Available online at www.ijpe-online.com

International Journal of Performability Engineering

Vol. 13, No. 5, September 2017, pp. 598-609
DOI: 10.23940/ijpe.17.05.p5.598609

A Covert Communication Scheme based on DNA Microdots for Port Hopping

Leyi Shi[a,b,*] , Yuwen Cui[a], Xiaotong Liu[a], Hui Sun[a], Zhiyu Xue[a], Shufen Zhang[b,c]

[a]*College of Computer and Communication Engineering, China University of Petroleum (East China), Qingdao, 266580, China*
[b]*Hebei Key Laboratory of Data Science and Application, Tangshan, 063210, China*
[c]*North China University of Science and Technology, Tangshan, 063210, China*

Abstract

Port hopping is an effective solution for Moving Target Defense (MTD), which randomly changes the server's service port number to provide a robust communication against malicious Denial of Service (DoS) and Distributed DoS (DDoS) attack. Although a series of novel and feasible port hopping mechanisms have been proposed and implemented, most of them cannot prevent the messages transmitted in the network from being intercepted by an attacker. This paper addresses the problem of defending the eavesdropping attack with the port hopping process. We propose a new module that combines the properties of port hopping and the encryption of DNA microdots to resist the eavesdropping attacks in the network. The proposed port hopping process is compatible with the UDP and TCP protocols, in which the four IP addresses equipped in the server stand for the different nucleotides of DNA strands. We implement the proposed scheme and conduct the theoretical analysis on it. The theoretical analysis and experimental results illustrate that the proposed scheme can effectively defend against the DoS/DDoS and eavesdropping attacks.

Keywords: port hopping; Moving Target Defense; moving target defense; Denial of Service; DNA microdots; eavesdrop attack

(Submitted on March 16, 2017; Revised on June 2, 2017; Accepted on August 15, 2017)

© 2017 Totem Publisher, Inc. All rights reserved.

1. Introduction

The Internet is becoming an indispensable technology of human society. Meanwhile, the Internet in its original form was designed to be an open and distributed environment that makes attackers take advantage to connect to the Internet. Thus, there are many potential online dangers and many variables with each individual personality - only you can decide when they are ready, such as DoS/DDoS, eavesdropping and deceptions attacks [19].

Denial of service attack is typically attempting to flood a target host with a heavy traffic to temporarily or indefinitely deplete the computer resources or network bandwidth. It will interrupt or suspend services of a host to the legitimate users. There are two general forms of DoS attacks: crash services and flood services. Considering adversaries that can eavesdrop and launch DoS attacks to the applications' open ports, solutions based on port hopping have been proposed [15]. Port hopping is an effective moving target defense mechanism [5] that turns the asymmetric scale of network attacks and defenses, dynamically maps a service's port to an unused pseudo-random port [16], can provide a robust communication environment for clients and servers. The port hopping is designed to allow the client to access the server's services by assigning the ephemeral and synchronous random port number. However, the existing port hopping mechanisms cannot work properly when the attackers can capture and analyze the network packets.

The DNA molecule is a double helix, resembling a ladder that is twisted along its length that carries the genetic instructions used in growth development. The four bases found in DNA are adenine (A), cytosine (C), guanine (G) and thymine (T). The structure of the DNA double helix and the detailed structure of two basic pairs are represented in Figure 1. Each nucleotide in DNA has a sugar component joined to a phosphate group at one point on the sugar, and a nitrogen

* Corresponding author.
E-mail address: shileyi@upc.edu.cn.

containing base attached at another point. DNA contains two such chains, twisted around each other to form a double-stranded helix with the bases on the inside. Every A on one chain forms weak bonds with a T on the other strand, and every C on a strand bond weakly to a G on the opposite chain. Inspired by this, the idea of DNA computing was introduced to solve the complex mathematical problem in 1994 [1]. Then, the microdots as the emerging field of information security achieved lots of development. The microdot is a means of reducing the size into small discs of text or an image to conceal messages that sent for steganographic purposes in Germany between World War I and World War II. The DNA microdots have been used to store and encrypt the message in terms of DNA sequences for hiding the original data. It has been verified that it is still extremely difficult for an adversary to read the message without knowing the specific primer sequences when it somehow detected such a microdot. Thus, the DNA microdots, with a large data storage capacity, will be useful for secure data transmission over Internet.

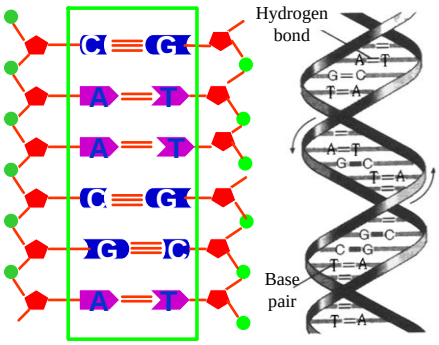

Figure 1. DNA Molecular Structure

In this work, we present a new scheme based on the DNA microdots technology to improve the security of the random port hopping. This paper combines random port hopping technology and traditional DNA microdots hiding technology to transfer information. Furthermore, we use four IP addresses to denote the four different nucleotides through an algorithm of encrypting ciphers as high volume DNA microdots data density in receivers that will be difficult for attackers to capture and analyze the communicated messages. It is still extremely difficult to decrypt the message without being aware of the specific primer sequences, even if an adversary somehow detected such a sequence of IP addresses. We summarize the contributions in this paper as follows:

- We present a new scheme to resist the DoS/DDoS attacks and the eavesdropping attacks. The scheme applies the DNA microdots to the technology of random port hopping, and can be used to hide the communicated messages from attackers.
- We develop a new DNA encoding rule to encrypt the communicated messages.
- We propose an access authentication method in receivers in order to receive the DNA encoding sequence from the sender. Four IP addresses will be configured in receivers, which stand for the four based founds in DNA to receive the DNA encoding sequence sent by sender.
- We build a prototype and evaluate it. The result shows that if the attackers can intercept and capture the communicated messages in the network, it is difficult to find the original messages.

