International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Wireless Security Via DNA Inspired Network

Nandini P. Nagtode[1], Monika Rajput[2]

[1]M.E. Istyear (CSE), P. R. Pote COE&M, Amravati, India

[2]Assistant Professor, P. R. Pote COE&M, Amravati, India

Abstract: ***With the growing pace of Internet and network technology day by day, the security threats are also increasing for the users, due to lot of information flow on the network. There are various adversaries who always try to break into the system in order to steal the crucial information or to destroy the integrity of data. So information security becomes necessity for modern computing systems. There are some sectors like government, banks, military who can't afford any leaks to their secret data. From our past to till date the secret writing techniques are used to protect the data from the adversaries and the techniques such as cryptography and stegnography are most common and widel. Universal use of wireless networks and popularity amongst the users to connect to the internet creates incentives for attackers and allows them to stepping-stone attack the wireless connection to steal the legitimate user's data by exploiting the data packets travelling through wireless media and use several malware and sniffing attack techniques. Wireless network resources are more vulnerable to interceptions with intruders taking advantage of connections to acquire access into the access point. In this work we are taking inspiration from DNA bases for encrypting and decrypting the user's data and use DNA algorithm for users to access their own wireless network and prevent intruders accessing to the same wireless access point. This makes the user more reliant on the authentication of their data as it travels through the wireless network. In this research we have to use the bases of DNA nucleotides for a substitution and mutation security protection which is converting the user's details into DNA sequences intended for users accessing list to the wireless network AP and also encrypting and decrypting the dataflow stream such as plain text or pictures using DNA cryptography methods for authentication.DNA is the next generation security mechanism.***

Keyword: DNA,DNA Sequence; Alignment; wireless security; encryption; decryption; XOR; PCR.

1. Introduction

Wireless networks serve as a communication mechanism between devices and can improve efficiency, productivity and cost effective networking. Wireless Local Area Network (WLAN) connects computers to the network using an access point device, which typically has a coverage area of up to 100metre range. Also ad hoc networks such as Bluetooth are designed to connect remote devices such as laptops and mobile phones because of their shifting network topologies, whereas WLAN use a fixed network infrastructure [1]. Organisations and individuals can benefit when wireless communication resources are well protected. The protection of wireless communication however, is a complicated task, which includes taking measures such as management operation and access control. While these measures will not prevent all penetration and unauthorised access, they can reduce many common adverse events and risks associated with them. Universal use of wireless connections and their popularity amongst users is a huge benefit, allowing them to use the same connection for several devices, and therefore accessing to the wireless network when needed. However the wireless network medium is more vulnerable to interceptions with intruders taking advantage of connection to get access into the router. Wireless connection is becoming a prime target of hackers to eavesdropping and attacking the wireless network which disrupt the service of the legitimate users. Wireless network connections need to travel around the venue with robust security mechanism maintaining confidentiality, availability and integrity of the users. The design of encryption algorithms is based on complex problems in order to ensure the security takes effect, the DNA is proposed as a next generation type of security, started by Adleman pioneering of first DNA computing which marked as the new era of DNA and the operations in computing [2]. Now DNA cryptography science has become the forefront field of cryptography of international research, however in international context the design, analysis and application of DNA is still in the exploratory study and the effective application is still very difficult.

2. Related work

In the recent year few works on qualitative and quantitative analysis on DNA based cryptography as well as many new cryptographic techniques are proposed by the researchers. Bibhash Goyet al[3][4][5] proposed a DNA sequencing based encryption and decryption process . Tushar Mandge et al[6] designed a DNA encryption technique based on 4*4 matrix manipulations and using key generation scheme which makes data much secure[7]. Miki Hirabayashi and Akio Nishikawala [8] have proposed theoretical and empirical based analysis on application of DNA cryptography. such conceptual work can be useful in the wireless security.

3. DNA

DNA stands for Deoxyribonucleic acid which store genetic information of the entire living organism ranging from human being to small viruses. It is also called as an information carrier and consists of long polymer of small units called nucleotides. Further nucleotides consist of three components: Nitrogenous base, five Carbon sugar and Phosphate group. Nitrogenous base consists of four bases: Adenine, Thymine, Cytosine and Guanine (A, T, C, G), all the complex information about organism are stored with the combination of these bases. Adenine and Guanine are called purines, whereas Thymine and Cytosine are called pyrimidines. DNA is a double helix structure as shown in the Figure below.

