Journal of Computer Applications and Information Technology
Vol. 1, Issue. 2, June 2025, pp. 25~36

DNA Computing Inspired Network System by using a Wireless Network Security

Mazniha Berahim
Center for Diploma Studies, Universiti Tun Hussein Onn Malaysia, Johor, Malaysia.

Article Info

Article history:

Received Mar 17, 2025
Revised Apr 18, 2025
Accepted May 20, 2025

Keywords:

DNA Sequence Second Alignment
wireless security Fourth
encryption
decryption
XOR
PCR

ABSTRACT

Universal use of wireless networks and popularity among consumers to connect to the web generates incentives for attackers and enables them to stepping-stone attack the wireless link to steal information from legitimate customers by exploiting wireless media information packets and using multiple malware and sniffing attack methods. Wireless network resources are more susceptible to intruders using links to gain access to the access point. We take inspiration from DNA bases in this job to encrypt and decrypt user data and use a DNA algorithm for users to access their wireless network and stop intruders from accessing the same wireless access point. This makes the customer more dependent on their information authentication as they travel through the wireless network. In this study, we need to use DNA nucleotide bases for protection against replacement and mutation, which converts user information into DNA sequences designed for users who access the wireless network AP list and also encrypts and decrypts the information flow stream. Users access wireless list sequences using matching or mismatching sequences for a lawful user that helps identify intruders and make it inflexible to stop information, which is to enhance wireless security and management to mitigate the faults of past safety methods, while the present major problems of the absence of a mathematical understanding of encrypted DNA bases.

Corresponding Author:

Mazniha Berahim,
Center for Diploma Studies,
Universiti Tun Hussein Onn Malaysia, Johor, Malaysia.

1. INTRODUCTION

Wireless networks act as a mechanism of communication between devices and can enhance effectiveness, productivity, and cost-effective networking. Wireless Local Area Network (WLAN) connects pcs to the network using an access point device, typically up to a range of 100 meters. Due to their changing network topologies, ad hoc networks such as Bluetooth are also intended to link remote equipment such as laptops and mobile phones, while WLAN uses a fixed network infrastructure [1]. Organizations and people can benefit from well-protected wireless communication resources. Wireless communication security, however, is a complicated task that involves steps such as leadership, operation, and control of access. Although these measures will not avoid all penetration and unauthorized access, many prevalent adverse events and related hazards can be reduced.

The universal use of wireless links and their popularity among consumers is an enormous advantage, enabling them to use the same link for multiple devices and thus access the wireless network if necessary. The wireless network medium, however, is more vulnerable to interceptions with intruders using the connection to access the router. The wireless connection becomes a prime target for hackers to escape and attack the wireless network that disrupts legitimate users ' service.

Wireless network connections need to travel around the location with a solid safety system that keeps customers confidential, accessible, and integral. There are several protocols and norms for protecting wireless contacts, but intruders always discover fresh instruments and methods for sniffing and accessing

wireless contacts that violate lawful users ' privacy and safety vulnerabilities. While protecting wireless links is an ongoing challenge with the overall use of technology in private, business and technological settings. The worst case of a wireless network assault is full wireless network control by unlawful users. We consider this to explore the faults through present policies and safety techniques and suggest a solid, pro-active technique to obscure user information from unauthorized access and wireless details.

The design of encryption algorithms is based on complicated issues to guarantee that the safety takes impact, the DNA is suggested as a next-generation form of safety, initiated by Adleman pioneering initial DNA calculating, which signaled the beginning of a new age in DNA and computation [2]. Nowadays, the primary area of worldwide study in crypto is the encryption of DNA science, but the design, analysis and application of DNA are still in the exploratory study in the international context and the effective application is still very difficult.

The document's remaining sections are arranged this way: section 2 is associated research; section 3 looks at wireless security algorithms; section 4 highlights issues with present safety algorithms; sections 5 and 6 offer an overview of DNA and its representation; section 7 defines wireless DNA safety encryption and decryption techniques; section 8 is our suggested algorithm; section 9 discusses the novel.

2. RELATED WORK

Adelman first demonstrated in 1994 that a direct Hamiltonian HPP track issue could be encoded in DNA to assess and combinatorial experimental issue using DNA as a computational [2]. In 1995, Lipton expanded the concept of Aledelman to fix the issue of satisfaction [3] using a brute-force search algorithm based on DNA computing algorithms [4]. In 2000, Liu developed a model DNA computing system, called surface-based DNA computing, which solved the problem of satisfaction [3] with DNA cryptography with multiple apps in the field of cryptography [5]. A steganography algorithm to communicate data security using DNA concepts [7] introduces one-time DNA cryptography techniques for testing steganography technologies that enhanced DNA safety.