The rest of this paper is organized as follows: Section 2 analyzes the existing implementations. Section 3 provides the details of implementation of the DNA cryptosystems with port hopping and section 4 describes the performance evaluation. Finally, section 5 concludes this paper.

2. Related Works

H. C. J. Lee et al. [155] propose the random port hopping (RPH), where the UDP/TCP port number used by the server with a secret key shared between the server and the client. They show that the port hopping technique is effective in detecting and filtering malicious traffic, and hence improved the reliability of changeable traffic flow. However, their method needs to synchronize the local clock between the sender and the receiver. Badishi et al. [2], develop a more sophisticated technique. They introduce an ack-based method and overcome the problem of synchronization in port hopping. Then they propose a method [3] and architecture [4] based on the concept of random port hopping to build dams to protect servers from DoS attacks, which is called Beaver.

L. Y. Shi et al. [20], introduce a novel scheme of timestamp-based synchronization, and they also present a prototype that use a new tactic for port and address hopping. Z. Fu et al. [8], propose an algorithm to manage the time discrepancy through the local clock increase, called BiGWheel and HoPerAA. The algorithm works by communicating with multiple receivers in a port-hopping manner and realizing the RPH in the presence of clock-drift.

Hari and Dohi [11] develop a simulator that can operate independently to take place the sensitivity analysis of RPH in terms of the highest communication rate. They also propose a fine-grained RPH algorithm for more general DoS attack patterns. Then they develop a quantitative model of RPH by means of the discrete-time Markov chain (DTMC) and refine the existing RPH protocol in terms of the communication success rate [10]. Kumar et al. [14], propose an algorithm by using the IP addresses and random port numbers to initially server with a sharing cryptographic key. The client can use the random port number to exchange the messages with the server.

There are many traditional cryptographic algorithms that used to encrypt and decrypt messages for protecting secret information from divulging. In [23], first state the DNA strands can be useful to encode information. Adleman [1], G. Z. Cui et al. [7], X. Wang et al. [22], introduce the basic idea of DNA computing as a new field of cryptography that can realize several security technologies such as Encryption, Steganography, Signature and Authentication. They use DNA molecular as information medium.

Clelland [6] demonstrates an approach to send secret message by encoding the message as DNA strands among steganographic technique. In order to make the DNA microdots technique much securer and less predictable, Hamdy [18] proposes DNA-Genetic Encryption Technique (D-GET). This technique can transform the text of DNA sequence into an image and confuse the secret message with the text or image. In [113], the author presents a new encryption and decryption technique that using the One Time Pad (OTP) technique. This encryption and decryption technique can secure the data as DNA sequences and DNA structure.

The technique of DNA-Genetic encryption can transform the texts, videos and images into double stranded polymers with four different nucleotides: adenine (A), cytosine (C), guanine (G) and thymine (T) for hiding messages. Yunpeng Z et al. [24], propose a new index-based symmetric DNA encryption algorithm to prevent plaintext-oriented attack. This algorithm encrypts the DNA-sequence-based plaintext through a chaos key generator based on the Logistic Mapping. M. I. Khalil [12] evaluates two different encryption/decryption algorithms between RSA and a new suggested algorithm based on symmetric cryptography concept of the real-time audio signal. In [17], a novel and practicable method of DNA encryption is proposed to be used for hiding messages. This paper's work focuses on signing the data with a signature using DNA coding for limited bandwidth systems or low computation systems. The security of multimedia data attracts more attention due to the widespread transmission over various communication networks. R. Guesmi et al. [9], propose a novel image encryption algorithm to resist against the statistical and exhaustive attacks. This novel image encryption algorithm strengthens the cryptosystem based on a hybrid model of deoxyribonucleic acid (DNA) to compare with a secure hash algorithm SHA-2 and the Lorenz system. In addition, A. K. Verma et al. [21], design an application of DNA cryptography in Ad hoc Networks. The DNA encryption has been gradually applied to network security.

3. DNA Cryptosystems with Port Hopping

With the continuous extension of network applications, attacks to networks are increasing as well. In computer security, a covert channel of communication is hidden messages in secure access network. Therefore, the legitimate data cannot be detected by the attackers since the message is transferred to the access host. However, the opening and sharing of the Internet makes the information security more complicated than other system security. Under synchronous communication, the client sends a request for a service to the host server and waits for the response through an open port. Once the communication link is established, the open port is particularly weak for message transfer in network applications. The host will expose to DoS-style attacks. On the other hand, a lot of information is transferred and shared within the scope of the world through Networks, and then this characteristic of opening network make intrusion possible. Securing the communication channel involves ensuring that messages are encrypted and that they are not modified in transition. DNA strands, a technique of information hiding by encryption, can be used for steganography to provide rapid encryption and decryption of communication network. Figure 2 shows the scenario of DNA encoding.

Due to the presence of eavesdropping, in the classical communication, it is impossible to establish an unconditional security key. Attackers have the ability to eavesdrop the messages exchanged between the client and server. Firstly, the attackers perform a port scan on the network. Then, they can identify the open ports of the server and launch attacks to those open port servers. Finally, they perform the eavesdropping attacks. In the proposed scheme, we append the DNA microdots the random port hopping for hiding secret messages in the communication channel. This new scheme utilizes three concepts:

random port hopping (RPH), steganography, and mutual authentication. Therefore, it is referred to as the hybrid random port hopping technique. Consider a simple port hooping model as follows: sender A sends packets to receiver B through a random port ration channel with port number changed every time unit Δ. There are four credible IP addresses labeled by $IP = \{IP_1, IP_2, IP_3, \cdots, IP_n\}$ in receiver B standing for the synthetic nucleotide sequence between paired bases adenine (A), thymine (T), guanine (G) and cytosine (C). During this time, the messages sent by sender A will be converted into a sequence of letters consisting of A-P that can easily transform the letters into a long-term storage of DNA nucleotide. The DNA encoding message will be received by the receiver B through the four authorized access IP addresses. In Figure 3, we can see the communication mechanism of how receiver B receives packets sent by sender A with DNA cryptosystems.

