Wireless Security Protocol in DNA Bio-Inspired Network

Abdulraqeb Alselwi

A thesis submitted in partial fulfiment of the requirements of Liverpool John Moores University for the degree of Master of Philosophy

March 2015

Wireless Security Protocol in DNA Bio-Inspired Network

By

Abdulraqeb Alselwi

Abstract:

The 21st century communications have evolved rapidly and spread all over the world using the Wi-Fi network which has provided benefits of connection which become more desirable for users to connect to the internet. These benefits are driving the world to a major internet security issues that links to harm their own sensitive data and it resulting for generates encouragement for attackers to drill the legitimate user's Wi-Fi connection to access to where they want to organize and eavesdropping the data passed to hack them through and revealing it to check whether it is useful for them, hence exploiting packets travelling through the user's Wi-Fi and using of the powerful of super sniffer techniques by the hackers to break in to such as malware and sniffing software that allows them to crack on the Wi-Fi to steal the data of the user who uses the eavesdropper Wi-Fi without their knowledge, these sniffers open to the hackers access to the user's data like bank details and other data, it could be using their details for a crime such as find their identity which make the world more concerns about their personal information and they are looking for the latest security protocols to protect their Wi-Fi network.

Wi-Fi security introduces a number of vulnerabilities that give hackers an opportunity to cause harm to the Wi-Fi users by stealing information, accessing the Wi-Fi network to compromise the Wi-Fi network as a way to access the enterprise network which is used by some security protocols. This would allow a hacker to use sniffers to access the Wi-Fi enterprise network which is used in coffee shops across the world and other trading premises by probing the SSID of their Wi-Fi. Near by the hackers would be able to crack the security protocols such as WPA or WPA2 which are the latest protocol that users use for their Wi-Fi security keys.

In our research we have taken different security methods to secure the Wi-Fi network using the bio-inspired DNA is the idea comed from the Deoxyribonucleic Acid DNA because that DNA have several important features including the random nature of the sequences denoted by alphapet characters A, C, G and T to perform encoded unique DNA sequences that is transmitting the secrets and the DNA encryption comes from the biology of the DNA science of the human and animals.

Our research has achieved basic steps which encrypt the user's static data to DNA sequence to use it for a security access key this work is functioning successfully to DNA bases and experimentation prove in the implementation at chapter 5, and we used the symmetric cryptographic keys in DNA sequence encryption to be similar at both parties with the admin(Wi-Fi) and clients and this is the basic step for this project and it needs to implement the dynamic DNA to make the keys more secure for each user and we have explained how we can match and mismatch these encrypted data and how they need to updated automatically to new security keys with the dynamic DNA sequence in future work [1].

The achievements of our research are proposed to convert user data to a DNA security sequence to use it in the same way as the existing security protocols such as WPA2 but in DNA format with the dynamic key and static user data will keep the security key rubost durig the automatic updates, hence the static data and dynamic data can be updated automatically when adding the dynamic data to the project in future work for the user access key and this can be suitable for multi-users to form an autonomous Wi-Fi connection and DNA security key to mitigating some flaws of that existing security protocols techniques has such as sharing the same security key on the same Wi-Fi network users.

Acknowledgement

Foremost, I would like to express my sincere gratitude to my Supervisor Bob Askwith who has directed me to the way that I have to be and supported me throughout my research and my thesis, and who by his guidance helped me in all the time of research and writing of this thesis. And this has benefited me, gaining more knowledge and getting it through his knowledge and experience while allowing me the room to work in my own way.

I thank him for his patience regarding several meetings and opinions that I have suggested to him which I finally I found the right way that I have to do, I am measuring his encouragement and efforts while looking for ways that from the thread to find the question for the research.

I thank my fellows in the University from all different departments for their research discussion problems and advise me to attend some of the events that the University puts on such as conferences and group meetings.

Last but not least; I would like to thank my family in Yemen my parent Ali Noman Alselwi who encouraging me to continue on the MPhil degree, and my wife who supported me during my study and preparing the house management stuff.

Contents

List of Figures:

List of Tables:

Abbreviations:

AES	Advance Encryption Standard
AP	Access Point
ARP	Address Resource Protocol
ASCII	American Standard Code for Information Interchange
CBC-MAC	Cipher Block Chaining Message Authentication Code
CCMP	Counter mode CBC-MAC Protocol
CPU	Control Process Unit
CRC	Cyclic Redundancy Check
CTS	Clear To Send
D	Decryption
DA	Destination Address
DES	Data Encryption Standard
DoS	Denial of Service Attack
DNAEDM	Deoxyribonucleic Acid Encryption and Decryption Methods
DNA	Deoxyribonucleic Acid
E	Encryption
EAP	Extensible Authentication Protocol
EAP-LEAP	Lightweight Extensible Authentication Protocol
EAP-FAST	Flexible Authentication via Secure Tunneling
EAP-MD5	Message Digest 5
EAP-TLS	Transport Layer Protocol
GTK	Group Temporal Key
ICV	Integrity Check Value
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPv4	Internet Protocol version 4
IV	Initial Vector
JDBC	Java Database Connectivity
JDK	Java Development Kit
LAN	Local Area Network
FMS	Fluhrer, Mantin and Shamir
MAC	Media Access Control
MAC	Message Authentication Code
MIC	Message Integrity Code
MPDU	Media access control Protocol Data Unit
mRNA	Messenger Ribonucleic Acid
NP	Nondeterministic Polynomial time
OTP	One Time Pad
PBKDF2	Password-Based Key Derivation Function 2
PCR	Polymerase Chain Reaction

PKCS#5	Public Key Cryptography Standard #5
PMK	Pairwise Master Key
PSK	Pre-Shared Key
PTW	Pyshkin, Tews and Weinmann
RADIUS	Remote Authentication Dial in User Service
RC4	Rivest Cipher 4
RSA	Rivest Shamir Adleman
RTS	Request To Send
SID	Service ID
SIM	Subscriber Identity Module
SQL	Structured Query Language
SSID	Service Set Identification
SSL/TLS	Secure Socket Layer/Transport Layer Security
TA	Transmitter Address
TGi	Task Group I
TK	Temporal Key
TTLS	Tunnel Transport Layer Security
TKIP	Temporal Key Integrity Protocol
URL	Uniform Resource Locator
WLAN	Wireless Local Area Network
Wi-Fi	Wireless Fidelity
WEP	Wired Equivalent Protocol
WEP2	Wired Equivalent Protocol
WEP+	Wired Equivalent Protocol plus
WPA	Wi-Fi Protected Access
WPA-PSK	Wi-Fi Protected Access Pre-Shared Key
WPA2	Wi-Fi Protected Access 2
XE	Express Edition
XOR	Exclusive Or

Chapter 1:

Introduction

1. Introduction:

The internet is a global network connecting millions of computers exchanging data, news, opinions and online services, which are centrally controlled as the operator, can choose which internet services to use and make available to the global reference for scale of internet use and population. The internet is not synonymous with World Wide Web (WWW) as the internet is a massive network of networks to connect millions of computers together. The WWW is a way of accessing information over the medium of the internet for sharing data. The question of reliability of the internet is important, services such as Voice over IP (VoIP), video conferencing, streaming media, gaming and online trading (e-commerce) have stringent requirements on end-to-end reliability. Reliability in today's internet is often questioned, which is implies that it is hard to provide across internet service provider boundaries partly due to lack security on both incentives and mechanisms for ISP[2][3]. The internet has been available everywhere using broadband, it is approaching universal service, and reporting of the speeds achieved by broadband services has become more reliable. On the other hand there are concerns about reliability as a growing range of services move into the internet and it is reasonable to expect that demand for reliability will increase and security is in demand too with this increasing range of services and broadband speeds[4].

Internet reliability concerns are growing due to the broad range of services and security issues that are required to secure the internet whether wired or Wi-Fi. Internet security includes internet browsing security and network security and it aims to apply rules and measures to use against threats such as attacks that lead to a high risk of fraud in the exchanging of data through the internet network. It requires the use of the latest security to encrypt this data through applying different methods of cryptography and protocols that are existing and reliable, and they are suitable for protecting information from attackers who are listening over the internet network or Wi-Fi[5].

However the networks are a telecommunication network that allows computers to exchange data transferred through the network and the data transferring is in the form of packets that is established using either cable media or Wi-Fi media. The network is very important to make connections to the right people and the right organizations, and the network provides the most productive and proficient way to succeed in our connecting relationships with the globe to exchange the data that is needed to be sent. But people get lots of problems when using the network as they get viruses on their computers when using websites from the internet, or connecting to the internet, and pick up problems that are around when browsing for example infected computers, such as Denial of Service attacks (DoS) to disable the network and there are lots of attacks which make the network vulnerable to attacks. The hackers can use these DoS attacks when breaching into the Wi-Fi connection as the vulnerability of networks and computer systems consists mainly of neglecting the security and the security mechanisms; added to these types of attacks can be data modification or capture or taking control over a system as the consequences of network threats become more and more dangerous[6].

The internet network security whether wired or Wi-Fi, is needed for the degree of resistance and protecting the data from harm as the internet connects millions accessing the limitless information. However, this raises the risk of loss of data integrity and loss of privacy. With the help of cryptographic methods and protocols, the security protocols are designed to protect communication in a secure manner therefore a set of security extensions is needed to provide security and authentication by transforming data using encryption and decryption, and in our project we have chosen DNA inspired as the new extension way in security.

Not all the existing security that we have are good; the problem is still there and the world is looking for different ways to breach the latest security protocols to find any flaws and exploiting those flaws as a stepping stone intended for attacks on the sensitive information that is run through the networks and in chapter 2 we have discussed the recent attacks with the Wi-Fi security protocols and how the security key is broken using the sniffers on the network.

Wi-Fi network is a computer network that uses Wi-Fi data packets to connect to the internet network node usually providing a connection through an access point to get internet access. Wi-Fi is one of today’s leading technologies, which is based on IEEE 802.11 and it is used worldwide as it deployed in every corner of the planet, as it is too easy to install and used by a variety of users and premises such as coffee shops. As the Wi-Fi spreads, its waves around the domain area to allow the devices pick up their signal for connecting to the internet it is open to any user to access the Wi-Fi, which causes vulnerability and gives a path to the attackers to access the internet. The Wi-Fi networks require a security mechanism to prevent attackers from stealing data or damaging computers using a variety of viruses; therefore networking suffers from many problems with the wireless local area network (Wi-Fi) using access point devices with coverage range around 150 to 300 feet’s make it prone to malicious attacks, via the Wi-Fi signals which are the backbone of attacks and cause the major problems to the Wi-Fi network which needs to minimizes the existing harms but not solving the whole problems. Here since the IEEE issued the Wi-Fi networks they wanted to secure it using the security mechanisms that were used in wired networks,[7] but they ended up with lots of experiments in which they were trying to tackle and solve the security issues that Wi-Fi was facing through their signals because attackers found it easy to access the sensitive information. Unfortunately the problem is still out there today and there is no barrier which can stop intruders from attacking the Wi-Fi network[8], therefore in the last decade the IEEE have solved some of the Wi-Fi network issues with a few security protocols up to now and the common ones are WEP, WPA and WPA2[9], [10][5][11].

Individuals and organizations use Wi-Fi for their own benefit for sending and receiving data resources when reassured that this Wi-Fi is fully protected. However, Wi-Fi network is taking management operation and access control using the modern security mechanism while these actions on track will not prevent all penetration and unauthorized access. Attackers are always using the Wi-Fi network medium because they find it the open gate to stepping-stone and launch an attack and so the Wi-Fi is becoming the prime target for eavesdropping and attacking which disrupts the service of the legitimate users, while Wi-Fi network is free to travel around the venue but it essentially calls for robust security mechanism to maintain confidentiality, availability and integrity.

Security has raised the major concern in Wi-Fi network domain, which opens the vulnerabilities of data transmitting between two or more devices in the Wi-Fi

The network is facing a threat to the security and trust that users need to protect their data assets from such unauthorized access, denial of service attacks, spoofing and eavesdropping. To counter these issues which Wi-Fi networks face, various standard authentication and encryption techniques are combined with security mechanisms to secure the Wi-Fi domain in order to tackle eavesdroppers that used for connections to the internet for sending and receiving data hence new security protocols, encryption and decryption are needed or updated for the trusted security and authentication [8].

2. Research Aims and Objectives:

There are existing versions of security protocols around used for Wi-Fi protection and on the other hand lots of attackers looking for ways to break these security protocols using different techniques such as sniffer software and to get through the Wi-Fi network and violating the privacy of the legitimate user to steal sensitive information such as bank details or any related data that help them to launch a new attack against this legitimate user.

Our new method of security is looking to at least find a way of mitigating or adding new techniques to the current security mechanism using the DNA inspired protocol. In this way, we cannot prove the full protection of the Wi-Fi network yet however we can illustrate that DNA is the new generation for the next era and might prove the satisfaction of security beside the current security mechanisms.

The DNA cryptography has become the leading field of international research as it is still in its exploratory study to find new ways of using the DNA such as in security encryption and decryption that's already been done up to now, and the DNA started by Adelman pioneering of first DNA computing that marked the new era of DNA in computing.

The main objectives of our research are:

- To investigate alternatives to the existing protocols to do wireless security for multi-users with isolating security key for each user
- To investigate how DNA encryption can be applied to wireless security key access
- To develop and experiment software with act novel DNA security program
- To demonstrate how the user data is encrypting to DNA sequences Format and save it to database

Below is the charts of the system process and discipline on symmetric encryption algorithm using the DNA nucleotides to encrypt the user data to a security key in DNA bases and save it in the database as an innovation for the security of the Wi-Fi, to form independent security access connection for each user's device and to deliver the reliability integrity and confidentiality for the legitimate user when sending and receiving their own data over the wireless connection between the user's device and the Wi-Fi to the internet.

In this intellectual project the DNA Bio-inspired are not determined to use the real biological DNA for this process, it is only the idea come from the DNA of biology and how each biology has its own unique DNA in real life. Moreover, here is a brief explanation of this DNA process software we have the Admin interface where the admin role is adding the user to registered and encrypt their data to DNA bases and then save the DNA based to the database, the encryption process shows in details in chapter 5. And the admin can test the user's DNA sequence key by accessing as a legitimate user to authenticate the user and the process compare the key against the record with the database and if the sequence match then grant connection otherwise grant disconnect.

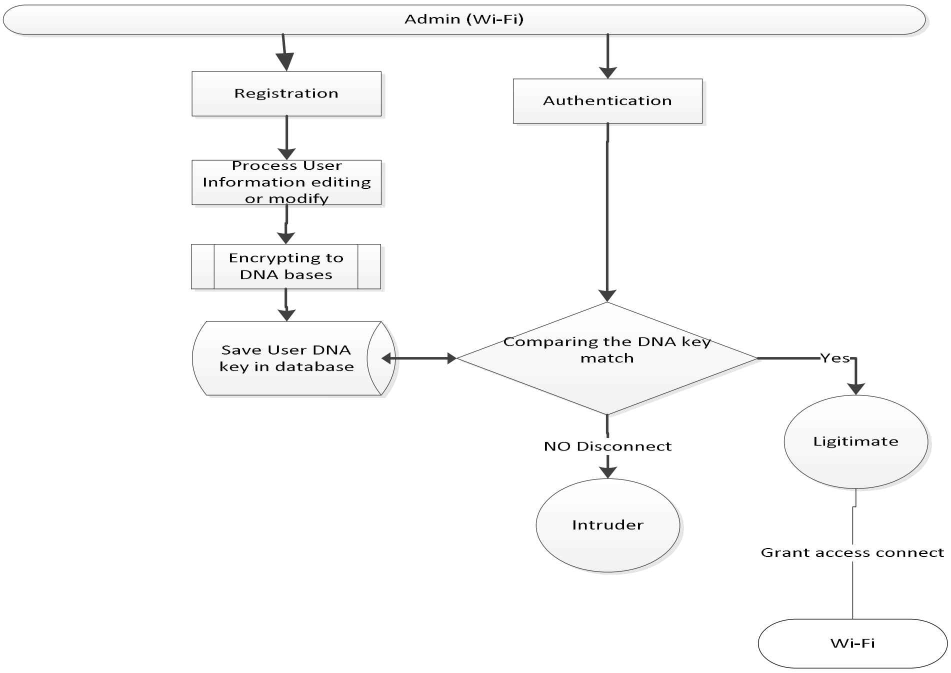


Figure 1 Diagram of the Wi-Fi connection process with DNA encryption match

Also the following diagram is the user interface and it serve the symmetric DNA algorithm developed and implemented in the user side with the Polymerase Chain Reaction (PCR) of the DNA and the primer numbers should be the same with the admin and the user which is to get known of the keys by the user and admin.

The user does not have the privileges like the admin, because the admin have the privilege of the whole controls and modifies of all the users, the reason for this, because the each Wi-Fi should be access only by one admin for the purpose of security access management. With the user interface merely the user have to insert his data and translate it to DNA sequence which should be the same with the DNA sequence stored in the database otherwise it won't be able to connect to the Wi-Fi and this resulting to a disconnection.

Also the system authentication won't allow two users use same DNA sequence key to the Wi-Fi this is concurrency access the reason of this to block the hackers who capture the packet and reveal the DNA sequence key, if the legitimate user find out that he/she blocked by the system then he/she knew that there in attack, and their security key is stolen by the hacker then in this case they should report to the admin in instruction to modify and alteration the DNA sequence key to get a new key.

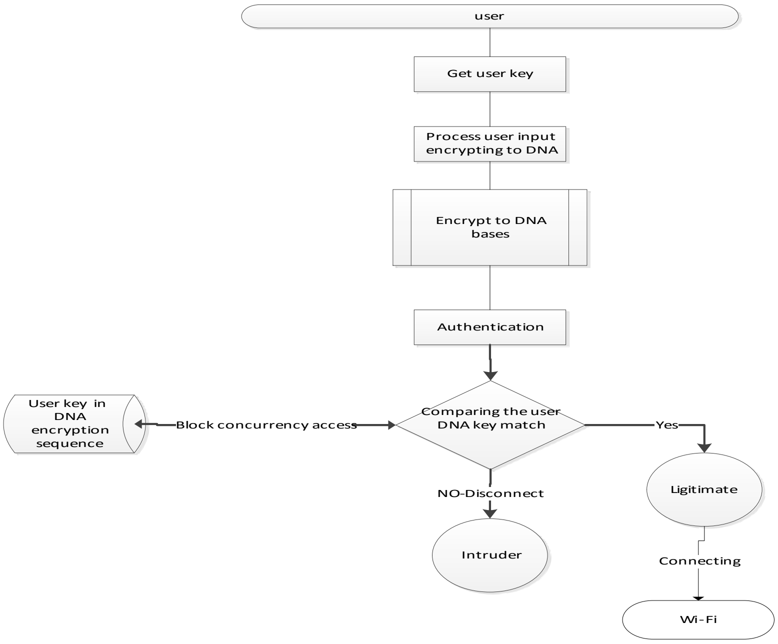


Figure 2 User device access to Wi-Fi with DNA sequence key access

Here we have tested the user interface access to the Admin (Wi-Fi) interface in java and we have created the java software to act as a system for security controlling access which include a user interface and a Wi-Fi interface and it processing the user data to encoding it with the DNA four nucleotides which can be encrypted to a signature of DNA sequence as a DNA key and these tests are demonstrated in chapter 5 and above we have the two diagrams of the user process access and the Wi-Fi as admin who controls the users and the database of the proposed DNA Security Protocol for Wi-Fi system, here every user record is inserted and converted to DNA sequence encryption to serve as a security key and save it in the database by the admin as this is basic more discussion about the diagrams above in chapter 5, therefore DNA sequence and the contribution of this proposed idea is that DNA can compare the exact sequences for matching the security key for each user want to access to serve the connection of Wi-Fi security and provide trusted security and authentication to the user. This protocol is not approved for the whole system yet as a new security protocol but it opens the path to add security mechanisms and functions to make it more sophisticated and effective in different ways and to change the Wi-Fi security to a robust security protocol when investigating how to solve the current flaws that current security protocols have. The interesting aspect of this innovation is that the researchers are moving to DNA domain as a new security era and they have released lots of searches in DNA that provide security to the data protection exploiting the benefit of DNA hidden data to its bases as encryption which makes it hard for the attackers to break into this DNA bases because they don't know the prime keys and if they knew the prime keys then we can change the coding of the keys to a new prime keys.

The remainder of the thesis structure is as follows: chapter 2 is literature review, chapter 3 is the discussion of different existing DNA encryption and decryption methods, chapter 4 requirements and methodology of the research, chapter 5 is the proposed idea of DNA security protocol for the Wi-Fi authentication, chapter 6 is the evaluation, chapter 7 is the conclusion and future work and finally chapter 8 is the references and following this is coding of the implementation using Java NetBeans software program.

Chapter 2

Literature review

2.1 Introduction

Introducing the wireless networking and security protocols to allow Wi-Fi networks providing security to secure the Wi-Fi connection between the user and their Wi-Fi router in order to prevent any intruders from accessing or sniffing the Wi-Fi packets of the legitimate users.

To prevent the hackers of revealing the data it needs encryption is the process of encoding messages or information is such a way that only authorized parties can be read it, and here the DNA is an interesting medium for hidden messages[33]; in an encryption scheme the message or information referred to as plaintext is encrypted using an encryption algorithm generating cipher text that can be read if decrypted and the encryption uses a pseudo-random encryption key generated by an algorithm. It is in principle impossible to decrypt the message without possessing the key and authorized users can decrypt the message with the key provided by the originator to recipient.

The existing Wi-Fi protocols have been modified during last decade, due to a variety of attacks that left clues from the intruders on how to break into the Wi-Fi security protocols or stealing the data through capturing it packets during the monitoring the Wi-Fi traffic of the user. This makes the Wi-Fi network prone to lots of different attacks that cost users of stolen sensitive data information such as bank details and personal identity ID by the attacker's hacking techniques.

In this section is the fine point of the common security protocols that IEEE developed and their benefits during a certain time of how they are not enough to protect the Wi-Fi network.

The first Wi-Fi security protocol was WEP Wi-Fi Equivalent Privacy implemented by IEEE 802.11 as a default encryption protocol[13] and introduced in 1997 for Wi-Fi security. Then several years passed and this protocol became more vulnerable when its cryptography was scrutinized and numerous attacks were announced because of the exploiting of flaws found by the attackers and weaknesses that made this protocol insecure and it could not be relied on any more. Then after this protocol, IEEE developed WPA to overcome the flaws in WEP in 2004 and they kept updating it as the process had been broken into, and finally developed WPA2 to solve flaws in WPA. So here, we have to understand how wireless security developed through these security protocols to where we are now; it developed from a very basic security protocol and they were monitoring their experience with the current protocol in order to solve the flaws and amend it to the next generation protocol. Therefore, our project is new and it begins from basics using a different way, which is DNA.