3. WIRELESS SECURITY ALGORITHMS

The Electrical and Electronics Engineering Institute (IEEE) developed the first wireless LAN mainstream standard [8]. It began with 802.11 supporting the data rate of 2Mbps then the subsequent versions produced with greater support for bandwidth. Each version includes wireless communication with the industry's requirements.

A. Wired Equivalent Privacy (WEP)

Also derived from these norms, security protocols developed over some time. It began in 1999 with the implementation of Wired Equivalent Privacy (WEP) to provide safety compared to the safety of wired networks. In WEP RC4 is used to provide confidentiality and CRC–32 for data integrity and a 24-bit value known as Initialization Vector (IV) used to produce the main flow with WEP cryptography [9].

B. Wi-Fi Protected Access (WPA)

WiFi Protected Access (WPA) was launched in 2003 to fix WEP faults and is applied as an intermediate alternative for 802.11i. This is intended to address WEP problems without requiring new hardware. MIC Messages Integrity Code is used for integrity compared to CRC-32 with WEP, WPA uses Temporal Key Integrity Protocol, the (TKIP) for encryption, and each packet has one hundred eighty bits. WPA-PSK (Pre-Shared Key) is used for authenticating between two parties in order to start a conversation. Additionally, WPA-Enterprise offers strong security for internet connections and remote verification dial-in user service (RADIUS) [9].

C. Wi-Fi Protected Access 2 (WPA2)

In 2004, WPA2 was implemented to improve WPA. WPA2 authentication and provide greater WPA-like PSK and Enterprise encryption and create the Pairwise Transient Key PTK important by 4 ways handshake [9].

4. PROBLEM

The shared key can be readily revealed in WEP cryptography assessment, as well as not providing key management as the same main that has been used for a long time. The WEP key size is 40-bit, which is low, making it vulnerable to brute force attack and in shared key authentication, access within a range of AP

and access to sensitive information can result in man in middle attacks [9].

Alternative to using the more modern Advanced Encryption Standard (AES), WPA uses antiquated RC4 cryptography, which is vulnerable to attacks such as denial-of-service (DoS) attacks and is probably threatened by TKIP's hash function. To generate the password, customer service Set Information (SSID), and By pair Master Key (PMK) provided by the hash technique. Only 1.8n + 14 and n bytes are acquired using the passphrase of safety resistance, so the PMK only passphrase that is vulnerable to dictionary attacks and data breaches must be guessed [9].

WPA2 is susceptible to accessibility issues such as Command instructions like RTS and CTS are vulnerable to DoS assaults as well as leadership due to blocking, water damage, and is not encrypted to document network topology so attackers can evaluate network traffic.

Additionally, since WPA2 shares GTK with all registered users, rogue users can inject fake GTK packets, which then allow authorized users to monitor another authorized users and decrypt their information or install malware to compromise the devices of other users.

5. DNA SYNOPSIS

DNA is living things' biological substance, Deoxyribose Nucleic Acid. Four chemicals—adenine A, cytosine C, guanine G, and thymine T—make up the code that DNA uses to store information. These bases' sequencing and ordering are to supply alphabetical-looking device data. This offers the ability and potential for numerous data-related mathematical and statistical solutions and offers to name, addressing and other features. Adleman discovered the computational capacity of DNA in [10].

The Calculating DNA sequence is known as DNA computation. Using DNA sequences in conjunction with conventional encryption to achieve mixed safety, various issues with important storage capability have been solved using the parallelism method [10].

It is possible to employ genetic code for information encapsulation on the constantly demanding encoding of information on communication techniques, particularly wireless communication, which requires a solid data encryption system to challenge ever-increasing assaults on data traffic as the issue is that intruders continue to sniff on network traffic and therefore DNA encryption provides data protection when passed through intruders.

Any activity that translates the phase and converts the main sequence command into a nucleotide sequence using a sequence alignment that is useful for detecting any intrusion attacks or sniffing accessed into a wireless network by measuring the threshold value of the exact DNA sequence signature designed to process the sequences of fixed nucleotides to combine nucleotides for the sequence.

