Generation of Cryptographic one-to-many Mapping IPv6 Address using S-AES

N. Hakiem*, A. U. Priantoro*, M. U. Siddiqi*, T. H. Hasan**
*Electrical & Computer Engineering Department, **Science in Engineering Department
Faculty of Engineering, International Islamic University Malaysia
P.O. Box 10 50728 Kuala Lumpur Malaysia
{g0729261@student., unggul@, umarsiddiqi@, talib@}iium.edu.my

***Abstract*- The proliferation of enterprise wireless network raises the security concern in any organization despite the unarguable benefits it brings about. At the same time, the initiatives to migrate from IPv4 (Internet Protocol version four) to IPv6 (Internet Protocol version six) is gaining momentum across the globe to resolve the IP address depletion problem as well as reaping the benefit of it.**

This research proposes a new scheme to manage IPv6 addresses in an enterprise wireless local area network (WLAN) which may be implemented into DHCPv6 (Dynamic Host Configuration Protocol for IPv6) software. Each user will be assigned a group of IP addresses that are generated cryptographically whose parameters as user attributes. Each time user trying to access the network it will be given different IP address which will be generated using S-AES (Simplified Advanced Encryption Standard) algorithm using parameters assigned to that user so that there is a one to many mapping between user and IP addresses.

Therefore, the network administrator will be able to identify user realtime from the IPv6 address to facilitate tracking of network anomalies or violation of policies. By the pseudo random IPv6 address generation, we will be able to protect user's privacy even though the communication is transparent end-to-end.

Keywords— Address Management, Advance Encryption Standard, DHCPv6, IPv6, WLAN.

I. INTRODUCTION

IEEE 802.11a/b/g standard specifies (PHY) physical layer and MAC (medium access layer) for enabling Ethernet protocols over the wireless medium or better known as WLAN (wireless local area network). This technology enhances the way people are connected to the network significantly since no more hassle with the cable. Everyone can get connected to the network everywhere as long as the radio signal from the AP (access point) is there. Combined with DHCP (Dynamic Host Configuration Protocol), made our lives even easier. Configuration of the client, i.e., setting the IP address, gateway and DNS (Domain Name Server) is automatic. Therefore, more and more WLANs are deployed worldwide.

Meanwhile, since 1990s researchers started realizing the limitation of the IPv4 (internet protocol version four) in terms of the address space. IPv4 network has been growing beyond the design intention so that the remaining address space will be depleted. For that reason and also experiences gained from the IPv4 development, a next generation protocol, IPv6 (IP version six) has been proposed to solve the problem of IP address depletion and also making the IP protocol more efficient, secure and flexible. For example, IPv6 uses 128 bits to represent IP address compared to IPv4 that uses "only" 32 bits. This change provides us with almost unlimited number of address so that IP address space will not be problem anymore. If we calculate the IP address density on the earth surface, we can assign 3.4 trillion IP address per square centimeters of earth surface. This will allow us to give a unique (global) IP address to almost any device conceivable in the future.

IPv6 networks have been deployed all over the world although not as wide as IPv4 yet. And eventually all existing IPv4 networks will have to migrate to IPv6 since more and more governments mandate this migration, including Malaysia [1]. In the near future we will see more and more WLAN and IPv6 deployed worldwide. Our concern here is with the management of IPv6 address in enterprise WLAN, such as universities, mid-sized and large companies, and government agencies.

IP address management is one of the important aspects of network management to improve the security and enforcing the network policy set up by the organization. In WLAN environment the feasible solution is to use DHCP server to automate the IP address assignment whenever a network client wants to connect to the network. DHCP server assigns IP address to requesting client from the pool of IP address configured by the network administrator. It does not keep record of which IP address is assigned to which client and when. Whenever traffic anomaly or policy breach or internally-generated security threat it is difficult to pinpoint the culprit since no record of IP address assignment is kept. Expensive devices and software as well as the expert must be called upon for investigation.