REMOVED (PLAGIARIZED ARTICLE)
Abdulraqeb Alselwi Bin Askwith, Madjid Merabti
School of Computing and Mathematical Sciences
Liverpool John Moores University, Liverpool, UK
A.A.Alselwi@2015.ljmu.ac.uk; M.Merabti@ljmu.ac.uk; R.Y.Askwith@ljmu.ac.uk
The 15th Annual Post Graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting (PGNet2014)

Licensed Under Creative Commons Attribution CC BY

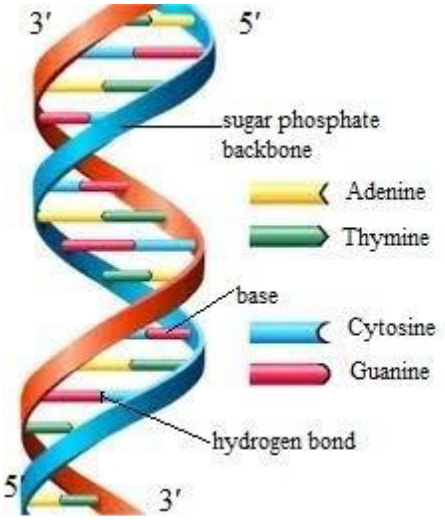

Figure 1: Double helical structure of DNA

DNA double helical structure was discovered by the two Nobel laureate Watson and Crick and therefore it is also called a Watson-Crick complementary structure, where A and T form hydrogen bond with each other, whereas C and G forms bond with one another. In this structure of DNA both the strands are anti parallel to each other, means if one strand starts from 3′ to 5′, then another strand is from 5′ to 3′.

4. Wireless Security Algorithms

The Institute of Electrical and Electronics Engineer (IEEE) created the first mainstream standard for wireless LAN [9]. It started with 802.11 which supported 2Mbps data rate then the later versions created with higher bandwidth support. Eachversion incorporates with the needs of the industry wireless communication.

A. Wired Equivalent Privacy (WEP)

Security protocols also derived from those standards and evolved over a period of time. It started with introduction of Wired Equivalent Privacy (WEP) in 1999 for providing the security compared to the wired networks security. In WEP RC4is used to provide confidentiality and CRC-32 for data integrity and a 24 bit value known as Initialization Vector (IV)used with WEP cryptography to generate a key stream[10].

B. Wi-Fi Protected Access (WPA)

WiFi Protected Access (WPA) was introduced in 2003 to solve the flaws of WEP and it is implemented for 802.11i thus it is intermediate solution. This is intended to address the problems of WEP without requiring new hardware.WPA uses Temporal Key Integrity Protocol (TKIP) for encryption and generates 128 bit for every packet and uses MIC Messages Integrity Code for integrity compared to CRC-32 with WEP, and used WPA-PSK (Pre-Shared Key) for authentication between two parties for initiating the communication. Also WPA-Enterprise for networks and Remote Authentication Dial In User Service (RAUIUS) provide robust security for wireless network.[10]

C. Wi-Fi Protected Access 2 (WPA2)

WPA2 was introduced in 2004 to enhance over WPA.WPA2 authentication and provide stronger encryption PSK and Enterprise similar to WPA, and generate the key by 4 ways handshake for deriving Pair wise Transient Key PTK [10].

5. DNA synopsis

DNA stands for Deoxyribo Nucleic Acid, a genetic material in living organisms. The information in DNA is stored as codeof four chemical substances namely; Adenine A, Cytosine C, Guanine G and Thymine T. The order and sequences of these bases is to provide information about devices formed with alphabetical appearance. This provides capacity and potential for many mathematical and statistical solutions dealing with data and provides naming, addressing, and other functionality. The computational capabilities of DNA has been found by Adlemanin [11]The computation carried out using DNA sequence is called DNA Computing. Diverse problems with significant storage capacity have been solved using parallelism method has combined tradition cryptography with DNA sequence to introduce hybrid security[10]Information encryption using DNA sequences can be used on the ever demanding information encryption on communication methods especially wireless communication which is in need of robust data encryption scheme to challenge ever growing of attacks on the data traffic as the problem is that intruders, keep sniffing on network traffic hence DNA encryption providing a data protection when passed by intruders. Every activity which translates the phase and converts the main command of the sequence into nucleotides sequence, using the sequence alignment useful for detecting any intrusion attacks or sniffing accessed into wireless network through measuring the threshold value of the exact DNA sequences nature which constructed to process the fixed nucleotides sequences to combine the nucleotides for the encrypted parameters security values. [12]

