IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. V (May-Jun. 2014), PP 22-31
www.iosrjournals.org

Securing IPv6's Neighbour and Router Discovery, using Locally Authentication Process

Simanta Sarma
(Hod & Asstt Professor, Deptt of Computer Science, SBMS College, Sualkuchi, India)

Abstract:*Internet Protocol version six (IPv6), the next generation Internet Protocol (IP), exists sparsely in today's world.Internet Engineering Task Force (IETF), in IPv6, allowed nodes to Auto configure using neighbour discovery protocol. Neighbour Discovery (ND) and Address auto-configuration mechanisms may be protected with IPSec Authentication Header (AH). However, as it gains popularity now a day, it will grow into a vital role of the Internet and communications technology in general. IPv6, the latest revision of the Internet Protocol (IP), is intended to replace IPv4, which still carries the vast majority of Internet traffic as of 2014. Protecting all traffic will include Address Resolution Protocol. To protect this, IPSec will need agreed Key. For Key setup, UDP packet is sent, which requires IPSec for secure communication. So IPSec requires Agreed Key and for Key setup IPSec is needed, this creates a loop. To solve this problem Locally Authentication Process is presented in this paper and we provide a taxonomy for the IPv6 Neighbor and Router Discovery threats, describe two new cryptographic methods, Cryptographically Generated Addresses (CGA) and Address Based Keys (ABK), and discuss how these new methods can be used to secure the Neighbor and Router discovery mechanisms. In this process will provide a certificate of ownership of IP address on network Interface card and Public key to provide authorization. On the other hand, it will also reduce the network load.*

Keywords : *Stateless Address Auto-configuration, Neighbour Discovery, Cryptographically Generated Address (CGA), MYSEA, IPsec, MLS, IP next generation, Multilevel security, Router Discovery, Secure Neighbour Discovery (SEND), Public Key Infrastructure (PKI), Digital Certificate, Security Attacks in IPv6*.

I. Introduction:

Twelve years ago, when the basic design for IPv6 [1][2] was being decided, it was hardly possible to foresee the kinds of wireless environments that are now being considered for use with IPv6.In the Internet Protocol version six (IPv6), also known as the next generation Internet Protocol, lies the future of communications for networked computers and possibly the future of all telecommunications. IPv6 is a complete redesign focusing on eliminating the weaknesses of its predecessor, IPv4. The used IP version 4(IPv4) was developed long time back. By the end of 2012, the number of mobile-connected devices will exceed the number of people on earth, and by 2016 there will be 1.4 mobile devices per capita [1]. IPv4 address space is of 32 bits. The theoretical limit of IPv4 addresses is 4.3 billion addresses. The aggravate problem of exhaustions of addresses, was mitigated by the introduction of Classless Inter-Domain Routing (CIDR), and reduced even more by the adoption of Network Address Translators (NAT). Other problems facing IPv4 are the lack of deployed security, and the rapid growth of the size of the routing tables. Before implementing CIDR the backbone routing table was growing at very high rate as compare to memory technology. The Internet Engineering Task Force (IETF) designed a next generation protocol Internet Protocol version 6 (IPv6) to solve these problems and eventually replacing the existing Internet Protocol, IPv4. This IPv6 was designed after having the rich experience of almost 30 years, of IPv4. IPv6 functions that manage the local link were designed with physically protected, trustworthy links in mind. However, now people are planning to use IPv6 on public radio networks, such as Wireless LANs at airports, hotels, and cafes. Even though the actual link may still be somewhat protected with layer 2 authentication, access control, and encryption some of the nodes on the link may be untrustworthy.

In this research paper, we focus on IPv6 Neighbor Discovery (ND) and Router Discovery (RD) functions. Their current definition relies on the assumption that there are no untrustworthy nodes at the local link. In practice, even a single untrustworthy node can launch various kinds of attacks, including Denial-of-Service (DoS), and masquerade. The current set of RFCs [6][7][8][9] do acknowledge the situation to a degree, but do not provide much detail about how to use the suggested protection mechanism, IPsec. Unluckily, there are a number of problems when using IPsec for securing Neighbor Discovery [10]. In IPv4, the configuration of IP addresses is done manually by the network administrator or with the help of DHCP server. Apart from manual configuration and state full auto-configuration, using DHCP, IPv6 has stateless auto-configuration. Stateless auto-configuration does not require manual configuration of hosts, and additional servers and state-full auto-configuration, hosts obtain interface addresses and configuration information and parameters from a server.

II. Background

In this research paper, we will first briefly touch upon the most widespread way of autoconfiguration in IPv4—Dynamic Host Configuration Protocol (DHCP) [5]. The problems stemming from the design of DHCP will let us understand the design goals behind autoconfiguration protocols of IPv6. After introducing both the addressing schemes of IPv6 and the ND protocol, we give an overview of the Secure Neighbor Discovery (SeND) protocol.

