Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

RANDOMNESS TEST OF CRYPTOGRAPHIC ONE-TO-MANY REVERSIBLE MAPPING FOR IPV6 ADDRESS GENERATION

[1]NASHRUL HAKIEM, [2]MOHAMMAD UMAR SIDDIQI, [3]SIGIT PUSPITO W. JAROT, AND [4]AKHMAD UNGGUL PRIANTORO

[1]Department of Informatics, Faculty of Science and Technology, UIN Syarif Hidayatullah Jakarta
[1, 2]Department of Electrical and Computer Engineering, Faculty of Engineering, IIUM
[3]Indonesia Telecommunication Regulatory Body, Ministry of Communication and Informatics Republic of Indonesia.
[4]Surya University, Indonesia
E-mail: [1]hakiem@uinjkt.ac.id, [2]umarsiddiqi@iium.edu.my, [3]sigit.jarot@gmail.com, [4]unggul@surya.ac.id

ABSTRACT

This paper presents simulation results on randomness test of a cryptographic one-to-many reversible mapping between user space and the IPv6 address space. A one-to-many reversible mapping mechanism is developed which may be embedded into a DHCPv6 (Dynamic Host Configuration Protocol for IPv6) server in the stateful mode within an enterprise local area network (LAN). Each time a user accesses the network, the DHCPv6 server is able to assign a dynamic IPv6 address. The dynamic address (obtained through one-to-many mapping) is to protect the user from unwanted behavior analysis exploiting IPv6 addresses, thus protecting user privacy. However, the dynamic address can be uniquely linked to the user (through many-to-one reversible mapping) if the need arises. The randomness of the dynamic address (one-to-many mapping) for IPv6 address assignment is evaluated based on uniformity using monobit (frequency) test, and avalanche effect is evaluated using Hamming distance tests. Simulation results show that the randomness in terms of uniformity (occurrence of 1's or 0's are around 50%) and the Hamming distance (the difference between Interface IDs at approximately 50%) are accepted. The decision rule of randomness is set at the 1% significance level with the P_{value} of monobit (frequency) test, and the P_{value} in Hamming distance tests is taken to be more than 0.01. IPv6 addresses generated by a one-to-many reversible mapping mechanism are considered to be random with a confidence level of 99%.

Keywords: *Ipv6 Address, Randomness, Uniformity, Avalanche Effect, Monobit, Hamming Distance, P-Value.*

1. INTRODUCTION

The one-to-many reversible mapping mechanism [1] is developed which can be embedded into the DHCPv6 (Dynamic Host Configuration Protocol for IPv6) servers in the stateful mode [2],[3]. The aim of this mechanism is to improve IPv6 addresses generation in terms of privacy and security via DHCPv6 in an enterprise local area network (LAN).

Each time a user accesses the network, a dynamic IPv6 address is assigned via a DHCPv6 server in the stateful mode. The dynamic address (one-to-many mapping) is to protect a user from unwanted behavior analysis exploiting IPv6 addresses, thus protecting user privacy. However, the dynamic address can be uniquely linked to the user (many-to-one mapping) if the need arises to improve network visibility, thus protecting network security.

The requirement of a one-to-many reversible mapping for IPv6 address generation is that it should manage the 64-bit Interface ID part of an IPv6 address. It is assumed that the mechanism has to be able to manage up to 2^{18} registered user IDs within an enterprise local area network.

The first criterion of one-to-many reversible mapping is that the processing speed for generating and identifying an address must be practical. Secondly, the collision probability of the Interface ID part of an IPv6 address must be very small. The proposed mechanism should integrate well with the existing mechanism (DHCPv6). Eventually, the mechanism should be able to perform validation for generating and identifying IPv6 addresses.

In this paper, the performance of a one-to-many mapping for stateful IPv6 address assignment proposed in [1] is evaluated in terms of

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

randomness test based on uniformity using the monobit test and avalanche effect using the Hamming distance test. These tests are to measure the randomness of the Interface ID for a particular user in order to protect user privacy.

The remaining of this paper is organized as follows. Section II describes works related to this research and Section III briefly reviews one-to-many reversible mapping. Section IV describes the method of the randomness test while Section V gives the simulation results and a discussion on these findings. Section VI provides the conclusion of this paper.

2. RELATED WORKS

A. IPv6 Address

IPv6 has 128 bits to specify the address of a node which is represented in hexadecimal format with colon notation [4]. An example of a unicast IPv6 address is shown in Figure 1. The first 48 bits are allocated for the network address and the following 16 bits are allocated for a subnet prefix within the network. The remaining 64 bits are allocated for the Interface ID.

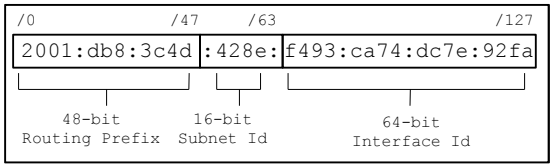

Fig. 1. Example Of Unicast Ipv6 Address

Table 1. Ipv6 Address Generation Mechanism

Mechanism	Advantages	Disadvantages	Target Application	Remarks
Auto config	No DHCP server required	No control over IPv6 address usage	Unmanaged network, ad hoc net, sensor net, etc.	RFC 4941, January 2007 [5]
DHCPv6	Control over IPv6 address usage	Requires DHCP server; planning	Managed Enterprise net, home net,	RFC 3315, July 2003 [2]
CGA	Verification of address owner	Requires asymmetric key cryptography	Mobile network	RFC 3972 Oct 2005 [6]
Multi-key CGA	Verification of address owner, enhanced mobility	Requires asymmetric key cryptography; proxy server	Mobile network	US Patent 7925027 B2, 12 April 2011 [7]
Random	Unique Local Unicast	Temporary address	Local Unicast	RFC 4193 October 2005 [5],[8]
	Address			

B. IPv6 Address Generation Mechanism

IPv6 supports different mechanisms for assigning IP addresses to nodes as shown in Table 1. There are a number of researches concerning IPv6 address generation with advantages and disadvantages as well as the objectives of their applications. One of them is Dual Addressing Scheme (DAS) over IEEE 802.15.4 Wireless Sensor Networks [9], however it has different target application with the one-to-many reversible mapping in this paper.

