Architecture of Multipath VoIP using Modified Secret Sharing Algorithm

K.Maheswari
Associate professor
Department of Computer Apllications
SNR Sons College

Dr.M.Punithavalli
Director
Department of Computer Apllications
Sri Ramakrishna Engineering College

ABSTRACT

Voice over Internet Protocol is an integration of Computer and telephony. It is the replacement of present telephone technology. There are some difficulties that are faced by VoIP users such as paket loss, delay, security, echo, bandwidth overhead and throughput. The critical problem is providing security and reducing packet loss. In this paper, the architecture of multipath VoIP routing using modified shamir's secret sharing algorithm is implemented to provide more security with the reduced end-to-end delay. The algorithm is modified in the distribution phase of shares. The simulation results show that it achieves better performance. This work is implemented in NS-2.

General Terms

This paper focuses network security and communication.

Keywords

Security, multipath, VoIP, secret sharing and delay.

1. INTRODUCTION

Multipath routing is a routing technique of networks. It uses multiple alternative paths through a network. This provides a variety of benefits such as fault tolerance, increased bandwidth or improved security. Sometimes the multiple paths can be overlapped, edge-disjoined or node disjoined with each other. The implementation of multipath routing deployment [14] is practically very difficult. Much research is needed to overcome these facilities.

- Divide the message into multiple pieces [6] [7] and routes them to the destination through the selected multiple paths.
- The dynamic source routing protocol AOMDV [11] is used in Multiplex and Multicast environment
- Instead of sending through a single path, shares are sending through multiple paths with minimal threshold value.
- The enemy cannot reconstruct the original message-very difficult to decode
- Confidentiality and privacy are at greater risk in VoIP systems unless strong controls are implemented and maintained.

2. BACKGROUND STUDY

The secret "secretsh" is divided into the share se,cr,et and sh and is shown in Figure 1. A person with zero shares knows only that the word secretsh consists of eight letters. Any T out of n shares are used to reconstruct the secret Lagrange polynomial interpolation scheme is used.

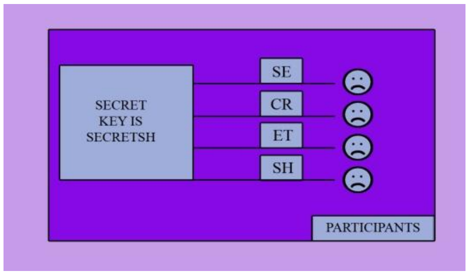

Figure 1 Secret Sharing

When the use of internet grows, automatically the complexity of the security problem increases. It becomes very difficult to solve the security problem in terms of large volume of data, busy and heavy network. Actually, many application services do not consider the security [9]. User authentication, confidentiality and integrity of signaling message or media stream are required for secure VoIP communication system [9] [12] [13]. The prominent challenging of VoIP network is providing security [10]. This scheme is developed for cheating identification and cheater detection. [17].

The benefits of Multipath routing include:

- **Optimal paths utilization**: By ranking paths by some (possibly time-varying) metrics, optimal paths for packet transmission can be selected at any given time.
- **Load balancing**: By distributing traffic over multiple routes, congestion and bottlenecks between nodes due to limited bandwidth can be mitigated.
- **Fault-tolerance**: By sending the same packet along all discovered routes, higher degree of fault-tolerance can be achieved. The destination node can successfully receive the packet as long as at least one of the routes does not fail. Obviously, this broadcasting approach is not bandwidth efficient.
- **Higher aggregate bandwidth**: By utilizing all discovered routes higher aggregate bandwidth can be achieved.

A Multipath routing protocol can ensure reliable communication [8] [16] by discovering and selecting reliable paths. The multiple paths are set up in a similar manner as that of the AODVM protocol. Some of the multi path routing protocols are discussed in this section.

Split Multipath routing protocol [15]

Split Multipath routing (SMR) [5] is introduced in by Lee and Gerla. The main objective of SMR is to reduce the frequency of route discovery processes and thereby reduce the control overhead in the network. The protocol uses a per packet allocation scheme to distribute a load into multiple paths.

