Chapter 4

IPv6 Security Issues and Evaluation

4.1 Introduction

As networks are mushrooming, the growth and development of IPv6 is gaining more importance. The wide scale deployment of this protocol into operational networks raises certain issues with security being one of the most compelling ones. The next generation internet protocol (IPng) introduces vulnerabilities in addition to those inherent in IPv4. While the existing security infrastructure like IPSec, SSL, PKI, and DNSSec might be sufficient for IPv4, the protocol security associated with IPv6 and migration networks needs to be assessed and analyzed. Until the time complete migration to IPv6 takes place, the internet migration techniques need to be secured. If left unprotected, these techniques pose a serious threat to networks.

Initially during the design phase of end-to-end model, internet was seen as knowledge sharing "friendly" environment with no inherent security architecture. But the present day internet has become a hostile environment with network vulnerabilities. The introduction of IPv6 into current operational networks is seen as one of the biggest security challenges. With IPv4, the internet's end to end model has worked well for the past three decades (Bradner, 2006), but due to address space depletion, complex set of configurations and limited security for exponential growth of internet, the migration to next generation of internet protocol i.e. IPv6 seems inevitable. As a result of large scale deployment of IPv6, security (Treese, 2004) has become an intrinsic issue in modern day internet-based computing. Although introduction of IPv6 will give birth to new protocol attacks, the existing and known IPv4 threats will certainly prevail in a polymorphic manner in IPv6 (Caicedo, Joshi & Tuladhar,2009).Security framework in IPv6 is similar to one in IPv4 (Convery & Miller,2004) with IPSec being mandatory, which was earlier considered optional in the legacy protocol. IPv6 might be inherently more secure than IPv4 in an ideal and well-coded application environment, but in reality the IPSec deployment with IPv6 will face same challenges and issues as prevalent in IPv4-IPSec deployment. Since most of the security breaches occur at the application level, the successful deployment of IPSec does not guarantee any network security. IPv6 is therefore usually deployed without any cryptographic protection making it vulnerable to network attacks. The migration from IPv4 to IPv6 has its own security implications which can influence the confidence of stakeholders who are ready for transition. During migration phase legacy IPv4 protocol has to coexist with IPv6 for substantial amount of time leaving room for older network vulnerabilities. This chapter presents an analysis of network attacks that are common in IPv4 and makes a comparative analysis of how these attacks may impact the IPv6 network. We also establish guidelines and principles for mitigating these attacks. This chapter also addresses the security issues that arise while migrating to IPv6. Later in this chapter, we carry an in-depth survey of Internet Security Protocol (IPSec) which provides a framework with sublime options for encryption and authentication of data packets. Although IPSec is the panacea for securing IP protocol, its implementation and management is unequivocally complex in nature. The implementation involves key management and exchange through IKE, protocol negotiations and establishment of security associations which can significantly decrease performance and degrade IP communication. This fact has a significant impact on real time communication. We carry out an empirical investigation of the parameters that are affected by implementation of IPSec in IPv6 and 6to4 Tunneled Migration Networks. The investigation is significant and evaluates about the performance decay that is encountered by incorporating security. The simulation approach is used and measurements are performed in OPNET Simulator ver. 14.5.

4.2 Security Vulnerabilities in IPv4/IPv6

Depletion of address space and security vulnerabilities was the main motivation behind the deployment of IPv6. Several unanticipated vulnerabilities are likely to further emerge with large scale deployment of the new internet protocol. The following section throws light on some of the possible vulnerabilities and attacks, and additionally provides relevant security guidelines.

4.2.1 Reconnaissance Attacks

In this type of attack, the intruder gains as much information about the target network by network scanning as he does through passive data mining techniques. The network scanning provides intruder specific information regarding hosts and internetworking devices and their interconnections and also some loopholes which can be exploited (Seo & Kent, 2005). In IPv4, methods like ping sweeps, port and application scans are mostly used for collecting this information. Ping sweeps (which help in determining IP addresses that are being used in the organization) flood a network with ICMP or layer 4 ping messages that solicit a reply. Based on the data obtained, an intruder formulates hypothesis regarding layout of the target network. After learning about the network and its reachable systems, Port scans help hackers to listen to specific services (Ford, 2005) on ports that could be potentially vulnerable.

In IPv4, port scanning is a simple task as most of the IPv4 segments are class C addresses with 8 bits allocated for host. Scanning an IPv4 subnet at the rate of one host per second amounts to 2^8 hosts × (1 sec/1 host) × (1 min/60 sec) = 4.267 minutes. In IPv6, this scenario is totally different as it uses 64 bits for subnet addressing and 64 bits for host addressing. Therefore an IPv6 subnet requires 2^{64} hosts $^{\times}$ (1 sec/1 host) × (1 year/ 31,536,000 sec) = 584,942,417,355 years

Scanning such a large address space is almost impossible (Convery & Miller, 2004; Popoviciu, 2006) making Reconnaissance attack very difficult in IPv6. However there are other ways around. The multicast address structure in IPv6 allow an intruder to find major key systems like routers, servers etc allowing it to scan vulnerabilities in these systems. Software tools like NMAP (Network Mapper) and Alive6 program (shipped with THC-IPv6 attacking toolkit) also help in launching Reconnaissance attacks in IPv6.

The large address space in IPv6 makes Reconnaissance attacks difficult, but not impossible. There are several recommendations to help thwart such attacks. The major network identifier devices should not be sequential and should not start at the lower end of the IPv6 subnet. From a security point of view, it is not a good idea to list the router as the first host on the network.

The usage of Random node ID's is recommended making scanning of the subnet more difficult. Any random mechanism of assigning the host address is good as long as there is a balance between security and maintainability. Many newer operating systems support the use of private addressing for end hosts. The use of private addressing with random node ID's can help keep the hosts randomly allocated and evenly distributed across the subnet.

4.2.2 Host Initialization Attacks

The host initialization process in IPv4 is carried out with protocols like ARP and DHCP. These protocols are vulnerable to spoofed communications by making end hosts to communicate with rogue or compromised devices or getting these devices configured with manipulated network information like DNS server address, default gateway address or address mask etc (Treese, 2004). In IPv4, a DHCP client usually boots up by broadcasting a message. Before the valid DHCP server responds to the client, a rogue DHCP server responds. In this way, a rogue server is able to set initial critical settings including the default gateway DNS server thereby enabling Man-in-the-Middle attacks. Thus DHCP messages can be spoofed allowing an attacker to utilize all the valid messages on the server.