C. Stateful Address Generation

Using SLAAC (stateless address autoconfiguration) eases the burden of administration of the network. However it is vulnerable [10]. Therefore a managed network using DHCP in the stateful mode is one the solution to address this problem [11]. This paper concerns to manage Interface ID's of unicast IPv6 addresses in the stateful mode (using DHCPv6). DHCPv6 has default mechanisms to assign IPv6 address to the node as shown in Table 2.

Table 2. Dhcpv6 Interface ID Generation

Mechanisms	Advantages	Disadvantages	Remarks
EUI-64	unique identifier	Threatens the privacy of users	RFC 4291, February 2006 [4]
Random	Easy implementation	Difficult to identify IPv6 address owner	WorldCIS2011, Feb. 2011 [11]

3. ONE-TO-MANY REVERSIBLE MAPPING

A. Motivation

The various backgrounds of the development of one-to-many reversible mapping for IPv6 address generation in enterprise local area networks are:

1) IPv6 address owner identification is important for improving network visibility in order to improve the security of the enterprise local area network.

2) Changing the interface identifier, and the global scope addresses generated from it, over time makes it more difficult for eavesdroppers and other information collectors to identify the node when different addresses are used for different transactions that actually correspond to the same node [5].

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

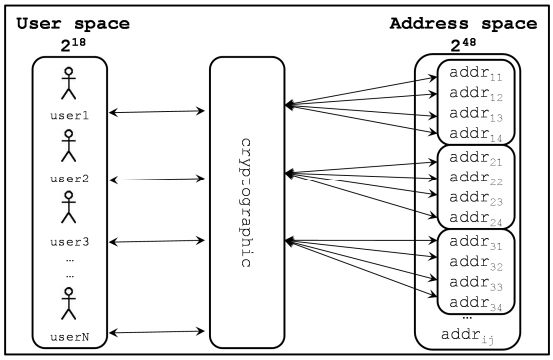

Fig. 2. Cryptographic One-To-Many Reversible Mapping

The main requirement of a generated dynamic IPv6 address is that it should manage the 64-bit Interface ID part of the IPv6 address. It is assumed that there are a maximum 2^{18} registered users ID's within an enterprise local area network.

B. One-to-many Reversible Mapping Development

The mechanism that manages the 64-bit Interface ID part of an IPv6 address uses an address format as shown in Figure 3. Another criterion of a generated dynamic IPv6 address is that the network administrator should be able to easily identify an IPv6 address owner. However, this mechanism should generate IPv6 addresses dynamically (difficult to identify) for a particular user in order to protect user privacy.

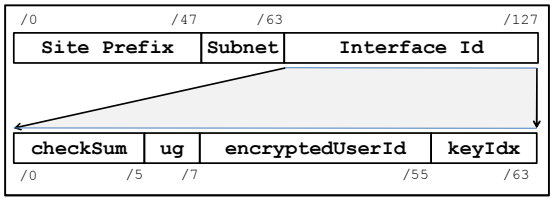

Fig. 3. Interface Id Format

One-to-many reversible mapping has been developed using the Advanced Encryption Standard with a Cipher Feedback mode of operation (CFB-AES) [1]. The simulation software of a one-to-many reversible mapping has been developed [12] in the Java environment.

C. Interface ID Generation

Interface ID generation is illustrated in Figure 4. Figure 5 illustrates the `encryptedUserId` process. The one-to-many mapping between the 18-bit user ID and the 48-bit encrypted user ID can be represented as:

$$P \leftarrow R \mid p \qquad (1)$$

where the 48-bit user ID P is a concatenation of a 30-bit R (random number) and the 18-bit p (user ID).

From (1), it can be seen that same p can have a number of P (one-to-many mapping) because of the additional R bits. However such P is clearly visible and thus conflicts with one of the objectives to protect user privacy. Therefore encryption is performed using CFB-AES which has a high avalanche effect such that any change of a bit in P may affect many bits of C significantly to produce a pseudorandom effect that actually corresponds to the same user ID p.

$$C = E\ (K, IV, P) \qquad (2)$$

where E denotes the encryption of P under key K and Initialization Vector IV; and C is the encrypted user ID which will be embedded in the Interface ID.

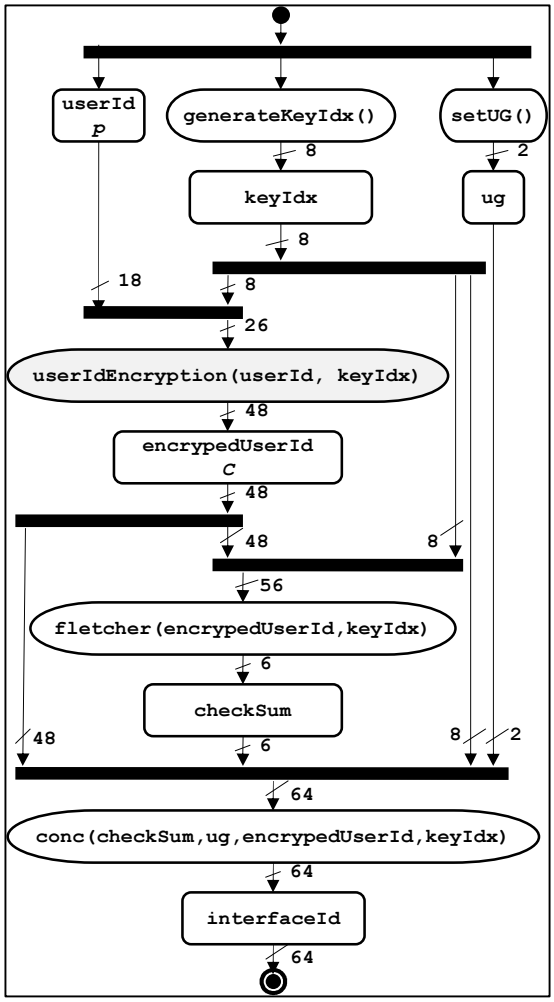

Fig. 4. Interface Id Generation

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The details of the CFB-AES encryption (2) are as follows:

$$C_k = P_k \oplus S_s[E(K, C_{k-1})] \quad (3)$$

where k is the second block to the end block, while the first block encryption also depends on IV (Initialization Vector) as follows:

$$C_1 = P_1 \oplus S_s[E(K, IV)] \quad (4)$$

D. User ID Identification

IPv6 address user owner identification is important to improve network visibility and enhance network security. The mechanism may be implemented as a complement of the network monitoring software in order to improve network security [13].

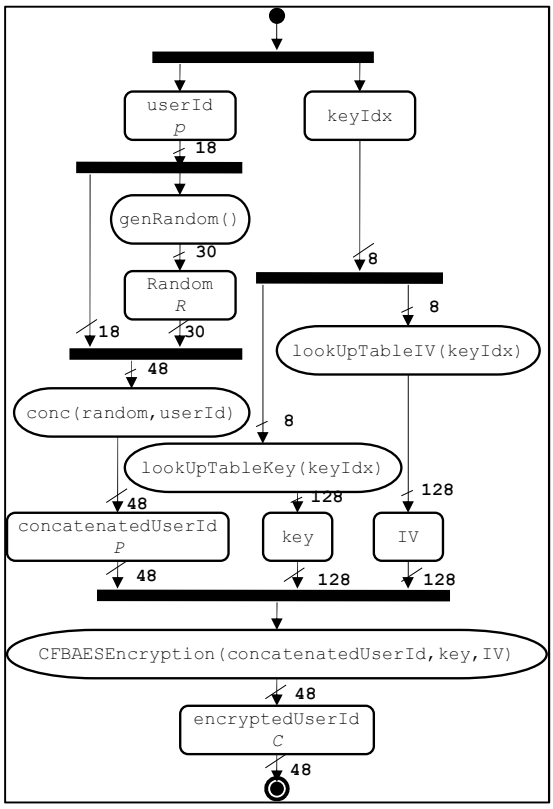

Fig. 5. User Id Encryption

To obtain p to identify an 18-bit user ID from a member of C which is part of the Interface ID, it has to perform validation first as depicted in Figure 6. There is a `userIdDecryption` process which is illustrated in Figure 7 and can be represented as:

$$P = D(K, C) \quad (5)$$

where D denotes the decryption of C under the key K to produce a 48-bit user ID. After that, it simply eliminates the first 30 bits (R) from P.

$$p \leftarrow P - R \quad (6)$$

This produces a user ID (p) from some P (many-to-one mapping).

For the identification process, it has to obtain P from C (5). This encrypts both the first block and the rest of the blocks which can be seen in (7) and (8).

$$P_1 = C_1 \oplus S_s[E(K, IV)] \quad (7)$$

$$P_k = C_k \oplus S_s[E(K, C_{k-1})] \quad (8)$$

where k is the second block to the end of the blocks and s is segments unit of bits.

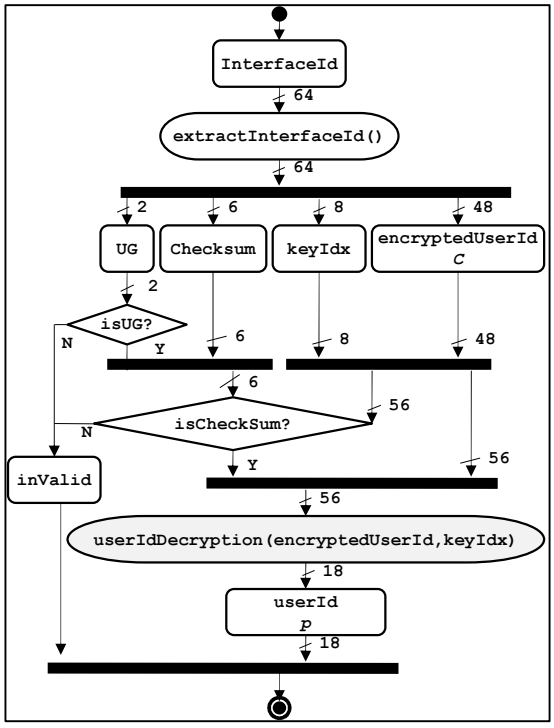

Fig. 6. User Id Identification

E. Evaluation

The performance of the one-to-many reversible mapping for the stateful IPv6 address assignment proposed in [1] has been evaluated for which the processing speed for generating an address and identifying an address was found to be practical (<100 ms) [14]. The collision probability of the Interface ID part of the IPv6 address is very small

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

indeed [14]. The proposed mechanism is able to be implemented easily within the existing mechanism (Dibbler DHCPv6) [15]. The checksum is embedded in the Interface ID generation for validation of the IPv6 address [1],[14].

