MOLECULAR BIOLOGY INSPIRED MUTUAL AUTHENTICATION SCHEMES FOR WIRELESS BODY AREA NETWORK

Esma Ergüner Özkoç[1] **, Mike Mannion*[2]

[1] Başkent University, Ankara; [2] Glasgow Caledonian University, Glasgow
[1]Turkey, [2]UK

* Corresponding Author: e-mail: eeozkoc@baskent.edu.tr

Abstract: As the use of Wireless Body Area Network (WBAN) becomes widespread, concerns about the security of the data they produce and transmit are also increasing. One of the basic security requirement for WBAN communication include authentication. In this study, a certificate-less mutual authentication scheme is proposed. The scheme was developed using pseudo-DNA cryptography techniques (due to its features such as randomness and rule less, easily generated and accessible, similarity to the binary system and no need for high-tech laboratory conditions) in addition to modern cryptography techniques, to increases the level of security without adding additional computational costs to the system.

Key words: Authentication, Pseudo DNA cryptography, DNA computing, Wireless Body Area Network-WBAN.

1. INTRODUCTION

A Wireless Body Area Network (WBAN) is a network of small wearable sensors and computing devices that can be attached to or located inside humans or animals. A WBAN can be used to collect, store and transfer health data e.g. heart rhythms, brain signals, temperature, blood pressure, blood glucose levels, and monitor the condition of a wearer's health. The data can be processed locally and/or transmitted for remote processing using a telephone or internet-enabled device, and in principle acted upon more quickly if necessary. WBANs are increasingly being used for applications across diverse sectors including telemedicine, health insurance, veterinary science, education, entertainment, sports, farming, soldiering [1]. The range is increasing as technical knowledge advances, especially in sensor technology (smaller sizes, less energy consumption, more computing capabilities), increases in battery longevity and the rollout of 5G communications.

Mutual authentication is a commonly used security practice in which communicating entities authenticate each other before actual communication occurs. Certificated mutual authentication occurs when encryption keys are generated by a trusted third-party certification authority or Key Generation Centre (KGC). This introduces the risk that the third party's security is compromised (the key escrow problem) [2]. In addition, for WBANs, in which data is constantly updated over a network e.g. location tracking, then adding third-party communications into the mutual authentication data transmissions protocols can increase performance runtime and computational costs. In certificate-less mutual authentication, both parties generate the required keys by themselves, verify each other and neither a certification authority nor a KGC are involved.

The design of a WBAN application needs to balance several qualities including effectiveness, computational efficiency, resource efficiency, security and often physical weight. Security is concerned with preventing damage, destruction, and unauthorized access or changes to data. Security enhancement mechanisms include authentication between communicating parties, maintaining data confidentiality, protecting data integrity, availability, access control and non-repudiation [3].

In molecular biology, a Deoxyribo Nucleic Acid (DNA) is a molecule that carries the genetic information (data and instructions) necessary for the vital functions and biological evolution of all organisms and some viruses. The genetic information is converted into functional products, many of which are proteins e.g. antibodies, enzymes that play important roles in our bodies. The genetic information conversion process is achieved by exposing DNA molecules to different specific chemical processes e.g. translation, transcription. In DNA (or Bio-) Computing the idea is that different information storage and processing problems we wish to solve are mapped on to a set of DNA Molecules. These molecules can then be exposed to a series of chemical processes that can replicate well known computational processes. The result is a new set of DNA molecules that represent possible solutions to the information storage and management problems. Since many of the chemical reactions execute in parallel, there is optimism that DNA Computing might offer significant process performance improvements on modern day computers. In addition, DNA offers significantly more efficient data storage, cheaper production costs, and reduced operational power consumption than silicon. Adelman's use of DNA molecules for a solution of the non-polynomial Hamiltonian path problem [4] is regarded as the beginning of DNA Computing. In practice, we are a long way from realizing DNA Computing, so the field of Pseudo DNA computing has emerged in which traditional solutions to current information storage and processing problems are being generated that imitate molecular biology information storage and processing approaches. Many DNA-based cryptography solutions have been proposed for encryption algorithms [5-7], image encryption algorithms [8, 9], OTP (One Time Pad) [10, 11], data hiding and steganography [12, 13] authentication [14,15] and watermarks [16]. Often solutions have been biochemical or by simulating DNA functions (Pseudo or Virtual DNA cryptography [17]).

This paper proposes a novel certificate-less mutual authentication scheme between a WBAN Client and an Application Provider that combines ideas from modern cryptography with those from molecular biology.

Section 1 gives related works and our contribution. Section 2 describes the architecture of a WBAN and presents an introduction to the fundamentals of molecular biology including Central Dogma, DNA structure and calculation principles. Section 3 explains the proposed WBAN authentication scheme in detail. A security analysis of the proposed method is presented in section 4. Section 5 sets out some conclusions.

1.1. Related Works

Sensors used in WBAN architectures are normally constrained by memory capacity, physical size, energy consumption needs, communication capability and processing power. These constraints can reduce security levels. For example, attackers can take the advantage of the low level of Signal-to-Noise-Ratio (SNR) of the WBANs, which can lead to an increase in packet loss rate, to make denial of service attacks. Attackers can also eavesdrop traffic between elements of a WBAN architecture and inject new messages into the system or replicate old messages. One of the basic security requirements for WBAN is the focus of this study: authentication.

