International Conference on Green Energy and Environmental Engineering(GEEE-2017)
International Journal of Computer Science, Communication & Information Technology - CSCIT
Vol.4 pp.10-14

Security Threats of Migration From IPv4 to IPv6

Aisha Ali Elzegr
The higher Institute of Technology and Science, Computer Science department
Elkoms-Libya
elzegra@uni.coventry.ac.uk

Amer R. Zerek
Zawia University. Faculty of Engineering, Electrical and Electronic department
Zawia- Libya
anas_az94@yahoo.co.uk

Abstract— Migration from Internet Protocol version 4(IPv4) to Internet Protocol version6 (IPv6) has become an arrogant need because of the growth of the internet network and increase the demand on more and more address spaces, but this migration has brought new security issues and led to complicate existing security issues whether in IPv6 or in the defending technologies such as Internet Protocol Security (IPsec), Intrusion Detection System (IDS) and Firewalls. This paper deals with some security threats facing IPv6 and (IPsec), (IDS) and firewalls some of these threats are existing in IPv4 but changed its behavior in IPv6 and some of it arise with IPv6, also this paper suggests solutions to mitigate these threats.

Keywords — security, migration, IPv4, IPv6, firewall, IPsec, TCP and IDS

I. INTRODUCATION

IPv4 was conceived in the middle of 1970s, and shortly thereafter in 1981 its functionality was defined by the Internet Engineering Task Force (IETF) [1]. IPv4 was the first Internet Protocol to be globally deployed; it uses 32 bit address space, which allows for about 4,294,967,296 unique addresses [2]. This huge number of addresses space supposed to be used for quite a long time. However, as the internet has grown hugely which has increased the demand on more and more address space, that resulted serious lack of available address space, where in 1992 this shortage of addresses space was classified as a serious issue may will lead to inability of IPv4 to keep up with the growth of the internet [3].

II. ALTERNATIVE TECNOLOGY IPv 6

In 1994 IETF introduced a new version of the internet protocol, the internet protocol version 6 (IPv6), also called IPng, to overcome many issues that the current internet protocol IPv4 suffer of [2]. The new generation IPv6 and before talking about its features, it must be underline that IPng is not in fact superset of the existing version IPv4; IPv6 is a completely new protocols suite [4]. IPv4 inability to handle increase the requirements of internet network, also the depletion of allocated addresses have made the migration to new Internet protocol inevitable. Some of the main distinguishing attributes of IPv6, that make this version a suitable alternative are auto configuration and the capability of expand addresses, support for extensions and more options, header simplification format and flow label which provide high speed and enhance monitoring, also united framework which support end-to-end security principle for the network[5].

III. PROBLEM DOMAIN

Since the migration from IPv4 to IPv6 has become fact and reality pension the security threats will be part of this migration, some of these threats linked to IPv6 features and some linked to the defense techniques that used to protect IPv4 and IPv6 networks such as firewalls, (IPsec) and IDS.
This paper provides an analysis of these security problems that came up with IPv6 and faced the defense techniques (firewalls, IPsec and IDS) in order to give solutions that could mitigate the harm of these threats.
These IPv6 security threats are described in the following points

A. Reconnaissance attack:

In this type of attacks adversary seeks to learn about the target network as much as possible. This attack has two methods use to collect information about the target network, firstly an active network in this type scanning is the way of collecting information, secondly passive data mining, and that happens through general documents or search engine. The information that attacker seeking to know are about network devises and hosts and how they communicate, based on these information, the mean of attack will be chosen. [7]. In IPv4 network, methods such as ping sweeps, application scan and port scan are mostly used to gather information about the target network, ping sweeps also called Internet Control Message Protocol(ICMP) is 'technique used to determine which of a range of IP addresses map to live hosts' immersion network of the victim with layer 4 ping messages or ICMP that requires a response, based on these data, an attacker formulates hypothesis about the target network. The next step after understanding the target network is port scan that helps hacker spying particular services on port that might be possibly vulnerable [5].The following is the condition of this attack in IPv4, and how it deals with IPv6.

