Paper: ASAT-14-260-CE

14th International Conference on
AEROSPACE SCIENCES & AVIATION TECHNOLOGY,
ASAT - 14 – May 24 - 26, 2011, Email: asat@mtc.edu.eg
Military Technical College, Kobry Elkobbah, Cairo, Egypt
Tel: +(202) 24025292 –24036138, Fax: +(202) 22621908

Performance Analysis for VoIP NAT Traversal in a Secured SIP System

A.D. Elbayoumy*, Y.M. Ehab†

Abstract: Voice over IP technology has rapid growth on network convergence in deployment of converged networks within enterprises. Most enterprises today sit behind Firewalls and also use private IP addressing behind NATs (Network Address Translators). These NATs cause significant problems for multimedia over IP to work and function properly. The de-facto Internet standard Internet Protocol (IP) is not secure. All types of business conducted through Internet, raised the requirement for a secure protocol. IP Security Working Group of IETF has been working on IPSec (IP Security) protocols to protect the IP traffic on the packet level. There are problems faced when an IPSec traffic is intended to pass through a NAT device. NAT and IPSec is very hard to use together without a standard way which would provide simple management and interoperability between vendors. Nowadays there are many techniques and solutions are used to allow popular applications to work through NATs. In this paper we present the details of the problem and issues associated with NATs and then survey some ways to solve this problem in SIP which aspire to become the dominant protocol on the internet for establishing calls. As a case study, we simulate a VoIP network and study the behavior and quality of VoIP under this model. We study all the potential parameters that can deteriorate the quality of VoIP such as jitter, End-To-End delay, packet delay variation, and the effect of adding security to VoIP networks that has been measured using OPNET (Network Simulation Tool).

Keywords: VOIP, SIP, IPsec, RTP

1. Introduction

NATs have become important elements in today's networks. NATs provide an added layer of security for LANs, making internal IP addresses inaccessible on the public Internet. Thus, attacks against the network must focus on the NAT router itself. Like firewalls, this increases security because you need protect only a single access point. Network Address Translation (NAT) is being used by many service providers and private individuals as a way to get around the problem of not having enough IP addresses. NAT solves this problem by mapping internal addresses to external or public addresses. An internal IP address:port pair is mapped to an external IP:port, and whenever the NAT receives a packet with the external IP:port, it knows how to reroute the packet back to the internal IP address and port.

However, nothing comes without an expense. For example, NATs and Firewalls cause significant connectivity problems between nodes separated by NATs/Firewalls and preventing them form communicating with each other [3]. These connectivity problems are more severe in complex protocols that negotiate secondary flows of data on the application

* Egyptian Armed Forces, ashraf_diaa2@hotmail.com
† National Defense Council, yehab@hotmail.com

layer. This type of communication is found in many protocols such as SIP, H.323, etc. used in peer-to-peer applications [5].

SIP is being deployed for Voice over IP (VoIP), video conferencing, instant messaging, as well as new converged data and voice applications. SIP has today become the signaling protocol of choice for establishing real-time communications, including Voice over IP (VoIP) calls. The problem of NAT traversal is particularly troublesome for interactive multimedia communications such as those established and managed by SIP . The motivation for this paper is due to a plethora of problems enumerated and the multitude of solutions developed to solve them.

2. Network Address Translators (NAT)

"Network Address Translation is a method by which IP addresses are mapped from one realm to another, in an attempt to provide transparent routing to hosts. Traditionally, NAT devices are used to connect an isolated address realm with private unregistered address to an external realm with globally unique registered addresses".[2] NAT was designed as short term solution for the IPv4 address exhaustion to allow multiple hosts in a "private" network to share public IP addresses while a more permanent solution is being developed. Because of its intended temporary nature it has been designed to cause minimal network changes and without making any changes to hosts or other routers. [4]

NATs usually found on the edge of network as a functional unit of a router or gateway. NATs divide the network into "inside" and "outside" and they operate in a very simple way. NATs intercept each IP packet, examine it and then decide what to do with it. NATs might discard the packet or forward it as it is or alter its IP address and checksums. They either alter the source or destination IP address based. the direction i.e. from inside to outside or the opposite direction. There are also another variant on NATs which is port translating NAT or NATP, they work in a similar way but the mapping is done for the IP address and the port as a pair which allows even more sufficient usage of the public IP addresses.

Thus a whole private network with unregistered IP addresses can access to Internet since the source IP addresses of the outbound packets are replaced by the NAT device with a registered address, such that the modified packets can be routed properly. Similarly, the destination IP address of inbound packets is replaced by the address of the ultimate destination.

3. Types of NAT

There are four types of NATs. As defined in [5] they are:

1. Full Cone
2. Restricted Cone
3. Port Restricted Cone
4. Symmetric

For a given internal address, the first three types of NAT maintain a mapping of this internal address that is independent of the destination address being sought. The fourth type of NAT will allocate a new mapping for each independent destination address.

Unless the NAT has a static mapping table, the mapping that opens when the fi rst packet is sent out from a client through the NAT may only be valid for a certain amount of time (typically a few minutes), unless packets continue to be sent and received on that IP:port.

- **Full Cone**
  In the case of the full cone, the mapping is well established and anyone from the public Internet that wants to reach a client behind a NAT, needs only to know the mapping scheme in order to send packets to it. For example, as shown in Fig. 1 a computer behind a NAT with IP 10.0.0.1 sending and receiving on port 8000, is mapped to the external IP:port on the NAT of 202.123.211.25:12345. Anyone on the Internet can send packets to that IP:port and those packets will be passed on to the client machine listening on 10.0.0.1:8000.