Braided Multipath routing

Braided Multipath routing protocol has been introduced in the year 2001. The authors suggested that node-disjoint Multipath routing is not energy efficient; these node-disjoint paths consume more energy. BMR protocol uses a technique called path reinforcement [4] [16]. By using reinforcement a mobile node makes a local decision about setting preferences among its neighbors. Thus, 67% of maintenance overhead can be saved in the BMR protocol compared to other node-disjoint Multipath routing protocol.

Multipath ad hoc on demand distance vector protocol (AODVM)

To improve the performance of AODV protocol, a Multipath version of AODV called AODVM has been proposed in 2003 [3]. In the AODVM protocol, a destination node selects paths that pass through more reliable nodes. The AODVM protocol reduces overhead.

Multipath AODV with path diversity (AODVM/PD) protocol[2]

AODVM/PD protocol is designed to take advantage of a Multipath route while reducing interference among different paths. A concept of correlation factor between two paths is introduced and used while making a routing decision.

AODV with controlled flooding (AODV-CF)

The AODV protocol with controlled flooding (AODVCF) has been proposed. A regular ad hoc routing protocol like AODV uses a broadcast technique to discover a path. The authors suggested that the broadcast technique used by AODV is not efficient if there are frequent route breakages in the network. The authors have proposed a controlled flooding technique so that a set of alternative paths are discovered in addition to the main path. The other objective of controlled flooding is to reduce the number of control messages generated in the network.

Split-n-save Multipath routing protocol

The Multipath version of the AODV protocol (AODVM) has been modified to implement the split-n-save protocol to achieve two major objectives: network survivability and satisfiability. The authors designed a simple multiplexing policy for switching traffic into different paths. According to this policy, a source node will switch paths after transmitting ‘k’ number of packets along a path.

AODV Multipath Router approach (AODVM-R)

When performing route discovery, the source and intermediate nodes maintain multiple routes to the destination. To ensure loop freedom the RREQ packet includes path information (path from the source to the router). Primary and secondary routes will have the same sequence numbers. When a link breaks, a node tries to repair the route using alternate paths. If still there is an unreachable destination, the node sends an RERR message to its neighbors. If the primary route works for a long time, alternate paths might timeout because they are not used. While the primary route is being used, send REFRESH message to the alternate routes occasionally to refresh them. AODVM-R reduces number of route discoveries, but the total overhead is not significantly reduced because of refresh message overhead. Refresh message period can be carefully tuned to reduce overhead. AODVM-R performs slightly better than AODV in terms of packet delivery ratio, but the improvement is minimal.

Ad Hoc On-Demand Multipath Distance Vector Routing (AOMDV)

To keep track of multiple routes, the routing entries for each destination contain a list of the next hops along with the corresponding hop counts. All the next hops have the same sequence number. For each destination, a node maintains the advertised hop count, which is defined as the maximum hop count for all the paths. This is the hop count used for sending route advertisements of the destination. The performance study of AOMDV relative to AODV under a wide range of mobility and traffic scenarios reveals that AOMDV offers a significant reduction in delay, often more than a factor of two. It also provides reduction in the routing load and the end to end delay.

Ad-hoc Over Distance Vector Multipath (AODVM)

Data source is responsible for maintaining alternate routes to a sink. It is scalable with the number of flows per source. In addition to stopping the flow and doing a broadcast route discovery, the source may have the option of trying an alternate path. Intermediate nodes are not allowed to send a route reply directly to the source. To ensure that nodes do not participate in more than one route, whenever a node overhears one of its neighbors broadcasting an RREP packet, it deletes that neighbor from its RREQ table. Because a node cannot participate in more than one route, the discovered routes must be node-disjoint.

Ad hoc On-demand Distance Vector Multi-path (AODV Multipath)

In AODV Multipath, node-disjoint paths are established during the forwarding of the route reply messages towards the source, while in AOMDV node-disjointness is achieved at the route request procedure.

