EFFECTIVE VOICE CALLS ADMISSION FOR AUTHORIZED USER IN INTER VOIP NETWORK

Subashri T[1], Vaidehi V[2]

[1,2]Department of Electronics, MIT Campus, Anna University, Chennai-44
tsubashri@annauniv.edu[1], vaidehi@annauniv.edu[2]

ABSTRACT

IP based voice transmission technology is a flexible, simpler and a cost effective implementation of voice transmission. It provides a real convergence of various networks. This voice transmission technology does not support a quality that is equivalent to digitized voice, which is available in the existing PSTN networks. In addition to this, data network vulnerabilities affect the VOIP service causing a drop in the utilization of voice communication. In this paper, the quality of service for voice calls is ensured with the integration of CAC mechanism with the bandwidth link utilization which makes an estimation of the demanded bandwidth. In terms of security, prevention of ARP cache poisoning attack is achieved by use of the signed MAC address response in local area networks. It makes the network confident that the admitted user is an authorized user and also it verifies that only the authorized users' information is exchanged over the local area network. Also an approach that makes it difficult for the hacker's to hack the data exchanged over the quality channel has been proposed.

KEYWORDS

Bandwidth link utilization, CACA, LU-CAC, MAC addresses Hash value.

1. INTRODUCTION

With the growing speed of large scale internet industry it is now possible to transmit all real time data over the internet protocol. The internet protocol plays a major role in the real time services offered in the internet world. One such technology is voice over internet protocol. Sending digitized voice over the internet protocol is an approach to make voice call. VOIP is an attractive technology and it is adopted in home and business environments, because of their cheaper call rates compared to the PSTN based fixed networks and it also provides greater flexibility in terms of added features in addition with the existing voice communication techniques. As the IP based networks do not have CAC mechanisms the new flow would suffer packet loss and/ or significant delay. To prevent this, QoS is guaranteed for both new and existing calls by the decision making process of CAC mechanism, introduced in the IP networks. The PSTN network consists of call admission control mechanism. If the number of calls exceeds the capacity of the links, the request for new calls will be rejected while all the other calls in progress continue without any problem.

The admission of a voice call is done by the CACA (Call Admission Control Agent) [1]. But in the case of IP based VOIP networks, this CAC mechanism is not provided, and hence QoS will not be guaranteed. The traffic which keeps entering the network even beyond the networks capacity limit consequently causes both the existing and the new flows to suffer packet loss and /or significant delay [2]. By the CAC mechanism integrated with the call manager, the rejection of voice calls and QoS is guaranteed. A very important aspect from the corporate point of view for the lack of success of VOIP technology is its security. VOIP technology is integrated with the workplace making the hacker's job easier if packets are routed through unsecured data packets on a public network.

The transmissions of speech across data networks are mostly vulnerable to attacks. Thus the attacker poses a threat to the security services which is available in the VOIP network. Different

DOI : 10.5121/ijnsa.2010.2416

attacks cause several changes towards the secured information. Depending on the kind of attack several changes have to be made to the security of a network. Some of the security attacks may prevent use of all the available user resources. Thus all the services and features available to the enhanced users are destroyed making the purpose of the VOIP communication a failure due to this security problem. Quality ensured user authentication is very important for VOIP conversation. Without this verification for authentication, all the calls may get dropped even if the user resource quality is enhanced. In this paper, an approach which ensures that the authorized user is able to get the enhanced QoS guaranteed channel for their communication is provided by the integration of CAC mechanisms with user authentication procedure at the server [3]. This paper is organised as follows: chapter 2 gives the details of admission of voice calls, chapter 3 presents proposed method for securing ARP cache poisoning and chapter 4 discusses the experimental results for admission of voice calls using delay analysis and continued by the verification of prevention of ARP cache poisoning attack. Finally, conclusion is given in the chapter 5.

2. Admission of voice calls using delay analysis method in differentiated Services

Call manager provides the overall framework for communication within a corporate environment. Gatekeeper provides address translation and admission control services to the calls. Call manager and gatekeeper communicate with each other by using the H.323 signalling protocol as shown in Figure 1. A location defines the topological area connected to other areas by links with a limited bandwidth that are registered to a call manager. A zone is a collection of H.323 endpoints that have been registered with the gatekeeper.

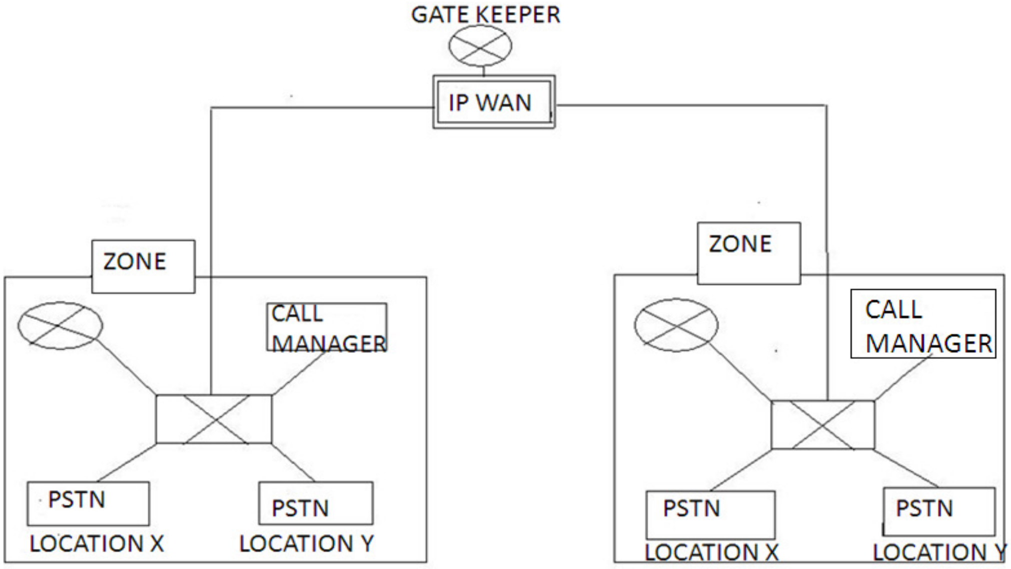
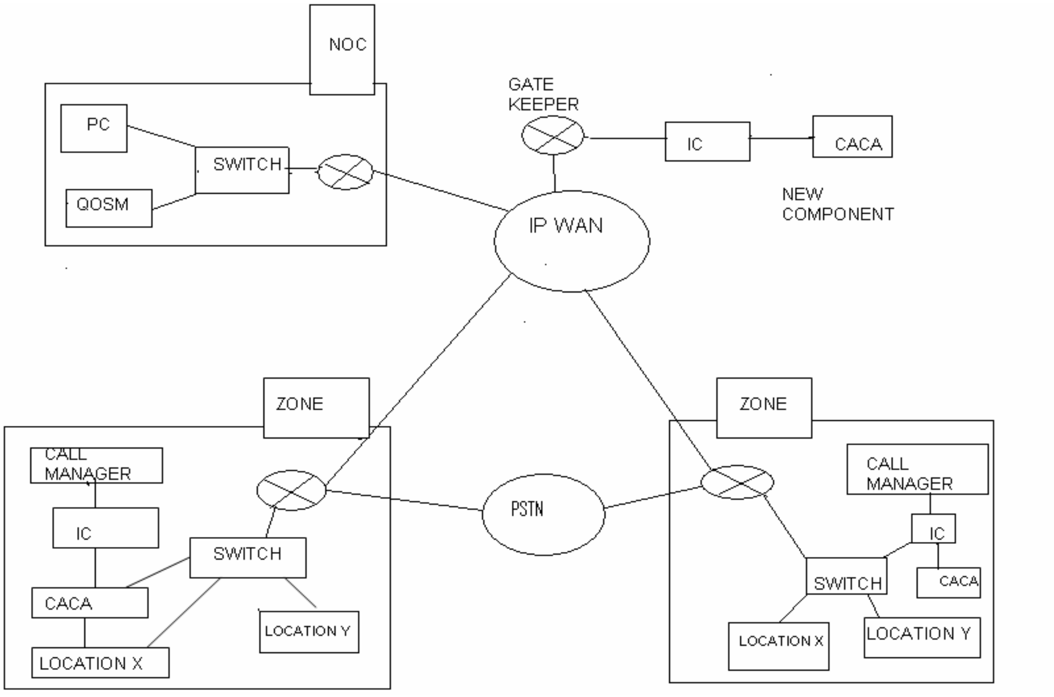


Figure 1. Block Diagram of the VOIP system

Call Manager as well as Gatekeeper performs admission control for calls between locations in a zone or calls between zones, aiming to provide a certain degree of QoS to voice over IP networks. To call within a zone, only the Call Manager located in the enterprise environment is invoked to perform CAC. However, for a call traversing multiple zones, not only Call Managers but also the related Gatekeeper may be involved to perform CAC.

