Available online at www.ijsrnsc.org

IJSRNSC

Volume-5, Issue-3, June 2017
Research Paper

Int. J. Sc. Res. in
Network Security
and Communication

ISSN: 2321-3256

www.ijsrnsc.org

Security Enhancement of IPV6 Using Advance Encryption Standard and Diffie Hellman

Mohammad Amjad

Dept. of Computer Engineering, Faculty of Engineering and Technology, Jamia Millia Islamia, India

Corresponding Author: mamjad@jmi.ac.in, Tel.: 011-2698-0281

Received 18th May 2017, Revised 30th May 2017, Accepted 26th Jun 2017, Online 30th Jun 2017

***Abstract*:** The internet protocol version 6 was developed to extend and eventually replace IPV4s capabilities but it poses several significant security issues. The stress in this paper is to identify the vulnerabilities that come in IPV6 and how to remove those vulnerabilities. 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. For this reason a node will always have the same Interface ID whenever it connects to a new network. Because the nodes IP address does not change, the node will be vulnerable to privacy related attacks. To remove this issue along with other vulnerabilities I will use a mechanism that randomizing the interface ID during its generation and more importantly, the verification process. The interface ID is also enciphered by using Advance Encryption Standard (AES). To enhance the security cryptographic algorithm Diffie Hellman for authentication and AES algorithm for encryption and decryption process is used both for the address of IPV6 as well as the message generated by the sender and receiver using the services of IPV6. In the proposed method both the combination of AES and Diffie Hellman is used to ensure authenticity and remove susceptibility. The proposed method is implemented in C# on .NET platform to realize the method.

Keywords: IPV6, Randomized Interface ID, AES, Diffie Hellman, Datagram, SLAAC, Duplicate address.

Nomenclature: AES (Advance Encryption Standard), DoS (Denial of Service), CN (Content Node), OUI (Organizationally Unique Identifier), SLAAC (Stateless Address Auto Configuration), IID (Interface Identifier), CGA (Cryptographically Generated Addresses), EUI (Extended Unique Identifier), NS (neighbor solicitation), CBID (Crypto-Based Identifiers), MD5 (Message Digest five), DAD (Duplicate Address Detection).

I. INTRODUCTION

IPv6 is an Internet layer protocol used for assigning network addresses to communicate with devices across the Internet. IPV6 was firstly introduced by IETF (Internet Engineering Task Force) in mid-1990. 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 (it’s 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.

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. The IP address is formed by the combination of the subnet prefix and the Interface ID (IID). The subnet prefix composes the 64 leftmost bits of the IPv6 address. For public addresses it is obtained from a router via router advertisement messages. The IID composes the 64 rightmost bits of the IPv6 address. 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 and then use some technologies to remove those vulnerabilities. Then the new method is proposed for the removal of vulnerabilities. SLAAC (Stateless Address Auto Configuration) is an unique feature of IPV6 for generating IP addresses automatically for large organizations [6]. It does not need any human intervention. As soon as a node joins a network, it configures its IP address. Thus it works in a Plug and Play fashion. It is used with other mechanism ND (Neighbor Discovery) to discover their neighbor routers and hosts. ND and SLAAC together can be termed as NDP (Neighbor Discovery Protocol). By using NDP, nodes on the network may get the information about the routers and process DAD (Duplicate Address Detection) [3]. In the network, communication between nodes takes place by exchanging messages, router solicitation (RS) message, router advertisement (RA) message and neighbor solicitation (NS) message [3][4]. When a host joins a network, it sends a RS message to the router and then router reply by sending RA message containing their prefix. To avoid conflicts on the network host processes DAD (Duplicate Address Detection) [6] by sending NS message. Organization of remainder of the research work is organized as follows. Section II is about the related works and recent findings in this field. Section III is describes about different techniques to remove vulnerabilities in the next generation IP. Section IV presents insight into the proposed method and describes about the algorithm used. Section V introduces the different actions on the proposed method by generating the symmetric key and verification method. Section VI deals about performance of the proposed method and simulation results. Section VII concludes the research work and focuses on findings also.