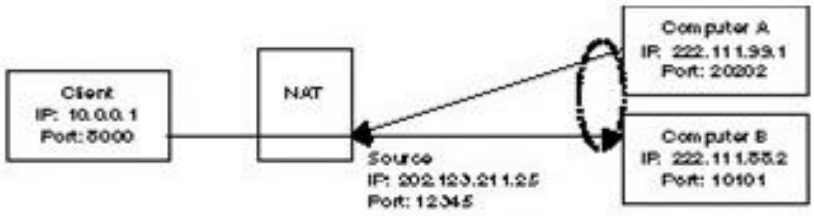

Fig. 1 Full Cone NAT

- **Restricted Cone**
  In the case of a restricted cone NAT, the external IP:port pair is only opened up once the internal computer sends out data to a specific destination IP. For example, in the case where the client sends out a packet to external computer 1, the NAT maps the client's 10.0.0.1:8000 to 202.123.211.25:12345, and External 1 can send back packets to that destination. However, the NAT will block packets coming from External 2, until the client sends out a packet to External 2's IP address. Once that is done, both External 1 and External 2 can send packets back to the client, and they will both have the same mapping through the NAT.

- **Port Restricted Cone**
  A port restricted cone type NAT is almost identical to a restricted cone, but in this case the NAT will block all packets unless the client had previously sent out a packet to the IP AND port that is sending to the NAT. So if the client sends to External 1 to port 10101, the NAT will only allow through packets to the client that come from 222.111.88.2:10101. Again, if the client has sent out packets to multiple IP:port pairs, they can all respond to the client, and all of them will respond to the same mapped IP:port on the NAT.

- **Symmetric**
  The last type of NAT – symmetric - is different from the first three in that a specific mapping of internal IP:port to the NAT's public IP:port is dependant on the destination IP address that the packet is sent to. So for example, as shown in Fig. 2 if the client sends from 10.0.0.1:8000 to Computer B, it may be mapped as 202.123.211.25:12345, whereas if the client sends from the same port (10.0.0.1:8000) to a different IP, it is mapped differently (202.123.211.25:45678).

4. Problem Description (Traversality)

Because of the services the NATs and Firewalls offer they become important elements of today networks which have changed the internet address architecture to be a collection of private address realms connected by NATs to the global address realm in which every device has a global unique address. But this was not without a price, Firewalls and NATs break the IP connectivity model by preventing hosts residing in "outside" networks from initiating a connection with host residing in the "inside" network[6].

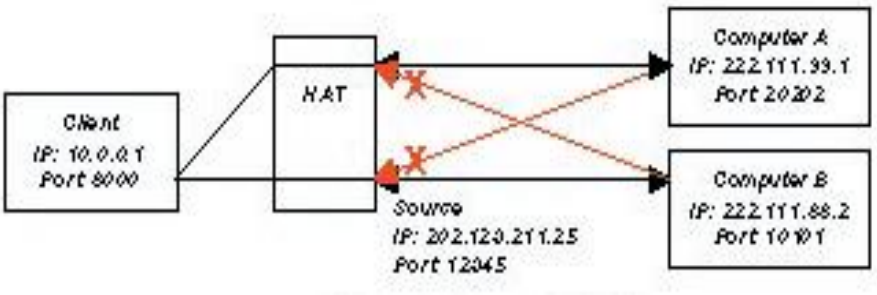

Fig. 2 Symmetric NAT

This behavior is more obvious in connection oriented protocols such as TCP, for example many Firewalls are configured to allow connection only if they are imitated by internal host. To do so Firewalls drop inbound SYN packets making it impossible for any external host to initiate a connection with internal one. If both hosts A and B are behind Firewalls then it will be impossible for them establish a connection although the connection itself do not violate the firewall policy.[6] Such configuration is reasonable to limit access to the internal network, however this cause a severe problem for peer to peer communication (P2P). The nature of P2P communications which based on incoming calls from unknown/untrusted hosts limits the possibility to solve the problem by pre-configuring the Firewall.[7]

Many multimedia and P2P protocols negotiate secondary flows in the application level. Session Initiation Protocol (SIP) for example, sends an IP address and port to the other party where the audio should be sent. As a result this audio stream will be dropped at Firewall. If the host is behind a NAT and is using a private IP address SIP will eventually send this IP address to the other party, but all packets that will be sent to this IP address will be dropped because it is unroutable.

Also there are difficulties to pass IPSec traffic through a NAT device. The main objective of IPSec is to protect an IP packet's integrity. This means that IPSec tries to prevent any modifications to the packet. Since NAT modifies the IP header, IPSec evaluates this as a violation of integrity and discards the packet. ESP in Transport mode protects the TCP/UDP header, but does not care about the source and destination IP addresses. Thus, modification of the IP address does not violate the integrity check. But if the packet is a TCP or UDP packet, NAT should modify the checksum that is protected by ESP, which in turn causes the integrity check to fail. This leaves us with only one working solution: ESP in Tunnel mode. But there may be other problems regarding IKE. If you are using IKE in Main Mode, and if IKE authentication employs pre-shared keys, then you are in trouble. Since Main Mode requires peer authentication, and preshared key IKE authentication includes the host IP addresses, a NAT device in the middle would cause IKE authentication to fail. NAT and IPSec is very hard to use together without a standard way which would provide simple management and interoperability between vendors.

5. Methods for Solving NAT/Firewall Traversal of SIP

Most organizations wishing to reap the benefits of IP rich media communications will ultimately face the firewall/NAT challenge. In practice, most organizations implement firewalls and NATs concurrently; consequently, traversing one does not necessarily negotiate both. A number of ways exist for traversing these devices as described below. Eventually, all firewalls will need to be SIP capable in order to support the wide-scale deployment of realtime communications. Several solutions have been proposed to work around the firewall/NAT traversal issues that limit SIP-based communication.

5.1 Avoiding the Firewall and NAT Device

One obvious way for organizations to overcome the Firewall/NAT problem is to avoid using them. For most organizations, the security risks of this solution are too great; furthermore, obtaining enough routable IP addresses for the entire organization may prove difficult and expensive. There are, however, a number of organizations, particularly among educational institutions, that have little firewall protection, and they do not use NAT. Some network administrators have attempted to solve the media traversal problem by routing media and SIP signaling traffic around a firewall or by opening up the firewall rules so broadly that all SIP and media traffic can pass through. In nearly all situations this is a poor solution for a variety of reasons.

In order to eliminate the need for firewalls in SIP networks, some people have suggested that duplicate network infrastructures be built exclusively for SIP. In practice this isn't a viable option. Carriers must have the ability to support billing and authentication systems and services on the same networks as the media sessions. Enterprises can't afford to build duplicate networks. SIP also relies on DNS for routing calls. One of the advantages of SIP is its promise to offer integrated voice and data applications as well.