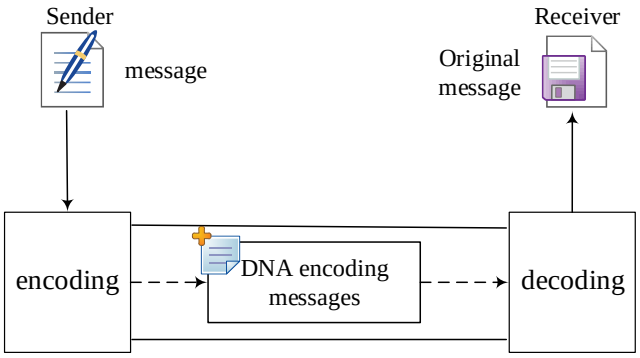

Figure 2. The scenario of DNA encoding

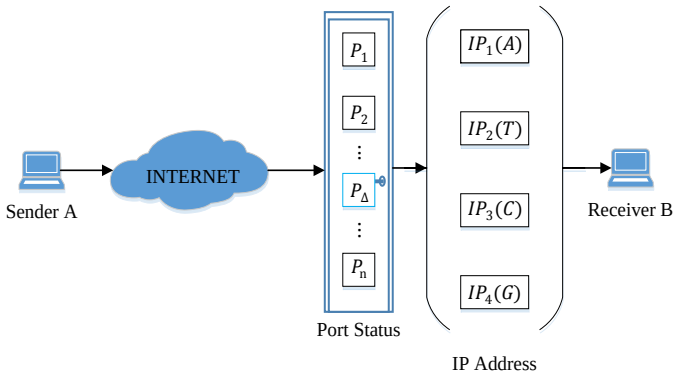

Figure 3. The communication model of port hopping based on DNA cryptosystems

3.1. DNA encoding scheme

The DNA microdot is a means of concealing messages in the Double-strand to transmit secret information. A DNA-encoded message can be expressed as a binary sequence where everything can be encoded by two states of 0 and 1. So we use a simple substitution cipher to encode characters in two nucleotide base pairs. The easiest way to encode is to represent these four units as four binary figures: A (00); T (01); C (10); G (11). According to this primer encode, there are sixteen kinds of encoding rules as listed in Table 1.

Table 1. DNA encoding rule

-	A (00)	T (01)	C (10)	G (11)
A (00)	AA (0000)	TA (0100)	CA (1000)	GA (1100)
T (01)	AT (0001)	TT (0101)	CT (1001)	GT (1101)
C (10)	AC (0010)	TC (0110)	CC (1010)	GC (1110)
G (11)	AG (0011)	TG (0111)	CG (1011)	GG (1111)

However, the traditional DNA cryptosystem through four binaries figures that implements the data encoding will expand the space capacity of the encrypted messages rapidly. The process of sending the encoded message by a sequence of IP addresses is inadequate. Because, in our scheme, the DNA encryption strands act as a substitute for the sequence of IP addresses. For this purpose, we designed a new DNA encoding rule based on the aforementioned rule to reflect the biological characteristics and pairing principles of the four nucleotides are shown in Table 2.

Table 2. New DNA encoding rule

-	A (IP1)	T (IP2)	C (IP3)	G (IP4)
A (IP1)	AA (A)	TA (E)	CA (I)	GA (M)
T (IP2)	AT (B)	TT (F)	CT (J)	GT (N)
C (IP3)	AC (C)	TC (G)	CC (K)	GC (O)
G (IP4)	AG (D)	TG (H)	CG (L)	GG (P)

The uppercase letters sequence from A to P is used for to achieve a big compression ratio. There will be a minimum number IP address to transmit messages by the new DNA encoding rule. The encryption algorithm based on new DNA encoding rule is defined as:

$$M = \{m_1, m_2, m_3, \cdots, m_n\} \tag{1}$$

$$P = \{p_1, p_2, p_3, \cdots, p_n\} \tag{2}$$

$$Key_i = P_i \quad MOD \quad 255, 1 \le i \le n \tag{3}$$

$$E(Key, M) = \{e_1, e_2, e_3, \cdots, e_n\} \tag{4}$$

The sequence of message packets is expressed as M and the set of P represent the sequence of random port number with different timestamps. In equation (3) and (4), the encrypted letter sequence is output which must match the service port.

3.2. Message Encoding and Retrieval

In this method we implement the data encoding and decoding methods of nucleotides by integrating the transformation algorithm with statistical compression schemes. In order to make efficiently express plaintext as DNA sequence, the encryption method presented in this paper requires encryption the plaintext triple.

a) Translate the plaintext as ASCII code. In our scheme, the plaintext will be encoded as ASCII characters, so it can be simplified the process of DNA encryption with 8-bit binary numbers. For example, the plaintext 'A' will be expressed as $[A]_{10}$ = 65 based on ASCII code, and then it could be expressed as $[A]_2$ = 01000001.

b) Encoding and translating the ASCII code as uppercase letters between A and P. Prior to encoding the plaintext into DNA sequence, we introduce an encryption algorithm to conduct XOR with a key. In this encryption, the key is generated by the random port number to produce chaotic pseudo-random number. In other words, the plaintext will be encrypted as different uppercase letters in different port numbers.

c) Encrypting the uppercase letters as DNA sequence. Unlike the traditional DNA encryption, we introduce a new DNA encoding rule, which is a more optimal encoding algorithm to compress the uppercase letters on DNA sequence. The new DNA encoding is beneficial to compress the DNA encoding sequence.