II. RELATED WORK

In the year 2013, Hosnieh Rafiee and Christoph Meinel [3] presented that 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. This document proposes the use of a new algorithm in the generation of the IID to reduce computational cost while, at the same time, securing the node against some types of attack, like IP spoofing. These attacks are prevented by the addition of a signature to messages sent over the network and by direct use of a public key in the IP address.

In the research paper of Emre Durda and Ali Buldub find and analyses that IPV6 and IPV4 threat happens on two stages. First part focuses on the attacks with IPV4 and IPV6 similarities. Second part is focuses on the attacks with new considerations in Ipv6.

Clause Castelluccia, Gabriel Montenegro, Julein Laganier and Christophe Neumann presented an opportunistic encryption scheme strictly layered on top of IPv6, assuming that a node needs to send data toward another node. The main contribution of this paper is to propose a solution that is fully distributed and does not rely on any global Trusted third Party (such as DNSSEC or a PKI). The IPsec gateways are discovered using IPv6 anycast, and they derive authorization from authorization certificates and Crypto-Based Identifiers (CBIDs). The result is a robust and easily deployable opportunistic encryption service for IPv6.

Stefen Hermann and Benjamin Fabia revels that The next generation of the Internet Protocol (IPng) is currently about to be introduced in many organizations. However, its security features are still a very novel area of expertise for many practitioners. This study evaluates guidelines for secure deployment of IPv6, published by the U.S. NIST and the German federal agency BSI, for topicality, completeness and depth. The later two are scores defined in this paper and are based on the Requests for Comments relevant for IPv6 that were categorized, weighted and ranked for importance using an expert survey. Both guides turn out to be of practical value, but have a specific focus and are directed towards different audiences. Moreover, recommendations for possible improvements are presented. Our results could also support strategic management decisions on security priorities as well as for the choice of security guidelines for IPv6 roll-outs.

Hyungon Kim and Jong Hyouk Lee [8] proposes a Diffie-Hellman key based authentication scheme that utilizes the low layer signaling to exchange Diffie-Hellman variables and allows mobility service provisioning entities to exchange mobile node's profile and ongoing sessions securely. By utilizing the low layer signaling and context transfer between relevant nodes, the proposed authentication scheme minimizes authentication latency when the mobile node moves across different networks. In addition, thanks to the use of the Diffie-Hellman key agreement, pre-established security associations between mobility service provisioning entities are not required in the proposed authentication scheme so that network scalability in an operationally efficient manner is ensured. To ascertain its feasibility, security analysis and performance analysis are presented.

III. TECHNIQUES TO REMOVE THE VULNERABILITIES IN IPV6

There are a number of technologies already exist which try to solve the security issues that arise in the network by using IPV6. Some techniques analyzes what type of router should be used so that less security issues arise and some try to use different types of algorithms to reduce those security issues.

III.I UI-64 Method:

Standard method of generation of IP interface IDs (IID) is Extended Unique Identifier (EUI-64) i.e. offered by IEEE Standard Association [6]. EUI-64 is the combination of OUI (Organizationally Unique Identifier) assigned by IEEE RSA and the extension identifier assigned by hardware manufacturer. Limitation of this approach is that it generates same IID whenever a node joins a network. So it makes intruders easy to track the node.

III.II CGA (Cryptographically Generated Addresses)

In this method a cryptographic public key is attached with IPV6 address in SeND (Secure Neighbor Discovery) protocol to generate random interface IDs. The resulted IPV6 address is called CGA [9]. For security point of view corresponding private key is then be used to sign message sent from the addresses. In this interface identifier is generated by computing a cryptographic hash function from public key and auxiliary parameters. CGA is the concatenation of modifier, subnet prefix, collision count, public key and optional extension fields. CGA is computed by using 9 step algorithm defined in rfc-3972 and can be verified by re-computing the hash value and by comparing the hash value with identifier. CGA prevents spoofing and stealing of existing IPV6 addresses. First limitation of this technique is that protection works without a certification authority. So an attacker can create a new address from an arbitrary subnet prefix and its own public key. Second limitation is that there is no method to prove that the address is not CGA so an attacker can take anyone's CGA and present it as a non-CGA.