6. STRING AND BINARY IN DNA

When the sequence rises dramatically, spatial complexity appears to be the main problem in coping with the DNA search structure, every DNA molecule in a hash table is transformed to Numeric number prior to the pairing procedure [11] sequence alignment as a basic technique for finding prevalent patterns between sequences, identifying significant areas consisting of matching characters between two sequences. Some matching characters results in a measure of sequence similarity [12]. Encoding the DNA to bases as it represents the characters in these bases of DNA as shown in Figure 1 below:

Character=codon	Character=codon
A=AGC	U=CAT
B=ACC	V=TCC
C=TTG	W=GGG
E=CGG	X=CTA
F=TGG	Y=AAA
G=TTT	Z=CTT
H=CGC	0=TCA
H=GCT	1=CCC
I=GTA	2=TTT
J=TGA	3=GCA
K=GAA	4=GGC
L=TGC	5=CCT
M=CCT	6=CGC
N=CTC	7=ACA
O=AGG	8=GGG
P=TGT	9=ATT
Q=CAA	,=GAT
R=TTT	.=GAT
S=CCC	:=AAA
T=TTC	

Figure 1. Strings and the DNA codon [13]

7. DNA ENCRYPTION AND DECRYPTION METHOD

A. Data flow encryption and decryption using DNA bases

To demonstrate the conversion to polarized, the consumer's messages travel through a secure cipher-text DNA transmit which encodes a simple communication or image in distinct bases 0-B, 9-D, 02-E, and 11-G [14]. Before the digital file is sent to DNA, the image is first transformed into a matrix of bits, and the pixel values of the image must be jumbled in order to be decrypted into the base pairs of DNA.

After converting simple text into binary values in terms of 0s and 1s, the ASCII code is used to create the DNA code, which consists of three bases and strands. Since each letter is eight bits long, [7]. Figure 2 describes the movement of information by converting the wireless government channel to ASCII code and then encrypting it to a segment of DNA.

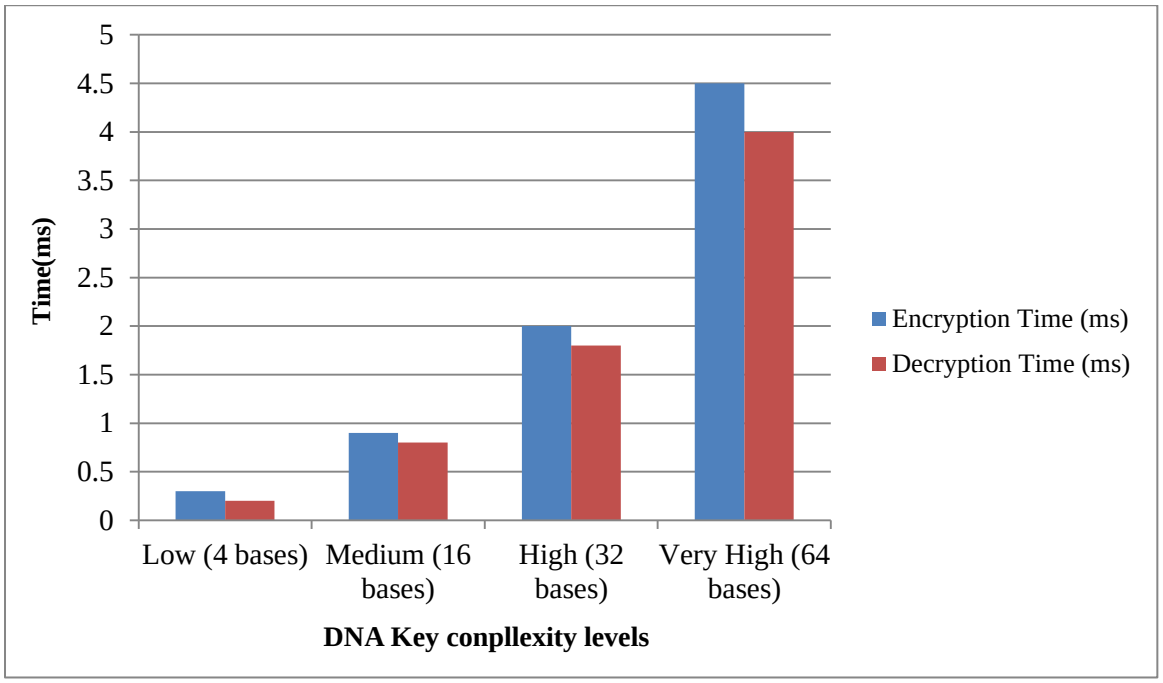

Figure 2. Encryption and decryption comparison

Figure 3 describes encryption and decryption time comparison across different DNA key complexity levels. As the number of DNA bases increases, both encryption and decryption times rise, indicating a trade-off between security strength and performance.