2.2 Types of Wireless:

In the context of wireless the target is to manage radio resource sharing and the wireless is recently addressed with the mobile networks such as WiMAX, Wi-Fi and so on[14] and the Wi-Fi is the media for transferring of information between two or more nodes. The most common wireless technology is the radio; with the radio, waves distances can vary and it encompasses various types of fixed, mobile and portable applications, the wireless networking could be GPS, sensors, satellite television, cordless telephones and Bluetooth and there is a lot of wireless technology that is communicating with the devices for portable purposes such as headphones, keyboard, mouse and etc.

2.2.1 Wireless Wide Area Network

Wireless WAN are networks that typically cover large areas such as between neighboring towns and cities, these networks can be used to connect branch offices of businesses or as a public internet access system, the wireless connections between APs are usually point to point microwave links on 2.4 GHz band, it contain base stations BS gateways, AP and wireless bridges relays. It provides internet access to mobile subscribers over regional or even global region, it would be desirable to generate additional revenue from the available wireless capacity providing incremental data services[21] on the WAN, and can connect remote devices or networks and may offer complex and comprehensive services[22].

2.2.2 Wireless Local Area Network

Wi-Fi LAN provides quick access to the internet and is widely deployed in hotspots areas. It links two or more devices over a short distance and it provides a connection through access point AP to access internet[23] while use of spread spectrum or OFDM technologies may allow users to move around within a local coverage area using IEEE 802.11 Wi-Fi standard there are three spread spectrum wireless technologies and they are not interoperable. The three technologies are direct sequence spread spectrum, frequency hopping spread spectrum and infrared. And it will operating in the 2.4 or 5.8 GHz[24] and the research of this project is focusing on the wireless network Wi-Fi security using the DNA security as a protocol for authentication and encryption. From the invention of Wi-Fi technology people have been committed to address the Wi-Fi security, in recent years enterprises have paid more attention to protect the internal network using various sorts of security software such as firewalls against external network as the wireless network allows the attackers to access into the internal network of the organizations passing by through the boundary of the physical security and this makes the wireless more vulnerable to diversity of attacks[25]. Our research is focusing on the Wi-Fi experimenting the DNA security to find a new protection mechanism for the Wi-Fi.

2.3 Overview of the Wi-Fi:

The IEEE in 1988 established a committee to develop the 802.11 standard of all the 802 standards with the data link layer and physical layer of the OSI reference model, the IEEE 802.11 committee held two Wi-Fi workshops before releasing the first version in 1997 [26] and it was the first approved international interoperability standard for Wi-Fi. The 802.11 standard supports three transmission methods, including radio transmission within 2.4 GHz[27]. In 1999, IEEE ratified two amendments to the IEEE 802.11 standard, IEEE 802.11a and IEEE 802.11b that define radio transmission methods and modulation techniques. Wi-Fi equipment based on IEEE 802.11b quickly became the dominant Wi-Fi technology. IEEE 802.11b equipment transmits in the 2.4 GHz, offering data rates of up to 11 Mbps. IEEE 802.11b was intended to provide performance throughput security features comparable to wired LAN. IEEE 802.11a operates in the 5GHz unlicensed National Information Infrastructure (UNII) frequency band delivering data rates up to 54 Mbps.[27]

The proposed 802.11g standard was rapidly adopted by consumers starting in 2003 due to the desire for higher data rates and reductions in manufacturing costs.[28]

2.4 Wi-Fi network Architecture:

Wi-Fi network architecture defines the components of Wi-Fi network, to establish a connection between the Wi-Fi router and the devices, initially starting with scanning to find the existing Wi-Fi network in a nearby region, then it will pick up the list of the scanning network names using the SSID of the network identity with the specifying list of Wi-Fi channels of the clients to start connecting with probe. [29]

2.5 Wi-Fi security functions

Wi-Fi provides network interactions over a limited distance using the Radio Frequency RF or the infrared IF signals Wi-Fi without cables or wiring, and the Wi-Fi access points are attached to the access point AP to communicate with AP through the Wi-Fi adapter. The Wi-Fi has a variety of issues such as:

- Availability: to maintain the capability to receive or send data and to prevent DoS attacks that block service availability.
- Authentication: to establish the identity of the sender and receiver and any integrity check or confidential information is often meaningless if the sending or the receiving party is not properly established.
- Authorization: is generally tightly coupled with the authentication, authorization establishes what you are allowed to do after you have identified yourself.
- Access control: the capability to control the access of entities to resources based on various properties: attributes, authentication, policies and so on
- Encryption: The transmitting of data though Wi-Fi as plain text to meaningless ciphers text based on some algorithm; decryption is the act of turning the meaningless bytes to meaningful plain text.
- Wi-Fi Local Area Network security designed a security to protect the network from various breaches to which Wi-Fi transmissions are susceptible, as the Wi-Fi signals have no limited boundary and hence it's prone to illegitimate access over network resources, resulting in the vulnerability of private and confidential data.[8]

2.6 Wi-Fi issues:

The signal is broadcasting and sharing with other signals of the Wi-Fi network causing other Wi-Fi networks to listen to the traffic that they share in the range that makes it difficult to secure this range and could cause the data revealing to third party. It is also difficult to locate the third party devices which are trying to sniff or access the Wi-Fi network while the signals spread around the 150 to 300 meters distance, also the Wi-Fi network faces huge security issues because current security protocols are not confidentially secured and they are poor at the encryption purposes and prone to attack and unauthorized Wi-Fi equipment may interference with and degrade the performance of authorized services.[30]

2.7 Wi-Fi attacks Type:

- ➢ MAC spoofing: reconfiguring an attacker's MAC address to pose as an authorized Access Point
- ➢ Eavesdropping: Capturing and decoding unprotected application traffic to obtain potentially sensitive information
- ➢ AP: Pretending as authorized AP by inspiring the Wi-Fi SSID to attract the user.

- Man in the Middle: the sender sends the message to the receiver but it passes through three positions first the sender sends it then it passes by the attacker and finally arrives to the destination.

2.8 Cryptography is the major support to protect data:

The idea of cryptography is to code the signals or code data using keys for securing the communication from the presence of third party using keys and signature for verification or encryption and the process of the encryption in cryptography is flourishing due to the research.[31] Modern cryptography comes with rapid growth of internet and network, and is heavily based on mathematics and computer science. Cryptographic algorithms are designed around computational hardness assumptions making such algorithms hard to break by the adversary. It is theoretically possible to break such as a system and the cryptography related technology has legal issues, to expect a criminal to provide their decryption key to law enforcement is unconstitutional. Protecting personal privacy and proprietary information during transmission over insecure networks and maintaining confidentiality are becoming increasingly important factor. The principles applied to secure computer networks are usually underlined on the level of security therefore the network needs to be protected by a user authentication procedure to protect against an intruder accessing the network then attacking it; then ensure the data confidentiality cryptography technology needs to be applied in handling and the network needs to be trusted by applying security to close the loophole and strictly utilizing the confidentiality data to improve network security and integrity in such a way that performance status can be monitored. [32]

2.9 What is Authentication?

The Authentication is the act of confirming the truth of an attribute of the data being in process and identification of data identity and in the usual process, it identifies the people who are accessing their own accounts and in the formal government process with authentication, validating the identity of the documents or certificates. Here the authentication is used for network based businesses including online services for users authentication schemes to protect businesses and clients against security threats. In authentication it uses usernames and passwords for a two factor authentication, session key exchanging and dynamic password scheme, these process will be compared by the server at the business side to check whether they match or not the database files, which if this is prone to attack could put people at risk of their financial accounts or private business accounts[34] being hacked. The authentication is accepting proof of identity given by a credible person who has evidence that the identity is genuine.

2.10 What is a security key?

The key here we are looking for is a key cryptography or a security key, which is a piece of information parameter to determine the functional output of a cryptographic algorithm or cipher and it specifies a plaintext into a cipher text. The security of the key is influenced by two factors: the key condition and the storage location of the key, accordingly the key measure condition of the information system, the leak of the key will do great harm to the global security of the system, here the key needs continued improvement to the system to ensure the security of the sensitive information is functional and accurately reliable [35]. The security key has other uses such as digital signature and messages authentication codes MAC, here the secrecy of the key provides security

2.11 Wi-Fi Security Protocols

Wi-Fi networks are providing mobility that is becoming prone to attacks, and because of to these attacks the Wi-Fi network need security to deter these threats. And there are three security protocols that Wi-Fi networks implement for protection.[10]

In 2004 WPA appeared and was more active and the world moved to this new protocol which came after the consequences of lots of intrusions break in to WEP and it served the purpose of solving the problems in the WEP cryptography method[36]. It has two operating modes: Enterprise mode and PSK (Pre-Shared Key) mode and in order to fix the weakness discovered in WEP, the WPA Wi-Fi Protected Access was released by Wi-Fi Alliance and the security has been enhanced because of anti-replay protections and key management scheme avoid key reuse in WPA, however some weaknesses are also applicable to WPA despite the different key between any two encrypted packets in RC4[37]. Then a new protocol came to the surface called WPA2 which is the final IEEE 802.11i amendments to the 802.11 standard ratified in June 2004, WPA2 uses the Advanced Encryption Standard AES for data encryption and AES is stronger than TKIP thus providing additional network protection[38] WPA2 was not designed to be hardware compatible with WEP as WPA was, it implements the mandatory elements of IEEE 802.11i standard and introduced to CCMP Counter Mode with Cipher block chaining Message Authentication Code Protocol which used the AES block cipher and CCMP is created to replace the TKIP and WEP[39].

WPA2 has a number of security weaknesses including using a dictionary attack which it took up to 10 minutes as explained in [40] and this result of cracking the WPA2 as the channel 6 in the access point is prone to attack through bypass several layers of protection [40]. Also another vulnerabilities with WPA2 shows at Time Memory Trade Off TMTO attacking the CCMP which used the PN, A2 length of payload to compute the counter value and can be pre-computed by an unauthorized user which resulted in this attack and the dictionary attack used the Airtight of access point of transmitting data encrypted using GTK and client supposed to decrypt that traffic exploiting the insider authorized user can sniff and decrypt data from other authorized users scan their Wi-Fi devices install malware and compromise the device to access the privacy of authorized users.[8]

In addition, the vendors keep changing the Wi-Fi security protocols due to the changing of the technology, which gets in to the hands of the intruders; as these technologies are the ladders for the intruders to climb on to steal the data of the companies or persons. Here are the protocols that the world relies on as follows:

2.12 Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy protocol (WEP) was the first Wi-Fi protocol for securing the first standard of IEEE 802.11 that was introduced in 1997, and this WEP protocol was first implemented to secure the Wi-Fi in 1999 as part of IEEE 802.11 security standard[10]. This was provided to distinguish this security protocol WEP from the wired network.

It uses the RC4 stream cipher for confidentiality and CRC-32 mechanism for integrity, WEP constructs the cipher text by performing the XOR on the plain text and an RC4 key stream. A Key stream is 40 bit, 104 bit and 232 bit key concatenated to a 24 bit initialization vector (IV) used by WEP[10], [39] A 24 bit IV is simply too short to ensure that a collision will not happen. In 2004 there were a lot of reports of attacks against the WEP which is due to the key size of WEP 40 bit key size and WEP 104 bit key size and these attacks are: the Fluhrer, Mantin and Shamir (FMS) attack, the KoreK attack, the Pyshkin, Tews and Weinmann (PTW) attack and the ChopChop attack.[41]

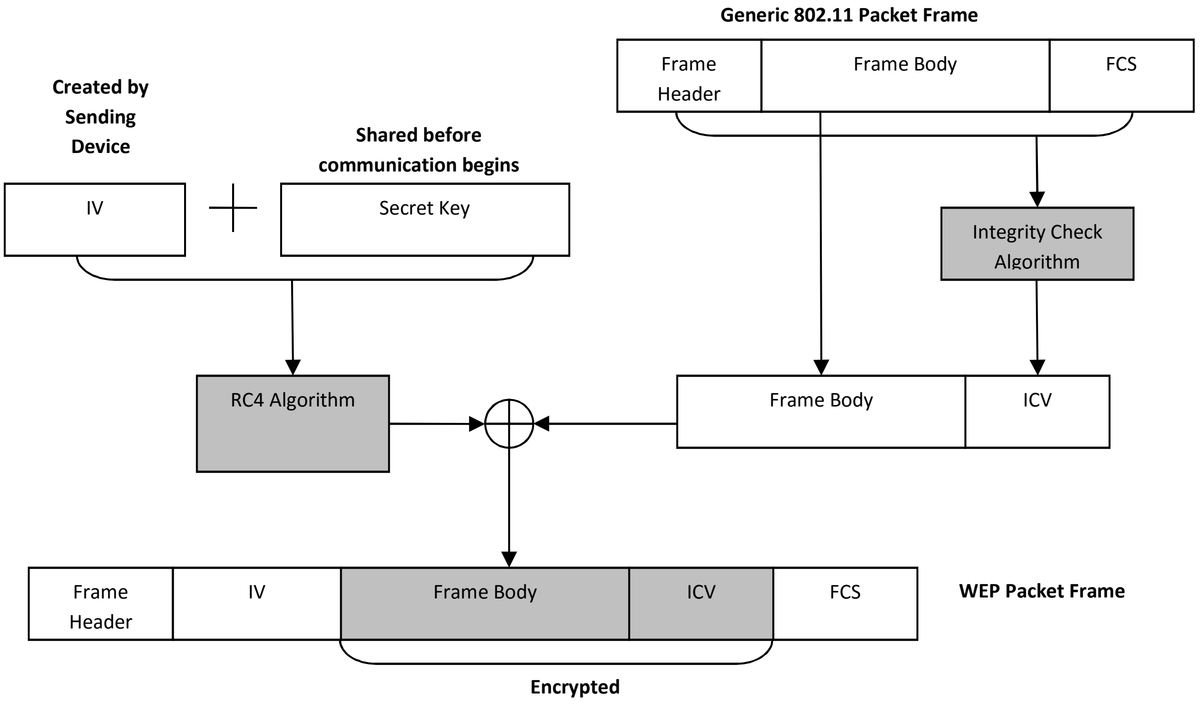


Figure 3 WEP Process

[42]

2.12.1 WEP Weaknesses as follows:

- A shared Wireless security key
- Each packet doesn't have authentication
- Vulnerable to threats such as modifications, eavesdropping and DoS attacks
- RC4 can't protect plaintext which is vulnerable to attacks

WEP uses RC4 secret key stream cipher to encode and decode packets, which is created by Ron Rivest of RSA, and the process of WEP is shown on the figure (1).

2.12.2 The steps of WEP process as follows:

- Initial Vector (IV) of 24 bits is produced and attached to the secret key of 40 bits to form key value for RC4 stream cipher
- The output of RC4 stream cipher is a Pseudo Random sequence
- Integrity check process through Cyclic Redundancy Check (CRC) is performed on each packet and able to find a single bit error to generate Integrity Check Value (ICV)
- The ICV is attached with XOR together and to output the RC4 stream cipher

- WEP frame assembled and repeat this on each packet. [43]

2.12.3 WEP non-standards protocols

- WEP2:

  This is the technical enhancement to WEP for the early 802.11i, which has been implemented by some companies and now able to handle WPA or WPA2, and extended both the key stream to 128 bits and IV. WEP2 needs extra changes, as it is not clear that if can stop any brute force attack or eliminate the duplicate of IV.

- WEP $_{plus}$:

  WEP+ is a proprietary enhancement to WEP avoiding the weakness of IV, but this cannot be relied on because of its limitation roles.

- Dynamic WEP:

  The dynamic changes made to 802.11i as part of TKIP but not for the actual WEP algorithm.[11]

2.12.4 WEP Issues:

- WEP is considered a weak cryptography protocol; the shared keys tend to be poor quality and can be discovered using cryptanalysis.
- The size of the key 40 bit is not enough for protection, thus it is prone to threats
- Poor key process that provides poor management and quality.
- Attackers can block the connection through sending a large number of messages to the access point
- Initialization Vector can be reused, which makes data easy to be decrypted without the knowledge of encryption using various technical tools for this purpose
- Denial of Service (DoS) attacks can be launched using a transmitter to generate powerful radio signals to interfere with the wireless transmitter to block the radio path
- The impact on availability of electromagnetic energy emitted could jam the wireless frequency making it inactive.[10]

2.12.5 The existing attacks on WEP

WEP protocol has several vulnerabilities with a long list of attacks over the last few years, and the main weaknesses are the initial vector IV and the internal states of key streams[44].

2.12.5.1 *Chopchop attack*:

This attack was created with the pseudonym Korek in 2004, and can decrypt the last bytes of plaintext-encrypted packet, when the Integrity Check Value ICV is attached with plaintext. These attacks exploit the insecurity of this four-byte checksum. This checksum allows integrity checking of encrypted packets and thus make attackers use this to decrypt packets. In addition, the name chop came after the attacker chops the packet's byte from the end of the captured packet and modifies the checksum and sends the packet to the AP access point. Thus, attackers guess the packet is correct and the AP accepts the packet then the attackers proceed to guess the first part of the byte. And if the last part was incorrect then AP will discard the packet which will lead the attacker to proceed on a different guess.[10]

2.12.5.2 *Fluhrer, Mantin and Shamir (FMS) attack*:

Was a successful attack on WEP using the weaknesses of RC4 algorithm, the encrypted packets with the IV initialization vectors can be eavesdropped by the listening to the network packets, thus the attacker is easily able to recover the first byte of key stream since plaintext is encrypted. The attacker can easily know the initialization vector first three bytes of packet key that is transmitted unencrypted with packets. This makes the attacker gather a large amount of encrypted data and generate different possible values, enabling the attacker to recognize the correct key.

2.12.5.3 *Pyshkin, Tews and Weimann (PTW) attack*:

This attack appeared in 2007 and utilizes the analysis of RC4 stream cipher; this key was successful because it is independent of the key byte being attacked unlike FMS and Korek attack, it utilizes more bytes of the key stream and byte count depending on the length of IV and secret key. It broke the 104-bit WEP key. [10]

2.13 Wi-Fi Protected Access (WPA)

WPA was introduced in 2003 by the Wi-Fi (Wireless Fidelity) alliance to overcome the weaknesses of WEP, thus they cannot use WEP anymore. WPA provides enhancement security but the use of WPA is similar to WEP, and WPA obtains higher security with encryption and authentication. therefore the packets are secure and can't be intercepted as WEP[37] which address the WEP cryptographic problems.[10]

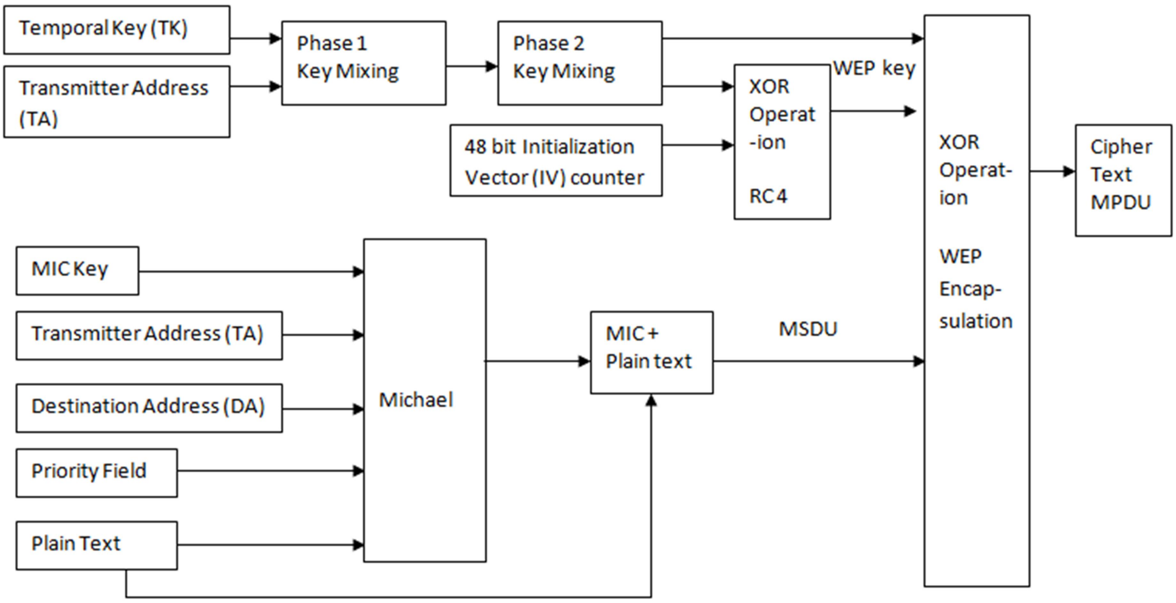
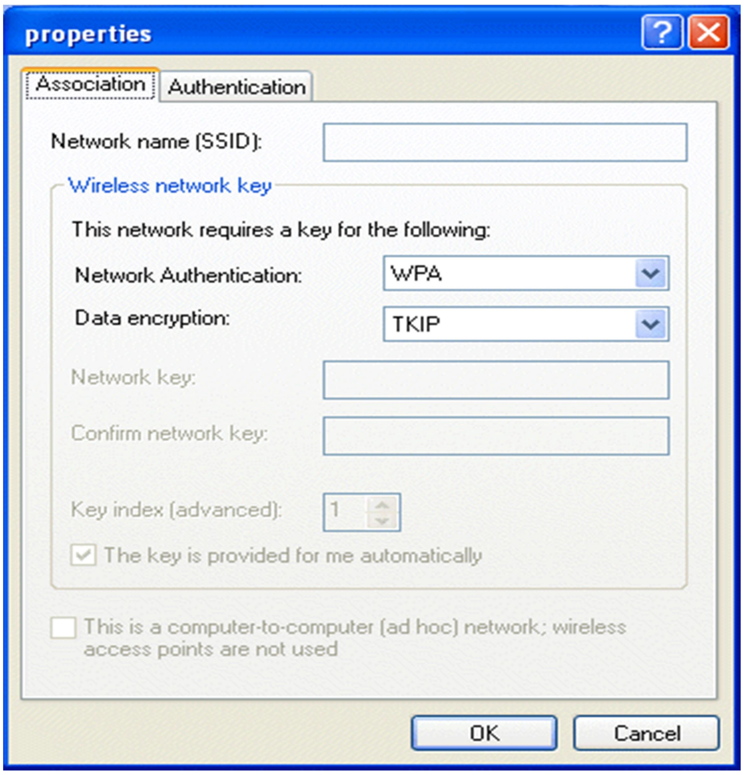


Figure 4 WPA -TKIP process

[10]



Network name (SSID):

Wireless network key

This network requires a key for the following:

Network Authentication: WPA

Data encryption: TKIP

Network key:

Confirm network key:

Key index (advanced): 1

☑ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Figure 5 WPA-TKIP installing to wireless security properties

WPA uses Temporal Key Integrity Protocol (TKIP) for encryption, and uses a 128 bit packet key and the Integrity is generated by Message Integrity Code (MIC) in algorithm called Michael[39] compared to CRC-32 in WEP. Moreover, the TKIP can provide replay protection. In authentication, it used two mechanisms:

- WPA-Personal or WPA-PSK (Pre-Shared Key):

This is used between two parties for initiating the communication, and the PMK (Pairwise Master Key) in TKIP must be in place. The WPA-personal is an authentication for personal use such as homes, for the authentication of 256-bit key never transmitted over air, when they hold 256-bit key before starting the communication.