2.1. Neighbour Discovery Protocol

Neighbor Discovery (ND) is one of the most important functions of ICMPv6. As an ARP replacement, it is responsible for finding other hosts on the segment. Regular ND specifications do not include any security provisions. Nodes can make any claims about who they are, as long as they belong to the right multicast group. Most multicast group memberships are assigned automatically, and without any human intervention needed. In IPv6, a host automatically gains some privileges when it has an address. Therefore, the security design for IPv6 is based more on the networking topography than a logical set of privileges and limitations: everyone outside the security perimeter is considered a potential attacker, but insider threats are not considered. ND messages are implemented as a set of ICMPv6 Types and Options, like redirection or a ping service. ICMPv6's Option field [11] provides a generic interface allowing extending ICMP's functionality. For example, Source Link Layer Address(SLLA) is an option type 1 and Target Link Layer Address (TLLA) is an option type 2. To learn the link-layer address of another node that is assumedto be directly attached to the local link, the node that needs theaddress sends a Neighbor Solicitation (NS) message to amulticast address specified by the target address. If the targetnode is indeed present, it should be listening to the multicastaddress. Upon receiving the solicitation, it replies with aNeighbor Advertisement (NA) message. The default operationis illustrated in Figure 1. Additionally, thespecificationdefines that the messagesmaybe protected with IPsec AH. From the security point of view, there are additional problems besides authentication. First, the NA includes a number of flags. One of the flags indicates that the replying node is actually a router. Another one is an "override" flag, specifying that the information in the packet should replace any information that the receiver(s) of the packet may already have. However, unless the authentication keys are strongly bound to IP addresses.

Nodes on the link monitor the reach ability of local destinations and routers in the Neighbor Unreachability procedure [7]. Normally the nodes rely on upper-layer information to determine whether peer nodes are still reachable. However, if there is a sufficiently long delay on upper-layer traffic, or if the node stops receiving replies from a peer node, the NUD procedure is invoked. The node first waits for a small random delay, and then sends a targeted NS to the peer node. If the peer is still reachable, it will reply with a NA. However, if the soliciting node receives no reply, it tries a few more times, eventually deleting the neighbor cache entry. If needed, this triggers the standard address resolution protocol. No higher level traffic can proceed if this procedure flushes out neighbor cache entries after (perhaps incorrectly) determining that the peer is not reachable.

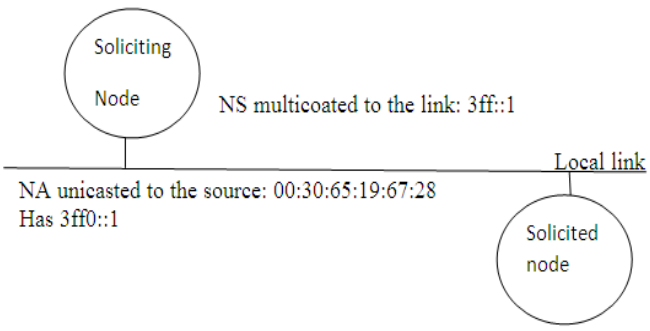

Figure 1: neighbor protocols procedure

2.2. Address Auto-Configuration

Stateless Auto-configuration is the one of the most useful feature that lies in IPv6. The configuration can be done automatically without using any specific protocol such as DHCP. This very feature enables an IPv6 host to configure link-local (an address having link-only scope that can be used to reach neighboring nodes attached to the same link), site-local (an address having scope that is limited to the local site) and global addresses (an address with unlimited scope) for each of its interface. This feature is obtained by the protocol called Neighbor Discovery Protocol (NDP). This protocol includes router (a node that forwards IP packets not

explicitly addressed to itself) discovery, stateless address auto-configuration, address resolution, neighbor reachability, duplicate address detection and redirection.

The address auto-configuration assumes that only the trustworthy nodes will form a network, where the communication has to take place. That is the nodes in local link know each other well. But this is not the case every time. Any malicious node or untrustworthy node can manage to reside in the local link network. This node can affect all the other nodes. This is where security factor comes in. IPv6 should make sure that no such malicious node should be able to join the network providing harm to others.

2.3. Secure Neighbor Discovery

The Secure Neighbor Discovery (SeND) protocol [2], [3] proposes to address theinsider threats discussed above. The main idea behind SeND is to use asymmetriccryptography to enforce authentication and integrity without changing the zeroconfiguration paradigm of the regular ND protocol. IPsec is supposed to be the solution to IP protocol-based security needs, but itfaces many practical problems, such as the initial key distribution [12]. Internet KeyExchange (IKE) is an implemented infrastructure to support IPsec's needs for transport ofkeys, but it requires IPv6 connectivity to work. There is a twofold problemin bringing a similar approach to protecting lower networking layers as a part of IPv6security. The first problem is that of momentum. Unlike enhancements of the Web, IPv6networking has no appeal to a regular user, as it does not provide any instantly observableimprovements. The second problem is a major paradigm shift. Asymmetric cryptography has been historically used to protect data, by working at the highest layers of the OSI model. SeND uses asymmetric cryptography at the lower layers, which is a very novel idea. SeND, since it is an augmentation of the ND protocol, also encodes its messages in ICMPv6by creating a few new Option Types shared among the already existing ND messages. Following ICMP messages are used by Neighbour Discovery Protocol.