- Reconnaissance attack in IPv4:

In IPv4 networks, port scanning is a relative simple task as most IPv4 segments are Class C, with 8 bits allocated

for host addressing. Scanning a typical IPv4 subnet, at a rate of one host per second, translates into:

$2^8\ hosts\ * \frac{1sec}{1host} * \frac{1min}{60se} =\ 4.267\ minutes$ [8].

- Reconnaissance attack in IPv6:

The subnets size of IPv6 is a very huge compared with the subnets size of IPv4, where the size of first one is 64 bits and the second one is 8 bits, this increase in the subnets size in IPv6 makes this attack a very difficult to launch, IPv6 uses for subnet addressing 64 bits and for host addressing 64 bits. Therefore a subnet of IPv6 requires $2^{64}\ hosts * \frac{1sec}{1host} * \frac{1year}{31,536,000sec} =$ $584{,}942{,}417{,}355\ years\ to\ be\ scaned$[8], scanning a large address space such this, is nearly impossible, difficulty lies in the way of collecting information such as ping sweep or port scan, are become more difficult to achieve in any IPv6 network. However, in IPv6 network to determine victim system there are another ways for that. the adversary may discover that an administrator of network uses scheme sequentially numbering for assigning IP addresses to the hosts, therefore, determine host to scan it becomes easier [7]. Also, another opportunity for attackers to scan a system is that, the structure of IPv6 multicast addresses helps an adversary identify set of main components of this network, such as routers and DHCP servers, thereby attackers can scan the vulnerabilities of these components. Regardless of these differences that mentioned above, the techniques of reconnaissance attack is the same in both IPv6 and IPv4. moreover, IPv6 network is more depending on (Internet Control Message Protocol Version 6) (ICMPv6 is a protocol used for different activities such as Neighbor Discovery (ND) process, diagnostic for activities, error reporting during packets processing to function duly) [9]. There are other software methods facilitate launching the Reconnaissance attack in IPv6 such as (Network Mapper) NMAP. [10]

In IPv6 this attack is difficult but not impossible, and to protect a network from this attack some recommendation are proposed:

The main identifier devices in a network better not to be sequential. In terms of security, the router should not list on the network to be the first host. Node ID's randomization can make subnet scanning more difficult. For the end hosts the private address feature is supported by the majority of new operating systems. Both private addressing and node ID's randomization can keep random allocation for the hosts and equally distributed via the subnet. Using IPsec service can decrease packets sniffing.

B. Fragmentation attack:

This attack uses fragmentation as mean to avoid security devices of a network, such as Network Intrusion Detection System (NIDS) or stateful firewall [8] . The other use of this attack is to attack the infrastructure of the network directly. (NIDS is a system for intrusion detection which attempts to detect any access that unauthorized to the computer network by analyzing traffic of the network in order to discover any malicious activities)[11].

- Fragmentation attack in IPv4

Fragmentation in IPv4 is mechanism used for fitting the datagram of IPv4 into smallest (Maximum Transmission Unit) MTU on the path among end hosts [7]. (MTU used by TCP to specified the biggest size of every packet in all transmission process) [12], fragmentation as well uses to obfuscate attack to avoid NIDS or any other product for security monitoring. However, the majority of modern firewalls and NIDS devices have the ability to do reassembly of packets after that match them to signatures of attack which limit the effectiveness of this attack.

- Fragmentation attack in IPv6

The specification in IPv6 protocol, the use of intermediate nodes for packets fragmentation is not acceptable [13]. Because in the network of IPv6, the use of MTU is an obligation, in addition packets fragmentation is allowed only in the source nodes or end node. IPv6 similar to its predecessor IPv4, the current firewall and other security devices that used with IPv6 implement fragments reassembly; for the purpose of mitigate the fragmentation attacks [8].

