SHIV SHAKTI

International Journal of in Multidisciplinary and Academic Research (SSIJMAR)

Vol. 4, No. 3, June 2015 (ISSN 2278 – 5973)

Removing Security Issues Of Ipv6 Using Diffie Hellman Algorithm

Manjeet

M.Tech. Scholar, Deptt. Of ECE, S (PG) I T M, Rewari

Impact Factor = 3.133 (Scientific Journal Impact Factor Value for 2012 by Inno Space Scientific Journal Impact Factor)

Global Impact Factor (2013)= 0.326 (By GIF)

Indexing:

ABSTRACT

The default method for IPv6 address generation uses an Organizationally Unique Identifier (OUI) assigned by the IEEE Standards Association and an Extension Identifier assigned by the hardware manufacturer (RFC 4291). For this reason a node will always have the same Interface ID (IID) whenever it connects to a new network. Because the node's IP address does not change, the node will be vulnerable to privacy related attacks. Currently this problem is addressed by the use of two mechanisms that do not use MAC addresses or other unique values for randomizing the IID during its generation: Cryptographically Generated Addresses (CGA) (RFC 3972) and Privacy Extension (RFC 4941). The problem with the former approach is the computational cost involved in the IID generation and, more importantly, the verification process. The problem with the latter approach is the lack of necessary security mechanisms and that it provides the node with only partial protection against privacy related attacks. To enhance the security in the IPV6 address we use well known cryptographic algorithm called Diffie Hellman.

INTRODUCTION

The world of technology continues to grow larger and broader every single time. Thus, it is crucial for an enterprise to start deploying IPv6. However, some critical issues regarding security occurred in IPv6 deployment. Thus enterprise network exposed to more threats and attacks when they deploys IPv6. When threats increase, then the risks will increase.

IPV6 was firstly introduced by IETF (Internet Engineering Task Force) in mid 1990's. IPV6 is a next generation protocol that tries to overcome the problems due to IPV4. IPV6 provides 128-bit address space that is 3.4*(10)^38 addresses. This address space is very large(its in trillions in trillions). As we all are aware of the use of internet enable resources worldwide so the need of IP addresses are increasing day by day. That results in the deployment of IPV6. Because the addresses provided by IPV4 are only 4,294,967,296 (4 billion) and have been used almost. Several experts forecast that IPV4 will be finished completely in upcoming years because of insufficient addressing space so the migration from IPV4 to IPV6 is necessary to meet the requirement of future network[1].

As we are trying to migrate from IPV4 to IPV6,there are some security issues that arise. Some are due to IPV4 and some are due to IPV6. Firstly we will define the features of IPV6, secondly identify the vulnerabilities due to IPV6 and then use some technologies to remove those vulnerabilities.

SECURITY ISSUES OF IPV6

There are lots of security risks and threats occur in the deployment of IPV6 protocol. These vulnerabilities can be defined as [4], [5]-

1. Reconnaissance attack - Attackers may get information about host and network devices and their interconnection in the targeted network by using two methods- ACTIVE and PASSIVE methods. In the active method intruders do scanning of the data and in the passive method they fetch the essential data about the enterprise network[2] .

2. Extension Header - Long chain of headers make a security device difficult to do deep packet inspection in the transport layer header and will increase as the malicious node will fragment the packet into very small size. Thus it will force the security device to reassemble those small packets before inspection[3].
3. Denial Of Service(DoS) Attack - As intruders split the packets into small size of fragments so it will send large number of fragments to the target system until it become overload and crash the system.
4. Malicious router - As IPV6 use SLAAC for autoconfiguration of IP address so a malicious router may decide to serve as a legitimate router and misguides the packets in the network.
5. Failure of DAD and NUD processes - A malicious router may falsely respond to DAD (DuplicateAddress Detection)and prevents new nodes to join the linkthus results in false NUD (Neighbour Unreachability Detection)[4].
6. ICMPV6 related attacks - ICMPV6 send error notification to multicast address thus intruders may misuse it by sending a certain packet to multicast address. And it will cause multiple responses and may impose DoS attacks.

PROPOSED METHOD

We introduce the simple solution with the less over head and it's very difficult almost impossible for the intruder to break the security of the network. First we are generating the random IP addresses of all the nodes, for the encryption of IP address, we use Diffe Helman algorithm and generate the unique IPV6 address which is not recognizable by the attacker.