5.2 Gateway to PSTN

Rather than have any concern with employing IP communications outside the LAN, organizations can use a gateway to convert from IP voice and video on the LAN to PSTN voice and video over the public circuit-switched network. Use of a gateway eliminates the concern for network firewall traversal because no data packets cross the firewall. It also overcomes the NAT issue because all calls made to endpoints on the LAN are routable, and calls coming into the LAN through the gateway are routable. Today most IP telephones use a gateway to communicate with non-IP telephones both within and without an organization. Gateway approaches are local solutions, however, that requires all locations participating in the call to have a corresponding gateway behind the last layer of NAT and firewall they have deployed. Using PSTN gateways also removes the converged network cost savings and mobile use benefits an all-IP solution provides.

5.3 Full Proxy

SIP or H.323 proxies can be used to negotiate the NAT or both the NAT and the firewall depending upon how they are configured. Proxies act like a gateway, but instead of converting from one IP communications protocol to another, the same protocol is used on both sides of the proxy. A proxy has knowledge of both the public and private IP networks and makes the IP call effectively look like two separate calls: one from the endpoint in the private network to the proxy and a second call from the proxy to the endpoint in the public network. Internally, the proxy puts these two calls together thus resolving the NAT issue.In some cases NAT is deployed at multiple locations along the network path: multiple points within the enterprise, and even within the external network at the ISP. For a proxy to work, it needs to be deployed at every NAT.

5.4 Tunnel Media Through the Firewall

Other possible solutions include using IPSec VPNs or proprietary protocols to transport SIP signaling and media through a tunnel. A tunnel solution requires that both parties participating in the call be known in advance so the tunnel service can be set up prior to any calls. Either an upstream service provider or the call recipient must install compatible SIP tunneling hardware and/or software. As SIP becomes more ubiquitous for voice communications, called parties may be located anywhere on the public Internet. If the called party is not programmed into the tunnel solution in advance, communication is not possible. Similarly if the called party moves, then tunnel equipment must be reconfigured.

Both parties participating in a call must have their network infrastructure configured to route traffic back to the other caller through the tunnel. This means they cannot both be using the same network address space such as private addresses. Another issue with tunneling SIP media is the tunnel equipment may add unacceptable latency to the media traffic. For example, IPSec relies heavily on encryption, a time intensive task, to provide security. Tunnel equipment that performs encryption in software may add unacceptable latency to the media streams resulting in poor voice or video quality.

5.5 SIP Application Layer Gateway

Application level gateways (ALG) are firewalls that are programmed to understand specific IP protocols, like H.323 and SIP. Rather than simply looking at packet header information to determine if packets can or cannot pass, ALGs go deeper by parsing the data in the packet payload. [8] H.323 and SIP both put critical control information in the payload, such as which data ports the voice or video endpoint is expecting to use to receive the voice and video data from the other endpoint in the call. By understanding which ports need opening, the firewall dynamically opens only those ports needed by the application, leaving all others securely closed. This technique of opening small numbers of ports in the firewall dynamically is called “pinholing”.

ALGs require a proxy if a NAT is being used to hide internal addresses. Some firewall manufacturers build the Proxy into the ALG, but it must be there to negotiate the NAT. ALGs can affect network performance, placing a heaver load on the firewall due to the parsing of the packet payloads. Moreover, if there are multiple levels of firewall/NAT combinations, each firewall/NAT in the call path must be upgraded to support ALG functionality.

5.6 Firewall Control Protocol (MIDCOM Devices)

Figure 3 shows that middle box communication (MIDCOM) is a scheme very similar to the ALG method; however, in the MIDCOM approach to firewall and NAT traversal, protocol intelligence is not built into the firewall. Instead, the SIP or H.323 protocol knowledge is built into a different device, called a “trusted system,” that tells the firewall which ports to open for a given voice or video call. [9] The advantage of this technique, in principle, is that firewalls do not have to be continually upgraded as protocols change or as they come in and out of fashion. Its disadvantages are similar to those of ALG. Additionally, the firewall would require an initial “forklift” upgrade to implement the MIDCOM strategy. This method is still under development in an Internet Engineering Task Force working group.

5.7 Session border Controllers

Many enterprise customers are reluctant to replace their existing firewalls with new SIP-capable firewalls because they have spent a great deal of effort setting up security policies. Also, they trust the equipment they have. Yet enterprises must overcome the limitations of their existing firewalls, whether they have firewalls with no SIP functionality or SIP ALG firewalls with limited SIP functionality.

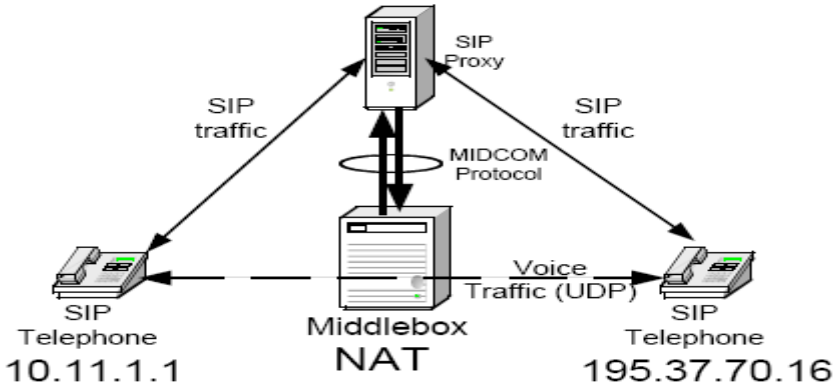

Fig. 3 Middlebox Communications Scenario

This need has triggered the development of a new type of product which some people call the "enterprise session border controller, such a device designed to work in networks where a corporate firewall is already in place. This device can be considered a firewall just for SIP traffic which can be installed either in a standalone configuration, or as part of the DMZ of the existing firewall . Essentially It assumes control of SIP traffic without involving the existing firewall in the process.