This research proposes a new scheme to manage IPv6 addresses in an enterprise wireless local area network (WLAN). In the proposed scheme, each user will be assigned a group of IP addresses that are generated cryptographically whose parameters as user attribute. In our proposal the objective of cryptographically generating address is to assert user's address ownership by the network administrator (non-repudiation of address). Each time user trying to access the network it will be given IP address which will be generated

using cryptographic algorithm using parameters assigned to that user so that there is a one-to-many mapping between user and IP addresses. This will also enhance the security and privacy of end users since they can not be tracked by their IP addresses by eavesdroppers, which is crucial since all users will be assigned global IP addresses [2]. Assignment global IP addresses are one of the effort of the researchers to restore the extinguishing feature of the Internet which is end-to-end transparent communication, due to depletion of addresses in IPv4 [3].

Therefore, the network administrator will be able to readily identify users from the IPv6 address to facilitate tracking of network anomalies or violation of policies, it will reduce the burden of network administrator as well as enhancing the security of the internal network. By the pseudo random generation of IPv6 address, we will be able to protect user's privacy even though the communication is transparent end-to-end [4].

The remainder of this paper is organized as follows. Section 2 describes briefly the background related to this research. Section 3 and 4 explains the proposed IP address generation mechanism and it's result. Section 5 concludes the contribution of this paper and future works that should be done.

II. BACKGROUND

A. IPv6 Address

In IPv6, 128 bits are used to specify the address of a node which format is shown in Figure 1.

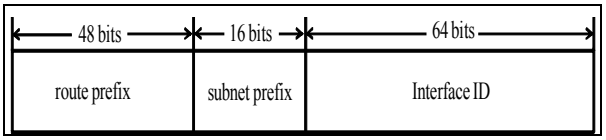

Fig. 1. IPv6 address format

The first 48 bits are allocated for network address which is globally unique, thus globally routable. The following 16 bits are allocated for subnet prefix within a network to allow network administrator defining the desired internal network hierarchy. The remaining 64 bits are allocated for interface ID for nodes. This proposal focuses on the mechanism to generate this interface ID in order to simplify the IP address management in enterprise WLAN.

B. Stateless Address Configuration

IPv6 was designed to provide indefinite support to the existing IPv4 as well as expanding network services to support ubiquitous networking whereby most of electronic devices are interconnected such as sensor networks, RFID's as well as ad hoc networks [5]. In order to support a wide array of devices' capabilities and constraints, IPv6 has several mechanisms to facilitate "plug and play" autoconfiguration and manual configuration of nodes. However the latter practice is not highly recommended considering the complexity of the address which is comprised of 128 bits.

Stateless autoconfiguration is intended for ease of deployment of unmanaged network or network whose nodes have limited capability such as sensor network. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information and information advertised by routers [6].

In stateless auto configuration IP address can be derived from MAC address [5] or other mechanism such as Cryptographically Generated Address (CGA) [7] and its extension, Multi-key CGA (MCGA)[8]. CGA was originally defined for resolving security issues in Neighbor Discovery protocol. It generates the interface ID by using one way hash function with user's public key and auxiliary parameters as the input. When required, anyone can verify the binding between the public key and the interface ID portion of the IP address by regenerating the interface ID using the public key and associated auxiliary parameters. A user who send a signed message, using his/her private key, from the IP address and attaching the public key and the auxiliary parameters can be verified by the packet recipient without a Public Key Infrastructure (PKI). This is very useful to secure the Neighbor Discovery protocol in unsecured environment such as public hot spots to prevent spoofing. As extended usage of CGA, it has been proposed to secure other protocols such as the Mobile IPv6 (MIPv6) protocol [9,10]. Further enhancement was done to support multiple hash function [11].