To sum up, we convert the ASCII code, which corresponds to the valid plaintext character, into 8-bit binary code and the random key to be used for the algorithm is generated by the pseudo-random port number. The port number used for communications is changed in every time unit such like parties are hopping. The dynamic mutation based on key identity is referred to as port hopping, and mutation based on service identity is also referred to as port hopping. The mutation of port number based on the time changed with millisecond. Let t_i represents the current timestamp of the server host, and then the port number for the service identity will be expressed as P_i, $1 \le i \le n$.

The purpose of using this encoding technique is the pretreatment of the encrypted plaintext. Through the encoding process presented above, the plaintext will be expressed as the DNA sequence in the form of the nucleotide. The schematic block diagram is shown in Figure 4. Based on Figure 4, proprietary cryptographic algorithms can be described as follows:

- Step 1: Input the message $M = \{m_1, m_2, m_3, \cdots, m_n\}$ to be sent by sender, and then convert M into an 8-bit extended ASCII code M_{bin}.
- Step 2: Use the 8-bit pseudo-random number which is produced by the pseudo-random port number to conduct XOR with $m_{bin_i} \in M_{bin} = \{m_{bin_1}, m_{bin_2}, m_{bin_3}, \cdots, m_{bin_n}\}, 1 \le i \le n$. Obtain the binary sequence M'_{bin}.
- Step 3: Take the 8-bit number $m'_{bin} = \{m'_{bin_1}, m'_{bin_2}, m'_{bin_3}, \cdots, m'_{bin_n}\}$ $1 \le i \le n$ to conduct XOR with 0xF0 and shifts every 8-bit number in the binary sequence M'_{bin} to the right four bit. Obtain the pair sequence M_{xor} and M_{shr}.
- Step 4: Make an addition in $m_{xor} \in M_{xor} = \{m_{xor_1}, m_{xor_2}, m_{xor_3}, \cdots, m_{xor_n}\}$, $1 \le i \le n$ and $m_{shr} \in M_{shr} = \{m_{shr_1}, m_{shr_2}, m_{shr_3}, \cdots, m_{shr_n}\}$, $1 \le i \le n$ with 0x41.

- Step 5: Formalize two binary sequences.
- Step 6: Transfer these binary sequences into a DNA base sequence by new DNA encoding rule.

Algorithm 1: DNA Encoding Algorithm	
Input: the sending message, the random port number	
Output: the DNA encoding sequence	
1:	Get input message *M* and random port number *P*
2:	Initialize *key* = *P* MOD (255), j=0
3:	**For** *i* = 1, 2, 3, …, n
4:	Compute $m'_{bin_i} = f(m_i, XOR, key)$
5:	Compute $m_{xor_i} = f(m'_{bin_i}, XOR, 0xF0)$
6:	Compute $m_{shr_i} = f(m'_{bin_i}, SHR, 4)$
7:	Compute $E_{(j,j+1)} = f((m_{xor_i}, m_{shr_i}), +, 0x41)$
8:	j=j+2
9:	**End for**
10:	Formalize the encoding sequence *E*
11:	Return the DNA encoding sequence *E*

The process of decryption is an inverse process of encryption. Receivers obtain secret keys from the pseudo-random port number, and then decrypt the encryption sequence of DNA microdot according to the contrary operation of above algorithms. The decryption process is given as follows in detail:

- Step 1: Get the DNA base sequence $E = \{e_1, e_2, e_3, \cdots, e_n\}$.
- Step 2: Formalize the DNA base sequence into two binary sequences E_{bin} and E'_{bin}.
- Step 3: Make a subtraction in E_{bin} and E'_{bin} with 0x41. Obtain the result of the logical operation as E_{sub} and E'_{sub}.
- Step 4: Shifts the 8-bit number $e'_{sub_i} \in E'_{sub} = \{e'_{sub_1}, e'_{sub_2}, e'_{sub_3}, \cdots, e'_{sub_n}\}\ 1 \le i \le n$ to the left four bit and then performs arithmetic addition with $e_{sub_i} \in E_{sub} = \{e_{sub_1}, e_{sub_2}, e_{sub_3}, \cdots, e_{sub_n}\}\ 1 \le i \le n$ and get E_{opt}.
- Step 5: Take $e_{opt_i} \in E_{opt} = \{e_{opt_1}, e_{opt_2}, e_{opt_3}, \cdots, e_{opt_n}\}\ 1 \le i \le n$ to conduct XOR with the 8-bit pseudo-random number which is produced by the pseudo-random port number.
- Step 6: Convert the binary sequence into letter sequence which is the original plaintext.

Algorithm: DNA Decoding Algorithm	
Input: the DNA encoding sequence, the random port number	
Output: the original messages	
1 :	Get input DNA encoding sequence *E* and random port number *P*
2 :	Initialize *key* = *P* MOD (255), j=0, Formalize *E* into E_{bin} and E'_{bin}.
3 :	**For** *i* = 1, 2, 3, …, n
4 :	Compute $e_{sub_i} e'_{sub_i} = f((e_{bin_i}, e'_{bin_i}), -, 0x41)$
5 :	Compute $e_{shl_i} = f(e'_{sub_i}, SHL, 4)$
6 :	Compute $e_{opt_i} = f(e_{shl_i}, +, e_{sub_i})$
7 :	Compute $m_{bin_i} = f(e_{opt_i}, XOR, key)$
8 :	**End for**
9 :	Formalize the encoding sequence E_{opt} into M_{bin}
10 :	Return the original message *M*

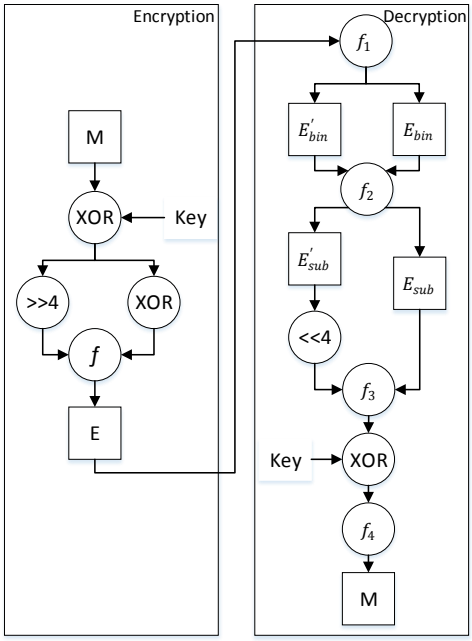

Figure 4. Flowchart of the encryption and decryption algorithm

The system consists of: an encrypted dataset, a key generated by the pseudo-random port number and a new DNA encoding rule to be described in Section 3.1. To describe the process clearly, Figure 5 demonstrates a simple procedure of character conversion by preparing the message.