- WPA-Enterprise:

Which is used for enterprise networks, IEEE 802.1x and Extensible Authentication Protocol (EAP) provide stronger authentication. Hence, Remote Authentication Dial in User Service (RADIUS) server is vital which delivers tremendous security for wireless networks.

The Extensible Authentication Protocol has different methods:

1. EAP-Lightweight
2. EAP-LEAP
3. EAP-Flexible Authentication
4. EAP-FAST
5. EAP-Message Digest 5 (MD5)
6. EAP- Transport Layer Protocol (TLS)
7. EAP- Tunnel Transport Layer Security (TTLS)
8. EAP- Subscriber Identity Module (SIM)
9. EAP infrastructures are: Peer, Authenticator and Authorization for Validates credentials.[10]

2.13.1 WPA drawbacks:

The flows allowed the intruder to cause DoS attack, if the attacker could bypass several layers of protection and WPA initializes its encryption scheme consequently make it easier to crack WPA.[40]

2.13.2 WPA Weaknesses:

WPA-PSK is based on the pairwise master key (PMK) that is derived from the concatenation pf the passphrase, SSID, length of the SSID and nonce, the algorithm of PMK= (password, SSID, SSID length, 4096, 256) the result is hashed 4,096 times to generate a 256-bit value combined with nonce values, by capturing the 4 ways handshake the data required to subject the passphrase into a dictionary attack. [40]

WPA uses old cryptography RC4 instead of superior Advance Encryption Standard (AES), which has become more vulnerable to attacks such as DoS attacks and liable to threats due to hash function of TKIP. To generate the Pairwise Master Key (PMK), passphrase and Service Set Identifier SSID which are fed into hash algorithm, the passphrase is leading only 2.5n +12 and n bytes of security strength hence to identify the PMK only Passphrase needs to be guessed which is vulnerable to dictionary attack and break-in to data. [10]

2.13.3 WPA attacks:

1. Chopchop Attack:

It allows the attacker to decrypt the last byte of the message of encrypted packet through emitting a message with 128 packets to the network. The attack exploits the weaknesses of the 4-byte CRC-32 checksum named integrity check value (ICV). As the checksum correct or incorrect, is checked by the AP to distinguish encrypted packets. If the packet is correct and the AP received, it from an unauthenticated client an error message will be generated. If the checksum gets incorrect message it will discard it. And the attacker will capture a packet for decryption to guess last byte and correct the checksum.[39]

2. Beck-Tews Attack:

Its purpose was to crack the WPA encryption in 2008 by Martin Beck and Erik Tews, the attacker must have a clue of IPv4 bytes there must also a rekeying interval for TKIP, the attacker first has to capture the traffic until the encrypted ARP (Address Resource Protocol) request or response is found. The 8 byte Michael MIC and the 4-byte ICV checksum form the last 12 bytes of the packet. Then the attacker decrypts the unknown plaintext.[39]

3. Ohigashi-Morii Attack (Beck-Tews + Man-in-the-Middle)

Is the upgrading of Beck- Tews attack on WPA-TKIP, for this attack a man in the middle attack is superposed to the Beck- Tews attack with tips to reduce the execution time of the attack.[45]

4. Michael Attacks:

The Michael algorithm is producing a hash of some plaintext, Beck and Tews found a reversing of the Michael algorithm, and this attack is based on the flaws in Michael. Beck found that if the internal of Michael reaches a certain point, the Michael algorithm resets. Then injection is enabled on some text in the packet, and add a string that resets the Michael algorithm, then the packet is modified while the Michael result remains correct [45].

5. The Hole196 Vulnerability

Found by Sohail Ahmad in 2010, this comes from page 196 of the standard paper about 802.11 where the hole is located in this protocol, the attacker is an authorized user, first sends an ARP request with MAC-address and IP address of the AP access point. The AP client will update their ARP tables, and send their packets to the MAC-address of the attacker. The attacker will receive the packets decrypted by the AP and re-encrypted with the current key to enable him to read it.[45]

6. Dictionary attack

WPA (PSK) a key-recovery attack as the key is a word from the dictionary, the handshake is the main flaw for the attacker, the hash key exchange with client and AP for connecting the eavesdropper can wait for hash to try finding the key with a dictionary attack.[45]

2.14 Wi-Fi Protected Access 2 (WPA2)

WPA uses old cryptography RC4 instead of superior Advance Encryption Standard (AES), which has become more vulnerable to attacks such as DoS attacks and liable to threats due to hash function of TKIP. To generate the Pairwise Master Key (PMK), passphrase and Service Set Identifier SSID which are fed into hash algorithm, the passphrase is leading only 2.5n +12 and n bytes of security strength hence to identify the PMK only Passphrase needs to be guessed which is vulnerable to dictionary attack and break-in to data. [10]

WPA2 was designed by Task Group I (TGi) and employs Counter Mode with CBC-MAC Protocol (CCMP) to encrypt network traffic, and CCMP employs Advance Encryption Standard (AES) for encryption algorithm.[40]

2.14.1 WPA2 Personal:

WPA2 Personal does not require an authentication server and performs between the client and the AP generating a 256-bit PSK from a plain text pass phrase where that PSK in conjunction with SSID and SSID length forms the mathematical basis for the PMK to be used in key generation. [36]

2.14.2 WPA2-Enterprise:

Used for a large number of users such as in Universities and corporations, WPA2 Personal with shared key for all participants in the wireless network is not feasible. Then WPA2 Enterprise authenticates users against a user database RADIUS. In the RADIUS server, it establishes an SSL/TLS tunnel to prevent third parties, in this tunnel an authentication protocol is used to supply username and password to the RADIUS server. The protocols are designed to authenticate the client against the server only not the opposite. [46]

WPA2 has become the de-facto standard for wireless equipment, any wireless hardware that doesn't meet the standard should be avoided[26]. When targeting these devices one single TKIP client allows an attacker to take down the complete wireless network, the behavior of the AP depends on the security such as WPA2, which is mainly for supporting encryption schemes. [47] The most important feature of WPA2 is the introduction of CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) which uses the Advanced Encryption Standard (AES) block cipher. CCMP was created to replace TKIP and WEP. CCMP currently provides the highest level of integrity, confidentiality and availability.[39]

The drawback for the shared key is not an easy way to administer the key; it may leak to intruders enabling them to access the wireless network.

2.14.3 WPA2 Attacks:

V. Kumkar, A. Tiwari, P. Tiwari have explained the WPA2 procedure attacks and they follow the Access Point attack steps till the security key shows successfully, when they first start monitoring the wireless interface, then start collecting the four ways authentication handshake, so they check whether the channel is 1, 6 or 11 and they locate this access point in channel 6. Then they use the command prompt which De-Authenticates the station from the access point finally applying the dictionary attack on capturing the encrypted IV.[40]

2.14.4 WPA2 weaknesses:

The vulnerability is the attack against PSK key, which is discovered in WPA as well PMK is a string of 256 bits or a passphrase 8 to 63 characters used to generate such as string PSK=PMK=PBKDF2 (password, SSID, SSID length, 4096, 256) where PBKDF2 is a method used in PKCS#5, 4096 is the number of hashes and 256 is the length of output. The PTK is derived from PMK, using the 4 way handshake and all information used to calculate its value is transmitted in plaintext. The 4 way handshake could be subjected to dictionary and brute force attacks.[36]

The WPA2 problems are prone to availability such as jamming and flooding control frames such as Request to Send (RTS) and Clear to Send (CTS) are prone to DoS attacks and management to report network topology are not encrypted thus enabling attackers to analyze the network traffic. Also GTK in WPA2 is shared among all authorized clients thus malicious authorized may inject spoofed GTK packets then authorized user can sniff other authorized user and decrypt their data or may install malware to compromise other user's devices. [10]

WPA2 Enterprise which is based on port-based 802.1x access control protocol is prone to attack and the de-authentication may lead to MAC address spoofing or sniffing out.[48]

2.15 Further Wireless Security:

There is further security that wireless networks need to secure their connections and the wireless network has two access levels that can be set-up for wireless networks, one network type is secured and the other is unsecured open access. The open access allows any device to access point to connect without security, while the secured network uses various security protocols with wireless features to provide wireless security, as we mentioned the main security protocols have been used since the wireless network began and have been used worldwide. Here are some of the further security protections in wireless network:

2.15.1 RADIUS Servers and Proxy servers:

The wireless network provides a connection through authentication server proxy server which is required for the user to have a username and a password to gain access to the internet[49] using RADIUS which is for authentication and encryption as it uses digital signatures to authenticate clients and permit them access to the Wi-Fi, as it sends encrypted bytes during the identification process in order to verify their identities, and the client will encrypt the response data using these received bytes, RADIUS uses digital certificates and encryption algorithm protocols such as EAP, MSCHAP and PEAP[50]

2.15.2 MAC (Media Access Control) addresses filtering:

The MAC address needs to set as enabled to enhance the wireless security, as wireless clients SSID and encryption keys can join the wireless network MAC address filtering additional checks. [49]

2.16 Summary

In this chapter we have explained some of the common wireless and mobile networks which serve as a media for transferring data to and from the users using the radio waves techniques, and these wireless networking technologies such as WPAN Wireless Personal Area Networks, Bluetooth, Ad Hoc, Infrared, Wireless mesh Network, Wireless Metropolitan Area Network, Wireless Wide Area Network and Wireless Local Area Network Wi-Fi which we are focusing on in this research. It has different standards and because the wireless network is the main important mechanism for transferring the information, in this case, the wireless networks are becoming more prone to attacks and vulnerable and the transferred data is in danger. Wi-Fi requires security to prevent various breaches, wireless network designed various security protocols and it became the most important role that is required to secure the connections and prevent fraudsters or hackers from accessing the wireless network using security protocols such as Wired Equivalent Privacy WEP, Wi-Fi Protection Access WPA, and Wi-Fi Protection Access 2 WPA2. Nevertheless, these security protocols are still not providing the full protection because hackers are still breaking them and we have mentioned the common issues for each protocol. This means security needs extra research to reach the point of robust protection that reflects the flaws and prevents third parties accessing the wireless network security.

Chapter 3

DNA encryption and decryption methods

3.1 Introduction:

On the biological level, the relationship between cryptography and molecular biology is irrelevant but the study of modern computing, biotechnology and DNA disciplines begin to work closely, DNA cryptography and information science was born after research in the field of DNA computing by Adleman. It is a new field and has come to the forefront of international research on cryptography. Many scholars from all over the world have carried out a large number of studies on DNA cryptography in terms of hiding information in DNA microdots[51].

In this chapter we introduce DNA cryptography from some DNA experimented methods that have been done around the globe and these methods have been tested for data protection and implemented with the network traffic security that has served to protect the data using the encryption and decryption technique of DNA cryptographic methods that test been proved by a few scholars and researchers. In this position we have considered to understand what DNA cryptography is and how this can benefit us in a security role that will hold data using DNA encryption and decryption methods, ways of protecting the most sensitive data and investigating the DNA methods to considerate the DNA cryptography field which can provide data safeguard that could be useful and reliable to offer it with Wi-Fi security protocol. The DNA security methods may show us to the future digital information security. Therefore, this chapter is illustrating the DNA methods that have been used to secure and protect the data.

Here we have explained briefly some of the nine DNA methods mentioned in this chapter and there are few more but this is what we focused on for the DNA experiments and how encoding and decoding data works, that it could provide security to information technology.

3.2 What is a DNA cryptography

DNA, Deoxyribonucleic Acid, is a molecule that encodes the genetic instructions used in the development of known living organisms and DNA is a nucleic acid; each nucleotide is composed of nitrogen containing nucleotides bases, which are Guanine (G), Adenine (A), Thymine (T), or Cytosine (C). DNA computing may not be fast but it is massively parallel, it has the potential to solve huge mathematical problems[52]. The DNA computing represents a serious threat[52] to various encryption schemes such as the data encryption standard DES, various groups have suggested with binary digits in computing using the sequence of nucleotides in DNA A for 00, C for 01, G for 10 and T for 11 in order to hide data well in DNA as steganography.

DNA cryptography is a newborn cryptography field, which has emerged in the research for DNA computing, in which DNA is used as a medium of information and modern biology technology is used as a tool for implementation. Moreover, the DNA is based on four letters in which the vast parallelism and extraordinary density of information inherent DNA molecules are explored for cryptographic purposes such as encryption, authentication, signature, etc. DNA newborn cryptography is far from mature in both theory and realization. However, research into DNA cryptography is still more on theory than in practice. The constraints of its high standards of high-tech laboratory and limits calculation, combined with means of work, intensive extrapolations prevent all DNA computing from being effective in today's world security and DNA is good because people are looking to encrypt their data when sending and receiving on the network and the researchers found that DNA is the most robust security tool and they implement it with lots of successful experiments and that's why it is good in security protection.

Adleman used the first pioneering study of DNA in computing, to solve a Hamiltonian path problem, and manifest a new era of DNA computing technology, using the DNA cryptography. This was then extended by Lipton to solve the NP-complete problem of satisfaction, computing of DNA use in parallel with capacity processing at the molecule to have born data structure and method of computing. There are attacks on computation before the challenges of information security as Boneh et al. proved a breaking to the data encryption standard (DES) using the tools of DNA computing.

Clelland found a research of DNA steganography to concealing data in a packet using the computing DNA encryption. In addition, the DNA is a new path for encryption and decryption and it is in initial stages to solve issues of data. Other DNA methods technology in basic investigation and trials focus on why there is not a general theory on the use of DNA in cryptography. [53]

3.3 DNA Encryption and Decryption methods (DNAEDM):

3.3.1 Method 1

There are many issues in amplifying the DNA sequences to encrypt data. Two pairs of primers chain reaction PCR, which is fast DNA process for encryption amplification that currently used in biology, the DNA, has a double strands and therefore need it to compliment the strands and the DNA for series of enzymes. The PCR is highly sensitive so that each molecule can be targeted to be amplified in 10 ∧ 6 after 20 cycle. It would be very hard to amplify the sequence of an encrypted without perceptive the best pairs of primer message. [54]

Advantages:

1- To reduce the coding redundancy of information and increase efficiency compared to traditional methods of encoding.

2- Using the technology of digital encoding DNA the conventional encryption method such as DES or RSA used to pre-treat the plaintext.

3- Digital coding DNA sequence for convenient mathematical operation and logical operation.

In this system, the message is based on the user text and converts the message in to hexadecimal and binary code. Message is divided into several parts, is used as an end of message is used as another key. Digital encoding DNA is applied to the message and the message with the message encoded DNA bases and PCR amplification are performed using two pairs of bases such that the key and the compression is performed for data of variable length.[54]

3.3.2 Method 2

Clelland conceived the microdots to develop an extension of this principle, then the following researchers used the DNA strands to hold secret messages, in a method the table of Clelland demonstrated the DNA coding of each character and number. Moreover, it is clear in the Clelland algorithm that it is a simple substitution cipher that encodes characters in sequences of DNA by using the following coding.

E: x→Y
xϵ {A, B, C,.Z, and 0,1,…9, "."",":";"}
Yϵ {xyz: x, y, z ϵ {A, C, G, T}

The encoding function} is corresponding D: Y→X.

Clelland et al. showed the two primers with synthesized DNA sequences, the process of this algorithm is clarifying the encoding of forward and the decoding reverse primer. These sequences are mixed up with dummy strands.

The Vital requirements are:

- Length= length of dummy strand DNA primers
- Message # copies of each dummy =# copy of the DNA message the receiver must know the decoding function and begins to decode message. The primers were used for polymerase chain reaction and in the final step of the DNA sequence to be amplified and sequenced decoded to enhance security you can use artificial components which are not random.[55]

Character=triple	Character=triple
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	

Table 1 Clelland DNA base coding

[55]

3.3.3 Method 3:

This method explains a different way but using the binary and these binaries are converted to DNA bases, Leier et al. used this way with binary digits of 0s and 1s encoded information into DNA sequences where the resulting DNA sequence was mixed with dummy strands and hence could only be detected and isolated if the primer sequence is known[56].

With result like $\{0_2|1_2\}_{e.}$ the start and end marker have primer sequences on one site for the polymerase chain reaction, it is very similar to the algorithm of Clelland et al.[55]

3.3.4 Methods 4:

Wong developed a steganography algorithm based on DNA, which is capable of storing data in the living organisms. The data are translated into a DNA sequence that is inserted into a vector. The insert sequence is flanked by two primer sequences, which do not exist in the genome. This vector is introduced into a cell of a living organism where it coexists and is replicated with the genomic DNA. To extract the data they used a polymerase chain reaction.

Wong used a substitution cipher like Clelland et al to encode a text of the song in a DNA sequence, and stored it in Deinococcus radiodurans for example ionizing radiation, so that the song text can be stored for hundreds of years.[55]

3.3.5 Method 5:

Arita et al developed a steganography algorithm based on the degenerative genetic code. Amino acid codes are redundant such that the translation of mRNA into proteins is a substitution cipher with the following characteristics.

- E: X→Y
- X$\epsilon\{xyz: x, y, z \epsilon$ {A, C, G, U}}
- Yϵ{A, C, D, E, F, G, H, I, J, K,L, M, N, P,Q, R, S, T, V, W, Y, stop}

However, the inverse function D: Y→X is not injective.

An example:

Threonine (T) =E(ACU) = E(ACC) = E(ACA) = E(ACG)

The triplet threonine is redundant in the third base to mutations and the third base does not influence the translation of the threonine and the translated protein. These mutations are called "synonymous substitutions" unlike "non-synonymous substitutions". Arita et al. translates each letter of the English alphabet in six codons. A value of 0 means to keep the original base at the third position of a codon, while a value of 1 means to change in the third base at that position. Arita et al. adds a parity bit for each letter, to keep it odd to detect possible error.

They encoded “KEIO“ into the *fts*Z gene of the Bacillus subtilis which is essential for cell division and demonstrated that as expected the changed codon sequences did not affect cell division, the colony morphology, growth rate and frequency of sporulation of these bacteria. To extract the encoded message one has to know the original sequence so that one can decide whether the codon is the original or the modified.[55]

3.3.6 Method 6:

This method has been issued by Guangzhao Cui, Limin Qin, Yafeng Wang and Xuncai Zhang and they proposed an encryption scheme using DNA synthesis, PCR amplification and DNA digital coding for preprocess to the plaintext and traditional theory of cryptography. To get different cipher text to prevent attack from PCR primers, as it used to be the difficult to amplify the message-encoded sequence without knowing the correct PCR two primer pairs, the PCR is fast DNA amplification. The PCR is a very sensitive method and a single target DNA molecule can be amplified to 10^6 after 20 cycles, thus can affect many DNA strands in a short period.

Here PCR primer 20-27 per nucleotides is high stability, and special function in PCR to have the correct primer pairs. When the intruder does not know the correct two primer pairs and captured the packet encoded in sequence by PCR amplification, he must choose two primer sequences from about 10^{23} kinds of sequences and it is difficult in a biological problem. The complementary rule that is proposed with this method of ~0=1 and ~1=0 is for DNA digital coding. Identical to the complementary rule of the nucleotides bases, the binary digital coding of DNA sequences prevails over character DNA coding to decrease the redundancy of the information coding and improve the coding compared to traditional DNA, and the DNA is very convenient for mathematical operation, DNA is able to do digital computing and adapt with existing computer processing.

Then this method is explaining the encryption key as the message sender designs a DNA sequence, which are 20-mer oligo nucleotides long as a forward primer for PCR amplification. The sender will translate the plaintext M into hexadecimal code by using the built-in computer code, then hexadecimal is translated into binary and into the binary cipher text C this is preprocess to get a completely different cipher text message to prevent attack from a possible word as PCR primers. This cipher text is converted to DNA sequence and put a number of dummies and each dummy has same structure as the secret message and generated it to send DNA mixture though channel and transmits it to intended receiver over a secure channel, as a secret message DNA sequence the message receiver also designs a DNA sequence which is

20-mer oligo nucleotides to reverse primer for PCR amplification and transmits it to the sender. Here encryption key$_A$ is issued that is a pair of PCR primers and public key$_e$, get the mixture DNA with dummies can be easily find the secret message as the receiver has a correct PCR two primer pairs through a secure way, then amplify the secrete message by perform PCR on DNA after this can retrieve the plaintext.[53]

3.3.7 Method 7

In this method, a steganography algorithm has been proposed by Amal Khalifa and Ahmed Atito to secure data using DNA play fair cipher for encryption and substitution to hide secret messages into DNA bases. The DNA sequence is desirable for hiding data for any medium[56].

3.3.8 Method8

The user's packets pass through the Wi-Fi traffic in a secured DNA channel for cipher text which encrypts the plain message or image in a kind of binary bases 00-A, 10-T, 01-C and 11-G [57] to demonstrate the conversion to binary, as in the images it need to scramble the pixel value to encrypt it in DNA bases, the image is converted into a binary matrix and then the binary are converting to DNA bases according to 00-A, 10-T, 01-C and 11-G, also the plain text of such characters input into corresponding DNA coded output based on code set. The plaintext is encoded into the ASCII code and then converted into binary value in terms of 0s and 1s now the input character equivalent DNA code of three bases nucleotides of DNA, as each character is 8 bits in length.[12] Figure 7 explains the data flow through Wi-Fi public channel converted in ASCII code then encrypted to DNA sequence.