6. Proposed Algorithm

The proposed framework for secure communication over wireless connection is to create an isolated user DNA sequences for accessing keys designed for each user which accessing to their own wireless network Access Point AP. Thus the DNA nucleotides is the proposed algorithm for this process, so each user will have their own DNA sequence which is converted from the user data provided to be complex and to get a complex DNA bases sequence which then is storedat both connectors the portable device of the user and the wireless router device for comparison authentication security, if the DNA sequences at the portable device and the wireless router are matched then access granted otherwise mismatched then deny access to the wireless network. The proposed work consists of the following components:

A. Database

User information is stored in a database created within the system which includes static details such as first name, last name, email address, user name, and password and dynamic details such as CPU speed, number of browsed web pages

REMOVED (PLAGIARIZED ARTICLE)
Abdulraqeb Alselwi, Bob Askwith, Madid Merabti
School of Computing and Mathematical Sciences
Liverpool John Moores University, UK
A.AAlselwi@2013.ljmu.ac.uk, R.J.Askwith@ljmu.ac.uk, M.Merabti@ljmu.ac.uk
The 15th Annual Post Graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting (PGNet2014)

Licensed Under Creative Commons Attribution CC BY

and mouse travel distance which are optional to put the DNA sequences are more complexity and attackers can't break it or guess your common details. Thus the static and the dynamic are flexible for expanding the columns when needed by the programmers to increase the security complexity and make it harder to attack. The additional information is important for case of the common known details of the same users whom use the same wireless network or even external users such as attackers or intruders to secure his/her connection and encrypt the two ways communication therefore increasing probability of unauthorised access to wireless network. Details will be compared to the existing records within the database to compare the degree of the DNA sequence with the observed sequence in the wireless router for a decision whether to grant access or block. To make the encryption more robust we are adding extra encryption by adding DNA strands from its octet to the encryption process.

B. DNA Conversion Algorithm Code

First of all the database should be created for recording user profile and the columns of the database have to be multiple forgetting a sequence for each record in order to align these sequences and place it as the key match for the security match,below is the example of selecting one column of the databasewhich is first name field as shown below and we need toconnect the database for data entity query.

```
// connect to Database information
ResultSet rs1 = conn.SQLSelect("select FName from
PROFILE ");
while (rs1.next()) {
s1 = rs1.getString("FName");
for (int i = 0; i < s1.length(); i++) {
```

After connecting the database then each entity so at each field is converted to ASCII code as shown below.

```
// conversion code to ASCII
char c = s1.charAt(i);
a = (int) c;
```

Now after converting the data entity to ASCII code, all the ASCII codes will be converted to DNA sequences from the ASCII code we will get the binary codes, and these binary codes will be converted to the binary of DNA sequences as A=00, T=01, C=10 and G=11 as demonstrated below:

```
// Conversion to DNA sequence
for (int q = 0; q <= bin.length() - 1; q++) {
d1 = mat[q];
d2 = mat[q + 1];
q = q + 1;
if (d1 == 0 && d2 == 0) {
A = "A";
f = f + A;
jTextArea1.append(A);
} else if (d1 == 0 && d2 == 1) {
B = "T";
f = f + B;
jTextArea1.append(B);
} else if (d1 == 1 && d2 == 0) {
C = "C";
f = f + C;
jTextArea1.append(C);
} else if (d1 == 1 && d2 == 1) {
D = "G";
f = f + D;
jTextArea1.append(D);
```

According to our coding for converting to DNA sequences we can change the bases nucleotides for each binaryto make it hard to guess by intruders for example A=00 wecan code it to AAA=00 for triple nucleotides

```
if (d1 == 0 && d2 == 0) { A = "AAA"; f = f + A;
// or AGAT=00 for quadruple nucleotides.
if (d1 == 0 && d2 == 0) { A = "AGAT"; f = f + A;
```

C. DNA parameter sequences

$xi=xj$

$x$is the DNA nucleotides and i, j are the length of the sequence. And x is the vital comparison between the two devices, which the x sequence in the user device should match the x sequence at the wireless router and the comparison will be compared to score the degree of each sequence to match or mismatch as shown below:

$\sigma(xi,xj)$

$xi=xj$->*match that legitimate user*

$xi\neq xj$->*mismatch intruder*

$\sigma(xi,xj)$	score
$xi=xj$	1
$Xi\neq xj$	0

The binary of 0 and 1s are the function for on and off if the $xi=xj$ then the sequences are matched and its 1 means as on that grant a connection if the $xi\neq xj$ score 0 which means as off and deny connection which is intruder.

