Modified Secret Sharing over a Single Path in VoIP with Reliable Data Delivery

Mrs.K.Maheswari[1], Dr.M.Punithavalli[2]

[1]Associate professor, Department of Computer Applications
SNR SONS College, Coimbatore- 641006, Tamilnadu, India

[2]Director, Department of Computer Applications
Sri Ramakrishna Engineering College, Coimbatore -641022
Tamilnadu, India

Abstract

Voice over Internet Protocol (VoIP) is a new fancy and up growing technology. A major change in telecommunication industry is VoIP. The transmission of Real time voice data is not as easy as ordinary text data. The real time voice transmission faces lot of difficulties. It suffers from packet loss, delay, quality and security. These factors will affects and degrade the performance and quality of a VoIP. This paper addresses the security and packet delivery ratio of a VoIP using modified secret sharing algorithm over a single path with reduced packet loss. The simulation results show that higher security and reduced packet loss is achieved in terms of end – to – end delay and packet delivery ratio. The user gets bad quality of VoIP at the receiver side. This makes the deployment of real time application a challenging task. To overcome these challenges in VoIP, several solutions have been reported already. The proper selection of active path in the routing protocol has a great impact in terms of packet delivery ratio and route discovery process. To provide end to end security between the source destination pair, the single path routing scheme is introduced.

Keywords: *VoIP, Secret Sharing, packet loss, security, single path.*

1. Introduction

Confidentiality is very important requirement for any kind of data transmission. The data in VoIP networks are not subject to eavesdropping. Preventing data from people who do not need to know. It is a packet switched and interactive network. The traditional Public Switched Telephone Network (PSTN) is circuit switched. The circuit switched network is secure one but the packet switched internet is not. It is designed with less security features. In conventional public switched telephone networks (PSTN), entire communication paths were administered by a few authorized telephone companies. It was therefore difficult for a malicious person to wiretap conversations over telephones because persons who were allowed to access the network were carefully restricted. The recently grown internet protocol telephone or VoIP has multiple intermediates exist between the two endpoints (telephones). Therefore, the risk of man-in-the-middle attack increases.A message is divided into shares which are sending through a single path [Abdur Rashid Sang, et al.(2010)]. The modified shamir's secret sharing algorithm [A. Shamir (1979)] is implemented to provide reliable data delivery.

The transmission technology of VOIP must be in digital is shown in Figure 1. The caller's voice is digitized. The digitized voice is compressed and then separated into packets using complex algorithms [10].These packets are addressed and sent across the network which is to be reassembled in the proper order at the destination. Again, this reassembly can be done by a carrier, and Internet Service Provider, or by PC.

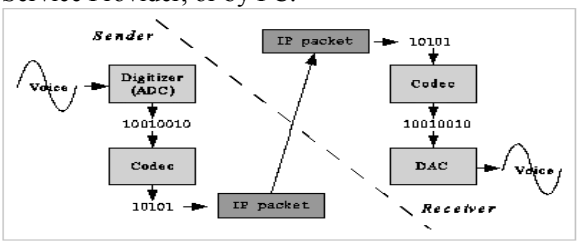

Figure 1 Transmission Technology of VoIP

During transmission on the Internet, packets may be lost or delayed, or errors may damage the packets. Conventional error correction techniques would request the retransmission of unusable or lost packets, but if the transmission is a real-time voice communication this technique obviously would not work, so sophisticated error detection and correction systems [Christos tachtatzis, et al (2008)] are used to create sound to fill in the gaps.

The fundamental idea of secret sharing is the secret message is sending through a single specified path using Ad-hoc On Demand distance Vector (AODV) routing [C.E.Perkins, et al (2001)] [M.K.Marina, et al

(2001)]. The enemy can easily compromise the message by troubling any one of the nodes all along the path. To solve this, the message is divided into shares or pieces. The pieces are sending through the specified path [Christos tachtatzis, et al (2008)].

A certain number of shares are used to reconstruct the original secret message. This is termed as Threshold secret sharing. Any shares less than threshold cannot do anything.

