The security issues of IPv6 routing protocol-A study

Ramneet kaur[1] , Dr. Sandeep sharma[2]
Department of computer science and engineering
Guru Nanak Dev University
Amritsar, India

ABSTRACT---IPv4, the current version of the Internet Protocol deployed worldwide, has proven remarkably robust, easy to implement, and interoperable with a wide range of protocols and applications. Though substantially unchanged since it was first specified in the early 1980s, IPv4 has supported the scaling of the Internet to its current global proportions. However, the ongoing explosive growth of the Internet and Internet services has exposed deficiencies in IPv4 at the Internet's current scale and complexity. IPv6 was developed specifically to address these deficiencies, enabling further Internet growth and development ,but IPv6 is also prone to routing attacks such as wormhole attack, delay attack etc.

***Keywords:* IPv6, Routing attacks, OSPFv3, Wormhole attack, Link spoofing attack**

1. INTRODUCTION

Network security is a primary issue of today's research and it consists of policies and provisions that are adopted in order to prevent or monitor unauthorized access to a data in a network. The authentication of network security is possible in three ways:

a. **One factor authentication**: A method that consists of using authentication on the basis of username and the passwords.
b. **Two factor authentication**: When a user has something such as Signed digital certificate, swipe card etc. to authenticate itself.
c. **Three factor authentication**: When user itself is used for authentication such as finger print and retina scan.

Network security can be achieved through hardware and software. The software is required to be constantly updated and managed to protect from various threats. In computer networks an **attack** is any attempt to destroy, alter, disable, steal or gain unauthorized access to or make unauthorized use of a resource.

Network security model is a seven layer model .According to Joshua; NSM divides the task of securing the network into seven sections . The importance of this model lies in the fact that unity is needed among all the layers in securing the network. The roles of various layers are:

PHYSICAL
VLAN
ACL
SOFTWARE
USER
ADMINISTRATIVE
IT DEPARTMEMTAL

Fig1.seven layer model

a. Physical layer: The main focus of this layer is to provide physical security .physical security has many forms such as alarms, cameras etc.
b. VLAN layer: VLANs implement access control lists that prevent an access from the user that do not need to access it.
c. ACL layer: Access control lists are created on this layer, and are used to allow or deny access to the users.
d. SOFTWARE layer: This layer keeps software up to date in order to lessen the software threats.
e. USER layer: This layer gives stress upon user's knowledge about security on the network.
f. ADMINISTRATIVE layer: This layer stresses upon the training and knowledge of all the members of the management.
g. IT DEPARTMEMTAL layer: This includes administrative layer plus it department has full access to any device in the network.

2. IPv6 Protocol

The new IPv6 that has been proposed to overcome the shortcomings of ipv4 has following specifications that are different from IPv4[1]:

2.1 IPv6 Header structure

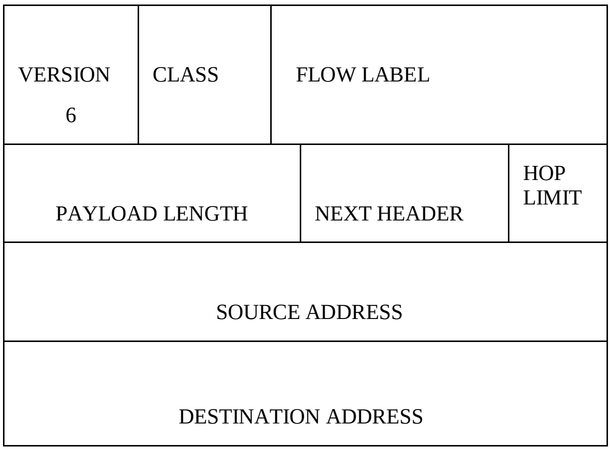


Fig2.IPv6 Header Structure

a. 128 bit address space is used in IPv6 whereas IPv4 had 32 bit address space
b. The IPv6 sender and receiver hosts perform packet fragmentation and reassembly. IPv6 routers do not perform this job.
c. A new stateless address auto configuration capability is introduced that automatically configure ipv6 addresses on new nodes.
d. The use of internet control message protocol is required and is compulsory, versus its optional use in IPv4.
e. According to specification of ipv6, the following six extension headers are also included: hop by hop options header, destination option header, fragmentation header, authentication header, encapsulating security payload header.