Node Disjoint Multipath Routing (NDMR)

Node-disjoint Multipath routing (NDMR) [1] extends the AODV protocol with new features such as the path accumulation and reverse-route-table. But NDMR discovers multiple node-disjoint paths by using fewer overhead packets compared to the AODV protocol. Formation of a disjoint path is the main focus of the NDMR protocol.

AODV with Backup Routes (AODV-BR)

A node may receive numerous RREPs for the same route if the node is within the radio propagation range of more than one intermediate node of the primary route. In this situation, the node chooses the best route among them and inserts it to the alternate route table. When the RREP packet reaches the source of the route, the primary route between the source and the destination is established and ready for use. Nodes that have an entry to the destination in their alternate route table are part of the mesh. The primary route and alternate routes together establish a mesh structure. AODV-BR technique provides robustness to mobility and enhances protocol performance. However, AODV-BR does not perform well under heavy traffic networks.

Performance optimization using an efficient N- to -1 Multipath discovery protocol finds multiple node disjoint paths from every node.. This scheme combines concurrent Multipath routing and alternate Multipath salvaging techniques and provides more security and reliability. This work focuses on the performance gains from Multipath routing and the techniques of the construction and the usage of the paths. Reliability is the probability of message generated at one place in the network and routed to the intended destination. It is developed to provide route failure protection. Threshold secret sharing scheme and Multipath routing idea is proposed to provide more reliability and security. Secret sharing cryptography [10] is used to improve security. Little information redundancy is achieved in this work.

The PSTN is not fully meshed network with every operator connected to every other, which is impractical an inefficient also. Therefore the calls may be routed through intermediate operator networks before they reach their destination. One of the major problems in PSTN routing is determining how to route this call in the most cost effective [15] and timely manner. Multipath routing [8] promises to path breaks, network congestion through load balancing and reduced end-to-end delay. Security remains important factor that impedes the deployment of media streaming applications over the VoIP network. This frame work provides security [1] in an efficient manner. This makes reduced packet loss over multiple paths. Distributing the shares through multiple paths becomes more challenging to the attackers. It is a one-way routing between source and destination.

3. ARCHITECTURE OF SECRET SHARING OVER MULTIPATH

The general architecture of multipath transport of VOIP stream is depicted in figure 2. At the sending side, the voice is packetized compressed by encoder. Then the streams are partitioned and assigned to many paths by a traffic allocator. These paths are maintained by a multipath routing protocol AOMDV (Adhoc Ondemand Multipath Distance Vector). The data will arrive at the destination and put in to a buffer to restore the original order.

Finally the voice data is extracted from the buffer to be decoded and displayed. The general architecture of multipath transport of online application does not consider security measures. The security enhancements in the design of multipath voice streaming is incorporated.

Strong authentication, access control mechanisms, key management, policy enforcement are needed to protect the data. Some VoIP networks are not powerful to perform encryption. Newer IP phones are able to provide encryption at reasonable cost. Security controls and policies must be updated. Confidentiality and privacy are at greater risk in VoIP systems unless strong controls are designed and maintained. Worms, viruses and other malicious software are extraordinarily common on personal computers connected to the internet. This work is focused to overcome the complications introduced by security requirements for VoIP.

Multi path routing is known as traffic dispersion. Sending packets to multiple destinations simultaneously is called multicasting. It is also called as multipart delivery and is shown in Figure 3. The main application of multicasting is teleconference which includes many participants. Most of the current research is focusing on this area. It occupies more space in the area of routing. The fundamental idea of secret sharing is, the secret message is sending through a single specified path. 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 multiple independent paths. 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.