- Dividing the secret message into N multiple pieces called shares [Berry Schoenmakers (1999)][Hanoch, et al (2006)]
- The enemy has to compromise at least T shares
- Designed for cheating detection and cheater identification
- Modified Shamir's Secret sharing scheme is implemented

The subjective performance [A.Baciocola, et al (2005)] of VoIP quality is predicted by E-model by an average listener combining the impairment caused by transmission parameters. The rating can be used to predict subjective user reactions, such as the Mean Opinion Score (MOS) [11].

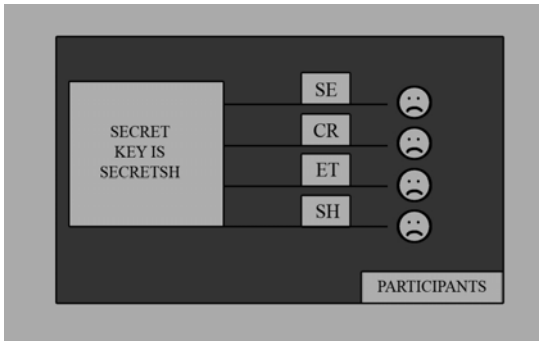

Figure 2 secret sharing in VoIP

According to ITU-T Recommendation, the E-model rating *R* is given by the following expression [ITU-T Rec. G.107 (2003)].R = R0 − Is − Id − Ie + A.
Where R -Transmission rating factor
R0 - signal to noise ratio
Is - the combination of all impairments which occur more or less simultaneously with the voice signal
Id - the mouth-to-ear delay impairment factor
Ie - equipment impairment factor
A - The advantage factor or expectation factor

The resulting score is the transmission rating *R* factor, a scalar measure that ranges from 0 (poor) to 100 (excellent). *R* factor values below 60 are not recommended [A. D. Clark (2001)] [R. G. Cole (2001)]. According to [ITU-T Rec. G.107 (2003)], the *R* factor is related to MOS as follows:

For R < 0 MOS = 1
For 0<R<100 MOS = 1+ 0.035R + 7R(R-60) (100-R)x10^{-6}
For R > 100 MOS = 4.5

The E-Model not only takes in account the transmission statistics, but it also considers the voice application characteristics, like the codec quality, codec robustness against packet loss and the late packets discard. According to [A.Baciocola, et al (2005)], the above equations can be reduced to the following expression. where *Id* is a function of the absolute one-way delay *Ie* is, in short, a function of the used codec type and the packet loss rate R = 93.4 - Id-Ie

Section 2 reviews the security threats of VoIP functions. This is followed by the threshold secret sharing scheme of VoIP in section 3. In section 4, the results are analyzed. Finally section 5 concludes the work.

2. Background Study

When the use of internet grows, automatically the complexity of the security problem increases. It becomes very difficult to solve the security problem. Actually, many application services do not consider the security. User authentication, confidentiality and integrity of signaling message or media stream are required for secure VoIP communication system.
The security threats are

- Eavesdropping and recording phone calls
- Tracking calls
- Stealing confidential information
- Modifying phone calls
- Making free phone calls
- Pranks / Practical jokes
- Board room bugging
- Sending spam (voice or email)
- Denial of service (DoS),
- Alteration of voice stream,
- Toll fraud,
- Redirection of call,
- Accounting data manipulation,
- Caller ID impersonation,
- Unwanted calls and messages

3. Threshold Secret Sharing Scheme in VoIP

This system divides a message into N pieces. Each N participant gets one share of the secret message

respectively. Any shares less than threshold cannot learn anything. The T (Threshold value of shares) out of N participants can rebuild the original secret message. This is called (T, N) threshold secret sharing scheme. The Shamir's Lagrange Interpolative Polynomial scheme is used to reconstruct the original. It is designed especially for identifying cheaters.

A secret sharing scheme consists of two algorithms

- Dealer
- Combiner

Dealer generates and distributes shares. The combiner collects and reconstructs the shares.

