IPV6 SECURITY OVERVIEW AND IMPROVEMENT USING DIFFIE HELLMAN

[1]Minhaj Alam Fatmi, [2]Kavita Dagar

[1]M.Tech. CSE (FCEM), [2]Assistant Professor CSE, H.O.D (FCEM)
[1]Department of Computer Science and Engineering (FCEM),
[1]M.D.University, Faridabad, India.

Abstract : The current Internet version has a number of security problems. The Internet lacks effective privacy and effective authentication mechanisms beneath the application layer. The internet protocol version 6 (IPv6) which is also called internet protocol next generation (IPNG), remedies these shortcomings by having two integrated options that provide security services and improve the level of reliability. The first option is called the Authentication Header (AH) which provides authentication and data integrity and the second options is called the Encapsulating Security Payload (ESP) which provides data integrity and confidentiality to IPv6 datagrams. These both are defined as extension header in IPv6.The internet protocol (IPv6) was developed to extend and eventually replace IPv4'scapabilities but it poses several significant security issues. The emphasis 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 (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. To remove these issue along with other vulnerabilities (Reconnaissance attack, Extension Header, Denial Of Service (DoS) Attack, Malicious router, Failure of DAD and NUD processes) by the use of mechanism that randomizing the IID during its generation and more importantly, the verification process, but it is the lack of necessary security mechanism and it provides the node with only partial protection against privacy related attacks. In this proposed method to improve the security, I am using cryptographic algorithm called Diffie Hellman (for authentication) and AES algorithm (for encryption and decryption).

***IndexTerms* - IPv6, Security issues of IPv6, IPsec, Randomized Interface ID, Extension Header, Security improvement of IPv6, Deffie Hellman, EUI-64, AES, Datagram.**

I. 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 deploy IPv6. When threats increase, then the risks will increase. 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'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 (it is in trillions in trillions). As we all are aware of the use of internet enable resources worldwide so the need of IP addresses is 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 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. During the design of IPv6 the IETF took the opportunity to make further improvements above and beyond providing extra addressing space which makes IPv6 extensible and highly adaptable to future requirements.

In shorts, technically the main features of IPv6 are:

- Efficient and Extensible IP datagram.
- Large address space / Expand addressing capabilities.
- Server-less auto-configuration (Plug-N-Play) & reconfiguration.
- More efficient and robust mobility mechanisms.
- IPv6 uses IPSec mandatory.
- Efficient and hierarchical addressing and routing infrastructure.
- Stateless (Router Advertisement) and stateful (DHCPv6) address configuration (SLAAC).
- Built-in security, strong IP-layer encryption and authentication.
- Flow labeling (for QoS) capability.
- New protocol for neighboring node interaction.
- Extensibility

1.1 IPv6 Header Format

Version (4 bits)	Traffic Class Priority (4 bits)	Flow label (24 bits)
Payload Length (16 bits)	Next Header (8 bits)	Hop Limit (8 bits)
Source Address (128 bits)		
Destination Address (128 bits)		

Fig 1.1: Header Format of IPv6

Version (4-bits): It represents the version of Internet Protocol, i.e. 0110.
Traffic Class (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).
Flow Label (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media.
Payload Length (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.
Next Header (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's.
Hop Limit (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded.
Source Address (128-bits): This field indicates the address of originator of the packet.
Destination Address (128-bits): This field provides the address of intended recipient of the packet.

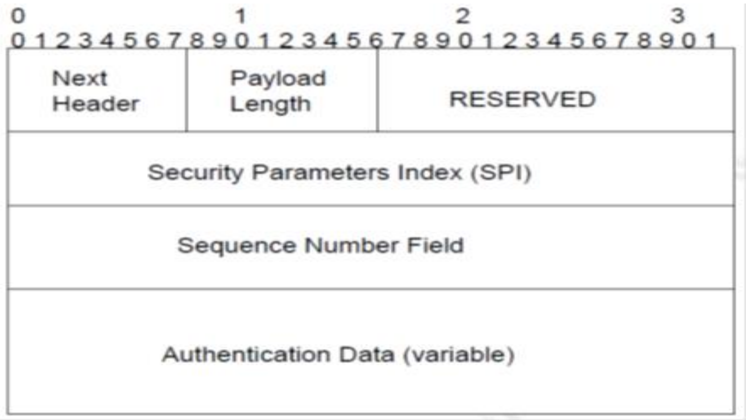
1.2 IPv6 Security Improvements

The IPv6 protocol is designed to ensure end-to-end security over a connection. The major addition is IPSec, which consists of a set of cryptographic protocols designed to provide security in data communications. The RFC4301 instead makes IPSec mandatory to use in IPv6 while it is optional in IPv4. IPv6 provides two security headers that can be used separately or together depends upon the different level of security need for different user.