***Router Advertisement:** This message is used by Routers to inform other nodes existing on all links, to which they are connected, of its presence and other link related information. The process occurs periodically or in response to a Router Solicitation message.

***Neighbour Solicitation:** These messages have 3 main purposes. The first is to discover the link layer address of a neighbour as part of the address resolution process. This process replaces the use of ARP requests and replies in IPv4. The second purpose is to determine the reachability of a neighbour. The last is to detect the presence of duplicate IPv6 addresses during the address auto configuration process which is detailed later in this report.

***Neighbour Advertisement**: These messages are either in response to Neighbour Solicitations, or sent by a neighbour to announce a change in its link layer address. Upon receipt of a Neighbour Advertisement, a node will update its neighbour cache which contains mappings between IPv6 and link layer addresses of neighbours.

III. Threats in Address Auto-configuration

The stateless address auto-configuration allows a host to connect to the network without registering /authenticating itself. It simply configures the address and start communicating with other nodes on the network. Since node does not have to authenticate itself, any malicious node can get access to network. It can cause various kinds of threats which are explained as follows:

3.1. Redirect Attack:

Another big threat is in Router Solicitation / Advertisement message. In Neighbor Discovery, attacker can make fake advertisement of itself as default router, causing immediately timeout of all other default routers as well as all on- link prefixes. Node received advertisement and start forwarding its packets to this particular router causes man in middle and DoS attack.

3.1.1. Malicious Last Hop Router

A malicious router can send spoofed RA messages, pretending to be the target of RSmessages. This would establish such a router as the default router. If the actual routerwas compromised, it would become a perfectly functional proxy, allowing hosts to carryon with regular transmissions. At the same time, the attacker could tunnel data out of therouter to another computer, where sniffing for credentials could occur.

3.1.2 Neighbor Solicitation/Advertisement spoofing

A malicious node can send a NS message with a wrong Source Link Layer Addressoption, or a NA message with a wrong Target Link Layer Address option. Either one ofthese messages would populate attacker

the target's Neighbor Cache with wrong IPMAC mappings. The target would send information to the wrong nodes, setting itself upfor man-in-the-middle attacks and password and other sensitive information sniffing,effectively creating a redirection or DoS attack.

3.1.3. Spoofed Redirect Message

An attacker can spoof a Redirection message by sending an order to a valid host. Hostsvalidate the source of a Redirection message by the Link Layer address. Without anauthorization method, such a message can be sent by anyone on the local network withthe ability to forge the sender's Link Layer address.

3.2. DoS Threats: DoS—spoofing NUD and DAD replies can effectively DoS machines as their neighbors think they have gone off-line (NUD spoofing) or the attackers neverallow them to get on-line (DAD spoofing).

3.2.1. Parameter Spoofing

RA messages contain extra parameters that can be helpful to the auto configuring hosts. In case such parameters are falsified, nodes might be forced to follow rules that might getthem to talk to wrong hosts, or lose connectivity. The Current Hop Limit is one of thefields propagated in RA messages. If this parameter is set to an artificially low number,the packets will be dropped before they reach their intended destinations. Anotherpeculiar aspect of the ND protocol is that one of its parameters can be used to indicate tohosts to use DHCPv6.

3.2.2. Duplicate Address Detection DoS

In networks where entering hosts obtain their addresses with stateless address auto configuration [8], an attacking node could launch a DoS attack by responding to every duplicateaddress detection attempt. If the attacker claims the addresses,then the host will never be able to obtain an address. Thisthreat was identified in RFC 2462 [8] and an early attempt tosolve the problem was made by Nikander [12].

3.2.3. Bogus Address Configuration Prefix

Similar to the previous attack, a spoofed and invalid network prefix can be sent out to a host attempting address auto configuration. The host will then create an address out of thewrong network prefix, effectively placing it on a wrong network. This will result inlosing connectivity because of the incorrect return address.

3.3.Spoofing:

Spoofing is a way to achieve denial of service (DoS) attack, in an IPv6 network, in the Duplicate Address Detection (DAD) procedure. Attacker on the local link waits until a node sends a Neighbor Solicitation packet. The attacker falsely responds with a Neighbor Advertisement packet, informing the new node that it is already using that address. Upon receiving the Neighbor Advertisement, the new node generates another address and repeats the DAD procedure; the attacker again falsely responds with a Neighbor Advertisement packet. Finally, the new node stops initializing its interface.