C. DHCPv6

As a complementary of stateless autoconfiguration there is stateful autoconfiguration which is widely used in managed network, such as enterprise and campus networks. In the scheme, hosts obtain interface addresses and other configuration information from a server. Servers maintain a database that keeps track of which addresses have been assigned to which hosts, or the binding information. DHCPv6 simplifies network administration and requires minimum or no manual configuration of DHCPv6 clients [12]. Thus a DHCPv6 client may be given different IP address each time it requests to the DHCP server. Although DHCPv6 server maintains the binding information, and can be logged for later retrieval, it (the binding information) is only known to the DHCP server. Any network node requires the information must send queries to the DHCP server.

DHCPv6 message format is as follows: all DHCP messages sent between clients and servers share the same fixed format header. Other configuration parameters are included in options area which has variable length [12]. This message option has been used to handle IPv6 address allocation.

Recently there is an increasing interest to merge the goodness of DHCPv6 and CGA [13]. Since CGA address generation is computationally expensive, it was suggested to offload the operation to a proxy in an environment whereby hosts do not support CGA address generation by themselves or use DHCPv6 server to manage CGA addresses via registration. In either case, a mechanism to ensure that the IP

address generated is routable within the link duplicate address detection (DAD) [6] will be executed before an address is assigned to an interface by the host. However, it is worth noting that DAD can be disabled when deemed unnecessary by system administrator.

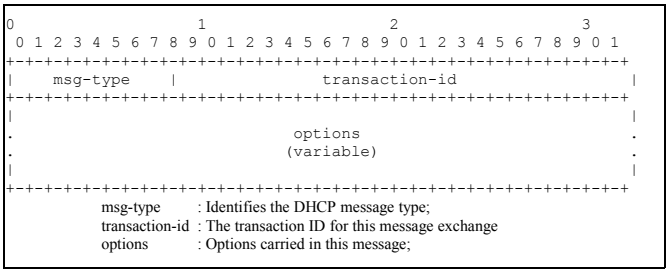

Fig. 2. DHCPv6 Client/ Server Message Format

IPv6 address configuration mechanisms previously described, do not facilitate IPv6 address owner detection in real time which may be of interest to enterprise wireless network administrator for various reasons. In the next section, we describe a novel IPv6 node interface ID generation mechanism that supports IPv6 address owner identification in real time. The mechanism takes advantage of the huge size of IPv6 address.

D. Advanced Encryption Standard

Advanced Encryption Standard (AES) selected Rijndael (designed by Rijmen – Daemen in Belgium) which has characteristics of: Resistance against all known attach, speed and code compactness on a wide range of platforms, and design simplicity.

The input of AES Rijndael encryption and decryption algorithms is a single 128-bit block as a square matrix of bytes. This block is copied into the state array which is modified at each stage of encryption or decryption, depicted in Figure 2. At the final stage, state is copied to an output [14].

III. PROPOSED MECHANISM

A. Framework Development

We propose to generate IP address which can be exclusively mapped to each individual user in real time. Identification of the owner of valid IP address is done by masking the interface ID with a certain binary mask. Further, to reduce the probability of coincidental match of randomly generated interface ID, checksums are embedded in the generated interface ID [15]. Thus, theoretically a valid user can have sufficient number of IP addresses for his exclusive use, a many-to-one mapping from the IP address space to the user space.

In that framework [15], User Id bit are distributed within Interface Id in the fix position instead of using cryptographically method. It is shown the normal distribution with average of 0.70 and standard deviation of 0.052. This means that the generated IPv6 addresses that belong to the same user have higher degree of similarity. This increasing similarity is due to the insertion of user ID and checksum bits which are identical for all IPv6 addresses belong to the same user. This might be exploited to infer IPv6 address owner by network adversaries which may raise further security and privacy concerns. Therefore, it is desirable in this paper to reduce the cross correlation which is related to Hamming Distances values of the generated IPv6 addresses belong to the same user.