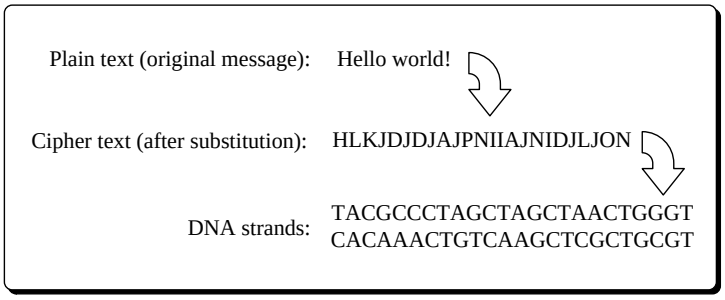

Figure 5. The procedure of character conversion

3.3. Data Transmission

In the DNA encryption module described in Section 3.1 and Section 3.2, the receivers received the concealed message need the data hidden transmission with the random port hopping scheme. The hidden transmission communication module will be illustrated in this section.

RPH is the main component, performs port hopping for senders, can randomly generate a port number by various functions. Firstly, it generates an immediate number based on the timestamp generation rule of the receiver and sender. Secondly, the pseudo-random port number will be selected by the current generation number. Then, the receiver and sender perform a network communication to transfer the plaintexts. The architecture of random port hopping is not a part of our mainline business logic, but is the dependency of the model on a covert communication scheme.

Our focus of implementation is on conveying the DNA microdots through four IP addresses. The DNA nucleotide will be converted into IP addresses and received by the receiver. By using agile destination-address based authentication, the receiver gains efficiency to regenerate DNA nucleotides. Suppose that the encrypted DNA strand is AC and the convert IP address is chosen for authentication. Figure 6 illustrates the data transfer process by port hopping between sender and receiver.

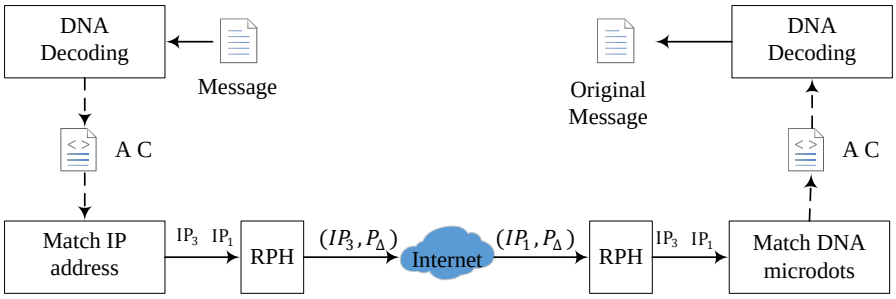

Figure 6. Data transfer process by port hopping

4. Performance Evaluation

The DNA nucleotide is a good medium for data hiding because of its great length and high randomness. Therefore, we introduce the DNA microdots into a port hopping scheme for defend against eavesdropping attacks. This technique has been implemented by Python on Ubuntu16.04 LTS GNU/Linux operating system. Also, a number of standard tools will be used to perform local LAN traffic monitoring, port monitoring and statistics, such as:

- Wireshark for local LAN traffic monitoring.
- Namp for port scanning.
- Tcpdump for statistics.

We assess the practicality of our approach through two experiments. In the first one, we set up a sniffer to collect the accessed sequences from the sender, and then compare the differences between these 3 projects: transmitted in plaintext, transmitted in DNA encryption and transmitted in our scheme. The comparison included how messages were transmitted from the sender to the receiver. The software of Wireshark has been used to implement these tests. This test only need to capture packets and measure the performance, thus the NAT is not set up on each project. Table 3 shows the parameters that were used in this project.

We assess the practicality of our approach through two experiments. In the first one, we set up a sniffer to collect the accessed sequences from the sender, and then compare the differences between these 3 projects: transmitted in plaintext, transmitted in DNA encryption and transmitted in our scheme. The comparison included how messages were transmitted from the sender to the receiver. The software of Wireshark has been used to implement these tests. This test only needs to capture packets and measure the performance, thus the NAT is not set up on each project. Table 3 shows the parameters that were used in this project.

Table 3. Parameter for testing

Parameter	Sender	Receiver
Operation System	Ubuntu *16.04 LTS*	Ubuntu *16.04 LTS*
Testing tools	NAMP *v7.12*	Wireshark *v2.2.1*, Tcpdump *v4.8.1*
Programming Language	Python	Python
IP Address	192.168.222.1	192.168.222.36 192.168.222.136 192.168.222.156 192.168.222.232

4.1. Security Verification

We develop simple analytical models to evaluate the security verification of our scheme in the presence of eavesdropping attacks. To demonstrate the effectiveness of our covert communication scheme, we introduce a mechanism of network communication between the sender and the receiver. For example, the sender intends to tell the receiver he will arrive in Beijing tomorrow in secret. To imitate an attacker's behavior, we consider that the attacker does not know any of the covert communication scheme, and blindly sniffers the packets in the network. In order to evaluate the security of our covert communication scheme, we choose " I will arrive in Beijing tomorrow" as the message sent to the receiver's computer. The messages sent to the receiver's computer include plaintext, the traditional DNA encrypted message and the messages of our covert communication scheme. We capture the network packets and filter out the unrelated connections through Wireshark, and then get the list of network packets.