The QoS-provisioning system is integrated into the current VoIP systems to enable both Site utilization based Call Admission Control (SU-CAC) and Link Utilization based Call Admission

Control (LU-CAC) to be well utilized and supported. With this system, the overhead of resource reservation at the core routers will be pushed to the agents in the QoS-provisioning system, which overcomes the weakness of the current VoIP system [2] in applying the LU-CAC, performing resource allocation to better support the SU- CAC mechanism.



F

igure 2. Block Diagram of QoS Provisioning VoIP system

This VOIP QoS-provisioning system consists of a Call Admission Control Agent (CACA) and the Integration Component (IC) as shown in Figure 2. The CACA has two modules. They are Utilization Computation Module and Admission Decision Module. The Integration Component (IC) integrates CACA with the existing VoIP systems. IC in the VOIP system provides call signalling process modules to monitor and intercept the call setup signalling from Gatekeeper or Call- Manager, and retrieves the useful message and passes it to the CACA. Call admission decision is made by the CACA.

2.1 Components of the QoS-Provisioning System

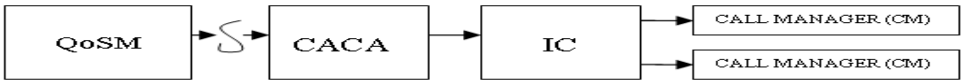


Figure 3. Components of the QoS-provisioning system

Figure 3 shows the components of QoS provisioning system. The function of QoS manager is to provide user interface to control and monitor components. It provides registration to the distributed agents and co- ordination among the distributed agent in the same QoS domain. It co-operates with the peer QoSMs that belong to other QoS.

There are two sub modules on call admission control agent, namely utilization computation module, and admission decision making module. Utilization computation module performs deterministic (or) statistical delay analysis to obtain the maximum bandwidth utilization. The admission control is done with specific CAC mechanism by using the admission decision making module.

2.2 Existing solutions for call admission control mechanism

It is necessary to frame a methodology for providing absolute differentiated services for real time applications which can be used to derive delay bounds without specific information on flow population [6]. S. Wang and D. Xuan authors has proposed a method which employs a utilization based admission control approach for flow admission which does not require delay computation at admission time, and hence scalable to larger systems. Static Priority Schedulers [3] in differentiated service networks assign priorities on a class by class basis, with the same priority for each class and on each router [5], Thus allowing different routers to assign different priorities to classes achieving significantly higher utilization bounds in the absolute estimation of differentiated services[9][12].

As priority assignment has direct impact on the delay performance of individual packets in static-priority networks, it must be carefully addressed. In the DiffServ domain, applications are differentiated by their classes. Accordingly, previous studies [4],[7],[8] assume that priorities are assigned on a class basis only, where all the flows in a class are assigned the same priority [10],[11]. Generalized priority assignment algorithms, where the flows in a class may be assigned different priorities and flows from different classes may have the same priority.

A good survey in both absolute and relative differentiated services has been done by authors D. Xuan and R. Betti in proposed premium service model, which provides equivalent of a dedicated link between two access routers. It provides absolute differentiated services in priority driven scheduling networks with two priorities, in which the higher priority is reserved for premium service [7]. An algorithm which provides both guaranteed statistical rate delay bounds and address scalability through traffic aggregation and statistical making is described to provide guaranteed service without per flow state management by using a technique called Dynamic Packet State (DPS) has been proposed by S. Blake et al[10].

The admission control needs to be explicitly computed to verify delays for the new and exciting flows for every new flow request. As the number of flow requests increases, this procedure becomes too expensive [11]. In such cases, UBAC (Utilization Based Admission Control) is used [1][2]. Although UBAC was primarily proposed for pre-emptive scheduling of periodic tasks on a simple processor, it is also used for centralized systems. In the case of aggregate scheduling, flow and population insensitive delay analysis has been done [13]. Lower bounds on these analyses are a function of network utilization, max hop count and other shaping parameters that are independent of network topology. A better delay bound is derived in static priority scheduling network which primarily focuses on real time communication applications within DiffServ domains. Priority assignment methods for ring network and ATM networks are the two specific areas of concern within DiffServ domains [11].

It is observed that the existing methods are not capable of meeting the deadline requirement. Hence this paper proposed, Deterministic delay based method for guaranteeing end to end delay.

2.3 Design of a Call Admission Control Agent (CACA)

The Call Admission Control Agent (CACA) is a key component in the QoS- provisioning system. It consists of two modules. The utilization computation module performs delay analysis and computes the maximum bandwidth utilization. It usually runs at the configuration time. The computed utilization will be allocated to LU-CAC mechanism. At the runtime, the admission decision making module will make an admission decision for each incoming call request, based on the allocated bandwidth utilization (by the utilization computation module) and the currently consumed bandwidth. The maximum link utilization is the maximum value of the link utilization under which the end to end delay can be guaranteed with LU-CAC.

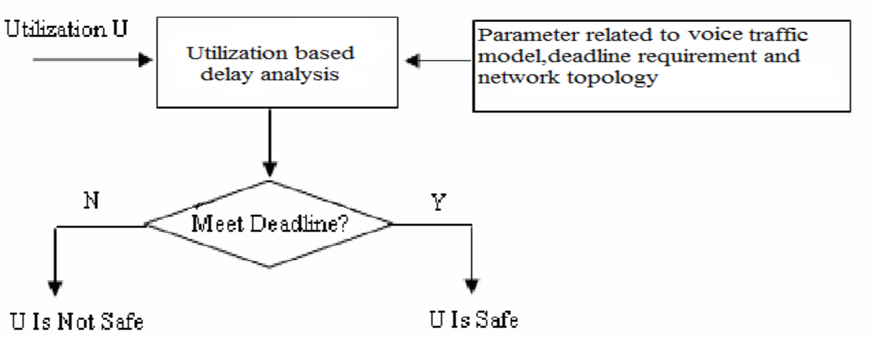

Utilization U
Utilization based delay analysis
Parameter related to voice traffic model,deadline requirement and network topology
Meet Deadline?
N
Y
U Is Not Safe
U Is Safe

Figure. 4. Utilization verification procedure

The utilization computation module has a sub module called Link Utilization Computation. The main task of this sub module is to compute the maximum link utilization for LU-CAC by calling a procedure, named utilization verification procedure. Given the voice traffic model, the network topology, and the voice traffic deadline requirement, for any input of link utilization U, the worst-case delay (deterministic case) or delay distribution (statistical case) with deterministic delay analysis methods is computed as shown in Figure 4. Then, it verifies whether the link is safe or not for ensuring the end-to-end delay to meet the deadline.

Generally, there are two distinct types of delays suffered by a voice packet from source to destination: fixed and variable. Fixed delays include propagation delay, transmission delay, and so on. Variable delays arise from queuing delays in the output buffers. All fixed delays can be obtained by well-known experimental data or by using existing tools. However, it is difficult to obtain the variable delays. Therefore, all the calls currently established in the network must be known in order to compute queuing delays.