Shamir's construction for (*T, N*) secret sharing scheme is algebraic and is based on the polynomial interpolation. Assume K is the secret to be shared among N participants, S_1, S_2... S_N are shares, P_1, P_2... P_N can hold one share of the secret respectively. The dealer obtains the i^{th} participant *Pi*'s share *Si* by evaluating a polynomial of degree (*T*-1)

$f(x) = K + a_1 x + \ldots\ldots a_{T-1} x^{T-1} \bmod p$ at x=I (i=1,2,…,N):

$Pi \rightarrow Si = f(i)$ (1)

Where

a_1, a2, a3,…..a_{T-1} are coefficients which are selected randomly, part of a secret message

P is randomly chosen large prime number.

To indicate the security features of routes the vector P= [p_1,p_2,….,p_M] is used.

P_i (i=1,2,…..M) is the probability that a route i is compromised. It is assumed that $P_1 \leq P_2 \leq \ldots\ldots \leq P_M$. The paths are ordered based on its cost value. The distribution of shares n= [n1, n2,…..,n_M]

where

n_i is the number of parts of a message sent through thr route i. $n_i \geq 0$ and it is an integer.

$$\sum_{i=1}^{M} n_i = N \quad (2)$$

The probability that the message is compromised equal to the probability that T or more shares are seized.

The combiner side, the knowledge of minimum number of T shares ,f(i_1), f(i_2),….f(i_T), the original polynomial f(x) can be reconstructed by Lagrange interpolation.

$$f(x) = \sum_{j=1}^{T} S_{ij} . l_{ij}(x) \bmod p \quad (3)$$

Where

$$l_{i_j}(x) = \prod_{k=1, k\neq j}^{T} \frac{x - i_k}{i_j - i_k} \quad (4)$$

At the source

$$T = \sum_{i=1}^{N} h(Si) P^{2(i-1)} + \sum_{i=1}^{N-1} cp^{2i-1} \quad (5)$$

Where c is a positive constant, security features are added with shares.

At the destination

$$T^* = \sum_{i=1}^{N} h(s_i^*) p^{2(i-1)} \quad (6)$$

For each S_i^*

$$\left\lfloor \frac{T - T^{\cdot}}{p^{2(i-1)}} \right\rfloor (\bmod\ p) == 0 \quad (7)$$

Choosing the most appropriate values of (T, N) and allocating them on to the paths is very important. (T, N) threshold secret sharing algorithm is applied to the message at source. If one node compromise data, all the shares traveling through the node would be compromised.

Reactive, demand – driven algorithm is AODV (Ad hoc on demand Distance vector routing). It discovers a route to a destination only when it sends a packet for forwarding to that destination. The discovered routes are maintained by route maintenance procedures.

A link has a limited life time. The link will expire when the two end nodes are in out of transmission range. In on-demand routing protocols link status will not be updated until they are used. The broken link will cause a number of route errors and generates a packet loss. Therefore, each link is given an appropriate life time. If this value is too small, link expires too soon. If the value is very large, links break early before the timers expire. It degrades the overall performance.

A predefined static life time is assigned for T1 seconds. In static life time scheme, the two clock time attributes are used.

- Born state
- Last used state

Born state indicates a new link is found in the route. The last used state indicates timestamp when the link is last used to forward a packet. There are two situations that will cause a link to be removed from the route.

- Route error is received or link is broken
- Timeout

If a link is removed because of the reception of a route error, the life time is calculated as

l=CurrentTime()- link[i,j].born (8)

If it is removed because of timeout, the life time l is calculated as

l = link[i,j].lastused – link[i,j] (9)
.born

LIFETIME is a variable indicating the estimation of the link lifetime. It is always assigned a static value. The modified algorithm is given below

Step 1: Create set S, which includes all the possible network security state vectors

S= $s_1,s_2,\ldots s_m$. .There should be totally $2^M - 2$ elements in set S.

Step 2: Calculate Pstate (s) for each element s according to

$$Pstate\ (s) = \prod_{i=1}^{M} Pi^{\ Si\ (1-p)^{1-Si}} \quad (10)$$

Where i varies from 1, 2,…. . , m.