As shown in Table 4, we can find the information that the length of some network packets is zero, and the destination IP addresses are different. Meanwhile, the destination IP address of 192.168.222.136 has two different network packets, and the length of packets is greater than zero. Through the analysis, the length of DNA encrypted messages come to 136 with four times the length of the plaintext. No doubt, the length of network packets, generates by our covert communication scheme, is null. The receiver now receives the packet carrying the encrypted payload, extracts and decrypts it using the DNA encoding rule. Then the receiver can get the same plaintext through the above ways.

Considering that the sender sends “I will arrive in Beijing tomorrow” without any link encrypting or point-to-point encrypting to the receiver, the attackers will capture the packets as shown in Figure 7. In Figure 7, we can see the plaintext in the capture packets compared with that in Figure 8. Hence, it was vulnerable to eavesdropping attacks. As shown in Figure 8, it is difficult for the attackers to obtain the plaintext immediately without any information about encryption or decryption of messages sent by the sender. However, sending an encrypted message from the sender to the server is useless for professional hackers, who grasp the existing encryption algorithms like the palm of their hands. The experimental results present above indicate that using encrypted message would be secure in network communication, but not always efficient in an open network environment. In Figure 9, we cannot find any related information of transferred messages in the received packets. On the other hand, it seems that the sender interconnects with many receivers, so that the real receiver is hidden. The attack cost will increase, because some assailants would untowardly find out the rule of network communication to mount malicious attacks.

Table 4. The capture and filtrate of the network packets

Source	Destination	Info
192.168.222.1	192.168.222.36	53512→8528 Len=0
192.168.222.1	192.168.222.36	53512→8528 Len=0
192.168.222.1	192.168.222.36	53512→8528 Len=0
192.168.222.1	192.168.222.156	53512→38651 Len=0
192.168.222.1	192.168.222.232	53512→1902 Len=0
192.168.222.1	192.168.222.136	53512→38651 Len=0
192.168.222.1	192.168.222.156	53512→38651 Len=0
192.168.222.1	192.168.222.136	53512→38651 Len=0
192.168.222.1	192.168.222.36	53512→8528 Len=0
192.168.222.1	192.168.222.156	53512→38651 Len=0

```
00 0c 29 80 75 c3 00 50  56 c0 00 08 08 00 45 00   ..).u..P V.....E.
00 3e 7d bf 00 00 80 11  7f 14 c0 a8 de 01 c0 a8   .>}..... ........
de 88 d1 08 96 fb 00 2a  1a 7d 49 20 77 69 6c 6c   .......* .}I will
20 61 72 72 69 76 65 20  69 6e 20 42 65 69 6a 69    arrive  in Beiji
6e 67 20 74 6f 6d 6f 72  72 6f 77 2e               ng tomor row.
```

Figure 7. The capture packets of plaintext of the message

```
00 0c 29 80 75 c3 00 50  56 c0 00 08 08 00 45 00   ..).u..P V.....E.
00 a4 7d b9 00 00 80 11  7e b4 c0 a8 de 01 c0 a8   ..}..... ~.......
de 88 d1 08 96 fb 00 90  cf c1 54 43 43 47 47 47   ........ ..TCCGGG
47 54 43 41 43 41 54 43  43 54 41 47 43 54 41 47   GTCACATC CTAGCTAG
43 54 47 47 47 54 47 43  43 54 47 54 43 41 47 54   CTGGGTGC CTGTCAGT
43 41 54 43 43 54 43 54  43 41 43 43 43 54 47 47   CATCCTCT CACCCTGG
47 54 54 43 43 54 41 54  43 54 47 47 47 54 47 54   GTTCCTAT CTGGGTGT
43 47 43 43 43 54 54 43  43 54 54 54 43 54 54 43   CGCCCTTC CTTTCTTC
43 54 41 54 43 54 43 41  43 54 47 47 47 54 43 47   CTATCTCA CTGGGTCG
43 41 41 41 43 54 41 43  43 54 41 41 43 54 47 54   CAAACTAC CTAACTGT
43 41 47 54 43 41 41 41  43 54 43 41 43 41 41 54   CAGTCAAA CTCACAAT
47 54                                              GT
```