Many authentication schemes have been developed to meet the authentication requirement of WBANs

(i) Non-cryptographic based schemes include physiological signal based, channel-based, and proximity-based schemes. These schemes generally are based on an assumption (for example, wearable sensors can measure the same type of electrocardiogram parameters), which limits the application scope of the approaches because it requires special hardware or software. Cryptographic schemes have less limitations in terms of special hardware/software compared to these schemes [18].

(ii) Cryptographic based schemes include public key infrastructure (PKI), identity-based cryptosystem (IBC) and elliptic curve cryptography (ECC). In PKI, a user's identity and public key require a certificate generated by the certification authority (CA), so issuing, managing, and maintaining certificates in these protocols is a challenge to be tackled. IBC-based methods were proposed [19] to avoid the certification problem. User credentials are used as public key and no certificate is needed. However, most of the IBC-based methods cannot provide user anonymity. ECC-based methods provide the same security level as other cryptographic methods with smaller key sizes to improve efficiency. However, ECC-based protocols require the clients to verify public keys through public-key certificates. Therefore, Shen et al. [20] suggested an ECC based certificate-less authentication scheme. Each method has strengths and weaknesses, and designing a WBAN authentication scheme that meets competing desired security requirements remains a complex challenge.

1.2. Our Contribution

By carefully exploring the characteristics of WBAN architectures and DNA structures we designed a pseudo-DNA inspired authentication scheme. Our contribution is twofold.

- We have adopted the molecular biology functions (translation, transcription) and Pseudo-DNA cryptography in addition to the modern cryptographic methods to the WBAN authentication scheme to strengthen security without additional computational cost.
- We have designed a certificate-less mutual authentication in which the WBAN Client and ASP authenticate each other and during the authentication phases a certification authority is not required.

2. PRELIMINARIES

For clarity, we present some basic information about WBAN architecture designs and information processing in molecular biology around which our proposals are based.

2.1. WBAN Architecture

Structurally, a WBAN is a set of nodes connected by short-range wireless communications. Figure 1 illustrates a WBAN Architecture.

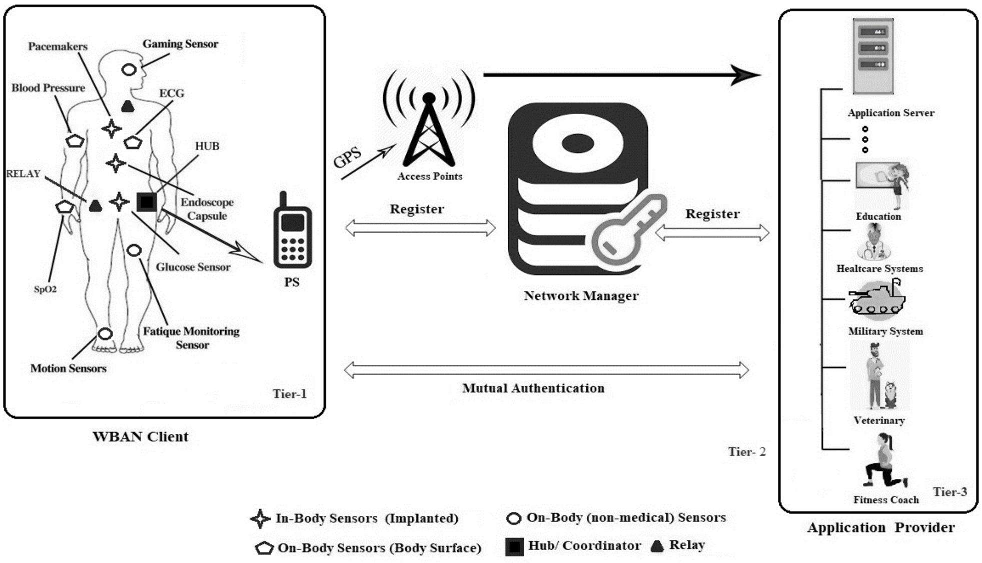


Figure 1 Overview of the WBAN Architecture

It contains three entities: (i) a WBAN Client configured as a set of sensors connected to the user that requests one or more services from an Application Provider (ii) a Network Manager (iii) an Application Provider that provides services through the network for an authenticated WBAN Client. These nodes are organized into three tiers [1]:

Tier-1 (User and WBAN Client) consists of the network infrastructure of nodes that collect data from the body and prepares the data for transmission outside the WBAN. The data is communicated to a Personnel Server (PS) (e.g. a mobile phone), which acts as a gateway and transfers the data to Tier 2.

Tier 2 (Network Architecture) consists of the Network Manager and a network infrastructure of Access Points. The Network Manager is used to generate a unique code at registration. The Personnel Server communicates through Access Points. Basically, at this tier communication tries to connect WBANs to other networks.

Tier 3 (AP) consists of the network infrastructure of the AP which communicate with the WBAN Personnel Server.

2.2. Certificate-less Mutual Authentication

In this paper a certificate-less mutual authentication scheme is proposed to enhance the security of the data that is transmitted between a WBAN Client with a PS in Tier1 and an Application Provider in Tier3. Mutual authentication is a process of authenticating data passed between two parties in a communications link. In a WBAN environment, the WBAN Client authenticates the Application Provider and vice-versa. In traditional cryptography, encryption keys are generated by a trusted certification authority or Key Generation Centre (KGC). In certificate-less cryptography, both parties generate the required keys by themselves, verify each other and neither a certification authority nor a KGC are involved, which minimizes the risk of the third party being compromised (the key escrow problem).