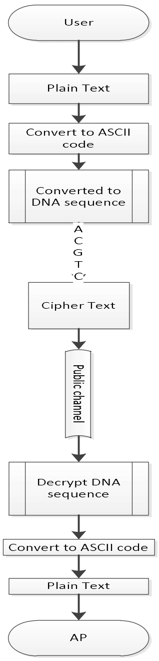


Figure 6 Encryption and Decryption through pubic channel

The figure above explains the encryption and decryption of the DNA in the Wi-Fi network for protecting the data flow within the Wi-Fi network, the encryption process starts with a message that contains characters to input it in the encryption system by encoding process to become as a cipher text and pass it to the public channel for encryption protection to prevent attackers reading the plaintext, and then start a new process which is the decryption system to convert the sequence of DNA into a binary and then ASCII to return in the output plain text.[1]

3.3.9 Method 9

In this method, DNA can be implemented in the hardware such as Wi-Fi network inside the AES security key, to encrypt and decrypt the message using DNA to generate the key for this purpose with AES making it difficult to break the encryption message. DNA uses double stranded molecules and the complementary DNA strands are held together to form a double helix structure. C. T. Celland, V. Risca and Bancroft C have demonstrated the way the process of hiding secret messages that were encoded among a multitude of random DNA, makes the message hard to break, without prior knowledge of the message, based on the primer key sequences. So when sending the message to the receiver end the original message using the primer key PCR to the DNA strands, the original message is obtained by knowing the two primers added at the beginning of the encryption. The PCR is a very sensitive method and can be amplified to 10^6 after 20 cycles; therefore, a lot of DNA can be amplified using PCR amplification to make the gate blocked towards the adversary to prevent access to the original message sequence. The binary codes are also used for encoding data; the ASCII (American Standard Code for Information Interchange) used a 7bit binary in order to represent certain text such as f letter 1100111 as a bit string and converting the text to ASCII value and then to corresponding binary code as shown below

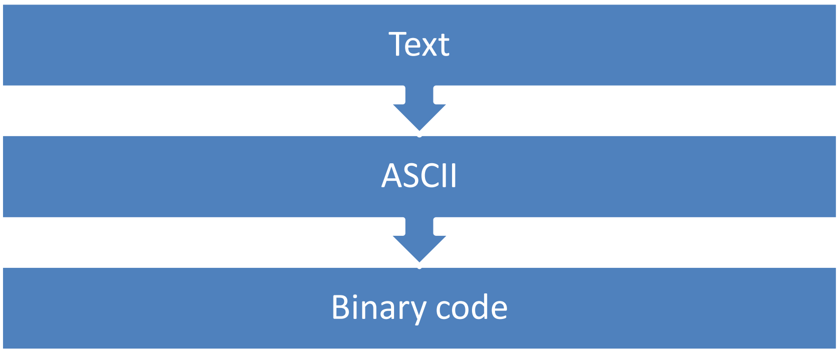


Figure 7 Converting the text and numbers to ASCII and Binary

The DNA encoding process inputting sequence which is in form text applied to DNA processing, the process converts the input text or number into corresponding DNA coded output using a secure communication channel then data coded in the ASCII form and next step enter to binary conversion which bases on 0's and 1's now the input have three characters of DNA bases each character has its unique DNA triple bases sequence as shown below

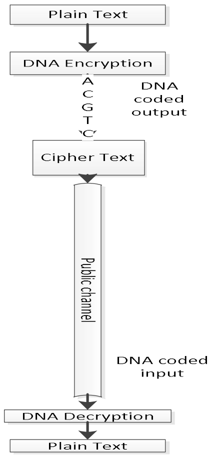


Figure 8 Data flow for DNA encoding and decoding

This shows the process of DNA encryption and decryption using the DNA coding as the initial process begins with character of the text and the input text is converted by encoding process where unique base triplet is assigned for characters and numerical this process is cipher text and this cipher is transmitted over a public channel to the decryption process by giving the cipher text as an input to the decryption process and turn the triplet DNA bases into equivalent character as a process of reverse encryption. Moreover, this process of encryption and decryption is keyed in to the AES algorithm with the WPA2 encryption and decryption process methods. This is input to AES for a new process to double the security of the Data messages[1]

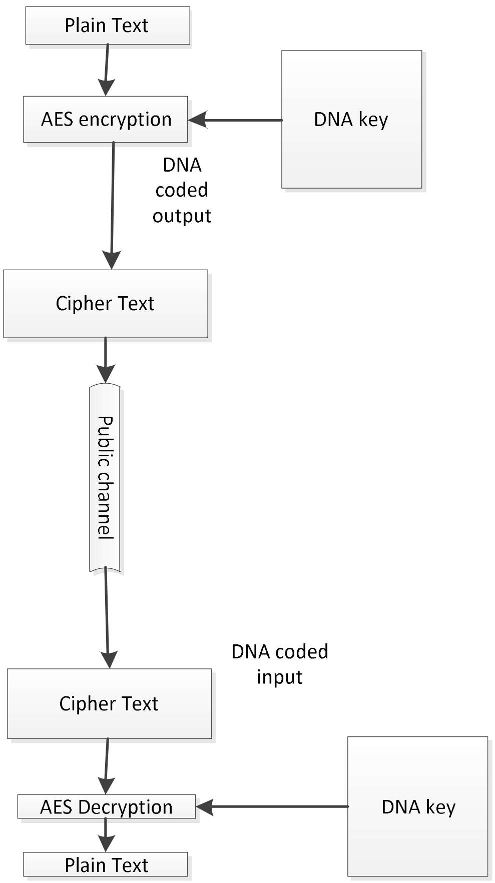


Figure 9 DNA key pass through AES security key

[1]

The text message to be sent is encrypted using AES encryption algorithm, the Advanced Encryption Standard AES is a standard for the encryption of electronic data which is asymmetric key algorithm meaning the same key is used for two processes encryption and decryption, and AES can be used 128, 192 and 256 bit. Since it is used for 128 bit, each character of the message produces 24 bits a total of 120 bits used for the message and the rest 8 bit for padding. The padding can be divided into 4 bits in as forward primer and 4 bits as a reverse primer then DNA is using 128 bit encrypted cipher. [1] This method is not implemented with the encryption security key and that’s why we use this in our research therefore they only encrypt the data flow to gain double security as they mentioned it in their article, and we take this to benefit from the double security of the data flow and use it with our encrypted DNA security key.

3.4 Summary

There are a lot of interesting results here as they are telling us their theory methods but these methods are needed to be clear in practice for data protection to find out what functions and tools that we could pick up from them in order to embed them and know how they are providing to data safeguard with their DNA input and output results in terms of security encryption and decryption.

We have focused on different methods of DNA encryption and decryption, that have been researched and also we have seen that in the DNA computing which represents these nucleotides in sequential bases of DNA computing using 0s and 1s, to hide (encrypt) data in these bases. And some of these methods are screening the extraction of the DNA sequences that processed with PCR for encoding the data and decoding using the reverse primer of PCR, the DNA security protection outcomes of different methods tested and executed to protect the data drive using a technical probe and given that encryption of DNA to the physical action to secure the information that is needed to be hidden from the intruders.

Chapter 4

Problem Analysis

4.1 Introduction

The things we have reviewed in the DNA field are very interesting but it is not clear how we can apply them to the practical environment and as was showed in the DNA methods we have considered and suggested different ways that DNA can be used for the determination of DNA-based security, for example we have looked to the different DNA security techniques that are used in cryptography. This chapter is explaining what are the problems that Wi-Fi is facing and the points that can be required to achieve the method of DNA mechanism to secure the user's Wi-Fi from hackers and put them outside the scope of Wi-Fi perimeter

4.2 Problem Analysis:

As the intruders are listening to the Wi-Fi communication between the legitimate user and the AP and use their internet service provider as their stepping-stone for all kinds of attacks and this problem can be traced back to the ISP and then the legitimate user through the IP address that is provided to both, while at the same time the attacker doesn't own that IP address. Therefore when the IT security expert's investigating the source of the attack, at the same time the intruder is free and impossible to get traced, this issue is concerning the Wi-Fi networks users around the world as the sniffers software are increasing every second and hackers have evolved these sniffers to provide them extra functions to attack to be adapted with the changes to the new intelligent techniques and to be visible to use by a variety of attackers around each Wi-Fi network and start eavesdropping the packets that legitimate users send or receive. A number of technical challenges are posed to address these issues, such as security breaching and attacks that appeared for the IT experts who find it hard to protect their own networks as well and even discover the intruders who accessed their networks.

The idea here needs to focus on and help to tackle and reduce these attacks using different experiments outside the existing Wi-Fi security protocols or which could be embedded into them if it could provide satisfactory security to monitor the Wi-Fi network connection access, and to address these challenges including preventing unauthorized users from using Wi-Fi network who pretended to be legitimate users by controlling your computers using some sniffer software which could enable a break-in to the Wi-Fi security protocol to steal sensitive information from your computers or jamming the Wi-Fi tunnel using DoS attacks to block the internet network.

The Wi-Fi security never ends with robust satisfactory security because intruders keep launching different attacks and the existing security protocols provide a good security for an initial time until the intruders discover the flaws to find out a gap to break-in. The result is that we feel our Wi-Fi can be attacked and the security key decoded at any time and because the Wi-Fi waves travel around 300 meters this makes the attacks start in probes of the Wi-Fi waves that travers and let the hackers trying to use the active scanning to probe and send a request to get a Wi-Fi AP responding and active scanning is like a ping system, also active scanning tool sends a probe to a target that triggers to tell AP to send a probe reply. It may probe a honey-pot to set a trap and detect or counteract attempts at unauthorized use of information systems. So active scanning in Wi-Fi signals tool could be sniffing by tuning to various radio channels of 1 or 6 or 11 which could decode Wi-Fi security access traffic through medium share as shown in the in the figure below of the medium share radio channels.

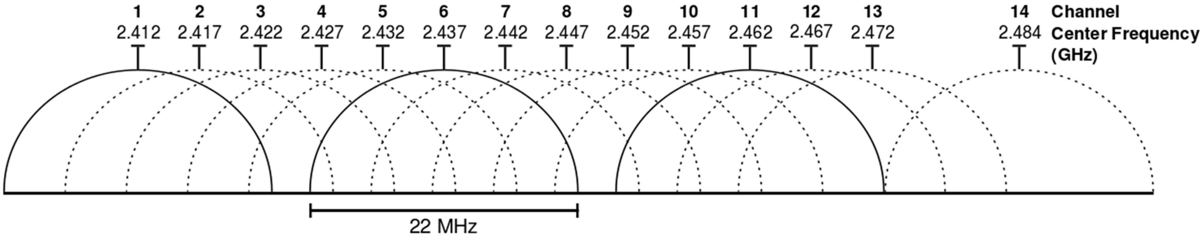


Figure 10 Wi-Fi Channels of 2.4 GHz

With the prevalence of Wi-Fi devices, more users are seeking ways to connect remotely to networks via the untrusted third party networks that provide Wi-Fi networks for users around the area to connect to the Internet. These untrusted networks could be accessed by anyone including intruders. The attacker gains access to the Wi-Fi network through rogue access by issuing an SSID to be the same as the SSID of a user having the same Wi-Fi network SSID name in the same area at the same time. This issue lets the legitimate user reveal their own security key on the third party's SSID, which lets the user give access to a third party Wi-Fi network and lets the intruders reveal the security key of the legitimate user to use their Wi-Fi network to pretend as a legitimate user and launch several attacks on the legitimate user who uses the same Wi-Fi network. It allows eavesdropping on all the packets that pass through the intruder's sniffing software, simplified the ways to disclose all the packets running through the Wi-Fi active scanning, and get what they are looking for such as the user's sensitive data like bank details and passwords for different website accounts like emails or company's staff username and password account.

4.3 Potential solution:

We propose the solution of the DNA Bio-inspired point of view for the purpose of encryption mechanism to secure and hide data based on DNA sequences of the user's login details in the Wi-Fi network to compare the registered data at both parties, the legitimate user device and the Wi-Fi router device. This DNA sequence consist of static data and dynamic data is future work to add with static because including dynamic elements this help the legitimate user have a new security key on each access and this keeps updating the sequence key with increasing the confusing for the reconnaissance of the attackers who attempting to capture the packet, here DNA bases provide a potential solution with dynamic data to update the key and advance an authentication access for only the legitimate users.

The purpose of this is to increase the complexity of the security key DNA sequences and to use the DNA sequences as an encrypted security key. The regular changes to DNA sequences are making it hard for the intruders to discover the DNA security key because the dynamic data are the best to automatically change regularly.

4.4 Requirements:

The requirements for this system are:

- Software that is converting the user's details to a DNA format automatically in a coding conversion to DNA sequences
- Database to store the user details
- Frames of the software such as NetBeans program to prove each user's data has been converted to DNA format bases in terms of encryption characters A, C, G and T
- DNA based generator used algorithms to use it for matching sequence
- Based on the DNA methods encryption and decryption for confidentiality of data in the public domain of Wi-Fi the data flow applying encoded text to public channel cipher text to be meaningless to a third party.

The DNA sequence objective of the user interface is to encrypt the data input to the system for a control access and decrypts it to match or mismatch comparison to permit access or deny access for the process of access control. After this initial stage and the comparison stage has been implemented for a future work this process will use a like security key in DNA Sequence format that automatically converted, to produce a DNA secret key access encrypted with DNA sequence and this is the DNA security.

4.4.1 In potential solution we need two steps

4.4.1.1 The Authentication:

In this step which is the target suggestion that future work will be on which is to input the user's data in the database then from there the system will convert the plaintext of the user's details to a DNA format then we can get a DNA sequence format by the software automatically, and combining these DNA sequences in a rank to store them at both parties user device and Wi-Fi device to match the sequence to comply with the DNA accessing control like the existing security protocols. This DNA sequence rank is becoming a Wi-Fi security key. Moreover, these DNA sequences will have a dynamic DNA sequence that is renewing the security key and making the intruders confused all the time when they need to access, because if they capture the packet the system will change the sequence using the dynamic DNA sequence and make it hard to guess the new key. The Wi-Fi party will keep these in its security key place inside the device that it needs to be secured and the user's device will do the same purpose to store this DNA base as a security key. The Authentication is an order to confirm the truth of an attribute of a single data of the entity in the database, in contrast to identification and the process of actually confirming the identity of the Wi-Fi user. Its purpose is to confirm the identity of the user accessing by comparing their DNA sequence in the portable device or any other device with the DNA sequence stored at the Wi-Fi network to validate the user identity access and ensuring these DNA sequences are matched or mismatched.

If it is matched then the identification for the access is truthful and authenticated and gain access to the Wi-Fi device, otherwise the DNA is mismatched which cause a zero binary and this 0 means off which means the authentication is untruthful and result is denied access to the Wi-Fi network. It also means the authentication is comparing the DNA sequence of the user's data itself on the user device, to the known DNA sequence in the Wi-Fi network, which is the original DNA sequence security key as a signature that compares, and they both have to be exactly the same. Here the DNA is in a chain management of security authentication to read through the process of security for connecting both parties, user devices and the Wi-Fi devices too and bonds them when they recognize each other. This can offer a solution that can be much more difficult to counterfeit and at the same time is easy to verify.

4.4.1.2 Data flow encryption and decryption:

For the data flow here DNA is being used because of its vast parallelism and the amount of data which can be processed in DNA, which results in the cryptography of DNA purposes such as encryption and decryption using various DNA encryption and decryption with PCR that has been used and tested in some of the DNA methods, for authentication, and signature. Here we will use DNA encryption and decryption for the purpose of data flow in the Wi-Fi network which is for processing secure images and texts that a user needs to receive or send through the Wi-Fi DNA encryption to secure them through the public channel, in order to provide integrity and confidentiality for the Wi-Fi network security in both ways of security sending and receiving the data flow in DNA encryption and decryption which hides the users data in DNA bases to encrypt and decrypt the message. In this data flow, public channel security we can use the AES with this system to process the dataflow encryption and decryption and then it will become more secure as it will serve the data protection that serves with WPA and WPA2, therefore this is the future work with AES.

This process is consists of:

4.4.1.3 ASCII conversion:

The encoding scheme for characters of upper case and lower case, numbers and the punctuation symbols, the ASCII was developed to represent text in computer and communication equipment as the encodes of text based on ASCII. ASCII uses short descriptive phrases for each character. ASCII uses 8 bit binary code to represent a certain text and other characters, the binary code is used to convert the characters or symbols to equivalent ASCII value and then into corresponding binary code.

4.4.1.4 DNA bases Encryption process:

The DNA comes after converting the ASCII code to binary codes then the binary codes will be encoded to DNA bases that represent characters or numbers that are applied to the DNA process. This process converts the input data such as characters or numbers into the DNA bases output as encryption for a secure public connection channel. The whole process of DNA encryption is coded in the ASCII, this will be converted into binary value to gets its encoding of the DNA characters 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 in the coding solution in chapter of solution. This is the process of DNA sequence encryption with the data flow that is aimed to secure the Wi-Fi network data through the public channel, where the DNA coding triplet is representing each number or character to become as a cipher text when travelling through the Wi-Fi public tunnel.

4.4.1.5 DNA bases Decryption process:

After completing the process of functions that is passing in encryption from plain text in to cipher text and travel through the Wi-Fi public channel, it is intended to secure the plain text from intruders and make it complex to break the DNA coding.

A new process begins on the other side of the party to decrypt what is sent to the receiver by giving the cipher text as an input to the other party for decryption to start to convert the triplet DNA code in to the equivalent binary and then to ASCII code then reverse back to the original text.

4.5 Methodology:

In this research we have used the DNA methods in authentication as the current DNA research is available for encryption and decryption only, and other data flow processes which has been implemented using DNA computing which the DNA computing was first discovered by Friedrich Miescher and James[1] and Adleman was first introduced and demonstrate DNA computing used to solve a directed Hamiltonian path problem[58].

Sensitive information must be protected against unauthorized access; here we propose a new biometrics DNA authentication system that is based on biometric DNA security to secure the Wi-Fi access as the common use of biometric measuring and analyzing a person's unique DNA sequence. Here we will use the DNA sequence of the user's details that is converted automatically to DNA sequence format with the static and dynamic user data as a security behavior to measure the user's DNA key whether it matched or not, and to recognize whether it is the legitimate user or intruder by counting the number of times of wrong DNA sequence to the Wi-Fi for accessing and this behavior will provide the confidentiality and integrity to the legitimate user who accesses with the same DNA sequence to the Wi-Fi gate access. DNA matching behavior biometrics is generally used for authentication while the Wi-Fi physical biometrics can be used for either identification to determine the ingress user or authentication. Therefore, the DNA information enhances the accuracy in authentication enabling the development of DNA based user identification. DNA cryptography is a new field computation and new technology like PCR Polymerase Chain Reaction, which has the high-level computational ability and is capable of storing huge data. The cryptography process can make use of different methods in the one-time-pads OTP which is one of the most efficient security algorithms, while a method based on the DNA splicing technique is detailed in the case of the one-time pad algorithms the plain text is combined with a secret random key or pad which is used only once the pad is combined with the plaintext or an XOR operation. [59]

4.5.1 DNA Security method:

4.5.2 DNA Security Key

The user data that is inserted into the database table can be used for Wi-Fi access Security key for identification of the user who is accessing the Wi-Fi network, and this DNA key should be compared to the key stored at the Wi-Fi device as a representative access of the Wi-Fi network, the AP can recognize the device through matching the DNA key in the database table at the Wi-Fi with the DNA key of the user device for authentication and this key can be added to multiple devices, therefore this DNA Security key is mandatory to admit the legitimate users only.

4.6 Summary:

In the problem analysis we have discussed the issues of the Wi-Fi attacks and how the intruders are exploiting the Wi-Fi connection for their ways to attack, and what are the flaws that allows them to access their targets, here the Wi-Fi has huge challenges towards the Wi-Fi security while the intruders have gained more experience in terms of decoding the security of the packets or the security key using their own sniffer software through scanning the Wi-Fi signals through tuning the channel 1, 6 or 11 as it allows the attacker to bridge on them to gain access using the SSID that is broadcasting the name of the Wi-Fi network. And in the solution for these problems we have picked up the DNA bio-inspired security to change the security key for the Wi-Fi network using the DNA sequences as a security key solution whose purpose is to hide the user's data and convert it to DNA sequence and we have shown the functions of authentication of the users access control for identifying the legitimate user's and they can gain access after their trusted identity and comparing decision of the DNA sequences against the database and the key at the user device with the Wi-Fi network device to match the DNA sequence security key.

The DNA is aimed to secure the Wi-Fi network through the public channel and to use the DNA sequence for control access to the Wi-Fi network as well to the legitimate users only using the DNA sequence as a security key and because the current security protocols use a short security key to access, therefore here we use the DNA because it has a long sequence and hard for the intruders to guess the triplet DNA key.

Chapter 5

The proposed DNA Security Protocol for Wi-Fi system

5.1 Introduction

In this research, we present the DNA sequence computation to the technology of Wi-Fi security protocol in order to propose a new security method for Wi-Fi network access, to manage the users accessing the Wi-Fi network connection independently, instead of sharing a Wi-Fi security key. Currently Wi-Fi security is sharing the same security key with all users on the same Wi-Fi that could allow these users who are accessing the same Wi-Fi network connection to eavesdrop on the packets with a view to stealing sensitive data from other users or to eavesdropping the staff activities of the organization when sharing the same security key.

In this chapter we proposed frameworks for encrypting and decrypting the strings into a DNA security key for each user, the encryption is converting the user's data input to a DNA sequence to store it in the database, because the database will held several user's keys and create an isolated DNA security key for each user to get independent Wi-Fi connection to the internet which is comparable to the server that controlling access of the users to the system when the user access the Wi-Fi network using their own encrypted DNA security key the process have to compare their key stored in the database with the key they provide to access the Access Point (AP) and this compare will check the similarity of access if it matched then it will equal to 1 in binary and grant a successful connection otherwise it will equal to 0 zero and grant a disconnect to the Wi-Fi.

There for we have testing the implementation and it gives us the result that we accomplished such as encrypting the user's data and compare it when the user require to access to the Wi-Fi as we have developed two interfaces both are acting as a user and a Wi-Fi device and the Wi-Fi is holding a database and in the database is the encrypted data of the users.

This chapter includes the implementation and the algorithm that processes the matching of the access control to the Wi-Fi interface and this act as a Wi-Fi device is performing as an Admin to control the users and manage their encrypted DNA keys and controlling access to the Wi-Fi, in this section we go in details and illustrating the conversion of each user's data to the Admin to process and substitution the encryption of the plain user's data and encrypting it to the DNA sequence format and translate it into DNA sequence and then store it in the database which finally becomes as a security key for match or mismatch, and this user's security key is static data and it needs to add the dynamic security key to enhance the security for the access control and prevent the hackers to use the key again because with the dynamic DNA sequence data will get updated routinely on each access.

In chapter 4 we have explained the problems with the existing Wi-Fi security key due to eavesdropping, sniffing and cracking the security key using modern sniffer techniques, thus here we recommended basic solution with static data merely to this using a complicated security key with the DNA encryption, to encrypt the user's security key to a DNA sequence meaning each user has its own DNA security key to access, this means the key is not shared with other users. In addition, this key has two prime keys that are known only to the legitimate user and these prime keys can be set to a triple or quadruple sequence for each string or number to make it hard to guess by the hackers.

5.2 DNA solution and recommendation

In this intellectual project the DNA Bio-inspired are not determined to use the real biological DNA for this process, it is only the idea come from the DNA of biology and how each biology has its own unique DNA in real life.

DNA implementation is tested successfully using the Java program and the result we have got is encrypting the data string to a DNA sequences, this means that the project still need a future evolvements such as adding the dynamic data to the process to make a primer keys even more difficult to break into, the system this will propose a new self-updated security key for each user, or if they used the static data then each user will have a static security key encrypted in DNA sequence and could be not secure if it revealed to hackers or eavesdropper and on this case the user needs to update his DNA security key by changing the static data into a new static data and get a new security key in the database.