2.4 Utilization-based Deterministic Delay Analysis

If the deadline requirement is deterministic, then the worst-case queuing delay d_k suffered by any voice packet and the buffer of output link 'k'is bounded by

$$d_k \leq \frac{c_k - 1}{c_k - u_k} u_k \left[\left(\frac{\sigma}{\rho} \right) + y_k \right] \tag{1}$$

$$c_k = \left(\sum_{i \in I} c_i \right) / c_m \tag{2}$$

Where c_k is the capacity of the link. σ is the burst size, ρ is the average rate at the entrance of the network, u_k is the utilization of the link. y_k is defined as the worst case queuing delay bound suffered by any packet upstream from layer-k and it is given by,

$$y_k = \sum_{l=1}^{k-1} d_l^{\wedge} \tag{3}$$

$$d_k^{\wedge} = r\left(\frac{\sigma}{\rho} + y_k\right) \tag{4}$$

By using the equation (3) and (4) we get,

$$d_k^{\wedge} - d_{k-1}^{\wedge} = r\, d_{k-1}^{\wedge} \tag{5}$$

$$d_k^{\wedge} = (r+1)\, d_{k-1}^{\wedge} = (r+1)^{(k-1)}\, d_l^{\wedge} \tag{6}$$

We know that delay of link $d_l^{\wedge} = \mathrm{r}\ (\sigma/\rho)$, therefore, $d_k^{\wedge}$, the maximum of worst-case delays suffered by any voice packet at layer-k link servers, can be bounded as follows,

$$d_k^{\wedge} \le r\left((r+1)^{k-1}\right) * \left(\frac{\sigma}{\rho}\right) \tag{7}$$

y_k can be bounded as,

$$y_k \le \sum_{l=1}^{k-1} d_l^{\wedge} \le \sum_{l=1}^{k-1} r(r+1)^{(l-1)} \left(\frac{\sigma}{\rho}\right) = ((r+1)^{k-1} - 1) \tag{8}$$

Therefore the maximum end to end delay can be bounded as

$$d^{e2e} \le y_{h^{\wedge}+1} \le ((r+1)^{(h-1)} \frac{\sigma}{\rho} \tag{9}$$

2.5 Utilization-Based Statistical Delay Analysis

If the deadline requirement is probabilistic, as in this case, d_k is a random variable and D_k is denoted as its deadline. The violation probability of delay for any voice packet with the highest priority suffered at the buffer of output link k is bounded by

$$\mathbf{P}(\mathbf{d_k} > \mathbf{D_k}) \le \begin{cases} {}^{1}/_{\sqrt{2}} \prod \left[\exp\left(-24 * \left(1 - \frac{u_k}{u_k^2}\right) * \left(\frac{D_k}{\frac{\sigma}{\rho}}\right)\right)\right], u_k \ge {}^{D_k}/_{\frac{\sigma}{\rho}} \\ {}^{1}/_{\sqrt{2}} \prod \left[\exp\left(-6 * \left(1 - \frac{u_k}{u_k^3}\right) * \left(u_k + \left(\frac{D_k}{\left(\frac{\sigma}{\rho}\right)}\right)^2\right)\right)\right], u_k \ge {}^{D_k}/_{({}^{\sigma}/_{\rho})} \end{cases} \tag{10}$$

The end to end deadline violation probability can be bounded as,

$$P\left\{d^{e2e} > \sum_{k\in R} D_k\right\} \leq 1 - \prod_{k\in R}\left(1 - P\{d_k > D_k\}\right) \tag{11}$$

The utilization-based delay analysis techniques shows that, under the given network topology and traffic model, the queuing delay or deadline violation probability at each output queue depends on link bandwidth utilization. By limiting the utilization of link bandwidth, the overall delay or deadline violation probability can be bounded. Given the deadline requirement, with the utilization-based delay analysis techniques, the maximum link utilization computation can obtain the maximum link utilization, which will be applied in the LU-CAC mechanism to perform admission control.

2.6 Site Utilization Computation based CAC (SU-CAC)

The main task of this sub module is to compute the maximum site utilization for SU-CAC. Site utilization computation SU-CAC mechanism tends to underutilize the network resource while providing end-to-end delay guarantees. The objective in the maximum site utilization computation is to optimize the overall site bandwidth utilization. The proposed maximum link utilization computation will be based on the end to end link maximum utilization computation and further splitting each maximum link utilization to the pair of sites that share this link. Given the network topology and the limitation of link, bandwidth is allocated to the voice traffic and the overall bandwidth utilization to sites is optimized as follows:

$$\text{Maximize} \sum\nolimits_{R} u_{R} \tag{12}$$

$$\text{Subject to} \sum\nolimits_{R\in k} u_{R\leq} u_{k}\text{, for each link k} \tag{13}$$

$$u_{R}^{0} \leq u_{R}^{1}\; u_{R}\text{, for each route R} \tag{14}$$

Where u_k is the maximum bandwidth of link k allocated to voice traffic $R \in k$ represents all routes among any pair of sites R going through link k, u_R is the bandwidth of R allocated to voice traffic, u_R^0 and u_R^1 are the lower and upper bandwidth bounds for R allocated to voice traffic. In the above equations, (12) is the overall bandwidth utilization, (13) shows that the bandwidth preallocation to each pair of sites is being constrained by the link bandwidth limitation, and (14) is the user requirement for bandwidth preallocation to each pair of sites. This is a linear programming problem, which can be solved in polynomial time. The output, i.e., the preallocated bandwidth, will be used as the bandwidth limitation in the SU-CAC mechanism.

3. Proposed Method for Securing ARP Cache Poisoning Attack

Here, an approach for the secured ARP request and response between the client and the server is proposed. The block diagram of ARP cache prevention architecture is presented in Figure 5. Client 1 needs the MAC address of the client 2 in the network for making communications. ARP program in client 1 gives the MAC address of client 2 from its ARP cache table. If client 2's address is not found in the ARP cache table, it sends the request to the server and tries to find the MAC address of client 2. The ARP table contains the IP and MAC address of the clients. The table is available for the use of the two clients involved in the communication and remains invisible to the other clients. In the server, broadcasting of ARP request results in forged ARP replies from the hackers, causing false communication between the client and the hacker. Instead of broadcasting the request to the entire network, the newly created relay agent is used for processing the secure ARP request and response. Server relay agent takes the responsibility of sending the request and replying to the client in a secured manner, thereby establishing a proper user communication between the sender and the receiver.

After the client sends a request, the server relay agent sends a response which is hashed with SHA-256 algorithm and encrypted using the RSA algorithm. Therefore only the authorised clients who are all connected to the server relay agent are permitted to exchange these ARP requests and responses in a secured manner.

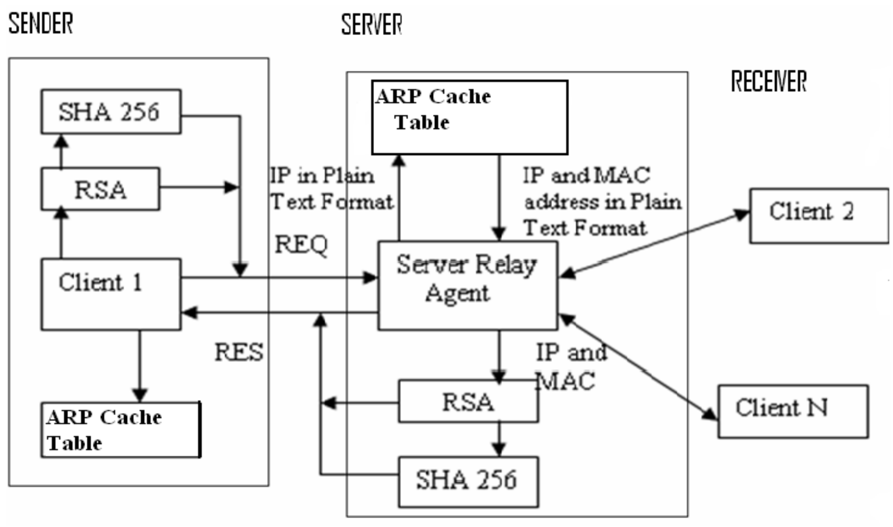


Figure 5. Block diagram of ARP cache prevention architecture

Thus the authorized client can decrypt and use this secured response from the server relay agent. After some time period, if client 1 is no longer communicating with client 2, then the system delete the entries in the ARP table. So it becomes for eavesdrop to poison the ARP request and reply. Since the clients can only request the server to give the destination's MAC address, the network broadcast overhead of ARP request is also reduced.

4. Experimental results for admission of voice calls using delay analysis method

4.1 Estimation of Queue Bandwidth

Network Simulator 2 is used to simulate the VoIP traffic. By using NS2 the queue bandwidth between the source and the destination node is simulated. In Figure 6, X axis represents time and Y axis represents bandwidth in Mbps.