The certificate-less mutual authentication process consists of 3 phases: Registration, Login and Authorization, and Password Changing. Registration is performed only once for each user and the initial values of the parameters that the parties will need during the login and authorization are assigned i.e. WBAN Client identifier and password. When a User wishes to use the WBAN application services, the WBAN Client connects to the Application Provider server, whereupon the Login and Authentication phase is initiated and the User enters the identifier and password that were set up during Registration. A Network Manager is not required for Login and Authentication and the WBAN Client can change the password without the participation of a Network Manager or an Application Provider. The Password Changing phase is performed when the WBAN Client requests to change the password during the Registration phase.

2.3. Molecular Biology Background

This section provides some foundational information about DNA and Central Dogma.

DNA structures (“Information structures”). Genes frame each person’s unique identity and how their body responds to different external stimuli. Gene expression is the process by which the information encoded in a gene is used to direct the assembly of proteins, large complex molecules that maintain the structure and function of the body's tissues and organs.

DNA molecules can be as long as several hundred million nucleotides. Each nucleotide consists of a nitrogenous base, a sugar and a phosphate group. The nitrogenous base can be one of Adenine (A), Cytosine (C), Guanine (G) and Thymine (T). Sequences of nucleotides are categorized as exons or introns. Exons are used for the protein formation process. Introns are not.

A DNA molecule is structured as a double helix (Watson - Crick Model) i.e. two strands of connected nucleotide chains are twisted around each other. A nucleotide in one strand is paired with a nucleotide in the other strand. Those with base A are always paired with those with base T. Those with base C pair are always paired with those with base G. A DNA Strand can be viewed as a word over the four-letter alphabet (A, C, G, T).

Central Dogma ("Information Processing"). The principal process steps of gene expression are known as the Central Dogma. The Central Dogma sets out that the genetic information held in DNA molecules is converted from DNA to Ribo Nucleic Acid (RNA) to functional products. The most common functional products are proteins. Each RNA molecule is formed as a chain of nucleotides and is usually single-stranded. The genetic information conversion from DNA to RNA is known as Transcription. The conversion of RNA to proteins is known as Translation.

(i) Transcription: The DNA structure is considered to have two strands, a Template Strand and Non-Template Strand. The RNA structure is formed by taking the complement of the Template strand in the DNA Structure but replacing Thymine (T) with Uracil (U). The RNA structure becomes almost identical to the Non-Template strand in the DNA structure but with Us replacing Ts. Table 1 shows an example of RNA Structure formed from a DNA structure. The shaded highlighted elements are the Introns.

Table 1. Example of a Transcription Process

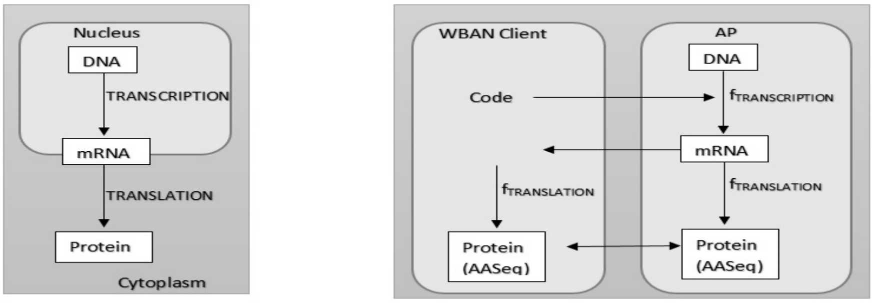
DNA Structure	
Non-Template Strand	*ATG TAC GTT AGA GTG CAA GTG CGT GTT AGT ACA TTC ACT TTC GCC AAT*
Template Strand	*TAC ATG CAA TCT CAC GTT CAC GCA CAA TCA TGT AAG TGA AAG CGG TTA TTA*
RNA Structure (first pass – take complement of DNA Template Strand and replace Ts with Us)	
	AUG UAC GUU AGA GUG CAA GUG CGU GUU AGU ACA UUC ACU UUC GCC AAU UUA
RNA Structure (second pass – remove Introns)	
	AUG UAC GUU AGA GUG ~~CAA GUG~~ CGU GUU ~~AGU ACA~~ UUC ACU UUC ~~GCC AAU~~ UUA

(ii) Translation: After transcription, the RNA structure is translated into a Protein structure by mapping each 3-letter RNA triplet (reading left to right) to a protein element called a codon using a genetic code table. Some triplets are especially reserved e.g. AUG is a commonly used to indicate the start of the protein, UAA is commonly used to indicate the end of the protein. Table 2 shows the how the RNA Structure in Table 1 is mapped to a Protein Structure.

Table 2. Example of a Translation Process

RNA Structure	
	AUG UAC GUU AGA GUG ~~CAA GUG~~ CGU GUU ~~AGU ACA~~ UUC ACU UUC ~~GCC AAU~~ UUA
Protein Structure	
	START *Tyr Val Arg Val Arg Val Phe Thr Phe* ***STOP***

Central Dogma and Authentication Analogy. In this paper the processes of transcription and translation are imitated in a certificate-less mutual authentication scheme. The "protein" is the authenticated security code. Only one DNA sequence is stored in the Application Provider. Many users can be verified by the system by producing different security codes, none of which are stored in the system. If a WBAN Client and the Application Provider produce the same security code, they authenticate each other. The WBAN Client can produce a security code without knowing the entire DNA only with the code information that they have. Figure 2 demonstrates the analogy of the Central dogma in a cell and Authentication scheme.