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

1.2.1 Authentication Header (AH)

It is an extension header of IPv6 that provides authentication and data integrity for the entire IPv6 packet. Authentication means that if an endpoint receives a packet with a specific source address, it can be assured that the IP packet did indeed come from that IP address and Integrity means that if an endpoint receives data, the content of that data has not been modified along the path from the source to the destination. The extension supports many different authentication technics. The extension is algorithm independent. Authentication Header provides data-origin authentication and protection against replay attacks. A.H can prevent IP spoofing attacks.



```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

Next Header	Payload Length	RESERVED
Security Parameters Index (SPI)		
Sequence Number Field		
Authentication Data (variable)		

Fig 1.2: Authentication Header Format

1.2.2 Encapsulating Security Payload (ESP)

It is another extension header of IPv6 that provides integrity and confidentiality. ESP also delivers data-origin authentication, protection against replay attacks, and limited traffic flow confidentiality, as well as privacy and confidentiality through encryption of the payload. ESP is flexible and algorithm independent.

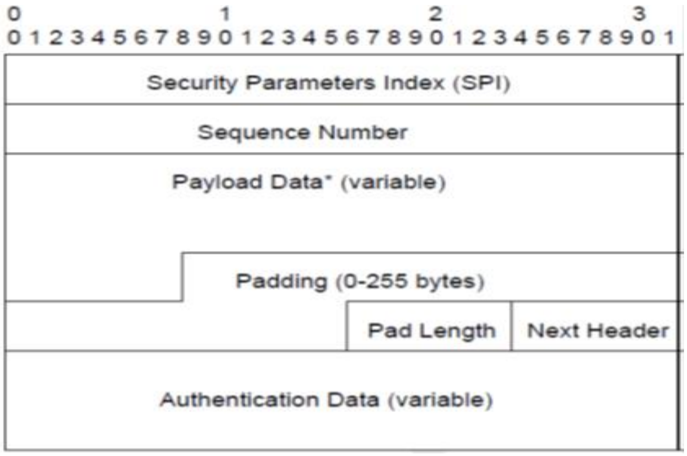


Fig 1.3: ESP Header Format

1.2.3 Neighbor Discover (ND)

ND (Neighbor Discovery) is the mechanism used to discover their neighbor routers and hosts. This is a network layer protocol, like IPv4 equivalents ARP and RARP. SLAAC (Stateless Address Auto Configuration) is a unique feature of IPV6 for generating IP addresses automatically for large organizations [6]. ND works very closely with address auto-configuration, which is the mechanism used by IPv6 nodes to acquire configuration information. 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) [16]. In the network, communication between nodes takes place by exchanging messages- router solicitation (RS) message, router advertisement (RA) message and neighbor solicitation (NS) message [17]. 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) [16] by sending NS message. Both ND and address auto-configuration contribute to make IPv6 more secure than its predecessor.

II. Literature Review

HOSNIEH RAFIEE, CHRISTOPH MEINEL IEEE-2013

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 (RFC4291). 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 (RFC4941). 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.

EMRE DURDA, ALI BULDUB

Internet using is increasing rapidly. Internet occurred as a result of communicating nodes with each. New internet users are joining to this structure and development of it is going on. In such a big structure, communication of two nodes is possible only if they find each other. Various addressing protocols have been developed to obtain this. The well-known is called Internet Protocol (IP). Currently IP is used IP Version 4 (Ipv4). IPv4 has limited address. This limited address does not meet the growth of Internet. Because of inadequate internet address, IP Version 6 (IPV6) was developed in 1995. IPv6 brings many enhancements. IPv6 was designed with security in mind. It is bringing security enhancements into modern IP network. This paper analyses IPv6 and IPv4 Threat Comparisons 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.