Controlling this attack can be achieved by: packets fragmentation is allow at the source nodes only, because the networks of IPv6 use the discovery method MTU (based on Internet Control Message Protocol version 6, ICMPv6) as an obligation condition [14]. MTU maximum transmission unit, is the largest size of unfragmented packet which can cross from node to node [15]. ICMPv6 is an basic component of IPv6, the nodes of IPv6 use ICMPv6 (Internet Control Message Protocol version 6) in reporting errors that faced it in packets processing, and perform other functions to the Internet layer, such as diagnosis (ping tool), IPv6 nodes have to implement all messages under this specification [16]. The minimal size of MTU for IPv6 network is 1280 octets. All fragments that less than the 1280 octets is recommended to be discarded unless a packet was the last one in the data flow, and this is for security purposes. The usage of fragmentation an attacker can get numbers of port that are not exist in the first fragment, in this case intruder can avoid the security devices monitoring expecting to get data of the transport layer protocol in this fragment condition[14]. The intruder can cause an overload from this big number of fragments, this overload of fragments, will make the targeted systems crash. The solution for this issue is by limiting fragments number and its arrival, also when possible, deny IPv6 fragments that are destined to an internetworking device, and ensure adequate IPv6 fragmentation filtering capabilities.

C. Routing attack:

This kind of attack focuses on redirect or disrupts traffic flow in the victim network. There are many ways to accomplish this attack, such as rapid announcements, remove routes, bogus announcements of routes, and flooding attack, Particulars of these attacks differ, according to the protocol that used [8]. Also in IPv6, the routers can use (ND) protocol in order to determine its link layer address and prefix information for each other. However, in this case malicious nodes can impersonate the default gateway of a network segment, and a receiving nodes do not validate Router

Advertisements (RA). Therefore, this nodes that received a fake router advertisements will communicate based on this advertisement and that will lead to block the victim to get to the right network [17].

- Routing attack in IPv4:
  The currently, authentication cryptographic is used to protect routing protocols in order to protect routing announcements via the network, which is Message Digest Algorithm 5 (MD5)authentication, is the most popular implementation to verify integrity of data [18].
- Routing attack in IPv6:
  This mechanism of protection that used in IPv4 will remain without any change with IPv6 networks [8]. Also the security mechanism of some protocols will not change during the transition process from IPv4 to IPv6 [18]. Border Gateway Protocol (BGP) where it is extended / updated in order to carry the routing information of IPv6, where BGP still depend on MD5 TCP for authentication [19].
  In IPv6, routers are used ND to know each other's existence and determine the prefix information and the addresses of their link layer [17]. However, this case can also let node of the malicious to impersonate the default gateway of a network segment [8]. Receiving nodes do not validate RA router advertisements. Therefore, all nodes that receive a fake router advertisement will update their communications parameters based on this RA without cautious. The nodes of the malicious can spread bogus / fake address prefix information in order to reroute legal traffic to block the victim from reaching its destination. This problem can be avoided by configure nodes in way does not accept all (AR) messages. Instead nodes should be accepting messages from routers already listed only. Also Dynamic Host Configuration Protocol version 6 can be used to distribute the needful addresses prefix information [17]. Furthermore nodes use (DHCPv6) to obtain information of configuration; such as DNS addresses [20].devices authentication can help to mitigate this kind of attack.

D. DHCP and ARP Attacks

Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) attacks try to subvert initialization process of the host or device which used as access transit point for the host. Generally this involves subversion bootstrap conversations of host either by spoofed communication or rogue devices. This kind of attack attempts to get the end host to make communication with rogue devices or to configure communication with DNS server, default gateway [7].

