Abstract—Internet Protocol relays data across boundaries. This paper outlines the attacks and performance factors of IPv4 and IPv6 protocols. A small network of computing devices that started as ARPANET project is now a worldwide network of devices for most of users. This global network, the Internet, has become an integral part of worldwide economy and life of individuals. Internet Protocol (IP) v4 is the basic building block of the Internet and has served well, but it has limitations that hinder its growth. The solution is IPv6, which addresses inherent problems of the earlier version. However, due to the increased overhead in IPv6 and its interaction with the Operating system that hosts this communication protocol, there may be network performance issues. In this paper, we investigated the Performance related metrics like throughput, delay, jitter and CPU usage are empirically measured on a test-bed implementation. As a result the various features of both the protocols based on the performance evaluation are provided.

Keywords— IPv4, IPv5, IPv6, Throughput, Jitter, Delay.

I. INTRODUCTION

Computer networks have impacted people of different ages from almost all walks of life. A researcher in India can concurrently work with a fellow researcher say in the USA, by simply connecting to his computer. Computers are said to be ‘interconnected’ if they can exchange data and ‘autonomous’ computers are those that have the freedom to use their own processing power, memory and other resources. The interconnection may be via copper wires, optical cables, micro-wave links, laser or even communication satellites. Each organization chooses hardware technologies appropriate to its needs creating several heterogeneous networks. It is necessary to exchange data and program among these heterogeneous networks. To solve this problem, a technology evolved, that enabled the connection of disparate physical networks and makes them function as a coordinated system. This technology is called internetworking and the resulting network an internet. US government agencies realized the importance and potential of the internet technology during the late 1960’s and began to fund its research. The ARPA (Advanced Research Projects Agency) played a lead role in the development of the ARPA, with experience gained from its own net-work called ARPANET began to work intensely on a global internet. Before the advent of computer networks communication is based on telecommunications system, where communication between calculation machines and early computers was performed by human users by carrying instructions between them and known to be distributed processing. Their work caught the attention of many researchers and a board called Internet Control and Configuration Board (ICCB) was set up to co-ordinate the work. The ICCB came up with a set of standards that specified the details of how computers communicate and also a set of conventions for interconnecting networks and routing (transferring) data among them. Technically referred as the TCP/IP Protocol suite, this could be used to communicate across any set of interconnected networks. The global internet (called Internet, with a capital I) thus began during the early 1980’s when ARPA started using TCP/IP protocol on computers. Within about seven years since its inception, the Internet had spanned across hundreds of networks across USA and Europe. By 1994 it reached over 3 million computers in 61 countries. This exponential growth continued and by 2001 there were 140,000,000 hosts (computers) linked to this massive heterogeneous network. With TCP/IP as its backbone, the Internet has a vast number of applications to offer like electronic mail, remote login and file transfer. The revolutionary application, which brought the Internet into public consciousness, is the World Wide Web (WWW for short). Like most other networking protocols, the TCP/IP is made up of different layers, with each layer responsible for a different role in data communication. TCP/IP Protocol Suite is normally considered to be a 4-layer system. Transferring a message from an application program on one machine to an application program on another involves transferring the message down through successive layers. The data, in the form of packets or units called Protocol Data Units (PDUs), travels through the sender’s layers, travels across the network and goes up the receiver’s layers. Thus Network is a system of interconnected communication devices that can communicate with one another and share information. Networks are of three types. These are Local Area Networks (LAN). In this network system computers are interconnected in a limited geographical area, such as network of computers.
in college computer laboratory or network of computers in office, building etc., Secondly, Wide Area Network (WAN) is a network system that covers a large geographical area such as different cities of country or different countries of the world. In WAN telephone lines, satellites, microwave, fiber optic etc. are used as transmission media. And Finally Metropolitan Area Network (MAN) is a network system that covers area of a single city. Usually, MAN connects more than one LANS in a city or town and covers a smaller geographical area than a WAN. The cable television, telephone companies or local corporations use MAN.