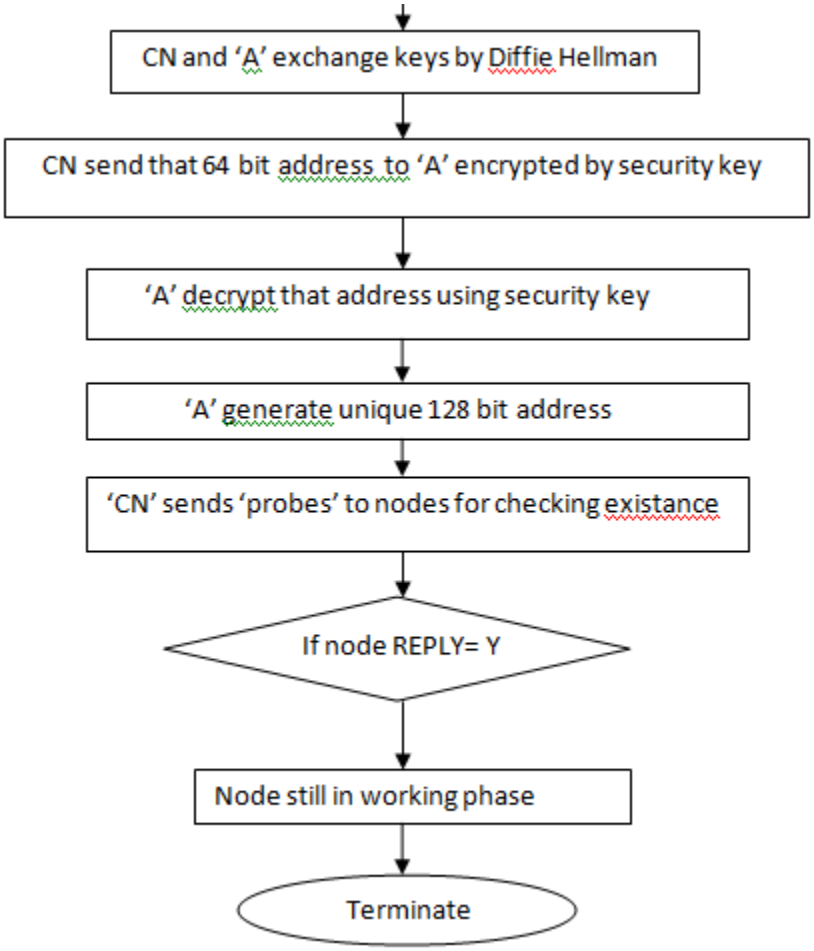
IPV6 address is of 128 bit. 128 bit IPV6 address contains 64 bit MAC address and 64 bit IP address.

First, we break this 128 bit address into 64 bit MAC address and 64 bit IP address as MAC address is same but the IP address is different for every node.

Second, then we apply diffie hellman algorithm on 64 bit IP address and make encrypted text.

Third, now we combine 64 bit MAC address and 64 bit encrypted IP and make unique 128 bit IP address.

Fourth, now this address is forward over network and make the network secure.



CONCLUSION

As it is known that privacy is an important issue in present time because of number of attacks in the network. So the best method for securing a network is generating random interface identifier so that intruders can not track the IP address easily and data can be secured. Methods for generating random ID are CGA, Privacy Extension Method and SSAS. Here some techniques in which EUI-64,CGA and Privacy Extension has limitation and some are gud enough like SSAS and i-SeRP. SSAS takes less time to remove the vulnerabilities in comparison to CGA.But still SSAS has limitation because it takes a long computational time for processing. while i-SeRP calculate the risk value and then decide to use right model to counter the risks. In the proposed solution as 128 bit unique address is generated so it will prevent the malicious nodes to enter in the network and make the network secure. Because in the proposed work 'certification authentication' is used for preventing malicious node. And secrets will be exchanged by 'Diffie hellman Key Exchange Algorithm'. And to know the existence of malicious nodes, periodically challenges will be send.So it is more secure than other described method.

REFERENCES

[1] Vineeth. M.V, Rejimoan.R, "Evaluating the performance of IPV6 with IPV4 and its distributed Security Policy",(ICT 2013).

[2] Ali ,W.N.A.W,et. Al Distributed policy for IPV6 deployment in sustainable energy & environment (ISESEE)2011.

[3] Durdagi E. and A. buldu IPV4/IPV6 security and threat comparison. Procedia- Social and Behavioral Science,2010.

[4] Chao, H. C.,sttuttgen, H.J.,wattington,D.G.,"IPV6: The Basics For The next generation Internet", IEEE communication Magazine,2004.

[5] Abdur Rahim chaudhary,"In-depth analysis of IPV6 security Postures",IEEE 2009.

[6] Hosnieh Rafiee, Christoph Meinel, "SSAS: A Simple Secure Addressing Scheme for IPv6Autoconfiguration" 2013 Eleventh Annual Conference on Privacy, Security and Trust (PST)