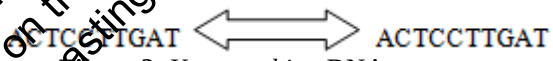

Figure 2: Key matching DNA sequences

For a successful establishment of the wireless connection between the user device and a wireless AP, user sends the request to AP for the authentication, and then AP sends user a challenge. User reply back the encrypted sequence key using primer key *kx*to AP, now access point decrypt the key *kx* sequence key *xi* for matching it with the wireless AP sequence*xj* and if matching gets success then connection is established else connection dropped.

D. Secure DNA Public Channel

The vast parallelism and extra ordinary information density inherent in DNA are explored for cryptography purpose such as encryption, authentication and signature. The DNA keys weuse here is Polymerase Chain Reaction (PCR) for using twoprimer pairs the keys are *Kx*and *Ky*, the keys should be knownto secure the public channel. We use XOR to secure thechannel of normalized binaries by gaining high compression factor and plaintext bytes are bit-wise XORed with the outputbytes to produce ciphertext. The used keys for security channel are the XOR forcompression factor as the XOR operation with sufficiently longkeys sequences between two parties such as a wireless routerand a user device exchanging messages over the wireless channel not the internet, exchanging messages using XOR asthe two parties use long sequences with enough entropy wouldprotect the messages against third parties, and PCR

REMOVED (PLAGIARIZED ARTICLE)
Abdulraqeb Alselwi, Bob Askwith, Madjid Merabti
School of Computing and Mathematical Sciences
Liverpool John Moores University, Liverpool, UK
A.A.Alselwi@2013.ljmu.ac.uk, R.J.Askwith@ljmu.ac.uk, M.Merabti@ljmu.ac.uk
The 15th Annual Post Graduate Symposium on the Convergence of Telecommunications;
Networking and Broadcasting (PGNet2014)

Licensed Under Creative Commons Attribution CC BY

which usesthe two prime keys for complexity break in to connection keys.The *kxi*and *kxj*are the DNA sequences keys for the user andwireless device. The key security will have the same sequencesat the user device is *xi* and the wireless device is *xj*, while *ky*keyis for the data flow encryption

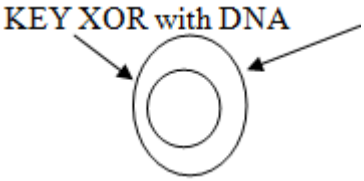

Figure 3: Secure channel with PCR Keys and XOR.

XOR will use the *k* to be performed and XORed combining the correct key as the key is given by user which is his profilestored to convert it into DNA sequence, the key which is usedwill be private key which will be generated to DNA bases andpassed to the router through the secured channel to compare it with the other similar private key which is stored at the wireless router as observed sequence. In case the DNA layer can be broken then another two layers is represented one for the messages in DNA encryption, and decryption in DNA bases as it is difficult to break which is the interior channel security encryption. Thus key *ky*is PCR key which is the external for the message key by combining the key with the DNA encryption, to secure the message which is encrypted into DNA substitution and mutation using one the DNA encryption and decryption method for a doubling security to the user data flow which pass through the public channel and if the intruder hacks our code then we can change the DNA pattern in the DNA code for leads to secure the public channel and using our two PCR keys will be more difficult to break.

7. Future Scope

We demonstrate the user profile sequences in the database, the methods of extracting the user records to convert them to nucleotides bases that will be the keys for matching the sequences, at the portable device and same sequence put it for network observation in the wireless router which is the second key inherited from the user sequence and store it in the wireless device for detection and matching process, the matching sequences are effect between two parties using the parameters techniques of the wireless communication to generate the user signature sequence such as a threshold value of the encoded DNA sequence in the network connection to a corresponding XOR with DNA Keys ACTCCTTGAT ,DNA nucleotides sequences. Then the keys have to compare the signature corresponding sequence with the wireless observed sequence for find similarity degree value aimed at match or mismatch sequences. Then the threshold value of the nucleotides sequences will decide whether this user is a legitimate user or an intruder, as we know the intruder has no sequences for matching then the value degree of sequences is zero or the sequences do not match the observed ones in the system which means it is an intruder and raises negative alarms for blocking the connection. Also the users on the same network can be identified by their unique DNA sequence if they try to break in to the other legitimate user at the same wireless network, the DNA sequence is useful for intrusion detection to detect the breakthrough the alarmed raised of negative access that the sequences mismatched or try to guess the victim user's details.