The host initialization attacks do not change much when ported to IPv6 (Shah & Parvez, 2015). IPv6 provides provision for Stateful and stateless auto configuration of IP addresses thereby relieving the network administrator from the cumbersome task of manually assigning IP addresses and maintenance of DHCP servers in large enterprises. Stateless auto configuration works by combining two pieces of information: the network prefix, which can be obtained from the routers located in the network segment to which the host is attached and the hardware address, which can be obtained from the host’s NIC card. Stateful auto-configuration uses the services of DHCPv6 server for generating the required address. The IPv6 neighbor discovery protocol is the key player in stateless auto configuration. After address generation, a node uses the services of NDP to discover other nodes using the same link. The protocol also lets the node discover routers and gateway devices to maintain reachability information on the detected active neighbors. NDP messages form part of ICMPv6 which is used for error reporting and diagnostic purposes. To configure an interface network address, a node first sends a router solicitation message (RS) to all routers multicast address to find the router and obtain network prefix value. Once the address has been configured, a node can use duplicate address detection (DAD) to check if that address is unique. In DAD procedure, a node sends a neighbor solicitation (NS) packet encapsulated with its tentative IP address with the purpose of obtaining a response packet from any node that might already be using the newly generated address. If the reply to the NS message is negative, the node that generated the address assumes it to be unique and uses it.ICMPv6 messages open the door for many attacks like Denial-of-Service (DOS) and Man-in-the-Middle (MITM) attacks when they are not secured through IPSec. The DAD procedure can be used as a platform to launch DOS attack. For executing this, an attacker usually sniffs the local link for a NS packet. The attacker falsely responds with neighbor advertisement packet informing the new node that it is already using that address. Upon reception of NA, the new node again generates another address and repeats the DAD procedure, the attacker again falsely responds with NA packet. Eventually the new node gives up without initializing its interfaces. An MITM attack gets executed when a malicious node impersonates a network segment’s default gateway. The malicious node takes advantage of the fact that receiving node does not validate router advertisements (RA).Thus any node that receives a false RA updates its communication channel parameters blindly based on RA. A malicious node can propagate bogus address prefix information to re-route legitimate traffic to prevent the victim from accessing the network

To detect DHCPv6 auto configuration or neighbor discovery abuses in IPv6, no security tools are available till date. These messages are normally filtered out at a router or a firewall like ICMP message. Since most of these attacks have limited domain, they therefore have a minimal impact on the network. The Secure Neighbor Discovery Protocol (SEND) is used as an alternative to IPSec for securing the Neighbor Discovery Protocol. SEND uses cryptographically generated addresses (CGA's) to verify the sender's ownership of claimed address. CGA's are IPv6 addresses in which part of the address is generated by applying a cryptographic one way hash function based on a node's public key and auxiliary parameters. The hash value can then be used to verify the binding between public key and node's address. In some environments, network administrators use a static entry for default route of a system which can be a cumbersome process.

4.2.3 Broadcast Amplification Attack (Smurf Attack)

The Broadcast Amplification Attack gets executed when an attacker spoofs the source address of victim and sends an echo request message to the subnet broadcast destination address. All the end hosts respond back to the spoofed source address and thus flood the victim with echo reply messages. The spoofed messages can be used to attack a single host at once or at least to use all hosts on a network to attack a single host. The first one can be used to run DOS attack against the whole network while the latter one is a kind of Distributed DOS in which many hosts try to interrupt a single host. These types of attacks are called amplification attacks because they multiply the quantity of packets i.e. payload on the network. If an attacker sends packets with a spoofed source address to a multicast group and all nodes in that group respond to that message, the spoofed source address, i.e. the address of the victim will be overwhelmed with traffic. A simple tool such as Smurf6 from the THC-IPv6 attacking toolkit can send echo requests to the "all nodes" multicast address ff02::1. Sometimes, the victim may reside on a remote subnet. In that case all local nodes will be sending echo replies via their default router to the remote host i.e. the attack would not only affect the remote victim but also the local network.

A number of popular operating systems don’t respond to echo request from a spoofed source address directed at the link local multicast address. Some uncertainty still exists in the protocol about whether end nodes should respond to ICMP messages with global multicast address as the source address. The ingress filtering of packets with IPv6 multicast source address is recommended and those packets with a multicast source address at the border of the network should be dropped.

4.2.4 Header Manipulation and Extension Headers

The transport layer information of the packet (TCP or UDP) is indicated by extension headers in IPv6 (RFC 2460).Within the IPv6 header, extension headers are indicated by the next header field and are used to extend the functionality of the protocol. If abused maliciously, extension headers pose a serious threat to a network. A packet can be crafted with unlimited number of extension headers linked together in a big list leading to DOS of intermediary systems along the transmission path or destination systems. Chain-linked list of extension headers is also a way of evading firewalls and network intrusion detection systems. These list-based extension headers could break the payload into a second fragmented packet that cannot be checked by the firewall that is only looking for the initial fragment. Extension headers can be manipulated in this way, thus denying services to the destination host or crashing the hosts stack.

These attacks are normally evaded by simple filtering on extension headers or having firewalls that have highly sensitive rules for header scanning. The extension headers that require special handling and attention include Destination options, Mobility and Routing headers. To control different extension headers, a number of different options are available in the Internet Operating Systems (IOS) IPv6 Access Control List (ACL). It is recommended to carry out parsing of complete extension header chain in all routers or middle boxes that receive a packet with extension header which is simpler than adding another level of security. Parsing the entire extension header chain quickly requires hardware optimization which may be difficult (or nearly impossible) because total header structure is non-deterministic.

4.2.5 Routing Attacks

These attacks focus on re-routing and redirecting traffic flow, causing disruption in a network. The major approaches usually include flooding of packets, quick announcement and removal of routes and bogus router implantations. Routing attacks can be used to redirect traffic through intermediate hosts before it reaches the actual destination. This could make the destination host believe that traffic was sourced from intermediate node and it could be used to evade firewalls that don't check for the presence of routing extension headers. Routing Headers provide a base for launching MITM attacks or to rebound/relay packets from a potential victim. Currently there are two types of routing headers; RH0 and RH1. Due to replacement of destination address at every layer-3 hop that processes the routing header, RH0 is always vulnerable. This behavior makes it difficult for firewalls to determine the actual destination of the packet and compare it with firewall policy.

Several protocols don't change their security mechanism while transitioning from IPv4 to IPv6.The Multiprotocol-BGP was extended to carry IPv6 inter domain routing information. Therefore BGP continues to rely on TCP MD5 for authentication. The Intermediate System-to-Intermediate System (IS-IS) protocol (Callon, 1990) was extended in a draft specification (Hopps, 2008) to support IPv6.The Open Shortest Path First Version 3 (OSPFv3) (coltun, 1999) and Routing Information Protocol Next Generation (RIPng) (Malkin, 1997) have also undergone major change by removing the authentication fields from protocol specification. The Security Mechanisms to secure protocols that have changed with IPv6, OSPFv3, and RIPng are implemented inconsistently across internetworking devices. The usage of IPSec and IPv6 hop limits is recommended to secure the routing protocols and network devices.