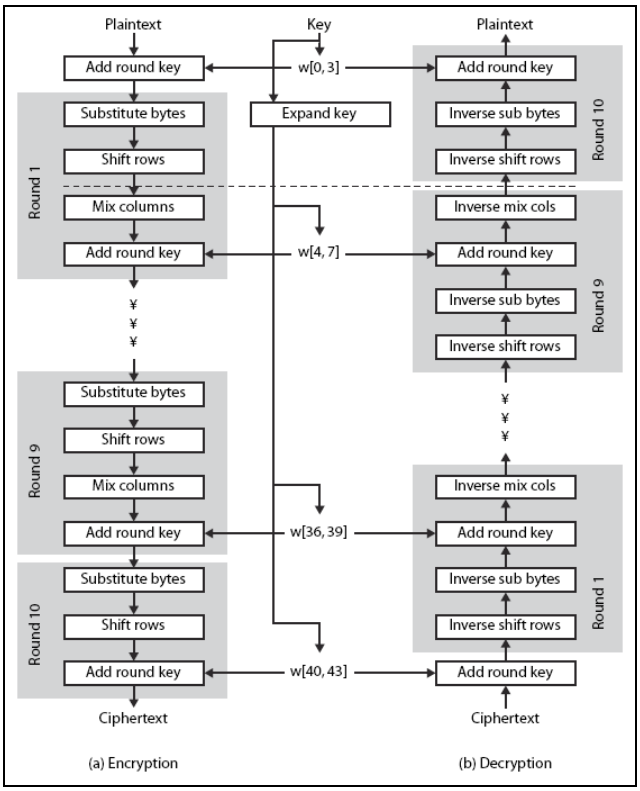

Fig. 3. Rijndael Cipher

B. Proposed Mechanism

Simplified AES has similar properties and structure to AES with much smaller parameters. Figure 4 depicts the structures of S-AES which encryption and decryption algorithm. It takes a 16-bit block of plaintext input, key, and produces a 16-bit block of text of output [16].

In this phase, Interface Id format depicts in Figure 5. It contains of 6-bit Checksum, static Universal/ Local (1-bit) and Group/ Individual (1-bit), 48-bit Encrypted User Id, and 8-bit of Key Id. Each of Key Id has 48-bit length which can be retrieved via look up table.

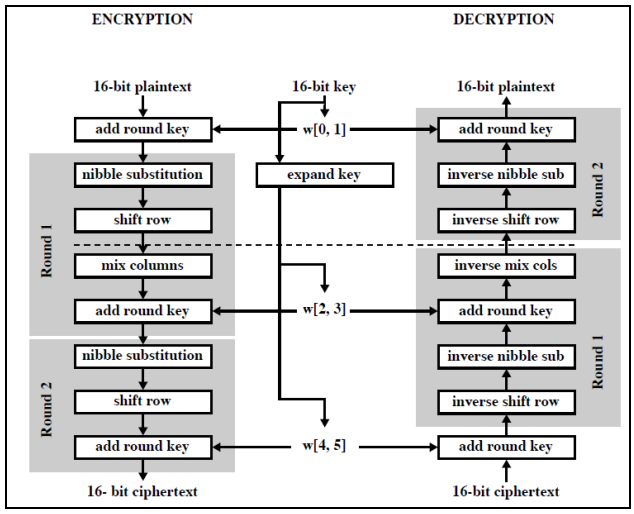

Fig. 4. Simplified-AES Cipher

Fig. 5. Proposed Interface Id format

48-bit Encrypted User Id derives from 18-bit User Id as depicted in Figure 6. This User Id splits into three parts, each part concatenates with 10-bit random to form 16-bit plain. It will be encrypted using S-AES encryption and all three encrypted User Id have been concatenated to construct 48-bit Encrypted User Id.