The objective is to maximize the security. The share allocation scheme achieves both data confidentiality and integrity. Assume that (T,N) secret sharing scheme is applied to the message to be protected at source node. A share allocation scheme is applied to M node disjoint paths. There are totally M paths such as [P_1, P_2... P_M] available from the source to the destination. But $P_1 \leq P_2 \leq P_3 \leq \ldots \leq P_{M.}$ paths are ordered from more secure one to less secure. If the path were not compromised all shares are in a safe condition. To allocate N shares onto the M available paths. The share allocation n= [n_1,n_2,….$n_{M]}$ where n_i is the number of shares allocated to path I, n_i is an integer and it is greter than or equal to 0.

P= [P_1, P_2... P_M] denotes the security characteristics of the paths, where Pi (i = 1,2,…,M) is the probability that the path i is compromised.

A share allocation scheme is used to allocate N shares onto the M available paths.

$$\underline{n_i} \geq 0, \sum_{i=1}^{M} n_i = N \tag{1}$$

n_i is an integer, $n_{i \geq} 0$

Atleast one share and at most T-1 shares are allocated to each of the available paths.

n= [n_1,n_2,….$n_{M]}$ number of shares allocated to path i. $1 \leq n_i \leq$T-1, I = 1,….,M

$$\sum_{i=1}^{M} n_i = N \tag{2}$$

According to the secret sharing scheme, the probability that the message compromised equals to the probability that T or more shares are compromised. At least one share and at most T-1 shares are allocated to each of the available paths. This share allocation forces the enemy to compromise all the paths to compromise the secret message. This probability equals to the probability that all the paths are cooperated. The probability that all paths are compromised is

$$P_{msg(n)} = \prod_{i=1}^{M} Pi \qquad (3)$$

The maximum security depends only on the selection of the path. P_i is a probability for satisfying $0 \leq Pi \leq 1$. More number of paths to distribute the shares with less probability and more security of the data is delivered.

The dispersion of voice is shown in Figure 4. The arrangement of nodes is called Dumbell topology. The secrets are shared via multiple paths.

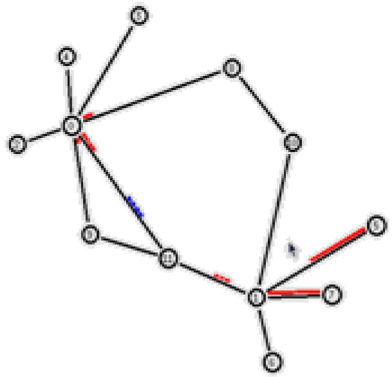

Figure 4 Dumbbell Topology of VoIP

The Parameters considered are Increased Path, Varying Cost and Various Codecs.

The algorithm is

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

$$Pstate(s) = \prod_{i=1}^{M} Pi^{Si(1-p)^{1-Si}} \qquad (4)$$

Where i varies from 1, 2,…. . , m.

Create set S′□ , 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

- $N \geq n_{1\geq} n_{2\geq} \ldots\ldots \geq n_m \geq 0$
- $\Sigma\, n_i = N$ 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 S′□ ; or they are sub-optimal share allocations if more elements present in set S′□

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

This scheme is Resistive towards the following Attacks Eavesdropping, Malicious Intruders and Cheating Detection. The data drop is a serious issue and is shown in Figure 5. The chance of drop is very low in this scheme because shares are sending multiple paths. But sometimes, there may be packet drop occurs due to heavy load or bad channel condition and less bandwidth.

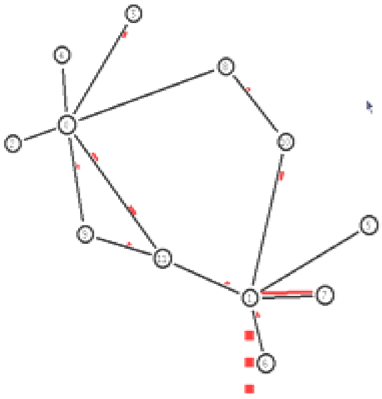

Figure 5 Data Drop in Dumbbell Topology of VoIP

The sender of VoIP may be phone or PC receives signals from microphone. The speeches are divided in to shares. The shares are sending through a multipath router. The shares are sending through multiple paths. During this voice transmission, it may be eavesdropped. This arrangement is shown in Figure 2. The receiver receives from multipath receiver router.