These changes give rise to strong vulnerabilities which are summarized below:

A. **Hop by hop options :**The header can have multiple hop by hop options, an attacker can use invalid option which can lead to issuing of " parameter problem" message to the sender .An attacker sends falsely crafted packets to the router ,burdens the router that leads to the dos attack . There is one more vulnerability that is related to some options in a hop-by-hop options header. The header uses Pad1 and pad n options. The requirement is this that these padding bytes must be zero filled. However the verification of the right implementation of this is not required. The hop-by-hop options headers options may act as a covert communication channel. This can be resulted via non zero filled padding bytes .we can use certain pattern for the padding and the other options. Such a pattern may lead to the communication of covert channel information. For example, we can use multiple Pad1's instead of a single pad n , or we can use a pad n followed by a Pad1 and this may communicate information.

B. **Stateless address configuration (slaac)**:slaac raises serious security issues. One of the issues about slaac is its trust model with respect to network trusting a node that auto configures itself on IPv6. A new auto configured node is allowed an unchecked access is allowed to the link. This unchecked access makes a node to acquire global prefix by advertising ICMPv6 messages for neighbor discovery. With this a node can construct globally routable address and uses it without approval or any kind of permission.

C. **Multiple addresses**: The assignment of multiple addresses to an interface challenges the filtering rules in access control lists and firewalls. In such cases there is need for the firewall to learn all the addresses dynamically and filtering rules will need to be automatically generatable .IPv6 lacks in such capabilities. Therefore simpler methods must be used that use some kind of identification tokens in place of addresses in order to identify a host or an interface. Such identification mechanism is not currently defined at OSI layer 3.

D. **ICMPV6 filtering**: The use of ICMPv4 messages in IPv4 is not compulsory, it's optional. Normal network operation does not require it. Blocking of all ICMPv4 messages is done by many IPv4 network security administrators. This kind of blocking is not possible for IPv6 networks because basic the use of ICMP messages are compulsory in ipv6.so an attacker can modify ICMPV6 packets to cause an error response.

E. **IPV6 tunneling**: Tunneling techniques are classified according to the mechanism by which the address of the node at the end of the tunnel is determined by the encapsulating node. In the method of router-to-router or host-to-router, the **IPv6** packet is tunneled to a router. In host-to-host or router-to-host methods, the **IPv6** packet is tunneled all the way to its final node or we can say the final destination. This specification of tunneling ipv6 via ipv4 has raised some security issues. All 6 to 4 capable routers regard other 6 to 4 routers and relays as being “on link”. The trust between 6 to 4 routers and relays lead to an attack that can be forwarded to 6 to 4 networks, IPv6 networks or IPv4 networks.

3. IPv6 Routing

For IPv6-based networks, IPv6 routing provides transmission capabilities between host’s .These hosts are located on different segments within a large IPv6-based network. IPv6 network segments, which contain links or subnets, are connected by IPv6 routers. These devices pass IPv6 packets from one network segment to another. This process is called IPv6 routing and is shown below