- DHCP and ARP Attacks in IPv4:
  DHCP server exploits a broadcast messages that comes from a client, which will allow to a fake DHCP to answer to the host in time before any valid DHCP be able to respond. This will allow the rogue device (DHCP) to put critical communication settings, such as DNS server, default gateway, thus enable other kinds of attacks. In addition there is possibility to DHCP server messages to be spoofed, which will enable an attackers to consume every DHCP available messages [8]. Likewise in IPv4 some technologies are developed to address and deal with some types of these attacks such as DHCP and RAP [7].
- DHCP and ARP Attacks in IPv6:
  In IPv6 there is no added security attribute that can be equivalent to ARP and DHCP. Since stateless auto configuration possible to be able to provide suitable replacement to DHCP in several cases, the servers of DHCP do not have common use in IPv6 network and are not widely available in the modern servers' operating systems [8]. ND protocol is the alternative to ARP in IPv6 networks, a L2 addresses are not binding statically to a Layer 3 IP address. Also, the Layer 3 of IPv6 address and it's locally ID interface can be used at global level of IPv6 network. Therefore, all security issues that related to the ARP not exist in IPv6 network [21].
  Rogue device is unauthorized device introduced to the network, this device can be laptop, DHPC, DNS, switch, route or any wireless access points. This kind of attack is fairly popular in the networks of IPv4 and its behavior remains the same in IPv6 networks. In the IPv6 networks the use of IPsec in a comprehensive way and by use devices authentication can mitigate or avoid this kind of attack to somewhat. Also the stander of 802.1x can help to avoid this attack [14]. 802.1x is a standard from IEEE, was created for Port based Network Access Control (PNAC) in order to enhance security. It supplies authentication technique to any device wants to link to WLAN or LAN [22].

E. Broadcasts amplification attack (Smurf):

Broadcast amplification attack, commonly known as (Smurf) attack, is tool for Denial-of-Service (DoS) attacks which exploits the ability of sending echo-request messages with the address of the destination sub network broadcast, and source address (spoofed), this attacker uses the IP of its victim, therefore, every end host on the sub network will respond to this spoofed address, thus the victim will be flooded with echo replay messages [23].

- Smurf attack in IPv4:
  In IPv4 network this kind of attack has a mitigation way. if directed broadcasts of IPv4 is disabled on the router, and when an attacker sends echo - request messages to the IP broadcast address of the subnet, they will reply on their victim by one echo-message, contrary to all the responses that came from network devices, this attack has become less spread, but it still can be used, and this attack still under observation [7].
- Smurf attack IPv6:
  In IPv6 network it is impossible to find the broadcasts address, which means every amplification attack, such as smurf, DoS, can be stopped [13]. The specifications of IPv6 prevented the ICMPv6 packets generated in response to the messages to the IPv6 multi-destination address. And adoption new standards should add more improvements. (ICMPv6) is the Internet Control Message Protocol used for the Internet Protocol version 6 or (IPv6) [22].

Some common operating systems do not respond to request that come from a spoofed address which directed towards the link of local multicast address. Some disputes still exist about whether should the end nodes reply to the messages of ICMP that come from global multicast addresses [7]. Filtering IPv6

address multicast source packets is recommended, also at the network border a multicast source packets should be reduced.

F. Headers Extension .

The information of transport layer of TCP packet or User Datagram Protocol (UDP) packet are specified in IPv6 by extension headers (RFC2460). In the header of IPv6, the header field next to extension headers are used to indicate the extension headers and to extend the protocol functionality. Extension headers can pose very serious threats to a network. IPv6 packet can contains huge number of the extension headers that linked in a large list that lead to DoS of middle systems over the transport path or destination systems. where these list that based on extension headers is a way to evade intrusion detection systems and firewalls. these chain list could break payload to another fragmented packet which can not be checked by firewalls that are looking only for initial fragment. In this way extension headers can become manipulation tool, that lead to prevent services to the target host or the hosts stack can be crashed [23].

