Securing IPv6's Neighbour Discovery, using Locally Authentication Process

[1]M. N. Doja, [2]Ravish Saggar
[1] Department of Computer Engineering, Jamia Millia Islamia, New Delhi.
[2] Research Scholar Singhania University, Faculty: BCIIT, New Delhi.

Abstract :
Internet Engineering Task Force (IETF), in IPv6, allowed nodes to Autoconfigure using neighbour discovery protocol. Neighbour Discovery (ND) and Address auto- configuration mechanisms may be protected with IPSec Authentication Header (AH). 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. 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), Secure Neighbour Discovery (SEND), Public Key Infrastructure (PKI), Digital Certificate, Security Attacks in IPv6.

1. Introduction

The availability of IPv4 addresses is exhausting due to massive growth of the internet and the proliferation of internet-connected devices other than computers like mobile phones, PDAs etc. 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.

Apart from making large address space of 128 bits in IPv6, IETF added many new features. This includes address auto-configuration, host discovery, optimized header, protocol extensibility etc. 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. It allows a host to generate its own addresses using a combination of locally available information and information advertised by routers. In state-full auto-configuration, hosts obtain interface addresses and/or configuration information and parameters from a server.

2. Neighbour Discovery Protocol

The Neighbour Discovery protocol is improvement over many process defined in IPv4. New functionality has also been added. The neighbour Discovery Protocol is used for following purposes by nodes.

2.1. For Autoconfiguration of IPv6 Address.
2.2. To determine network prefix,routers and other parameters.
2.3. For Duplicate IP address detection (DAD).
2.4. To determine layer two address of nodes on the same link.
2.5. To find neighbouring routers that can forward their packet.
2.6. To keep track of which neighbours are reachable and which are not (NUD).
2.7. To detect changed link-layer addresses.

To perform all above mentioned work ND uses five ICMPv6 messages: a pair of Router Solicitation / Router Advertisement messages, a pair of Neighbour Solicitation / Neighbour Advertisement messages and an ICMP Redirect message.

3. ICMPV6 Messages

Following ICMP messages are used by Neighbour Discovery Protocol.

3.1. 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.

3.2. Router Solicitation: Upon the enabling of an interface of a node, these messages can be used to request all routers on the same local link to send Router Advertisements immediately, rather than waiting until the next periodically scheduled advertisement.

3.3. Redirect : These messages are used by routers to tell hosts that a better on-link router exists for a given destination address.

3.4. 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.

3.5. 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.

4. 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.

5. Address Auto-Configuration Process

The sequence of signals generated during stateless Auto-configuration is given in Figure 1.

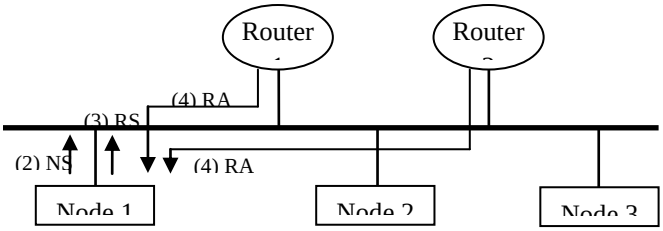

Figure 1. Process of address auto-configuration

The steps are as follows:

5.1. At the very first, a link local address is being generated by the new node. It then allocates it to one of the its interface. This link local address contains the prefix of fe80:: /64 and the 64 bit interface id as shown in Figure 2. This address is tentative address.

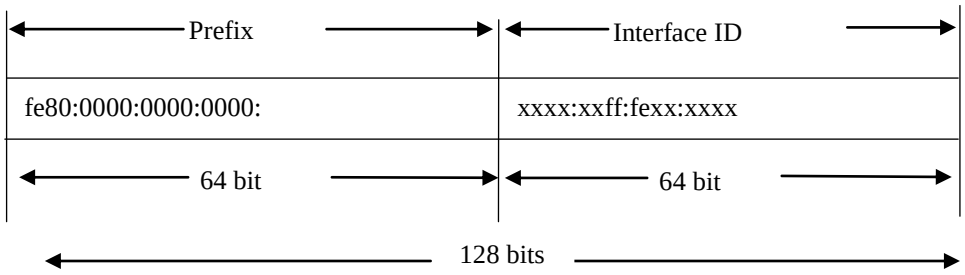

Figure 2. link-local address in ipv6

The node joins the following multicast groups. The all node multicast group(FF02::1)and the solicited-node multicast group, for the tentative address.