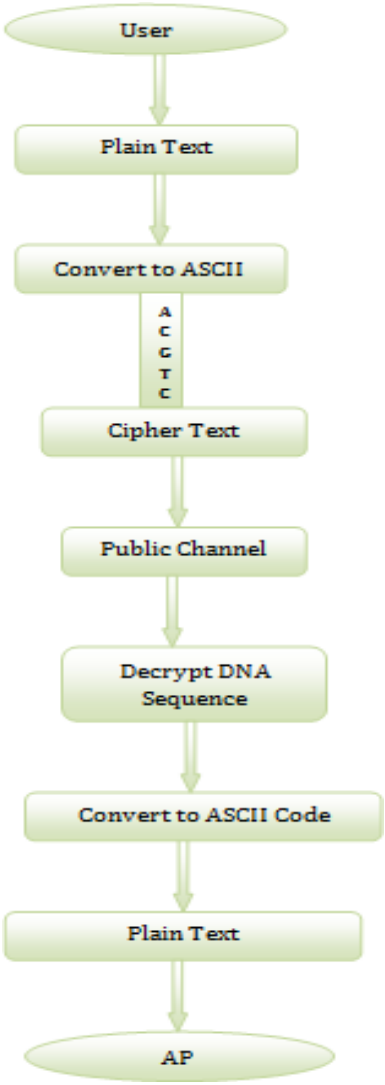

Figure 3. Cryptography and Decryption using a public network

The procedure of encryption starts with a message that contains characters, which is then entered into the system of encryption using a decoding method to become an encrypted text and transferred to a encoding protection across a public route to stop predators from knowing the first version text [15]. This process explains how to encrypt and decrypt DNA in a wireless network to safeguard the data stream inside the wireless network.

8. PROPOSED ALGORITHM

The suggested structure for safe wireless communication is to produce an isolated user DNA sequence for accessing keys intended for each user accessing their Access Point AP wireless network. Thus, the DNA nucleotides are the proposed algorithm for this process, so that each user will have their DNA sequence that is converted from the user data provided to be complex and a complex DNA bases sequence that is then stored on both The client's mobile gadget as well as the wireless router device for comparison authentication security when the DNA sequences are stored on the mobile deviation. The proposed work includes a number of elements:

A. Database

User data is kept in a system-generated database that includes static details such as login credentials, email, customer identity, initial and final names, and dynamic details such as CPU speed, number of browsed web pages, and mouse travel distance optional to place DNA sequences are more complex and attackers

cannot crack or suppose your popular details.

Thus the static and the dynamic are flexible when the programmers need to expand the columns to boost the complexity of the safety and make it more difficult to attack. Additional data is essential for commonly recognized user details that use the same wireless network or even external users such as attackers or intruders to secure their link and encrypt both. Details will be checked against the database's current information in order to match the complexity of the genetic code with the detected pattern in the wireless network router when deciding whether to allow connection or prohibit.

The user enters their information into the database system and then the algorithm converts that information into the ASCII format to binary and then DNA sequence, which is then stored on the wireless device as measured sequence records in cipher format of DNA bases, as shown in Figure 4 below.