4. SIMULATION RESULTS

The area of network security consists of the policies and provisions of network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network accessible resources. The access of data is controlled by network administrator. The area of network security starts with authenticating the user with the username and a password. This is called one factor authentication. The user has mobile phone, ATM card and security token. These are two factor authentications. The user will also use finger print or retinal scan. This is known as three factor authentication.

Once authenticated a firewall enforces security access mechanisms to prevent unauthorized access. This factor may fail to verify the harmful content such as computer worms, Trojans being transmitted over the network. These malwares are controlled by anti-virus software or an intrusion prevention system. Communication between two systems may be encrypted to maintain privacy. It is possible to allow packets with the same source and destination to take multiple paths. The advantage if this is to reduce congestion and recovering node failure.

6.4.1 Effects on End-to-End Delay

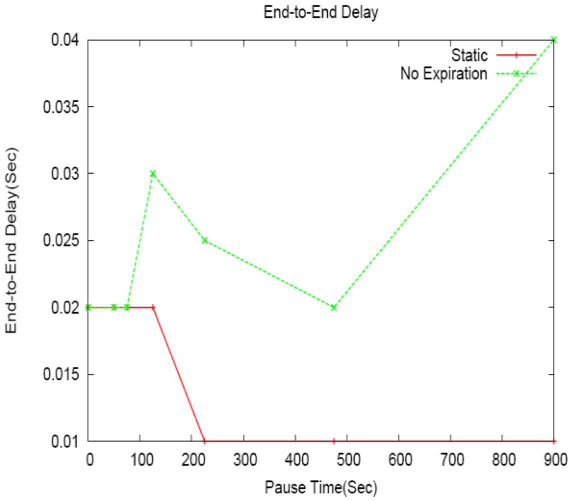

Figure 6 Times versus Delay in Multipath

There is a probability of multiple paths found in the simulation environment. The increased number of paths increases the security level. The increased level of paths based on the cost spent for this route. The number of path determines the security level of the network. The static life time value shows very less amount of delay in this figure 6. The reason behind this is the alternate path facility. The route error will not create any routing overhead because there are more paths. In this simulation the reduced delay is achieved.

Latency is the time that elapses between the initiation of a request for data and the start of the actual data transfer. This delay may be in nanoseconds, milliseconds and seconds but it is still used to judge the efficiency of networks.

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

6.4.2 Effects on Path Finding

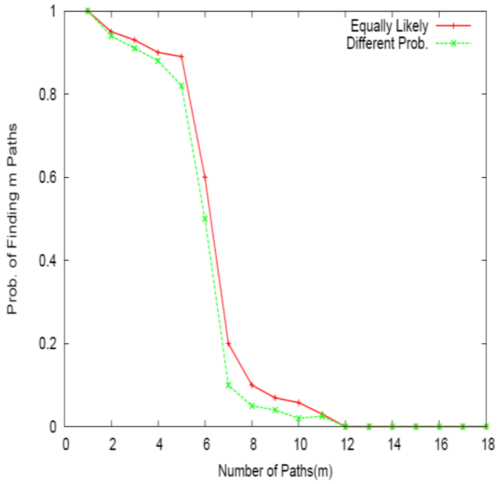

Figure 7 Number of Paths versus finding Paths

The Probability of path finding is a difficult process in networking environment. But if there are more paths, the delivery is more with less time. The speed of transmission and above 98% of delivery is assured in this scheme. The more paths are finding in this scheme and are shown in figure 7. The most secure path is discovered and added to the list of paths. Each time a new path is added, the transformation is performed. The dijsktra’s algorithm is used to find the more secure path.

Internet congestion occurs when a large volume of data is being routed on low bandwidth lines or across networks that have high latency and cannot handle large volumes. The result is slowing down of packet movement, packet loss and drop in service quality.