Here we recommend to evolve this project by adding the dynamic sequence and the process with renewal the keys on behalf of the user and then he/she will be relaxed and not worried about their own assets through the Wi-Fi or any other purposes that could be used for maybe a server to control the users or clients.

Here we think in this chapter we are trying to solve some of the design frame work that goes some way towards the problem of the security key because the current security keys are easy to break into, and they use only one shared security key for all the users to access the Wi-

Fi and using DNA sequence in Wi-Fi security key makes it harder to guess or sniff for the intruders, when using the DNA encrypted static and dynamic data to the Wi-Fi.

Here we have designed a few frames for the static data only because the dynamic data is needed to be considering for holding a graded data at both user device and Wi-Fi device in order to get the same dynamic sequence when updating the security key.

5.3 Used Technology of DNA Process access and conversion

The Java cryptography architecture JSE platform use the JDK 1.8 and 8.1 version of the java, this java software refers to the package that supply a concrete implementation of classes ending with .java and methods that is starting with public static for encryption to DNA bases and another method for decryption from DNA to plain text in the admin class interface using functionality of the cryptographic algorithm by declaring the variables of the key generation of the DNA bases and then convert to ASCII numbers char character = inputString.charAt(i);. then convert it to 8 bits binary numbers String.valueOf(Integer.toBinaryString(0x100 +inputAscii[i]) and then convert these binary bits to the DNA letters according to the values of each letter A=00, C=01, G=10 and T=11.

```
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 = "C";
                f = f + B;
                jTextArea1.append(B);
        } else if (d1 == 1 && d2 == 0) {
                C = "G";

                f = f + C;

                jTextArea1.append(C);

        } else if (d1 == 1 && d2 == 1) {

                D = "T";

                f = f + D;

      jTextArea1.append(D);
```

In addition, when this process complete then the interface is connected to the database to store the DNA bases String URL = "jdbc:derby://localhost:1527/security-access"; and the process of the admin interface is discussed in details in this chapter with the capturing of the user input data to produce the output encryption of the DNA. With using, the symmetric cryptographic encryption and the key primers should be the same with the admin and the user and only known for both interfaces for the purpose of matching the security key.

Here in this diagram illustrating the generating data of the admin class in the package of the java and ending this with the translating of the generating the key to DNA bases as shown in the admin class and the user class below.

The admin diagram can test the authentication of the key for each user at this time is very important to know the length of the key must be exactly the same as the length of the user data input and it won’t accept it as a key if it exceeding the key length. The plain text is the secret plain data stored in the database after the substitution to DNA bases. The admin have the privileges to authenticate the registered users and examine whether the new user exists or no for the control access management.

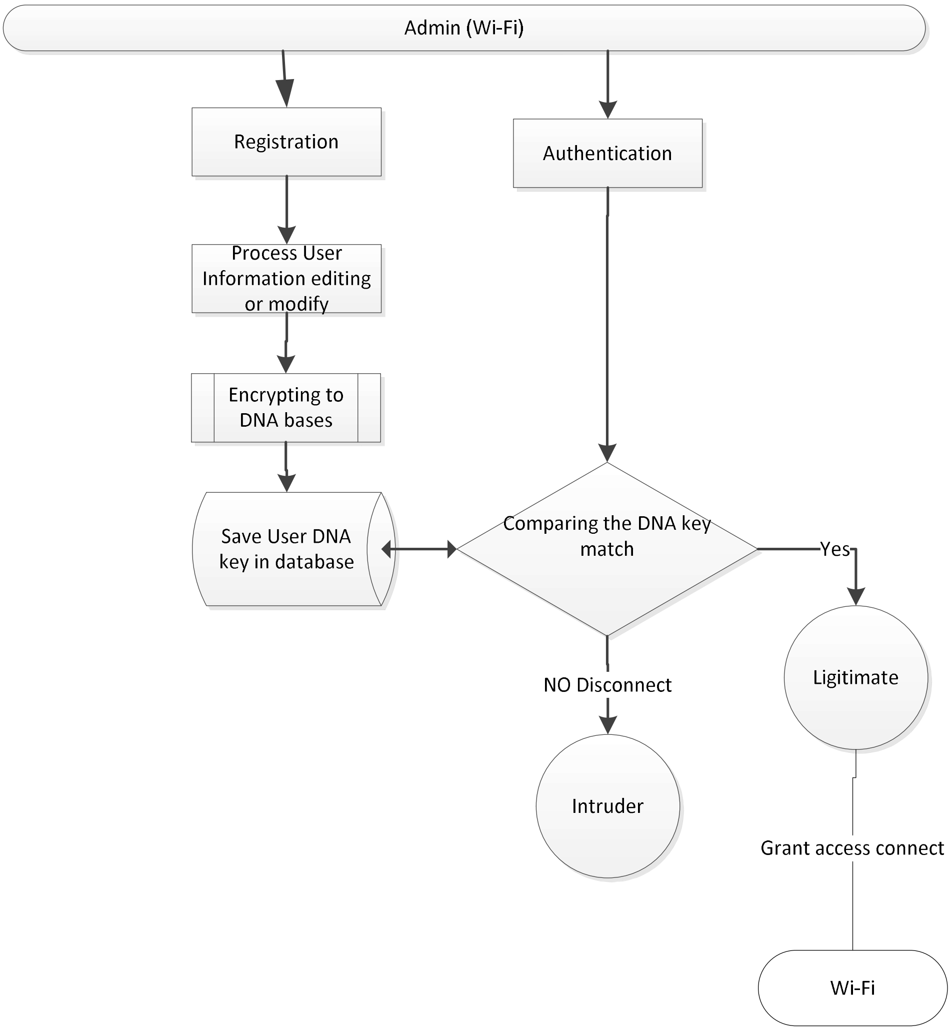


Figure 11 Admin DNA process

On the users interface is symmetric DNA algorithm developed the nucleotide keys should the same with the admin (Wi-Fi) keys therefore executed in the user adjacent with the Polymerase Chain Reaction (PCR) of the DNA and the keys of the hidden data in the DNA bases ought to be the same with the admin process java class algorithm.

Clients or users do not have the privilege comparable with admin, since the admin have, the privilege of the entire controls such as modifies and updates the security keys, the purpose intended for this, merely the admin or a legitimate user for the purpose of security amendment access management must access each Wi-Fi. The user boundary just have to insert plain data then the system encrypt it to DNA sequence using the symmetric cryptography with secret keys and the output is the DNA sequence as should be the matching with the DNA sequence stored in the database by the admin otherwise it won't be able to connect to the Wi-Fi and this resulting to a disconnection.

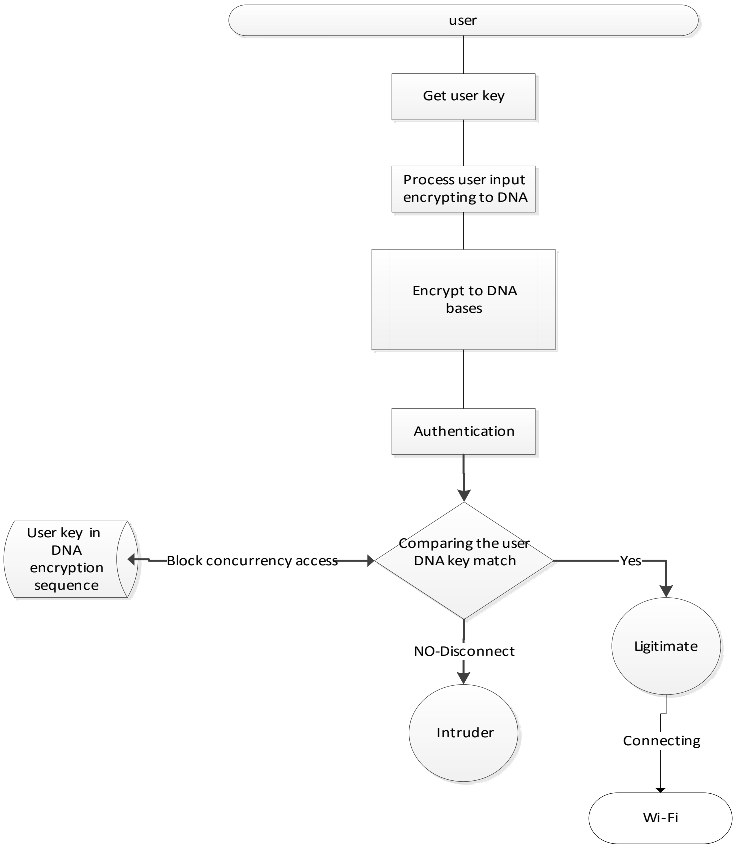


Figure 12 User access process

In the domain of the DNA encryption security the symmetric algorithm cryptographic should be the same with encryption and decryption and consists in processing user plain data applying to a cipher with ASCII then binary and with the DNA nucleotides each of them has its own binary value such as A[00], C[01], G[10] and T[11]. Moreover, produce the encryption output of DNA sequences like AGAAGGTCCA meaningless to the hackers who does not know the key of the nucleated of the triplet DNA sequences.

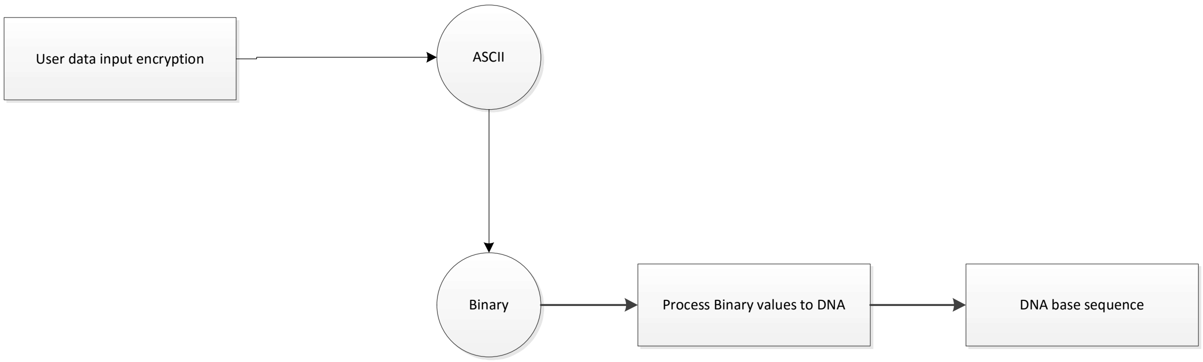


Figure 13 Encryption process to DNA bases

Character=triple	Character=triple
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 14 Substitution alphabet

The decryption process is determined by the key from the encryption DNA sequences to binary then find the values of the binaries of 1s and 0s to the ASCII which then produce the output of the original plain data of the user. In the decryption process is to recognize what the user data has been saved in the access control list. In addition, the key with the decryption is symmetric this is to be known only with the user process and the admin process, and if the key changed in the admin then it should be change to same key with the user.

The decryption method side removes the padding and restores the original user plain data length.

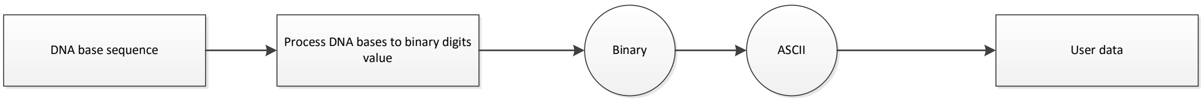


Figure 15 Decryption Process

5.4 DNA Sequence encryption key

The Wi-Fi security protocol may require the DNA bases to secure the Wi-Fi access control processing using the DNA match or mismatch sequence to monitoring the users who are eligible to access the Wi-Fi network and those who are not allowed to access the Wi-Fi router by comparing their DNA sequences (security key) that is encrypted from static data to DNA sequences compared with the access list of the Wi-Fi eligible users.

The DNA frames we created in this chapter convert the user data to DNA and then store it in the database. This conversion to DNA sequence is the core accomplishment and succeeded in forming an encryption using the bases of the DNA code of the first letters such as a derived from Adenine, C from Cytosine, G from Guanine and T from Thymine and they are called DNA nucleotides.

These nucleotide letters encrypt any letter or number, and this process is converting to these DNA sequences letters using the binary digits of 0s and 1s as the binary bases 00-A, 10-T, 01-C and 11-G therefore each symbol or alphabet or number has its own value in the binary digits of the ASCII, then the plain data is converted to binary that is encoded into the ASCII code binary value in terms of 0s and 1s which results as the input characters or numbers are equivalent DNA encrypted code of three bases nucleotides of DNA, as each character is 8 bits in length binary and this binaries are converted to DNA bases,.

ASCII table

Char	Binary	Small Char	Binary	number	Binary
A	1000001	a	1100001	0	0000
B	1000010	b	1100010	1	1
C	1000011	c	1100011	2	10
D	10000100	d	1100100	3	11
E	1000101	e	1100101	4	100
F	1000110	f	1100110	5	101
G	1000111	g	1100111	6	110
H	1001000	h	1101000	7	111
I	1001001	i	1101001	8	1000
J	1001010	j	1101010	9	1001
K	1001011	k	1101011	10	
L	1001100	l	1101100		
M	1001101	m	1101101		
N	1001110	n	1101110		
O	1001111	n	1101111		
P	1010000	p	1110000		
Q	1010001	q	1110001		
R	10100100	r	1110010		
S	1010011	s	1110011		
T	1010100	t	1110100		
U	1010101	u	1110101		
V	1010110	v	1110110		

W	1010111	w	1110111		
X	1011000	x	1111000		
Y	1011001	y	1111001		
Z	1011010	z	1111010		

Figure 16 ASCII table for characters and numbers

The DNA encoded process in the implementation frame converts the input text or number in the Admin frame using the two-primer keys process to create the Polymerase Chain Reaction PCR into a corresponding DNA coded sequence to acquire a secure encrypted key of the user's data provided, and this key is the DNA sequence format.

The DNA sequence seems to belong here in this process we use the process; Polymerase chain reaction PCR that is fast DNA process for encryption compression, and the DNA has double strands and therefore to complement the strands, the PCR is highly sensitive. The primers were used for polymerase chain reaction and in the final step of the DNA sequence to be amplified and sequenced to enhance security.

In the Wi-Fi users data flow needs to be highly secured, with this project we can use the method of processing the encryption and decryption of the user data and here is some explanation of the process of the data flow such as text and images in the Wi-Fi traffic. In this method, DNA can be implemented in the hardware such as Wi-Fi network, to encrypt and decrypt the message using DNA to generate a key for this purpose with AES making it difficult to break the encryption message. DNA uses double stranded molecules and the complementary DNA strands are held together to form a double helix structure. Celland, Risca and Bancroft have demonstrated the way the process of hiding secret messages that were encoded among a multitude of random DNA which make the message hard to discover based on the primer key sequences. So when sending the message to the receiver end, the original message using the primer key PCR to the DNA strands, the original message is obtained by knowing the two primers added at the beginning of the encryption. The PCR is a very sensitive method that can be amplified to $10^{\wedge}6$ after 20 cycles; therefore, a lot of DNA can be amplified using PCR amplification to make the gate blocked towards the adversary to prevent access to the original message sequence. The binary codes are also used for encoding data, the ASCII (American Standard Code for Information Interchange) as shown in the table above used 8bit binary in order to represent certain text as a bit string and converting the text to ASCII value and then to corresponding binary code.

The DNA encoding process inputting sequence which is in form of text applied to DNA processing, the process converts the input text or number into corresponding DNA coded output using a secure process of the primer keys then data coded in the ASCII form and next step enter get the ASCII binary and then convert the binary which based on 0's and 1's to a corresponding DNA bases character which is set the input has three characters of DNA bases each character or number from the binaries and forming to its unique DNA triple bases sequence.

The process of DNA encryption and decryption using the DNA coding as the initial process begins with character of the text and the input text is converted by the encoding process where the unique base triplet is assigned for characters and numbers this process is called cipher text because it encrypt the strings or integers to DNA sequences and this cipher is transmitted over a public channel to the decryption process by giving the cipher text as an input to the decryption process and turning the triplet DNA bases into equivalent character as a process of reverse encryption. This is input into Admin frame get a new security encryption process to secure of the Data[1]

The user data is encrypted using primer keys for conversion using encryption algorithm, the encryption here we used is asymmetric key algorithm meaning the same key is used for two processes encryption and decryption.

5.1 DNA parameter sequences

$$x_i=x_j$$

x is the DNA nucleotides and i, j are the length of the DNA sequence. Moreover, x is the vital comparison between the two devices, which the x sequence in the user device should match the x sequence at the Wi-Fi router and the comparison process comparing to score the degree of each sequence to match or mismatch as shown below:

$$\sigma(x_i,x_j)$$

$x_i=x_j \rightarrow$ match then legitimate user

$x_i \neq x_j \rightarrow$mismatch intruder

$\sigma(x_i,x_j)$	score
$x_i=x_j$	1
$x_i \neq x_j$	0

Table 2 Scoring of DNA Matching result

The binary of 0s and 1s are the function for on and off if the $x_i=x_j$ then the DNA sequences are matched and if score 1 means on then grant a connection access to the Wi-Fi, if the $x_i \neq x_j$ score 0 which means as off and deny connection to intruder.

5.2 Matching DNA sequence connection and Key matching

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

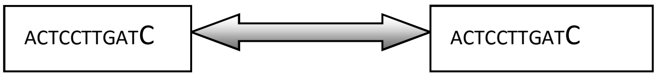


Figure 17 DNA sequence key for matching the security key between the two parties

5.3 Secure DNA public channel

The vast parallelism and extraordinary information density inherent in DNA are explored for cryptography purposes such as encryption, authentication, and signature. The DNA keys we use here is Polymerase Chain Reaction (PCR) for using two primer pairs the keys are *Kx* and *Ky*, the keys should be known to secure the public channel. We use XOR to secure the channel of normalized binaries by gaining high compression factor and plaintext bytes are bit-wise XOR with the output bytes to produce cipher text.

The used keys for security channel are the XOR for compression factor as the XOR operation with sufficiently long keys sequences between two parties such as a Wi-Fi router and a user device exchanging messages over the Wi-Fi channel not the internet, exchanging messages using XOR as the two parties use long sequences with enough entropy would protect the messages against third parties, and PCR which uses the two prime keys for complexity break in to connection keys. The kx_i and kx_j are the DNA sequences keys for the user and Wi-Fi device. The key security will have the same sequences at the user device is *xi* and the Wi-Fi device is x_j, while *ky* key is for the data flow encryption

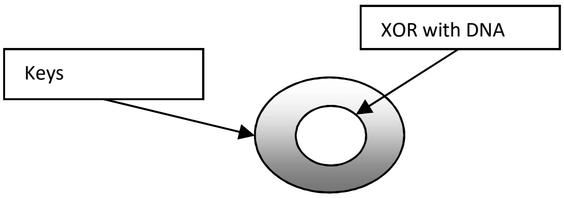


Figure 18 Security channel with PCR keys and XOR

XOR will use the k to be performed and XOR combining the correct key as the key is given by user which is his profile stored to convert it into DNA sequence, the key which is used will be a private key which will be generated to DNA bases and passed to the router through the secured channel to compare it with the other similar private key which is stored at the Wi-Fi router as observed sequence. In case the DNA layer can be broken then another two layers are 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 of the DNA encryption and decryption methods for a double 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 codon for leads to secure the public channel and using our two PCR keys will be more difficult to break.

Following is the implementation effort discussion consists of the following components:

5.4 Database

User information is stored in a database created within the system, which includes static DNA sequences for all the users. In this database, we have chosen to design static DNA encrypted data so the intruder cannot guess what the user's static DNA on the access process is when converted to the DNA sequence key. The access key will be compared to the existing records within the database to compare the degree of the DNA sequence with the observed sequence in the Wi-Fi router for a decision whether to grant access or block.

In the next figure is the opening pace to connect to the database where the user’s keys are kept subsequently encoded each user’s static data and encrypt it to DNA sequences, at this time the database correspondingly is secured and encrypted using the right of entry control such as the username and the password, this is administratively controlled and edited by the admin user in mandate to control all the users accessed to the wireless router.

5.5 Database security

Database encryption in Java as we used JDBC driver and to add the extra advanced security to protect the database connection, here the JDBC driver used external authentication if you are trying to connect to the database. You can use the SSL authentication to connect to the database. The Java secure socket extension provides a framework and an implementation for a java version of the SSL that the JSSE support the data encryption between server and client authentication, and message integrity. It abstracts the complex security algorithms and handshaking mechanisms and simplifies application development by providing a building block of application developers.

In addition, the code for SSL is:

```
Import java.sql.*;
Import java.util.Properties;
Public class nameof class{
Public static void main(String[] args) throws Exception{
String url = “jdbc:derby://localhost:1527/security-access”;
+”(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=LOCALHOST)(PORT=1527))”
+”(connect_data=(service_name=security-access)))”;
Driver driver = new org.apache.derby.jdbc.ClientDriver();
Properties props = new Properties();
Connection conn = driver.connect(url, props);
Conn.close();
}
}
```

JDBC thin driver support for database advanced security as the classes are included in the ojdbc5.jar and ojdbc6.jar files, the security parameters for encryption and integrity usually set in sqlnet.ora, set using a java Properties object or through system properties. In addition, the database support for Login Authentication.

Basic login authentication through JDBC consists of user names and passwords, as with any other means of logging in to the database; specify the username and password through a java properties object or directly through the getConnection method call. This JDBC thin driver implements a challenge response protocol to authenticate the user.

Additional to the database is SSL security connection to JDBC driver in Properties to set parameters for the object in opening connection between the client and the database access. In addition, oracle database has multiple ways to authenticate to the database, with those methods come multiple risks if authentication is not handled properly. The most obvious vulnerable is default account and password. As oracle used this default account with password to be expired once installed.

The access control is critical for properly securing the database, after a user has been authenticated; access controls dictate what the user is allowed to do. It is important to implement controls at the database level and the database links is to ensure that only authorized links are leveraged. Oracle database vault enables transparent enforcement of operational controls within the database around when, where and how the database is accessed and by whom, as well as controls over what happens within the database from an administrative perspective. It enforces change control policies on database structures and set a variety of user access controls per policy. Also support the Kerberos which is a network authentication protocols that provides the tools of authentication and strong cryptography over the network, Kerberos helps secure your information across the entire enterprise by using secret key cryptography .

We can use extra security to encrypt the database in order to prevent any attacks that could pose the database data and therefore using the SSL or Kerberos can help security the database to make it strong and protected well.