These attacks can be avoided by filtering on the extension headers or by very sensitive firewalls rules for headers scanning controlling all extension headers types can be done by many options that available in the Internet Operating Systems IOS and Access Control List (ACL IPv6). Also parsing the complete extension headers chain in the network routers and middle boxes which receive the packets with extension headers.

IV. FIREWALLS, IP SECURITY AND INTRUSION DETECTION SYSTEM FROM IPv4 TO IPv6

: This section will discusses number of techniques that are used to provide high level of security for networks of both protocols 4 and 6, also this part is to show the relationship between these technologies and IPv4 and IPv6 what has been changed in these technologies form v4 to v6, Are both versions supporting these technologies the same strength? and what has to be taken into account to improve the relation between these mechanisms and both protocols. These techniques are as following:

- Internet Protocol Security (IPsec):

IPsec is an open standard framework was developed by the Internet Engineering Task Force IETF, IPsec is to secure the communication of the internet protocol by encrypting and authenticating every IP packet during communication sessions [5] IPsec was created to provide more security to the IP. In IPv4 network IPsec is an optional attribute, therefore, the functionality of IPsec in IPv4 is limited, on the other hand in IPv6 IPsec is a mandatory attribute, since security was taken into account from beginning in IPv6 design[9]. Also IPsec uses to protect data flow among two hosts which means (host to host), two security gateways (network to network), or among host and security gateway (network to a host) [8].

The relation among IPsec and both protocols IPv4 and IPv6 is that, IPv6 originally supports the IPsec while IPv4 does not support it. IPsec was created in integration with IPv6 as well was natively required in every standard and implementation of IPv6 [5]. However, RFC 6434 advised to use the term should use IPsec in IPv6 instead of must [9].The reason might be because of requirements of computing of encryption processes in IPsec, because not all devices have enough capabilities, for instance, household appliance, printer, and smartphones. As a result, migration into IPv6 with the usage of IPsec will be applicable solution for many kind of threats. However, this is cannot prevent the transmissions of unencrypted packets in the perspective future [8].

Despite all of that IPv6 and IPsec may have a stronger relationship than IPv4, but IPv4 can also use IPsec. In addition, the implementations of IPv6 IPsec today are less ubiquitous than IPv4. However, IPsec usage is not original attribute in IPv4. IPv4 is considered less secure than IPv6 because the design of IPv6 is supported natively IPsec approach. This is opinion can be true or not, because not all communications of IPv6 would obtain IPsec, the reason is the scalability problems and operating expenses. IPsec attribute can be used by IPv4 but would not be native feature in IPv4.

- Intrusion Detection System IDS

Intrusion detection is a kind of system for security management for networks and devices. IDS inspects every outbound or inbound network activities and specifies patterns which might indicate a system or network detects threat from adversary attempting to breach or break into a system. Definitely, the old version of the IP (IPv4) will be replaced by the new generation IPv6. Despite IPv6 security attribute is better than IPv4, some security problems are still exist in IPv6. So the importance of IDS for the IPv6 network appear to a critical issues [12]. Also, security mechanisms such as IDS have more support for IPv4 protocol than for IPv6 where v6 less supportive either in performance or in features[10].

Misuse detection and anomaly detection are the main techniques of IDS. The technique of anomaly detection uses measure the distance among the dubious activities and the norm based upon chosen threshold as way of determining abnormality. The technique of misuse detection looks for the signature of malicious pattern based on some rules or signatures for detecting intrusive behaviour. The major difference among technologies of IDS is that, the anomaly system can detect any new attack but it has high false alerts rate. Whereas, the misuse model has low false alerts rate but it cannot detect new attacks [7]. The IDS with the IPv6 support ought to take into account a few facts that the IPv6 protocol has brought, for instant the IPv6 extension headers. The IDS must implement a suitable support to all kinds of extension headers of IPv6 [6].