CLAUDE CASTELLUCCIA, GABRIEL MONTENEGRO, JULIEN LAGANIER AND CHRISTOPHE NEUMANN EL.AT.

This paper presents an opportunistic encryption scheme strictly layered on top of IPv6. Assuming that a node needs to send data toward another node, our proposal enables the dynamic configuration of an encrypted tunnel between the two nodes' IPsec gateways. 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 any cast, 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.

STEFFEN HERMANN AND BENJAMIN FABIAN EL.AT.

The next generation of the Internet Protocol (IPv6) 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 EL.AT.

Wireless communication service providers have been showing strong interest in Proxy Mobile IPv6 for providing network-based IP mobility management. This could be a prominent way to support IP mobility to mobile nodes, because Proxy Mobile IPv6 requires minimal functionalities on the mobile node. While several extensions for Proxy Mobile IPv6 are being developed in the Internet Engineering Task Force, there have been little attentions paid to developing efficient authentication mechanisms. An authentication scheme for a mobility protocol must protect signaling messages against various security threats, e.g., session stealing attack, intercept attack by redirection, replay attack, and key exposure, while minimizing authentication latency. In this paper, we propose 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. SECURITY ISSUE IN IPV6

There are many security risks and threats occur in the deployment of IPV6 protocol. These vulnerabilities can be defined as following:-

- **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.
- **Extension Header** - Long chain of headers makes 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
- **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.
- **Malicious router -** As IPV6 use SLAAC for auto configuration of IP address so a malicious router may decide to serve as a legitimate router and misguides the packets in the network.
- **Failure of DAD and NUD processes -** A malicious router may falsely respond to DAD (Duplicate Address Detection) and prevents new nodes to join the link thus results in false NUD (Neighbor Unreachability Detection).
- **Malware** - There is no particular implementation in IPv6 which will allow changing the classical approach to malware. However, worms that use the internet to find vulnerable hosts may find difficulties in propagation due to the large address space.
- **Sniffing** - This is the classical attack that involves capturing data in transit across a network. IPv6 provides the technology for the prevention of these types of attacks with IPSec, but it does not simplify the problems for keys management. For this reason, this technique can still continue to be practiced.
- **L7 Attacks** - Here we refer to all those types of attacks performed at Layer 7 of the OSI model. Also considering a worldwide adoption of IPSec, this type of attacks will remain almost unchanged. Buffer Overflow, Web Applications Vulnerability, etc., cannot be stopped through the IPv6 adoption. There is also another consideration: if IPSec will be implemented as a standard for communication between endpoints, all devices such as IDS/IPS, firewalls and antivirus will only see encrypted traffic, promoting this type of attacks.