The connection of database has the authentication of encryption access such as username and password

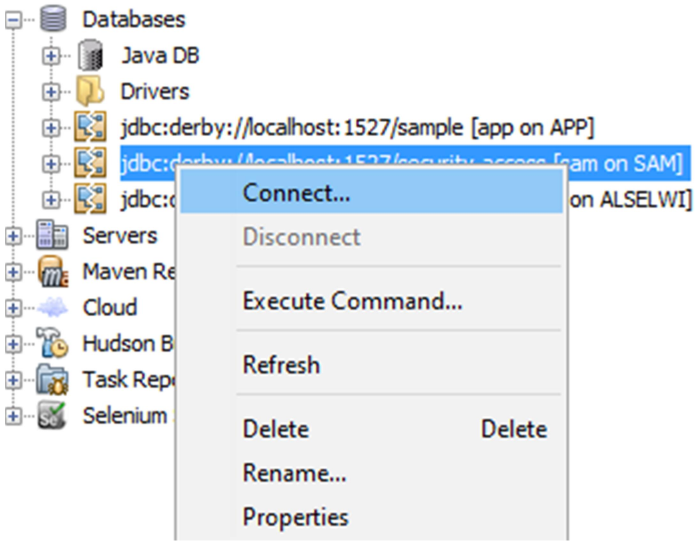
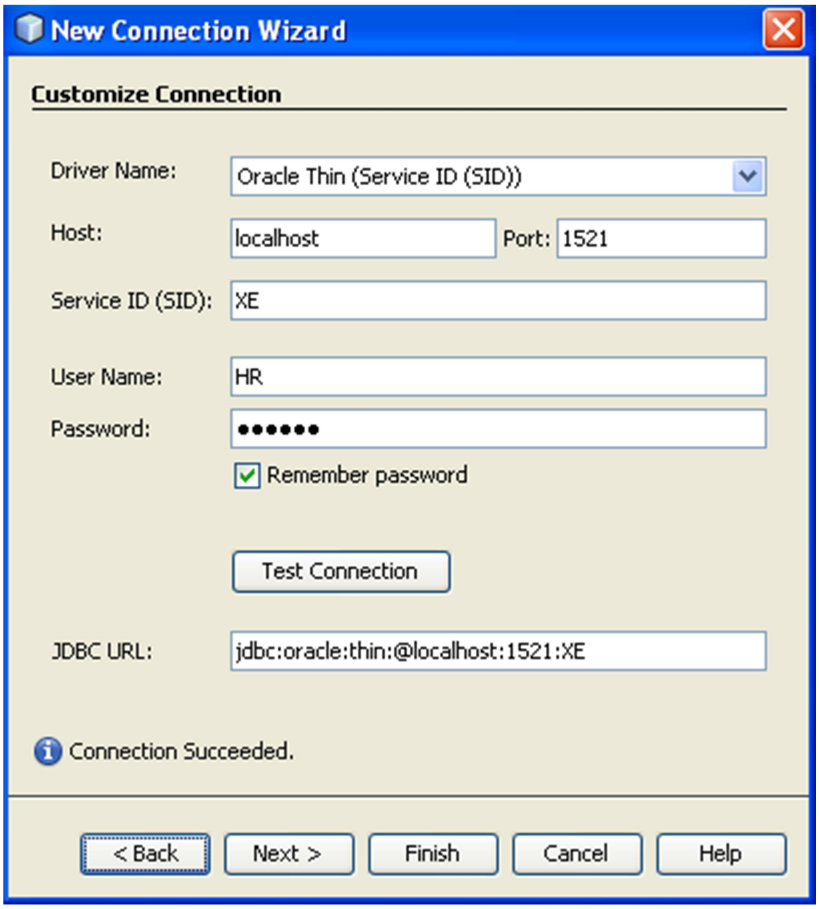


Figure 19 Connecting to a Database

The Java NetBeans database is connected to Oracle database JDK (Java Development Kit) and the connection panel of the wizard needs the details of driver name for the Oracle, host, as it should be local host for a remote connection where the database is installed, port number which should be 1521 as a default service ID XE is default for oracle database XE, username for the administering account and the password that you used during database installation[60]



Customize Connection

Driver Name: Oracle Thin (Service ID (SID))

Host: localhost Port: 1521

Service ID (SID): XE

User Name: HR

Password: ●●●●●●

☑ Remember password

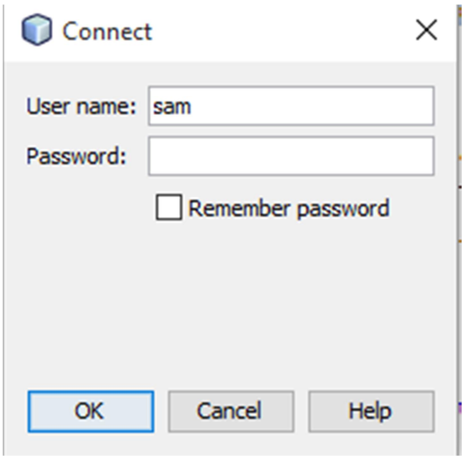
JDBC URL: jdbc:oracle:thin:@localhost:1521:XE

Connection Succeeded.

Figure 20 Connection to a database using additional security access

[60]

Below is the connecting process to the administrative database using the user name and password therefore each Oracle database has a list of valid database users, to access a database a user must run a database application and connect to the database instance using a valid username defined in the database, and oracle database enables you to set up security for the users in a variety of ways. When creating a user account you can specify limits to the user account which is a profile collection of attributes that apply for a user. The database has a policy requirement for securely storing and retrieving database username and password for a user to get the authentication to access the database by presenting acceptable credentials. In addition, it must grant the access only after authentication with credentials, and that username and password must be stored in a file separate from the executing body of the program's code and must not be word readable. And database credentials may reside on the database server, in this case a hash number identifying the credentials may be stored in the executing body of the programs code, and stored as part of the authentication server, and may occur on behalf of a program as part of the user authentication process at the authentication server in this case there is no need for programmatic use of database credentials. [61]



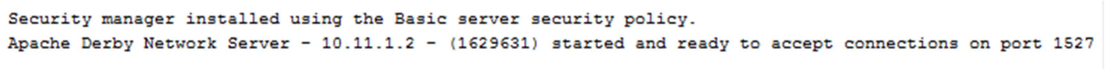
User name: sam

Password:

□ Remember password

Figure 21 administrator security access to the database

Below is the database driver manager that is secured by the security manager using the server security policy, this result of the connection to the database drive and it uses the Apache derby to allow the connection at port 1527 of localhost.



```
Security manager installed using the Basic server security policy.
Apache Derby Network Server - 10.11.1.2 - (1629631) started and ready to accept connections on port 1527
```

The figure further down is the Admin interface to act like a wireless router who consent the users to access to it through the encrypted DNA security key, and this key is deposited in the database behind this interface, and when the user’s key is matched then it allows access to the internet as genuine independent user own a private traffic outside other users.

The administrative database security that organizes all the users at one database and makes a control restriction or limits to the users by adding some of the functions to the database and keep the users in control during their access; also each user will have their own username and password on the field of the database so when accessing the database they can access only their record and can modify it when needed.

This interface consist of the encryption which is to encrypt the user data to save it to a DNA sequence list in the database, also it have the decryption role to decrypt the encrypted sequence to a plain text data to reveal the encrypted data.

When the user want to access the wireless then this interface will process his query to access and when recognized, then the user will grant a successful connection to the wireless, and if the user not found it would deny access and grant disconnect to the interface.

The benefit of this to compare the user data with the data sent to compare if the it is not match then will be granted 0 which means off and get disconnect, also if it is matched with the sequence in the database will grant 1 binary means on to grant connection.

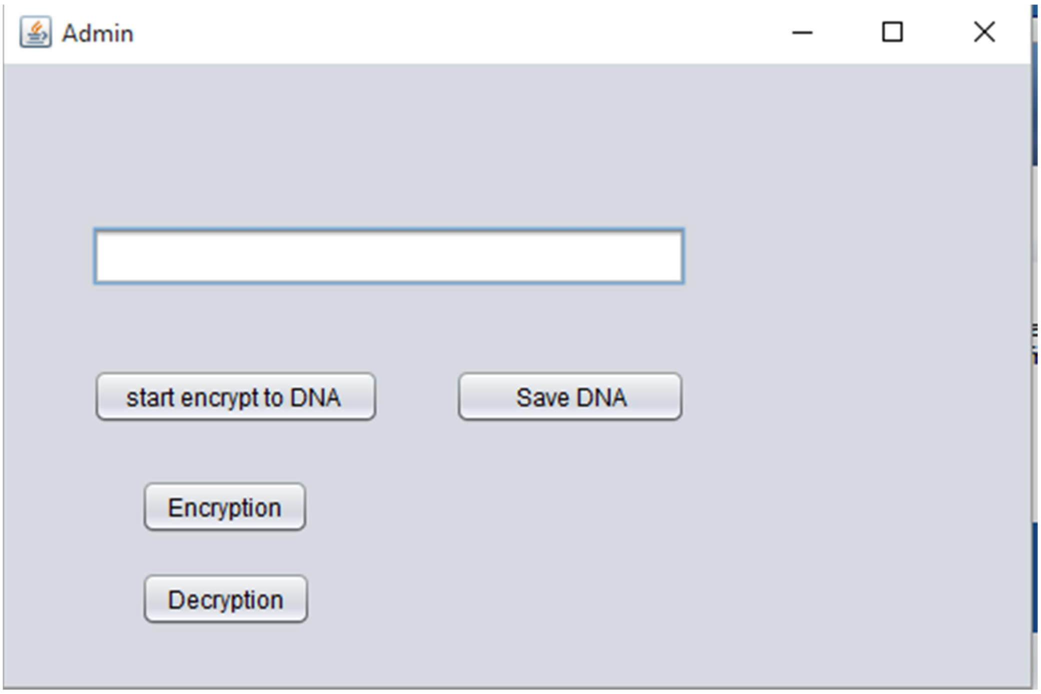
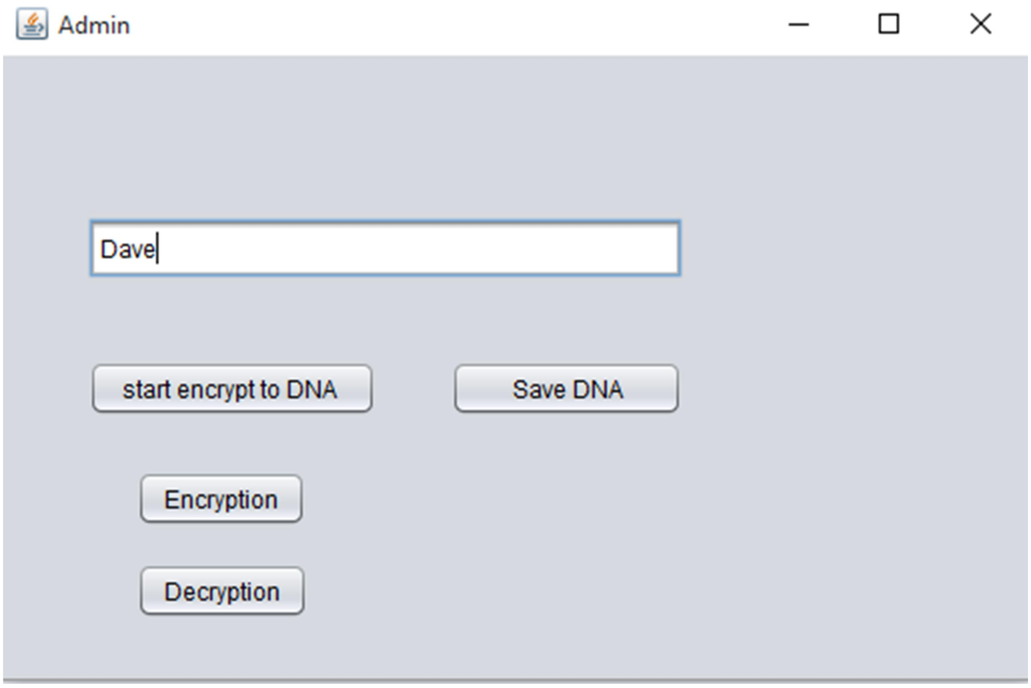


Figure 22 Admin of Wi-Fi device security access control to the database

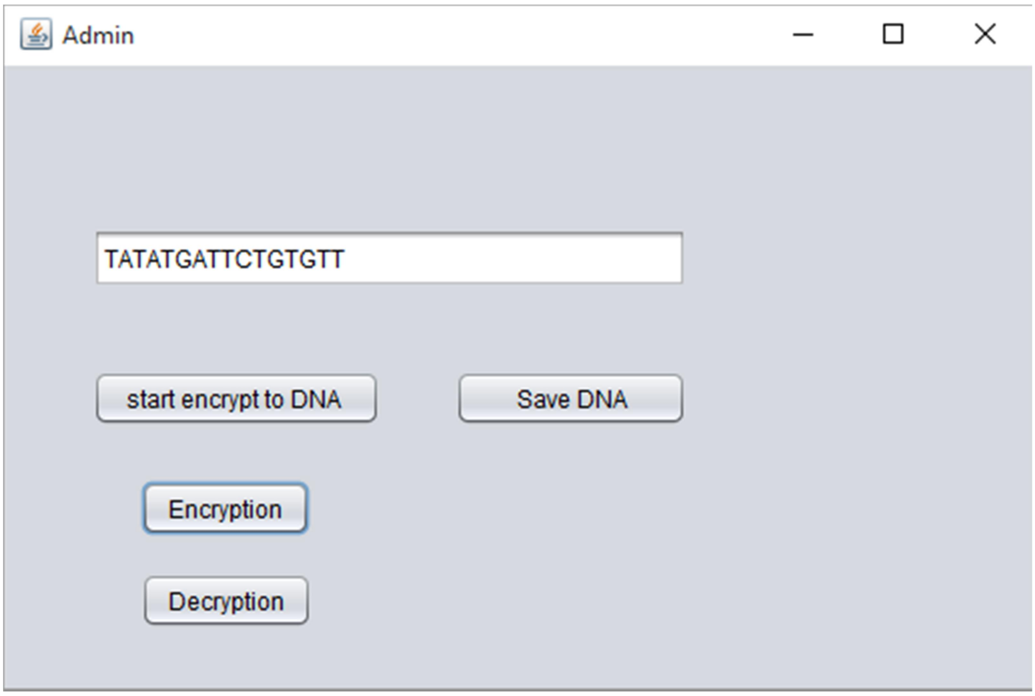
The following figure is to illustrate of how the interface process the plain text for example we have a user Dave as input data which is static data in one text field in the main interface of the admin who will add this user to the control access of the interface access record.



Dave

Figure 23 Processing the string in textfield

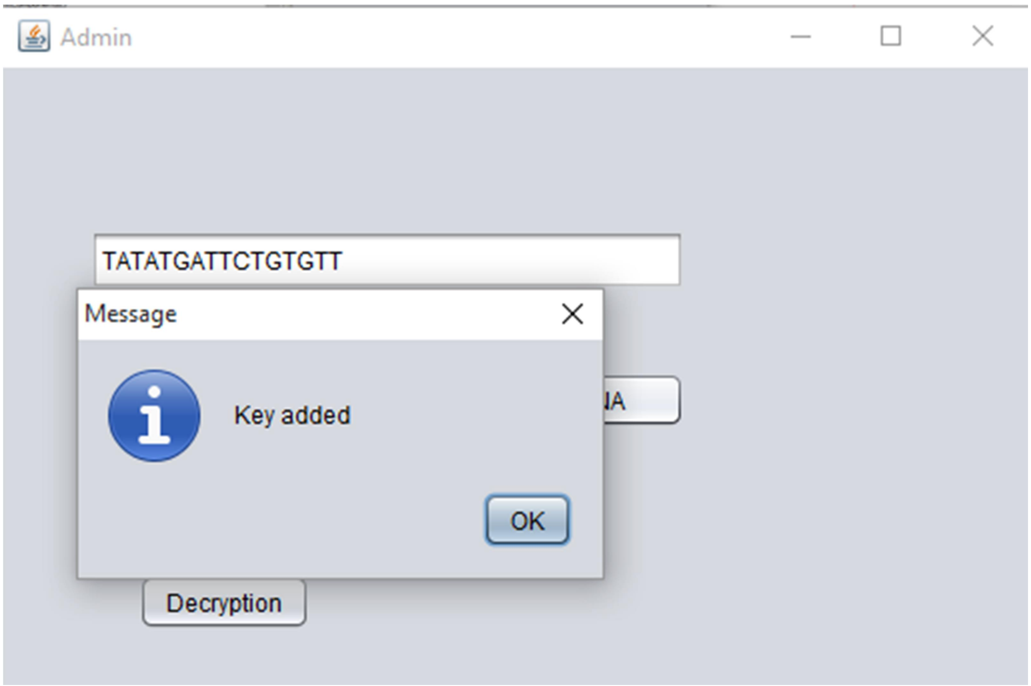
Here this figure translated the plain text of the user Dave and have been encrypted it to these DNA sequences such as TATATGATTCTGTGTT, therefore each user will be encrypted to DNA sequence similar to this process, of encrypting data to sequence and they should be unique because each user he/she should be a unique access key encrypted to an unique DNA sequence.



TATATGATTCTGTGTT

Figure 24 The result of conversion to DNA in textfield

If the user such as Dave has been encrypted to DNA sequence then when we have to save it to a database we can click on save DNA, and then it will show a confirmation that it has been added to the database and a message will show as key added.



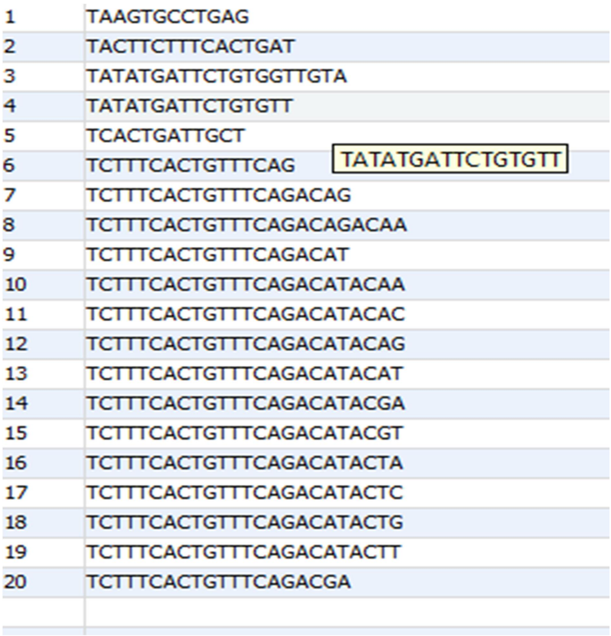
TATATGATTCTGTGTT

Key added

Figure 25 shows the result of adding the DNA sequence to Database

After we have added the encrypted data of the user such as a name or anything and then DNA sequence stored to a database sequence like the one bellow and also the user Dave we have added is showing here on the list which TATATGATTCTGTGTT this sequence if we decrypt it and the decryption will be Dave.

In this list the admin can monitor the users who are allowed to access to the interface and also he has the control to modify or edit any data such as delete or add the user to the block list, also the future work here for this list is to add lots of functions such as know when accessed to the wireless list and locate them also monitor their activities behavior in the admin control.

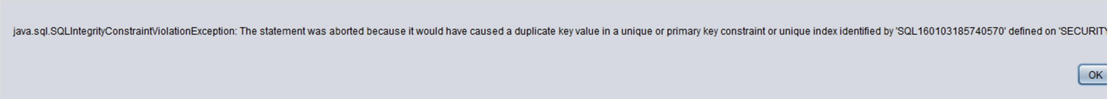


1	TAAGTGCCTGAG
2	TACTTCTTTCACTGAT
3	TATATGATTCTGTGGTTGTA
4	TATATGATTCTGTGTT
5	TCACTGATTGCT
6	TCTTTCACTGTTTCAG
7	TCTTTCACTGTTTCAGACAG
8	TCTTTCACTGTTTCAGACAGACAA
9	TCTTTCACTGTTTCAGACAT
10	TCTTTCACTGTTTCAGACATACAA
11	TCTTTCACTGTTTCAGACATACAC
12	TCTTTCACTGTTTCAGACATACAG
13	TCTTTCACTGTTTCAGACATACAT
14	TCTTTCACTGTTTCAGACATACGA
15	TCTTTCACTGTTTCAGACATACGT
16	TCTTTCACTGTTTCAGACATACTA
17	TCTTTCACTGTTTCAGACATACTC
18	TCTTTCACTGTTTCAGACATACTG
19	TCTTTCACTGTTTCAGACATACTT
20	TCTTTCACTGTTTCAGACGA

TATATGATTCTGTGTT

Figure 26 The list of user security keys encrypted to DNA

This message shows that if the encrypted data is already in the database then it is duplicated and the key should be unique therefore, we cannot add this user to the access list of the wireless interface and now it should be rejected to the list.



```
java.sql.SQLIntegrityConstraintViolationException: The statement was aborted because it would have caused a duplicate key value in a unique or primary key constraint or unique index identified by 'SQL160103185740570' defined on 'SECURITY
```

Figure 27 show the duplication in database

This interface is the user interface which that keeps the user data and encrypts it to a DNA sequence using the DNA button, which then will encrypt the input data in the text field to a DNA and save it in the user interface for the future access, and then next button is the connection to connect to the admin wireless after matching the user sequence in the database list.

