algorithm which will hide the proxy nodes which is next to the caller and which is present before the destination .consider the figure 3 in this p1 and p4 are the proxy nodes present after and before the caller and receiver in the network by hiding those nodes we can prevent the data from hackers.

4. FIGURES

Shortest path tracing (see Figure 1) which shows the shortest path in which the voice has been transmitted from p1to p4,p2 and p3.Tracing voice calls(see Figure 2) shows in which paths the voice has been transferred from caller to receiver.



racing vo

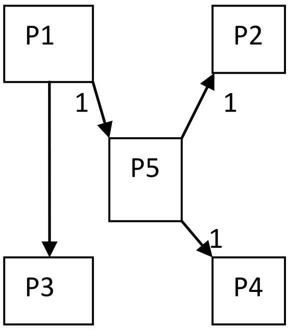


Fig 1: Shortest path tracing

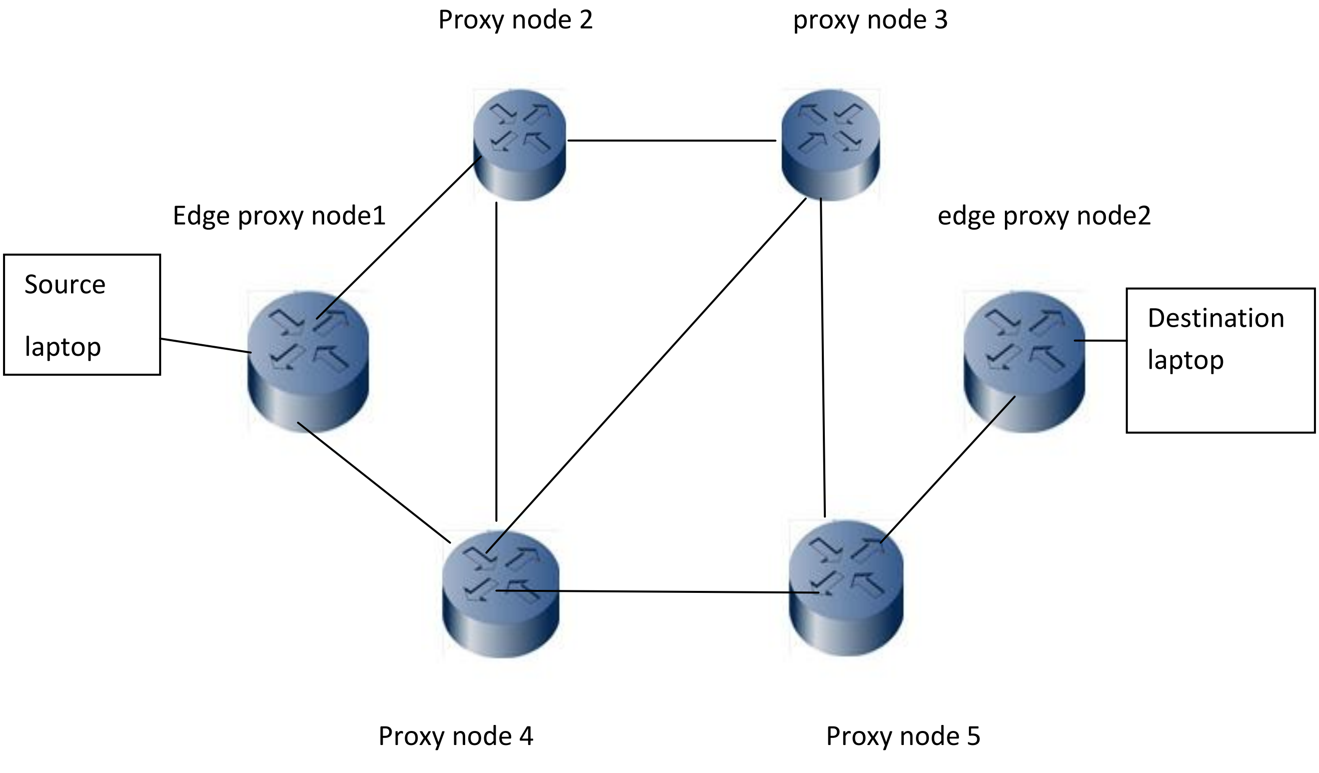
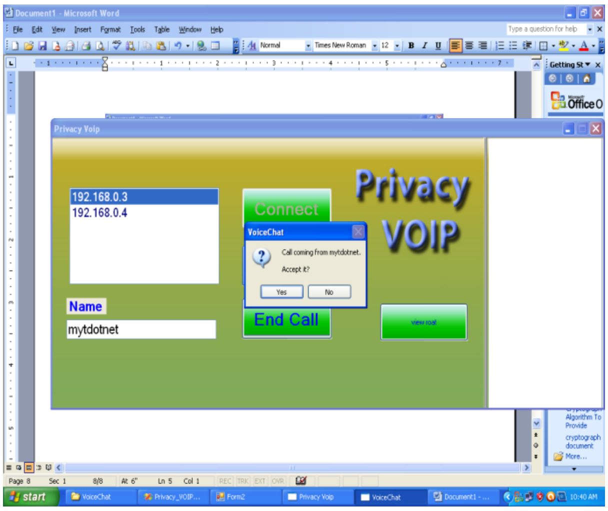


