International Journal of Engineering & Technology, 7 (4.19) (2018) 624-628

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Secure Data Communications using Cryptography and IPv6 Steganography

Ra'ad A. Muhajjar*[1], Farah A. Badr[2]

[1]*Dept. of Computer Science, College of computer Sc. And IT., Basrah University, Iraq*
[2]*Dept. of Computer Science, College of Science, Basrah University, Iraq*
**Corresponding Author Email: raadmahjar@yahoo.com*

Abstract

Security is an important topic in any communication especially if the communicating endpoints have confidential data and require utilizing special techniques to protect it. In this research paper, cryptography method was combined with steganography to enable sending confidential data by utilizing IPv6 protocol header as a cover to conceal secret messages. Flow label field is the field that will be used as a covert channel to exchange critical data between the endpoints. To generate the encryption/decryption key, a proposed pseudo-random number generator was applied. The generated numbers show good statistics when tested using standard statistical tests. In cryptography, RC6 was executed in CBC mode to encrypt/decrypt N blocks of data. For origin authentication, a proposed MAC was implemented to the encrypted data to obtain MAC value that will be sent along with the encrypted data to the receiving endpoints. After obtaining the encrypted data and the MAC, both will be embedded in IPv6 flow label field.

Keywords: *Data Hiding, Cryptography, Steganography, Network Steganography, TCP/IP.*

1. Introduction

Information security has evolved as a significant manner in our daily life. The new transmission technologies development forces specific strategies of security mechanisms more specifically in the state of data communications. Network security significance will be expanded as the size of data being exchanged across the Internet [1]. Security presence can be felt in every aspect of communication, and it is very vital in many applications especially in the Military Sector. So, the users may require secure and private communications in order to protect their confidential data from hacking during the transmission over an open channel [2].

Cryptography and steganography are very interactive methods for secure communications. Using only Cryptography isn't enough for protecting the secret data, As well as for steganography. Thus to increase the security level of information and to maintain the secrecy, the privacy of data, the two techniques are used together. Cryptography can be used wherever steganography is inefficient and steganography can be used wherever cryptography is inefficient. Both security methods provide protection in their own ways, but to add multiple layers of security it is always considered a good practice to utilize a combination of these techniques [3].

The typical methods of stenography, utilize digitize media files (such as images, text, or audio files) as a cover object to conceal secret data. Hiding data within network level by utilizing protocols is relatively a new branch of data hiding. All the techniques that utilize protocols to hide data can be divided within the generic term of protocol steganography (i.e. network steganography). The advantages of network steganography [4]:

- **Suitable as a communication link:** Covert channels could be implemented and designed at any layer of the TCP/IP. This conflicts with media steganography techniques; since in media steganography transmitting a single file requires transmitting a single block of stego-object, where the length of the embedded file is strictly controlled by the cover object size.
- **The Short lifespan of stego object:** Network steganography differs from media steganography, in that a stego-object transmitted through a network doesn't have a long lifecycle. This is because in network steganography the cover is the network itself. Once the message is extracted from the cover, packets will be discarded; the stego object is also destroyed.
- **Flexible bandwidth:** Since the bandwidth of media steganography methods is restricted by the cover file size, network steganography methods bandwidth is only restricted by the selected protocol nature and the network capability.

The paper is structured as follows: Section 2 presents selected steganographic methods that were accomplished in IP protocol. The proposed system is introduced in section 3. Simulation environment is reviewed in section 4, the analysis and the results are discussed in section 5 and finally, the conclusion of the paper is in section 6.