Network layer protocols are
- CLNP Connectionless Networking Protocol
- EGP Exterior Gateway Protocol
- EIGRP Enhanced Interior Gateway Routing Protocol
- ICMP Internet Control Message Protocol
- IGMP Internet Group Management Protocol
- IGRP Interior Gateway Routing Protocol
- IPv4 Internet Protocol version 4
- IPv6 Internet Protocol version 6
- IPSec Internet Protocol Security
- IPX Internetwork Packet Exchange
- Routed-SMLT
- SCCP Signalling Connection Control Part
- AppleTalk DTP

The demand for the ubiquitous personal communications is driving the development of new networking techniques. In the wireless communication the security of the data plays the vital role. To improve the security of the data being transmitted various techniques are employed. Internet Protocol is a set of technical rules that defines how computers communicate over a network. There are currently two versions: IP version 4 (IPv4) and IP version 6 (IPv6). IPv4 was the first version of Internet Protocol to be widely used, and accounts for most of today’s Internet traffic. There are just over 4 billion IPv4 addresses while that is a lot of IP addresses; it is not enough to last forever. IPv6 is a newer numbering system that provides a much larger address pool than IPv4, amongst other features. It was deployed in 1999 and should meet the world’s IP addressing needs well into the future. IPv4 is the dominant addressing protocol used on the Internet and most private networks today.

With the current exponential growth in Internet users worldwide, combined with the limited address range of IPv4, the number of available public IPv4 addresses remaining is very limited. IPv6 is the next-generation Internet protocol that will replace IPv4, providing a vastly expanded address space. The major difference between IPv4 and IPv6 is the number of IP addresses. There are 4,294,967,296 IPv4 addresses, 340,282,366,920,938,463,463,374,607,431,768,21,456 IPv6 addresses. The technical functioning of the Internet remains the same with both versions and it is likely that both versions will continue to operate simultaneously on networks well into the future. To date, most networks that use IPv6 support both IPv4 and IPv6 addresses in their networks.

The most obvious difference between IPv6 and IPv4 is the address size. IPv6 addresses comprise 128 bits, whereas IPv4 addresses comprise 32 bits. This difference results in a huge expansion in available IP address space:
- IPv4: 232 addresses equal 4.3 billion addresses (less than the global human population of 4.7 billion)
- IPv6: 2128 addresses. Because the last 64 bits are used to allocate addresses within a subnet that leaves 264, which equals 18 billion subnet addresses.

This paper is organized as follows. In the section 2 the related work based on the IPv4 and IPv6 performance and deployment are discussed. In the section 3 the proposed study on both the protocols is and its attacks is provided. The section 4 discusses the various attacks of the protocols. The section 5 discusses the various performance factors of the protocols. In Section 6 discusses ipv4 shortcomings and ipv6 threats. And finally in Section 7 the conclusion is provided.

II. RELATED WORK

In this section the various methodologies and techniques that are discussed by various authors in papers are provided. In the paper, proposed by Shaneel Narayan (Member IEEE), Peng Shang, Na Fan, the various performance issues such as the delay in the network transfer, the management of the CPU time in efficient manner for the different type of the operating system is provided.

In the paper proposed by Xianhui Che, Dylan Lewis, the interoperability of the IPv6 protocol with the earlier versions, the transition mechanisms, the security aspects, the cost based on the speed of the protocols are discussed.

Marvin R. Márquez in his proposed research paper the various transitions why the transfer of the IPv4 to the IPv6 version is taken place and the special features of the version 6 protocols, their advantages are provided.

III. PROPOSED WORK

In this section the internet protocol versions 4 and 6 addressing, sub netting, their security, cost and other features are provided. IPv6 has been designed as an evolutionary step from IPv4 and it addresses problems inherent in IPv4, plus offers new opportunities for services that can be provided via computer networks.
Internet Protocol Version 4

The following figure is the schematic structure of the addressing for IPV4 protocol. It consists of the type of the version, the total length of the packet to be transmitted, the type of the service offered by the providers, the packet identification field, and the time slice field. The length of the IPV4 is small that is $2^{32}$ hence the number of individual users on the network is small. Hence the packets can be transmitted within the estimated time with lower CPU cost and time. The packets are delivered without the retransmission.