Most service providers use some sort of SBC in their core network to perform a number of tasks related to their SIP services. One of these tasks is to make sure that the SIP services can be delivered to their customers. They may use STUN, TURN, ICE for this by acting as a server component for these protocols. However, not all clients support these protocols so the SBC may also use a far-end NAT traversal (FENT) technology for NAT traversal. The goal of far-end NAT traversal is to allow inbound and outbound VoIP calls to succeed in the highest possible number of cases, even when one or both call parties on the call are behind one or more address-translation-enabled firewalls. No requirements on the subscriber-premise's hardware, software, or firewall should be permitted – the subscriber's experience should be to simply plug in a properly configured VoIP phone and start making calls.

The FENT function will aid remote SIP clients by transforming any SIP message by rewriting all relevant information and relay media, as well as keeping the client on the NATed network reachable. Typically, this far-end NAT traversal solution is implemented by continuously sending dummy packets through the firewall to keep pinholes open for the media to cross, or by asking the client to re-register in short intervals to keep those ports available.

5.8 STUN, TURN and ICE

These are all methods proposed by IETF in an attempt to solve the firewall/NAT traversal issue with intelligence in the clients together with an external server.

- **STUN**

As shown in Fig. 4 STUN (Simple Traversal of UDP through NATs) requires a STUN client on the phone or other end point device, which sends packets to a STUN server on the Internet. The STUN server replies with information about the IP address and ports from which the packets were received and detects the type of NAT device through which the packets were sent. The STUN client in the end point uses this information in constructing its headers so that external contacts can reach them without the need for any other device or technique. STUN requires that the NAT device allow all traffic that is directed to a particular port, and that the traffic is forwarded to the client on the inside. This means that STUN only works with less-secure NATs, so-called "full-cone" NATs, and that the internal client will be exposed to an attack from anyone who can capture the STUN traffic. STUN may be useful for some, but is generally not considered a viable solution for enterprises. In addition, STUN cannot be used with symmetric NATs. This may be a drawback in many situations as most enterprise-class firewalls are symmetric.

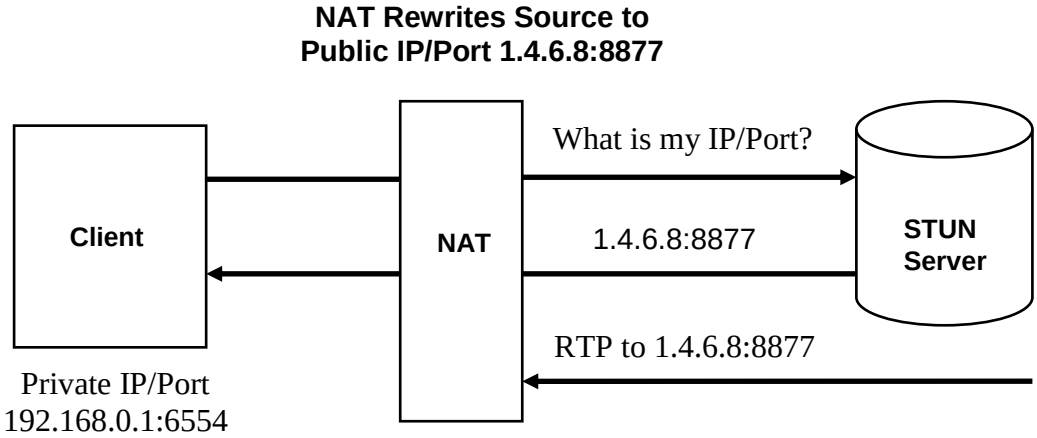

Fig. 4 The STUN protocol

- **TURN**

A significant supplement to STUN that utilizes an externally-hosted Media Proxy to deal with symmetric NATs is Traversal Using Relay NAT (TURN). The goal of TURN is to enable calls to pass through symmetric NATs. As in Fig. 5 endpoints could be equipped with the intelligence to negotiate with the TURN server to allocate and send media to a globally-routable media relay. Instead of sending media based on SDP information, it relays media for each call symmetrically, using the same source port on which it listens for incoming media.

A major criticism of this approach is the amount of bandwidth wastage and latency induced by routing all media to a central rendezvous location, and subsequently, to the other party. Calls between two neighboring endpoints often find their media routed out the firewall and back unnecessarily.

- **ICE**

Interactive Connectivity Establishment (ICE) is a method that tries to build intelligence into endpoints so that they can perform route discovery, path optimization, and even verify media flow before a call is deemed to be established. Prior to sending an INVITE, the caller performs a sequence of steps to characterize the firewall that it is behind:

- Obtains addresses of all usable interfaces (local, VPN)
- Checks the results from STUN If needed, negotiates a port with the TURN server
- Afterwards, the caller sends a list of available IP addresses/ports in the INVITE to the proxy.