III.III Privacy Extension Approach:

This is another method of randomly generating IIDs. In this interface identifier is derived from IEEE identifier. By using this identifier a node can generate a global scope address that changes over time. Thus it make difficult eavesdropper and other intruders to identify the addresses as different addresses are used in different transaction. It uses two methods for the generation and maintenance of randomize interface identifier. First in the presence of stable storage and second in the absence of stable storage. When stable storage is present it assumes the presence of 64-bit "history value" i.e. used as an input to generate the random IID using MD5 algorithm. When a system boots first time a random value should be generated and saved to the history for the next iteration of the algorithm. When stable storage is absent In this it uses configuration information like user identity, security key, and serial number to generate some data bits and append some random data and compute the MD5 digest as before. In this ingress filtering is used to prevent the use of spoofed the source address in the distributed DoS attacks. Limitation of this approach is that it prevents privacy related issues but not security related issues.

IV. PROPOSED METHOD

I introduces the simple solution with the less overhead and it's very difficult almost impossible for the intruder to break the security of the proposed network. In the proposed solution IP addresses will be fetched by SLAAC. For node authentication and key generation I use Diffie Hellman algorithm and it will generate the unique IPV6 address which is not recognizable by the attacker. For the encryption of IP address and the messages I will use AES algorithm which is a private key cryptography.

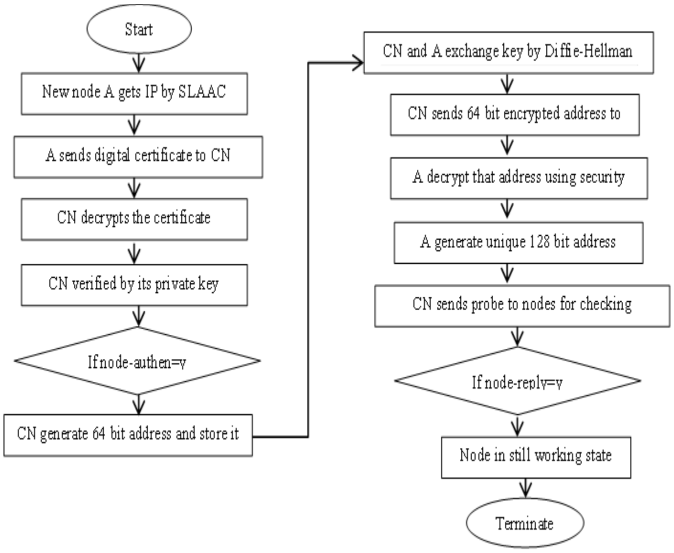

Start
New node A gets IP by SLAAC
A sends digital certificate to CN
CN decrypts the certificate
CN verified by its private key
If node-authen=y
CN generate 64 bit address and store it
CN and A exchange key by Diffie-Hellman
CN sends 64 bit encrypted address to
A decrypt that address using security
A generate unique 128 bit address
CN sends probe to nodes for checking
If node-reply=y
Node in still working state
Terminate

Figure 1: Flow chart of proposed method

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

- First, there is to 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 Diffie Hellman algorithm and AES algorithm is applied on 64 bit IP address and make encrypted text.
- Third, now I will 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.

1. The IP address is to be obtained by node A using Stateless Address Auto Configuration (SLAAC).
2. In the first step, both the parties will agree upon a shared symmetric key, initiator and responder both of them exchange the keys i.e. node A and the content node CN.
3. The first packet is sent from A to CN for verification in the form of digital certificate.
4. The certificate is decrypted by CN for further reference.
5. The node verification is performed and authenticated.
6. CN generates 64 bit valid pattern and update it in database.
7. The second packet is sent from the remote endpoint back to the A, this packet will be the exact same information matching the crypto suit policy sent by the A.
8. The third packet is sent from the initiator to the remote endpoint, this packet contains the key and nonce payload.
9. This fourth packet as we would expect comes from the remote endpoint back to initiator and contains the remote endpoints key exchange and Nonce payload.
10. The fifth packet is from the initiator back to the remote endpoint with a function which contains the nonce of A , nonce of CN, share secret key and Diffie-Hellman key. A secret key also contain the identity of initiator.
11. The sixth packet is from the remote endpoint to the initiator contains the corresponding key exchange.
12. If the node verifies it, then reply it with yes and indicates that it is still in working mode and finally the address generation and encipherment of address as well as message is generated using AES.