(a) Central Dogma in a cell (b) Central Dogma in a proposed authentication scheme

Figure 2. Central Dogma and Authentication Analogy

3. PROPOSED CERTIFICATE-LESS MUTUAL AUTHENTICATION SCHEME

In this section, a proposed WBAN certificate-less mutual authentication scheme to ensure secure data transmission between a WBAN Client (Tier-1) and an Application Provider (Tier-3) will be explained. The Scheme has three phases.

Transcription Function ($f_{TRANSCRIPTION}$): This function receives a DNA sequence and "Code" information (Start region, End region, Intron Regions -regions to be extracted from RNA-) as input. The function then creates an mRNA string corresponding to the DNA template string which is given as input and extracts the relevant regions according to the "Code" information (1). In the Registration phase, the Network Manager provides Coding Information in the form of the length of the start and end regions, the number of Intron regions and the length of the Intron region (including fix or variable) composing the Code. The specified Code information is determined by Network Manager and written to the client's device (PS) should be determined according to the security requirement of the related WBAN.

$$f_{TRANSCRIPTION}(DNA, Code) = mRNA \tag{1}$$

Translation Function ($\boldsymbol{f_{TRANSLATION}}$): The function takes mRNA data, the output of the transcription function, as input. The function generates the amino acid sequence (AAseq) determined according to the previously defined codon data (except the start and stop codon) (2). Every WBAN can create their own Codon dictionary according to their needs. In addition, groups consisting of more bases can be created instead of triple base groups.

$$f_{TRANSLATION}(mRNA, Code) = \text{AAseq} \tag{2}$$

Pseudo DNA Computing

For Pseudo DNA computing, the DNA bases A, T, C, and G are each represented by a binary string. Table 1 shows a range of different possibilities. All the logical operations can be performed over DNA bases like XOR, AND, OR, XNOR, NOT and binary coding for the DNA bases could be changed. In Table 4, eight kinds of binary code conversion are given for DNA bases. If the first conversion type {A↔ 00, T↔ 11, G↔01, C↔10} is chosen from Table 4, the corresponding results for XOR operation are given in Table 5. In the proposed scheme, the XOR operation is used between the identity of the WBAN Client and the DNA sequence. Any encoding map rule for DNA calculation can be selected. There are no restrictions on the selection.

Table 4. Kinds of schemes encoding map rule of DNA sequence

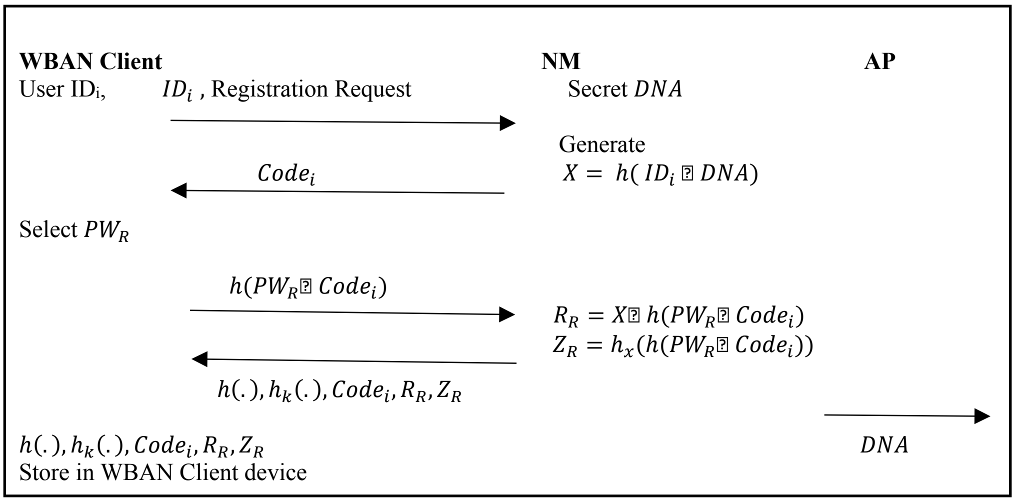
DNA Base	***Binary Code***							
A	*00*	*00*	*01*	*01*	*10*	*10*	*11*	*11*
T	*11*	*11*	*10*	*10*	*01*	*01*	*00*	*00*
G	*01*	*10*	*00*	*11*	*00*	*11*	*01*	*10*
C	*10*	*01*	*11*	*00*	*11*	*00*	*10*	*01*

Table 5. XOR operation for DNA sequence for the case: A- 00 T- 11 G-01 C-10

XOR	*A*	*T*	*G*	*C*
A	*A*	*T*	*G*	*C*
T	*T*	*A*	*C*	*G*
G	*G*	*C*	*A*	*T*
C	*C*	*G*	*T*	*A*

3.1. Registration Phase

Registration is performed only once. A User Identifier and Password are sent from the WBAN Client to the Network Manager. The Network Manager generates a unique DNA Strand which is used to generate an encrypted Registration Identifier, ZR, which is a function of User Identifier, Password and a subset of the DNA Strand. The DNA Strand is passed to the AP. The hashed Registration Identifier is passed to the WBAN Client. The steps of this phase are summarised in Figure 3.