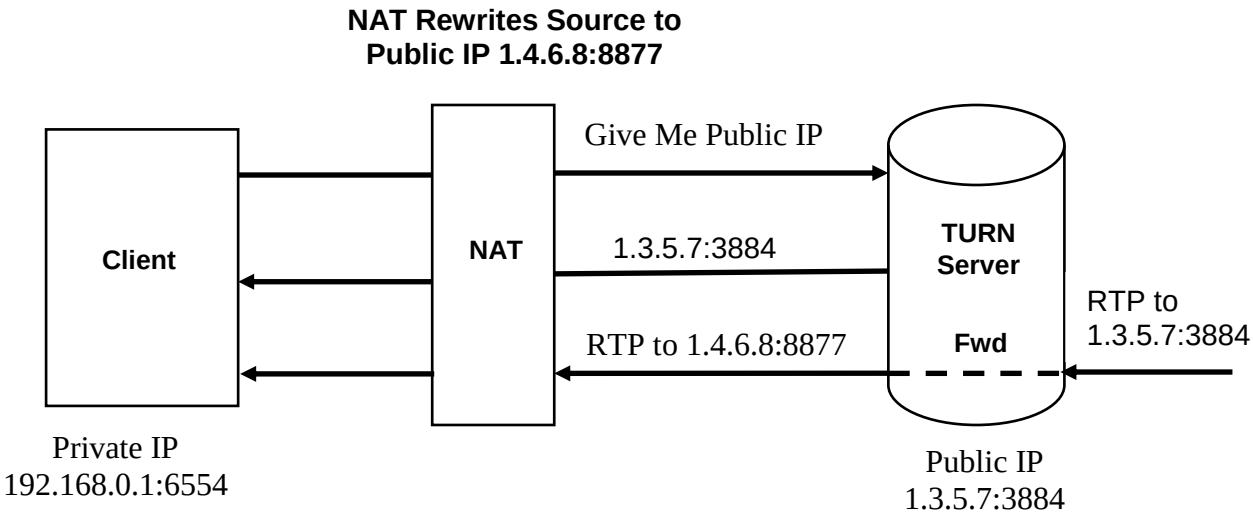

Fig. 5 The TURN protocol

As soon as the callee gets the INVITE, it follows a similar set of steps as did the caller. Next, it attempts to send STUN queries to the caller to see if it is possible to directly send media to any of the IP addresses it presented in the INVITE. Finally, the callee picks the address of highest preference in the INVITE to which the callee can confidently send media.

This approach is compatible with most known firewalls that support UDP. In addition to working with all types of NATs that support reflexive UDP admission. However, for ICE to work properly, both caller and callee must support ICE, and there should readily be a STUN and TURN server available. For this reason, it should be deployed only in a homogeneous, controlled environment. Furthermore, it is likely that the call setup will be delayed because of the steps involved in media path discovery by both the caller and callee.

6. Solving IPSec NAT Traversal of SIP

NAT Traversal is the most promising solution to overcome the problem faced when an IPSec traffic is intended to pass through a NAT device. NAT Traversal is a draft proposed to IETF by two different groups. One is prepared by SSH Communications, and the other is a result of a joint workshop of vendors. Two proposals are merged to form a single standard, since they had many common points. Major VPN vendors started using NAT Traversal in their products.

NAT Traversal is designed as a simple solution, which does not require any changes in the middle devices and existing protocols. Only requirement is the support for NAT Traversal at the edge devices. It also provides an automated way to accomplish NAT Traversal procedures, which minimizes the user intervention. The first step of NAT Traversal operation is determining whether the communicating parties support NAT Traversal or not. This is done

in the first phase of IKE negotiation, by sending a special vendor ID string to the other side. Successful exchange of vendor strings indicates that both sides support NAT Traversal. Upon verifying both parties support NAT Traversal, the second step is to discover if there is a NAT device in between. NAT discovery is also used to discover which peer is behind NAT, so that only that side sends the keep-alive messages. NAT discovery is a procedure to determine if the IP addresses or the ports change along the path. To accomplish this both sides calculates and sends the hashes of IP addresses and ports of both the source and destination to each other. Peers compare these values and judges that there is a NAT device on the path if they cannot find a match.
When a NAT device is discovered on the path, NAT-T negotiation and decision to use NAT-T takes place in quick mode. NAT-T negotiation decides what encapsulation mode is going to be used for NAT-T. These are UDP-Encapsulated-Tunnel and UDP-Encapsulated-Transport to replace normal tunnel and transport modes. Peers also send their original IP addresses if needed. In transport mode, peers should send their original IP addresses and ports whereas in tunnel mode peers should not, since they are included in the ESP payload.

If there is a NAT device on the path, something must be done to pass IPSec traffic through this device. This is the heart of the solution: the IPSec traffic between the hosts is encapsulated in UDP using the IKE port. Thus the encapsulated packets follow the same route as IKE packets. This avoids further modifications in the firewalls and assures that the NAT device modifies the NAT-T (NAT Traversal) packets, the same way it modifies the IKE packets.

7. Simulation Approach

Our simulation approach uses the popular OPNET Modeler simulation package. OPNET Modeler contains a vast amount of models of commercially available network elements, and has various real-life network configuration capabilities. This makes the simulation of real-life network environment close to reality. Other features of OPNET include GUI interface, comprehensive library of network protocols and models, source code for all models, graphical results and statistics, etc. This section describes in detail the simulation model, traffic model, various simulation configurations, as well as the simulation results.

7.1 Secure VoIP Network Simulation Model

Currently, there is no single VoIP signalling protocol, which has been exclusively adopted by the networking community. However, it is widely accepted that the SIP has a number of distinct advantages over H.323 and MEGACO, most notably its simplicity. Additionally, the IPSec framework of security protocols and architectures offer a myriad of flexible options when it comes to secure a VoIP network. For this reason, SIP and IPSec were chosen as the signaling and security protocols/architecture of choice on which the simulation model for the secure VoIP network was based. The simulation model was developed using the OPNET Modeler network simulation tool.

7.2 Network Topology

As Figure 6 shows, The shown network topology consists of three different administrative SIP domains, ‘site1’ to ‘site3’, every pair of which is interconnected by an IP router. The SIP proxy server with a co-located location server acts as the functional core within each SIP domain. The location server at each proxy server is configured with the location details, i.e. IP addresses of all the SIP nodes within the local domain and also the IP addresses of all the other SIP proxy servers in the entire network neighbourhood. The main components that build up the network model are the SIP nodes, SIP proxy servers, VoIP–PSTN gateways, IP routers

and IP cloud models. The VoIP protocol stack within the SIP related nodes is implemented over a UDP/IP infrastructure

7.3 Network Components Overview

The main components that build up the network model are the SIP nodes, SIP proxy servers, VoIP–PSTN gateways, IP routers and IP cloud models. The VoIP protocol stack within the SIP related nodes is implemented over a UDP/IP infrastructure. Figs. 7 and 8 represent the protocol stack implemented at SIP nodes and SIP proxy servers, respectively. Proprietary OPNET process models were developed for all the layers in the stack except for the physical layer, for which standard OPNET process models were used.

7.3.1. Call application layer model

The call application is the initiator of the voice call and also the call terminator at the destination host. The call application layer interacts with the SIP layer for call setup and disconnection and also directs the media application layer for generation and transmission of voice media.

The configurable simulation parameters at the call application layer are the total number of calls to simulate and their occurrence distribution. The specified number of calls is spread over the entire simulation duration, typically with an exponentially varying intercall occurrence interval.