4.2.6 Firewall Evasion by Fragmentation

Fragmentation attacks aim at evading network firewall and intrusion detection systems. The IPv4 protocol firewalls and IDS provide for deep packet inspection to reassemble packets and compare them to access control rules or attack signatures. Large amount of fragmented traffic has always been an early indicator of intrusion attempt because most baselines of internet traffic indicate that %age of fragmented traffic is low (Shannon & Moore, 2001).Both the fragments from either IPv4 or IPv6 can be used by hackers to hide or launch attacks on a node. By dividing the packet into small fragments, the attacker can make fragments look legitimate and can try to bypass filtering or detection. To determine the true motive of a hacker would require reassembling all packets. An Attacker can exploit end hosts weaknesses in the method of reassembling the fragmented packets. A common example of this would be overlapping fragments having an overlap in the offset and out of order fragments. In this case, the fragment id's do not match correctly with the data. Fragmentation attacks also involve an attacker sending an incomplete set of fragments making the receiving host wait for the last fragment in the set. Although the default fragments time out is 60 seconds which can consume resources on intermediate systems. Sometimes the attacker uses nested fragments i.e. fragments within fragments to launch attacks where IPv6 protocol has multiple fragmentation headers. Commonly used software to manipulate fragmentation headers includes tools such as Whisker, Fragrouter, Teardrop and Bonk.

Similar to IPv4, current IPv6 firewalls and IDS's implement fragment reassembly and other fragmentation checks to mitigate fragmentation attacks. The fragmentation checking process includes inspecting out of cycle fragments and switching these packets into sequence as well as inspecting the number of fragments from a single IP given a unique identifier to determine Denial of Service (DoS) attacks. Till date, IPv6 has no known fragmentation attack tool, but that does not eliminate the threat that such tools exist or can be easily created. Some security guidelines include:

a) When possible, deny IPv6 fragments that are destined to an internetworking device.

b) Ensure adequate IPv6 fragmentation filtering capabilities.

c) Drop all fragments except the last one having size less than 1280 octets.

4.3 Security Issues in Transition Networks

Migration to IPv6 cannot be achieved overnight. Both the protocols need to co-exist for a substantial period of time before IPv4 is phased out. The IETF has come up with several transition mechanisms like dual stacks, tunnels and protocol translation to aid the transition to IPv6.To evaluate the security implications of IPv4 to IPv6 transition and to select the appropriate transition mechanism for the network, the work has already started in 1990 and is still in the evaluation process due to the large infrastructural base of IPv4.This section lists the common vulnerabilities in the IPv4 to IPv6 migration networks and possible mitigation solutions.

4.3.1 Exploiting the Dual Stack

The main flaw with dual stack hosts is that IPv6 stack is enabled by default on several modern operating systems and IPv6 security policy is not enforced accordingly because naive or unaware users neglect the IPv6 migration. This might turn out to be quite dangerous because even if a network does not run IPv6, dual stack hosts are open to local IPv6 attacks. Consider a typical scenario in which an attacker knows that there are some operating systems having IPv6 enabled by default on that LAN. The attacker also learns that all the operating systems are protected against IPv4 attacks but not against IPv6 attacks. The attacker simply waits until a target operating system transmits its periodic router solicitation frame and the attacker might reply to it with router advertisement frame. This causes the node to complete its IPv6 initialization with stateless auto configuration (SLAAC).The next step for the victim machine is to run a DAD procedure. The attacker now has enough information about the target network and might launch IPv6 attack against the target operating system. The attack has a limited scope because the attacker is layer-2 adjacent to the potential victim. The attack success rate also depends on the victim not being protected against the IPv6 threats. Moreover if the network intrusion detection system (NIDS) is not IPv6 aware, the NIDS will not detect those attacks. These threats are also referred to as IPv6 latent threats i.e. existing threats just waiting to be activated. (Convery & Miller,2004)

Fortunately there are multiple ways to protect a dual stack host against the dual stack vulnerabilities.

a) Personal IPv6 Firewalls

Many of the existing network infrastructure components support IPv6 protocol. The need of the hour is to configure them correctly. Cisco Security Agent (CSA 6.0) is an example of a personal firewall and is IPv6 aware. The disabling of IPv6 stack or blocking all IPv6 traffic is a way of mitigating IPv6 latent threats.CSA 6.0 can block all traffic to and from a machine.

b) Microsoft's Group Policy Objects

Microsoft's GPO can be used inside an active directory domain to disable the IPv6 protocol on all interfaces.

c) Blocking Native IPv6 Traffic

The IPv6 Ethernet frames on a LAN with ether type 0x86dd can be blocked using a layer-2 switch. However, having a Virtual LAN Access Control List (VLAN ACL) or Port ACL is a more effective option

4.3.2 Exploiting Tunnels

Tunneling is used as a delivery mechanism of IPv6 traffic using existing IPv4 infrastructure. Before discussing about tunnel security, the network administrator should be able to make a clear distinction between the tunnel that is used within the network (i.e. connects two internal IPv6 networks over an IPv4 network) and a tunnel that is used to gain an IPv6 uplink to the internet for an inside network (i.e. a transition method if the ISP does not offer native IPv6). Since most IPv6 security methods lack authentication, integrity and confidentiality mechanisms, therefore all tunneling mechanisms are susceptible to following attacks (Hogg & Vyncke, 2008):

a) Tunnel Sniffing

If an attacker is able to sniff the IPv4 routing path, he can control the IPv6 tunnel and can execute MITM attacks. The data can be redirected without the knowledge of legitimate user.

b) Tunnel Injection

The attacker can spoof the source IPv4 address of one tunnel end point and inject packets into the IPv6 network of the other tunnel endpoint. If the tunnel end point accepts packets which match the IPv4 address of the other tunnel end point without investigating the inner IPv6 addresses (ACL's etc), the attacker can send any IPv6 traffic into the network. An IPv4-only attacker can send these spoofed packets to the tunnel endpoint; however an attacker is only able to send spoofed IPv6 packets but has no possibility of receiving them from the victim network. Thus, an attacker can only execute DOS attacks. To create forged 6in4 packets, the packet manipulation program Scapy is often being used (Biondi, 2011).

In general, when using tunnels to transfer IPv6 packets into a private network, the firewall should screen the incoming tunnel traffic just the way regular incoming traffic is analyzed. Packets that enter the network through a tunnel should not be able to circumvent any packet filters. The policy applied for incoming IPv4 traffic should also be applied to a tunnel interface for IPv6 traffic i.e. ingress filtering. Unicast Reverse Path Forwarding (uRPF) should be enabled in order to block injected traffic from spoofed source IPv6 addresses that reside on the inside network. ACL's or tunnel inspection mechanisms would prevent the encapsulation of the spoofed 6in4 packets. Using IPSec between two endpoints adds authentication, confidentiality and integrity to all connections between two networks.

4.3.3 Protocol Translation (NAT64)

The basic security drawback with NAT64 is that it breaks the end-to-end communication model and is thus incompatible with IPSec. Therefore IPSec use is not recommended. The protocol translation attracts DoS attacks in which an IPv6 attacker generates many outbound requests to deplete the IPv4 addresses and port pools of NAT64 device (Pool Depletion Attack). This type of attack is also possible in the IPv4-only NAT devices (Hogg & Vyncke, 2008). Although the Application Level Gateways (ALG) must inspect all packets which consume resources like CPU Time and Memory Load, the NAT64 ALG as well as IPv4-only ALG does not add any security component. They just perform the basic job of connecting two different internet protocols.