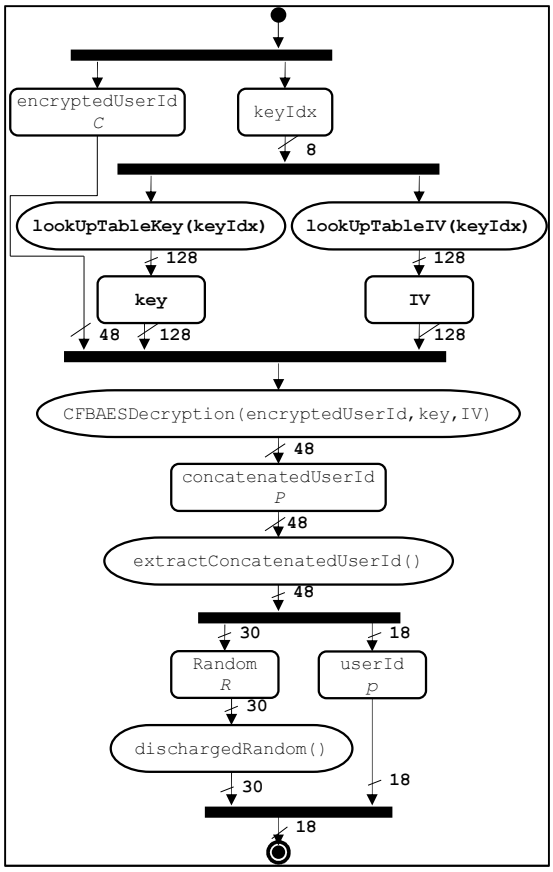

Fig. 7. User Id Decryption

4. RANDOMNESS TEST

A. Randomness

A random bit sequence could be interpreted as the result of the flips of an unbiased fair coin with sides that are labeled 0 and 1, with each flip having a probability of exactly ½ of producing a 0 or a 1 [16]. Randomness is a probabilistic property; that is, the properties of a random sequence can be characterized and described in terms of probability [16].

Various statistical tests have been developed to test the randomness such as the monobit (frequency) test, the runs test, the binary matrix rank test, the discrete Fourier Transform (spectral) test, and the Hamming distance test [16],[17].

This paper concentrates on randomness testing of the one-to-many mapping in terms of uniformity using the monobit test and avalanche effect using the Hamming distance test.

B. Performance Uniformity Test

The uniformity test determines whether the number of 1's and 0's in a binary sequence are approximately the same as would be expected for a truly random sequence, for which the expected probability of each is ½. This paper uses the monobit (frequency) test to measure the uniformity. The monobit test is used because this supplies the most basic evidence for the existence of non-randomness in a sequence. If this test is not passed, the probability of other tests failing is high [16].

C. Avalanche Effect

The avalanche effect occurs if one bit of the plaintext or the key is changed, then this should produce a significant change in the ciphertext [18],[19]. The expected avalanche effect value is about 50% of the bits changed [20]. This paper uses the Hamming distance test [21] to measure the avalanche effect.

The Hamming distance h for two vectors $x, y \in Z_2^n$ of length n is defined as the number $0 \leq h \leq n$ of positions where the vectors x, y differ $(h = x \oplus y)$ [17]. The Hamming distance test is used as a basic criterion in many avalanche effect tests such as the strict key avalanche criterion (SKAC) [22], the generalized avalanche criterion (GAC) test [23], and the strict avalanche criterion (SAC) test [17] .

In this paper, the term Hamming distance is used to compare two different Interface IDs to measure the avalanche effect, while the Hamming weight (number of ones) is used for a sequence of bits within an Interface ID for the monobit test.

D. Decision Rule

For test statistics, a P_{value} or tail probability that summarizes the strength of the evidence against the null hypothesis is used. In this term, the null hypothesis is that the sequence is random. If the P_{value} is equal to 1 then the sequence appears to have perfect randomness. The significance level or critical P_{value} is denoted by α. A common value of α in cryptography is about 0.01 [16].

The smaller the P_{value}, the more strongly the

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

test rejects the null hypothesis. The null hypothesis is rejected at level α if the P_{value} is smaller than α, otherwise the data appear to be consistent with the null hypothesis (the sequence is a random). If the computed $P_{value} < 0.01$ [16], then the sequence is considered to be non random with a confidence of 99%, otherwise, it is concluded that the sequence is indeed random with a confidence of 99%.

Each P_{value} is a different measurement for a sequence of bits within a block and for a sequence of blocks. The *erfc* which produced a standard half normal distribution is used to compare the value of the test statistic obtained from a sequence with the expected value of the statistic under the assumption of randomness [16]. The χ^2 distribution is used to compare the goodness-of-fit of the observed frequencies of a sample measure to the corresponding expected frequencies of the hypothesized distribution [16].

E. P_{value} within a Sequence of Bits

The P_{value} for a sequence of bits uses the complementary error function because it is related to the normal cumulative distributed function. The P_{value} can be calculated from:

$$P_{value} = erfc(z) \tag{9}$$

where *erfc(z) = 1 - erf(z)* which produces an upper tail probability. The complementary error function can be defined is [16]:

$$erfc(z) = \frac{2}{\sqrt{\pi}} \int_{z}^{\infty} e^{-u^2} du \tag{10}$$

where z is [16]:

$$z = \frac{S_{obs}}{\sqrt{2}} \tag{11}$$

and S_{obs} is the observed value which is used as a statistic in the test. This test makes use of that approximation to assess the closeness of the fraction of 1's to ½ [16]. For a sufficiently large amount of data, the distribution of the binomial sum is normalized by $\sqrt{n}$, and it will approximate to the standard normal distribution [16],[24],[25]. S_{obs} can be defined as:

$$S_{obs} = \frac{|S_n|}{\sqrt{n}} \tag{12}$$

where S_n is the difference of the Hamming distance (Hamming weight) and complement of the Hamming distance (Hamming weight). The S_n can be calculated as:

$$S_n = h - \bar{h} = h - (n - h) = 2h - n \tag{13}$$

where n is the sequence length, $n = h + \bar{h}$. In this case the value of n is 62, since there are 64 bits of the Interface ID. However two bits (7th and 8th bit) have fixed values of 0.

The expected S_n or S_{obs} value is 0. If S_n or S_{obs} is large, then this would make P_{value} being small (<0.01). In the monobit test, large positive values of S_n are indicative of too many ones, and large negative values of S_n are indicative of too many zeros. In the Hamming distance test, large positive values of S_n are indicative of too many different bits, and large negative values of S_n are indicative of too few different bits (the degree of similarity is high between two vectors).