5.3.1. After this there is Duplicate Address Detection (DAD), which takes care that the newly generated link local address is not already present on the network. The steps are as follows:
A Neighbor Solicitation (NS) message is being transmitted by the node, with target tentative address, on the network.

5.3.2. If any another node on the network is using the same link local address, then it returns the Neighbor Advertisement (NA) message.

5.3.3. If the new node gets the NA message, no link-local will be allocated to it and the interface will terminate. Else the new node will be initialized buy its link-local address and is assumed to be unique and valid.

5.2. Now the host will send Router Solicitation (RS) messages.

5.3. After this, all those routers who received the RS message will send back the Router Advertisement (RA) message.

5.5.1. If no RA is received, then node uses a state-full address configuration to obtain its addresses.

5.5.2. Else, the node receives the RA and gets the IPv6 address prefix.

5.4. Once the prefix is obtained by the host, it can create its unique site local and global addresses.

6. 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:

6.1. Multiple Interface Address:

IPv6 interface can have multiple addresses. Attacking node, using auto-configuration, can block large number of IP addresses for its interface and deny other workstation to acquire address. This poses a possible denial of service attack.

6.2. 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.

6.3. 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.

To prevent all these threats some security measures are to be taken. If not secured, it is vulnerable to various attacks. The following sections will describe some existing and proposed solutions.

7. Existing Solutions

There are few solutions to prevent these threats. These are as following:

7.1. IPSec

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.

It is an open standard and makes use of the following 3 basic protocols:

- Authentication Header
  AH provides connectionless integrity and data origin authentication for IP datagram and provides protection against replay attacks. That is it can be used by the nodes to authenticate the neighbor advertisement and the router advertisement messages.
- Encapsulating Security Payloads
  ESP provides confidentiality, data origin authentication, connectionless integrity, an anti-replay service and limited traffic flow confidentiality.
- Security Associations

SA provides number of algorithms and data that provide the parameters necessary to operate the AH and/or ESP operations. It is used to make sure that the nodes in a network are trustworthy. It depends upon the addresses generated by the neighbor discovery, security keys etc. This SA needs to be set up between all the communicating nodes in advance. It can either use the manual mechanism or can be done automatically. As the networks are growing and there are more and more nodes under one network the number of SAs in a single network also increases. This large number of SAs is difficult to maintain. Another problem is that IPSec needs to use NDP for configuring security association, but NDP is requiring IPSec. And hence this is not clear approach to deploy.

7.2. SEcure Neighbor Discovery (SEND)

The SEcure Neighbor Discovery (SEND) protocol is a security extension to the Neighbor Discovery protocol in IPv6. This protocol provides an alternative way for securing NDP. It makes use of a cryptographic method for the same. This protocol came with three additional capabilities: address ownership proof, message protection and router authorization.

It defines a set of new attributes

7.2.1 Cryptographically Generated Addresses(CGA)

Cryptographically Generated Addresses are used to make sure that the sender of a Neighbor Discovery message is the "owner" of the claimed address. A public-private key pair is generated by all nodes before they can claim an address. A new NDP option, the CGA option, is used to carry the public key and associated parameters.

7.2.2 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.

7.2.3 RSA Signature option

A new NDP option, the RSA Signature option, is used to protect all messages relating to Neighbor and Router discovery. Public key signatures protect the integrity of the messages and authenticate the identity of their sender.

7.2.4 New network discovery messages

Certification paths, anchored on trusted parties, are expected to certify the authority of routers. A host must be configured with a trust anchor to which the router has a certification path before the host can adopt the router as its default router.