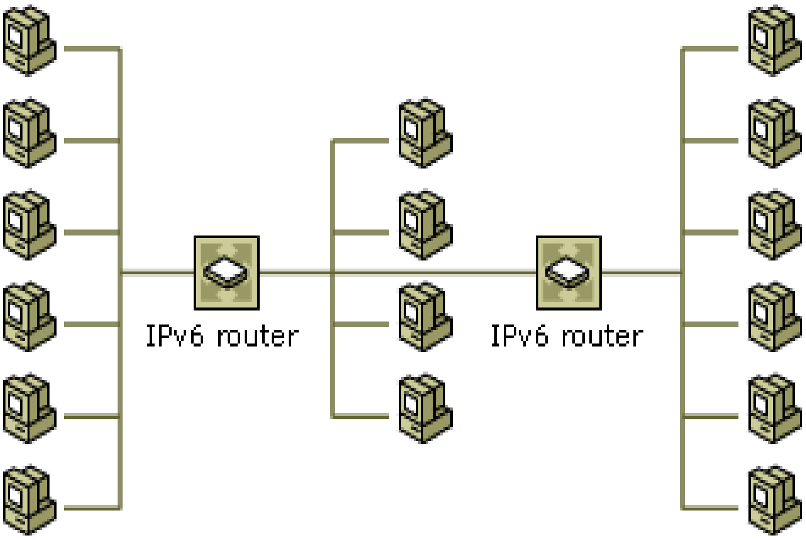


Fig.4 IPv6 Routing

These routers are multihomed hosts means a network host that requires two or more network interfaces to connect to each separated network segment.

3.1 IPv6 Routing Protocols

The routing protocols used in the ipv6 is same as used in ipv4,but some slight modifications have been made according to the requirement of ipv6.Ipv6 uses following routing types:

a. **RIPng (routing information protocol next generation):** RIPng is an extension of RIPv2 for support of IPv6.. The major differences between RIPv2 and RIPng are:

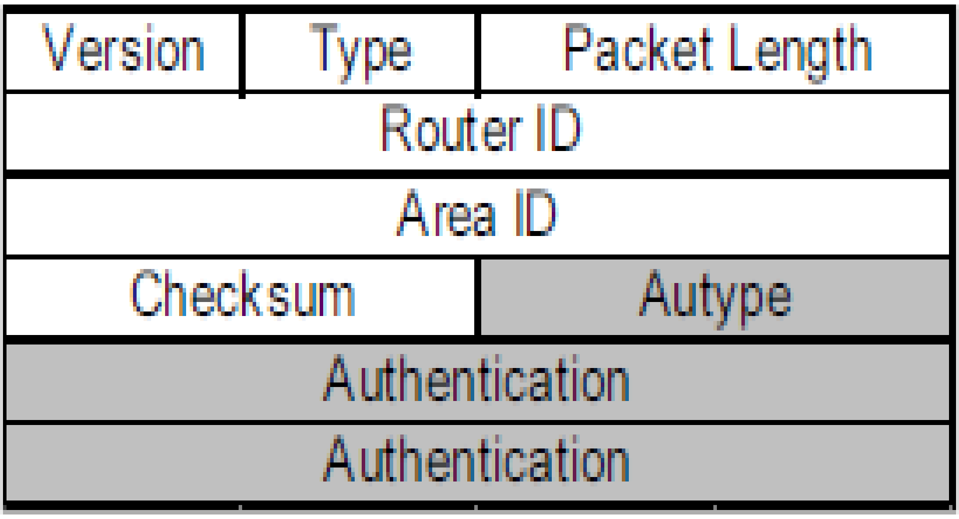
1. Support of IPv6 networking.
2. RIPng does not support update authentication while RIPv2 supports this.IPv6 routers are using IPSec for authentication.
3. RIP does not allow attaching arbitrary tags to routes, where as RIPv2 does ;
4. RIPv2 encodes the next-hop into each route entries; there is a requirement of specific encoding of the next hop for a set of route entries by ipv6.
5. Updates are sent on UDP port 521 using the multicast group FF02::9 by ipv6.

b. **OSPFv3 (**open shortest path first): **Open Shortest Path First** is a link-state routing protocol and is used for Internet Protocol (IP) networks. Link state routing algorithm is used by this protocol .It falls into the group of interior routing protocols and operates within a single autonomous system (OSPF collects link state information from available routers [7]. It then constructs a topology map of the network. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets. OSPF was designed to support variable-length subnet masking (VLSM) .it also supports Classless Inter-Domain Routing (CIDR) addressing models.