4.4 Internet Protocol Security (IPSec) as Solution

IPSec is the amalgam of protocols dispensing security in IP networks. It has been the rudimentary security component in IPv4 and IPv6 networks providing for data authentication, integrity and confidentiality. Earlier security was not embedded at the IP level however with emergence of large scale public and corporate internets, the user data became vulnerable to malicious activities like privacy attacks and thefts. To mitigate this and secure network traffic, IETF introduced IPSec for robust network communications.

IPSec was retrofitted as an additional component to provide interim security measure in IPv4 while as in Next Generation Internet Protocol IPv6, it's an integral element and implementation is mandatory to ensure security among the communicating devices. IPSec is administered in IPv6 as a part of extension headers identified by Next Header protocol number 50 for ESP and 51 for AH. The main objectives achieved by IPSec between two communicating peers over an untrusted network are Data Integrity, Data Confidentiality and Data Origin Authentication and Security against Replay attacks (Seo & Kent, 2005; Wikipedia, 2015). Data Integrity requires maintaining accuracy and consistency of data. The data should not be tampered while in transmission over public networks. Data Confidentiality demands encryption of data during transmission. This means even if data is accessed somehow, it cannot be interpreted. Data Origin Authentication verifies the source of data and ensures that it is sent by legitimate sender. In IPv6; IPSec is implemented using Site-to-Site network tunneling and plays a major role in ensuring that data is transmitted securely and efficiently. In fact most of the corporate VPN's (Virtual Private Networks) having branches throughout the world are secured through IPSec. Since IPSec is deployed at network layer, it ensures security of IP level packets only. Despite numerous benefits of IPSec, its implementation does have some performance issues. The issues are mainly attributed to complex key management and protocol negotiations between two communicating parties.

4.4.1 IPSec Architecture Analysis

The design of IPSec is expounded through RFC 4301 which describes security architecture for IPv4 as well as IPv6 (Hogg & Vyncke, 2008).The general framework of IPSec encompasses the following elements:

- Security requirement interpretation.
- Protocol specification for encryption (Encapsulated Security Protocol or ESP) and authentication (Authentication Header or AH).
- Negotiations on use of cryptographic algorithms for encryption and authentication.
- Negotiations of security policies and associations.
- Internet Key Management.

The IPSec lists down two protocol headers for providing network security and confidentiality; the Encapsulating Security Protocol (ESP) Header and Authentication header (AH) (Hagen,2006).Both these headers are implemented as extension headers in IPv6.The main difference between AH and ESP lies in the fact that AH does not provide the confidentiality option

4.4.1.1 Authentication Header

The Authentication Header (AH) as defined in RFC 4302 dispenses connectionless integrity and data source authentication (without confidentiality factor) for all end-to-end transmission of IP packets. AH provides varied authentication mechanisms and also protection against replay attacks. In IPv6; the AH having next header value of 51 in extension header succeeds Hop by Hop, Routing and Fragment extension headers. The AH is sand witched between Upper layer protocol headers (TCP, UDP) and the IP. Figure 4.1 illustrates the format of AH.

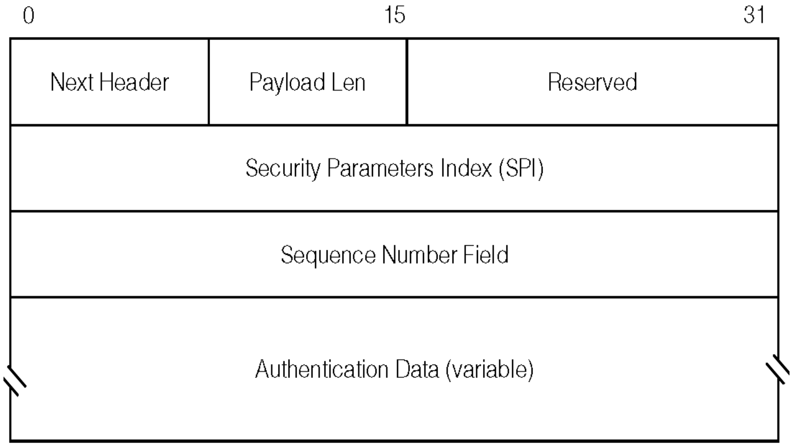
0
15
31
Next Header
Payload Len
Reserved
Security Parameters Index (SPI)
Sequence Number Field
Authentication Data (variable)

Figure 4.1 Authentication Header

○ *Next Header* implies the class of header that follows authentication header.

○ *Payload Length* defines the length of the header in four byte units.

○ *Reserved* Field is not used and is initialized to zero.

○ *Security Parameter Index* helps in unique identification of security association for a particular datagram.

○ *Sequence Number* makes a counter of number of packets sent from source to destination.

○ *Authentication data* contains the checksum value (integrity check value) for the packet. It is of variable size.

4.4.1.2 Encapsulating Security Protocol

The Encapsulating Security protocol header as defined in RFC 4303 provides for connectionless integrity, data source authentication and confidentiality of IP packet data.ESP encrypts the packet payload using different encryption algorithms to provide confidentiality. The potential services rendered by ESP are negotiated when Security Associations are established. In IPv6; the next header value of 50 in extension header indicates the ESP Header which consists of following fields as shown in figure 4.2

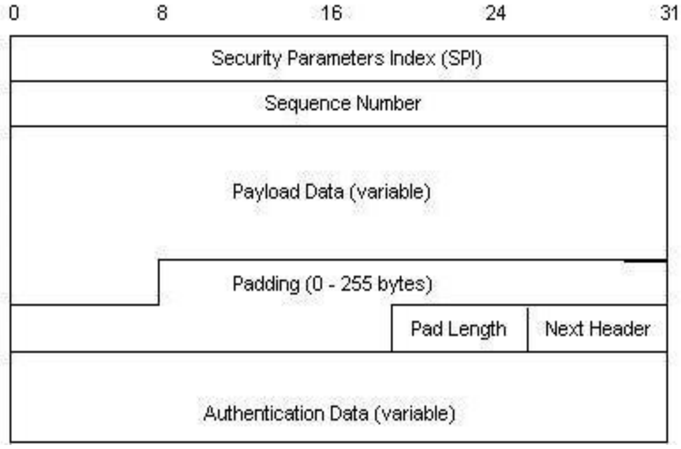

Figure 4.2 Encapsulating Security Protocol Header

- *Security Parameter Index* helps in unique identification of security association for a particular datagram.
- *Sequence Number* makes a counter of number of packets sent from source to destination.
- *Payload Data* contains encrypted data and initialization vector (IV) if mandated by encryption mechanism.
- *Padding* is used mainly to align packet in multiples of 4 bytes. It's also required because of encryption.
- *Pad Length* determines the length of padding used.
- *Next Header* implies the class of header following the ESP header.
- *Authentication data* contains the checksum value (integrity check value) for the packet. It is of variable size.