The SEcure Neighbor Discovery (SEND) uses Crypto-Generated Address (CGA), to make sure that the sender of a Neighbor Discovery (ND) message is the “owner” of the claimed address. CGA is a technique whereby an IPv6 address of a node is cryptographically generated by using a one-way hash function from the node’s public key and some other parameters. This CGA is used to prevent the stealing or spoofing of existing IPv6 addresses by assuring only ownership. But the issue is that because 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. However, the attacker cannot take a CGA created by someone else and send signed messages that appear to come from the owner of that address.

8. 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.

8.1. The basic terminologies used are:

- Certification Authorities [CA]
  Certification Authorities are responsible for the processing of request of issue, renewal and revoking of PKCs stored in request server.
- Authentication Server [AS]
  Authentication Server is a user an trusted Anchor . There is one AS for every subnet to provide authentication of any new node joining the subnet.
- 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.
  Database [DB]
  It is the place where AS stores the necessary data needed at the time of authenticating the node.
- Digital Certificate DC(X)
  Digital Certificate issued by X .
- Digital Signature DS(X)(Y)
  Digital Signature issued by X and generated using key Y.
- 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.

8.2. Working Process:

This solution assures that no node can communicate in network without having a Token, issued by AS. To protect the network from any intrusion node the following processes are used:

8.2.1. Request for Private Key and Public Key pair from CA: The Manufacturing Company requests CA to issue Private/Public Key pair Pr(CA)(MC)/Pu(CA)(MC) and digital Certificate, as shown in Fig.3. The CA issues Digital certificate DC(CA) that contains a Public Key Pu(CA)(MC) and the identity of the owner and makes it available publicly. The matching private key Pr(CA)(MC) is given to company, which keeps Private Key top secret. This certificate is a confirmation by the CA that the public key contained in the certificate belongs to company noted in the certificate.

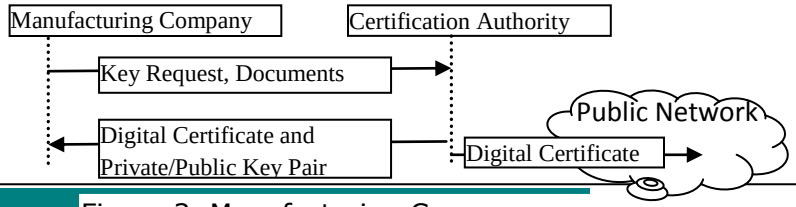

Figure 3. Manufacturing Company

8.2.2. Hard Wired Information in NIC

The company who is manufacturing the network interface card, to be installed on the nodes interested in communication over a network, generates digital signature DS(MC)(Pr(CA)(MC)) from NIC Number using private key Pr(CA)(MC), received from CA. The Digital certificate, digital signature and NIC number is hard-coded into interface card as shown in figure 4. This Hard coded information is used to verify the NIC by AS, using public key Pu(CA)(CA) provided by the CA.

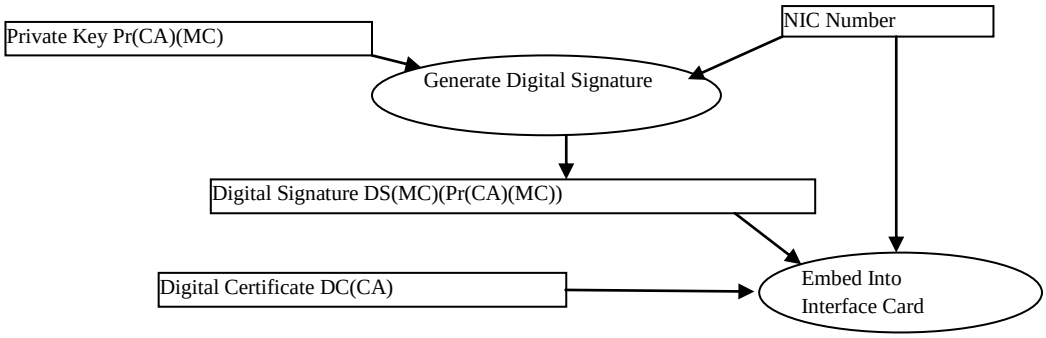

Figure 4. Generation of Information to be embedded into Interface Card

8.2.3. Digital Signature by Node

Node first generates TA and private/public key pair Pr(N)(N) and Pu(N)(N). The DC(CA), DS(MC)(Pr(CA)(MC)), TA, Public Key Pu(N)(N) and NIC number are collectively converted into fixed length message digest. This message digest is then encrypted using private key Pr(N)(N) to get digital signature DS (N)(Pr(N)(N)) as shown in figure 5.