2. Related Work

IP is an unreliable, connectionless protocol and is the primary protocol in the TCP/IP protocol suite which is responsible for addressing packets and routing them between hosts. IP comes in two versions (IPv4) and (IPv6). Cauich et al. [5] employ the Fragment Offset and the Identification fields in IPV4 header for messages hiding. Their method allows hiding 29 bits in every packet that is not fragmented. Zander et al. [6] suggest an improved 1-bit-per-packet covert channel by using the Time To Live field (TTL), analyzing initial TTL values and regular TTL occurring in the network. They proposed using two diverse starting values of TTL, the normal initial value as High-TTL (binary 1) and High-TTL -1 as Low-TTL (binary 0). In [7] one

approach they suggest is to use the type-of-service field of IP packet which is of 8 bits length to send data. In those 8 bits, 2 bits are unused and these 2 could be used to transfer the hidden data. Rowland [8], Dhobale et al. [9] and Goudar et al. [10] presented network steganographic methods which hide a secret message into identification field of IPV4 header (IP ID). IP ID approach allows up to 16-bits- per-packet. The shortcoming of these techniques (i.e. that are based on the fragmentation strategy), is when the fragmentation of packets occurs. A good amount of proposals have been done in IPv4 protocol. But future computer network infrastructure will use IPv6; IPv6 is the new generation Internet protocol that is set to slowly merge with and ultimately replaces IPv4. In [11] the authors suggest using the source address fields of (IPv6). They use the IPv6 source address field as a covert channel with the capability of transferring 64 bits-per-packet, each packet in their proposal will be assigned with a sequence number to indicate the order of packets at the receiver, and they performed AES with the private key to provide a high level of security. Bobade et al. [12] implemented a covert communication channel using flow label field in IPV6 header, to enhance the security of their proposal they utilized RSA encryption technique, they first encrypt the information then embed it in the flow label field .the capacity of their channel is 20 bits- per-packet.

3. The Proposed System

The proposed system aims to increase the level of security by using a combination of two security techniques: cryptography and steganography. Because while steganography hides the existence of a message cryptography distorts the message itself. To generate the key that will be used in the encryption/decryption process a proposed pseudorandom number generator was applied. When the encryption/decryption key is generated, CBC-RC6 encryption algorithm is implemented, then for origin authentication a proposed Message authentication code is utilized to calculate the MAC, after obtaining the ciphertext and the MAC, both values are embedded in IPv6 flow label field. The architecture of the proposed system is shown in Figure.1.

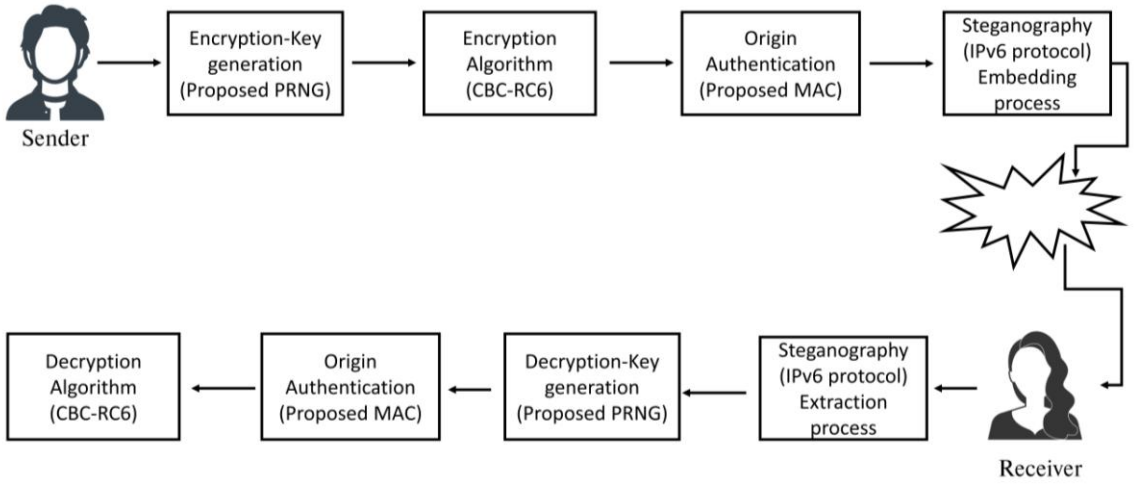

Fig. 1: Architecture of the Proposed System

3.1 Pseudo-Random Number Generator (PRNG)

The proposed system require using Pseudo-random number generators which are able to produce random numbers, to generate the encryption/decryption keys. The proposed generator is a simple and fast pseudorandom number generator to generate the encryption/decryption key. The seed must be unpredictable. Thus it must be random or pseudo-random, and it must be secure. The steps of generating the pseudo-random numbers are explained in Pseudocode 1. The results of the proposed PRNG were tested and they appear to be random since they pass the predetermined tests [13] as shown in Table.1.