3.3.1.Neighbor Discovery Spoofing

When the attacker spoofs certain Neighbor Advertisements, he can execute a MITM attack. By answering falsified Neighbor Advertisements to the issued Neighbor Solicitations from the victims, he redirects all IPv6 traffic over his "routing instance" in the same subnet

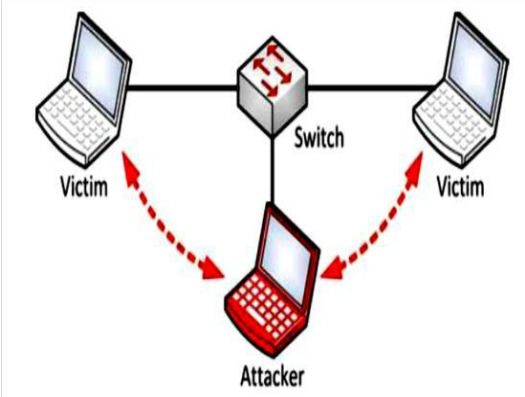

Figure 2: spoofing

3.3.2. Duplicate Address Detection message

A DoS attack is executed if the attacker answers to all Duplicate Address Detection messages (DADs) from a new IPv6 node (with a not yet assigned IPv6 address). The node always believes that this address is already in use and will never get an available IPv6 address and is therefore unable to access the network. This situation remains until the attacker stops the attack.

3.3.3.Rogue DHCPv6 Server address

An attacker can also place his own DHCPv6 server inside a network and distribute falsified values, e.g. a spoofed DNSv6 server address. If the clients accept this DNS server, they will get falsified DNS responses from now on if the attacker also owns the spoofed DNS server. With this attack, internal IPv6 users can be redirected to other (web-) servers than they intended to access. The picture below shows the basic attack in the local network.

IV. Solutions to prevent these threats:

4.1. Send As A Solution

SeND claims to solve the mutual authentication problem. An IPv6 address is afunction of a public key, and the public key is verifiably bound to the private key. Thisthree-way binding is supposed to prevent a malicious user from spoofing the IPv6address. Impersonation attacks would fail because of not being able to generate the IPaddress at all (lack of public key), or not being able to establish the binding betweenprivate and public keys (lack of private key).Replay attacks are supposed to be prevented by using nonce's and time stamps. Old packets should simply fail, being outside of the allowed time difference, or due toresponse with an old nonce.

4.1.1.Cryptographically Generated Address (CGA)

A CGA can be used either as a name for a Cryptographically GeneratedAddress, or the ICMPv6 Option. Both are at the foundations of SeND, but in this sectionwe are concerned with the first meaning. CGA looks like a regular IPv6 address withtwo 64-bit portions. The first 64 bits are the network prefix portion, announcing thesubnet number. The second portion is the Interface Identifier, which is derived using a SeND specific process.

4.1.2. Reply Attack

In order to prevent replay attacks, two new Neighbor Discovery options, Timestamp and Nonce, are introduced. Given that Neighbor and Router Discovery messages are in some cases sent to multicast addresses, the Timestamp option offers replay protection without any previously established state or sequence numbers. When the messages are used in solicitation-advertisement pairs, they are protected with the Nonce option.

4.1.3.RSA Digital Signature Option

Once the public key is obtained from CGA Option, the receiver can use itto decrypt messages encrypted with the corresponding private key. ICMPv6 Option 12allows us to use RSA digital signatures to establish authenticity of such packetexchanges. Here's a list of fields contained in a RSA Signature option:

· **Key Hash**—leftmost 128 bits of SHA-1 of the public key, used forconstructing the signature

· **Digital Signature**—variable length field containing PKCS#1 v1.5 [17]signatures, using the sender's private key over these entities:

* 128 bit CGA Message Tag value for SeND.
* 128 bit Source Address from the IPv6 header
* 128 bit Destination Address from the IPv6 header
* 8 bit Type, 8 bit Code and 16 bit Checksum fields from the ICMPv6header
* ND protocol message header, starting after the ICMPv6 checksum,and up to but notincluding ND protocol options
* ND protocol options preceding the RSA signature option

4.2. IPsec:

The neighbor discovery messages may be protected withIPsec AH [7]. Potentially, AH could be used by the hosts toverify that Neighbor Advertisements and RouterAdvertisements do contain proper and accurateinformation.Given a suitable set of AH Security Associations (SAs), thehost can verify that the ND messages it receives are reallyvalid and authorized. The proposed mechanism is quite cumbersome due thelarge number of SAs needed.Internet Protocol Security is meant for protecting the communication over the IP network. It supports network-level peer authentication, data origin authentication, data integrity, and data confidentiality (encryption) and replay protection. It basically uses the cryptographic security services for

protection or authentication and encrypts each IP packet of a communication session. These can be either between a pair of nodes, or between a pair of security gateways or between a security gateway and a node.