F. P_{value} within Frequencies of Blocks

For this purpose, P_{value} is to determine whether the proportion of ones within an M-bit block is approximately equal to $M/2$. A small P_{value} indicates large deviations from the equal proportion of 1's and 0's in at least one of the blocks. For each block, the proportion of 1's is computed. A chi-square statistic compares these block proportions to ½.

The statistic is referred to a chi-squared distribution with the degrees of freedom equal to the number of blocks. The P_{value} within the sequence of blocks can be calculated as:

$$P_{value} = \frac{\int_{x_{obs}^2}^{\infty} e^{-u/2} u^{N/2-1} du}{\Gamma(N/2) 2^{N/2}} = \frac{\int_{x_{obs}^2/2}^{\infty} e^{-u} u^{N/2-1} du}{\Gamma(N/2)} = igamc\left(\frac{N}{2}, \frac{\chi_{obs}^2}{2}\right) \tag{14}$$

where N is the number of blocks. For an N =1 block, it may uses (9).

Function *igamc* is the incomplete gamma function for *Q(a,x)* which is defined as [16]:

$$Q(a,x) \equiv 1 - P(a,x) \equiv \frac{\Gamma(a,x)}{\Gamma(a)} \equiv \frac{1}{\Gamma(a)} \int_{x}^{\infty} e^{-t} t^{a-1} dt \tag{15}$$

where

$$P(a,x) \equiv \frac{\gamma(a,x)}{\Gamma(a)} \equiv \frac{1}{\Gamma(a)} \int_{0}^{x} e^{-t} t^{a-1} dt \tag{16}$$

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and

$$\Gamma(z) = \int_0^\infty t^{z-1} e^{-t} dt \qquad (17)$$

where χ^2_{obs} measures of how well the observed proportion of ones (Hamming distance) within a given *M*-bit block matches to ½.

χ^2_{obs} can be defined as

$$\chi^2_{obs} = 4M \sum_{i=1}^{N} (\pi_i - \frac{1}{2})^2 \qquad (18)$$

where π_i is the proportion of ones in each *M*-bit block using the equation:

$$\pi_i = \frac{\sum_{j=1}^{M} \varepsilon_{(i-1)M+j}}{M} \qquad (19)$$

5. SIMULATION RESULTS AND DISCUSSION

A. System Environment

The system environment runs under Microsoft Windows XP Professional version 2002 Service Pack 2. The simulation has been developed, compiled, and launched using the Java™ Standard Edition Runtime Environment version 1.6.0. The simulation results are saved and can be opened for analysis using an office spreadsheet. The processor specification is AMD Turion™ X2 dual-core mobile technology RM-70 (1 MB L2 cache, 2.00 GHz, DDR2 800 MHz), supporting AMD HyperTransport 3.0 technology with RAM 1 GB DDR2 RAM.

Table 3 shows examples of the 128-bit key and 128-bit *IV* which have been used to generate Interface IDs. It has 2^8 (256) pairs.

B. Uniformity Test

Table 4 shows an example of a generated Interface ID using a static key and the *IV* table as shown in Table 3 which is `Key.CFB_KEY[55] = A6781379 24663511 50426844 8956333F` and `Key.CFB_IV[130] = B7536919 14542541 35865117 9031408C`. In this example, 256 sequences from the 2^8-bit plain text give rise to different Interface IDs being generated which belong to the same user ID, which is octal number 123456 (18 bits).

The fourth column shows the Hamming weight (number of 1's) for a particular Interface ID, S_{HW62} is the difference between the number of 1's and 0's within a block, while the sixth and seventh column represent the *erfc* and chi square within the block respectively. The last five rows are a statistical summary which represent of the summation, average, the lowest, the highest value, and the standard deviation.

Table 3. Key and IV Examples

No	Key	IV
1	A623132424113456	B623678913242411
	498767898901278F	345649878901278C
2	A624132524123457	B624679013252412
	498867908902279F	345749888902279C
3	A625132624133458	B625679113262413
	498967918903280F	345849898903280C
4	A626132724143459	B626679213272414
	499067928904281F	345949908904281C
5	A627132824153460	B627679313282415
	499167938905282F	346049918905282C
.	.	.
.	.	.
.	.	.
167	A789149025773622	B789695514902577
	515369559067444F	362251539067444C
.	.	.
.	.	.
.	.	.
252	A874157526623707	B874704015752662
	523870409152529F	370752389152529C
253	A875157626633708	B875704115762663
	523970419153530F	370852399153530C
254	A876157726643709	B876704215772664
	524070429154531F	370952409154531C
255	A877157826653710	B877704315782665
	524170439155532F	371052419155532C
256	A878157926663711	B878704415792666
	524270449156533F	371152429156533C

Figure 8 depicts the Hamming weight chart of the generated Interface IDs of Table 4. Here the `x` axis represents blocks (sequence of IPv6 addresses) and the `y` axis represents Hamming weight values. The Hamming weight average value is 31.473 and the standard deviation is 3.8592 for 256 blocks.

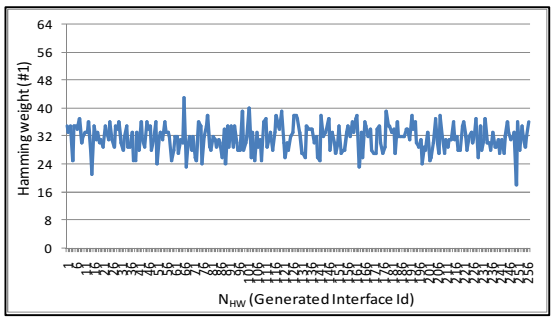

Fig. 8. Hamming Weight (#1) Chart

The Hamming weight gives a result in which the example first block of Table 4 indicates the number of 1's within the sequence of the Interface ID is 35. Figure 9 shows the distribution of S_{HW62}, where the highest occurrence is 30 for S_{HW62} = 2. Using (13), the S_{HW62} = 2×35 - 62

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

= 8. Figure 9 shows the distribution of $S_{HW_{62}}$, where the highest occurrence is 30 for $S_{HW_{62}} = 2$.