In both AH and ESP, message authentication and integrity are achieved by using keyed MAC (Message Authentication Code) based on symmetric encryption algorithms like MD5, SHA-1.IPSec protocol runs in one of the two modes: The Transport mode or The Tunnel Mode. The Transport mode IPSec establishes connections between two end systems directly. In this mode; the whole IP payload is protected leaving the original header intact. IPSec in the Tunnel mode creates a virtual secure tunnel between two gateway systems that lie in the path of two end systems. Tunnel Mode encrypts and encapsulates whole IP datagram and creates an outer IP header. The AH and ESP both operate in Transport as well as Tunnel Mode as shown in figure

4.3 and 4.4.The Transport mode ESP safeguards the original IP header and adds new ESP extension header with an optional trailer. These provide encryption of data payload. The Transport mode may also contain optional ESP authentication trailer which assists in HMAC authentication of original header and payload. The AH in Transport mode provides authentication of original IP header and payload by adding new extension header.

In Tunnel mode, ESP and AH create a new IP header that encapsulate the actual header and payload. In ESP, the original IP header and payload is encrypted as well as authenticated; while as compared to AH, it's only authenticated and not encrypted.

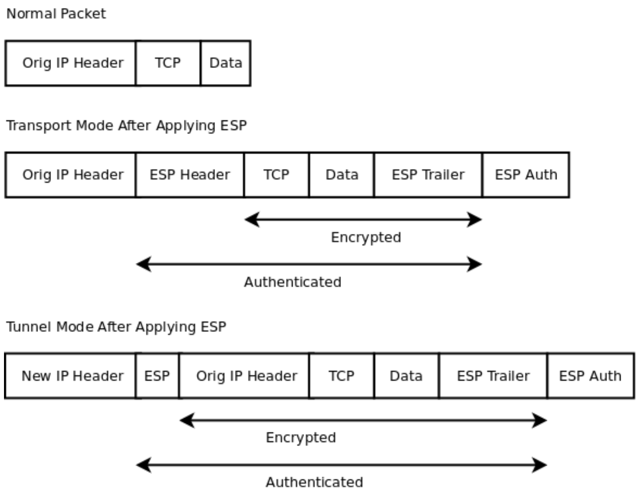

Figure 4.3 ESP Data Packet

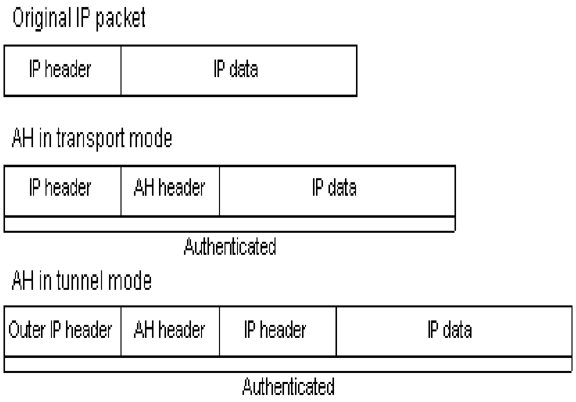

Figure 4.4 AH Data Packet

4.4.1.3 IPSec Security Association

Before the communication between two different peers, there needs to be establishment of agreements known as Security Associations (SA). The framework of security association rests on the following building blocks which include (Menezes, 2012):

○ *Time Validity* of Association
○ *Mode of Operation*-whether Tunnel or Transport
○ *Cryptographic Parameters* like Key, Encryption protocol and Authentication Mechanism.
○ *Sequence Number and Anti Replay Window*

Security Associations operate unidirectional, which means that if two nodes want to encrypt and authenticate a two way communication session; four security associations need to be established (two for encryption and two for authentication).A device can establish SA's with several nodes. To uniquely identify SA, combination of 32-bit Security Parameter Index (SPI) and endpoint IP address is used. Each IPSec header contains value of SPI which is used by end node to identify SA. Every communicating peer maintains a database for incoming and outgoing SA's. This database is commonly referred to as SADB (Security Association Database)

4.4.1.4 IPSec Key Management

For secure communication; two peers must agree on encryption algorithms, authentication algorithms and keys that are going to be used (Hogg & Vyncke, 2008).To facilitate this key exchange mechanism, IPSec uses IKE protocol. The IKEv1 as specified in RFC 2409 uses UDP on port 500 or 4500 with two phases: Phase 1 sets up secure communication channel for ensuing communications between end nodes. Phase 1 exchange which uses Diffie- Hellman key exchange conventionally executes in Main mode or Aggressive mode. The Aggressive mode is little faster but less secure. Authentication is achieved either through Pre-shared keys (RSA checksum encrypted with private key of sender) or combination of receiver's public key with its X.509 certificate. Phase 2 also called Quick mode involves negotiation on other parameters like encryption algorithms, keys/certificates which are used for actual communication. The IKEv1 phase 2 output results in SA that define security services needed to protect data traffic

4.4.2 Issues with IPSec

Despite IPSec's secure services which have contributed to its popularity, IPSec implementation suffers certain drawbacks (Shah & Parvez, 2014). These drawbacks are owing to complex key exchange mechanisms, protocol negotiations, Security Association setup. These issues are significant and have considerable amount of impact on the performance of network. For example, using IPSec Tunnels, nodes may suffer encapsulation and decapsulation delays due to additional new headers. These delays impede the performance and throughput of network. Additional headers also lead to increased packet size than permissible MTU of given node's interface (IPSec Issues, 2015). As a result, some routers may not fragment and forward the data packets if they are larger than permissible MTU. This results in increased packet drop.

The IPSec implementation is incompatible with NAT. The NAT Translation device fiddles with IP header which can render Authentication data as invalid and cause IPSec integrity check at receiver to fail. The Authentication data calculation involves source and destination IP address. With AH in Transport mode, the source address gets translated after the Authentication Data computation. This causes the message integrity check at the receiver to fail. With ESP in Transport mode, checksum calculation in TCP header includes the source and destination IP addresses. Because NAT revamps the source IP which renders TCP checksum as invalid. The checksum value needs to be re-computed by NAT device if encryption is not used. However this would cause message integrity check to fail. The only feasible option is IPSec ESP in Tunnel mode which does not cause incompatibilities.

NAT also elevates problems for IKE negotiations if the parameters are modified (Zheng & Zhang, 2009; Shah & Parvez, 2014). For example while using pre-shared key authentication in main mode; the address change can lead to tossing out packets.NAT can also lead to overlapping Security Association Database (SAD) entries when multiple nodes behind the NAT try to make a contact with same host. This host may send response packets to wrong nodes because of identically occurring Security Associations.

IPSec Implementation mandates for higher computational power in nodes for cryptographic hash calculations and key generations. Sufficient amount of power may not be available in Low Power Devices (6LOWPAN) and mobile phones.