Pseudocode 1. The proposed PRNG

```
Input: the seed of 128 bit
Output: PRNs each of length 128 bit
Procedure:
K =128
J=128
For S from 1 to N do
  For i from 1 to k do
          V (i) ← Seed (k)
             k← k-1
  End for
  For i from 1 to 128 do
          If (i<128) then
                    NV (i) ← bitxor (V (i), V (i+1))
          Else
                    NV (i) ← bitxor (V (i), V (1))
 End if
  End for
For i from 1 to 128 do
          NV1 (i) ← NV (j)
          j← j-1
End for
```

```
// Divide the result (NV1) into 16 group each of length 8 bits
K1← 1;    K2← 8;
For i from 1 to 16 do
                    G (i) ← NV1 (K1: K2)
                    K1← K1+8;
                    K2← K2+8;
 End for
 A← 16
 For i from 1 to 16 do
          R (i) ← G (A)
          A← A-1;
 End for
PRN (S) ← (R (1) ….R (16))
PRN1(S) ← (PRN (S) <<< 8)
Seed ← PRN1 (S)
End for
```

3.2 Encryption

The encryption process involves using RC6 encryption algorithm in CBC mode.RC6 will handle a block of fixed size each time, thus in order to process N of blocks RC6 needs to be operated in a mode of operation. CBC mode is a very popular mode to encrypt N of blocks using the same key, this mod was chosen due to its security, because unlike ECB mode the plaintext if repeated, will results in different ciphertext, this will increase the level of difficulty for predicting the resulted ciphertext. CBC requires an IV that will be shared among the sender and the intended receiver(s). The encryption process using CBC-RC6 is shown in Figure.2.

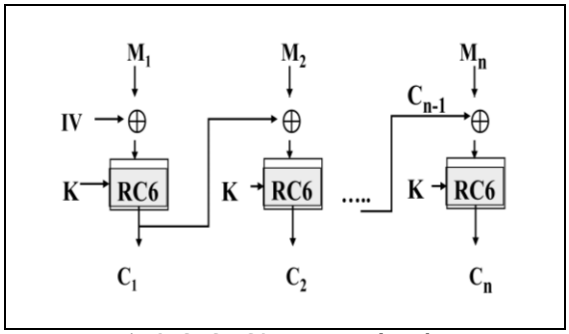

Fig. 2: CBC-RC6 encryption algorithm

3.3 Message Authentication Code (MAC)

Message authentication codes are commonly encountered mechanisms that provide data origin authentication, which is considered a stronger notion then data integrity. The proposed MAC has two processes as shown in Figure.3.

a) Authentication key derivation process (AKD)
This process will use the same encryption/decryption key to derive ($K^{/}$) which will be used in the first phase of the authentication process as shown in Figure.3.

b) Authentication process
The authentication process involves using a block cipher algorithm to encrypt N blocks of ciphertext to calculate the MAC that will be sent along with the ciphertext to the receiving entities. After obtaining (K/) from (AKD) process, this key will be used to encrypt the first block of ciphertext to obtain the first block of MAC (A1). Then each encryption phase will utilize the MAC resulted from the previous phase as the encryption key, this step will make each resulted value depends upon the previous ones which will help to indicate any changes at the receiver(s). The steps of calculating the MAC are illustrated in Pseudocode.2.