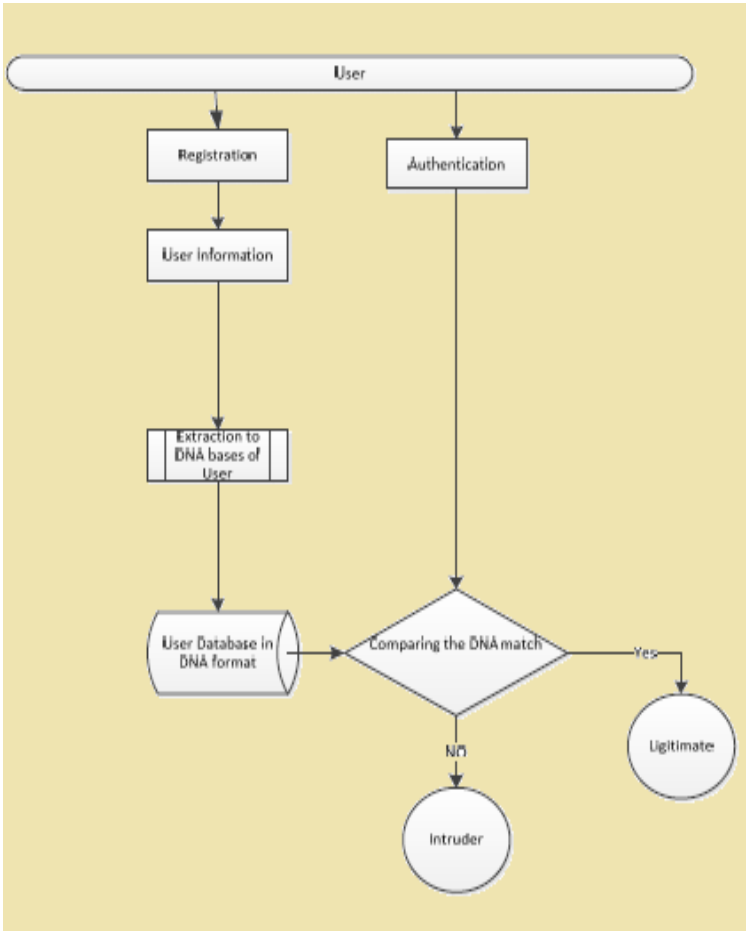

Figure 4. User records input

We add additional encryption by adding DNA strands from its octet to the encryption method to make the encryption more robust.

B. DNA conversion algorithm code

Initially, the file ought to be formed to record the user profile and the rows of the database should be multiple in order to obtain a succession for every document to ensure conformity these sequences and position them as the main match for the safety match, below is the instance of choosing a section in a table that is the first name area as displayed below and we need to link The databases to the data entry.

C. DNA parameter sequences Xi=Xj

Xis the nucleotides of DNA and I j is the sequence length. Andx is the essential comparison between the two systems, which the user device'sx sequence should match the wireless router'sx sequence, and the comparison will be compared to the degree of matching or mismatching each sequence as shown below:

σ(xi,xj)

xi=xj; match then the legitimate user xi≠xj; mismatch intruder

σ(xi,xj)	Score
xi=xj	1
xi≠xj	0

The binary of 0s and 1s is the feature for on and off if the xi = xj matches the sequences and its 1 means, as on, grants a link, if the xi = xj score 0 implies as off and denies the intruding link.

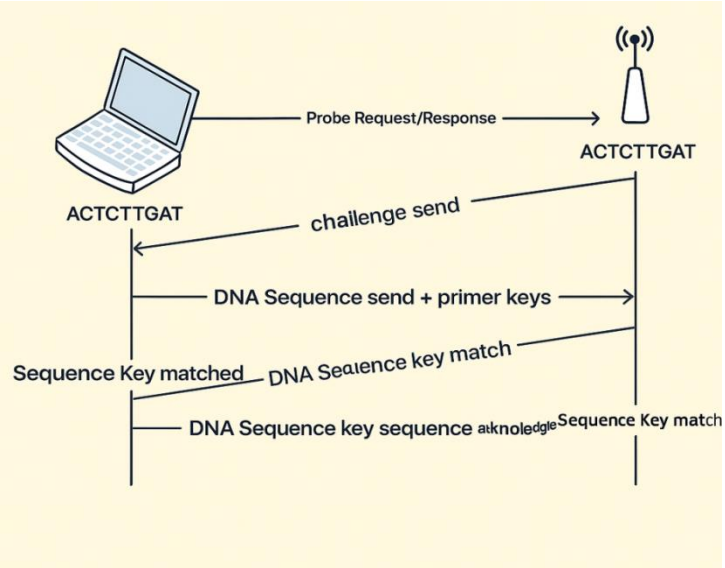

Figure 5. DNA sequences between two parties

Figure 6. Key matching DNA sequences

To successfully establish the wireless link the user transmits an authorization program to the wireless access point (AP) through the software's devices and the AP, after which the AP challenges the user. This access point decodes the primary kx sequence, vital xi, to match it with the xj sequence after the user responds to the encoded sequencing key utilizing the primer important kx to AP. of the wireless AP, and if matching succeeds, another link is set down as illustrated in Figure 5 and Figure 6.