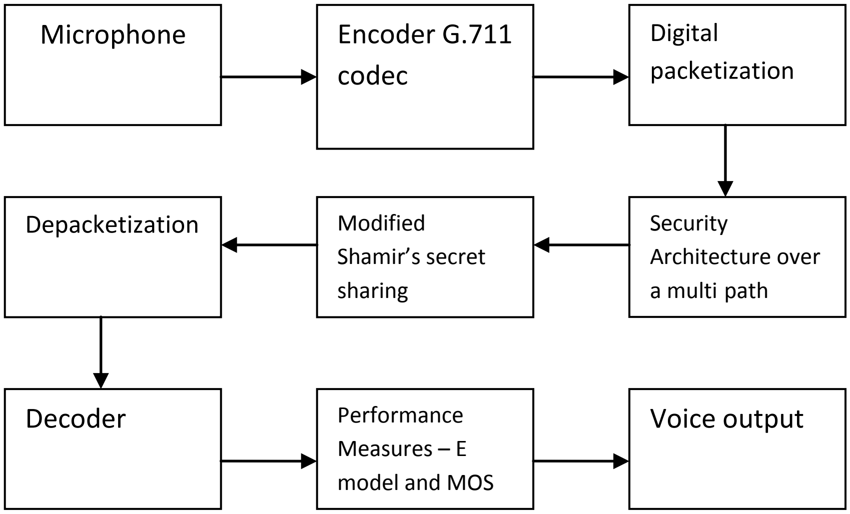
Microphone
Encoder G.711 codec
Digital packetization
Security Architecture over a multi path
Modified Shamir's secret sharing
Depacketization
Decoder
Performance Measures – E model and MOS
Voice output

Figure 2: Architecture of Secret Sharing over Multipath Routing

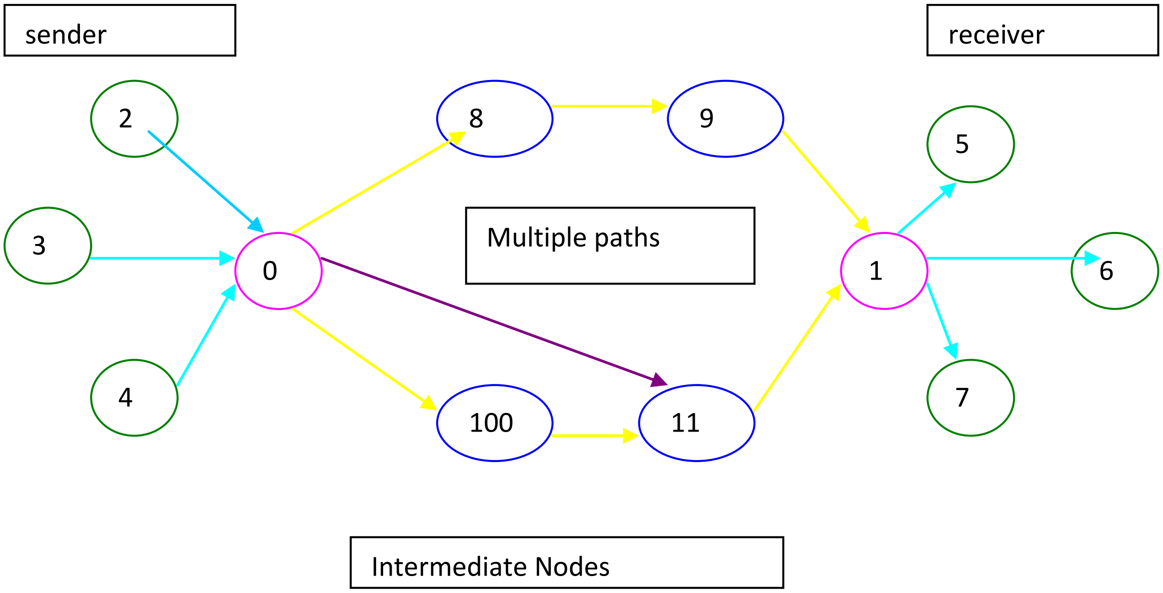

Figure 3: Structural Design of Secret Sharing over Multipath Routing

5. CONCLUSION

To operate this scheme effectively, nodes must maintain routing tables to specify the link connectivity. The weights in the table represent the probability of the link being chosen for the destination specified. It is simply a path length of one node to another. A random number will decide where the packet actually goes. All packets in a conversation take the same route.