V. KEY GENERATION AND VERIFICATION USING DIFFIE HELLMAN:

1. User A selects a random $\Upsilon \in Z_q^*$, where gcd (Υ, p − 1) = 1 and computes g′ = (g * Υ) mod p. Then, user A sends g′ to user B.

2. After receiving g′, B selects a random $k_B \in Z_q^*$, computes $r_B = g^k{}_B$ mod p, and sets e = Hash ($g'^k{}_A$) mod p and s_B = (xe + k_A) mod q. B then sends (r_B, s_B) to A. The pair (r_B, s_B) is a delegation proxy certification for proving that B delegates his signing capacity to A.

3. After the reception of the pair (r_B, s_B), A computes e'= Hash ($r^{\Upsilon}{}_B$) mod p and verifies the validity by checking if $r_B = g^s{}_B * y^{-e'}$ mod p.

4. If the equation $r_B = g^s{}_B y^{-e'}$ mod p holds, then A sets s_A = (s_B * Υ^{-1})mod q as a proxy key, sets (s_A, $g^s{}_A$ mod p) as public key pairs and sends the certificate request to the registration authority R_B.

5. According to certificate policy, R_B identifies user A and then forwards the certificate request to the certificate authority C_B for signing proxy certificate. 6. The key generated at both the end viz. sender A and receiver B should be able to verify the key for further communication.

7. The process of key generating and verification mechanism is shown in figure 2.

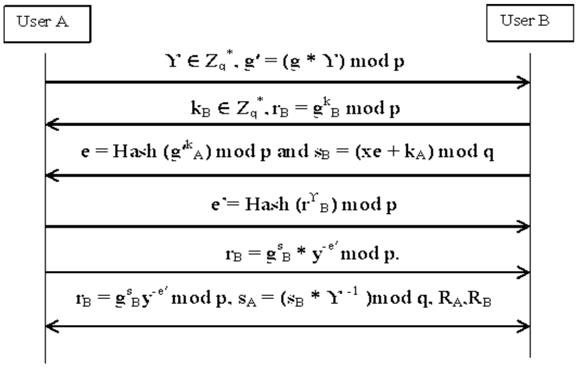

User A
User B
$\Upsilon \in Z_q^*$, $g' = (g * \Upsilon) \bmod p$
$k_B \in Z_q^*$, $r_B = g^k{}_B \bmod p$
$e = \text{Hash}(g'^k{}_A) \bmod p$ and $s_B = (xe + k_A) \bmod q$
$e' = \text{Hash}(r^{\Upsilon}{}_B) \bmod p$
$r_B = g^s{}_B * y^{-e'} \bmod p.$
$r_B = g^s{}_B y^{-e'} \bmod p$, $s_A = (s_B * \Upsilon^{-1}) \bmod q$, R_A, R_B

Figure 2: Key generation and verification process

VI. SIMULATION AND RESULTS:

For the purpose of showing the results, a module of program is written in .net platform and screenshot is taken of the final outputs. We can see in the figure 3 that how the IPV6 packets are captured and in the figure number 4 the set of keys are generated using AES of the size of 128 bits long. In the next stage it can be found that duplicate nodes are detected if any using the authentication procedure of Diffie-Hellman.