IPv4 protocol will be replaced by IPv6 protocol. Over time the protocol of IPv6 becomes increasingly accepted and usable everywhere globally. Definitely, IPv6 carries huge improvement compared to the existing version 4. IPv6 improves overall attributes and particular security attributes in modern IP networks. IPv6 brings lots of flexibility that decreases the security issues. However despite of all these improvements, a number of possible security threats are still exist and need considerations. many vulnerabilities and possibilities of misuse that known in the IPv4 network persist, in addition, emerged number of new security problems the specific for IPv6 [10].

- Firewalls

Firewalls are gateway to a secure Internet use to link the Internet to private networks [12]. Firewall mechanism represents one of the most significant security techniques, where they work as a filter to filter network traffic which enters the network or leaves it, the location of the firewalls can be between the Internet and a Local Aria Network (LAN) or a (LAN) and other network, or between segments of a (LAN), or even on each host inside a LAN. All packets are being

analysed and the results will be compared with the pre-defined suite of rules these packets might be accepted or discarded, or may will be sent to extra check point. Also protection that provided by firewalls are even more significant to a site is using the IPv6 since the functionality of Network address translation (NAT) is not offered by IPv6[9]. Therefore, firewalls are the only method that can protect the network of IPv6.

In addition, the rules of IPv4 firewall and the rules of IPv6 firewall are totally independent. Also packets of IPv4 do not inspect by rules put for IPv6, and the rules of IPv6 do not inspect by the rules put for IPv4. And packets of IPv6 are not checked by the rules' table of any other version of IPs, packets of IPv6 are inspected only by rules of IPv6 filter table, similarly the packets of IPv4 are inspected only by the rules of IPv4 filter table. In addition mobile IPv6 which is one of the main features, is not supported by most available firewalls for networks of IPv6[17]. Since firewalls are deployed in the majority of networks presently that can affect the deployment process of IPv6 protocol. Solving this issu can be done by The rules of filtering must be specified separately for the traffic of IPv6 and IPv4, which means firewalls of IPv6 network must support IPv6 [15]. Also The huge size of the extension headers has created many problems when firewalls started to deal with it which result to many implications for systems such as firewalls, for instance:

- A firewall might needs to analyze multiple extension headers to perform complete packet inspection Deep packet inspection (DPI), that could leads to decline in the performance of the WAN, firewall circumvention, or denial of service (DoS).
- Together fragmentation and extension headers could stop deep packet check.

firewall circumvention methods that use fragmentation can be alleviated by requiring in any IPv6 datagram, the first fragment must include the full packet headers that needed to apply a packet filtering policy.

V. CONCLUSION

Packet filtering can mitegate variouse attaces and as knowing firewalls are the must seqnificant tool for packet filtering then they should support IPv6 from difrent aspects such as IPv6 header chain and IPv6 transition technologies, so that can result in the same security polcices can be appled on both native or transition IPv6 traffic. Also defult denay policy should implimented in firewalls in order to prevent unwanted traffic. Also Impose restrictions on the maximum number of the extension headers depending on the firewall to control attacks that leverage the multiple extension headers.

Effective solutions to these security problems will definitely contribute to encourage for wide acceptance and thus usage of this protocol IPv6. it is importance to take all possible ways for provide the highest level of security. The mandate existing of IPsec in IPv6, and the flexibility of the extension headers options in IPv6. Practically all that can help, but cannot solve all security issues. However IPv6 has better security features such as the usage of encrypted communications and bigger address space, despite new security problems brought on by v6. To improve the protection in the network of IPv6 the recommendations are to use Firewalls as packet filter security mechanism and IDS intrusion detection. Also services that unneeded should be undergoing in filtering point (firewall). Nonetheless, security of the IPv6 networks and IPv6 protocol can be improved, all issues that IPv6 protocol and network suffer of it should not become an obstacle in the way of acceptance and usage of IPv6, and more development to it.