V. Proposed Solution

This solution envisages that only those nodes will be able to join the networks which have been authenticated by issuing valid token, issued by local trusted node. The basic purpose of token is to allow node to verify link local address and its owner ship on Public key.

The basic terminologies used are:

ADDRESS BASED KEYS

Addressed Based Keys (ABK) [19] use a cryptographictechnique known as identity based cryptosystems. Identitybased cryptosystems allow any publicly known identifier, suchas an E-mail address or the IP address of a node, to function asthe public key part of a public/private key pair. That is,basically any bit string may act as a public key. The trick liesin the way the corresponding private keys and a number ofparameters are generated.

Public Key [Pu(X)(Y)]

Pu stands for Public key. X denotes entity that has generated this key and Y identifies the entity for which it is generated. Like Pu(AS)(N) defines Public key generated by AS for node N.

Private Key [Pr(X)(Y)]

Pr stands for Private key. X denotes entity that has generated this key and Y identifies the entity for which it is generated. Like Pu(AS)(N) defines Private key generated by AS for node N.

Identity Based Key Algorithms

There are many algorithms available for identity basedcryptosystems. Shamir [20] introduced the idea of identitybased cryptography in 1984. Practical, provably secure identitybased signature schemes [21][22], and KeyAgreementProtocols [23] soon followed. Practical, provably secureidentity based encryption schemes [24][25] have only veryrecently been found.In identity based signature protocols, the host signs a messageusing its private key supplied by its IPKG. The signature isthen verified using the host's publicly known identity. Inidentity based key agreement protocols, two parties share asecret. Each party constructs the secret by using its ownprivate key and the other party's public identity. In identity based encryption, the encryptor uses the recipient's publicidentity to encrypt a message, and the recipient uses its privatekey to decrypt the cipher text.

Certified addresses:

Identity based algorithms are fairly similar to conventional public keycryptosystems from the practical point of view. Consequently,instead of using the addresses directly as public keys, onecould just use a conventional public key cryptosystem andcreate certificates. Like ABK, address certification relies on a trusted agent. In this method, each node generates its own signature key pair. The node then co-operates with the trusted agent to generate 1–3 random host identifiers. For example, the host identifier can be produced by hashing together a random number R_{host}generated by the host itself and another random number R_{ttp}provided by the trusted agent.

$$\text{Host ID} = \text{HASH}(R_{host}/R_{ttp}) \quad \text{Eq. 7}$$

Finally, the trusted agent signs a certificate that binds the host identifier to the host's public key. This can be an X.509certificate where the host identifier is used as the entity name.

Digital Certificate DC(X)

Digital Certificate issued by X .

* Calculating Digital Signature (DS)

Digital signatures for ABKs are calculated using the following algorithm:

sig =SIGN (hash (contents), IPrK, Params) Eq. 4

where:

sig	The digital signature.
SIGN	The identity based digital signature algorithm used to calculatethe signature.
hash	A one-way hash algorithm, e.g. SHA1-HMAC.
IPrK	The Identity based Private Key.
Params	The public cryptographic parameters.
contents	The message contents to be signed.

The recipient verifies the signature in the following way:

IPuK = IBC-HASH (ID) Eq. 5

valid = VERIFY (hash (contents), sig, IPuK) Eq. 6

where:

IBC-HASH	A hash function specific to the identity based algorithm thatgenerates the public key from the public identifier.
ID	The publicly known identifier used to generate the key.
IPuK	The Identity based Public Key.
Sig	The digital signature.
VERIFY	The identity based public key algorithm used to verify thesignature.
Params	The public cryptographic parameters.
valid	1 if the signature is verified, 0 if not.

*** Message Digest MD(X)**

Message converted into fixed size encrypted message. X represents the parameters which were converted into digest number.

*** Manufacturing Company [MC]**

Here Company refers to those companies which are involved in the manufacturing of NIC (Network Interface Card) of the node wishing to participate in the communication in a network.

***Tentative Address [TA]**

An IP Address Generated by node before it converted into permanent Address.

* Cryptographically Generated Address [CGA]

Cryptographically Generated Address use to authenticate sender.

***Token [TN(X)]**

The Token is a Digital signature generated by AS using public key Pr(AS)(AS) of public key of AS Pu(AS)(AS) and TA and is issued to node X.