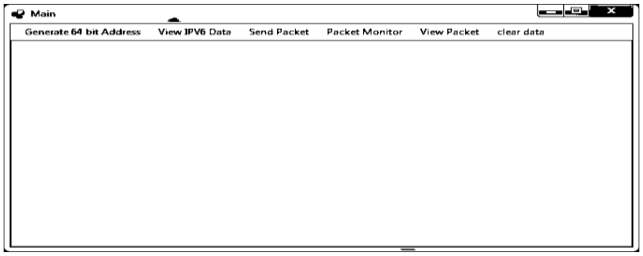
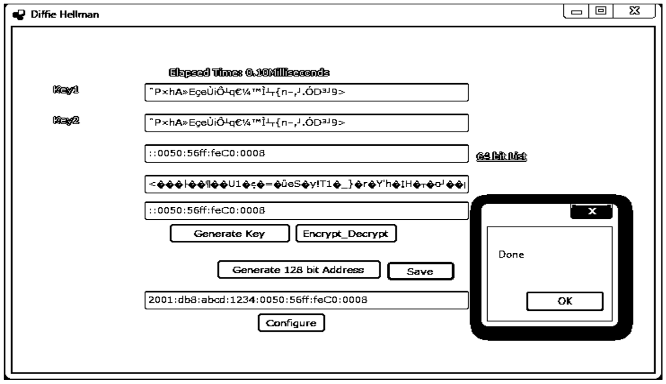


Figure 3: Front page to capture and deliver the packet

If the nodes are the authenticated then we will have the ciphering of the message as well as detection of malicious node if not found in the list of verified node. In the figure 3, code for the packet generation and then the packet capturing is shown by the CN. In the figure 4, the generated packet is encrypted using AES- using 128 bits



Elapsed Time: 0.10Milliseconds

Key1 ˆP×hA»EçeÙiÔ┤q€¼™Ì┴┬{n–,┘.ÓD³┘9>

Key2 ˆP×hA»EçeÙiÔ┤q€¼™Ì┴┬{n–,┘.ÓD³┘9>

::0050:56ff:feC0:0008

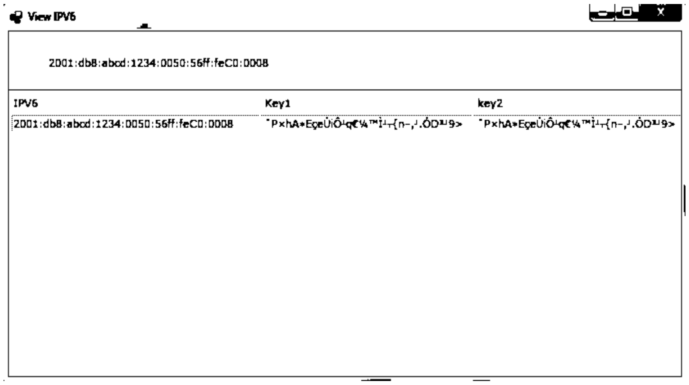
<���|��¶��U1�ç�=�ûeS�y!T1�_}�r�Y'h�ıH�┬�o┘��|

::0050:56ff:feC0:0008

2001:db8:abcd:1234:0050:56ff:feC0:0008

Done

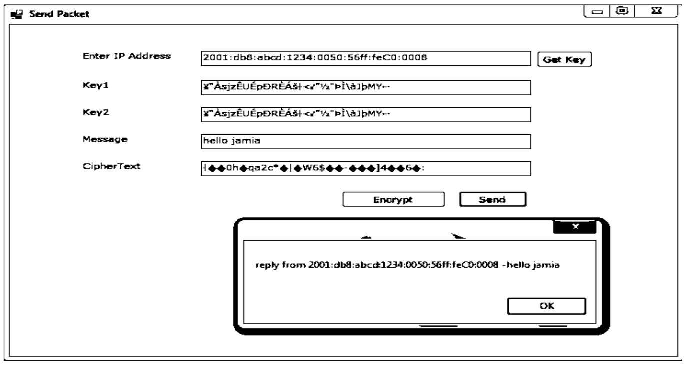
Figure 4: Encrypted key generated of the size of 128 bit