WBAN Client
NM
AP
User IDi,
ID_i , Registration Request
Secret DNA
Generate
$X = h(ID_i \square DNA)$
$Code_i$
Select PW_R
$h(PW_R \square Code_i)$
$R_R = X \square h(PW_R \square Code_i)$
$Z_R = h_x(h(PW_R \square Code_i))$
$h(.), h_k(.), Code_i, R_R, Z_R$
DNA
$h(.), h_k(.), Code_i, R_R, Z_R$
Store in WBAN Client device

Figure 3. Registration phase of the proposed scheme

i. When a User i registers, the WBAN Client sends a registration request for ID_i to the Network Manager.

ii. The Network Manager randomly generates a DNA strand e.g. from known databases. From this strand, the data structure *Code_i* is constructed, which consists of <Start region, Stop region, the Intron regions> and is returned to the WBAN Client. The Network Manager also calculates $X = h(ID_i \square DNA)$.

iii. User i selects a password, PW_R whereupon the WBAN Client calculates $h(PW_R \square Code_i)$, and sends it to the Network Manager. The use of a hash function prevents a user's password from being seen by a system administrator.

iv. The Network Manager calculates $R_R = X \square h(PW_R \square Code_i)$ and $Z_R = h_x(h(PW_R \square Code_i))$ and returns these to the WBAN Client to be used in the *Login* and *Authentication* phases.

v. $Code_i$, R_R and Z_R values and used hash functions are stored in WBAN client device. In addition to these generated DNA is passed to the AP over secure network.

3.2. Login and Authentication Phase

The *Login and Authentication* phase is implemented between the WBAN Client and the Application Provider. At Login, the WBAN Client uses the User Identifier and Password deployed at Registration. The steps of this phase are summarised in Figure 4.

i. User i enters ID$_i$ and PW_L. The WBAN Client calculates $h(PW_L\boxed{?}\ Code_i\ )$ and X' is calculated. X' is used as a key for a hash function to calculate Z'. If calculated Z' and Z_R are equal then User i has entered the correct password. If Z' and Z_R are not equal then the login request is rejected.

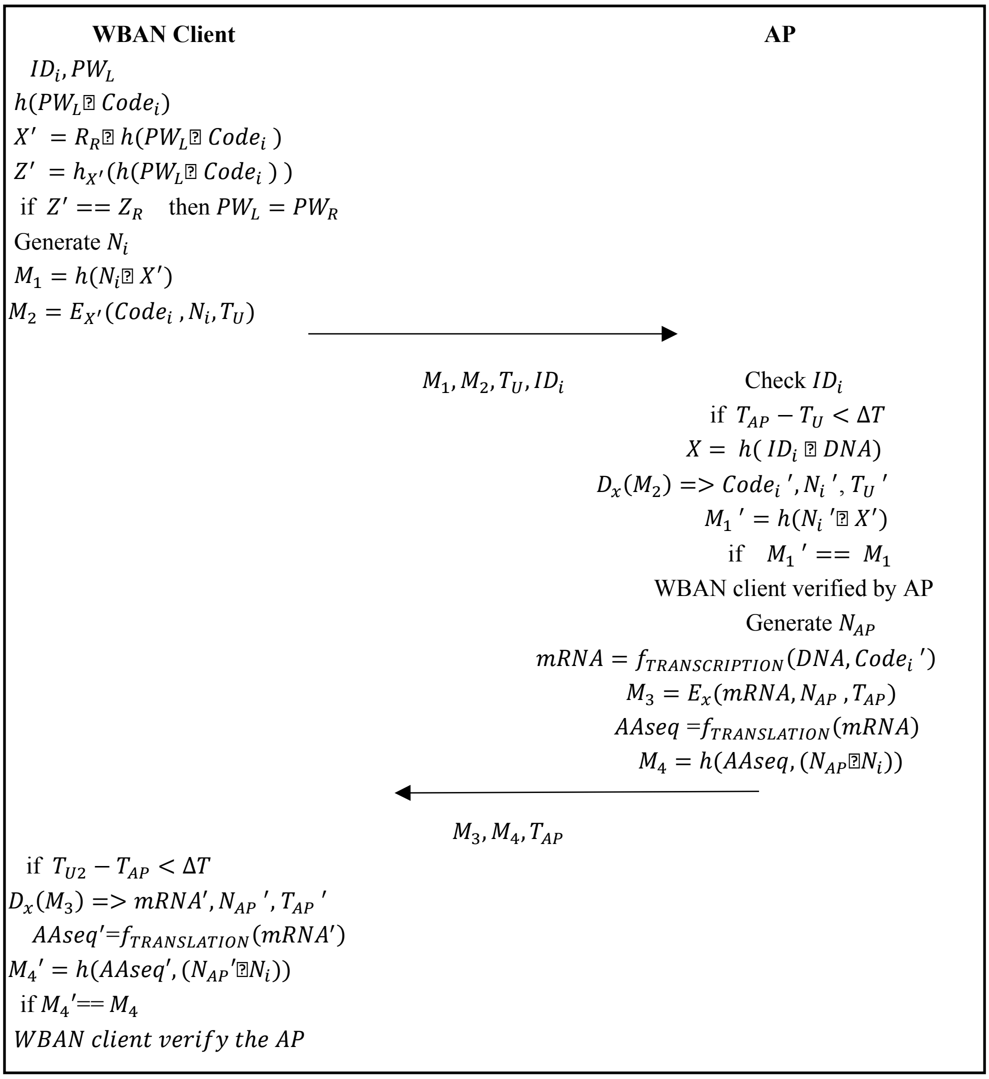
ii. If the PW_L is verified, the WBAN Client generates a nonce value (randomly generated number any used only once for each login) N_i and calculates $M_1 = h(N_i\boxed{?}\ X')$. The WBAN Client compose M_2 by encrypting the $Code_i$, N_i and current timestamp T_U . It then sends "M_1, M_2, T_U, ID_i" to the Application Provider.