7.3.2. Media application layer model

The media application layer is responsible for source and sink of the voice call media stream. At the source end, once the SIP connection is setup, the media application generates G.711 media packets at a regular interval of 20 ms during talkspurts and no packets are generated during silence periods.

7.3.3. SIP layer process models

The SIP layer models include the SIP user agent (UA) at the SIP nodes and the proxy server process model at the SIP Proxy server. The implementations are based on a subset of recommendations from Ref. [5], required to setup and tear down call connections .The configurable parameters of the SIP UA process are the SIP user ID, the name of the SIP domain it belongs to and the IP address of the local SIP proxy server. The SIP proxy server process model requires the domain name and the location server details to be configured.

7.3.4. RTP process models

The RTP process model provides services, such as timing reconstruction, loss detection and content identification of media stream. RTP utilises the sequence number and timestamp fields in the RTP header to provide these services.

The main functionality of RTP at the receiving end is to reconstruct a continuous stream of audio from the received audio packets, which may have undergone varying end-to-end network delays and packet loss.

7.3.5. IPSec layer

The IPSec layer, implemented between the IP and physical network layers in all network components, is responsible for providing confidentiality and authentication security services. It allows for various configurations of security services, such as providing confidentiality alone, or authentication alone, or both, by using ESP in transport or tunnel mode. The security policy at each end host can be configured such that security services are applied to only SIP signaling stream, to media stream, to both, or to none.

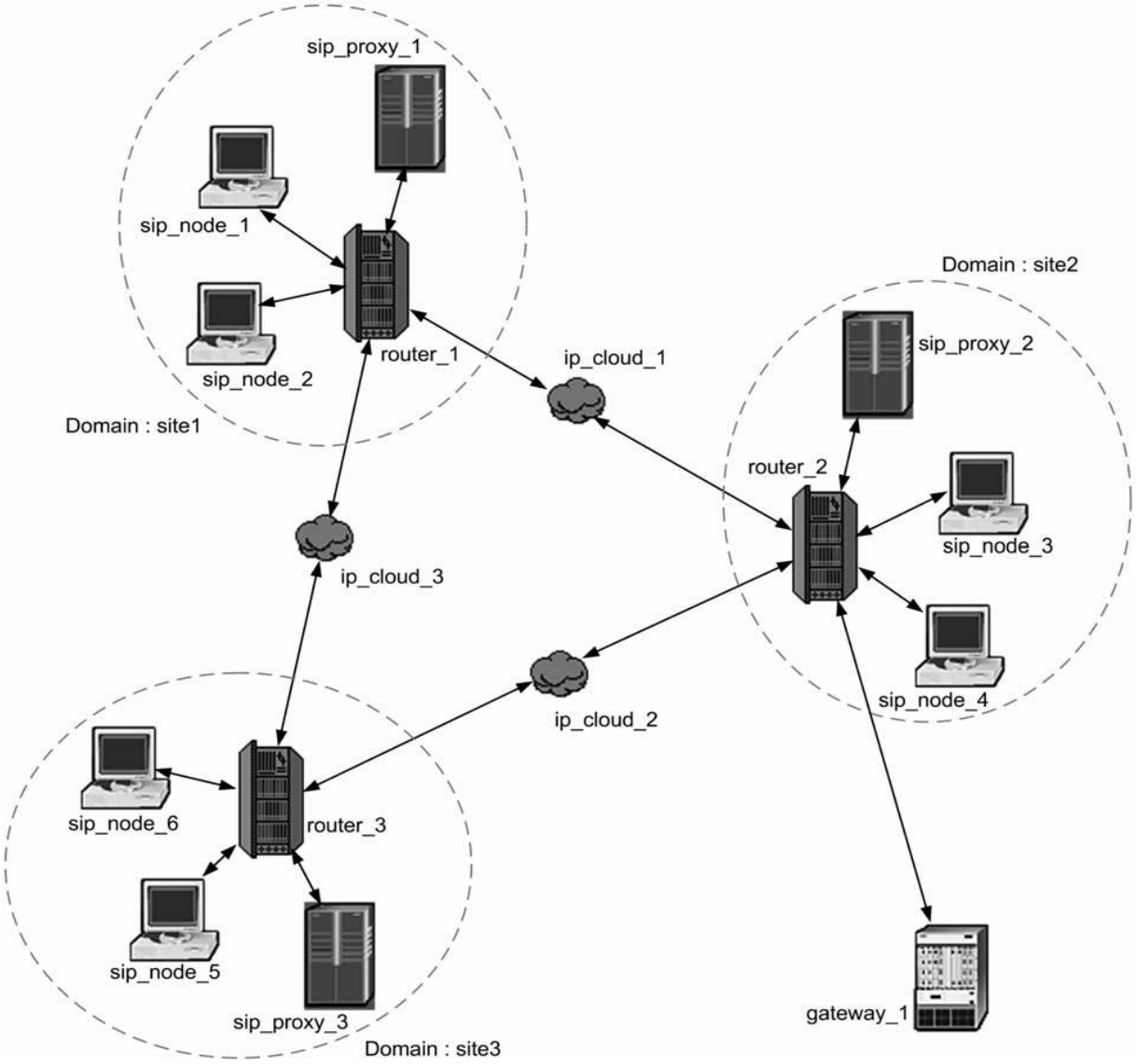

Fig. 6 SIP–VoIP network model topology.

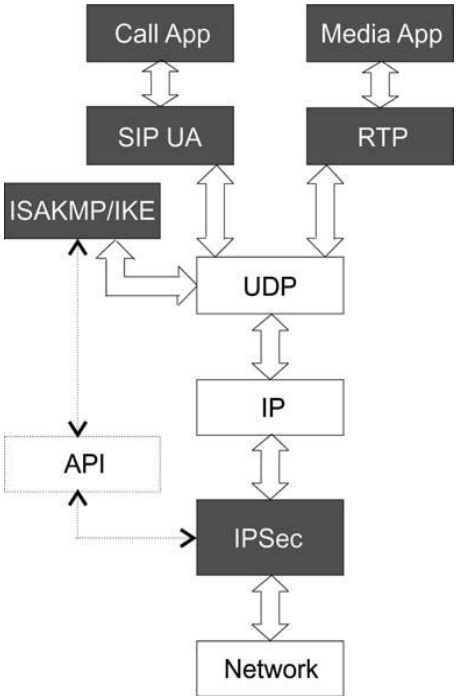

Fig. 7 SIP node protocol stack.