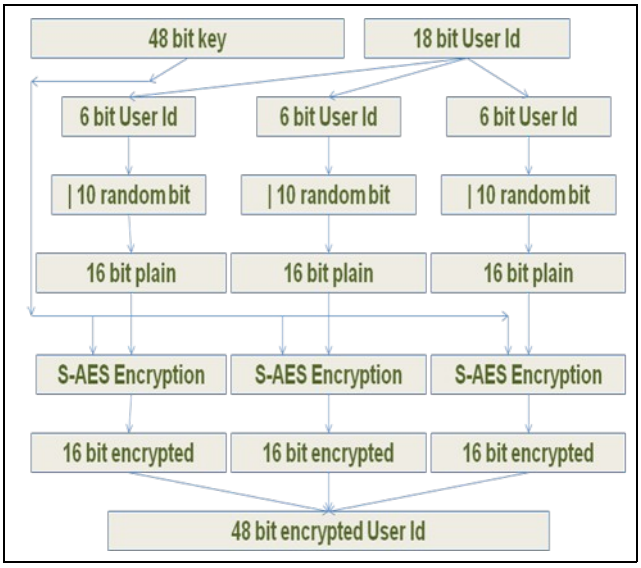

Fig. 6. Triple S-AES Encryption

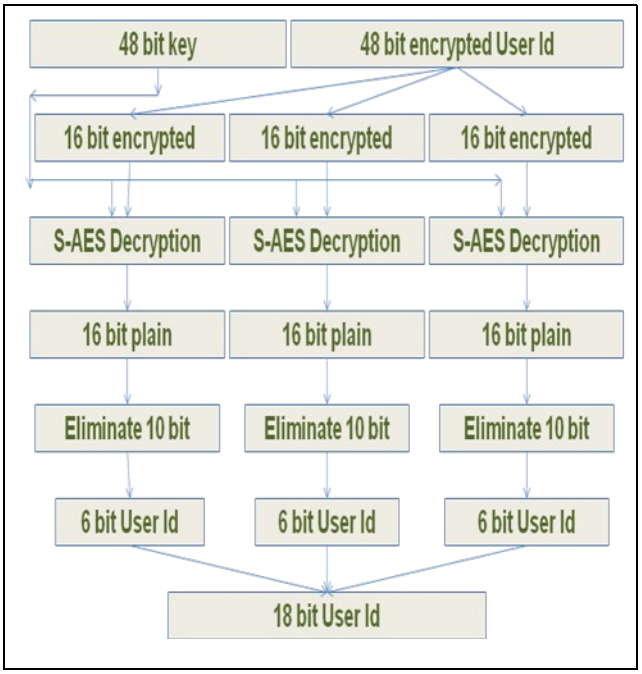

Fig. 7. Triple S-AES Decryption

Triple S-AES decryption algorithm can be seen in Figure 7. Encrypted User Id has been split into three parts which will be decrypted using S-AES to produce 16-bit plain text. Eliminate first 10-bit result to make original plain text which will be concatenated to get 18-bit User Id.

To generate Interface Id format which have Checksum, U&G bit, Encrypted User Id and Key Id, algorithm as shown on Figure 8 has been done. First step, it took 8-bit random number which look up table of 48-bit of Key Id. Next step is generating Encrypted User Id with input 18-bit User Id and 48-bit key using Triple S-AES algorithm. Checksum has been generated using formula [15] and finally, we construct Interface Id format as shown on Figure 5.