Create set S2 , which includes [1,1,…,1] only initially.

Step 3: Create set A, which include all the possible share allocation vectors

n = $n_1,n_2,\ldots\ldots n_m$.

To reduce the size of A

- N≥ $n_1 \geq n_2 \geq \ldots\ldots \geq n_m \geq 0$
- Σ n_i = N where i varies from 1, 2,…. . , m.

Step 4: All the remaining elements in A are optimal share allocations if [1,1,…,1] is

the only element in set S2 ; or they are sub-optimal share allocations if more elements present in set S2.

Step 5: Distributing the secrets in time domain basis by sending out the shares over a certain period of time. The link is estimated by its appropriate static lifetime value [in seconds].

Step 6 : If the value assigned is very small, the link will expire too soon. At the same time if the value of lifetime is too big, there may be a route error. This will degrade the overall performance.

Step 7: Choosing the optimal value of static life time shows the performance of this algorithm

4. Results and Discussion

The important performance metric is End-to-End Delay. It is also called as Packet Latency. This is calculated by the time of packet sent at the sender and received at the receiver. This calculation is not only based on this but also the packets that are successfully delivered at the receiver without any loss of information.

When network traffic is very high, there may be a chance of packet latency at the receiver. So the success depends on the channel capacity. If the channel is more capable and error free, then there is no latency of packets. So the optimized lifetime value shows the result of low packet latency.

The results confirms that the small static lifetime value causes increasing number of route request and decreased number of route error. The Delay gets increased if the static lifetime is large and is shown in figure 3.

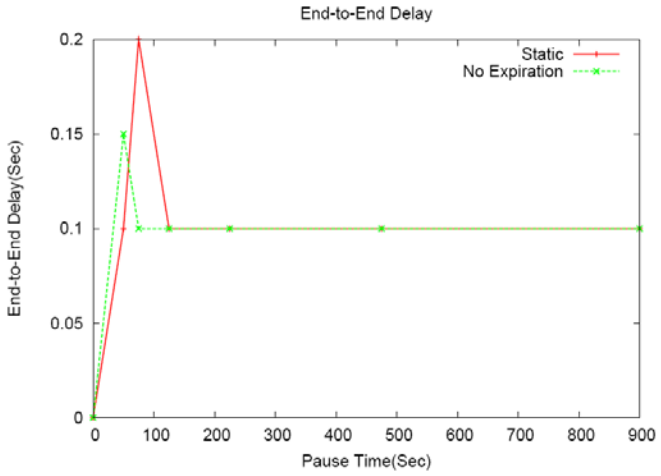

Figure 3 End – to – End Delay

The packet latency is calculated for packets that are successfully delivered. The transmission delay, propagation delay and queuing delay are the delay impairments that exist in IP networks. There are two types of latency.

- Protocol takes to discover a route to a destination
- Latency for a sender to recover when a route used breaks

It shows the average delay (time) in milliseconds spent to deliver each data packet.

Average End-End Delay = TimeDelay / PacketReceived

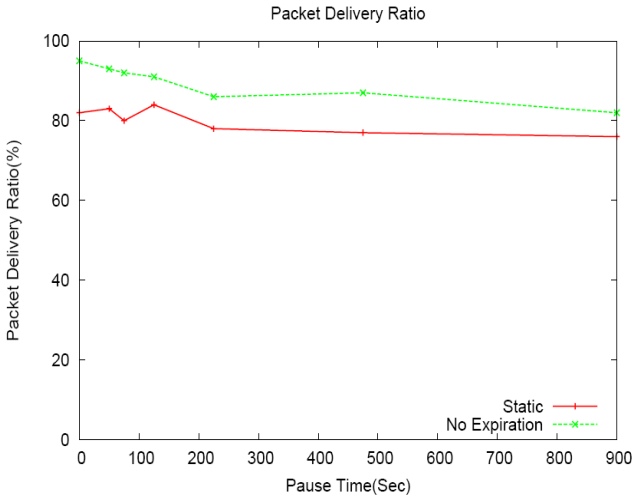

Figure 4 Packet Delivery Ratio

The application level performance metric is Packet Delivery Ratio (PDR). It is the ratio of packets that are received at the destination and sent at the source. It shows the ratio of total packets received at destination nodes, to total packets which are sent by source nodes.