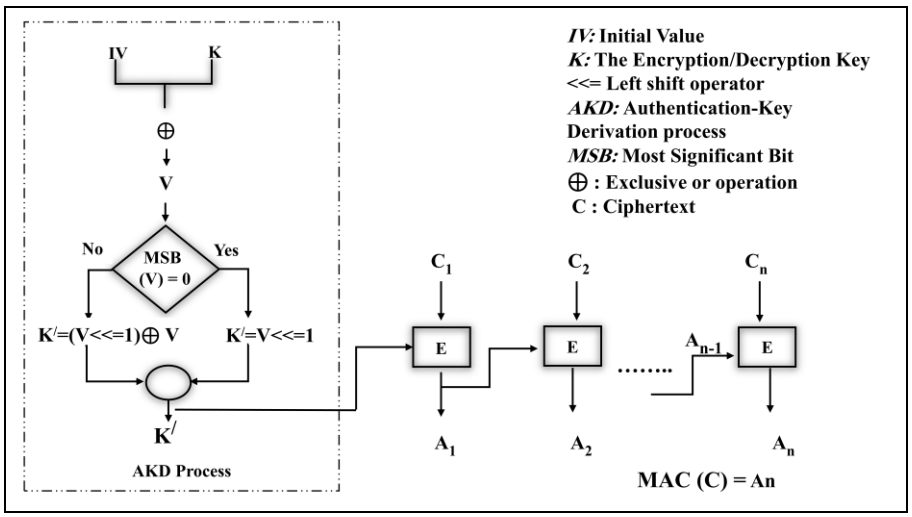

Fig. 3: The proposed MAC

Pseudocode 2. The Proposed MAC
Input: encryption key, initial value, ciphertext
Output: MAC value
Step 1: AUTHENTICATION-KEY DERIVATION PROCESS
V← bitxor (K, IV)
If (MSB (V== 0)) then
K'← (V≪=1)
Else
K'← bitxor ((V≪=1), V)
End if
Step 2: AUTHENTICATION PROCESS
A (1) ← Enc. (C (1), K')
For i from 2 to n do
A (i) ← Enc. (C (i), A (i-1))
Return (A (n))

The time required to encrypt the data and to calculate the MAC is shown in Table.2.

3.4 IPv6 Steganography

To maintain the secrecy of the secret message, the ciphertext along with the MAC will be embedded in flow label field of IPv6 header. In this research, the internet protocol (IPv6) was utilized since it is the new generation protocol that will replace the previous version (IPv4).

3.4.1 IPv6 Embedding Process

After encrypting the secret message and calculating the MAC, the message along with the MAC are concealed in flow label field. Flow label numbers ranging from 1 to FFFFF hex. The 20 bits (i.e. 5 hex characters) of the field in each packet will be used as follow: When embedding the data in flow label field, the first 8-bits of the field will be used to identify the sequence of each packet, the next 8-bits will be used to hide the secret bits, and the last 4 bits will be used to transfer the MAC. The capacity of the proposed channel will be 8 bits-per-packet. Although the proposal narrows the capacity from 20 bits-per-packet to 8 bits-per-packet, it will assure the correct order of packets at the receiver(s).

3.4.2 IPv6 Extraction Process

After receiving the packets from the sender, the receiver will arrange the received packets according to their sequence number, and rearrange MAC elements. The receiver will initially generate the decryption key by using the proposed PRNG, then check whether the received data were intact or changed by applying the proposed MAC. If the calculated MAC matches the received one then the receiver implements CBC-RC6 decryption; else the ciphertext will be rejected and the receiver will request to retransmit the packets.

3.5 Decryption

After authenticating the originator of the received messages using the proposed MAC, the receiver will use RC6 decryption algorithm in CBC mode. To retrieve the plaintext. The steps of CBC-RC6 decryption are shown in Figure.4. The time required to decrypt the received ciphertext and to recalculate the MAC is shown in Table.2.