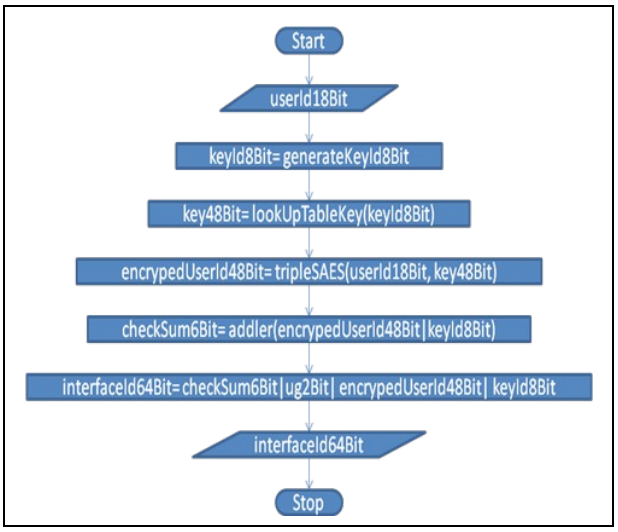

Fig. 8. Interface Id Generation

There are some steps to verify Interface Id's owner as shown on Figure 9. Firstly, check bit 7th and 8th as Universal and Individual bit respectively, if the value is "00", continue to the next step, and otherwise stop identifying. Next step is comparing checksum value with checksum generated, if the value is match, continue to the next step, and otherwise stop identifying. Eventually, it gets User Id using Triple S-AES decryption.

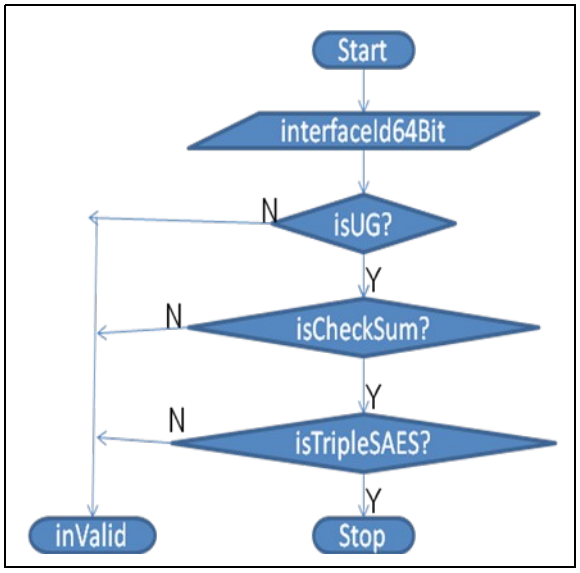

Fig. 9. Identify Interface Id

IV. Simulation Results

Generated Interface Id example using this mechanism can be seen at Table 1. This simulation has been developed and compiled using Java™ Standard Edition version 1.6.0 and its data store to text file which can be open and simply analyze using office Spreadsheet. It generates 512 different Interface Id belong to the same User Id, in this example is octal number 123456 (18 bits).

TABLE I. Generated Interface Id

```
64 bits Interface ID, Replaced 18 Bits UID & 6 bits checkSum
User Data Octal 6 Digits    = 123456
User Data Binary 18 Digits = 001010011100101110
7th & 8th bit (u & g) is 00.

 No                          64 Bin Interface ID
   1   0000010000011001000010011100011110100111101111001000001000011
   2   0011100011000111111110101100100111100100001001100100101011011
   3   1110100010011111001101111010111111111000110100000011001110000
   4   0011000001100101110000001010101111011110011001001111010011000
   5   0011000011011001000100010111010011100110011011110010011010100
 ...   . . . .
 508   1110000011000100111011011000101110010011101110001011100010011010
 509   0110000000011110000010010100001010100101000001001101000110000100
 510   0100010001010001111010000001000011100100100101011001101110111000
 511   1011000001001010000010110010111010000100110011101100010011000011
 512   1100110011100001101101111111110000110011000010010111101011101100
```

To measure the avalanche effect was used the arithmetic average of Hamming distances [17]. Table 2 shows the Hamming Distance of generated Interface Id. In this simulation result, it calculates 130186 comparisons for 512 encrypted addresses. It compares address 1 to 2, 1 to 3, and so on and it will get Hamming Distance. Hamming distance value is accumulation of comparison of two binary numbers, if the bit are same, the value is 0 and if it is different bit, the value is 1.