Fig 3:Flow analysis of voice transmission

4. COMPARATIVE STUDY OF EXISTING AND PROPOSED SYSTEM

Nowadays we are using Skype and Gtalk which is a third party, so we are entering into their environment for conferencing. We need a server to transfer the information from source to destination i.e,we are compromising our privacy at a certain level as they do not provide full security to our audio packets .In this proposed system we are not including a server as we are creating a personal network without the involvement of the third party. Next we are using a peer-to-peer network setup, the peer-to-peer VOIP network consists of a core proxy network and a set of clients that connect the edge of those proxy network. Finally we are setting up a VoIP route setup protocol. So we have the advantages like privacy can be achieved ,can make this application to run by using LAN or wifi ,cost advantage, clearance in voice transmission , can able to make conference calls and security will be achieved while transferring voice with the help of triple DES algorithm.

5. EXPERIMENTAL RESULT SCREEEN SHOT



192.168.0.3
192.168.0.4

Name: mytdotnet

Call coming from mytdotnet.
Accept it?

4. CONCLUSION

In this paper, we have addressed the problem of providing privacy guarantees in peer-to-peer VoIP networks. To overcome that First, we developed a personal network without the involvement of third party which consists of proxy nodes through which the voice will be transferred to the receiver so that the privacy will be guaranteed . Secondly, the path in which data transferred will be a shortest path or any other alternate path which will be selected with the help of shortest path and naive tracing algorithm through which we can achieve security. Finally, we focus on technical feasibility of privacy attacks and defenses on VoIP networks , we are enhancing the concept of conference call in p2p VOIP personal network and e will inform the receiver about the call arrival through message even if the receiver is busy with any other works in online and the security will be enhanced to avoid others hiring the communication between caller and receiver.

5. REFERENCES

[1] P. Syverson, G. Tsudik, M. Reed, and C. Landwehr. Towards an analysis of onion routing security. In workshop on design issues in anonymity and unobservability,2000.

[2] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second generation onion router. In 13th USENIX security symposium,2000.

[3] G. Perng, M. K. Reiter, and C. Wang. M2: Multicasting mixes for efficient and anonymous communication. In IEEE ICDCS,2006.

[4] A. Back, I. Goldberg, and A. Shostack. Freedom 2.1 security issues and analysis. Zero Knowledge Systems, Inc. white paper, 2001.

[5] Mudhakar Srivatsa, Arun Iyengar, Ling Liu and Hongbo Jiang. Privacy in VoIP Networks:Flow Analysis Attacks and Defense,2009

[6] S.Saroiu,P.K.Gummadi, and S. D. Gribble. A Measurement Study of peer-to-peer file sharing systems In Multimedia computing and networks(MMCA),2002.

[7] E. W. Zegura, K. Calvert, and S. Bhattacharjee. How to model an internetwork? In IEEE Infocom, 1996.

[8] GT-ITM: Georgia tech internetwork topology models. http://www.cc.gatech.edu/projects/gtitm/.

[9] The c sharp network programming. http://www.isi.edu.

[10] C# Network Programming book by Richard Blum.

[11] B. Fortz and M. Thorup. Optimizing OSPF/IS-IS weights in a changing world. In IEEE Journal on Special Areas in Communication, 2002.

[12] L. Qiu, V. N. Padmanabhan, and G. M. Voelker. On the placement of web server replicas. In 12th IEEE INFOCOM, 2001.