iii. When the Application Provider receives the message, it checks if ID_ia valid user identifier is or not. If ID$_i$ is valid then the Application Provider checks T$_U$ to confirm that the message was within a reasonable time interval (ΔT). If any of these checks fail then the login request is rejected. Otherwise the Application Provider calculates X to decrypt the M_2. After decrypting M_2, a concatenated T_U is constructed from the message to obtain $Code_i\ '$ and $N_i\ '$. Then calculates $M_1\ '$ by using obtained $N_i\ '$ from decryptedM_2. If calculated $M_1\ '$ and received M_1 is equal then the Application Provider authenticates the WBAN Client.

iv. The Application Provider generates a nonce value N_{AP}, and then calculates an $mRNA$ by using a $f_{TRANSCRIPTION}$ function (details are given in previous section). After transcription of the $mRNA,$ the Application Provider calculates $M_3 = E_x(mRNA, N_{AP}\ , T_{AP})$ and $AAseq$ by using a $f_{TRANSLATION}$ function. This function produces an aminoacid sequence from $mRNA$ according to a predefined conversion table between the Application Provider and the WBAN Client. And calculates M_4, hash of the $AAseq$ and $(N_{AP}\boxed{?}N_i\ ')$. The Application Provider sends "$M_3, M_4,\ T_{AP}$ " to the WBAN Client.

v. The WBAN Client checks the Timestamp validity that the message is received in reasonable time interval (ΔT) then decrypts the M_3 and obtains the $mRNA', N_{AP}\ '$and $T_{AP}\ '$. Calculates $AAseq'$ by using $mRNA'$. Then calculates $M_4' = h(AAseq', (N_{AP}'\boxed{?}N_i))$. If calculated $M_4\ '$ and received

M_4 is equal then WBAN Client authenticate Application Provider. At the end of this phase both parties (Application Provider and WBAN Client) are authenticates each other (mutual authentication). After this phase $(N_{AP}'\square N_i)$ can be used as a session key for the rest of the communication between Application Provider and WBAN Client.



WBAN Client

AP

ID_i, PW_L

$h(PW_L\square\ Code_i)$

$X' = R_R\square\ h(PW_L\square\ Code_i)$

$Z' = h_{X'}(h(PW_L\square\ Code_i))$

if $Z' == Z_R$ then $PW_L = PW_R$

Generate N_i

$M_1 = h(N_i\square\ X')$

$M_2 = E_{X'}(Code_i, N_i, T_U)$

M_1, M_2, T_U, ID_i

Check ID_i

if $T_{AP} - T_U < \Delta T$

$X = h(ID_i \square\ DNA)$

$D_x(M_2) => Code_i', N_i', T_U'$

$M_1' = h(N_i'\square\ X')$

if $M_1' == M_1$

WBAN client verified by AP

Generate N_{AP}

$mRNA = f_{TRANSCRIPTION}(DNA, Code_i')$

$M_3 = E_x(mRNA, N_{AP}, T_{AP})$

$AAseq = f_{TRANSLATION}(mRNA)$

$M_4 = h(AAseq, (N_{AP}\square N_i))$

M_3, M_4, T_{AP}

if $T_{U2} - T_{AP} < \Delta T$

$D_x(M_3) => mRNA', N_{AP}', T_{AP}'$

$AAseq' = f_{TRANSLATION}(mRNA')$

$M_4' = h(AAseq', (N_{AP}'\square N_i))$

if $M_4' == M_4$

$WBAN\ client\ verify\ the\ AP$

Figure 4. Login and Authentication phase of the proposed scheme

3.3. Password Change Phase

The Change Password mode is performed when the WBAN Client requests to change the password after the Registration phase. The Network Manager or the ASP are not required for Password Changing. Figure 5 shows that when a User I first enters their password into his / her device, the WBAN Client verifies the password. If the entered password is correct, a password change request can be accepted and the User is prompted to enter a new password. The R_R and Z_R values stored in the client device are calculated with the new password and the old values are updated.