- **Man-in-the-Middle** - The IPv6 is subjected to the same security risks that we may encounter in a man-in-the-middle attack that affects the suite of IPSec protocols.
- **Flooding Attacks** - A flooding attack is a Denial of Service (DoS) attack wherein the attacker sends a slew of SYN requests to a target's system in order to overwhelm the server and bring down the network / make it unresponsive to actual traffic. So, in short, it's exactly what it sounds like. The core principles of a flooding attack remain the same in IPv6.

TECHNIQUES TO REMOVE THE SECURITY THREAT IN IPv6

There are a number of technologies already exist which try to reduce 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. Here I am introducing some techniques:

- EUI-64 Method
- CGA(Cryptographically Generated Addresses)
- Privacy extension approach

IV. PROPOSED METHOD AND SOLUTION

I introduce the simple solution with the less overhead and it's very difficult almost impossible for the intruder to break the security of the network. In the proposed solution IP addresses will be fetched by SLAAC. For node authentication and key generation I will use Diffie Hellman algorithm and generate the unique IPV6 address which is not recognizable by the attacker. And for the encryption of IP address and the messages I will use AES algorithm. IPV6 address is of 128 bit. 128 bit IPV6 address contains 64-bit MAC address and 64 bit IP address. First, I will 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 I apply Diffie Hellman algorithm and AES algorithm on 64 bit IP address and make encrypted text. Third, now I 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. The proposed method will implement with a module of program written in .Net platform.

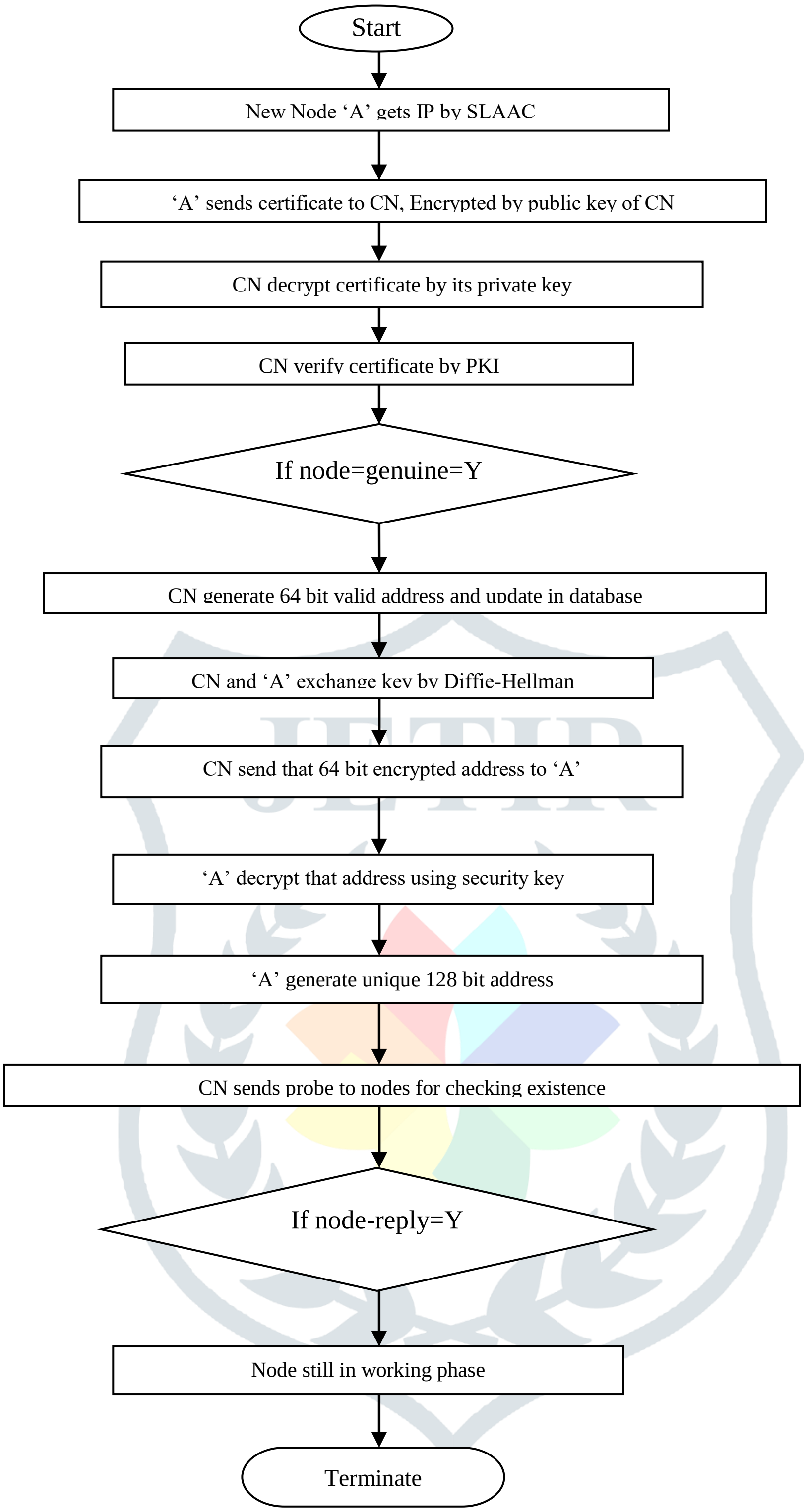

Start
New Node 'A' gets IP by SLAAC
'A' sends certificate to CN, Encrypted by public key of CN
CN decrypt certificate by its private key
CN verify certificate by PKI
If node=genuine=Y
CN generate 64 bit valid address and update in database
CN and 'A' exchange key by Diffie-Hellman
CN send that 64 bit encrypted address to 'A'
'A' decrypt that address using security key
'A' generate unique 128 bit address
CN sends probe to nodes for checking existence
If node-reply=Y
Node still in working phase
Terminate

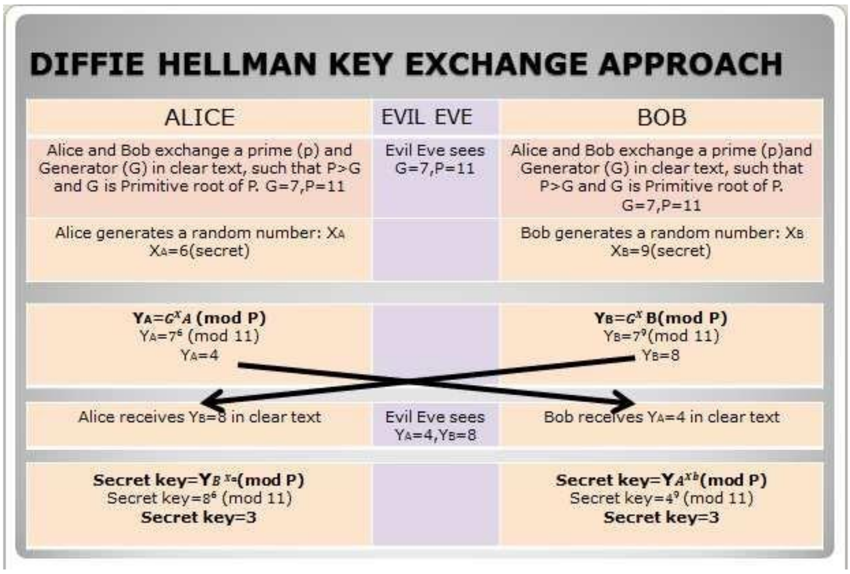
Fig 4.1: Flow Chart of Proposed Method

4.1 Diffie Hellman

Public key cryptography resulted from the need to be able to exchange keys between people around the world who had never met; it was impractical to have trusted couriers deliver secret keys to senders and receivers. Although in their 1976 paper Diffie and Hellman did not propose a public key cryptosystem, they did propose a scheme to do key exchange. The security of their method, called Diffie-Hellman key exchange, is based upon the discrete logarithm problem.

- Diffie Hellman is public key algorithm.
- Widely used in security protocols and commercial products.
- It is only used for key exchange not for encryption or decryption.