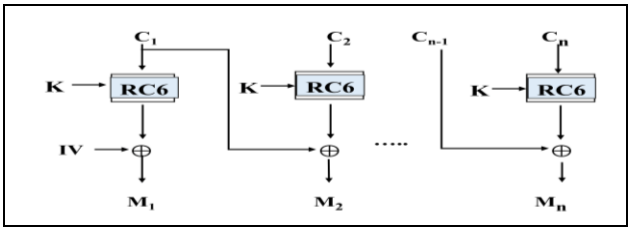

Fig. 4: CBC-RC6 decryption

4. Simulation Environment

In order to simulate the proposed system, GNS3 (graphical network simulator), was used as shown in Figure. 5.

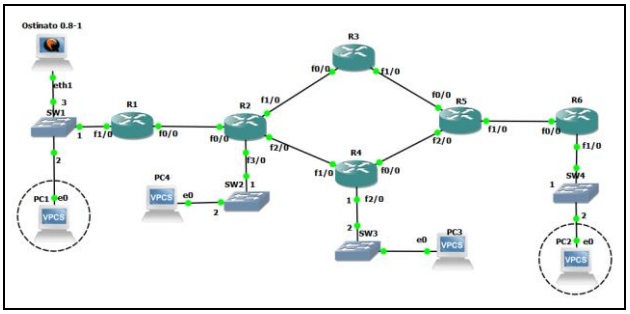

Fig. 5: GNS3 Topology

This topology was built to simulate sending IPv6 packets from PC1 to PC2. There are many network tools that enable crafting packets and replaying them (i.e., resend packets through network card).[14] In our experiments, we used Ostinato tool for interactive network packet crafting. Figure.6 show the packets that were sent from PC1 to PC2 and were captured by Wireshark.

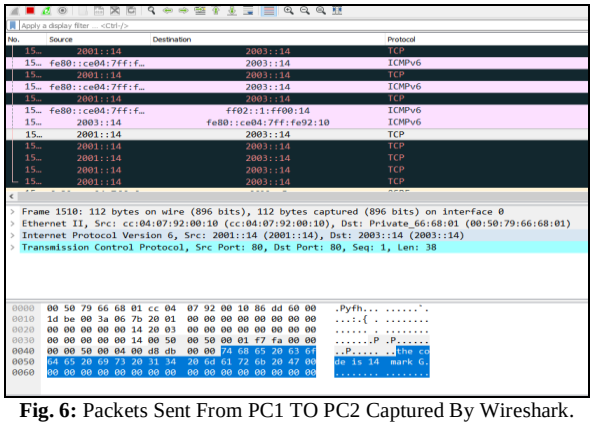

Fig. 6: Packets Sent From PC1 TO PC2 Captured By Wireshark.

5. Analysis and Results

From the analysis over a 1 Kbps link, the time required for transmitting let's say, 1 KB of information by the sender is far less than the time required by an intruder to decode the same information extracted from the header field. Thus, the practicality of the new proposed method lies in the fact that by the time the

intruder decrypts the message, numerous of packets resulting in heavy bulks of data would be received by the receiver. As an initial step, in order to measure the complexity in time it takes for different (numbers, alphabets and alphanumeric), and for varying number of inputs (10, 20, 30 and 40) characters. RC6 algorithm has been analyzed. Figure.7. shows the analysis made based on time for each kind of input.

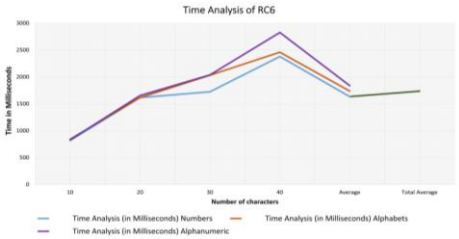

Fig. 7: Graphical Representation of the Analysis of RC6

The time is measured in milliseconds. The most important point to be noticed here at this step is that, as in the case of the encryption process at the sender side which takes time in the order of milliseconds, all the steps that follows would also be processed within a short period of time and the information will be sent, received and decoded by the receiver in the same order of time.
The result of the proposed pseudo-random number generator is shown in Table.1, as shown in Table 1, the generated sequences show good statistics when tested using standard statistical tests.