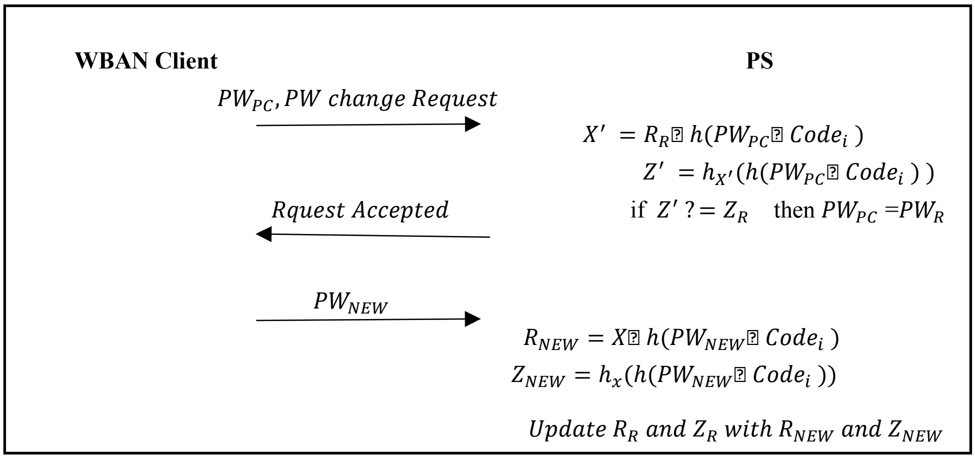

WBAN Client
PS
$PW_{PC}, PW\ change\ Request$
$X' \ = R_R\square\ h(PW_{PC}\square\ Code_i\ )$
$Z' \ = h_{X'}(h(PW_{PC}\square\ Code_i\ )\ )$
$Rquest\ Accepted$
if $Z'\ ?= Z_R$ then PW_{PC} =PW_R
PW_{NEW}
$R_{NEW}\ = X\square\ h(PW_{NEW}\square\ Code_i\ )$
$Z_{NEW}\ = h_x(h(PW_{NEW}\square\ Code_i\ ))$
$Update\ R_R\ and\ Z_R\ with\ R_{NEW}\ and\ Z_{NEW}$

Figure 5. Password change phase of the proposed scheme

4. SECURITY ANALYSIS

The password or verification table are not stored at neither Application Provider nor Network Manager. Thus, any **stolen verifier attack** cannot be successful. In registration phase, client can choose password, and later client easily update password without intervention of Application Provider or Network Manager. And client's password is not stored at any point on the Network. In login and authentication phase and registration phase, password is protected by cryptographic hash function (pre-image resistance) so that nobody can see the plain password including system administrator.

Proposed scheme is resist to **stolen device attacks** if the attacker obtains a WBAN Client device in which the $Code_i$ is embedded, attacker cannot calculate the $h(PW\square\ Code_i)$. Even if the R and Z values stored in the device are obtained the client's password cannot be obtained. And nobody can change password without knowing existing password. It avoids denial of service attack using stolen device.

Password is not transmitted during the login and authentication phase that nobody can steal it from messages between user and remote system. (**Man in the middle, Eavesdropping**). If the user enters the wrong password during the login and authentication phase, the wrong password can be easily detected on the client device (PS) without Application Provider or Network Manager interaction.

Mutual authentication is performed. So that both **server spoofing** and **user impersonation attack** are prevented. A server spoofing is an attack in which malicious person or program masquerading as a Network Manager or Application Provider in order to access confidential information about the user. Proposed scheme can prevent this type of attack by using Secret DNA of Network Manager which is also stored in Application Provider.

Proposed scheme resist to **replay attack**: randomly N_u, N_{AP} values are generated in each session. Nonce values $\{N_u, N_{AP}\}$ are not transmitted over insecure network as plain. They are protected with cryptographic hash function or encryption algorithms. In addition, if an attacker wants to replay the authentication messages in login and authentication phase, first he/she must choose a valid Timestamps then must calculate the corresponding values $\{M_2, M_3\}$ that is depend on $\{T_{AP}, T_U\}$ and randomly generated nonce values $\{N_u, N_{AP}\}$. It is fairly difficult task for proposed scheme thus attacker cannot validate himself as a legal parties.

Proposed scheme has resistance to **active attack** and **revelation of message content**. Messages sent/received during login and authentication phase are not in plain text format. All the transmitted messages are hashed with secure one-way (or Keyed) hash function or Encrypted. In addition to these the method does not require a certification authority, therefore it is called certificate-less scheme. The values produced / calculated as keys are used in encryption algorithms.

5. CONCLUSION AND DISCUSSION

WBAN security is still in its infancy even though there have been many studies on it. In this study, certificate-less mutual authentication scheme for WBAN Client and Application Provider is proposed which security is enhanced by using pseudo-DNA cryptography in addition to modern cryptography. Proposed scheme has resistance to stolen verifier table attack, server spoofing attack, revelation of message content, active attack and replay attack.

In this study, considering the WBAN system as a living organism, we have designed the authentication system for the WBAN system who has a DNA stored by Network Manager and Application Provider. We adapted the transfer of genetic information necessary for protein production in the cell from DNA to RNA using two basic functions (translation and transcription) in the verification scheme. Briefly, protein synthesis was simulated by using the code information in the WBAN Client and DNA in the Application Provider. It is assumed that authentication is successful if the same protein is synthesized on both sides.

In reality, the three nucleotides correspond to an amino acid and there are 61 different amino acids (excluding start-end). While realizing this structure in the cell with the translation function in the proposed scheme; values such as codon length, distinct amino acid number and synthesized protein length are left open. These values can be determined according to the criteria such as the number of users of the application, the security requirement, and a codon dictionary can be created. The same is true for WBAN DNA length.