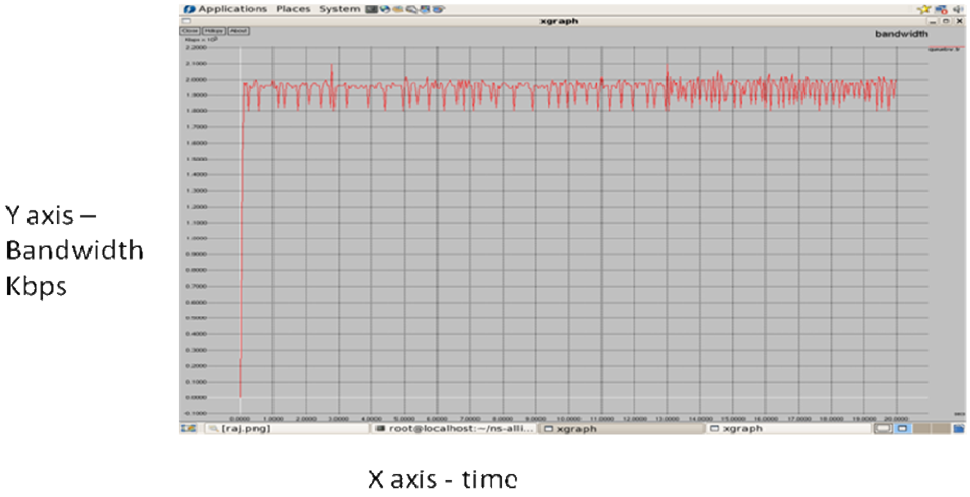


Figure 6. Queue bandwidth

4.2 Estimation of Queue size

Queue size is calculated between the source and the destination node. Queue size is the number of packets waiting in the queue between two nodes. By using the queue size the queuing delay can be calculated.

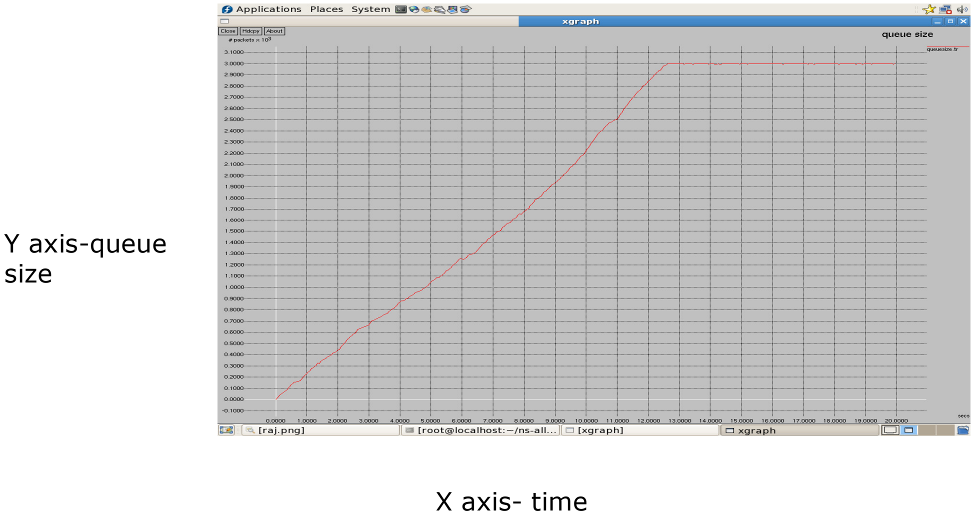
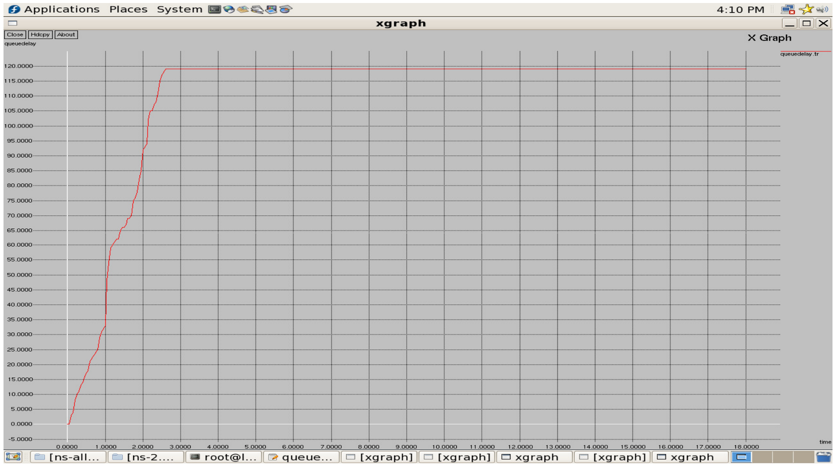


Figure 7. Queue Size

When the queuing delay is lesser than or equal to deterministic delay then the utilization will be safe else the utilization will not be safe. Figure 7 presents the performance of CACA for variation in queue size. In this Figure, X axis represents queue size and Y axis gives the number of calls admitted. Figure 8 presents the performance of CACA for variation in queue delay. In this figure X axis represents time and Y axis gives the number of calls admitted.



Y axis- queue delay

X axis- time

Figure 8. Queue Delay

4.3 Admission decision Making Module

The admission decision making module supports both the LU-CAC and the SU-CAC mechanism. To support the LU-CAC mechanism, the admission decision making module manages the network topology information and the routing information. There are two tables in supporting this mechanism: the bandwidth table and routing table. The bandwidth table has the information about the consumed bandwidth by voice traffic and remaining bandwidth for calls as shown shown in the Table 1. The routing information can be found in the Table 2.

Once the call request comes, each link along with the call route will be checked to see if there is sufficient bandwidth available. The call route of the source and destination of the call is stored in the routing table.

link	overall bandwidth	available bandwidth
$link_1$	40.0 Mbps	21.0 Mbps
$\vdots$	$\vdots$	$\vdots$
$link_L$	35.0 Mbps	15.0 Mbps

Table 1: Bandwidth table

source	destination	links
src_1	dst_1	$src_1 \rightarrow \cdots \rightarrow node_1^i \rightarrow \cdots \rightarrow dst_1$
$\vdots$	$\vdots$	$\vdots$
src_R	dst_R	$src_R \rightarrow \cdots \rightarrow node_R^i \rightarrow \cdots \rightarrow dst_R$

Table 2 Routing table.

If all the links along the call route have sufficient bandwidth left, then the CAC module will admit the call and decreases the available bandwidth for further calls. If sufficient bandwidth is not available, further calls are rejected. Once the call tears down, bandwidth requested by the call will be returned to the pool for each link along with the call route.

4.4 Simulation results of estimated and actual link

Figure 9 presents the estimated utilization of the link bandwidth as a function of time obtained using NS2. The estimated utilization represents the overall utility of link that can be used by the voice traffic. Figure 10 presents the actual utilization of the link bandwidth as a function of time. The actual utilization represents the final utility of link for incoming voice traffic through a CAC mechanism. From the maximum bandwidth utilization it is possible to find whether the utilization is safe or not. For a period of 0.000 seconds to 0.002 seconds, the link bandwidth is not allocated to any of the users. .