A method for two parties to agree upon a shared secret in such a way that the secret will be unavailable to eavesdroppers. This secret may then be converted into cryptographic keying material for other (symmetric) Algorithms. D-H key agreement requires that both the sender and receiver of a message have key pairs. By combining one's private key and the other party's public key, both parties can compute the same shared secret number. This number can then be converted into cryptographic keying material. That keying material is typically used as a key-encryption key (KEK) to encrypt a content encryption key (CEK) which is in turn used to encrypt the message data.



DIFFIE HELLMAN KEY EXCHANGE APPROACH

ALICE	EVIL EVE	BOB
Alice and Bob exchange a prime (p) and Generator (G) in clear text, such that P>G and G is Primitive root of P. G=7,P=11	Evil Eve sees G=7,P=11	Alice and Bob exchange a prime (p)and Generator (G) in clear text, such that P>G and G is Primitive root of P. G=7,P=11
Alice generates a random number: X_A X_A=6(secret)		Bob generates a random number: X_B X_B=9(secret)
$Y_A=G^xA$ (mod P) $Y_A=7^6$ (mod 11) Y_A=4		**$Y_B=G^x$ B(mod P)** $Y_B=7^9$(mod 11) Y_B=8
Alice receives Y_B=8 in clear text	Evil Eve sees Y_A=4,Y_B=8	Bob receives Y_A=4 in clear text
Secret key=$Y_B{}^{x_a}$(mod P) Secret key=8^6 (mod 11) **Secret key=3**		**Secret key=$Y_A{}^{x_b}$(mod P)** Secret key=4^9 (mod 11) **Secret key=3**

Fig4.2: Diffie Hellman Key Exchange Approach

4.1.1 Diffie-Hellman Algorithm

1. Sender and Receiver agree on a prime number p, q as its primitive root.
2. Sender and Receiver choose their so called private key ‘a’ and ‘b’ which is known to themselves only respectively.
3. Sender’s public key A= q^a mod p.
4. Receiver’s public key B= q^b mod p.
5. Sender and Receiver exchange their public key. Now Sender has B and Receiver has A.
6. Sender calculates B^a mod p= q^{ba} mod=S.
7. The receiver calculates A^b mod p=q^{ba} mod p=S.
8. Hence, the sender and receiver get ‘S’ as their shared secret key.

Suppose Alice and Bob want to agree on a shared secret key using the Diffie–Hellman key agreement protocol as shown in fig4.2. They will generate shared key as follows: first, Alice generates a random private value X_A and Bob generates a random private value X_B. Both A and B are drawn from the same set of integers. Then they derive their public values using parameters p and g and their private values. Alice’s public value is x=$G^x{}_A$ (mod p) and Bob’s public value is y=$G^x{}_B$ (mod p). They then exchange public values x and y. Finally, Alice computes ka=$y^x{}_A$ (mod p), and Bob computes kb=$x^x{}_B$ (mod p). Since ka = kb = k, Alice and Bob now have a shared secret key k [3].

So, to know the shared-secret key of the sender and the receiver, attacker would have to calculate the value of private key which is known to only sender and receiver. So, it’s tough for the attacker to get the secret key but not impossible. Plain text, Man-in-Middle attack, logjam attack and many more attacks still possible but very difficult to break the security if we take prime (P) at least 2048 bits long and implemented properly with authentication (DSA) and encryption (AES) algorithms.

4.2 AES Algorithm

- AES is a block cipher with a block length of 128 bits.
- AES allows for three different key lengths: 128, 192, or 256 bits.