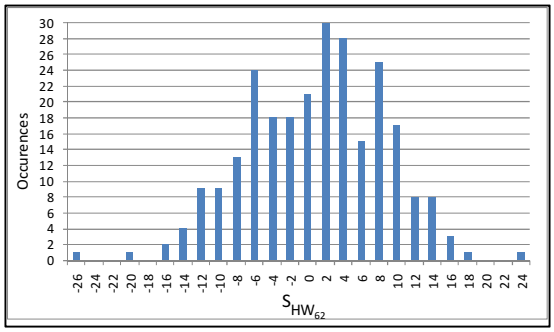

Fig. 9. $S_{HW_{62}}$ Occurrences

Table 4. Hamming Weight Of Generated Interface Ids

64-bit of Interface ID, User Data 6 Digits Octal = 123456 User Data 18-bit = 001010011100101110 7th & 8th bit (u & g) set to 00						
N_{HW}	48-Bit Plain	64-Bit IID	Hamming weight	$S_{HW_{62}}$	erfc	$(\pi-\frac{1}{2})^2$
1	000000000101010101010101 010101001010011100101110	010000001100101000100111001111111 111010101010101011111101011101010	35	8	$3.10e^{-1}$	$4.16e^{-3}$
2	000000010101010101010101 010101001010011100101110	110100001100101101101100101010101 010111000001100001111111011011001	33	4	$6.11e^{-1}$	$1.04e^{-3}$
3	000000100101010101010101 010101001010011100101110	111011001100100011101111101111001 000100010010111101101110100000101	35	8	$3.10e^{-1}$	$4.16e^{-3}$
4	000000110101010101010101 010101001010011100101110	000000001100100111110010011110101 000101000000111100110010100010000	25	-12	$1.28e^{-1}$	$9.37e^{-3}$
5	000001000101010101010101 010101001010011100101110	000111001100111011111110110010010 001011111010101001011011101010000	35	8	$3.10e^{-1}$	$4.16e^{-3}$
...	. . .	. . .	..	..	..	..
128	011111110101010101010101 010101001010011100101110	010101001011010110101101110100011 000110011110110110011101110101111	38	14	$7.54e^{-2}$	$1.27e^{-2}$
...	. . .	. . .	..	..	..	..
252	111110110101010101010101 010101001010011100101110	101101000011000100100110001101100 010000011100110001010100101110001	28	-6	$4.46e^{-1}$	$2.34e^{-3}$
253	111111000101010101010101 010101001010011100101110	000100000011011010111000011011010 101101101111110000110101111110110	35	8	$3.10e^{-1}$	$4.16e^{-3}$
254	111111010101010101010101 010101001010011100101110	111101000011011110000100110110001 100100010001110010010110100111111	32	2	$7.99e^{-1}$	$2.60e^{-4}$
255	111111100101010101010101 010101001010011100101110	100000000011010010100110010100011 010110111000110011101011100110001	29	-4	$6.11e^{-1}$	$1.04e^{-3}$
256	111111110101010101010101 010101001010011100101110	010110000011010111010001110000010 000110101100111110011100111010001	32	2	$7.99e^{-1}$	$2.60e^{-4}$
		n = 15872	8057	242	$1.25e^{2}$	$1.00e^{0}$
		Average	31.47	0.95	$4.89e^{-1}$	$3.92e^{-3}$
		Min	18	-26	$9.60e^{-4}$	$0.00e^{0}$
		Max	43	24	$1.00e^{0}$	$4.40e^{-2}$
		Std Dev	3.86	7.72	$2.83e^{-1}$	$5.38e^{-3}$

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

To measure the P_{value} from the first sequence example which has $S_{HW_{62}} = 8$, it may uses (12), $S_{obs} = \frac{|8|}{\sqrt{62}} = 1.016$. This shows that $P_{value} = erfc(\frac{1.016}{\sqrt{2}}) = 0.31$. Since $0.31 > 0.01$, it can be concluded that this sequence of Interface ID is considered to have good uniformity.

The lowest $S_{HW_{62}}$ is -26 and the highest value is 24. The lowest *erfc* is 9.60e^{-4} for $S_{HW_{62}}$ = -26 and the number of 1's within this sequence is 18. There are two occurrences for $erfc < 0.01$ (proportion = 2/256 = 0.007813), when $S_{HW_{62}} = -26$ ($erfc$ = 9.60e^{-4}) and $S_{HW_{62}} = 24$ ($erfc = 2.30e^{-3}$). The *erfc* average is 0.489; since 0.489 > 0.01, it can be concluded that the average of these Interface IDs is considered to have good uniformity.

The proportion of 1's within the sequence of Interface ID gives a result for which the example first row is 35/62 = 0.565. This is then compared to ½ to produce chi-square χ^2 which is (0.565 - 0.5)^2 = 4.16e^{-3}. This result has been used to calculate χ^2_{obs}.

The sequence of these Interface IDs gives an χ^2 of 1.0029. Using (18), the $\chi^2_{obs} = 4 \times 62 \times 1.0029 = 248.710$ and using (14), the $P_{value} = igamc(\frac{256}{2}, \frac{248.710}{2}) = 0.6163$. Since 0.6163 > 0.01, it can be concluded that these Interface IDs have good uniformity.