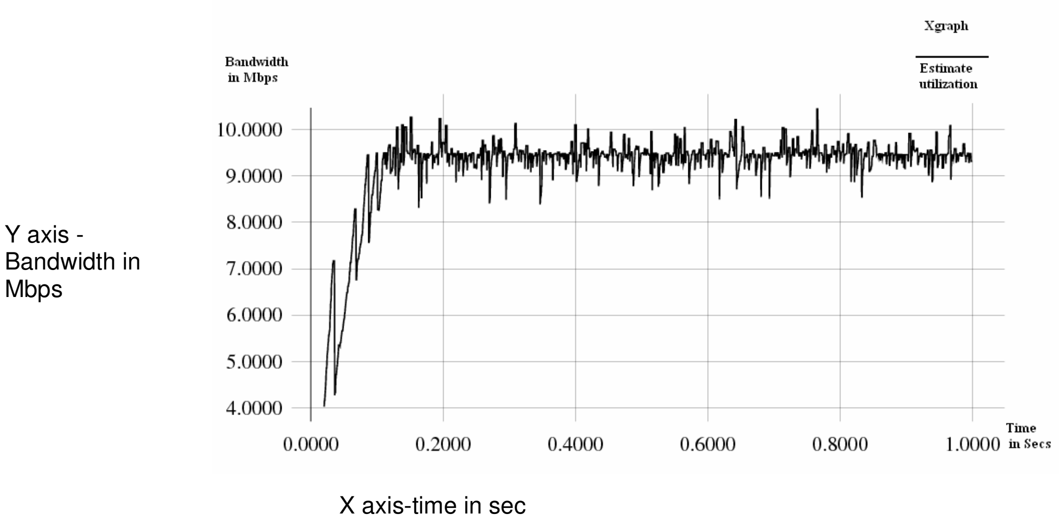


Figure 9. Estimated Link Utilization

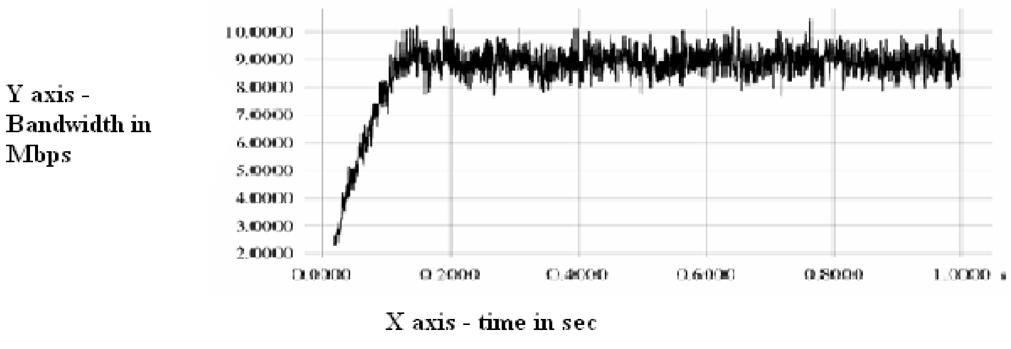
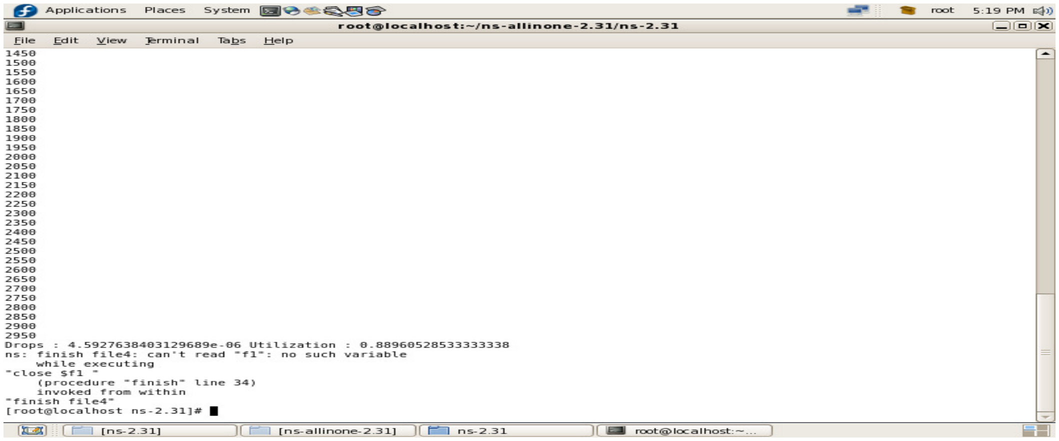


Figure 10. Actual Link Utilization

For a period of 0.18 seconds to 1.00 seconds the users are allowed to use an average of 95% bandwidth. The estimated utilization of link is obtained by using the utilization based delay analysis method. The actual utilization represents the final utility of link for incoming voice traffic through a LU-CAC mechanism. For a period of 0.00 to 0.02 seconds, the link bandwidth is not used by any of the users. From a period of 0.18 seconds to 1.00 seconds the users are allowed to use an average of 86.5% of bandwidth out of 95% of bandwidth. Some of the voice calls are blocked, where the requested bandwidth is more than that of the available bandwidth.

4.5 Packets drop of analysis

For a simulation period of 3000 seconds the total packets dropped is about 0.4% of original packets and the final utilization is about 88.9%. This is given in the Figure 11. Our utilization-based delay analysis techniques show that, under the given network topology and traffic model, the queuing delay or deadline violation probability at each output queue depends on the link bandwidth utilization. By limiting the utilization of link bandwidth, the overall delay or deadline violation probability can be bounded. Given the deadline requirement, with the utilization-based delay analysis techniques, the maximum link utilization can be computed, which will be applied in the LU-CAC mechanism to perform admission control.



```
1450
1500
1550
1600
1650
1700
1750
1800
1850
1900
1950
2000
2050
2100
2150
2200
2250
2300
2350
2400
2450
2500
2550
2600
2650
2700
2750
2800
2850
2900
2950
Drops : 4.5927638403129689e-06 Utilization : 0.88960528533333338
ns: finish file4: can't read "f1": no such variable
    while executing
"close $f1 "
    (procedure "finish" line 34)
    invoked from within
"finish file4"
[root@localhost ns-2.31]# █
```

Figure 11 Simulation of packets drop of LU-CAC mechanism

When the maximum link utilization is determined it is given as input to the utilization based delay analysis block. The Admission Decision Making Module can make the admission decision for the incoming calls, based on the overall bandwidth and consumed bandwidth.

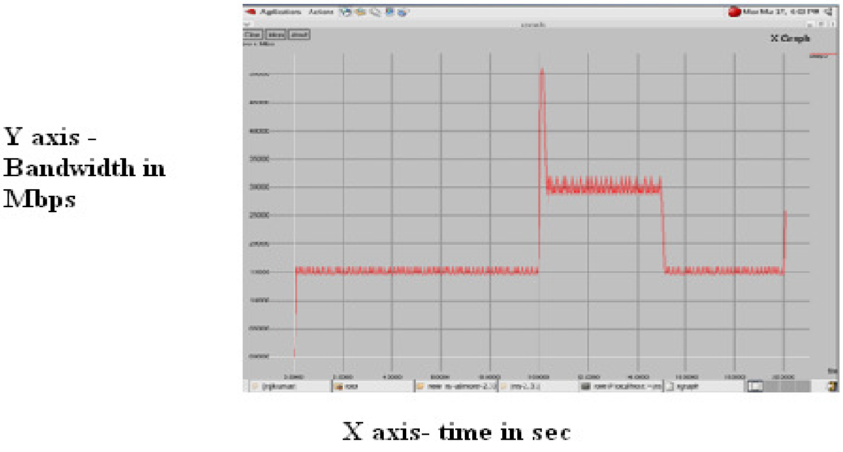


Figure 12 Deterministic delay estimation

Poisson distribution shows the exponential loss of packets (lambda) during call utilization. The call lifetimes also increases exponentially. The packets are not blocked for calls with an average lifetime of 180 seconds. Figure 13 presents the call admission probability as a function of time. It is observed that for a period of 0 to 4 seconds all the users get admitted offer which of user admission gets reduced due to packet loss.

Figure 14 gives the total packet drops without the CAC mechanism and with the CAC mechanism. Here Y axis represents the total number of dropped packets and X axis represents the time in seconds. For a period of 0 to 10 seconds there is no packet drops with CAC mechanism. But in the other case, the total number of packet drops gets increased even from zero seconds without CAC mechanism.