Features of ospfv3 for IPv6 are:

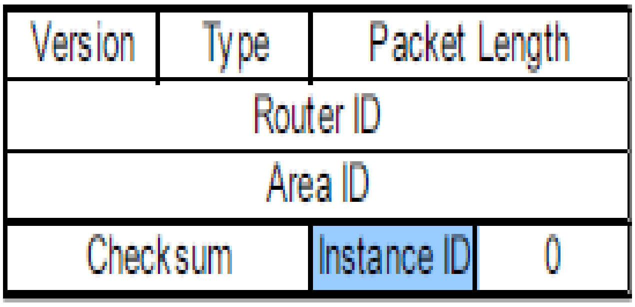
1. OSPF distributes ipv6 prefixes
2. Authentication using IPSec
3. It runs over a link ,not on subnet
4. Flooding scope has been added
5. Supports multiple instances per link

OSPFv3 and OSPFv3 header comparison



<table>
<tr><td>Version</td><td>Type</td><td colspan="2">Packet Length</td></tr>
<tr><td colspan="4">Router ID</td></tr>
<tr><td colspan="4">Area ID</td></tr>
<tr><td colspan="2">Checksum</td><td colspan="2">Autype</td></tr>
<tr><td colspan="4">Authentication</td></tr>
<tr><td colspan="4">Authentication</td></tr>
</table>

Fig5.OSPFv2



<table>
<tr><td>Version</td><td>Type</td><td colspan="2">Packet Length</td></tr>
<tr><td colspan="4">Router ID</td></tr>
<tr><td colspan="4">Area ID</td></tr>
<tr><td colspan="2">Checksum</td><td>Instance ID</td><td>0</td></tr>
</table>

Fig6.0SPFv3

1. Now the size of the header is 16 bytes ,it was 24 bytes in case of ipv2
2. The size of router id and area id is still 32 bits.
3. The router id 0.0.0.0 should not be used as it is reserved
4. There is a new field called instance field that has been introduced which runs multiple OSPF protocol instances per link.

EIGRP FOR IPV6: enhanced interior gateway routing protocol: The Enhanced Interior Gateway Routing Protocol (EIGRP9) is an advanced distance-vector routing protocol that is used to automate routing decisions and configuration in computer networks. In EIGRP a router shares information it has about the network with neighboring routers that belongs to the same logical area known as an autonomous system. Contrary to other well known routing protocols. EIGRP only shares the information that is required rather than sending the whole information. Therefore EIGRP helps in reducing the workload of the router by reducing the amount of data that needs to be transmitted between routers. Features of EIGRP are:

a. It supports variable length masking and classless inter domain routing.
b. MD5 authentication is used between two routers.
c. It does not send the entire routing table to neighbors instead it sends only the topology changes.
d. It uses advance distance vector routing
e. It is easy to configure.

4. VARIOUS ROUTING ATTACKS AND THREATS

1. **Wormhole attack**: In this a sequence of
Packets or application commands are manipulated at one place and then replayed at another location using private network of high speed to cause unauthorized access. The figure is showing the example of wormhole attack on request reply reactive (rreq) control protocol,a1 and a2 are two attackers and node s is the target node .when target node s forward the rreq to node c and node e ,these nodes will forward it to the nodes attack node a1 and to the node e respectively, as a1 and the a2 node consist of high speed channel so their request will reach first to the node d. So the node d will select the path DHCP as the routing path[8].