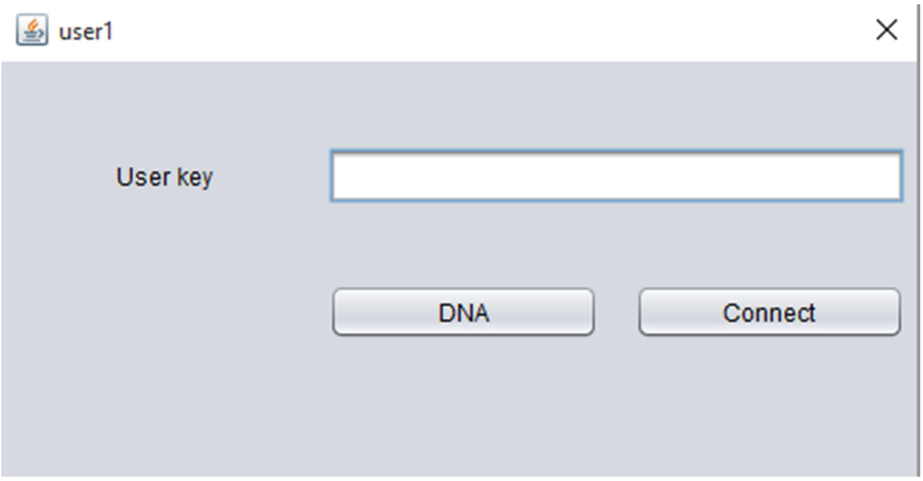
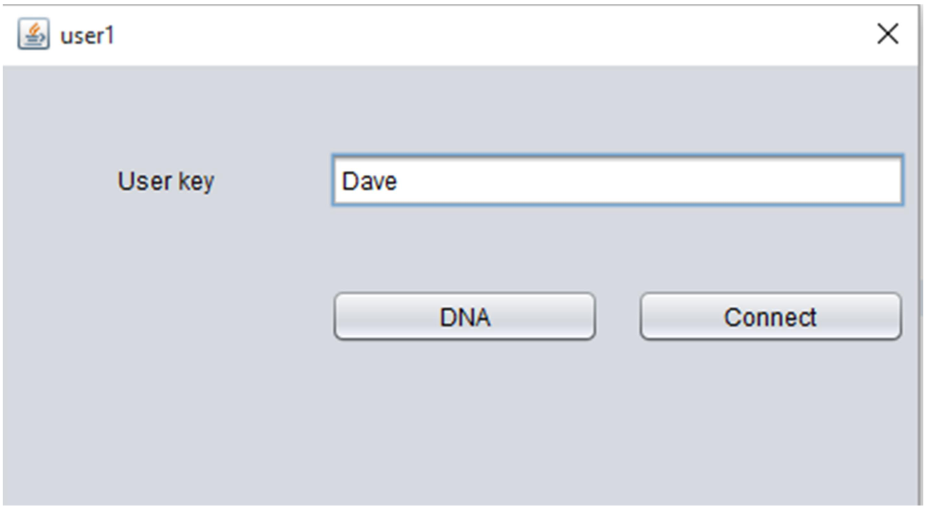


Figure 28 User security key access

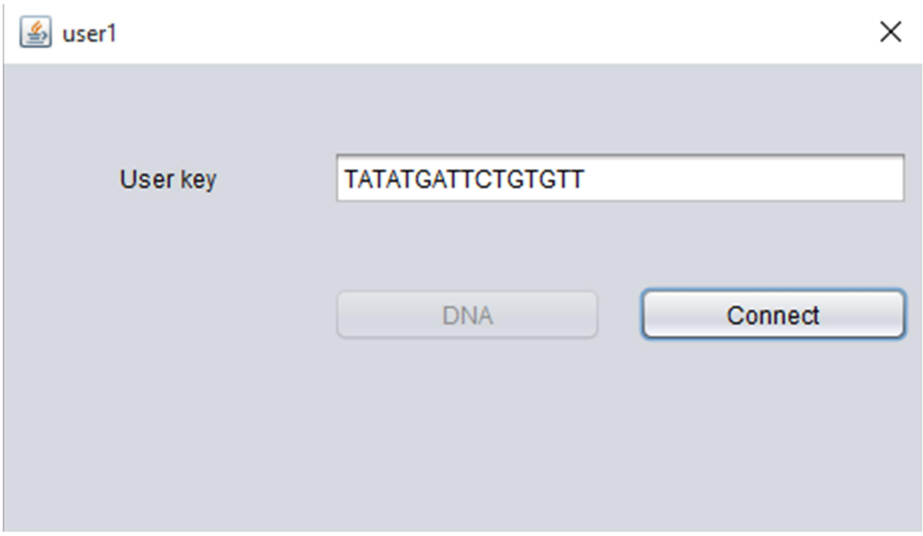
After we saved the encrypted user details in the database now the user is ready to encrypt his data in his interface, here the user is inputting his data in the text field as Dave initial input to access to the wireless interface and the future work will be held the dynamic data and this is static data we have so it needs the dynamic in order to make the keys is difficult be penetrate or capture and put the hackers outside the scope of hacking when using a dynamic key with static.



Dave

Figure 29 User keys in string before conversion to DNA

This interface is describing the encryption of user data to DNA sequence such as we have encrypted Dave to TATATGATTCTGTGTT and after encrypting it the button of DNA will be set as disable in order to save it in the user interface to get the device access to the wireless automatically with the need to add it again.

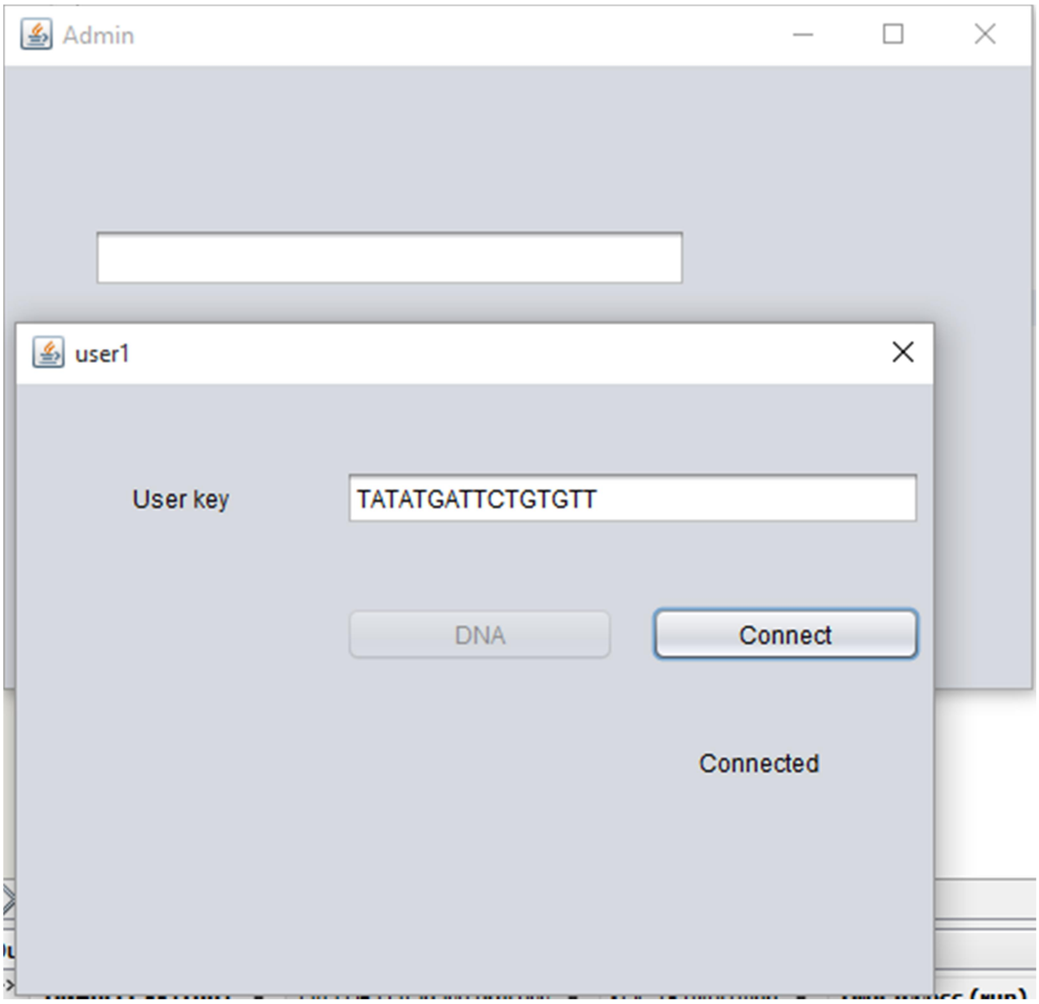


user1

User key TATATGATTCTGTGTT

Figure 30 User string converted to encrypted DNA

This figure is showing the user is connected to the wireless interface after it has been matched with the database list and grant access to the admin or wireless interface as a legitimate user.



Admin

user1

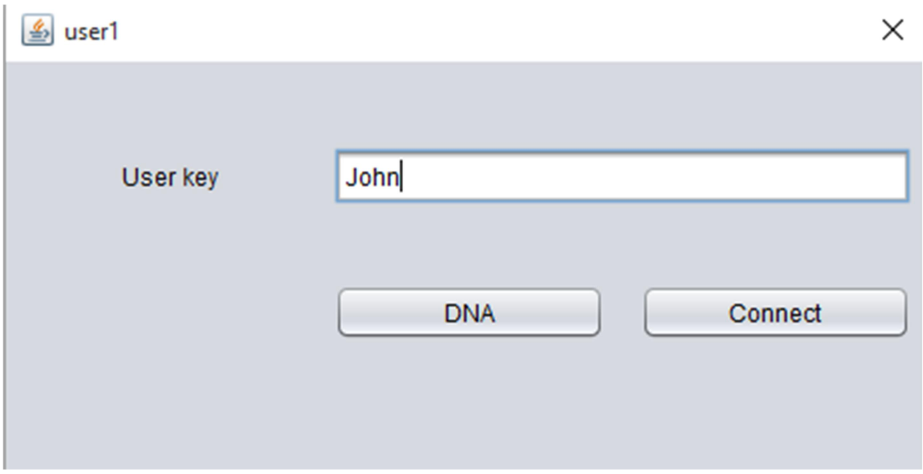
User key TATATGATTCTGTGTT

Connected

Figure 31 The result of connection the user to Wi-Fi after matched the key

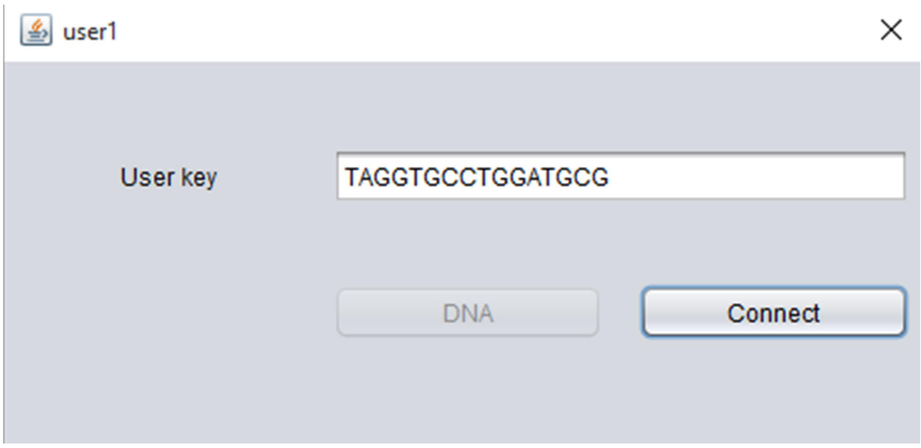
Here is showing the hackers who try to access using their guess words such as John and when the interface has a dynamic encrypted DNA sequence then it will be hard for the hackers access or even if they used the dictionary attack because the key is sent to access is different on the second access because this process will keep update the DNA sequence s of the dynamic data, therefore this is the dynamic is the next steps to be needed for this project.

For example the hackers tried to add John to the interface and encrypt it and when press connect the admin process will compare it with the database as a static data if the software match it then it will grant access otherwise it is out of the static encrypted data and will grant a deny access and disconnect rewarded.



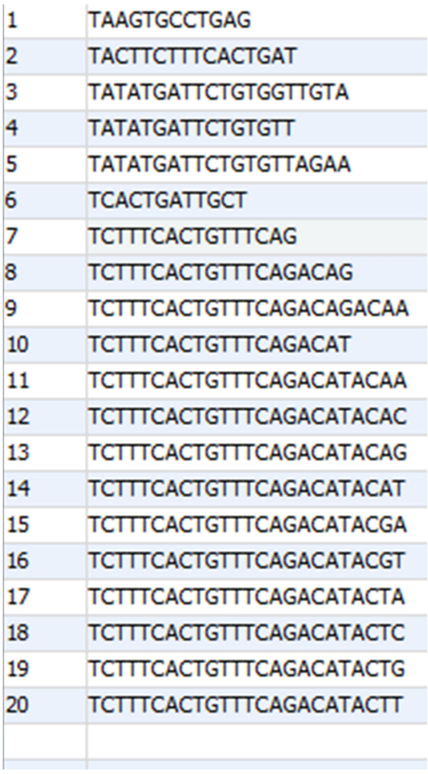
User key: John

Figure 32 User interface with intruder's data



User key: TAGGTGCCTGGATGCG

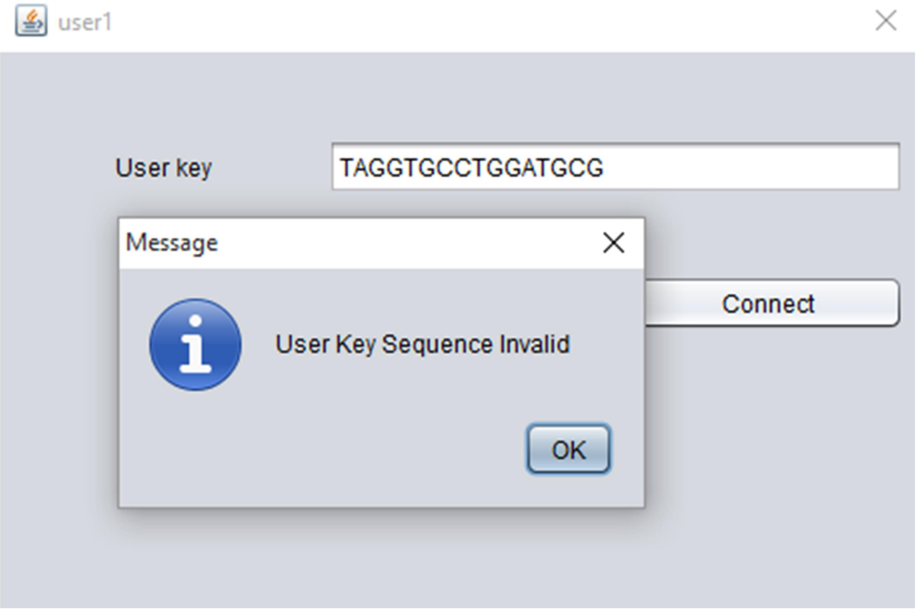
Figure 33 the intruder converts to DNA sequence



1	TAAGTGCCTGAG
2	TACTTCTTTCACTGAT
3	TATATGATTCTGTGGTTGTA
4	TATATGATTCTGTGTT
5	TATATGATTCTGTGTTAGAA
6	TCACTGATTGCT
7	TCTTTCACTGTTTCAG
8	TCTTTCACTGTTTCAGACAG
9	TCTTTCACTGTTTCAGACAGACAA
10	TCTTTCACTGTTTCAGACAT
11	TCTTTCACTGTTTCAGACATACAA
12	TCTTTCACTGTTTCAGACATACAC
13	TCTTTCACTGTTTCAGACATACAG
14	TCTTTCACTGTTTCAGACATACAT
15	TCTTTCACTGTTTCAGACATACGA
16	TCTTTCACTGTTTCAGACATACGT
17	TCTTTCACTGTTTCAGACATACTA
18	TCTTTCACTGTTTCAGACATACTC
19	TCTTTCACTGTTTCAGACATACTG
20	TCTTTCACTGTTTCAGACATACTT

Figure 34 Intruder is not matched with the security key in the database

Here is describing the user is not in the static encrypted sequence list database and showing a message as user key sequence invalid.

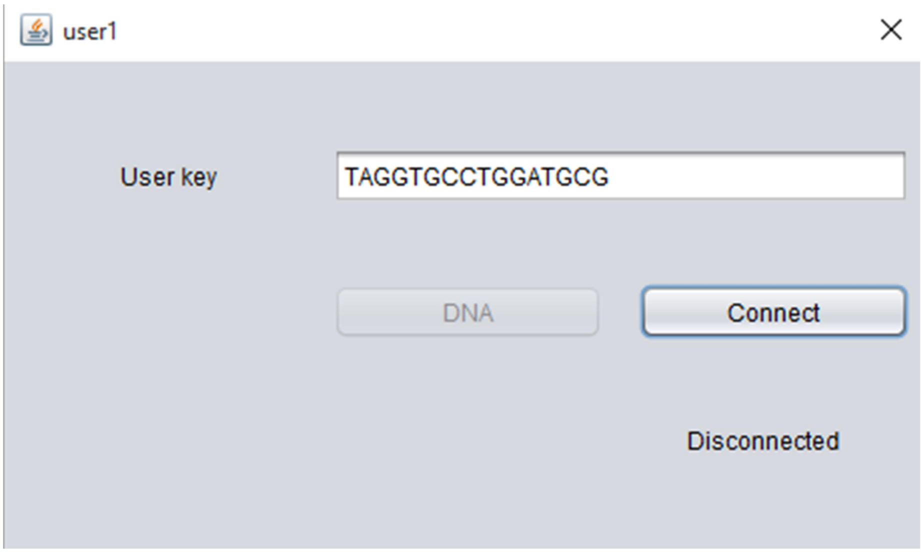


User key TAGGTGCCTGGATGCG

User Key Sequence Invalid

Figure 35 intruder key is invalid and refused to connect to Wi-Fi

Then hackers will grant disconnected to the wireless interface and because the DNA sequences are not matched which equal to 0 binary that means the compare of your static sequence with the sequences in the legitimate lists are not matched then grant off disconnected from the wireless.



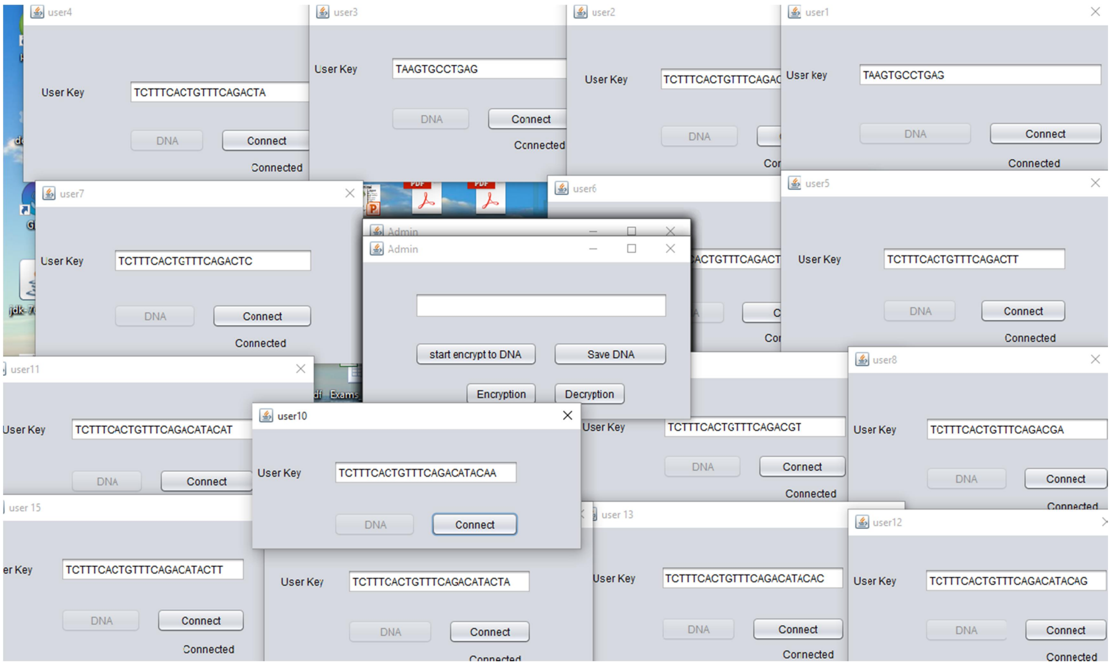
User key TAGGTGCCTGGATGCG

Disconnected

Figure 36 intruder is blocked and disconnected

This figure describing that many users are accessing to the wireless interface after comparing their encrypted records in the database list in order to compare and then match or mismatch the data in the database, also here the database is scalable which means that can hold up to tens or could be hundreds of users in the database therefore the database will be overloaded with the heavy network traffic to the wireless database.

In addition, here each user has their own independent connection outside the scope of the other users, and it will be hard for other users eavesdropping other users on same wireless network. Because user has his own user key access to the wireless network interface and we recommend adding the dynamic sequence for getting a difficult sequence key to put the hackers or eavesdroppers confused and hard for them to use the key captured.



User Key TCTTTCACTGTTTCAGACTA

User Key TAAGTGCCTGAG

User Key TCTTTCACTGTTTCAGAC

User key TAAGTGCCTGAG

User Key TCTTTCACTGTTTCAGACTC

ACTGTTTCAGACT

User Key TCTTTCACTGTTTCAGACTT

User Key TCTTTCACTGTTTCAGACATACAT

User Key TCTTTCACTGTTTCAGACATACAA

User Key TCTTTCACTGTTTCAGACGT

User Key TCTTTCACTGTTTCAGACGA

User Key TCTTTCACTGTTTCAGACATACTT

User Key TCTTTCACTGTTTCAGACATACTA

User Key TCTTTCACTGTTTCAGACATACAC

User Key TCTTTCACTGTTTCAGACATACAG

Figure 37 Database can overload many legitimate users to connect to the Wi-Fi

5.1 DNA conversion process algorithm code

First of all the database should be created for storing the encrypted user's security key for getting a sequence for each record in order to align this sequence and place it as a security key for matching access process to the Wi-Fi, below is the example of selecting column of the database which is User_key field as shown below to connect the database for data entity query.

```
// connect to Database information

ResultSet rs1 = conn.SQLSelect("select user_key from security ");

while (rs1.next()) {

        s1 = rs1.getString("user_key");

        for (int i = 0; i < s1.length(); i++) {
```