In future studies, by adding elliptic curve cryptography to the pseudo-DNA cryptography security level can be strengthened. Although the user passwords are not stored in the proposed system, the IDs of the users are kept in the Application Provider, but the Application Provider cannot match the ID and the real person. In addition, the ID can be tracked by the adversary as the ID is explicitly sent in the login messages. In this case, it can be said that the method provides semi-user anonymity. For this reason full user anonymity can be considered within the scope of future studies to protect the clients' privacy.

In addition, it is predicted that real DNA will be used in WBAN authentication schemes in the future. Considering the advantages of DNA computing, the integrated operation of DNA microprocessors with WBAN sensors positioned under the skin will be a prominent topic of study.

REFERENCES

[1] Polai, M., Mohanty, S., & Sahoo, S. S. A Lightweight Mutual Authentication Protocol for Wireless Body Area Network. *6th IEEE International Conference on Signal Processing and Integrated Networks (SPIN)*, March 2019, pp. 760-765.

[2] Arfaoui, A., Boudia, O. R. M., Kribeche, A., Senouci, S. M., & Hamdi, M. Context-aware access control and anonymous authentication in WBAN. *Computers & Security*, 88, 101496, 2020

[3] Shihong Zou, Yanhong Xu, Honggang Wang, Zhouzhou Li, Shanzhi Chen, Bo Hu, A Survey on Secure Wireless Body Area Networks, *Security and Communication Networks*, vol. 2017, Article ID 3721234, 2017 (9 p.). https://doi.org/10.1155/2017/3721234

[4] Adleman, L.M. Molecular computation of solutions to combinatorial problems. *Nature*, 369, 1994, p.40.

[5] Cui, G., Qin, L., Wang, Y., & Zhang, X. An encryption scheme using DNA technology. *3rd IEEE International Conference on Bio-Inspired Computing: Theories and Applications*, 2008, pp. 37-42.

[6] Prabhu, D. and Adimoolam, M. Bi-serial DNA Encryption Algorithm (BDEA). *arXiv preprint* arXiv:1101.2577, 2011.

[7] Wang, X., Zhang, Q. and Wei, X.P. A new encryption method based on Rijndael algorithm and DNA computing. *In Applied Mechanics and Materials*, Vol. 20, 2010, pp. 1241-1246. https://doi.org/10.4028/www.scientific.net/AMM.20-23.1241

[8] Maniyath, S.R. and Supriya, M. An uncompressed image encryption algorithm based on DNA sequences. *Computer Science and Information Technology*, 2, 2011, pp.258-270.

[9] Zhou, C., Wei, X., Zhang, Q. and Liu, R. DNA sequence splicing with chaotic maps for image encryption. *Journal of Computational and Theoretical Nanoscience*, Vol. 7, No. 10, 2010, pp.1904-1910.

[10] Borda, M., & Tornea, O. DNA secret writing techniques. *2010 IEEE 8th International Conference on Communications*, June 2010, pp. 451-456.

[11] Gehani, A., LaBean, T. and Reif, J. DNA-based cryptography. *Lecture notes in computer science*, 2950, 2003, pp.167-188.

[12] Liu, H., Lin, D. and Kadir, A. A novel data hiding method based on deoxyribonucleic acid coding. *Computers & Electrical Engineering,* Vol. 39, No. 4, 2013, pp.1164-1173.

[13] Tuncer, T. and Avci, E. A reversible data hiding algorithm based on probabilistic DNA-XOR secret sharing scheme for color images. *Displays*, 41, 2016, pp.1-8.

[14] Raju, P.V.S.N. and Parwekar, P. DNA Encryption Based Dual Server Password Authentication. *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications* (FICTA), Springer, Cham, 2014, pp. 29-37.

[15] Vijayakumar P., Vijayalakshmi V. and Zayaraz G. DNA based Password Authentication Scheme using Hyperelliptic Curve Cryptography for Smart Card. *Proc. of Int. Conf. on Recent Trends in Information, Telecommunication and Computing,* 2014, pp. 517-523.

[16] Lee, S.H., 2014. DWT based coding DNA watermarking for DNA copyright protection. *Information Sciences*, 273, pp.263-286.

[17] Saeed Al-Wattar A.H. et al. Review of DNA and Pseudo DNA cryptography, *International Journal of Computer Science and Engineering (IJCSE)*, vol. 4, No. 4, 2015, pp. 65-76.

[18] Li, X., Ibrahim, M. H., Kumari, S., Sangaiah, A. K., Gupta, V., Choo, K. K. R. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. *Computer Networks*, 129, 2017, pp. 429-443.

[19]. Shamir, A., Identity based cryptosystems and signature schemes. In: *Proceedings of CRYPTO'84*, 1984, pp. 47–53.

[20] Shen J, Gui Z, Ji S, Shen J, Tan H, Tang Y. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. *Journal of Network and Computer Applications,* Elsevier, 106, 2018, pp. 117–123

Information about the authors:

Esma Ergüner Özkoç –is an Assistant Professor (Ph.D.) in the field of Management Information Systems at Başkent University. Her teaching and research interests cover such disciplines as; bioinformatics, Information Security, Cryptography and MIS.

Mike Mannion –is the current Dean of the School of Computing, Engineering and Built Environment and is also a Professor in the Department of Computing at Glasgow Caledonian University. His research interests include, but are not limited to software engineering, network management and artificial intelligence.

Manuscript received on 18 February 2021