N_{HD}	i	j	HD Plain	HD IID ($IID_i \oplus IID_j$)	$S_{HD_{62}}$	erfc	$(\pi - ½)^2$
1	1	2	1	26	-10	2.04e^{-1}	6.50e^{-3}
2	1	3	1	30	-2	7.99e^{-1}	2.60e^{-4}
3	1	4	2	28	-6	4.46e^{-1}	2.34e^{-3}
4	1	5	1	24	-14	7.54e^{-2}	1.27e^{-2}
5	1	6	2	26	-10	2.04e^{-1}	6.50e^{-3}
...	..	..	..	..	..	..	..
16320	75	226	5	31	0	1.00	0
...	..	..	..	..	..	..	..
32636	253	255	1	32	2	7.99e^{-1}	2.60e^{-4}
32637	253	256	2	31	0	1.00	0
32638	254	255	2	29	-4	6.11e^{-1}	1.04e^{-3}
32639	254	256	1	30	-2	7.99e^{-1}	2.60e^{-4}
32640	255	256	1	29	-4	6.11e^{-1}	1.04e^{-3}
n = 1044480				995691	-32298	16339.8	132.49
Average			4.016	30.51	-9.9e^{-1}	5.01e^{-1}	4.06e^{-3}
Min			1	16	-30	1.57e^{-5}	0
Max			8	48	34	1	7.52e^{-2}
Std Dev			1.40	3.92	7.84	2.95e^{-1}	5.63e^{-3}

Table 5. Hamming Distance of Generated Interface IDs

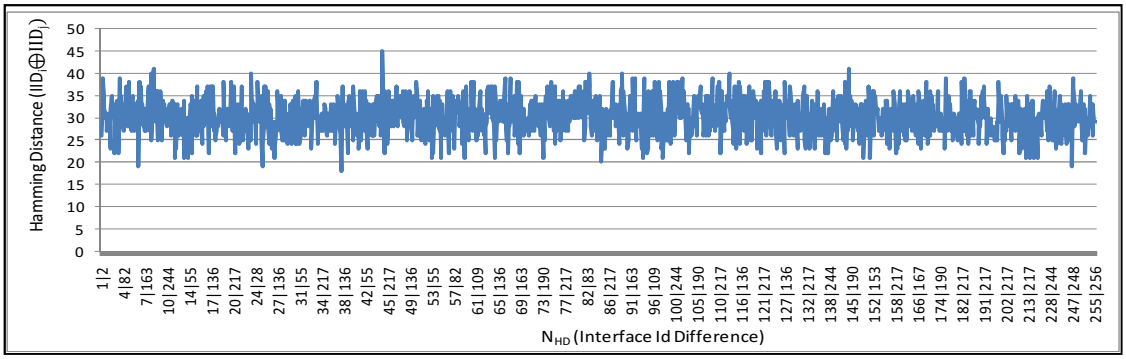

Fig. 10. Hamming Distance Chart

C. Avalanche Effect Test

Table 5 shows the Hamming distance of the generated Interface ID simulation results. It is performed over 32640 blocks for 256 encrypted addresses and compares Interface ID 1 (IID1) to Interface ID 2 (IID_2), IID_1 to IID_3, and so on in order to obtain all Hamming distances.

$$IID_i \oplus IID_j ; i = 1..N_{HW} ; j = (i+1)..N_{HW} \quad (20)$$

The range value of this Hamming distance is 0 to 62 (excluding the 7th and 8th bit of the Interface ID as they both fixed at 0). If the

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Hamming distance value is 0, it means that all 62 bits for both Interface IDs are same (the highest degree of similarity) and if the value is 62, it indicates that all 62 bits for both Interface IDs are different.

Figure 10 depicts the Hamming distance chart of the generated Interface IDs of Table 5. Here the x axis represents the difference of each Interface ID and the y axis represents Hamming distance values. The Hamming distance average value is 30.505 and the standard deviation is 3.919 for 32640 blocks.

The Hamming distance result for sequence number 1 which is the difference of Interface ID 1 and Interface ID 2 is 26. The value of *n* is 62, so using (13), the $S_{HD_{62}} = 2\times26 - 62 = -10$. Figure 11 shows the distribution of $S_{HD_{62}}$, where the highest occurrence is 3314 for $S_{HD_{62}} = 0$.

To measure P_{value} of the first sequence example for which $S_{HD_{62}} = -10$, it may uses (12), $S_{obs} = \frac{|-10|}{\sqrt{62}} = 1.270$. It shows that the $P_{value} = erfc(\frac{1.27}{\sqrt{2}}) = 0.204$.

Since $0.204 > 0.01$, it can be concluded that both Interface IDs have a good avalanche effect.

The lowest $S_{HD_{62}}$ is -30 and the highest value is 34. The lowest *erfc* is $1.575e^{-5}$ for $S_{HD_{62}} = 34$ for wihich the Hamming distance of sequence 22 and 91 is 48.

There are 211 occurrences for *erfc* < 0.01 (proportion = 211/32640 = 0.006465), which is 142 occurrences for $S_{HD_{62}} < -20$ and 69 for $S_{HD_{62}} > 20$. The *erfc* average is 0.5006; since 0.5006 > 0.01, it can be concluded that the average of these Interface IDs is considered to have a good avalanche effect.

The sequence of these Hamming distances gives an χ^2 of 132.490. Using (18), $\chi^2_{obs} = 4 \times 62 \times 132.490 = 32857.387$ and using (14), the

$$P_{value} = igamc(\frac{32640}{2}, \frac{32857.387}{2}) = 0.197 .$$

Since $0.197 > 0.01$, it can be deduced that these Interface IDs have a good avalanche effect.