After connecting the database then each entity s1 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 binaries and then the binaries will place the values of 0 and 1 to DNA sequences, from the ASCII code we get the binary codes, and these binary codes will be converted to the binary value 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 binary to make it hard to be guessed by intruders for example A=00 we can 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;
```

5.2 DNA conversion experiments

Conversion to DNA sequence code in the frame and store it in the database this is a unique primary key for the user which is variable character and they are converted to a DNA sequence, so these DNA coding are converted to ASCII code and then to binary code, then these binary codes are resulted to DNA sequences encryption thus the user details are concealed in DNA coding. We explained previously how the conversion process produces the code and forms binary digits through ASCII.

We can add dynamic records but it need consideration of which tool can be used as a dynamic with both devices to change both parties to the same value dynamic DNA sequence helps provide variable security key to the DNA sequences.

For this figure, the user will possess everything they require to adapt with the security to remain secure and to make them aware that this is the vital role as a security key for accessing to their Wi-Fi router. In addition, we explained how the converted to DNA sequence is is and save it in the database experiment and we showed the DNA coding that is needed for the security access matching purposes.

Therefore all these DNA coding have to be gathered to acquire a security key for matching order and authentication the main research aim here is to find a novelty with DNA and create it in a different way to serve as a security key.

The administrator has the main authorization to delete or add new users to the system for the Wi-Fi security access and therefore the administrator has their own username and password in the database.

5.3 Other Wireless access Authentication of DNA process

User enters his details to the database using the DNA elliptic, which is used for portable devices as a DNA key x_1 and x_2 as the equation shows at the following:

C= $x_1 i + x_2 j$ and i and j are the two parties of the user device and the wireless router.

The elliptic $E_i(i,j)$

User connect to Wireless access for checking the authentication

j picks up a key and sends it to i, and then the user i computes the key

For comparison and send it to the j

$x_1 i = x_2 j$

If they are equal 1 then they matched and the authentication is successful otherwise

$x_1 i \neq x_2 j$

They equal 0 and then off granted and unsuccessful.

5.4 Summary:

The achievement of this research is demonstrating the DNA security key that we developed from the conversion of DNA static or dynamic data, and the DNA key with dynamic data is to get the security key updated frequently and get the hackers confused and if they do break in the first time, they will lose the security key when it is updated to new security key, and we have explained how the user data converts to DNA-bases encryption; we proved this in the implementation to view the DNA conversion encryption, this encryption will be used as a security key for the user's device to access their Wi-Fi network when processing the matching technique. The DNA sequence security key will be converted to DNA format automatically.

In this research, we clarified the basic steps of the security key and how we converted them from plain data to an encrypted DNA security key, and stored them in the database to provide of the whole system requires building a fully functional Wi-Fi access control in a new security way with DNA.

The comparison explained the two-way handshake communication, which takes place for controlling the access to the wireless router, and monitors the users accessing to the Wi-Fi.

Chapter 6

Evaluation

In chapter 4, we said there are problems with the existing security protocols and these problems mean the security protocols need to be updated to solve the existing issues, as they are prone to break-in due to the flaws that hackers are looking for to break into the Wi-Fi. And here we have proposed our DNA security protocol as a different type of security for securing the Wi-Fi network and we have issued the basic steps to build a DNA security protocol and make it clear to implement it in the real world close to the existing security protocols as we are not saying this is the complete solution but at least it solves some problems that were explored with the existing security protocols such as the sharing security key and the Wi-Fi connection with isolation security key to each device. And additional to these solutions suggested that the DNA security key needs a dynamic DNA security key tool to get a complex DNA security key and this tool supports updating the security key regularly as opposed to the existing security key that remains the same key for ages and this proposed expected solution is advantageous instead of sharing one security key with all the Wi-Fi users, this solution DNA security key will establish a security key for each user's device rather than sharing it with all devices.

In chapter 5 what we have achieved is a DNA symmetrical conversion with the admin (Wi-Fi) and the user parties and tested it with java software it achieved the connection authentication using the DNA security key which converts the strings and numbers to DNA sequences from the static data to encrypt it into DNA bases the implemented process is authenticated with a well-matched or mismatched DNA sequence against the database stored for the Wi-Fi devices of the legitimate users. Therefore chapter 5 describes the initial argument solutions of the encryption to DNA bases and the experimenting of using the DNA bases in the database to match and mismatch the DNA security key if it match then the two parties connection is 1 and granting access and if the DNA sequence of the user device is not matching the DNA sequence of the Wi-Fi database then is equal to 0 and deny access to the Wi-Fi.

The initial stages are developing the DNA sequences conversion, which encrypt the data to DNA bases also the implementing process has the function to decrypt the DNA security key to an original data of the user. After encrypt the data in a rank of DNA sequences forming as a security key we have a process function to store it in the database as we have proved this test in the chapter 5 using java applications this implementation done in a logical not in a physical. We have successfully converted the static data to the DNA encryption and accessing the legitimate users through the comparison process whether legitimate user or intruder, the conversion formatted to DNA sequences kept as a unique in the database.

The DNA-inspired security algorithm mechanism is to provide a security authentication and protection for the Wi-Fi accessing using a DNA sequence as a technique that we have based on existing DNA encryption results. It has the possibility of controlling the access gateway to the Wi-Fi using the DNA sequence comparing method match technique, and apply this DNA security to support Wi-Fi network security and here we have explained about the DNA sequence encrypting to DNA bases alphabets, and tested it through the symmetric key that is should be the same with the user implementation process and the Wi-Fi admin implementation process.

These encrypted DNA bases in the database determination stand as the users security key; finally this could be evolved further when adding functional tools to be more robust to use for instance the DNA dynamic bases to keep the key self-updating furthermore to static data, and we have worked out on how it could capture the data with the stored ones in the database of the user's static DNA sequence key and process it to a new DNA sequences rank the investigation results in our implementation is end up with static data this demonstrations the feasibility of using DNA encryption and authentication access after matching the user security key to access to the admin(Wi-Fi) with using the static DNA sequence not the dynamic because this will be the next work after this research project. At that juncture, the next step that is outside the scope yet here this project is limited with user static data; here our intellectual challenge in this stage is to get the throughput of the Wi-Fi security to provide an initial step of the robust protection against the intruder.

In this research we have done the conversion to DNA-bases and the matching process between two parties or multi-users with the admin (Wi-Fi) and perceive the user key is stored in the database as a DNA sequences format also the database is encrypted and the admin can access it using their known username and password and the users can't access to the database.

Researchers said the DNA is secure enough, therefore we need to assume from the scholars' results and their findings that they proved the DNA is secure and it is the next security generation to rely on, which is proved through several researches with experiments and they found it hard to break in only after they try several time, and if they break the key therefore the key code of triplet DNA needs to be changed it in different key, and all what we have done is implemented it in a new encryption security key for multi-users and what we have to do is adapt this DNA in this new novelty of security for Wi-Fi network. We do not know yet whether it is secure enough, as we have not tested it physically because it is outside the scope to perform the entire research of the Wi-Fi security key. We are more interested in showing the feasibility and logical testing in the software using hypothesis of interfaces for Wi-Fi and users at this stage, intended for using DNA cryptography in practical applications. We have used these initial techniques to get the encryption in DNA and we believe our result is providing worthy preliminary security and these techniques are feasible in security and could lead to vulnerabilities because it is in elementary development and not added to it robust professional security functions to serve as an a new security protocol software.

In these works the software has a frame for the admin application and for a user that are basic and these applications need to be evolved more in order to prevent the common flaws in the Wi-Fi security perimeter and adapt the new tools to be comfortable with the changes to the security key and also the data traffic needs to examine how the DNA bases could secure the data connecting to the Wi-Fi. The brief of this software was to create the database in order to input user's DNA bases in the database as DNA sequences format for each user.

In addition, users we have to login access to their accounts of the user so the legitimate users can update their details after they get permission from the admin to update their data then they can access their own account via their username and password. Moreover, the administration account has an administrator's username and password access, this is for giving permission to the administrator to monitor the users and edit their accounts so the administrator has the priority of unlimited access to the user's Wi-Fi network.

Also in our research is that we used the DNA for comparison which is inspired by human genetics which reflect the similarities of a common ancestry that appears to be shared by all life on Earth, as they share genes, yet people have different hair color, facial structures and other traits, these differences between individuals result from very small differences in their DNA sequences. Similarly in DNA-inspired computing we may want to find the similarity of DNA sequences such as in a Wi-Fi security key that is extracted from the user's profile of DNA bases in this effort comparing the DNA sequences at the user device with the Wi-Fi and find the values of each if the value is equal to the digit 1 then grant on function and permit access to the Wi-Fi network otherwise if the comparison does not have any similarity value then is digit 0 grant off and deny access to the Wi-Fi network to intruder user.

Chapter 7

Conclusion and future work

7.1 Conclusion

We established the conversion of the plain text to an encrypted DNA sequence and store it in the database, this experiment is to extract the user data to convert them to DNA nucleotide bases key and use them as a security key for match the security key of the user's device during the synchronous connection to the Wi-Fi, then the security key is encrypted to DNA sequence for each user who wish to use the Wi-Fi connection to the internet, using their portable devices such as mobile phones, laptops and other personal devices and this DNA key of the device should be the same key sequence in the database of the Wi-Fi for network observation.

The DNA system in the Wi-Fi device uses the detection and matching process to compare the DNA sequence security key. And we have tested this process and matching in the implementation and we have described the theory to demonstrate how this technique is applied, and presented implementation results about practically how to encrypt and decrypt any user data to DNA sequences.

And the DNA sequence key in the Wi-Fi must be the same DNA sequence key with the user software for the purpose of the process of matching sequences technique which is the vital process using the parameters techniques the DNA signature sequence to match a threshold value of the encoded DNA sequence in the network connection to a corresponding DNA nucleotides sequences in the Wi-Fi observed the DNA sequences and find similarity degree value aims to match or mismatch DNA sequences.

The theory here shows how the DNA sequence provides good security when tested in the implementation as it was proved by other researchers as well that it gives good security, therefore in the matching process the value degree of DNA sequences if it is equal to zero then it isn't matched which means it is an intruder user trying to access and raises negative alarms for blocking the connection otherwise is equal to one and allows access legitimate user.

Also the users on the same network can be identified by their unique DNA, the DNA sequence is useful for intrusion detection to detect the break through the alarm is raised of negative access when it is equal to 0 meaning intruder is blocked that the sequences mismatched or try to guess the victim user's details in this case system can raise the alarm of this attempts.

In this work we could add and also demonstrated that DNA sequences can provide at least feasible security protection encrypted to DNA bases, and the DNA has concealed this data with its nucleotides bases using DNA encryption.

7.2 Future Work

Evolving the Wi-Fi security using DNA security techniques to mitigate the flaws of the current existing security protocols is a hypothesis, as we didn't reach to the final point of DNA security yet but at least propose the initial stages and the feasibility of DNA algorithm security for a Wi-Fi security key access point. In addition, this key will be translated from the data that a user can add to the Wi-Fi security settings to setup the security for the AP network that needed to be secure, and we have done the basic arguments for coding the data to DNA sequence encryption using Java for getting the encryption to DNA. Thus, the next steps are implementing the DNA dynamic security key as a dynamic security key adding with the satic DNA encryption key and test it with the physical devices and judgment the findings of the DNA key at both sides i.e. the Wi-Fi router and the user devices and check how well it could provide security to the Wi-Fi network.

Further development of the DNA encryption software for the user data, static and dynamic data, moreover implementing those data stored to the encrypted database will be the stepping stone to find the result and how this needs to be improved and done more securely, hence research is needed to implement the dynamic DNA tools or techniques.

This implementation experiment of DNA encryption process to Wi-Fi security protocol algorithm could be tested or improved with a WPA2 to solve sharing one security key for all users and to understand what findings we get and how to adapt it to be a robust security protocol;

Reference:

[1] 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.

[2] R. D. Lankes, “Credibility on the internet: shifting from authority to reliability,” *J. Doc. Sch. Inf. Stud. Syracuse Univ. Syracuse, New York, USA*, vol. 64, no. 5, pp. 667–686, 2008.

[3] Y. Li, Y. Zhang, L. Qiu, and S. Lam, “SmartTunnel : Achieving Reliability in the Internet,” *Res. Spons. by Natl. Sci. Found. Dep. Comput. Sci. Univ. Texas Austin*, 2006.

[4] W. Lehr and S. Bauer, “Assessing Broadband Reliability : Measurement and Policy Challenges,” no. 2009, pp. 1–38, 2010.

[5] U. Kumar and S. Gambhir, “A Literature Review of Security Threats to Wireless Networks,” *Int. J. Futur. Gener. Comminication Netw.*, vol. 7, no. 4, pp. 25–34, 2014.

[6] T. Mendyk-krajewska and Z. Mazur, “Problem of Network Security Threats 1,” *J. Wrocław Univ. Technol. Inst. Informatics, Wrocław, Pol.*, no. March 2009, pp. 436–443, 2010.

[7] M. T. Selvan, D. Rajeshwari, P. Priya, and K. N. Shiny, “Performance Effective Design of Bi-Quad Antenna with Parabolic Reflector over Traditional Omni Directional Antenna with Wireless Fidelity (Wi-Fi),” vol. 2, no. 3, 2015.

[8] 4SHWETA TRIPATHI PRATIM KAR, 2SUMEDH KOSHE, 3ANIKET GOSAVI, “STUDY OF VULNERABILITIES OF WLAN SECURITY PROTOCOLS,” *Journal, Dep. Comput. Eng. Fr. C. Rodrigues Inst. Technol. Vashi, Navi Mumbai*, no. September, pp. 109–112, 2013.

[9] A. Sari and M. Karay, “Comparative Analysis of Wireless Security Protocols : WEP vs WPA,” no. December, pp. 483–491, 2015.

[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. H. Lashkari, M. I. R. Mohammad, S. Danesh, and B. Samadi, “A Survey on Wireless Security protocols (WEP , WPA and WPA2 / 802 . 11i),” *Fac. KnowledgeManagement, Multimed. Univ. - 63100 CyberjayaMalaysia*, no. Iv, 2009.

[12] 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.

[13] A. Blank, “WEP Vulnerabilities and Attacks,” *Journal, Cryptogr. II*, no. 4005–706.

[14] L. Caeiro, F. D. Cardoso, and I. S. T. Inov-inesc, “Wireless Access Virtualisation : Addressing Virtual Resources with different Types of Requirements,” *Networks Commun. (EuCNC), 2014 Eur. Conf.*, pp. 1 – 5, 2014.

[15] M. W. Pan, H. Singh, S. Yong, J. Oh, and C. Ngo, “Principles of IEEE 802.15.3c: Multi-Gigabit Millimeter-Wave Wireless PAN,” *Journal, Samsung Electron. ∗ 75 W Plumeria Dr., San Jose, CA 95134, USA*, pp. 0–5, 2009.

[16] S. Chaumette and R. Laurent, “UbiPAN : A Bluetooth Extended Personal Area Network,” *Int. Conf. Complex, Intell. Softw. Intensive Syst. Dep. Comput. Sci. Univ. Bordeaux, Talence, Fr. Krakow*, no. Imis, pp. 774 – 778, 2010.

[17] M. Frodigh, P. Johansson, and P. Larsson, “Wireless ad hoc networking — The art of networking without a network,” *Journal, Erricson Rev.*, no. 4, pp. 248–263, 2000.

[18] C. D. Knutson and R. Woodings, “Infrared Data Communications in Wireless Personal Area Networks,” *Journal, Comput. Sci. Dep. Brigham Young Univ. Provo, Utah, USA*, 2001.

[19] W. Liu, H. Nishiyama, N. Kato, Y. Shimizu, and T. Kumagai, “A Novel Gateway Selection Method to Maximize the System Throughput of Wireless Mesh Network Deployed in Disaster Areas,” pp. 771–776, 2012.

[20] S. Tsong, M. Huei, T. Tsai, and Y. Tsai, “Condensed Downlink MAP Structures for IEEE 802 . 16e Wireless Metropolitan Area Networks (MANs),” *Conf. Veh. Technol. Conf. IEEE 71st, Dep. Commun. Eng. Nat. Cent. Univ.*, no. Dl, 2010.

[21] D. Krishnaswamy, “Network Economics Considerations for Incremental Data Services in Heterogeneous Wireless Wide Area Networks,” *Conf. Veh. Technol. Fall IEEE 72nd, Ottawa, Qualcomm Res. Center, San Diego Ca USA*, 2010.

[22] L. Zhang, C. Wei, and H. Tian, “Service Communities for the Convergence of Wide Area and Wireless Personal Area Networks,” *Wirel. Commun. Netw. Mob. Comput. Beijing Univ. Civ. Eng. Beijing, China*, pp. 1 – 5, 2010.

[23] S. Tang, H. Yomo, M. N. Shirazi, T. Ueda, R. Miura, and S. Obana, “Exploiting Network Coding for Pseudo Bidirectional Relay in Wireless LAN,” *Pers. Indoor Mob. Radio Commun. IEEE 20th Int. Symp. ATR Adapt. Commun, Res. Labs. Japan*, pp. 706–711, 2009.

[24] A. School, *Wireless Local Area Network (WLAN) Best Practices Guide*. 2011.

[25] C. Xu, H. Wang, and A. W. L. A. N. Overview, “Heterogeneous wireless LAN-based wireless network attack analysis and research,” *Uncertain. Reason. Knowl. Eng. Conf. Lanzhou China*, pp. 86–90, 2011.

[26] I. N. F. K. Benton and K. Benton, “The Evolution of 802 . 11 Wireless Security,” *Journal, UNLV Informatics-Spring*, no. INF 795, pp. 1–56, 2010.

[27] K. Scarfone, C. Tibbs, and M. Sexton, “Guide to Securing Legacy IEEE 802.11 Wireless Networks,” *Recomm. Natl. Inst. Stand. Technol. IT Lab. US. Dep. Commer. Gaithersbg. USA*, pp. 800 – 48, 2008.

[28] D. Ferro and B. Rink, “Understanding Technology Options for Deploying Wi-Fi How Wi-Fi Standards Influence Objectives,” *A Tech. Pap. Prep. Soc. Cable Telecommun. Eng.*, 2013.

[29] S. Jadhav, S. B. Vanjale, and P. B. Mane, “Illegal Access Point detection using clock skews method in wireless LAN,” *2014 Int. Conf. Comput. Sustain. Glob. Dev.*, pp. 724–729, Mar. 2014.

[30] G. K. Sandhu, G. S. Mann, and R. Kaur, “Benefit and security issues in wireless technologies : Wi-fi and WiMax,” vol. 1, no. 4, pp. 976–982, 2013.

[31] D. Anand, V. Khemchandani, and R. K. Sharma, “Identity-Based Cryptography Techniques and Applications (A Review),” *2013 5th Int. Conf. Comput. Intell. Commun. Networks*, pp. 343–348, Sep. 2013.

[32] M. Pattaranantakul, A. Janthong, K. Sanguannam, P. Sangwongngam, and K. Sripimanwat, “Secure and efficient key management technique in quantum cryptography network,” *2012 Fourth Int. Conf. Ubiquitous Futur. Networks*, pp. 280–285, Jul. 2012.

[33] R. Goutte, “Code for encryption hiding data into genomic DNA of living organisms,” *2008 9th Int. Conf. Signal Process.*, pp. 2166–2169, Oct. 2008.

[34] X. Ren, “A Novel Dynamic User Authentication Scheme,” *Commun. Inf. Technol. Coll. Inf. Sci. Technol. Jinan Univ. Guangzhou China*, pp. 713–717, 2012.

[35] O. Qingyu, “Security Evaluation Model of the Information System Based on the Security Characteristic Measure for the Key,” *Comput. Mechatronics, Control Electron. Eng. Dep. Information, Nav. Univ. Wuhan, China*, pp. 252–255, 2010.

[36] A. Akter, “Security Improvement of WPA 2 (Wi-Fi Protected Access 2),” *A.K.M. Nazmus Sakib al. / Int. J. Eng. Sci. Technol.*, vol. 3, no. 1, pp. 723–729, 2011.

[37] Y. Wang, Z. Jin, and X. Zhao, “Practical Defence against WEP and WPA-PSK Attack for WLAN,” *Journal, Sch. Electron. Inf. Eng. Tianjin Univ. Tianjin, China*, pp. 2–5, 2010.

[38] D. Security, S. Dss, I. Group, and S. I. G. Implementation, “Standard : Version : Date : Author : Information Supplement : PCI DSS Wireless Guideline Prepared by the PCI SSC Wireless Special,” no. July, pp. 1–33, 2009.

[39] J. Bonde, “Wireless Security,” *J. Univ. Minnesota, Morris*, pp. 0–5, 2011.

[40] V. Kumkar, A. Tiwari, P. Tiwari, A. Gupta, and S. Shrawne, “Vulnerabilities of Wireless Security protocols (WEP and WPA2),” vol. 1, no. 2, pp. 34–38, 2012.

[41] M. Beck and E. Tews, “Practical attacks against WEP and WPA,” *J. TU-Dresden, Ger.*, pp. 1–12.

[42] J. Hong and R. Lemhachheche, “WEP Protocol Weaknesses and Vulnerabilities,” *Comput. Netw. Secur. Res. Proj. , Oregon State Univ.*, 2003.

[43] J. Hong and R. Lemhachheche, “WEP Protocol Weaknesses and Vulnerabilities,” *Comput. Netw. Secur. Res. Proj. , Oregon State Univ.*, pp. 1–11, 2003.

[44] T. Tsukaune, Y. Todo, and M. Morii, “Proposal of a Secure WEP Operation against Existing Key Recovery Attacks and its Evaluation,” *2012 Seventh Asia Jt. Conf. Inf. Secur.*, pp. 25–30, Aug. 2012.

[45] M. Caneill and J. Gilis, “Attacks against the WiFi protocols WEP and WPA,” *Journal*, no. December, 2010.

[46] L. Nussel, “The Evil Twin problem with WPA2-Enterprise,” *SUSE Linux Prod. GmbH*, 2010.

[47] M. Vanhoef, F. Piessens, and E. D. Encryption, “Practical Verification of WPA-TKIP Vulnerabilities,” *Journal, ASIA CCS’13, Hangzhou, China*, 2013.

[48] F. H. Katz, “WPA vs . WPA2 : Is WPA2 Really an Improvement on WPA ?,” *Armstrong Atl. State Univ. Dep. Information, Comput. Eng. 11935 Abercorn Str. Savannah, GA*, pp. 1–4, 2009.

[49] R. freeth and A. K. Ranjana Shukla, Samad S. Kolahi, “Educational Institutes: Wireless Network Standards, Security and Future,” *Sch. Comput. IT Unitec New Zeal. Auckland, New Zeal.*, pp. 76–82, 2009.

[50] J. Dwyer, H. Bridewell, N. Nguyen, H. Jasani, and H. Heights, “Impact of Handoff

Delay on RADIUS Enabled," *Dep. Comput. Sci. North. Kentucky Univ. Highl. Height. KY 41099*, pp. 136–141, 2011.

[51] Y. Zhang, L. He, and B. Fu, "Research on DNA Cryptography," *Appl. Cryptogr. Netw. Secur. Coll. Softw. Microelectron. Northwest. Polytech. Univ. Xi'an, China*, p. 376, 2012.

[52] R. Mor and P. Kanth, "A Review Paper Of DNA Based Cryptographic 1 1 1,2," no. April, pp. 31–33, 2015.

[53] 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.

[54] D. Prabhu and M. Adimoolam, "Bi-serial DNA Encryption Algorithm (BDEA)," *Journal*, no. Affiliated to Anna University of Technology, Chennai, 2011.

[55] D. Heider and A. Barnekow, "DNA-based watermarks using the DNA-Crypt algorithm.," *BMC Bioinformatics*, vol. 8, p. 176, Jan. 2007.

[56] 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.

[57] 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.

[58] H. M. Alshamlan, M. El, and B. Menai, "Solving Shortest Hamiltonion Path Problem Using DNA Computing," no. c, pp. 76–82, 2012.

[59] R. Terec, M. Vaida, L. Alboaie, and L. Chiorean, "DNA Security using Symmetric and Asymmetric Cryptography," vol. 1, no. 1, pp. 34–51, 2011.

[60] "https://netbeans.org/kb/docs/ide/oracle-db.html?print=yes#connect (Connecting to Oracle Database - NetBeans IDE Tutorial)." .

[61] SANS Institute, "https://www.sans.org/security-resources/.../DB_Credentials_Policy.doc DataBase Credentials Policy." 2006.

Appendices

Appendix A

Internal Conferences:

A. *Abdulraqeb Alselwi (Cyber Security and Bio-Inspired Network Intrusion Monitoring)School of Computing and Mathematical Sciences, Liverpool John Moores University, Liverpool, UK Conference 18th Annual Post-graduate Research conference 14-15 March 2012*

B. *Alselwi, B. Askwith, M. Madjid (Wireless Network Using DNA Inspired Network) School of Computing and Mathematical Sciences, Liverpool John Moores University, Liverpool, UK Conference PGNET 2014 The National Symposium on the Convergence of Telecommunications, Networking and Broadcasting 23-24 June 2014*