- Most of our discussion will assume that the key length is 128 bits.
- Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.
- Except for the last round in each case, all other rounds are identical.
- Each round of processing includes one single-byte based substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key. The order in which these four steps are executed is different for encryption and decryption.
- To appreciate the processing steps used in a single round, it is best to think of a 128-bit block as consisting of a 4×4 matrix of bytes, arranged as follows:

byte0	byte4	byte8	byte12
byte1	byte5	byte9	byte13
byte2	byte6	byte10	byte14
byte3	byte7	byte11	byte15

- Therefore, the first four bytes of a 128-bit input block occupy the first column in the 4 × 4 matrix of bytes. The next four bytes occupy the second column, and so on.
- The 4×4 matrix of bytes shown above is referred to as the state array in AES.
- AES also has the notion of a word. A word consists of four bytes, which is 32 bits. Therefore, each column of the state array is a word, as is each row.
- Each round of processing works on the input state array and produces an output state array.

- The output state array produced by the last round is rearranged into a 128-bit output block.
- Unlike DES, the decryption algorithm differs substantially from the encryption algorithm. Although, overall, the same steps are used in encryption and decryption, the order in which the steps are carried out is different, as mentioned previously.
- The output state array produced by the last round is rearranged into a 128-bit output block. Unlike DES, the decryption algorithm differs substantially from the encryption algorithm. Although, overall, the same steps are used in encryption and decryption, the order in which the steps are carried out is different, as mentioned previously.
- As explained in Lecture 3, DES was based on the Feistel network. On the other hand, what AES uses is a substitution-permutation network in a more general sense. Each round of processing in AES involves byte-level substitutions followed by word-level permutations. Speaking generally, DES also involves substitutions and permutations, except that the permutations are based on the Feistel notion of dividing the input block into two halves, processing each half separately, and then swapping the two halves.
- The nature of substitutions and permutations in AES allows for a fast software implementation of the algorithm.

4.2.1 Structure of AES

The overall structure of AES encryption/decryption is shown in Fig4.3.

- The number of rounds shown in Figure 2, 10, is for the case when the encryption key is 128-bit long. (As mentioned earlier, the number of rounds is 12 when the key is 192 bits and 14 when the key is 256)
- Before any round-based processing for encryption can begin, the input state array is XORed with the first four words of the key schedule. The same thing happens during decryption — except that now we XOR the cipher text state array with the last four words of the key schedule.
- For encryption, each round consists of the following four steps:
  1) Substitute Bytes 2) Shift Rows 3) Mix columns and 4) Add round Key
- The last step consists of XORing the output of the previous three steps with four words from the key schedule.