2001:db8:abcd:1234:0050:56ff:feC0:0008

IPV6	Key1	key2
2001:db8:abcd:1234:0050:56ff:feC0:0008	ˉPxhA∗EçeÙiÔ┘q€¼™Ì┴┬{n-,┘.ÓD╨9>	ˉPxhA∗EçeÙiÔ┘q€¼™Ì┴┬{n-,┘.ÓD╨9>

Figure 5: Detection of duplicate addresses



Enter IP Address: 2001:db8:abcd:1234:0050:56ff:feC0:0008

Key1: ¥"ÅsjzÊUÉpÐRÈÁš|<«"½"ÞÌ\àJþMY←

Key2: ¥"ÅsjzÊUÉpÐRÈÁš|<«"½"ÞÌ\àJþMY←

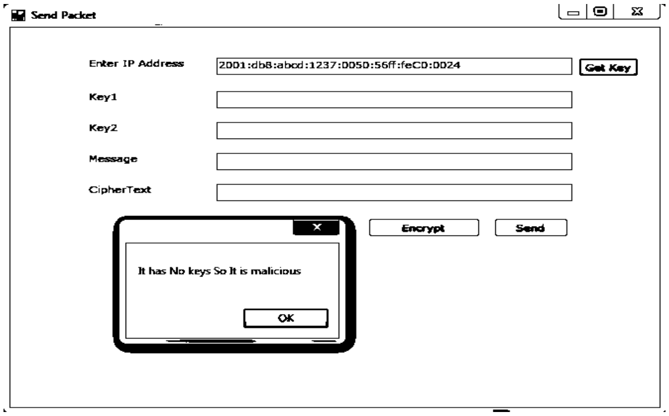
Message: hello jamia

CipherText: |◆◆0h◆qa2c*◆|◆W6$◆◆-◆◆◆]4◆◆6◆:

reply from 2001:db8:abcd:1234:0050:56ff:feC0:0008 -hello jamia

Figure 6: IPV6 address encryption

In the figure 5, we can now observe that after key generation and verification by Diffie-Hellman, whenever any address is found duplicate then it is reported. Then the address is encrypted using AES- 128 to ensure the authenticity and is shown in figure 6. In the figure 7 we may observe that after running the entire module simultaneously, the malicious node if any is to be find out.



Enter IP Address: 2001:db8:abcd:1237:0050:56ff:feC0:0024

It has No keys So It is malicious

Figure 7: Malicious Node Detected

Finally if any malicious node is found it is to be detected for the guaranteed removal of vulnerability.

VII. CONCLUSION AND FUTURE SCOPE

As we know that privacy is an important issue in present time because of the number of attacks increasing day by day in the network. So the best solution for securing a network from being tracked by an attacker is to change the node's IP frequently and by generating the random IID each time a node wants to generate a new IP address. So that intruders cannot track the IP address easily and data can be secured. There are two methods for generating random ID are CGA and Privacy Extension. But in these methods there are some limitation and issues like risk value and long computation time respectively. 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. In the proposed work, certification and authentication is used for preventing malicious node and secrets will be exchanged by Diffie Hellman Key Exchange Algorithm. To know the existence of malicious nodes, periodically challenges will be sending and also data or messages are encrypted by AES algorithm. So it is secure enough to give the security in the IPV6 network.

With the assumptions of limited number of nodes is successfully tested. But the test I did went smoothly and I had no problem, except for the fact that the suggested method is running on local network only. It may be tested for the Internet also.

REFERENCES

[1] M. Rostanski, M.; T. Mushynskyy, "Security Issues of IPv6 Network Autoconfiguration". In Proceedings of the 12th International Conference on Computer Information Systems and Industrial Management Applications (CISIM 2013), Krakow, Poland,; Springer: Heidelberg, Germany, 2013; pp. 218–228, 25–27 September 2013.