VI. Working Process:

Internet Protocol version 6 (IPv6) is a networking protocol that allows Windows users to communicate with other users over the Internet. It interacts with Windows naming services such as Domain Name System (DNS) and uses security technologies such as Internet Protocol security (IPSec), because they help facilitate the successful and secure transfer of IP packets between computers. Ideally, IPv6 is used in a pure environment, that is, an environment where IPv6 is the exclusive Internet protocol used between computers. Currently, however, pure IPv6 transmissions are attainable only with routers that support IPv6 and computers that are running Windows and that support IPv6. As IPv6 supplants IPv4, pure IPv6 across the Internet will become more prevalent and will eventually replace IPv4. Until that occurs, the transition technologies described in this reference can be used to bridge the technological gap between IPv4 and IPv6.

6.1. IPv6 Architecture

The IPv6 protocol component that is installed in Windows operating systems is a series of interconnected protocols that include Internet Control Message Protocol version 6 (ICMPv6), Multicast Listener Discovery (MLD), and Neighbor Discovery. These core protocols replace the Internet layer protocols in the Defense Advanced Research Projects Agency (DARPA) model. All protocols above the Internet layer rely on the basic services that IPv6 provides. Protocols at the Host-to-Host Transport and Application layers are largely unchanged, except when addresses are part of the payload or part of the data structures that the protocol maintains. For example, both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) must be updated to perform new checksum calculations that include IPv6 addresses.The following figure shows the architecture of the IPv6 core protocols in relation to the Open Systems Interconnection (OSI) model, the TCP/IP protocol architecture, and the other protocols in the TCP/IP suite.

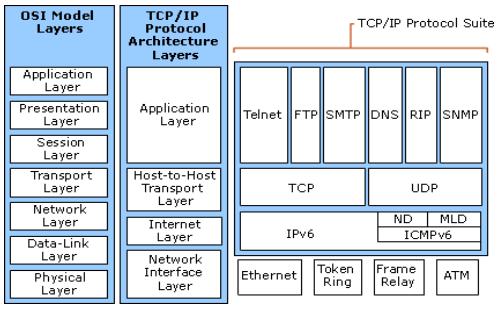

Figure 3: IPv6 architecture

6.2. IPv6 Core Protocols

Protocol	Function
IPv6	IPv6 is a routable protocol that is responsible for the addressing, routing, and fragmenting of packets by the sending host. IPv6 replaces Internet Protocol version 4 (IPv4).
ICMPv6	ICMPv6 is responsible for providing diagnostic functions and reporting errors due to the unsuccessful delivery of IPv6 packets. ICMPv6 replaces ICMPv4.
Neighbor Discovery	Neighbor Discovery is responsible for the interaction of neighboring nodes and includes message exchanges for address resolution, duplicate address detection, router discovery, and router redirects. Neighbor Discovery replaces Address Resolution Protocol (ARP), ICMPv4 Router Discovery, and the ICMPv4 Redirect message.
Multicast Listener Discovery	Multicast Listener Discovery is a series of three ICMPv6 messages that replace version 2 of the Internet Group Management Protocol (IGMP) for IPv4 to manage subnet multicast membership.

6.3. IPv6 Address Syntax

IPv4 addresses are represented in dotted-decimal format. These 32-bit addresses are divided along 8-bit boundaries. Each set of 8 bits is converted to its decimal equivalent and separated from the other sets by periods. For IPv6, the 128-bit address is divided along 16-bit boundaries. Each 16-bit block is converted to a 4-digit hexadecimal number and separated by colons. The resulting representation is known as colon-hexadecimal.
The following is an IPv6 address in binary form:
00100001110110100000000011010011000000000000000000010111100111011
00000010101010100000000011111111111111110001010001001110001011010

The 128-bit address is divided along 16-bit boundaries:
0010000111011010 0000000011010011 0000000000000000 0010111100111011 0000001010101010 0000000011111111 1111111000101000 1001110001011010

Each 16-bit block is converted to hexadecimal and delimited with colons. The result is:
21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

IPv6 representation can be further simplified by removing the leading zeros within each 16-bit block. However, each block must have at least a single digit. With leading zero suppression, the address representation becomes:
21DA:D3:0:2F3B:2AA:FF:FE28:9C5A

6.4. Verification of Certificate:

The message containing: DC(CA),DS(MC)(Pr(CA)(MC)) , Pu(N)(N), NIC number and DS (N)(Pr(N)(N)) are sent to AS. AS, then verifies Digital certificate DC(CA) by verifying public key Pu(CA)(MC) present in digital certificate with its database or from CA. However, it is not possible to verify from database, when AS does not have an entry into its database, of this particular company. Then AS sends request to the CA for verification of public key Pu(CA)(MC), present in Digital Certificate DC(CA).