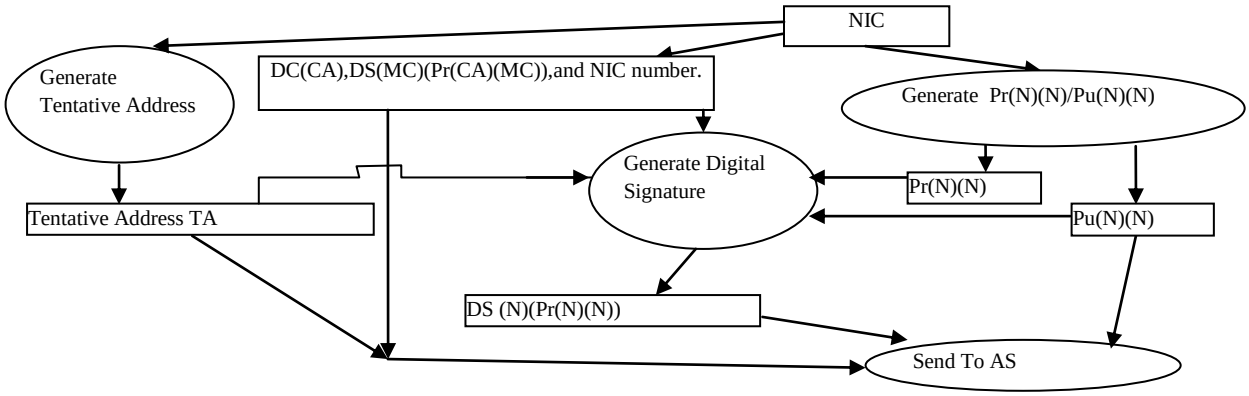

Figure 5. Node Processes

8.2.4. 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). Once, CA verifies Pu(CA)(MC), the Company details and corresponding Pu(CA)(MC) are stored in database of AS, so that, in future, company can be verified locally. This process is shown in figure 6.

8.2.5. 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.

8.2.6. Authentication of node:

Along with Digital signature DS (N)(Pr(N)(N)) the actual parameters DC(CA),DS(MC)(Pr(CA)(MC)), Pu(N)(N) and NIC number are also sent to AS. AS after confirming that NIC is not fake, AS verifies NIC number and corresponding TA, and for this purpose , AS creates message digest MD**(**DC(CA), DS(MC)(Pr(CA)(MC)) , Pu(N)(N) and NIC number and TA from message**)**. AS then decrypts the DS (N)(Pr(N)(N)) using Pu(N)(N) to get message digest. AS then compares both message digests as shown in figure 6. The matching of digests proves the owner ship of TA on Public key Pu(N)(N) key which authenticates the sender and integration of packet.