Table.1: sample of the Results of the proposed pseudo-random number generator

No	Sequence	Frequency test	Serial test	Poker test	Runs test	Autocorrel-ation test	Linear complexity
1	43914962A02CD7210C654BF699912A0C	3.7813	4.494	4.0952	4.9320	0.9129	64
2	E259EDD3F03ABCB18A57EE0D5559BF0A	1.1250	1.544	10.9524	2.8907	0.7303	64
3	93751B3A0827E2E94F7C190BFFF5608F	0.5000	2.043	13.2381	1.9571	0.1826	64

Table.2, shows the time required to accomplish the encryption process (encryption and authentication), and the time to implement the decryption process (authentication and decryption).

Table 2: Encryption/Decryption & Authentication time for different block sizes

Data size (bytes)	Encryption & Authentication time in milliseconds	Authentication & Decryption time in milliseconds
16	1,987.041	1,332.622
24	3,962.504	2,886.359
32	4,597.782	3,025.242
64	5,672.077	4,042.51

6. Conclusion and Future Work

In this paper we proposed a system to secure the communication channel between the communicating entities. The system combines network steganography with cryptography. Steganography in IPv6 was implemented for covert communications using flow label field. In cryptography, RC6 algorithm was implemented in CBC mode to achieve more security which is very useful in areas like Military. The proposed system provides higher level of security then others, because previous techniques only consider using Steganography whereas we are using cryptography followed by Steganography also the embedding process is more complex than the previous ones, in other words if packets were captured by an intruder, the intruder needs to know the key, the encryption algorithm that has been used and the way of embedding the information in flow label field, by that time numerous of packets will be received and decoded by the receiver. As a future work, a combination of IPv6 steganography with other layer protocols could be used to transfer data, also using additional security methods such as digital watermarking.

References

[1] P. Xue, H. Liu, J. Hu, and R. Hu, "A multi-layer steganographic method based on audio time domain segmented and network steganography," in AIP Conference Proceedings, 2018, p. 020046.
[2] P. Sharma and S. Dahiya, "Network Security with Cryptography," 2018.
[3] R. K. Yadav and M. Kushwaha, "Message Hiding Using Steganography and Cryptography," 2018.
[4] N. Singh, J. Bhardwaj, and G. Raghav, Network Steganography and its Techniques: A Survey vol. 174, 2017.
[5] E. Cauich, R. G. Cárdenas, and R. Watanabe, "Data hiding in identification and offset IP fields," in International Symposium and School on Advancex Distributed Systems, 2005, pp. 118-125.
[6] S. Zander, G. Armitage, and P. Branch, "A survey of covert channels and countermeasures in computer network protocols," IEEE Communications Surveys & Tutorials, vol. 9, pp. 44-57, 2007.
[7] T. G. Handel and M. Sandford, "Data hiding in the OSI network model," in Proceedings of Information Hiding: First International Workshop, 1996, pp. 73-93.
[8] C. H. Rowland, "Covert channels in the TCP/IP protocol suite," First Monday, vol. 2, 1997.
[9] D. Dhobale, V. Ghorpade, B. Patil, and S. Patil, "Steganography by hiding data in TCP/IP headers," in Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, 2010, pp. V4-61-V4-65.
[10] [R. Goudar, S. Wagh, and M. Goudar, "Secure data transmission using steganography based data hiding in TCP/IP," in Proceedings of the International Conference & Workshop on Emerging Trends in Technology, 2011, pp. 974-979.
[11] M. Alaa Qasim, D. Pawar, and I. Publication, ENCRYPTION & STEGANOGRAPHY IN IPv6 SOURCE ADDRESS vol. 4, 2013.
[12] S. Bobade and R. Goudar, "Secure data communication using protocol steganography in IPv6," in Computing Communication Control and Automation (ICCUBEA), 2015 International Conference on, 2015, pp. 275-279.
[13] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, Handbook of applied cryptography: CRC press, 1996.
[14] S.V. Manikanthan, T.Padmapriya, "United Approach in Authorized and Unauthorized Groups in LTE-A Pro", Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 10-Special Issue, 2018, pp. (1137-1145).