6.5. Network Address Translators

As defined in RFC 1631, a network address translator (NAT) is an IPv4 router that can translate the IP addresses and TCP/UDP port numbers of packets as it forwards them. For example, consider a small business network with multiple computers that connect to the Internet. Without a NAT, this business would need to obtain a public IP address for each computer on the network. With a NAT, however, the small business can use private addressing (as described in RFC 1918) and have the NAT map its private addresses to a single or to multiple public IP addresses.
NAT is a common solution for the following combination of requirements:

- The administrator wants to leverage a single connection over multiple computers, rather than connecting each one to the Internet.
- The administrator wants to use private addressing.
- The administrator wants to allow access to Internet resources without having to deploy a proxy server.

6.6. Verification of NIC

This process is used to Verify NIC. After verification of Pu(CA)(MC), AS extract NIC Number from Digital Signature DS(MC)(Pr(CA)(MC)),using Pu(CA)(MC), and compares it with NIC Number present in message. The matching of NIC number, confirms that NIC number is not fake.

6.7. Registered Private and Public key for node

After the authentication of node and verification of token request, AS then generates Private/Public key pair Pr(AS)(N) and Pu(AS)(N) for node. The Pu(AS)(N), along with TA are stored into AS. This information is stored to reply any request made by any node for verification of owner ship of Pu(AS)(N) of TA.

6.8. Issuance of Token

The Token is like a Digital signature created by AS of Public Key Pu(AS)(N), Pu(AS)(AS) and TA using Pr(AS)(AS). The basic purpose of token is to allow node to verify TA and its owner ship on Pu(AS)(N). This is done by comparing message digest from decrypting token with message digest from TA, Pu(AS)(N) and Pu(AS)(AS). This verification of TA and corresponding certified Pu(AS)(N) restrict the node to go to AS for verification of sender every time. This reduces network load.

6.9. DAD on Tentative address:

After receiving Token and other parameters from AS, AS then performs the DAD operation on tentative address. Nodes receiving DAD message performs the authentication of sender process using Token and other parameter. If any node replies DAD, it sends its token and other parameters to enquiring node. Node, then, performs authentication of sender, as explained above. If node receives message from authentic node, node again generates new TA. The node sends modification request with new TA, old TA and Token issues against old TA to AS. AS will verify node and modify its database accordingly. A new token is created to send to node again.

6.10. Communicating Using a Teredo Address

A Teredo relay is an IPv6/IPv4 router that can forward packets between Teredo clients on the IPv4 Internet (using a Teredo tunneling interface) and IPv6-only hosts. In some cases, the Teredo relay interacts with a Teredo server to help it facilitate initial communication between Teredo clients and IPv6-only hosts. The Teredo relay listens on UDP port 3544 for Teredo traffic.

Initial configuration for Teredo clients is accomplished by sending a series of Router Solicitation messages to Teredo servers. The clients use the responses to derive a Teredo address and determine whether they are behind cone, restricted, or symmetric NATs. If a Teredo client is behind a symmetric NAT, then it cannot function. You can see what type of NAT a Teredo client has discovered from the display of the **netsh interface ipv6 show teredo** command.

IPv6 router discovery processes:

- IPv6 routers periodically send Router Advertisement messages on the local link advertising their existence as routers. They also provide configuration parameters such as default hop limit, MTU, and prefixes.
- Active IPv6 hosts on the local link receive the Router Advertisement messages and use the contents to maintain their default router lists, prefix lists, and other configuration parameters.
- A host that is starting up sends a Router Solicitation message to the link-local scope all-routers multicast address (FF02::2). Upon receipt of a Router Solicitation message, each router on the local link send a unicast Router Advertisement message to the node that sent the Router Solicitation message. The node receives the Router Advertisement messages and uses their contents to build the default router and prefix lists and to set other configuration parameters.

VII. Conclusions

In this paper we have described a number of threats pertinentto current IPv6 Neighbor and Router Discovery, discussed twonew cryptographic techniques, Cryptographically GeneratedAddresses (CGA) and Address Based Keys (ABK), and brieflydescribed how these can be used to secure the Neighbor andRouter Discovery functions. The Neighbour Discovery protocol was introduced to facilitate the node to configure itself. But if ND protocol is not protected it can open flood gate for threats. To protect from threats SEND was introduced which uses CGA address[4]. The basic idea in CGA is to generate most of the 64 low orderbits in an IPv6 address as a cryptographic hash over a publickey and other parameters. The underlying cryptosystem can beany public key cryptosystem, such as RSA, DSA, or EllipticCurve based DSA. The missing part in Cryptographically Generated Address is that CGAs themselves are not certified, an attacker can create a new CGA from any subnet prefix and its own or anyone else's public key[5]. ABK uses either the low order bits of theaddress or all the bits of a routing prefix as a public key,relying on an identity based cryptosystem. Together these twomethods can be used to secure Neighbor Discovery in a waythat does not require any explicit security infrastructure. Further, the scheme presented, in this paper, ensures that owner of NIC number and its corresponding IP Address has sent the message. This provides message authentication to receiver. The Public-key mechanism is used to exchange secret key. This secret key is used to encrypt the message, to provide confidentiality. The message digest of encrypted message is used to provide integrity of message. Furthermore,

it is essential to encode the security parameter aswell as the address type into address bits. This may createfurther operational and other complications. If the security parameter were communicated in aprotocol message and not encoded into the IP address, anattacker could misrepresent the values and attack a weakermechanism than the one selected by the address owner. Further, the verification of TA and corresponding certified Pu(AS)(N), restrict the node to go to AS for verification of sender every time and in this paper are really effective only if the lower protocollayers are sufficiently protected or if the lower-layer attacksare considered unlikely or prohibitively expensive.