TABLE II. Hamming Distance

No	Comparison	Hamming Distance
1	1 | 2	39
2	1 | 3	32
3	1 | 4	28
4	1 | 5	22
5	1 | 6	34
...	...	...
510	1 | 511	25
511	1 | 512	36
512	2 | 3	27
513	2 | 4	29
...	...	...
130813	509 | 512	39
130814	510 | 511	34
130815	510 | 512	33
130816	511 | 512	37
Avg		30.49

Figure 10 depicts the Hamming Distance chart of generated Interface Id. Since the bit number of Interface Id is 64, the range value of this Hamming Distance is 0 to 64 (decimal number). If the Hamming Distance value is 0, it means that all 64 bit binary for both Interface Id is same and if the value is 64, it indicates that all 64 bit binary for both Interface Id is different. Expected Hamming Distance value as avalanche effect is about 50% of the bits change [18]. The Hamming Distance average is 30.49 (48%), it is not exactly 50%, it is reasonable because there are two bits (7th and 8th) of Interface Id have the same value, both set to 0. It can be concluded that using Triple S-AES may achieve avalanche effect expectation.

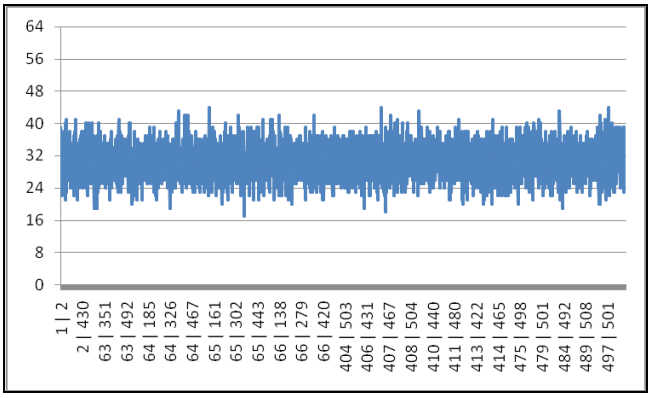

Fig. 10. Hamming Distance Chart

V. CONCLUSION AND FUTURE WORKS

In developing and third world countries internet bandwidth is a precious resource in organizations. Proper bandwidth management will definitely helps the organization to maximize its investment in internet connectivity, by minimizing junk traffic and prioritizing valid traffic. The proposed IPv6 address generation mechanism can be used to simplify the bandwidth management by recognizing users by his/her IPv6 addresses.

Another possible application is to facilitate network policy enforcement. Today more and more ICT services and applications migrate to web based services [19] which make controlling internet (including intranet) traffic using ports is not feasible anymore. Being able to recognize users by their IPv6 addresses can automate the decision whether to grant or deny access to certain internal and external servers. This will enhance the existing security measures already implemented in the network.

IPv6 address management in enterprise wireless network is of interest to network administrator. It helps network administrator to efficiently manage the network and improve the controllability and visibility of the network that in the long run will increase the ROI of ICT investment and compliance to regulations via policy enforcement. A simple mechanism to generate IPv6 addresses for enterprise wireless network was proposed that facilitates real-time user identification from their IPv6 addresses. The generated IPv6 address is embedded with user ID so that users can be identified by using Triple Simplified-Advance Encryption System. Check sum values also embedded to reduce the probability of randomly generated address coincides with valid IPv6 addresses generated by the proposed mechanism. Expected avalanche effect (50%) may achieve using this mechanism.

Since Simplified-AES is for academic purpose, it is an educational rather than a secure encryption algorithm [14]. In addition, it is breakable (vulnerable) with linear calculations [20]. Therefore, we should use AES (mode of operation) which resistant against all known attacks instead of using S-AES. We also should compare that result with current result and implement this mechanism into dhcpv6 software for example in Dibbler [21, 22].

ACKNOWLEDGMENT

The work was supported by the Research Management Center International Islamic University Malaysia under IIUM Endowment EDW B 0802-84.

REFERENCES

[1] Z. B. Zakariah and A. H. A. Hamzah. (2007, November, 26). "IPv6 Awareness Seminar for Malaysian Government Agencies; Moving The Nation Towards IPv6-Enabled by 2010; Policy and Regulatory Matters. Malaysian Communications and Multimedia Commission". Available: http://www.kettha.gov.my/system/uploaded/files/ipv6_sp4.ppt, accessed on June 16, 2010.