6. REFERENCES

[1] Dr.As'ad mahmoud As'ad alnaser, "secure data transfer based on multipath routing, International journal of academic research, vol 3,No.3,may 2011.

[2] Aristotelis Tsirigos and Zygmunt J.Haas, "Multipath routing in the presence of frequent topological changes", IEEE communications magazine,Nov 2001.

[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, 1999, pp: 148-164, 1999.

[4] Binod Vaidya, Joel J.P.C.Rodrigues and Hyuk Lim, ”Secure multimedia streaming over multipath wireless Ad hoc network: Design and Implementation”.

[5] D.Butcher ,X.Li, and J.Guo, ”Security challenge and defence in VoIP infrastructures”, IEEE trans. Systems, man and cybernetics- part c:Applications and reviews , vol 37,no.6,pp. 1152-1162,nov 2007.

[6] E.Gustafsson, G.Karlsson,” A literature survey on traffic dispersion”, IEEE networks, Apr 1997.

[7] Hanoch, Levy, Haim, Zlatokrilov,” the effect of packet dispersion on voice applications in IP networks”, IEEE / ACM transactions on networking.

[8] Hong Li and LorneMason,”multipath routing with adaptive playback scheduling for voice over IP in service overlay networks”.

[9] Housam Al-Allouni, Alaa Eldin Rohiem, Mohammed Hashem Abd El-Azizahmed,Ali El-Moghazy, ”VoIP Denial of Service Attacks Classification and Implementation,26th national radio science conference, march 2009.

[10] Hugo Krawczyk,”secret sharing made short”, 1998, Springer-verlag. [HKH09] Hui Tian , Ke Zhou, Hong Jiang, Jin Liu,Yongfeng Huang, Dan Feng, ”An M-sequence based steganography model for voice over IP”, publication in the IEEE ICC 2009 proceedings.

[11] D.B.Johnson,D.A.Maltz,Y.C.Hu,J.G.jetcheva, ”the dynamic source routing protocol for mobile ad hoc networks”, Nov 2001.

[12]]JoongMan Kim, SeokUng Yoon, HyunCheol Jeong, YooJae Won,” Implementation and Evaluation of SIP-based Secure VoIP Communication System”, IEEE/IFIP International Conference on Embedded and Ubiquitous Computing,2008.

[13]] Joongman kim, seokung yoon, yoojae won, jaeil lee, ”VoIP secure communication protocol satisfying backward compatibility”,second Intrntional conference on systems and networks communications,IEEE,2007.

[14] Kevork R. Piloyan, Vahé Nerguizian, “Novel Architecture for Routing Packetized Voice over Existing Internet Infrastructure without Using the Internet Protocol”, IJCSNS International Journal of Computer Science and Network Security, VOL.6.No.7B, July 2006.

[15] S.J.Lee and M.Gerla,” Split Multipath routing with maximally disjoint paths in ad hoc networks”, proc. of Int. Conf. on Communications, vol.10, pp.3201-3205, June 2001.

[16] Ryouichi Nishimura, Shun-ichiro Abe, Norihiro Fujita and Yoiti Suzuki,” Reinforcement of VoIP security with multipath routing and secret sharing scheme”, Jouranl of information hiding and multimedia signal processing, 2010,Vol 1,number 3, July 2010,ISSn: 2073-4212.

[17] A. Shamir, “How to Share a Secret”, Communications of the ACM, 22(11):612-613, November 1979.