8. Conclusion

The proposed method of encoding is far better and faster than conventional cryptography like DES and other DNA based encryption algorithms. In this work we have also demonstrated that DNA sequences can be used for encryption and decryption the data pass through the wireless channel which is the vital data for the user, and the DNA is concealed this data with its nucleotides bases using DNA encryption and decryption process by converting the plain text to ASCII and then DNA sequence then to binary digits of the DNA bases and send it to the public channel to the decryption process at the other party. In future work our idea is to evolve the wireless security using DNA security techniques to mitigate the flaws of the current security algorithms, as we didn't reach to the final point of DNA security yet but we at least propose the initial stages of DNA algorithm security for a wireless security access point.

References

[1] T. Karygiannis and O. Les, "Wireless Network Security 802.11,, Bluetooth and Handheld Devices," *Comput.Secur. Inf.Technol. Lab. Natl. Inst. Stand. Technol.*, no. 800-48, p. 119, 2002.
[2] L.M. Adleman, "Molecular computation of solutions to combinatorial problems.," *Science*, vol. 266, no. 5187, pp. 1021–4, Nov. 1994.
[3] Bibhash Roy, Gautam Rakshit, Pratim singha , Atanu Majumder, Debabrata Datta,"An improved Symmentric key cryptography with DNA based strong cipher "ICIecom-2011, feb '24-25 ' pp.1-5
[4] Bibhash Roy et al, "A DNA based Symmentric key Cryptography "-ICSSA-2011, 24-25 JAN'11
[5] Bibhash Roy, Gautam Rakshit, Pratim singha , Atanu Majumder , Debabrata Datta,"An enhanced key Generation scheme based cryptography with DNA Logic"IJCT-2010-11, Volume 1 no. 8,Dec '2011
[6] Tushar Mandge , Vijay chaudhari, "A DNA Encryption Technique Based on Matrix Manipulation and secure key Generation Scheme",ICICES journal 2013.
[7] Nucleotide base pairing of stands , http://dedunn.edblogs.org,2012.
[8] Miki Hirabayashi,AkioNishikawa,"Analysis of a DNA-Based Cryptosystem ", IEEE computer society, 978-0-7695-4514-1/11, 2011.
[9] P. Layer, Telecommunications and information exchange Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specificati. 1997
[10] S. Sukhija and S. Gupta, "Wireless Network Security Protocols A Comparative Study," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 2, no. 1, 2012.
[11] A. Cherian, S. R. Raj, and A. Abraham, "A Survey on different DNA Cryptographic Methods," *Int. J. Sci. Res. (IJSR), India Online ISSN 2319-7064*, vol. 2, no. 4, pp. 167–169, 2013.

REMOVED (PLAGIARIZED ARTICLE)
Abdulraqeb Alsewi, Boo Askwith, Madjid Merabti
School of Computing and Mathematical Sciences
Liverpool John Moores University, Liverpool, UK
A.A.Alsewi@2015.ljmu.ac.uk, M.Merabti@ljmu.ac.uk, R.J.Askwith@ljmu.ac.uk
The 15th Annual Post Graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting (PGNet2014)

Licensed Under Creative Commons Attribution CC BY

[12] C. Kreibich and J. Crowcroft, "Efficient sequence alignment of network traffic," *Proc. 6th ACM SIGCOMM Internet Meas. - IMC '06*, p. 307, 2006.

References

Nandini P. Nagtode received her B.E (IT) from P. R. Patil college of Engg & tech .Affiliated to SGBAU University, Amravati Maharashtra, India in 2013. Currently she is pursuing M.E. in Computer Science and Engineering from P. R. Pote College of Engineering And Technology Amravati, Maharashtra, India.

Monika Rajput completed her M.tech. Currently she is working as assistant professor in P. R. Pote College of Engineering and Technology Amravati, Maharashtra, India.

REMOVED (PLAGIARIZED ARTICLE)
Abdulraqeb Alselwi, Bob Askwith, Madjid Merabti
School of Computing and Mathematical Sciences
Liverpool John Moores University, Liverpool, UK
A.A.Alselwi@2013.ljmu.ac.uk, R.J.Askwith@ljmu.ac.uk, M.Merabti@ljmu.ac.uk
The 15th Annual Post Graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting (PGNet2014)

Licensed Under Creative Commons Attribution CC BY