Figure 8. The capture packets of DNA encrypted messages

```
00 0c 29 80 75 c3 00 50  56 c0 00 08 08 00 45 00   ..).u..P V.....E.
00 1c 7d ba 00 00 80 11  7e db c0 a8 de 01 c0 a8   ..}..... ~.......
de e8 d1 08 07 6e 00 08  e9 2b 00 00 00 00 00 00   .....n.. .+......
00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

Figure 9. The capture packets of our covert communication scheme

4.2. Performance Testing

We measure the following tests on our theoretical work to validate its effectiveness and feasibility. We assumed that the test data would start with 2^8, 2^9, 2^{10}, 2^{11} and 2^{12} of DNA nucleotides. The primary goal of our evaluation is to show that our convert communication scheme achieves a high message delivery ration and good latency. To demonstrate this, we have implemented and evaluated the local LAN traffic using Wireshark and the traffic graphing shown as Figure 10 where the message length sends to the receiver varies from 256 bases to 4096 bases.

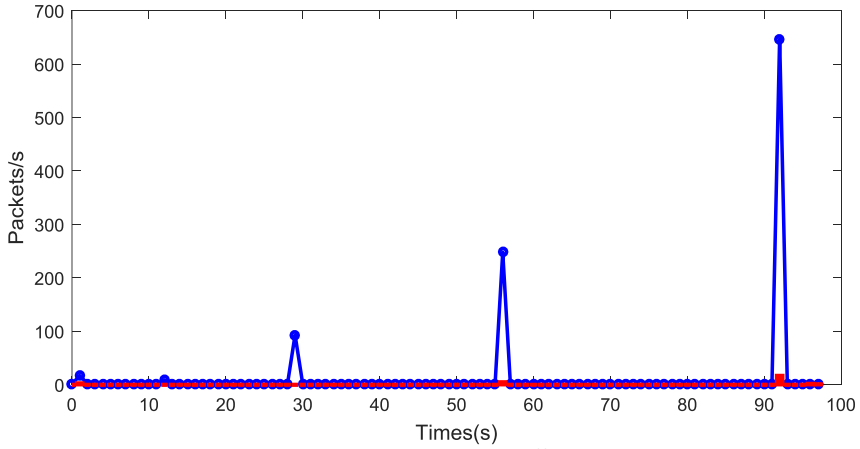

Figure 10. Local LAN traffic

We define the successful rate of communication μ by the probability that the packets sent by the sender can arrive at the receiver securely per unit time. Set n and m as the number of DNA nucleotides sent by sender and the number of DNA nucleotides received by receiver per unit time. In our scheme, four DNA nucleotides replace four static IP addresses in receivers, so that the number of access IP addresses in receivers equals the number of DNA nucleotides. Then, we have the access rate $\mu = n/m$. In the case where both sender and receiver use the i-th port number, the loss rate is given by $\mu' = 1 - n/m$.

As we can see in Figure 10, the red bar under the peak value presents the number of error accesses IP. We analyze the number of the error access IP to add up the DNA nucleotides in terms of the order of occurrence through Tcpdump. According to the five dataset statistics, the resulting dataset is listed in Table 5. As shown in Figure 11, what intrigued us about this chart was the ratio of the unreachable of authentication IP address access in receiver.

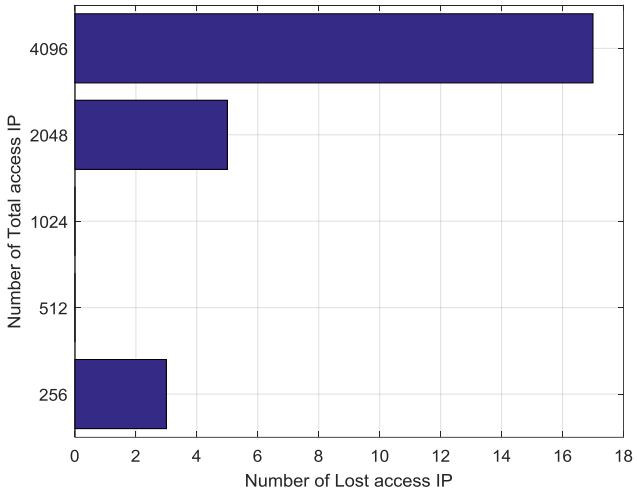

Figure 11. The unreachable of authentication IP address access in receiver

From Figure 11, it appears that greatly access losses with the minimum number of access IP. Based on the statistics analysis, the research shows that the access IP lost in the gap of port hopping. The matter was solved by introducing a FIFO-ordered rate-limited communication channel with port hopping. The experiment results demonstrated the effectiveness of the port hopping scheme based on DNA microdots to mitigate the effect of DoS/DDoS flooding attack and resist the

eavesdropping attacks. We use standard cryptographic functions with a sufficient amount of key material and change random keys with the random port number every hop timestamp. It can be reducing the complexity of malicious packet detection and filtering and deceive those attackers who monitor the network and capture the TCP packets. However, the DNA encoding scheme will be multiplying the length of the messages received by Receiver that is a challenge for dropping packets over network.

Table 5. The dataset of unreachable IP address

Number of all DNA nucleotides	Number of lost DNA nucleotides	The loss rate
256	3	1.18%
512	0	0
1024	0	0
2048	5	0.24%
4096	17	0.42%

5. Conclusion

In this paper, we presented a new scheme for applying the DNA microdot to the random port hopping to provide the security of the communication system. We introduced the integration of DNA nucleotide and IP address authentication. This technology makes it difficult for the communication situation to conduct an analysis for the hostile invaders. Through several experiments, we proved that this communication model is a dependable and utility solution for counteracting DoS/DDoS and eavesdropping attacks.

In this paper, we present the covert communication based on DNA microdots for port hopping that a meaningful exploration and research have made great development and innovation. It will enrich the field of DNA cryptography and covert communication. In the future, we will primary focus on how to encode data for les of very small size and achieve high volume data density by reducing the number of nucleotide. Consequently, the amount of authentication IP address access in the receiver will reach the optimum state and enhance the decoding efficiency of the DNA encoding. We will also consider the image and video received by the receiver in the future work.

Acknowledgements

This research was supported by the Open Project Program of Hebei Key Laboratory of Data Science and Application (No.20170320001).

References

1. L. M. Adleman, "Molecular Computation of Solution to Combinatorial Problems," *Science*, New Series, vol. 266, No. 5187, pp.1021-1024, Nov. 1994
2. G. Badishi, A. Herzberg, and I. Keidar, "Keeping Denial-of-Service Attackers in the Dark," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 3, pp. 191-204, 2007
3. G. Badishi, A. Herzberg, I. Keidar, O. Romanov, and A. Yachin, "Denial of Service? Leave it to Beaver," Working Paper, *TR CCIT*, vol. 595, 2006
4. G. Badishi, I. Keidar, A. Herzberg, O. Romanov and A. Yachin, "Denial of Service Protection with Beaver," *From Security to Dependability Proceedings of Dagstuhl Seminar*, pp.1-6, 2007
5. M. Carvalho and R. Ford, "Moving-Target Defenses for Computer Networks," *IEEE symposium on security and privacy*, vol. 12, no. 2, pp. 73-76, 2014
6. C. T. Clelland, V. Risca, and C. Bancroft, "Hiding Messages in DNA Microdots," *Nature*, vol. 399, pp.533-534, 1999
7. G. Z. Cui, L. M. Qin, Y. F. Wang, and X. C. Zhang, "Information Security Technology Based on DNA Computing," *IEEE International Workshop on Anti-Counterfeiting, Security*, Identification IEEE, pp.288-291, Xiamen, China, 2007