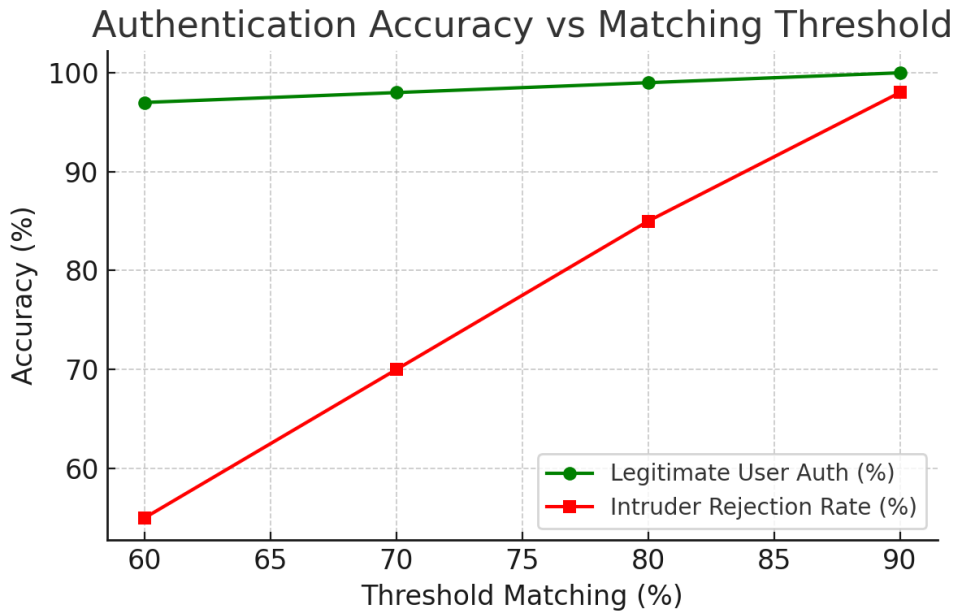

Figure 7. Authentication Vs. Matching threshold

The graph between authentication accuracy and matching threshold is illustrated in Figure 7.

D. Secure DNA public channel

The enormous scalability and exceptional concentration of data inherent in DNA are explored for algorithms like authentication, encryption, and signatures and signature. The Polymerase Chain Reaction (PCR) DNA keys that we utilize here are Kx and Ky, and they should be known in order to secure the public channel. PCR uses two priming pairs. We employ XOR to encrypt the communication channels of standardized categories by obtaining a high preservation factor. The encrypted code is created by bit-wise XORing the initial characters with the consequence bytes.

The safety channel keys used are the compression factor XOR as the XOR procedure with adequately lengthy key sequences between two parts, such as a wireless router and a user device that exchanges emails over the wireless channel and not over the internet.

Exchanging messages using XOR as both sides use lengthy sequences with sufficient entropy would safeguard messages from third parties, and PCR using the two primary keys to break complexity with the link keys. The kxi and kxj are the users and wireless computer DNA sequence keys. The mobile device's primary security code is xi, and the internet-connected device's code is xj. Their data stream is encrypted using the ky key. Secure route using XOR and PCR encryption is depicted in Figure 8.

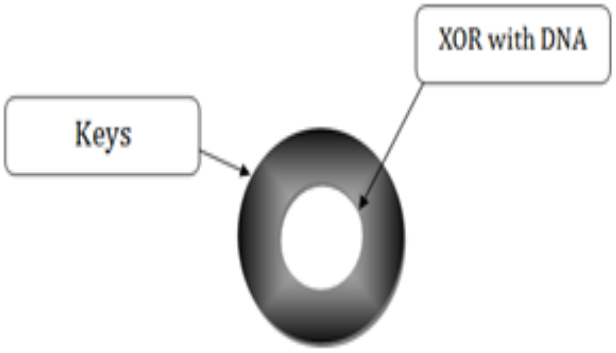

Figure 8. Secure route using XOR and PCR encryption.

The private key generated to DNA bases and sent over the secured channel-related to the router will be crucial in comparing it with the other similar private key preserved on the wireless connection as the

sequence noted. XOR will use the k to be performed and XORed to produce the right password as the key is supplied by the client whose profile exists when converting it to the exact sequence of DNA. Since the security digital encryption of the interior channel is difficult to crack, two more levels are shown for DNA decryption communication and decrypt in DNA bases if the DNA stage can be broken.