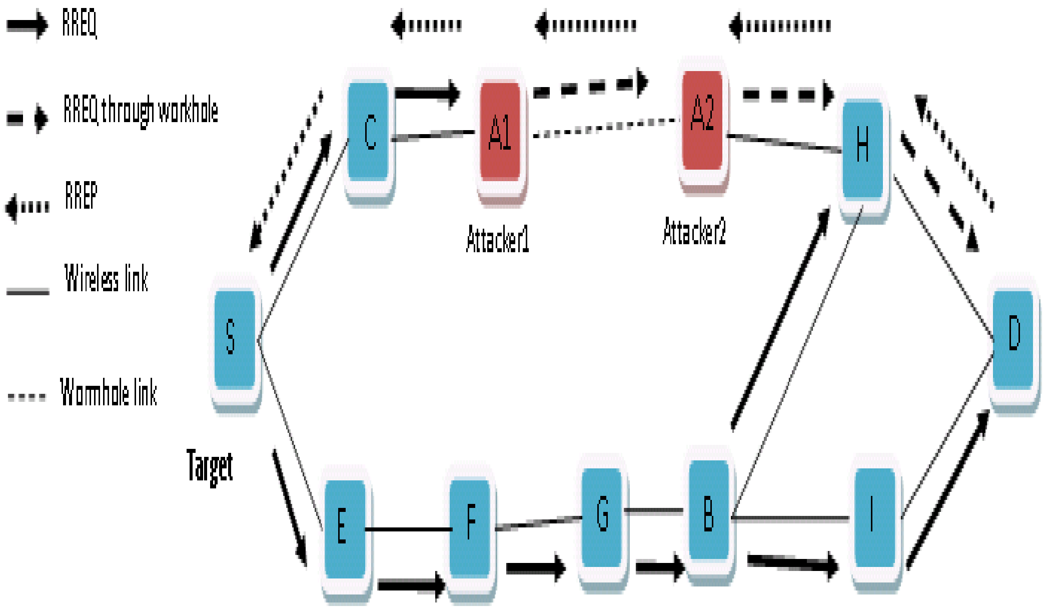


Fig7.Wormhole Attack

2. **Routing injection attack**: rerouting attacks sometimes called “rerouting” attacks, includes manipulating router updates to cause traffic to flow to unauthorized destinations.
3. **Masquerade attack**: These attacks are used to gain unauthorized access and to inject fake into the network. In this an attacker manipulates ip packet to falsify ip address.
4. **Black hole attack**: The venomous node sends falsified routing information and claims that its routing information is optimum and makes other nodes to adopt the same route. for example, in AODV ad-hoc on demand distance vector ,an attacker forward a fake RREP to the source node and claims that the routing information provided by him is the fresh information and this causes the source node to adopt the destination route that crosses the attack node. In the given figure, source node S receives fake routing information from attacker node A, and the source node chooses this path to send data to the destination node D.

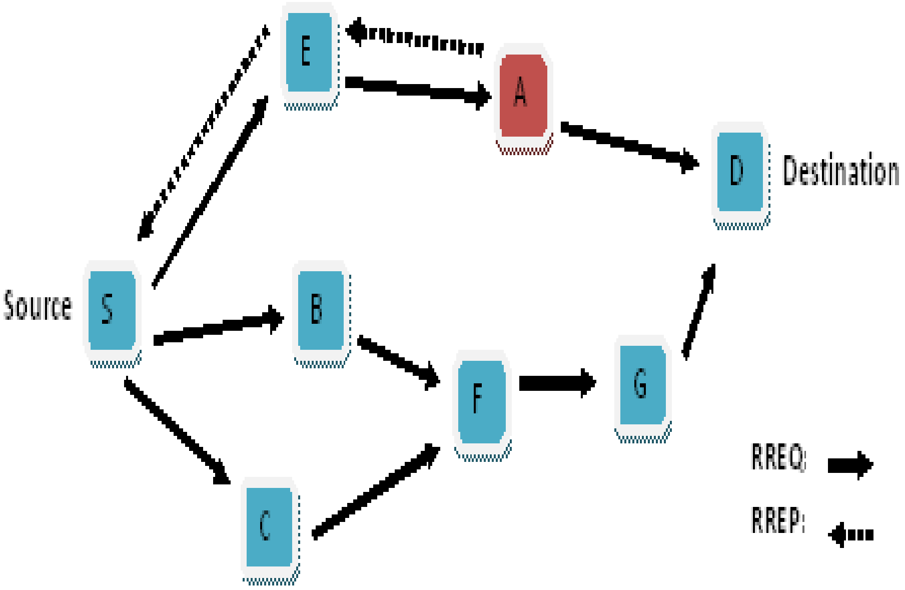


Fig8.Blackhole Attack

5. **Session hijacking attack**: In this attack an attacker inserts falsified IP packet after session establishment via IP spoofing , sequence number prediction.