PDR = Packets received / Packets Sent X 100

The packets may be dropped due to route error. If there is no alternate path, the packet may be dropped. It shows the number of data packets which were dropped during their journey to destination. To reduce packet loss, a small lifetime value is favored. A small life time value reduces route error and increases route requests. Therefore more data is in transmission with less route error.

The other type of packet drop is due to heavy collisions. When the traffic is very high, the packet loss caused by collision becomes more rigorous. The Time versus Packet Delivery Ratio is shown in Figure 4. The performance of packet delivery ratio in high traffic significantly affects the routing overhead.

5. Conclusions

The streaming of audio or video content over the Internet is a challenging task. This is due to the fact that the Internet is a packet switched network with a little quality of service (QoS) guarantee. The major challenge of the VoIP network is maintaining quality as well as security. This work shows the result in a better performance. In unipath routing, only a single route is used between a source and the destination. The most commonly used protocols are Ad hoc On-Demand Distance Vector (AODV). The simulation results show that the reduction of packet loss and improvement of security. The performance is satisfied in terms of quality. But the increased Delay and security are again a greater risk.

References

[1] Abdur Rashid Sang,; Jianwei Liu,; Zhiping Liu. performance comparison of single path and multipath routing protocol in MANET with selfish behavior, (2010).

[2] A.Baciocola, C.Cicconetti, G.Stea. User–level performance evaluation of voip using ns2, (2005)

[3] Berry Schoenmakers. A simple publicly verifiable secret sharing scheme and its application to electronic voting, CRYPTO 99 vol 1666 of lecture notes in Computer science, springer-verlag, pp: 148-164, (1999).

[4] A. D. Clark. Modeling the Effects of Burst Packet Loss and Regency on Subjective Voice Quality, Columbia University IP, Telephony Workshop, (2001).

[5] R. G. Cole and J. H. Rosenbluth. Voice over IP Performance Monitoring, ACM SIGCOMM, (2001) .

[6] Christos tachtatzis,David harle. performance evaluation of multipath and single path routing protocols for mobile ad-hoc networks, (2008).

[7] Hanoch, Levy, Haim, Zlatokrilov. the effect of packet dispersion on voice applications in IP networks, IEEE / ACM transactions on networking, vol.14, issue: 2, pp: 277-288, (2006) .

[8] ITU-T Rec. G.107. The E-Model, A Computational Model for Use in Transmission Planning, (2003).

[9] M.K.Marina, S.R.Das, performance of routing caching strategies in dynamic source routing, INt. Conf. on distributed computing system ICDCS, (2001) .

[10] C.E.Perkins,E.M.Belding-Royer,S.R.Das, Ad-hoc On Demand distance Vector (AODV) routing, (2001) .

[11]A. Shamir, “How to Share a Secret”, Communications of the ACM, pp: 612- 613, (1979).

First Author

K.Maheswari received her B.sc (Computer Science) from Madurai Kamaraj University and MCA. M.Phil. from Bharathidasan University. She is pursuing her Ph.d at Bharathiar University. She is currently working as an Associate Professor in the Department of Computer Applications, SNR Sons College, and Coimbatore. She has 16 years of teaching experience. She has presented research papers in several national and international conferences. She has published many research papers in various international journals. Her research interest is VoIP and network security.

Second Author

Dr. M. Punithavalli received the Ph.d., degree in Computer Science from Alagappa University, Karaikudi in May

2007. She is currently serving as the Director of the Computer Applications Department, Sri Ramakrishna Engineering College, Coimbatore. Her research interest lies in the area of Data mining, Genetic Algorithms and Image Processing. She has published more than 10 Technical papers in International, National Journals and conferences. She is Board of studies member in various universities and colleges. She is also reviewer in International Journals. She has given many guest lecturers and acted as chairperson in conference. Currently 10 students are doing Ph.D., under her supervision.