IPv4 Addressing

One of IP’s core functions is to provide logical addressing for hosts. An IP address provides a hierarchical structure to separate networks. Consider the following address as an example: 158.80.164.3. An IP address is separated into four octets:

First Second Third Fourth Octet
158 .80 .164 .3

Each octet is 8 bits long, resulting in a 32-bit IP address. A computer understands an IP address in its binary form; the above address in binary would look as follows:

First Second Third Fourth
10011110 .01010000 .10100100 .00000011

Part of the above IP address identifies the network. The other part of the address identifies the host. A subnet mask helps make this distinction. Consider the following: 158.80.164.3 255.255.0.0. The IP address has a subnet mask of 255.255.0.0. The subnet mask follows two rules:

• If a binary bit is set to a 1 (or on) in a subnet mask, the corresponding bit in the address identifies the network.
• If a binary bit is set to a 0 (or off) in a subnet mask, the corresponding bit in the address identifies the host. Looking at the above address and subnet mask in binary:

Address: 10011110.01010000.10100100.00000011
Subnet Mask: 11111111.11111111.00000000.00000000

The first 16 bits of the subnet mask are set to 1. Thus, the first 16 bits of the Address (158.80) identifies the network. The last 16 bits of the subnet mask are set to 0. Thus, the last 16 bits of the address (164.3) identify the unique host on that network.

Internet Protocol Version 6

The IPv6 is designed to promote higher flexibility, better functionality and enhanced security & mobility support. Because of these advantages, the service providers generally should be inclined to migrate to this newer version of Internet technology. Although IPv4 has proven to be robust, easily implemented and interoperable, the initial design did not anticipate the following:

- The exponential growth of the Internet and the impending exhaustion of the IPv4 address space
- The ability of internet backbone routers to maintain large routing tables
- The need for simpler and automatic configuration of IP addresses.
- The requirement of security at IP layer
- The need for better support for real-time delivery of data also called quality of service (QOS) for applications like VOIP, VOD etc.

<table>
<thead>
<tr>
<th>Version</th>
<th>Length</th>
<th>Service Type</th>
<th>Packet Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification</td>
<td>NA</td>
<td>DF</td>
<td>WF</td>
</tr>
<tr>
<td>Time to Live</td>
<td>Transport</td>
<td>Header Checksum</td>
<td></td>
</tr>
<tr>
<td>Sending Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Options</td>
<td>Padding</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IPv6 is a new version of the data networking protocol on which the Internet is based. The IETF developed the basic specifications during the 1990s. The primary motivation for the design and deployment of IPv6 was to expand the available addressing space of the Internet, thereby enabling billions of new devices (PDAs, cellular phones, appliances, cars, etc.), new users and „always-on” technologies (xDSL, cable, Ethernet-to-the-home, fiber-to-the-home, Power Line Communications, etc.).IPv6 has a 128-bit address space that can uniquely address 2128 network interfaces. So the new
address space supports 2^128 (approximately 340,282,366,920,938,000,000,000,000,000,000,000,000,000) address spaces. This expansion allows for many more devices and users on the Internet as well as extra flexibility in allocating addresses and efficiency for routing traffic. IPv6 has been designed with the principle of being able to coexist with IPv4 for a long period of time, avoiding breaking IPv4 networks and allowing all the existing services and applications to keep working without any disruption. At the same time, the way this coexistence works should allow a smooth transition from IPv4 to IPv6. In short, the basis of this coexistence and transition is having both protocols in the hosts at the same time (this is called dual-stack), and allowing the operating systems and/or applications to choose which protocol they use for each communication.