6. **Link spoofing attack**: In this attack target node selects attack node as its MPR.The malicious node can cook up data and routing traffic .in this an attacker node fake its links with non neighbor in order to disturb the routing operations. For example in the figure shown below node A is the attacker node and node T is the target node. The nodes A and node E are MPR of node T before the attack .the node A shows the fake link with the node D and becomes the only MPR of the target node.

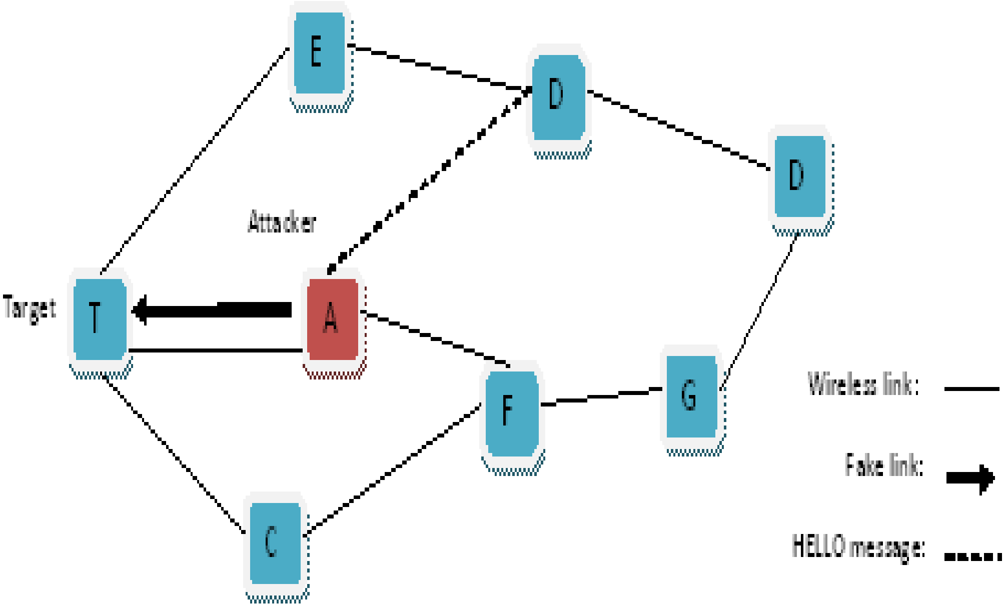


Fig9.Link Spoofing Attack

7. **Land attack**: In this attack an attacker sends a packet to the router with same IP address in source and destination address fields and with the same port number in the source port and destination port fields. This attack degrades the performance of the router.
8. **Smurf attack**: In this attack an attacker sends a large amount of ICMP echo packets to a subnets broadcast address with a spoofed source IP address from that subnet.

9. **Misrelay attack**: In this attack multiple attackers works in agreement to modify or drop IP packets in order to disturb the routing operation. For example, two attacker nodes A1 and A2 work in collusion. When the target node send some data to the attacker node sends it to the attacker node A2 as it is so that node T could not make out the node A1 as the attacker node .An attacker node A2 will then drop some packets and send the falsify packets to the destination node H.