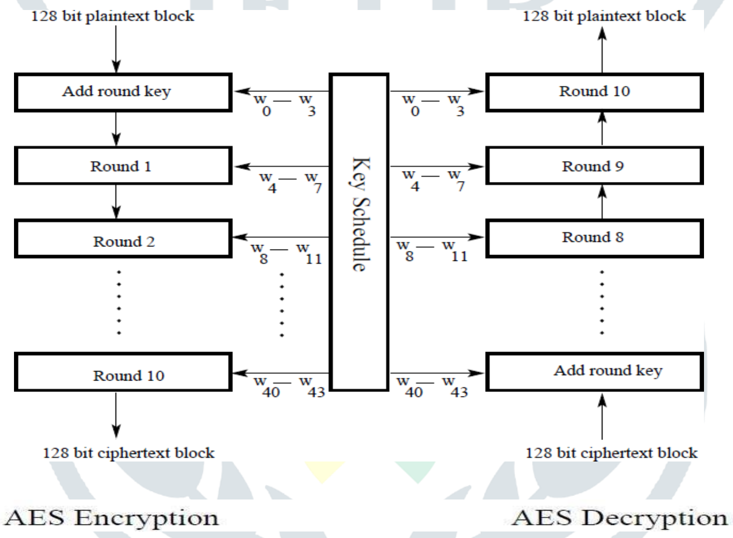


Fig 4.3: Shows the different steps that are carried out in each round except the last one.

- For decryption, each round consists of the following four steps:

1) Inverse shift rows
2) Inverse substitute Bytes
3) Add round key
4) Inverse mix columns

- The third step consists of XORing the output of the previous two steps with four words from the key schedule. Note the differences between the order in which substitution and shifting operations are carried out in a decryption round vis-a-vis the order in which similar operations are carried out in an encryption round.
- The last round for encryption does not involve the “Mix columns” step. The last round for decryption does not involve the “Inverse mix columns” step.

V. CONCLUSIONS

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. Here some techniques in which EUI-64, CGA and Privacy Extension has limitation and some are good enough like SSAS and i-SeRP, SSAS takes less time to remove the vulnerabilities in comparison to CGA. But in these techniques 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. 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 sending. And also data or messages are encrypted by AES algorithm. So it is secure enough to give the security in the network. My hypothesis was that energizer would last the longest in all of the aspects tested. My results do support partially of my hypothesis. I think the test I did went smoothly and I had no problem, except for the fact that the system is running on one system only. So it needs to be tested on network but without a doubt, IPv6 represents a big step forward compared to IPv4. The entire suite of protocols has been designed to bring improvements in both functionality and security. Many features have been built into the IPv6 specifications that are very useful for the both operation and the deployment of IoT (Internet of Things). So IPv6 will play a vital role in upcoming technologies.

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] S.thomson,T. Narten,T. jinmei, ”IPV6 stateless Address Auto configuration”, RFC 4862,Internet Engineering Task force,september 2007.
[7] Hosnieh Rafiee, Christoph Meinel, “SSAS: A Simple Secure Addressing Scheme for IPv6Autoconfiguration” 2013 Eleventh Annual Conference on Privacy, Security and Trust (PST)
[8] Athirah Rosli, Wan Nor Ashiqin Wan Ali, Abidah Haji Mat Taib, “IPV6 Deployment: Security Risk assessment using i-SeRP System in Enterprise Network” IEEE 2012
[9] Steven J. and G. Peterson, threat modeling-Perhaps it’s time. Security & Privacy, IEEE 2010.
[10] T. aura “Cryptographically Generated Addresses (CGA)”, rfc 3972, Internet Engineering Task Force, march 2005.
[11] T. narten, R.draves, S.krishnan, “Privacy Extension for Stateless address Auto configuration in IPV6”, rfc 4941, 2007.
[12] Behrouz A Forouzan, “Cryptography and Network Security” 4th Edition McGraw-Hill 2010.
[13] W. Stallings, “Cryptography and Network Security”: Principles and Practice, 6th Edition 2013, 596-625.
[14] Joseph Davies, Understanding IPV6, 2nd edition, 2008.
[15] https://www.ietf.org/rfc/rfc2631.txt and RFC 2460 -www.IETF.org.
[16] Deploying IPv6 Networks” -Popoviciu C., Levy-Avegnoli E., Grossetete, P. -Cisco Press.