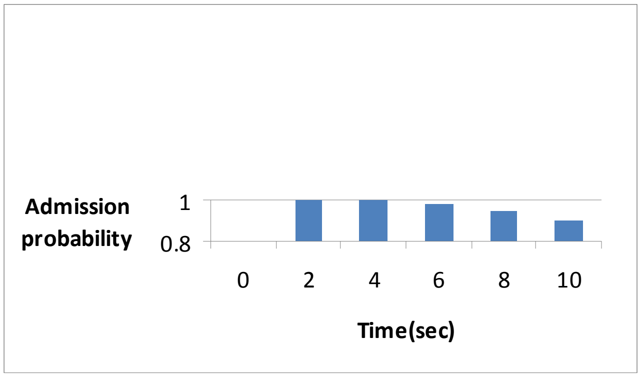


Figure.13. Probability of call admission as a function of time

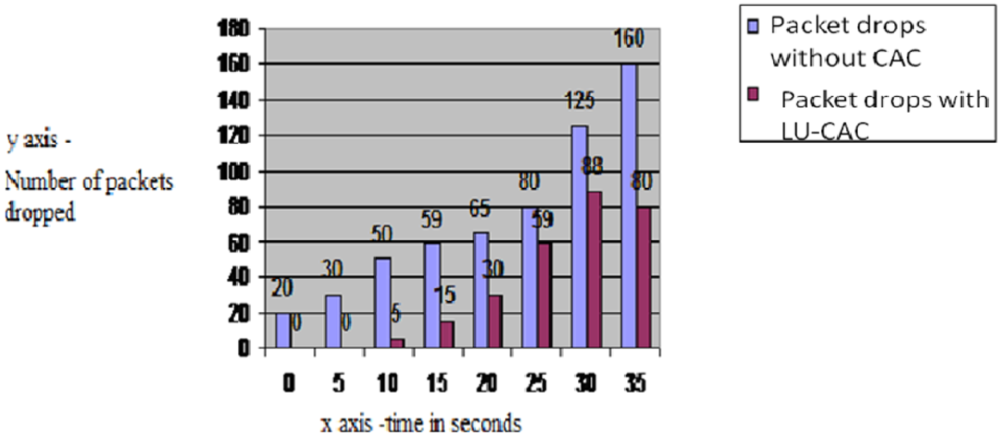


Figure.14. Packet drops with and without CAC mechanism

4.6 Performance of authenticated user voice admission procedure in VOIP Network

A call admission control mechanism offers service for 2 calls simultaneously. Due to limitations in space, only 4 calls are accepted for serving. Assuming with an example that 12 calls are arriving per day, their arrival pattern is determined to hold possion distribution. The service time for 2 simultaneous calls is exponentially distributed with μ = 8 calls per day. Hence their average number of calls in the service station, the average number of calls waiting for service and the average call lifetime can be calculated using the possion. The increase in performance of authenticated and unauthenticated user's access to the channel for voice calls are analyzed using probability based method. For example

Given λ= 12/day P (1) = probability of authenticated user wins all three calls
S=2 and k=4 P (2) = probability of losing all three calls
μ= 8/day P (3) = probability of winning of at least one trial

P`(n)=1-p(n-1)

$$P_0 = [\sum_{N=0}^{S-1} \frac{1}{n(\frac{\lambda}{\mu})} n + \frac{1}{S!(\frac{\lambda}{\mu})S} \sum_{N=S}^{K} (\frac{\lambda}{\mu S}) n - S] - 1$$

P_n is the probability of n^{th} trial

P(n) is the probability of winning the trail

E (N_q) = $P_0(\frac{\lambda}{\mu})S * \frac{\rho}{S!}(1-\rho)2[1-\rho K - S - (K-S)(1-\rho)K - S] = 0.4134$ calls (13)

Where ρ= (λ/ μ S)

E (N) average number of calls in the service station

E (W) is average number of calls waiting for service

E (N_q) is the q^{th} user call process at service station

E (N) =E (N_q) + S - $\sum_{N=0}^{S-1}(S-n)P_n$ = 0.4134 + 2- $\sum_{N=0}^{1}(2-n)P_n$ =1.73

E(W)=1/ λ E(N)

Where λ= μ[S-$\sum_{N=0}^{S-1}$(S-n) P_n = 0.1646 day

The probability that an authenticated user wins the channel access in CAC procedure against an unauthenticated user access is found to be 2/5. If each of authenticated and unauthenticated users makes three separate requests each to CAC mechanisms, then the probability of an authenticated user to win all three calls or lose all the three calls, or to win atleast one trial conveys the utilization of bandwidth within a link by an authenticated user. Consider three trails attempted by two users, the probability of authenticated user to win the first, second and third request respectively against an unauthenticated user is given below.

P (1) = P (2) =P (3) = (2/5), P (1`) = P (2`) =P (3`) = 1-(2/5) = 3/5. If the probability for first method is chosen by unauthenticated user then the entire bandwidth of the channel will be reserved for them.

4.7. Verification of ARP cache poisoning attack prevention within LAN

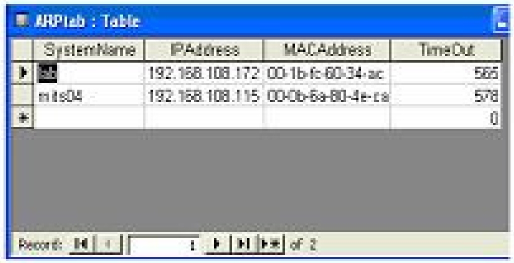
The following steps provide the pseudo code for verification of ARP cache poisoning attack prevention within LAN:

1. Get the ARP request from client 1 using server relay agent.

2. Broadcast the ARP request to all of its LAN users.

3. Get secured ARP response at the destination and send the destination MAC address to the sender.

Client to server communication has been simulated by using java socket programming. Clients send their IP address and MAC address to the corresponding LAN server through a link. The ARP cache table in the server updates the entries about the client. Any client within the same LAN can find the MAC and IP addresses of the other clients in the network. ARP request and response does this processes. Figure 15 shows that the updated entry for two clients in the ARP cache table in the server. If the IP address of the destination node is known, then the client can make a request to the server to know the MAC address.



ARPtab : Table

SystemName	IPAddress	MACAddress	TimeOut
[illegible]	192.168.108.172	00-1b-fc-60-34-ac	565
mits04	192.168.108.115	00-0b-6a-80-4e-ca	578
			0

Record: 1 of 2

192.168.100.108

Figure.15. ARP cache table updation Figure.16. Finding MAC address of the for 2 destination within LAN

This action has been explained in the Figure 16. In the client, destination IP address is encrypted and its hashed code value is determined. Figure 17 shows the exchange of the encrypted IP and MAC addresses and the figure 18 shows the decryption of these addresses and hence the correct IP and MAC addresses are obtained after the transmission. Thus the IP and MAC addresses are secured in the ARP request and response. The transmitted and received hash values are found to be equal and are displayed. Decryption process is applied to receive response. Verification of the generated key and received key ensures the secured ARP response for user communication. Decryption of the secured ARP response provides the destination MAC address to the server. By comparing the hashed codes of received and the generated values the authentication of the user is verified.

4.8 Verification procedure of ARP cache poisoning attack prevention on interwork

The following steps provide the pseudo code for verification of ARP cache poisoning attack prevention between LAN:

1. Get the ARP request from Client1 using server relay agent

2. Broadcast ARP request to all servers.

3. Send the secured ARP response from the destination along with MIC (Message Integrity code)

4. Get ARP response from server relay agent 2 for server relay agent 1 along with MIC.

When two users communicate with each other, if a secured VOIP call ARP should exit then cash poisoning attack should be prevented. For this reason a server relay agent has been created. This ensures secured ARP request. When broadcast happens Server relay agent additionally cares about security allowing only encrypted request and encrypted response.

Step 1, client 1 sends the request in encrypted form using RSA and the MIC1. The MIC1 is generated using a collision-free one-way hash function SHA256. Message digest using SHA 256 is calculated for the encrypted IP address. This statement "Client 1 Server Relay Agent: ARP req + MIC 1: (Message Integrity Code 1)" discloses the way of client to server interaction passing ARP request with message integrity code.

In step 2, once the server relay agent1 in LAN1 receives the request from the Client1, it calculates the message digest for the received encrypted IP address to create a similar MIC1 (say, MIC1*). If MIC1= MIC1*, then the request is accepted else it will be rejected. It will check the corresponding MAC address in its ARP table. The request will be the IP address of the Client1 which is in LAN2. Since the requested MAC address is in some other LAN the server relay agent cannot reply directly to Client1. Hence the request will be broadcasted to other server relay agent outside the network. This statement "Server Relay Agent1 broadcast the request to all the servers: ARP request + MIC 1"discloses about the server broad casting of ARP request to all the servers to find the destination.