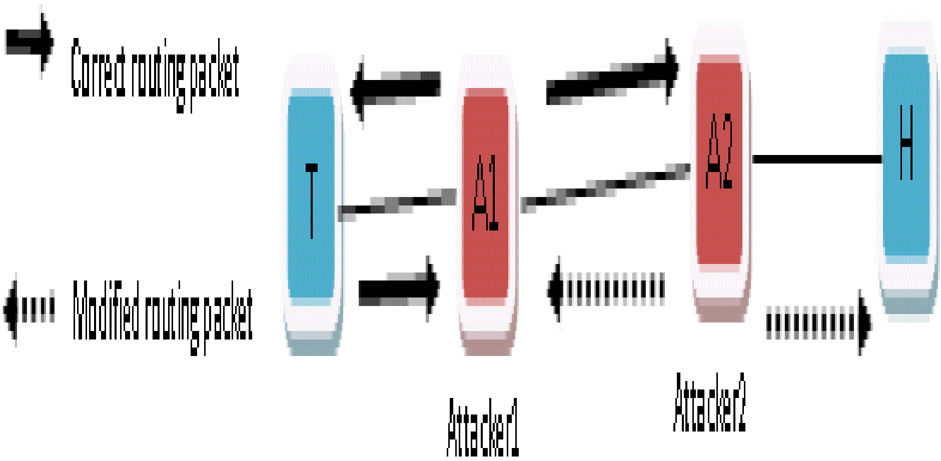


Fig10.Misrealay Attack

10. **IP flooding attack**: In this attack attacker deplete the network resources and node resources such as bandwidth, computational and battery power to cause severe degradation in network performance.

5.REMEDIES FOR ROUTING ATTACKS

ATTACKS	SOLUTIONS TO THE ATTACK
WORMHOLE ATTACK	Packet leashes are used to prevent the wormhole attack. In this method packet expiration time is calculated and is sent along with the packet so that packet travels to its specific destination and prevent it from travelling to any other destination.
BLACKHOLE ATTACK	Route confirmation request and route confirmation reply is used to avoid black hole attack.
LINK SPOOFING ATTACK	Location information based method is used for this kind of attack, this method uses cryptography with a time stamp and GPS
MISRELAY COLLUDING ATTACK	Each node is made to increase its transmission power .when power is made twice its original power then an attack can be detected.
IP FLOODING ATTACK	Each node keeps an eye on the neighbor node RREQ rate. If at some time the rate crosses its threshold limit then that node is recorded as a blacklist node.
REPLAY ATTACK	Timestamp with the use of asymmetric key is used to detect replay attack. The current time and the timestamp is compared and if time stamp and current time are too far from each other then that node is considered to be malicious .
SMURF ATTACK	Ingress filtering has been introduced that prevents from this attacks and also keeps track of this attack
SESSION HIJECKING ATTACK	Use SSL encryption for all the websites. Use WPA encryption for wireless network
LAND ATTACK	Ingress and egress filters are used to block all the packets that contain same source and destination IP address

6.CONCLUSION

The new capabilities of ipv6 protocol pave a way for various threats and attacks. some of the malicious attacks such as wormhole attack ,delay attack, link spoofing attack that causes the loss of information during transmission process are studied in this paper and possible remedies of the threats are summarized. .

7.REFRENCES

[1] Choudhary, Abdur Rahim, and Alan Sekelsky. "Securing IPv6 network infrastructure: A new security model." *Technologies for Homeland Security (HST), 2010 IEEE International Conference on*. IEEE, 2010.

[2] Alabady, Salah. "Design and Implementation of a Network Security Model for Cooperative Network." *Int. Arab J. e-Technol.* 1.2 (2009): 26-36.

[3] Ngadi, Md, Rasheed Hafeez Khokhar, and Satria Mandala. "A review current routing attacks in mobile ad-hoc networks." *International Journal of Computer Science and Security* 2.3 (2008): 18-29.

[4] Sánchez-Casado, Leovigildo, et al. "NETA: Evaluating the Effects of NETwork Attacks. MANETs as a Case Study." *Advances in Security of Information and Communication Networks*. Springer Berlin Heidelberg, 2013. 1-10.

[6] Zagar, Drago, and Kresimir Grgic. "IPv6 security threats and possible solutions." *Automation Congress, 2006. WAC'06. World*. IEEE, 2006.

[7] Jian, Sun, and Yin Ya Fang. "Research and implement of Ospfv3 in Ipv6 network." *Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), 2011*. Vol. 1. IEEE, 2011.

[8] Kannhavong, Bounpadith, et al. "A survey of routing attacks in mobile ad hoc networks." *Wireless communications, IEEE* 14.5 (2007): 85-91.

[9] Jayanthi, J. Gnana, and S. Albert Rabara. "Next generation internet protocol-Technical realms." *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on*. Vol. 9. IEEE, 2010.