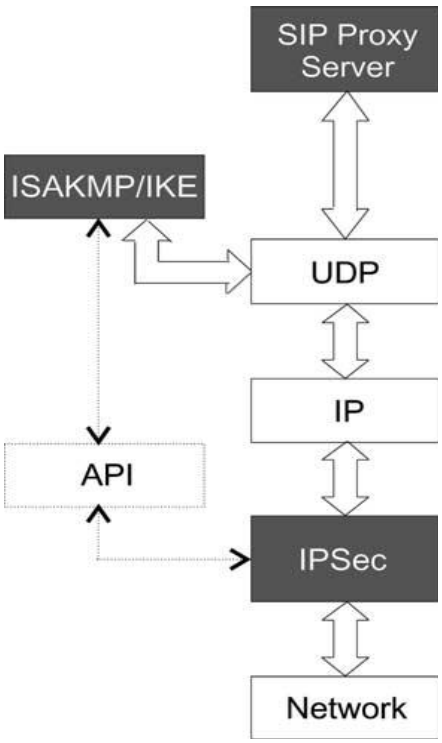

Fig. 8 SIP proxy server protocol stack.

7.4 Simulation Results

This section reports the results obtained to examine the impact of passing IPsec traffic through a NAT device on the quality of transmitting voice over communication links for different simulation times using OPNET simulator. The measuring criteria's used for evaluation are end to end delay, packet delay variation (jitter) , Mean Opinion Score **(**MOS).

7.4.1 End-to-End delay

Delay is the time interval in which a packets travels from one node to another node. It is caused by the time for endpoint to create packets, the time needed to fill data into packets, and the time to arrange digital data on a physical link. VoIP is very sensitive to delay; thus, it must be controlled and managed. As known, it is inefficient to wait for all packets arriving in an organized order; therefore, some packets may be dropped if they don't arrive in time and this can cause short periods of silence in the audio stream and causing bad VoIP quality. Ideally, the delay constraint for VoIP packets is not above 80ms . Fig. 9 show the end to end delay for plain IP and IPsec

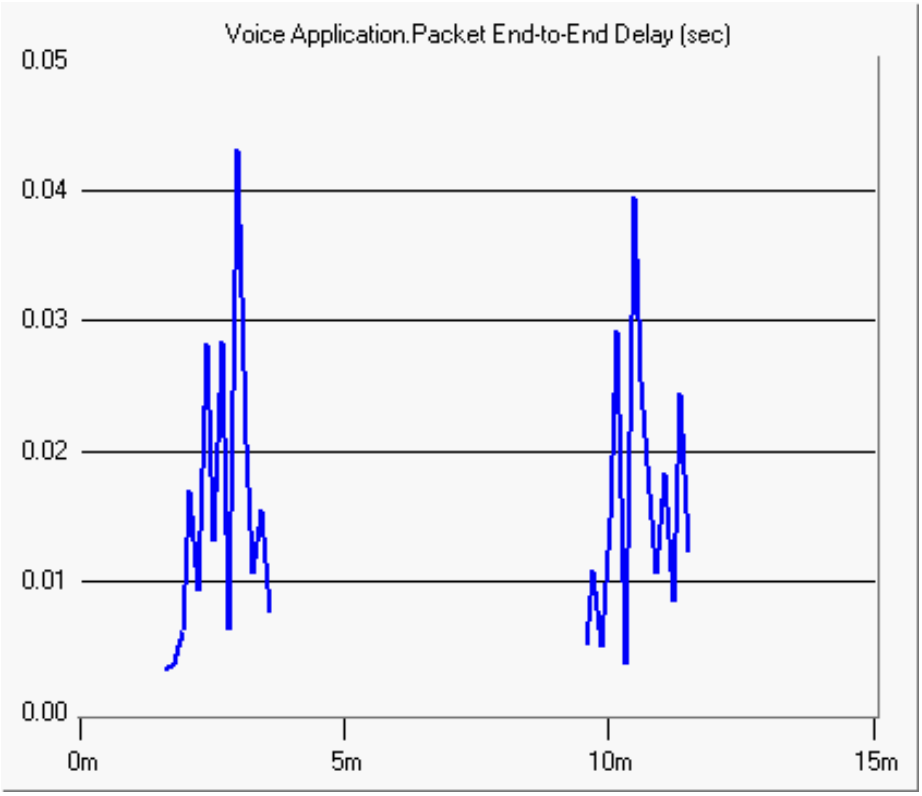

Fig. 9 SIP–VoIP End to End delay for plain IP and IPsec.

7.4.2 Packet delay variation (Jitter)

Jitter is the variation of delay of each packet. It is a very typical problem in packet switched network due to the fact that information is segmented into packets that travel to the receiver via different paths. Jitter is measured by the variance of time latency in a network. It is caused by poor quality of connections or traffic congestion . Sometimes it occurs when packets take different equal cost-links. It also occurs due to the dynamic change of network traffic loads. Jitter can be tolerated in data networks because arriving packets can be buffered. However, for real-time applications, such as voice, jitter has an imposed upper limit. When a packet arrives beyond the upper limit, the packet is discarded. This packet loss leads to quality impairment in VoIP . In order to reassemble voice signal successfully, the receiving device must account for jitter. Fig. 10 show the jitter delay for plain IP and IPsec