[2] R. AlJaafreh; J.Mellor ; M. Kamala.; B. Kasasbeh, "Bi-directional Mapping System as a New IPv4/IPv6 Translation Mechanism". In Proceedings of the Tenth International Conference on Computer Modeling and Simulation (UKSIM08), Cambridge, UK, IEEE Computer Society: Los Alamitos, CA, USA, 2008, pp. 40–45. 1–3 April 2008

[3] C. Medaglia and A. Serbanati, "An overview of privacy and security issues in the Internet of things," In Proceedings of the 7th International Conference on The Internet of Things. New York, NY, USA: Springer-Verlag, 2010, pp. 389–395, 04th Jan 2010.

[4] S. Raza, S. Duquennoy, J. Hoglund, U. Roedig, and T. Voigt, "Secure communication for the Internet of Things—A comparison of link-layer security and IPsec for LoWPAN" International Journal of Security and Communication Network", vol. 7, no. 12, pp. 2654–2668, Dec. 2014.

[5] Simone Cirani , Gianluigi Ferrari and Luca Veltri, "Enforcing Security Mechanisms in the IP-Based Internet of Things: An Algorithmic Overview" International Journal of Algorithm, Vol. 6, pp-197-226, February 2013.

[6] M. Brachmann, S. Keoh, O. G. Morchon, and S. S. Kumar, "End-to-end transport security in the IP-based Internet of things," In Proceedings of the 21st International Conference on Computer

and Communication. Network., 2012, pp. 1–5, 30th July -02 Auguts 2012.

[7] Tatipamula M. Grossetete P. Esaki H. "IPv6 Integration and Coexistence Strategies for Next-Generation Networks" IEEE Communications Magazine Vol. 42 No. 1 pp. 88-96, January 2004.

[8] Y. Qiu, J. Zhou, F. Bao, "Protecting All Traffic Channels in Mobile IPv6 Network", IEEE Wireless Communications and Networking Conference 2004 (WCNC 2004), Atlanta, pp- 160-165, 21-25 March 2004.

[9] Varsha Alangar, Anusha Swaminathanm, "Ipv6 Security: Issue Of Anonymity", International Journal Of Engineering And Computer Science IJECS, Volume 2 Issue 8 pp. 2486-2493, August, 2013

[10] Gelogo, Y. E. Caytiles, R. D. Park, B. "Threats and Security Analysis for Enhanced Secure Neighbor Discovery Protocol (SEND) of IPv6 NDP Security", International Journal of Control and Automation, Vol. 4, No. 4. PP:179-184, December, 2011.

[11] M. Amjad, Wireless Network Security: Susceptibility, Extortion and Kiosk" International Journal of Computer Science and Engineering IJCSE, Volume-I , Issue-3, ISSN: 2347-2693,. pp 10-14, November 2013

[12] Harsh Bhasin , Neha Kathuria, *"*Cryptography Automata Based Key Generation*",* International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.2, pp.15-17, June 2013.

[13] W. Stallings, "Cryptography and Network Security": Principles and Practice, 3rd ed., Prentice Hall Print.,2003, India, pp 596-625

[14] Bruce Schneier, "Applied cryptography: Protocol and Algorithm", 2nd Edition Wiley publication 2012, India, pp- 299-358

[15] Kaufman, c., Perlman, R., and Speciner, M., "Network Security, Private Communication in a public world", 2nd ed., Prentice Hall Print, 2002. India, pp 252-315.

[16] Behrouz A Forouzan, "Cryptography and Network Security", 2nd Edition McGraw Hill 2010, pp- 507-531

Author Profile

Dr. Mohammad Amjad has obtained his B.Tech. degree in Computer Engineering from Aligarh Muslim University Aligarh. He obtained his M. Tech. degree in Information Technology from IP University New Delhi and Ph.D. in Computer Engineering from Jamia Millia Islamia New Delhi. Dr. Mohammad Amjad is currently working as Assistant professor in the department of Computer Engineering, Faculty of Engineering & Technology, Jamia Millia Islamia (Central University) New Delhi. He has the four years industry experience and 15 years of teaching experience. He contributed thirty research papers published in various reputed journals, National and International conferences in India and abroad including the Countries like USA and China. He is actively involved in research and development activities in areas of MANET, WSN, Mobile Computing and Network Security systems.