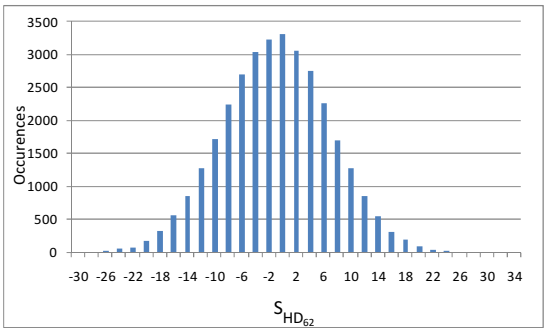

Fig. 11. $S_{HD_{62}}$ Occurrences

6. CONCLUSION

This paper has presented simulation results for randomness test in terms of uniformity using the monobit test and avalanche effect using the Hamming distance tests of a one-to-many mapping mechanism between user space and the Interface ID part of the IPv6 address space. The results showed that the expected uniformity proportion and avalanche effect of around 50% have been achieved. It showed that both the P_{value} of the monobit tests which represent uniformity for the sequence of bits and the frequency of blocks are more than 0.01. The P_{value} of the Hamming distance tests which represent the avalanche effect of both the sequence of bits and the frequency of blocks are more than 0.01. The Interface IDs which have been generated using CFB-AES can be considered to be randomly generated with a confidence level of 99%. Thus, in order to respect user privacy, the owners of the IPv6 addresses are difficult to identify by eavesdroppers.

REFERENCES

[1] N. Hakiem, A. U. Priantoro, M. U. Siddiqi, and T. H. Hasan, Generation of IPv6 Addresses Based on One-to-Many Reversible Mapping Using AES, in *Recent Progress in Data Engineering and Internet Technology,* Lecture Notes in Electrical Engineering. vol. 157, Springer-Verlag Berlin Heidelberg: 2012, pp. 183-189.

[2] RFC3315, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," in *Standards Track*, ed: IETF Network Working Group, 2003.

[3] H. Ju and J. Han, "DHCP Message Authentication with an Effective Key Management," *World Academy of Science, Engineering and Technology,* vol. 8, 2007, pp. 570 - 574.

[4] RFC4291, "IP Version 6 Addressing

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Architecture," in *Standards Track*, ed: IETF Network Working Group, 2006.
[5] RFC4941, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6," in *Standards Track*, ed: IETF Network Working Group, 2007.
[6] RFC3972, "Cryptographically Generated Addresses (CGA)," in *Standards Track*, ed: IETF Network Working Group, 2005.
[7] J. Kempf and C. B. Gentry, *Secure address proxying using multi-key cryptographically generated addresses*, Patent US 7925027 B2, to NTT DoCoMo, Inc., 2011.
[8] RFC4193, "Unique Local IPv6 Unicast Addresses," in *Standards Track*, ed: IETF Network Working Group, 2005.
[9] S. Yang, *et al.*, "Dual Addressing Scheme in IPv6 over IEEE 802.15.4 Wireless Sensor Networks," *ETRI Journal,* vol. 30, October 2008, pp. 674 - 684.
[10] S. Groat, M. Dunlop, R. Marchany, and J. Tront, "The privacy implications of stateless IPv6 addressing," *Proc. Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, Oak Ridge, Tennessee, 2010, p. 1-4.
[11] S. Groat, M. Dunlop, R. Marchany, and J. Tront, "What DHCPv6 says about you," *Proc. Internet Security (WorldCIS), 2011 World Congress on*, 2011, p. 146-151.
[12] N. Hakiem and M. U. Siddiqi, "One-to-Many Reversible Mapping for IPv6 Address Generation: Simulation Software Development," *Journal Of Theoretical And Applied Information Technology,* vol. 47, 31 January 2013, pp. 892 - 901.
[13] M.-S. Kim, Y. J. Won, and J. W.-K. Hong, "Application-Level Traffic Monitoring and an Analysis on IP Networks," *ETRI Journal,* vol. 27, February 2005, pp. 22-42.
[14] N. Hakiem, M. U. Siddiqi, and S. P. W. Jarot, "Collision Probability of One-to-Many Reversible Mapping for IPv6 Address Generation," *Proc. 2012 International Conference on Computer and Communication Engineering (ICCCE)*, Kuala Lumpur, Malaysia, 2012.
[15] N. Hakiem, *et al.*, "Implementation of IPv6 address generation mechanism for enterprise wireless local area network in open source DHCPv6," *Proc. 2010 International Conference on Computer and Communication Engineering (ICCCE)*, Kuala Lumpur, Malaysia, 2010, p. 1-5.
[16] NIST, "A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications," vol. Special Publication 800-22, ed: Technology Administration U.S. Department of Commerce, 2010.
[17] J. C. H. Castro, *et al.*, "The strict avalanche criterion randomness test," *Mathematics and Computers in Simulation,* vol. 68, 2004, pp. 1-7.
[18] H. Feistel, "Cryptography and computer privacy," *Scientific American,* vol. 228, 1973, pp. 15-23.
[19] W. Stallings, *Cryptography and Network Security, Principles and Practices*, 4 ed., Pearson Prentice Hall, 2006.
[20] F. L. Bauer, *Decrypted Secrets: Method and Maxims of Cryptology*, Fourth, Revised and Extended ed., Springer-Verlag Berlin Heidelberg, 2007.
[21] R. W. Hamming, "Error Detecting and Error Correcting Codes," *Bell System Technical Journal,* vol. 29, April 1950 1950.
[22] E. Dawson, H. Gustafson, and A. N. Pettitt, "Strict Key Avalanche Criterion," *Australasian Journal of Combinatorics,* vol. 6, 1992, pp. 147-153.
[23] P. R. Mishra, I. Gupta, and N. R. Pillai, Generalized Avalanche Test for Stream Cipher Analysis, in *Security Aspects in Information Technology,* Lecture Notes in Computer Science. vol. 7011, Springer-Verlag Berlin Heidelberg: 2011, pp. 168-180.
[24] D. E. Smith, De Moivre on the Law of Normal Probability, in *A source book in mathematics*, H. M. Walker, Ed., Dover Publications: 1985, pp. 75-84.
[25] S. Artstein, K. M. Ball, F. Barthe, and A. Naor, "Solution of Shannon's Problem on the Monotonicity of Entropy," *American Mathematical Society,* vol. 17, 2004, pp. 975-982.