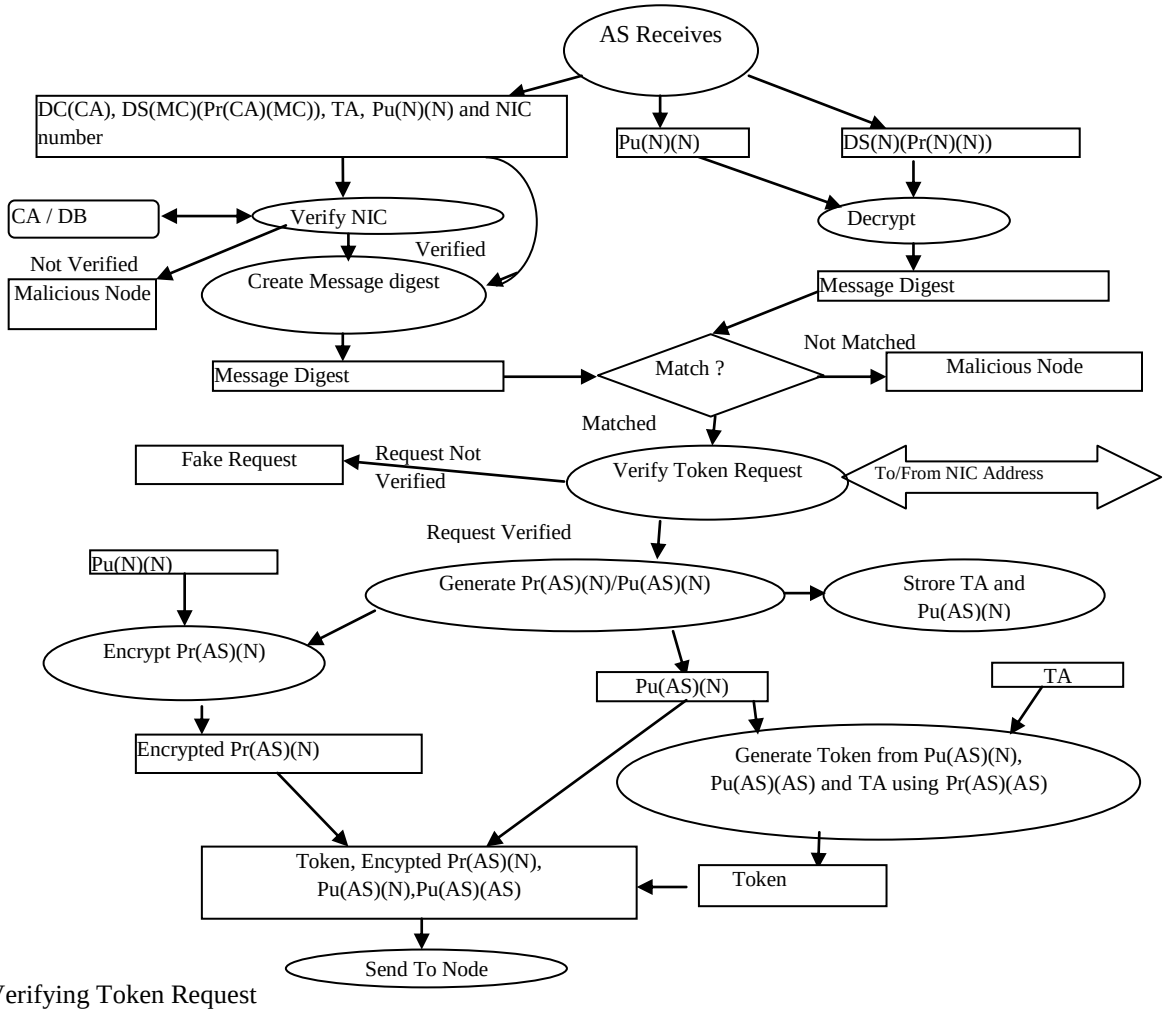

Figure 6. Working of AS

8.2.7. Verifying Token Request

It is essential to verify that ow t. AS then generates random number and encrypt it with Pr(AS)(AS). This encrypted number is again encrypted with public key of requester node Pu(N)(N) and sent to requester's NIC number address along with Pu(AS)(AS). After receiving this message from AS, requester node decrypts this message with its private key Pr(N)(N) and again decrypts it with Public key of AS Pu(AS)(AS) , to get actual random number sent by AS. This random number is now encrypted firstly with public key Pu(AS)(AS) of AS and then with private key of requester Pr(N)(N) and sent to AS. AS Decrypts encrypted number firstly with Public key Pu(N)(N) and then with Private key Pr(AS)(AS),to get the number sent by requester. The Matching of Number sent by AS and number received from requester validates that request is authentic. The message passing in this process is shown in figure 7.