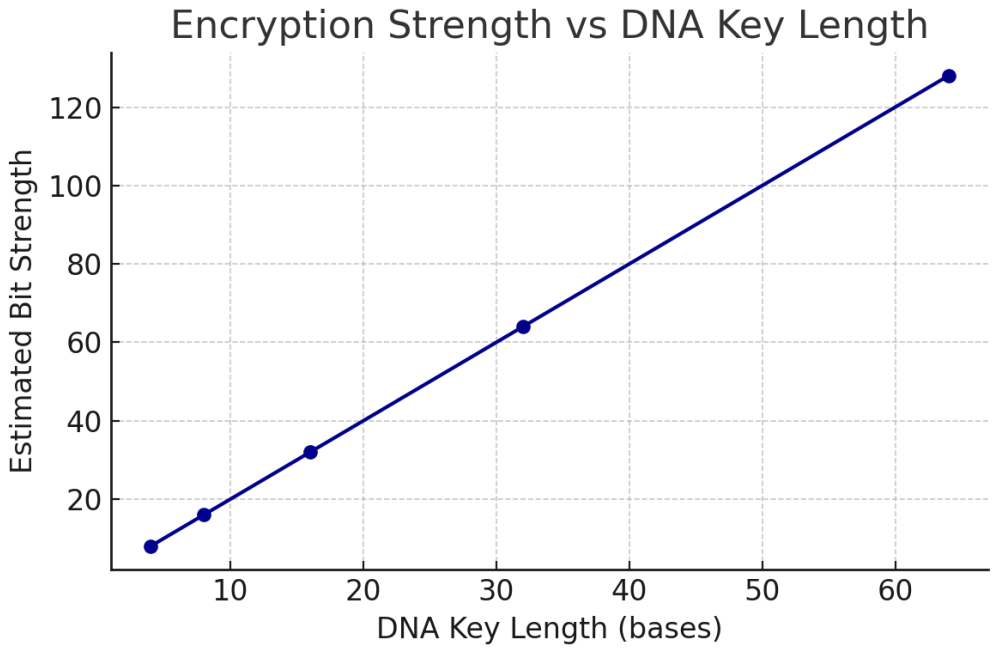

Figure 9. Encryption strength Vs DNA key length

Encryption strength and DNA key length is compared in Figure 9 effectively. Consequently, key ky is the PCR fundamental and, by fusing the password and DNA encryption, it functions as a secondary key for communicating with the key. By employing a single DNA decoding and encryption technique, we may safeguard the encrypted signal into DNA replacement and mutation, doubling the security of user data flowing over the open channel. If an intruder manages to crack our code, we can then change the DNA. The structure of the DNA sequence that makes using our two PCR keys and securing the open link more challenging.

9. NOVELTY

Our novelty is to present a DNA-inspired safety algorithm to authenticate wireless communication using DNA sequences instead of WPA2 as main access. We have suggested the concept of wireless network safety to show that DNA algorithm is the next generation for wireless network safety and we need to show the original steps for the emergence of wireless security using DNA algorithm as the DNA sequences are the primary biometric for each user device to allow a link to the wireless router for important encryption purposes.

10. CONCLUSION AND FUTURE RESEARCH

We show the user profile sequences in the database, the methods of extracting user records to convert them to nucleotide bases that will be the keys to match the sequences, the mobile device and the same sequence put it for network observation in the wireless router, which is the second key inherited from the user sequence, and store it for detection and matching in the wireless device. In order to generate the user signature sequence, similar to the desired threshold of the transmitted genome sequence in the transmission network connecting to that particular DNA Credentials ACTCCTTGAT DNA molecule sequence, the comparison of sequencing are carried out amongst two sides using internet-based parameter methods.

Then the keys have to compare the respective signature sequence with the observed wireless sequence to discover match or mismatch sequence resemblance degree significance.

Then the limit value of nucleotide sequences will determine whether this customer is a lawful user or an intruder, as we understand that the intruder has no matching sequences, then the quality degree of sequences is zero or the sequences do not match those found in the scheme, which implies that it is an intruder and increases adverse alarms to block the link.

The genome sequence is useful for detection systems in identifying an anomaly in the alarm height due to adverse communication that the combinations were unable to match or try to reconstruct the credentials of the victim user. Additionally, users on the exact same connection can be identified by their unique DNA arrangement if they would like to hack into another legitimate user on a wireless network that they share.

We have also proved in this job that DNA sequences can be used to encrypt and decrypt the information through the wireless channel, which is the user's essential information and the genetic material conceals this information with its nucleotide companies that utilize DNA cryptography and decryption operation by converting the plain text to ASCII and then DNA sequence to binary DNA bases numbers and sending it to the other party's government channel for decryption.