### Table: IPv6 Addressing

<table>
<thead>
<tr>
<th>Version</th>
<th>Priority</th>
<th>Flow Label</th>
<th>Payload Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 bits</td>
<td>4 bits</td>
<td>24 bits</td>
<td>16 bits</td>
</tr>
<tr>
<td>Next Header</td>
<td>Hop Limit</td>
<td>Source Address</td>
<td></td>
</tr>
<tr>
<td>8 bits</td>
<td>8 bits</td>
<td>128 bits</td>
<td></td>
</tr>
<tr>
<td>Destination IP Address</td>
<td>32 bits</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payload + Extension Head</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IPv6 Addressing**

The IPv6 protocol standard includes that the new protocol will have better support for options by using the extension headers, will provide for better security, and more choices in type of service. IPv6 providers can be seen as a security advantage. IPv4 based networks are attacked by brute force address and port scans of entire subnets. Once an assigned IP is known, the attacker only has to review 28 subnets and 216 site addresses to discover every host on that particular network, but this is totally ignored at IPv6.

**IV. ATTACKS ON IPV4 AND IPV6**

This section outlines attacks that are not fundamentally altered by IPv6:

- Sniffing
- Application layer attacks

**Sniffing**

Sniffing refers to the class of attacks that involves capturing data in transit across a network. The most common example of this is Tcpdump, which is included in most UNIX-like operating systems. An adversary executing sniffing attacks can often determine login credentials or view sensitive information in plaintext protocols. Although IPv6 provides fundamental technology to prevent sniffing with IPsec, it does not provide any simplification for the key management issues that have proved to be challenging. Until the key management issues (among others) are resolved, deployment of IPsec will be stalled and sniffing attacks will continue to be possible.

**Application Layer Attacks**

Application layer attacks refer to all the attacks performed at Layer 7 of the OSI model. This is the bulk of all attacks on the Internet today, and the vulnerabilities that enable these attacks represent the source of most of the insecurities in today’s networks. General attacks such as buffer overflows, Web application attacks (Common Gateway Interface [CGI] and so on), and viruses and worms all fall into this category. IPv4 and IPv6 are both, for the most part, neutral parties to application layer attacks. Certainly if the protocol had adopted more stringent authentication of IP addresses some of these attacks could be more easily traced, but the bulk of any blame in application layer attacks lies in the affected application, not the underlying transport. Even assuming the worldwide implementation of IPsec, application layer attacks change very little with IPv6 adoption. Even though a given connection can be cryptographically protected, there is nothing to stop an application layer attack from traversing the encrypted link and causing the same damage as if it were in the clear. The only difference is that tracing back the attack may prove easier because of the authentication in cases where Layer 3 information could otherwise be spoofed. However, if IPsec is more ubiquitously deployed from end station to end station, without some mechanism for key, all security protections will fall to the host. Because all a firewall or IDS sees is encrypted traffic, it cannot make any decisions based on such data.

**Rogue Devices**

Rogue devices are devices introduced into the network that are not authorized. Although this could most easily be a simple unauthorized laptop, more interesting for an adversary would be a rogue wireless access point, DHCP or DNS server, router, or switch. These attacks are fairly common in IPv4 networks and are not substantially changed in IPv6. If
IPsec were ever used in a more comprehensive way in the IPv6 protocol (including device bootstrap), authentication for devices could mitigate this attack somewhat. The 802.1x standard also has the potential to help here, though an undetected rogue device could funnel 802.1x authentication sequences to a compromised node acting as a AAA server while capturing valid credentials.

**Man-in-the-Middle Attacks**

Because the IPv4 and IPv6 headers have no security mechanisms themselves, each protocol relies on the IPsec protocol suite for security. In this fashion IPv6 falls prey to the same security risks posed by a man in the middle attacking the IPsec protocol suite, specifically IKE. Tools that can attack an IKE aggressive mode negotiation and derive a preshared key are documented. With this in mind, we recommend using IKE main mode negotiations when requiring the use of preshared keys. IKEv2 is expected to address this issue in the future.

**Flooding**

Though certainly the increase in IP addresses that can be spoofed may make flooding attacks more difficult to trace, the core principles of a flooding attack remain the same in IPv6. Whether a local or a distributed DoS attack, flooding a network device or host with more traffic than it is able to process or more than the link can transmit is an easy way to take a resource out of service.

V. PERFORMANCE FACTORS

In this section the various performance issues such as the address field, space, the throughput, the security issues, the jitter value, threats in IPv6 etc. are placed.