8. Z. Fu, M. Papatriantafilou, and P. Tsigas, "Mitigating Distributed Denial of Service Attacks in Multiparty Applications in the Presence of Clock Drifts," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 3, pp. 401-413, 2008
9. R. Guesmi, M. A. B. Farah, A. Kachouri, and Samet, "A novel Chaos-Based Image Encryption Using DNA Sequence Operation and Secure Hash Algorithm SHA-2," *Nonlinear Dynamics*, vol. 83, no. 3, pp.1123-1136, 2016
10. K. Hari and T. Dohi, "Dependability Modeling and Analysis of Random Port Hopping," *Proceedings of the 9th International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and trusted Computing*, pp.586-593, Fukuoka, Japan, 2012
11. K. Hari and T. Dohi, "Sensitivity Analysis of Random Port Hopping," *Proceedings of the 2nd International Symposium on Multidisciplinary Emerging Networks and Systems (MENS-2010)*, IEEE CS Press, pp.316-321, Xi'an, China, 2010
12. M. I. Khalil, "Real-Time Encryption/Decryption of Audio Signal," *International Journal of Computer Network and Information Security*, vol. 8, no. 2, pp.25-31, 2016
13. D. Kumar and S. Singh, "Secret Data Writing Using DNA Sequences," *In Emerging Trends in Networks and computer*

Communications (ETNCC), IEEE International Conference on, pp.402-405, Udaipur, Rajasthan, India, 2011
14. R. P. Kumar, J. Babu, T. Gunasekhar, and S. B. Bhushan, "Mitigating Application DDoS Attacks using Random Port Hopping Technique," *International Journal of Emerging Research in Management and Technology*, vol. 4, pp.1-4, 2015
15. H. C. J. Lee and V. L. Thing, "Port Hopping for Resilient Networks," *vehicular technology conference*, VTC2004-Fall. 2004 IEEE 60th, vol.5, pp. 3291-3295, 2004
16. Y. B. Luo, B. S. Wang, G. L. Cai, Luo, Yue Bin, B. S. Wang, and G. L. Cai. "Analysis of Port Hopping for Proactive Cyber Defense," *International Journal of Security and Its Applications*, vol. 9, no. 2, pp. 123-134, 2015
17. G. Madhulika, and C. S. Rao, "Generating Digital Signature Using DNA Coding," *In Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA)*, Springer International Publishing, pp. 21-28, Bhubaneswar, India, 2014
18. Mousa and M. Hamdy, "DNA-Genetic Encryption Technique," *International Journal of Computer Network and Information Security*, vol. 8, 2016
19. E. Sitnikova and M. Asgarkhani, "A Strategic Framework for Managing Internet Security," *11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, pp. 947-955, Xiamen, China, Aug 2014
20. L. Y. Shi, C. F. Jia, S. L, and Z. Liu, "Port and Address Hopping for Active Cyber-Defense," *Lecture Notes in Computer Science*, Springer, vol. 4430, pp.295-300, Berlin Heidelberg, 2007
21. A. K. Verma, M. Dave, and R. C. Joshi, "Securing Ad hoc Networks Using DNA Cryptography," *IEEE International Conference on Computers and Devices for Communication (CODEC06)*, pp.781-786, Swissotel Kolkata, Indiak, December 2006
22. X. Wang and Q. Zhang, "DNA Computing-Based Cryptography," *Fourth International Conference on Bio-Inspired Computing*, Beijing, China, 2009
23. J. D. Waston and F. H. C. Crick, "A Structure for Deoxy Ribose Nucleic Acid," *Nature*, vol. 25, pp.737-738, 1953
24. Y. P. Zhang, Z. Yu, W. Zhong, and R. O. Sinnott, "Index-Based Symmetric DNA Encryption Algorithm," *4th International Congress on Image and Signal Processing IEEE*, vol. 5, pp. 2290-2294, Shanghai, China, 2011

Leyi Shi received his PhD degree in computer science and technology from Nankai University, in 2008. He was a visiting scientist in the College of Computing Informatics at University of North Carolina Charlotte in 2011. He is currently a professor at College of Computer and Communication Engineering, China University of Petroleum (East China). His current research interest focuses on the network security, game theory and mobile Internet. He has published more than 60 research papers in several high-level academic journals. He is now a senior member of China Computer Federation, vice chairman of the Qingdao Yocsef Forum of CCF, and vice chairman of Shandong Computer Network Security Committee.

Yuwen Cui is a master student in the College of Computer and Communication Engineering at China University of Petroleum (East China). He received his Bachelor degree in Computer Science and Technology from Lanzhou University of Technology (LUT), Lanzhou, China in 2015. His current research interest focuses on the data security and cyber defense.

Xiaotong Liu is a master student in the College of Computer and Communication Engineering at China University of Petroleum (East China). He received his Bachelor degree in Computer Science and Technology from China University of Petroleum (East China), Qingdao, China in 2015. His current research interest focuses on Deep Learning, Cyber defense, and Web services.

Hui Sun is a master student in the College of Computer and Communication Engineering at China University of Petroleum (East China). He received his Bachelor degree in Computer Science and Technology from Ludong University, Yantai, China in 2015. His current research interest focuses on Cyber defense, and Web services.

Zhiyu Xue is a master student in the College of Computer and Communication Engineering at China University of Petroleum (East China). He received his Bachelor degree in Computer Science and Technology from China University of Petroleum (East China), Qingdao, China in 2015. His current research interest focuses on Cyber defense, and SDN.

Shufen Zhang received the Bachelor degree from Hebei University of Science and Technology in 1995, the Master degree from Yanshan University in 2005. Now she is a professor of the school of sciences, North China University of Science and Technology. Her research interests include Cloud Computing and Big data.