Our concept in future work is to develop wireless security using DNA safety methods to mitigate the faults of the present safety algorithms, as we have not yet reached the ultimate DNA region safety, However, if not we are proposing the original phases of the DNA technique safety for a wireless entry point for safety.

The system flow is now repeated in the conclusion. Strengthen it by:

- In contrast to WPA2/3, this technique improves wireless intrusion detection by providing bio-inspired, sequence-based identification.
- Real-world deployments may be impacted by hardware limitations for real-time DNA matching.
- Enhancing the logic used to generate DNA sequences in order to reduce false positives.

REFERENCES

[1] T. Kerygiannis and O. Les, “Wireless Network Security 802.11, Bluetooth and Handheld Devices,” Comput. Secur. Inf. Technol. Lab. Natl. Inst. Stand. Technol., vol. 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] G. Cui, L. Qin, Y. Wang, and X. Zhang, “Information Security Technology Based on DNA Computing,” 2007 Int. Work. Anti-Counterfeiting, Secur. Identif., no. 1, pp. 288–291, Apr. 2007.
[4] X. Wang, Z. Bao, J. Hu, S. Wang, and A. Zhan, “Solving the SAT problem using a DNA computing algorithm based on ligase chain reaction.,” Biosystems., vol. 91, no. 1, pp. 117–25, Jan. 2008.
[5] G. Cui, L. Qin, Y. Wang, and X. Zhang, “An encryption scheme using DNA technology,” 2008 3rd Int. Conf. Bio- Inspired Comput. Theor. Appl., pp. 37–42, Sep. 2008.
[6] A. Khalifa and A. Atito, “High-Capacity DNA- based Steganography,” 8th Int. Conf. Informatics Syst. - 14-16 May Bio-inspired Optim. Algonthms Their Appl. Track, pp.76–80, 2012.
[7] S. T. Amin, M. Saeb, and S. El-gindi, “A DNA- based Implementation of YAEA Encryption Algorithm,” Dept.Math. Fac. Sci. Assiyut Univ. Arab Acad. Sci. Technol.Marit. Transp. Sch., 2007.
[8] P. Layer, Telecommunications and information exchange Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specificati. 1997.
[9] S. Sukhija and S. Gupta, “Wireless Network Security Protocols A Comparative Study,” Int. J. Emerg. Technol.Adv. Eng., vol. 2, no. 1, 2012.
[10] 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,
[11] pp. 167–169, 2013.
[12] C. Kreibich and J. Crowcroft, “Efficient sequence alignment of network traffic,” Proc. 6th ACM SIGCOMM Internet Meas. - IMC ’06, p. 307, 2006.
[13] S. Lloyd and Q. O. Snell, “Sequence Alignment with Traceback on Reconfigurable Hardware,” 2008 Int. Conf. Reconfigurable Comput. FPGAs, pp. 259–264, Dec. 2008.
[14] C.T. Clelland, V. Risca, and C. Bancroft, “Hiding messages in DNA microdots.,” J. Nat., vol. 399, no. 6736,
[15] pp. 533–4,Jun. 1999.
[16] R. Soni, A. Johar, and V. Soni, “An Encryption and Decryption Algorithm for Image Based on DNA,” 2013 Int. Conf. Commun. Syst. Netw. Technol., pp. 478–481, Apr.2013.

[17] N. J. K, P. Karthigaikumar, N. M. Sivamangai, R. Sandhya, and S. B. Asok, “Hardware Implementation of DNA Based Cryptography,” Proc. 2013 IEEE Conf. Inf. Commun. Technol. (ICT 2013), no. Ict, pp. 696–700, 2013.
[18] Lackner, G. (2013). A Comparison of Security in Wireless Network Standards with a Focus on Bluetooth, WiFi and WiMAX. Int. J. Netw. Secur., 15(6), 420-436.
[19] Ferro, E., & Potorti, F. (2005). Bluetooth and Wi-Fi wireless protocols: a survey and a comparison. IEEE Wireless Communications, 12(1), 12-26.
[20] Chen, L., Ji, J., & Zhang, Z. (2013). Wireless network security (pp. 129-221). Beijing: Springer.
[21] Rawat, D. B., Yan, G., Bista, B. B., & Chandra, V. (2013). Wireless network security: An overview. Building Next-Generation Converged Networks: Theory and Practice.