**Address Space**

Comparing the IPv4 the IPv6 has better address space that is 128 bits for the location of the systems. Moreover the address bit structure is more simplified in the version 6 of IP. It also uses the Flow level field which is new in IPv6 that provides the series of the packet while data transmission. Thus, comparing with the IPv4 address space which is 32 bit the IPv6 provides much better service for the users.

**Throughput**

The throughput for both the protocols is provided by measuring its packet size in bytes. Both shows the same throughput levels since the throughput increases as the size of the packets increase. While comparing the case of the connectionless service, IPv4 provided the high throughput when number of packets increased.

**Security Issues**

Comparing the IPv4, the IPv6 offers greater address space with fewer intermediary proxies, plug and play services. The IPv4 is purely based on the local host connections. Moreover the scalability for IPv4 is less when comparing the IPv6. The IPv6 holds the end to end connection on the network. Hence it provides the connection oriented services that offer the higher security to the data on the transmission link. Since IPv6 provides the end to end network connection most of the video application like VOIP are ease with it. IPv6 has built-in Auto-configuration mechanisms that allow clients to communicate with one another without any human intervention. Because IPv6 mandates the inclusion of IP Security (IPsec), it has often been stated that IPv6 is more secure than IPv4

**Jitter Value**

IPv6 addresses can be automatically derived from IPv4 addresses, IPv6 tunnels can be built on IPv4 networks, and at least in the initial phase, all IPv6 nodes will follow the dual stack approach, that is, they will support both IPv4 and IPv6 at the same time. Jitter values, the variation in time between packets arriving at the destination are calculated for both the protocols. It shows that the IPv6 holds better space for transmission with lower jitter values since it holds the connection oriented services.

VI. SHORTCOMING AND THREATS OF IPV4

**Shortcomings**

1. With its 32-bit addresses, IPv4 currently allows for approximately 4 billion IP addresses. Although, during the time of its Creation IPv4 seemed to have enough addresses, the exponential growth of Internet has pressed for more addresses.

2. The Internet has grown with the addition of more and more networks and sub-networks. Routers, which route data through these networks must store up-to-date information of all these sub-networks. The IP addresses, which are stored in routing tables had to be divided into various classes to accommodate every sub-network. Hence the size of the routing tables has grown along with the Internet and now this poses a problem of decreasing the performance of the Internet. Schemes like sub-netting and CIDR that are currently being employed for IPv4 addresses are proving to be insufficient.

3. Security is a very important factor in the globally connected Internet. IPv4 does not provide any security mechanism such as the authentication of the packet sender or the encryption of the packets before delivery.

4. IPv4 does not have any feature to know the kind of data transmitted. This knowledge can be crucial especially when
we are dealing with real-time or multimedia data that should be treated as high priority data.

5. Another problem with an IPv4 network is of ‘lost packets’ within a network. The TTL (Time to Live) field in the IP header sets the life span of a datagram. If the datagram is unable to reach the destination within this time, it will expire. The computer on the receiving side simply requests the datagram be resent. This process can become time consuming and cause problems especially if we are dealing with real-time data.

6. During the process of broadcasting, IPv4 sends a packet to every address on the network. Although this has some uses, routers and other network resources tend to become overloaded from this. This insecure process also can cause network congestion and excessive collisions.

Threats in IPv6

The following nine attacks have substantial differences when moved to an IPv6 world. In some cases the attacks are easier, in some cases more difficult.

• Reconnaissance
• Unauthorized access
• Header manipulation and fragmentation
• Layer 3 and Layer 4 spoofing
• Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) attacks
• Broadcast amplification attacks (smurf)
• Routing attacks
• Viruses and worms
• Transition, translation, and tunneling mechanisms.

VII. CONCLUSION

In this research performance of two IP versions have been empirically discussed. The following specific conclusions can be drawn as follows:

• For packet sizes larger, IPv4 always gives a slightly better throughput than IPv6. However for small packet sizes the performance is almost identical.
• The average jitter value is lower for the IPv6 protocol since it uses the connection oriented service and also employs the Plug and play connections on the network. It also selects the network dynamically.
• The address space is larger for the IPv6 that improves the scalability for the users to locate the nodes on the network.

REFERENCES