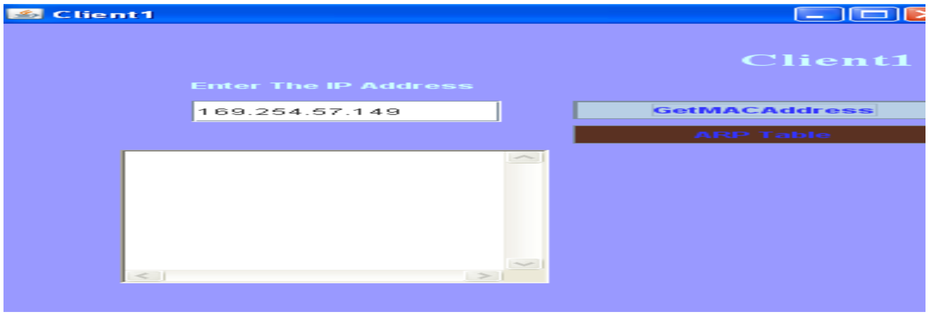
In step 3, the server relay agents in other LANs receive the request and check whether the corresponding MAC address for the request is there in its ARP table. If suppose server relay agent2 in LAN2 is having the MAC address for the requested IP address, it will reply to the server relay agent1 in LAN1. Server relay agent2 of LAN2 will get the public key of server relay agent1 of LAN1. Then it will encrypt the IP and MAC address and will calculate the message digest using SHA256 for the encrypted value. The response will be an encrypted value and MIC2 created using SHA256. This statement "Server Relay Agent 2 Server Relay Agent 1 ARP response + MIC 2"discloses the response of the sever relay 2 for the request of server relay 1. This response consists of identity of server relay agent 2.

In step 4, the server relay agent1 in LAN1 receives the response from server relay agent2 in LAN2. It will calculate the message digest for the received encrypted value. Then it checks whether the calculated message digest and the received message digest are equal. If both are equal, then it will send the response to the Client1 in LAN1. The response includes encrypted IP and MAC address and its MIC say MIC3.This statement "Server Relay Agent 1 ARP response + MIC 3" discloses the response of sever relay agent 1 with its own identity.

In step 5, the client receives the response and calculates the message digest for the received MIC and checks for the equality with the received MIC's. If both are equal, then it will decrypt the message and update the ARP table with the received time, else it will discard the reply and start requesting the server for the MAC address. Finally, the host A sends an acknowledgment. This statement "A Server Relay Agent 1: ACK" discloses the acknowledgement of server relay1.

4.9 Secured ARP request and ARP response analysis on internetwork

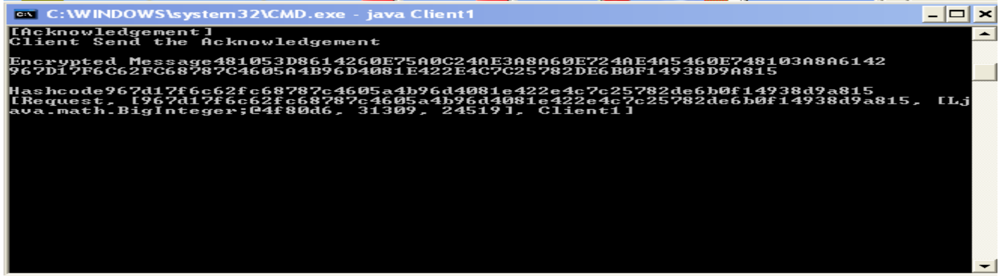
Figure 17 presents simulation of client 1 dialog module exchange with client 2 which gives the retrieval of client 2 MAC address for connectivity. After the entering destination address, client 1 encrypts the destination IP address using RSA algorithm and also encrypted IP address is given to hash algorithm to generate hash code for clients' identity.



```
169.254.57.149
```

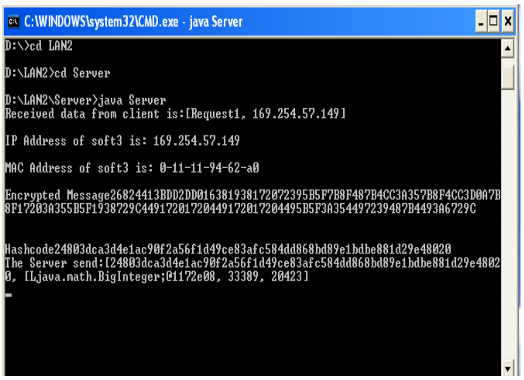
Figure 17: Finding destination MAC address between 2 clients.

Figure 18 presents the encrypted IP address for the user in LAN1 along with its message integrity code. Figure 19 and 20 present secured ARP response information exchange with transmission and reception. Figure 21 presents the comparison of generated and received hash code after the reception of secured response and Figure 22 presents the updation of destination MAC address by the sender.



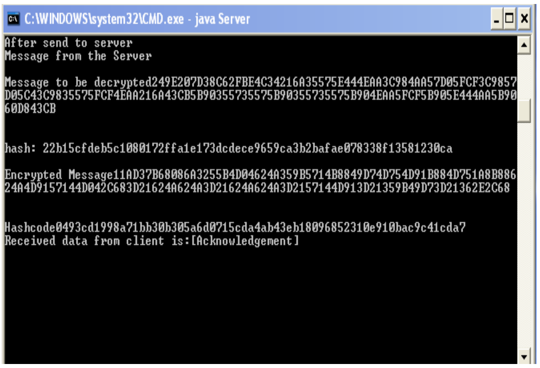
```
[Acknowledgement]
Client Send the Acknowledgement

Encrypted Message481053D8614260E75A0C24AE3A8A60E724AE4A5460E748103A8A6142
967D17F6C62FC68787C4605A4B96D4081E422E4C7C25782DE6B0F14938D9A815

Hashcode967d17f6c62fc68787c4605a4b96d4081e422e4c7c25782de6b0f14938d9a815
[Request, [967d17f6c62fc68787c4605a4b96d4081e422e4c7c25782de6b0f14938d9a815, [Lj
ava.math.BigInteger;@4f80d6, 31309, 24519], Client1]
```

Figure 18: Encryption of destination IP address and hashing of destination IP address.



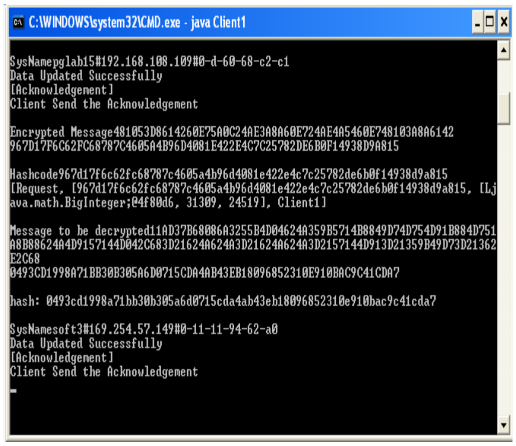
```
D:\>cd LAN2

D:\LAN2>cd Server

D:\LAN2\Server>java Server
Received data from client is:[Request1, 169.254.57.149]

IP Address of soft3 is: 169.254.57.149

MAC Address of soft3 is: 0-11-11-94-62-a0

Encrypted Message26824413BDD2DD016381938172072395B5F7B8F487B4CC3A357B8F4CC3D0A7B
8F17203A355B5F1938729C44917201720449172017204495B5F3A354497239487B4493A6729C


Hashcode24803dca3d4e1ac90f2a56f1d49ce83afc584dd868bd89e1bdbe881d29e48020
The Server send:[24803dca3d4e1ac90f2a56f1d49ce83afc584dd868bd89e1bdbe881d29e4802
0, [Ljava.math.BigInteger;@1172e08, 33389, 20423]
_
```

Figure 19: Secured ARP Response information exchange from server 2 to server 1.