4.4.3 Related Work

Due to large scale magnification in public internet, IPSec is used as a fundamental security solution. A lot of work is getting carried with the aim to overcome the complexities and evaluate the performance. (Klaue & Hess, 2005) have evaluated the effect of IPSec on Interactive communications. The work is significant and shows that IPSec can be used to secure multimedia communications over a wireless link without noticeably degrading the perceived quality. However; the main application of IPSec is in securing VPN’s. Authors (Miteshkumar & Arvind, 2013) discuss about the imperatives and issues of IPSec based VPN’s. The issues involved and performance evaluation is also done. VPN’s which are commonly used for private transmission over public networks provide a safe heaven for malicious activities unless protected by security protocols.(Yasinovskyy, Wijesinha & Karne,2009) discuss the impact of IPSec and 6to4 on VoIP quality over IPv6.The authors have conducted the experiment in a LAN environment and measured VoIP performance in varying background traffic conditions. IPSec as we know suffers divergence towards NAT. Authors (Ahmad & Yaacob, 2013; Heinlein, 2009) address and explore the issue of incompatibility between IPSec and NAT. In fact, (Ahmad & Yaacob, 2013) proposes a workable solution to implement end to end IPSec in heterogeneous IPv4 and IPv6 networks. Experimental results show that the mechanism is feasible to establish a successful IPSec connection across IPv4/IPv6 translation gateway. In addition to performance evaluation, significant work is being carried to introduce novel features in IPSec. For example; (Zheng & Zhang, 2009) introduce the IPSec security architecture and its mechanism, and give an in-depth analysis of the IPSec security. Due to the flaws of the pre-shared key authentication method and the fact that it is vulnerable to DoS attacks, they propose a dynamic pre-shared key generation method to avoid the harm to the system caused by crack of the pre-shared key. The improved method generates the pre-shared key dynamically before the SA negotiation. Every time when the SA is created, new pre-shared key will be automatically generated, the drawbacks of fixed pre-shared key are avoided. (Zhang et al, 2009) propose a software approach based on IPSec Thumbnail Protocol (ITP) to accelerate IPSec communication. They believe that by caching data segments of the original IP packet and constructing ITP Thumbnail packet to transfer, IPSec communication can be accelerated. They have implemented ITP prototype system on Linux platform. While deploying IPSec in the network, the most common overhead i.e. encapsulation/decapsulation impacts the quality of service of the network. This overhead has a direct impact on network delay and jitter, particularly in real time multimedia applications. A substantial amount of work is being carried out on measuring such parameters. (Yasinovsky et al, 2009) have conducted experiments in a LAN environment to determine the impact of IPSec and 6to4 encapsulation on VoIP quality in future IPv6 networks. They have measured VoIP performance in the presence of varying background traffic for each of four IPSec scenarios with IPv6 and 6to4 encapsulation, with and without NAT, and compared with IPv4.Their results indicate that VoIP quality due to using IPSec with IPv6, 6to4, and NAT in VPNs during the IPv4/IPv6 transition is not significantly different from using IPSec with IPv4, and that there is a minimal impact on voice quality as long as the network capacity is not exceeded. In (Babu, 2012), analysis and experimental results for an evaluation of the QoS of Voice traffic using IPSec is presented. The author measures certain metrics like Packet Delay Variation, MOS (Mean Opinion Score), Packet End to End Delay, Traffic Received and Traffic Sent. Experimental results demonstrate that, depending on the type of the traffic, the overall security of the networks is improved, with a reasonable decrease in term of performance. A similar kind of work can be found in (Klaue, 2005) where the authors measure the performance of voice and video communications in a LAN including a wireless hop. They evaluated the measurements in terms of network parameters like loss, delay, and jitter and with respect to perceived quality. Results show that IPSec can be used to secure multimedia communications over a wireless link without noticeably degrading the perceived quality.

4.4.4 Simulation Scenario Setup

This section describes the experimental setup for evaluating the impact of IPSec on Real Time applications like VoIP and Video conferencing in IPv6 and 6to4 Tunneling Migration Network. The simulation is carried in a controlled environment using elementary internetworking devices and network elements. The network devices that we use include workstations, internet gateways devices, IP backbones and communication links like Ethernet 100baseT and PPP_DS3 cables. The experiment is carried in three different networks scenarios: IPv6 Only, IPv6 with IPSec and 6to4 Tunneling (IPv4 to IPv6 Migration Technique).In first scenario no IPSec is configured in IPv6 only network. In second scenario IPSec Tunnel is configured between Routers R1 and R2.In third Scenario we check the impact on IPv4 to IPv6 migration network (6to4).In this scenario PC-1 and Server are running IPv6 while the network in between is IPv4.6to4 Tunnel as well as IPSec Tunnel is configured on R1 and R2.The topology used for the simulation is shown in figure 4.5.

All the three scenarios are modeled in OPNET simulator ver. 14.5.The network traffic consists of VoIP and video conferencing. We chose these two Real time applications because they are sensitive to delay and require desired performance. Any delay or distortion in the network will effect these applications. We chose the network as IPv6 due to its vast and rapid adoption.

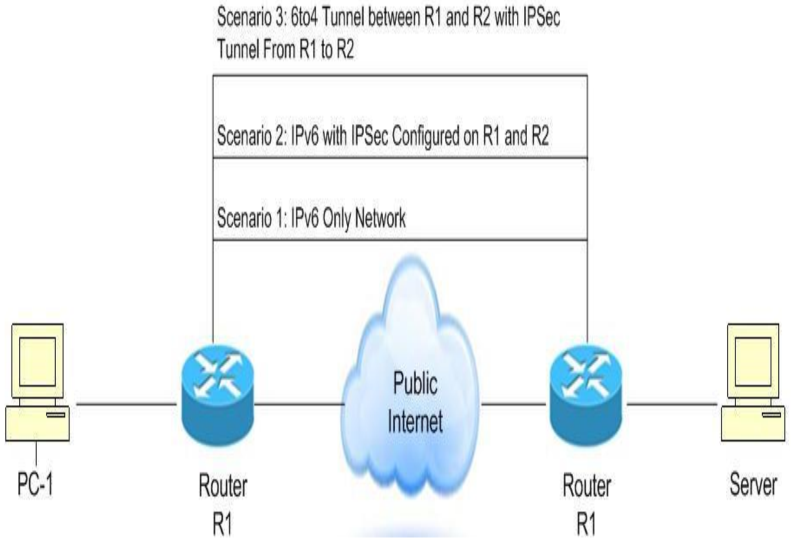
Scenario 3: 6to4 Tunnel between R1 and R2 with IPSec Tunnel From R1 to R2
Scenario 2: IPv6 with IPSec Configured on R1 and R2
Scenario 1: IPv6 Only Network
PC-1
Router R1
Public Internet
Router R1
Server

Figure 4.5 Network Topology for Simulation

Researchers have shown a notable interest on measuring IPv6 security performance metrics and behavior. As IPv4 address space has depleted and to maintain connection with the legacy protocol; we also evaluate IPSec effect on 6to4 which is one of the internet migration techniques.