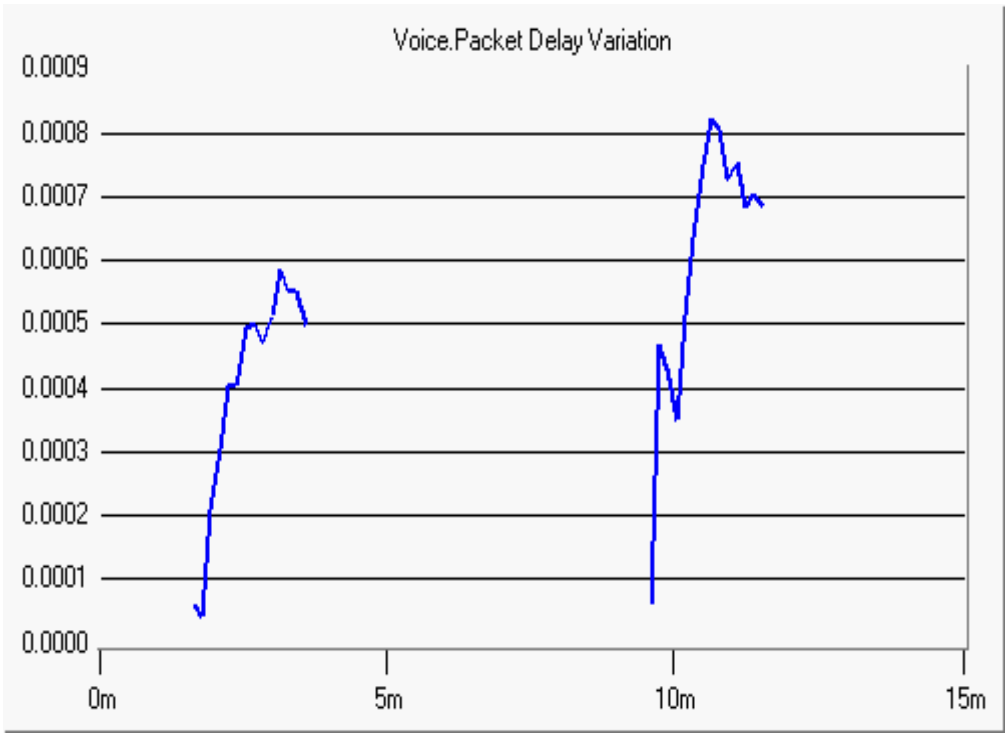

Fig. 10 SIP–VoIP jitter delay for plain IP and IPsec

7.4.3 Mean Opinion Score (MOS)

A MOS test is commonly used test methodology in subjective speech quality evaluation of speech codecs. Guidelines on how to perform a MOS test are given in []. To put it shortly, in a MOS test a group of subjects listens to a set of test samples, one sample at a time, and after each sample each subject indicates the quality of the sample by giving a score in range form one ('poor') to five ('excellent'). The MOS score is calculated as an average of scores given by all listeners.

The listening was performed in laboratory facilities and high-quality headphones were used in order to rule out all other factors contributing to the perceived speech quality but the transmission errors itself. The subjects participating to the experiment were selected to be non-expert listeners to better indicate the opinion of "normal" telephone users.

Prior to actual listening test each subject was provided a practice session of eight example test samples to introduce test procedure and the quality range he/she was to be confronted in the actual test. The scores given for the practice samples were not recorded as scores contributing to the result of the experiment.

Table 1 Different cryptographic algorithms and their MOS

Encryption Algorithm	MOS
NONE	4.1
DES	3.15
3DES	3.01
TEA	3.5
IDEA	3.25

8. Conclusion

In this paper a series of experiments are conducted on SIP based VoIP applications model, Performance analysis for multimedia over IP to work and function properly with NATs has been evaluated through a series of experiments on OPNET simulator .From experiment results, we observe that: the total End-To-End delay in which packets travels from one node to another node, and also the variation of delay of each packet (Packet Delay Variation) is increased by employing IPsec encryption and authentication services for VOIP signaling and media streams.

This paper also discussed NAT Traversal method (NAT-T) for IPsec. IPsec NAT-T presents an UDP based encapsulation method where the IPsec ESP is used for securing the payload. IPsec ESP encrypts only the payload of the data packet, and therefore even the NAT router changes the IP address of the packet, it does not effect to integrity check procedure that IPsec performs on receiver side to IPsec ESP HMAC value. IPsec AH remains incompatible with NAT because of this reason, since the whole data packet (incuding the IP headers/addresses) are to be encrypted - when using NAT and IPsec AH, the integrity check will fail on the receiver side and the IPsec packet is dropped.

As a future work, one can consider implementing important VoIP options such as VoIP conferencing and messaging. Also as a future work, one can look into assessing the network support and readiness of deploying other popular real-time network services such multimedia, video, and web conferencing.

9. References

[1] A. Elbayoumy, S. Shepherd, “A High grade secure VoIP system using The Tiny Encryption Algorithm”, University of Bradford, UK, 2004.

[2] Aurel Constantinescu M., Croitoru, V., and Oana Cernaianu, D. NAT/Firewall traversal for SIP: issues and solutions Signals, Circuits and Systems, 2005. ISSCS 2005. International Symposium on , Volume 2, 14-15 July 2005 Page(s):521 - 524 Vol. 2.

[3] Sechang Son, Allcock, B., and Livny, M. CODO: firewall traversal by cooperative on-demand opening High Performance Distributed Computing, 2005. HPDC-14. Proceedings. 14th IEEE International Symposium on, 24-27 July 2005 Page(s):233 – 242.

[4] cicso systems http://www.cisco.com/web/about/ac123/ac147/archived3/anatomy.html.

[5] Martin, M., Brunner, M., Stiemerling, M., and Fessi, A. Path-coupled signaling for NAT/firewall traversal. High Performance Switching and Routing, 2005. HPSR. 2005 Workshop on, 12-14 May 2005 Page(s):231 – 235.

[6] Saikat Guha and Paul Francis Characterization and Measurement of TCP Traversal through NATs and Firewalls Source: 2005, Usenix.

[7] Saikat Guha and Paul Francis Characterization and Measurement of TCP Traversal through NATs and Firewalls Source: 2005, Usenix.

[8] J. Rosenberg and H. Schulzrinne, “SIP Traversal through Residential and Enterprise NATs and Firewalls”. Internet Draft, Internet Engineering Task Force, Mar. 2001.

[9] Anonymous, “Traversing Firewalls and NATs With Voice and Video Over IP: An Examination of the Firewall/NAT Problem, Traversal Methods, and their Pros and Cons” . Wainhouse Research, Apr. 2002.