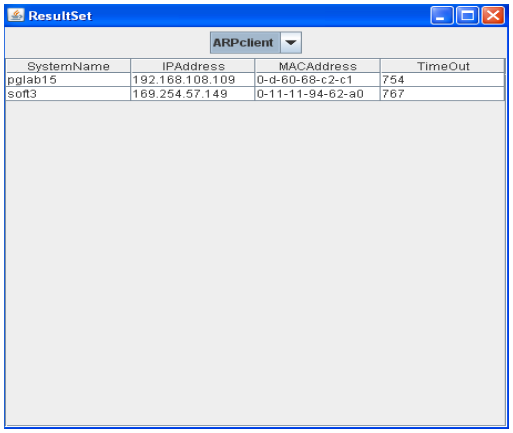
```
After send to server
Message from the Server

Message to be decrypted249E207D38C62FBE4C34216A35575E444EAA3C984AA57D05FCF3C9857
D05C43C9835575FCF4EAA216A43CB5B90355735575B90355735575B904EAA5FCF5B905E444AA5B90
60D843CB


hash: 22b15cfdeb5c1080172ffa1e173dcdece9659ca3b2bafae078338f13581230ca

Encrypted Message11AD37B68086A3255B4D04624A359B5714B8849D74D754D91B884D751A8B886
24A4D9157144D042C683D21624A624A3D21624A624A3D2157144D913D21359B49D73D21362E2C68


Hashcode0493cd1998a71bb30b305a6d0715cda4ab43eb18096852310e910bac9c41cda7
Received data from client is:[Acknowledgement]
```

Figure 20: Reception of secured ARP response in server1 from server 2.



```
SysNamepglab15#192.168.108.109#0-d-60-68-c2-c1
Data Updated Successfully
[Acknowledgement]
Client Send the Acknowledgement

Encrypted Message481053D8614260E75A0C24AE3A8A60E724AE4A5460E748103A8A6142
967D17F6C62FC68787C4605A4B96D4081E422E4C7C25782DE6B0F14938D9A815

Hashcode967d17f6c62fc68787c4605a4b96d4081e422e4c7c25782de6b0f14938d9a815
[Request, [967d17f6c62fc68787c4605a4b96d4081e422e4c7c25782de6b0f14938d9a815, [Lj
ava.math.BigInteger;@4f80d6, 31309, 24519], Client1]

Message to be decrypted11AD37B68086A3255B4D04624A359B5714B8849D74D754D91B884D751
A8B88624A4D9157144D042C683D21624A624A3D21624A624A3D2157144D913D21359B49D73D21362
E2C68
0493CD1998A71BB30B305A6D0715CDA4AB43EB18096852310E910BAC9C41CDA7

hash: 0493cd1998a71bb30b305a6d0715cda4ab43eb18096852310e910bac9c41cda7

SysNamesoft3#169.254.57.149#0-11-11-94-62-a0
Data Updated Successfully
[Acknowledgement]
Client Send the Acknowledgement
_
```

Figure 21: Comparison of generated and received hash Code



SystemName	IPAddress	MACAddress	TimeOut
pglab15	192.168.108.109	0-d-60-68-c2-c1	754
soft3	169.254.57.149	0-11-11-94-62-a0	767

Figure 22: Updation of MAC address by the sender.

In Figure 14, it is shown that in LU-CAC mechanism there is no packet drops below 10 sec. When a certain number of users try to get the link, only some of them are allowed to get the bandwidth based on the estimation of maximum utilization of link in the end to end estimation. If this end to end delay estimation is based on LU-CAC method, then the estimation of maximum utilization of the link is effectively calculated. The estimated average bandwidth by this method can be given assurance up to 86.5%. After the authenticated user's entry into the network area if he gets connected to unauthenticated user, then the entire bandwidth estimation will be used by the unauthenticated user. In a wired environment, the user's connectivity is based on the user's MAC address. Mapping IP address to MAC address is done by Address Resolution Protocol. ARP cache table maintains client's MAC address on the server cache. If cache table has the unauthenticated user's MAC address, there is a possibility of unauthorized user's voice calls getting connected. Hence there is reduction in bandwidth utilized by authorized users. To prevent this problem secured ARP request and secured ARP response is proposed.

Instead of allowing ARP response as such to the server ARP cache table, server allows only the secured ARP response to be updated by the ARP cache table. Figure 22 and 15 presents the time taken for detecting secured ARP request and ARP response and the updation of decrypted ARP response address informations in the ARP cache table. From these figures, the time taken for the complete secured ARP request and ARP response have been found as 700ns in inter LAN and 500ns within the LAN. So the total time to verify the user's authentication will not affect the VoIP packets transmission inside the LAN environment. Hence this method offers the effective utilization of maximum bandwidth available by only the users who are assured to be authenticated.

5 Conclusion

By integrating the Call Admission Control Agent (CACA) into the current VoIP system, the overall system can achieve high resource utilization while invoking relatively low overhead. In this paper, one of the confidentiality threats viz, ARP cache poisoning attack is considered and solution to the VOIP network system is proposed. Also, only secured clients are connected to the server and the server is allowed to provide client's IP-MAC mapping and their connectivity only to the intended client on the server's entry table. To provide message integrity for both client and the server, cryptographic hash function SHA256 is used. And for providing authentication for both the ends, RSA public key cryptosystem is used. RSA encrypts the network IP address and client's MAC address so that only the intended participants are allowed to decrypt and verify authentication at both ends. If a hacker tries to eavesdrop between the client and server, hacker cannot generate the message digest value of the client. So the Client's MAC address cannot be viewed by the hacker thus making the communication secure.

REFERENCE

[1] S.Wang, D.Xuan, R.Bettai, "Providing Absolute Differentiated services for Real time Application in Static priority scheduling networks," IEEE/ACM Trans. Networking, Vol.12, pp.326-339,2004.

[2] S.Wang, D.xuan,R.Betta, and W.zhao, "Differentiated Services with statistical Real Time Guraratees in static priority scheduling networks," Proc. IEEE Real time systems symp.Dec.2001.

[3] S.Chong and S.Li, Characterization based connection control for guaranteed services in high speed networks," Proc.IEEE Infocom,Apr.1995.

[4] S.Jamin,s.Shenkar,and P.Danzig, "Comparison of measurement basd admission controller-load service," Proc. IEEE Infocom,Apr.1997

[6] Christina L.Abad, "An analysis on the schemes for detecting and preventing ARP cache poisoning attack" IEEE processing ICDCSW'07

[7] R.Siva Kumar,T. Kim, N.Venkitataman and V.Bharghavan, "Acheieveing per flow weighted rate fairness in a core stateless network, processdings of IEEE ICDCS, march 2000.

[8] K.Nicols, jacobson, L.Zhang, A Two-bit differentiated services architecture for the internet, Internet Draft, Nov.1997.

[9] R.L.Cruz,SCED+: "Efficient management of quality of service guarantees, Proceedings of IEEE INFOCOM, March, 1998.

[10] S.Blake, D.Blake, M.Carlson, E.Davies, Z.Wang, and W.Weiss, "An architecture for differenciated service", RFC 2474,December 1998.

[11] I.Stocia,H.Zhang, Providing guaranteed without per flow management, proceedings of ACM SIGCOMM, August 1999.

[12] A.Dailians and A.Bovoupoulis, Real time admission control algorithms with delay and loss guarantees in ATM networks, IEEE proceedings, IEEE Proceedings of INFOCOM'94, 1994.

[13] G.Agarwal, B.Chen, W.Zhao,and S.Davari, "Guraranteeing Synchronous message deadlines with times token protocol,"Proc.IEEE Int'1 Conf.Distributed Computing Systems, June 1992.

Authors

V. Vaidehi received her B.E. in Electronics and Communication Engineering from College of Engineering, Guindy, M.E. in Applied Electronics and Ph.D. from Madras Institute of Technology, Chennai. She was a recipient of academic exchange fellowship of Association of Common wealth Universities. She has carried out funded projects on Tracking Algorithm for ship borne RADARS — funded by LRDE; GPS signal simulator — funded by Ministry of Information Technology; University Micro satellite — funded by ISRO; Semantic Intrusion Detection System — funded by Xambala Inc. Multi Sensor Data and Image Fusion, Power optimization in Wireless Sensor Network-funded by TCS. Currently she is a Professor and Head of Department of Information Technology, Madras Institute of Technology, Chennai. Her areas of interests are Networking, Parallel processing and Embedded systems.

Ms.T.Subashri received her B.E in Electronics and Communication Engineering from Thiayagarajar College of Engineering, Madurai, M.E in Communication Systems from Thiayagarajar College of Engineering, Kamaraj University, Madurai. Her areas of interests are Networking, cryptography & Network Security, Communication Systems. Currently she is pursuing her PhD from Anna University.