The parameters that we want to measure are *IP End-to-End Delay*, *Throughput*, *Jitter*, *Packets Drop Rate*, *Tunnel Delay* (Scenario 2 and 3). *IP End-to-End Delay* may be described as time taken for the packet to reach its destination from its source measured as the difference between the time a packet arrives at its destination and the creation time of the packet. *Jitter* may be defined as delay variation in packets belonging to same flow. This is an important QoS parameter and can impact the quality of streaming in video and voice applications. If two consecutive packets with time stamps ts1 & ts2 leave the source node and are sent back at time ts3 & ts4 the destination node, then:

Jitter = (ts4 – ts3) - (ts2 - ts1)

Negative jitter implies that the time differentiation across packets at the destination node was less than that at the source node. Typically tolerance level of voice data packets is about 0.075 seconds but preferable jitter is within 0.040 seconds. *Throughput* is defined as the average data transferred across the medium per unit time. *Packet Drop Rate is the* number of IP datagram's dropped by all nodes in the network across all IP interfaces. *Tunnel Delay* is the delay experienced by a packet coming through a tunnel, i.e. the difference between the time at which the packet is sent in on the tunnel and the time at which it is received at the opposite end, in seconds. This includes the encapsulation and decapsulation delays

4.4.5 Results

All scenarios were run separately and performance parameters were collected. The total simulation runtime for each scenario was 15 minutes. Figure 4.6 to 4.9 shows the result of performance parameters that were collected. For simplification the average of each collected value is shown in table 4.1.

	Network Scenario		
	IPv6 without IPSec	IPv6 with IPSec	6to4 Tunnel with IPSec
IP Voice			
Throughput (bits/sec)	48880.7	38706.3	36554.1
Packet Dropped (packets/sec)	0.022	0.0255	0.0768
IP End-to-End Delay (sec)	0.0711	0.0723	0.0744
Jitter (µsec)	0.0000149	0.0000197	- 2.4
Tunnel Delay (sec)	n/a	0.0031	0.0035
Total Delay (sec)	0.0711149	0.0754197	0.0779024
Video			
Throughput (bits/sec)	933355 .2	884961	867231.33
Packet Dropped (packets/sec)	0.0244	0.0255	0.0835
IP End-to-End Delay (sec)	0.0149	0.0155	0.0159
Tunnel Delay (sec)	n/a	0.0065	0.0098
Total Delay (sec)	0.0149	0.022	0.0257