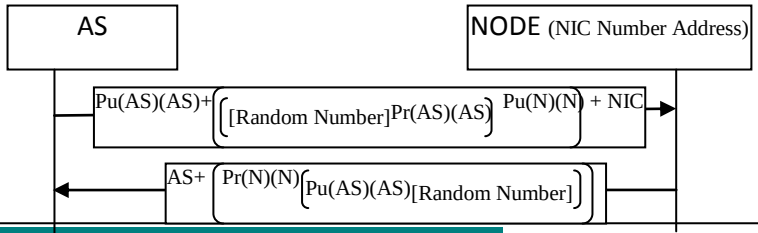

Figure 7. Authentication of Token

8.2.8. 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, as shown in figure 6. This information is stored to reply any request made by any node for verification of owner ship of Pu(AS)(N) of TA.

8.2.9. 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.

8.2.10. Message to claimant node from AS

The Token, Pu(AS)(N),Pu(AS)(AS), private Key Pr(AS)(N), encrypted with public key Pu(N)(N) are send to Node as shown in figure 8.

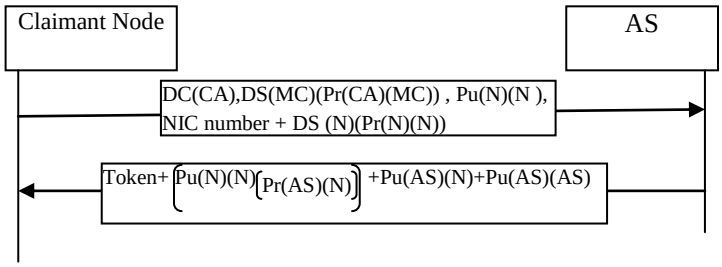

Figure 8. Message between Node and AS

8.2.11. 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.

8.2.12. Setup of Symmetric Keys between nodes

Once the node gets the AS Digital Certificate as token, node can proceed to setup Symmetric keys between nodes for secure communication. The token issued by AS is passed to receiver node, by sender's node. The Token containing TA and corresponding AS's certified public key is used for authentication of sender. After confirmation, receiver sends its token, other parameters and secret key, encrypted with public key Pu(AS)(N) of sender as shown in figure 9. Sender validates receiver in same way as receiver has validated sender and keeps this key secure. Now both the nodes have agreed on secret key and can communicate encrypted data using this secret key.

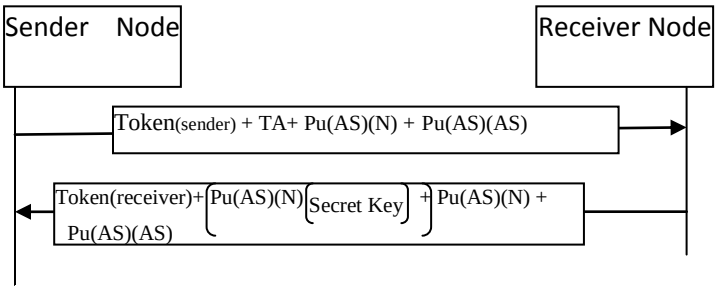

Figure 9. Message passing between Nodes

9. Conclusion

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 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]. This paper presented a method wherein no new node is allowed to enter the network until and unless it proves to be a non-malicious node. 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. Further, the verification of TA and corresponding certified Pu(AS)(N), restrict the node to go to AS for verification of sender every time. This will also increase the efficiency of network.

References

1) http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html
2) Ahmad AlSa'deh and Christoph Meinel;"Security Neighbor Discovery ";IEEE Security & Privacy MagazineCopublished by the IEEE Computer and Reliability Societies 1540-7993/12 ,July/August 2012. pp. 26-34
3) ByungGoo Choi1, JaeHyun Ryu 2, ChoongSeon Hong3, DongJin Kwak; International Conference on Computational Sciences and Its Applications ICCSA 2008; "Enhanced SEND Protocol for Secure Data Transmission in Mobile IPv6 Environment "
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) Amirhossein Moravejosharieh, Hero Modares and Rosli Salleh; "Overview of Mobile IPv6 Security " ;2012 Third International Conference on Intelligent Systems Modelling and Simulation; 978-0-7695-4668-1/12,2012 IEEE.
8) [8] Joseph Davies; Published By: Prentice Hall of India - 2008; "Understanding IPv6"; Second Edition; ISBN: 978-81-203-3463-2.