REFERENCES

[1]. D, Minoli. and J, Kouns. “Security in an IPv6 Environment”. Boca Raton: Auerbach 2009

[2]. A, Nizar “Comparison Study between IPV4 & IPV6”. International Journal of Computing Science Issues 9 (3), 314–317, May 2012.

[3]. S. Dutta, P.K. Mishra, G.M. Prasad, S. Shukla and S.K. Chaulya, “Internet Protocol: IPv4 Vis IPv6”. Asian Journal of Information Technology 11 (3), 100-101, 2012

[4]. R. Sankaran “Migration of IPv6-Security Issues”. International Journal of Computing Trends and Tecnology 4 (4), 567–572, 2013.

[5]. W. Azka, J. Parvez, “A Study of the Challenges and Security Aspects of Migration from Ipv4 to Ipv6”. International Journal of Advanced Research in Computer Science 4 (9), 1-92, 2013.

[6].V. Daniel. IPv6 Security: Transition from IPv4 to IPv6. Enschede: University of Twente, 2011.

[7]. V. Sharma, “IPv6 and IPv4 Security Challenge Analysis and Best- Practice Scenario”. Int. J. of Advanced of Networking and Applications 01 (04), 258–269, 2010.

[8]. S. Convery, D. Miller. “IPv6 and IPv4 Threat Comparison and Best- Practice Evaluation”. Cisco Systems 1, 1–43, 2004.

[9]. B. Dawadi, S. Ram, and A. Khanal, "Service Provider IPv4 to IPv6 Network Migration Strategies." Journal of Emerging Trends in Computing and Information Sciences 6.10, 2015.

[10]. P, Ciprian. Deploying ipv6 networks. Pearson Education India, 2006.

[11] S. Rubin, S. Jha, and B. P. Miller, "Automatic generation and analysis of NIDS attacks." Computer Security Applications Conference, 2004. 20th Annual. IEEE, 2004.

[12]. D. Murray, T. Kozinice, and K. Lee, "Large MTUs and internet performance." High Performance Switching and Routing (HPSR) 13th International Conference on. IEEE, 2012.

[13] D. Žagar, K. Grgić, and S. Rimac-Drlje,”Security Aspects in IPv6 Networks – Implementation and Testing”. Computers & Electrical Engineering 33 (5-6), 425–437, 2007.

[14] E. Durdağı, A. Buldu “IPV4/IPV6 Security and Threat Comparisons”. Procedia - Social and Behavioral Sciences 2 (2), pp. 5285–5291, 2010.

[15]. X. Liu, X. Li, “Packet Fragmentation in IPv6 over IPv4 Tunnels”, 2004.

[16]. A. Conta, S. Deering, and M. Gupta, ‘Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification’. The Internet Socity RFC 4443, 1–24, 2006.

[17]. C. Caicedo, J. Joshi, and S.Tuladhar, “IPv6 Security Challenges”. The IEEE Computer Society 42 (2), 1–42, 2009.

[18]. E. Lucia, (2013) IPv6 Security Overview: A Small View of the Future http://resources.infosecinstitute.com/ipv6-security-overview-a-small-view-of-the-future/ [29 October 2014]

[19]. M. Sameeha, “Look at IPV6 Security Advantages over IPV4”. The International Institute for Science, 2 (4), 32–38, 2012.

[20]. R. Droms, “Statless Dynamic Host Configuration Protocol (DHCP) Service for IPv6”. The Internet Society 1–9 , 2004.

[21]. S. Brun, “Workhorse 802.1x Standard Authenticates Network Connections”. Texas Instruments 1–5, 2008.

[22]. J. latief, J. Parvez,” Security Issues in Next Generation IP and Migration Networks” Volume 17, Issue 1, Ver. III (Jan – Feb. 2015), PP 13-18, 2015.

[23]. D. Žagar, K. Grgic, “IPv6 Secrity Threats and Possible Solutions”. IEEE 1 – 7, 2006.

ISSN 2356-5608