Table 4.1 Average Values of Simulation for experiment

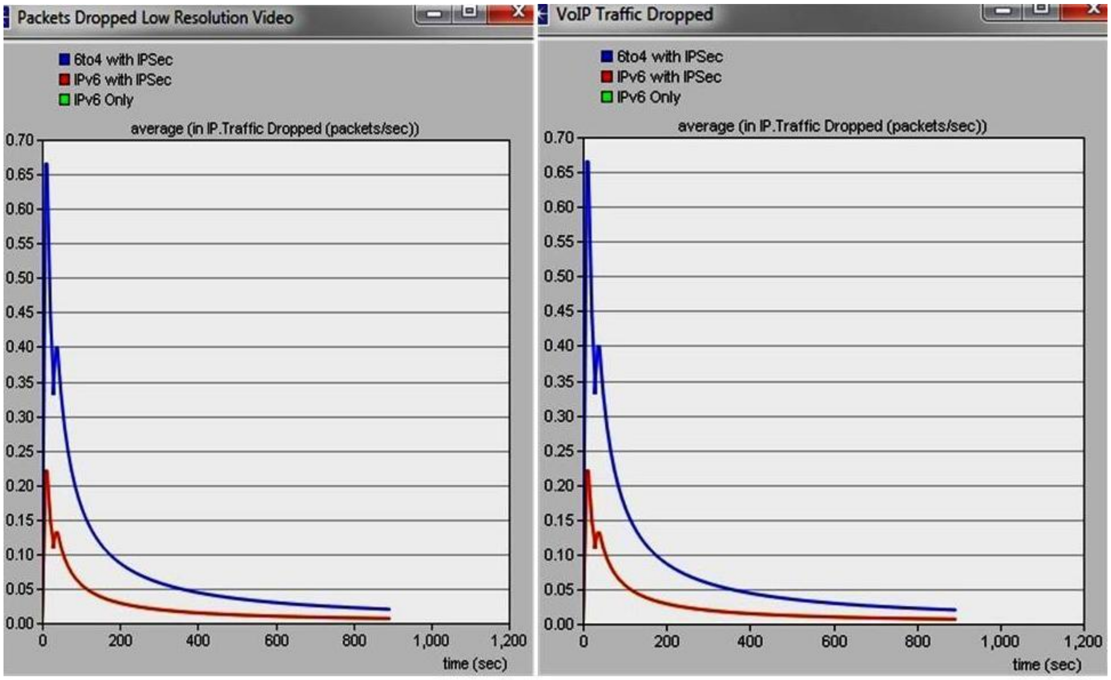

Figure 4.6 Packets Dropped (a) Video (b) VoIP

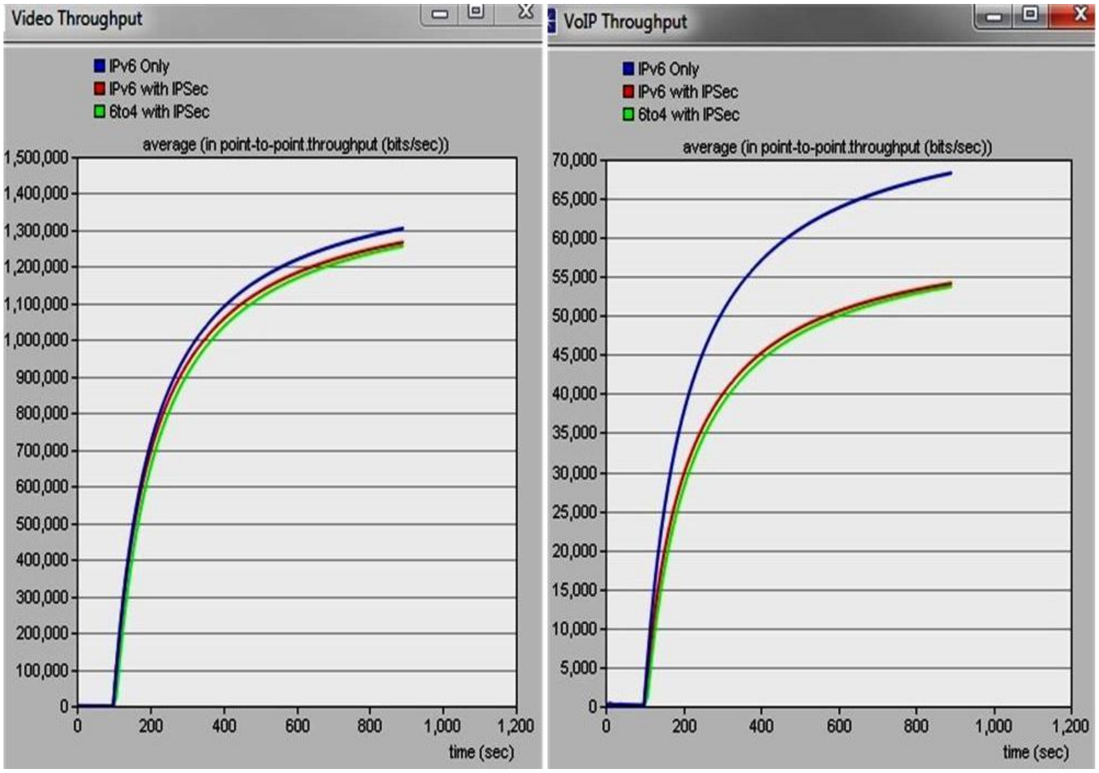

Figure 4.7 Throughput (a) Video (b) VoIP

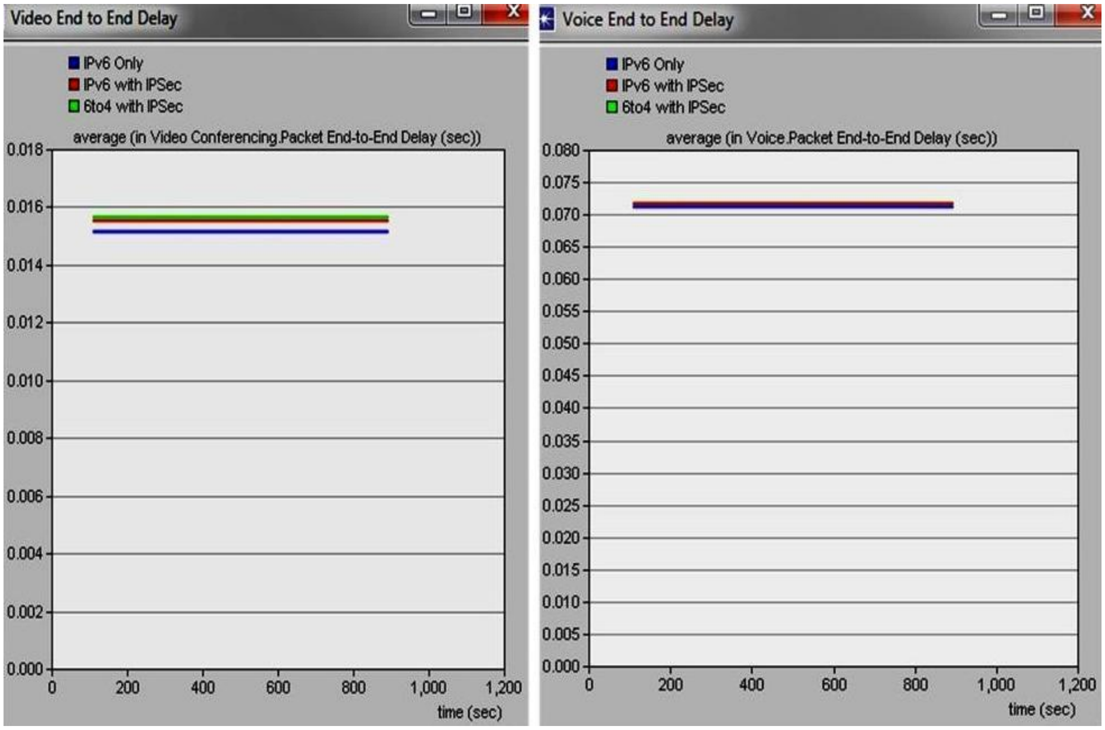

Figure 4.8 End-to-End Delay (a) Video (b) VoIP

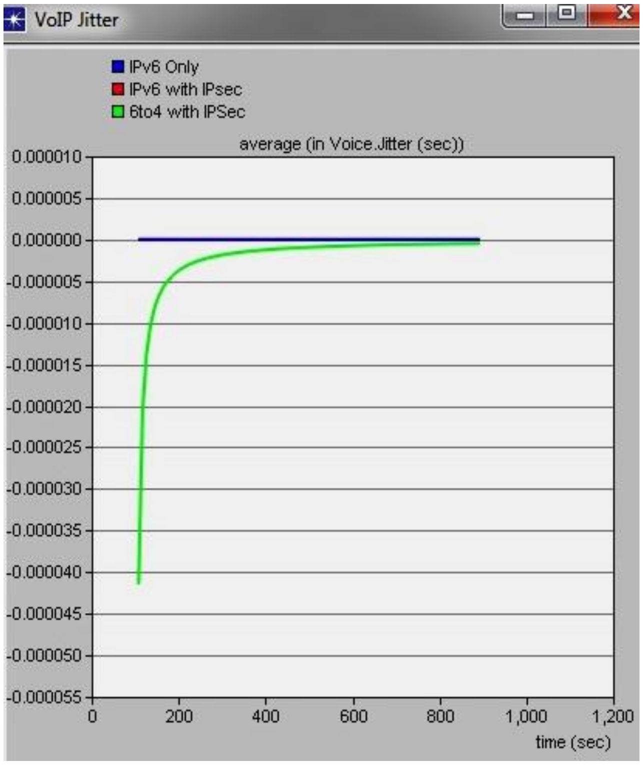

Figure 4.9 VoIP Jitter

Analyzing table 4.1, we notice that IPSec has a significant effect on IPv6 and 6to4 (IPv4 to IPv6) migration network. When we implement IPSec security we notice considerable decrease in throughput and increase in delay in the network. The delay is caused due to additional security headers that an IP packet has to handle. The nodes in addition to packet forwarding have to carry encryption/decryption, cryptographic hash calculations, Internet key exchange and encapsulation/decapsulation of data packets. This is a cumbersome process contributing to delay. The results also show that large packet drop rate is experienced by implementing IPSec on IPv6 and 6to4 Tunnel. In simulation we noticed that if we use IPv6 without IPSec; performance is fairly better but is less secure. Steps need to be carried in devising methods which can both be optimal as well as secure.

4.5 Summary

IPv6 has both advantages as well as drawbacks from the security point of view. To ensure suitable and timely deployment of IPv6, the security aspects should be thoroughly considered. IPv6 provides number of security features over IPv4, such as mandatory usage of IPSec, but these features come with overheads and performance issues. This demands optimization in hardware and software like enhancing router filtering capabilities or implementing strong firewall rules. The similarities in two protocols help in implementing strong security policies to secure IPv6 networks. However new and additional characteristics in IPv6 demand new solutions to protect the next generation of integrated computer networks.

IPSec is a broader step towards security in IPv4 and Next Generation Internet Protocol IPv6.This chapter examined IPSec architecture framework and made a discussion on its associated protocols. The chapter also highlights IPSec issues and its incompatibility with current IP Network. We also surveyed about recent work being carried out in this area. Later we made an empirical investigation of the parameters that are affected by implementation of IPSec in IPv6 and 6to4 Tunneled Migration Networks and compared the results with IPv6 network without using IPSec. We notice that IPSec has notable impact on the network and performance gets decreased while incorporating security. This performance decay affects Real time application like VoIP and Video conferencing which are most sensitive to delay. So there is always a tradeoff between choosing better security or optimal performance. The performance of the network can slightly be increased if complexities in IPSec are removed. The use of caching and dynamic key generation should be preferred. If we talk of Real Time applications, QoS models and techniques should be implemented to avoid packet drop and delay. A stripped down version of IPSec should be incorporated in low power devices and mobile phones because they don't have large computational power. An approach like Header compression technique needs to be devised for accelerating IPSec enabled communication.