[2] T. Narten, R. Draves, and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", The Internet Society RFC 4941, September 2007.

[3] Cooperative Association for Internet Data Analysis - CAIDA CAIDA : publications : presentations : 2005 : arin [Online]. (2005, October, 26). "apocalypse then: ipv4 address space depletion". Available: http://www.caida.org/outreach/presentations/2005/arin/arin200510.pdf, accessed on June 23, 2010.

[4] B. Carpenter, "Internet Transparency", IETF RFC 2775, February 2000.

[5] J. J. Amoss, and D. Minoli, "Handbook of IPv4 to IPv6 Transition, Methodologies for Institutional and Corporte Networks", Danvers : Auerbach Publications, 2008.

[6] S. Thomson, T. Narten, and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", IETF RFC 4862, September 2007.

[7] T. Aura, "Cryptograhically Generated Addresses (CGA)", IETF RFC 3972, March 2005.

[8] C. Gentry, J. Kempf, J. Wood, and Z. Ramzan, "IP Address Authorization for Secure Address Proxying Using Multi-key CGAs and Ring Signatures", Lecture Notes in Computer Sciences, SpringerLink, pp. 196-211. 2006.

[9] G. O'Shea, and M. Roe, "Child-Proof Authentication for MIPv6 (CAM)", SIGCOMM Comput. Commun. Rev., vol. 31, no. 2, pp. 4–8. 2001.

[10] J. Arkko, "Applying Cryptographically Generated Addresses and Credit-Based Authorization to Mobile IPv6", Work in Progress, June 2006.

[11] M. Bagnulo and J. Arkko, "Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (CGAs)", IETF RFC 4982, July 2007.

[12] R. D. Ed., J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", IETF RFC 3315, July 2003.

[13] I. v. Beijnum, "Interactions between CGA and DHCPv6", IETF Internet-Draft, 12 November 2007.

[14] W. Stallings, "Cryptography and Network Security, Principles and Practices, 4ed", Pearson Prentice Hall, 2006.

[15] N. Hakiem, A. U. Priantoro, M. U. Siddiqi, and T. H. Hasan, "IPv6 multi generated address for enterprise wireless Local Area Network", IGCES 2008. SPS-PGSS UTM, Johor Malaysia, pp. 154-158, December 2008.

[16] M. Musa, E. F. Schaefer, and S. Wedig, "A Simplified Rijndael Algorithm And Its Linear And Differential Cryptanalyses", Santa Clara, USA : Santa Clara University, 2002.

[17] F.S. Araujo et al., "Papilio Cryptography Algorithm", Departamento de Informatica e Matematica Aplicada, Natal-RN, Brazil.

[18] B. F. Ludwig, "Decrypted Secrets: Method And Maxims Of Cryptology, Fourth Edition", Springer-Verlag Berlin Heidelberg, 2007.

[19] M. Richard. (2007, September, 5). "10 Future Web Trends". Available: http://www.readwriteweb.com/archives/10_future_web_trends.php accessed on September 5, 2009.

[20] M. S. Davod, and B. H. Khaleghei, "On the vulnerability of Simplified AES Algorithm Against Linear Cryptanalysis", IJCSNS International Journal of Computer Science and Network Security, - Vol. VOL.7 No.7. July 2007.

[21] T. Mrugalski. (2009). "DHCPv6: Dibbler - a portable DHCPv6". Available: http://klub.com.pl/dhcpv6/, accessed on June 8, 2009.

[22] N. Hakiem, A. U. Priantoro, A. Mutholib, M. U. Siddiqi, and T. H. Hasan, "Implementation of IPv6 Address Generation Mechanism for Enterprise Wireless Local Area Network in Open Source DHCPv6", International Conference on Computer and Communication Engineering (ICCCE 2010), Kuala Lumpur, Malaysia, May 2010.