Acknowledgements:

The author would like to thank everyone, whoever remained a great source of help and inspirations in this humble presentation. The author would like to thank Gauhati University, Assam (Teaching Staff of Department of Computer Science); S.B.M.S College, Sualkuchi, Assam for providing necessary facilities to carry out this work.

References

[1]. Al-Radhi, A, A. 2011. IPv6 Promised Role in Mitigating Cyber Attacks: Really it's Time!.Swiss Cyber Storm-International IT Security Conference, Switzerland.
[2]. Fundamental Benefits of IPv6, http://www.ipv6now.com.au/primers/benefits.php
[3]. Minoli, D. Kouns, J. 2009. Security in an IPv6 Environment. CRC Press, USA.
[4]. T. Aura; Request for Comments: 3972; March 2005; Cryptographically Generated Addresses (CGA)
[5]. S. Thomson, T. Narten and T. Jinmei; Request for Comments: 4862; September 2007; "IPv6 Stateless Address Autoconfiguration "
[6]. Stefano M.Faccin and Franck Le ; "A Secure and Efficient solution to the IPv6 address ownership problem"; 0-7803-7605-6/02 ,2002 IEE Page : 162 -166.
[7]. AmirhosseinMoravejosharieh, Hero Modares and RosliSalleh; "Overview of Mobile IPv6 Security " ;2012 Third International Conference on Intelligent Systems Modelling and Simulation; 978-0-7695-4668-1/12,2012 IEEE.
[8]. R. Hinden and S. Deering, IETF RFC 4291: Internet Protocol Version 6 (IPv6)Addressing Architecture, February 2006.
[9]. C. M. Kozierok "IPv6 Interface Identifiers and Physical Address Mapping"[online] September 2005 [cited April 2007] available from, WWW:http://www.tcpipguide.com/free/t_IPv6InterfaceIdentifiersandPhysicalAddressMapping-2.htm.
[10]. S. Thomson and T. Narten, IETF RFC 2462: IPv6 Stateless AddressAutoconfiguration, December 1998.
[11]. A. Conta and S. Deering, IETF RFC 2463: Internet Control Message Protocol(ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, December1998.
[12]. P. Nikander, "A Scalable Architecture for IPv6 AddressOwnership", unpublished manuscript, available athttp://www.tml.hut.fi/~pnr/publications/draft-nikander-ipngpbk-addresses-00.txt, March 2001.
[13]. D. Thaler and J. Hagino, "IPv6 Stateless DNS Discovery",draft-ietf-ipv6-dns-discovery-04.txt, work in progress.
[14]. Steven Bellovin, "Security Problems in the TCP/IP ProtocolSuite", Computer Communication Review, Vol. 19, No. 2,pp. 32–48, April 1989.
[15]. A. Conta and S. Deering, Internet Control Message Protocol(ICMPv6) for the Internet Protocol Version 6 (IPv6), Specification, RFC2463, Internet Engineering Task Force,December 1998.
[16]. IEEE Draft P802.1X/D11: Standard for Port based NetworkAccess Control, LAN MAN Standards Committee of theIEEE Computer Society, March 27, 2001.
[17]. IEEE Std. 802.11i/D2.0, Draft Supplement to IEEE 802.11Standard: Specification for Enhanced Security, March 2002.
[18]. P. Nikander, Ed. And J. Kempf and E. Nordmark, IETF RFC 3756: IPv6 Neighbor Discovery (ND) Trust Models and Threats, May 2004.
[19]. M. Handley, Ed. E. Rescorla, Ed., IETF RFC 4732: Internet Denial-of-Service Considerations, November 2006.
[20]. S. Convery, D. Miller, "IPv6 and IPv4 Threat Comparison and Best-Practice Evalutation" [online] March 2004 [cited April 2007] available from WWW: http://www.cisco.com/web/about/security/security_services/ciag/documents/v6-v4-threats.pdf.
[21]. G. Fairhurst, "Address Resolution Protocol (arp)" [online], Aberdeen, UK: University of Aberdeen, December 2005 [cited April 2007], available from the WWW: http://www.erg.abdn.ac.uk/users/gorry/course/images/arp-eg.gif.